En ny säkerhetsskyddslag

Betänkande av
Utredningen om säkerhetsskyddslagen

Stockholm 2015

STATENS OFFENTLIGA UTREDNINGAR

SOU 2015:25

SOU och Ds kan köpas från Fritzes kundtjänst.
Beställningsadress: Fritzes kundtjänst, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: order.fritzes@nj.se
Webbplats: fritzes.se

För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer
på uppdrag av Regeringskanslets förvaltningsavdelning.
Svara på remiss – hur och varför.
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02)
En kort handledning för dem som ska svara på remiss. Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remiss.

Layout: Kommittéservice, Regeringskansliet.
Omslag: Elanders Sverige AB.
Tryck: Elanders Sverige AB, Stockholm 2015.

ISBN 978-91-38-24258-2
ISSN 0375-250X

Till statsrådet Anders Ygeman

Regeringen beslutade den 8 december 2011 att tillkalla en särskild utredare med uppdrag att göra en översyn av säkerhetsskyddslagstiftningen för att bättre anpassa den till det som krävs för att skydda verksamhet som har betydelse för rikets säkerhet och till de krav det internationella samarbetet ställer.

F.d. justitierådet och ordföranden i Högsta förvaltningsdomstolen Sten Heckscher förordnades att fr.o.m. den 8 december 2011 vara särskild utredare.

Förordnad sakkunnig har under hela utredningstiden varit f.d. generaldirektören Nils Gunnar Billinger.

Förordnade experter under hela eller delar av utredningstiden har varit chefsjuristen Bertil Persson (Affärsverket svenska kraftnät), rättssakkunniga Mats Rundström (Finansdepartementet), chefsjuristen Anders Sjöborg (Försvarets materielverk), numera justitiesekreteraren Chris Stattin Larsson, rättssakkunniga Evelina Säfwe, rättssakkunniga Izla Staifo och numera ämnesrådet Göran Olsson (Försvarsdepartementet), översten Roger Nordh (Försvarsmakten), numera departementsrådet John Ahlberk, rättssakkunniga Stefan Jansson och kanslirådet Ida Wettervik (Justitiedepartementet), chefsjuristen Key Hedström (Myndigheten för samhällsskydd och beredskap), juristen Ulrica Clerton (Polismyndigheten), juristen Britt-Marie Jönson (Post- och telestyrelsen), kanslichefen Eva Melander Tell, numera justitiesekreteraren Emily Alfvén Nickson, numera rådmannen Patrik Skogh och enhetschefen Ulrika Söderqvist (Säkerhets- och integritetsskyddsnämnden), numera biträdande säkerhetspolischefen Johan Sjöö och numera sektionschefen Annette Norman (Säkerhetspolisen), juristen Thomas Wallander (Totalförsvarets forskningsinstitut), f.d. enhetschefen Göran Berg och numera säkerhetsskyddschefen Jens Johanson (Transportstyrelsen) och f.d. departementsrådet Berndt Fredriksson (Utrikesdepartementet).

Som sekreterare anställdes den 23 januari 2012 hovrättsassessorn Karin Erlandsson, den 14 maj 2012 numera kanslichefen Helene Lövung och den 1 september 2013 avdelningsdirektören Martin Waern. Helene Lövung entledigades den 1 januari 2014.

Numera ämnessakkunniga Lotta Skarp har varit anställd som biträdande sekreterare mellan den 1 april 2012 och den 31 mars 2013.

Förordnandetider för experterna framgår av en förteckning som bifogas.

Tilläggsdirektiv beslutades av regeringen den 6 februari 2014 och den 11 september 2014 varigenom utredningstiden förlängdes.

Utredningens uppdrag är genom detta betänkande slutfört.

Sten Heckscher är ensam utredningsman och svarar ensam för innehållet i betänkandet. Experterna har deltagit i arbetet i sådan utsträckning att det trots detta är befogat att använda vi-form i betänkandet. Skilda uppfattningar i enskildheter och beträffande formuleringar kan förekomma utan att detta har behövt komma till uttryck i något särskilt yttrande.

Stockholm i mars 2015

Sten Heckscher

/Karin Erlandsson
Martin Waern

Förteckning över förordnandetider

Förordnad sakkunnig

F.d. generaldirektören Nils Gunnar Billinger fr.o.m. den 16 februari 2012

Förordnade experter

Numera departementsrådet John Ahlberk fr.o.m. den 16 februari 2012 t.o.m. den 31 juli 2012

F.d. enhetschefen Göran Berg fr.o.m. den 16 februari 2012 t.o.m. den 21 maj 2013

Juristen Ulrica Clerton fr.o.m. den 16 februari 2012

F.d. departementsrådet Berndt Fredriksson fr.o.m. den 16 februari 2012

Chefsjuristen Key Hedström fr.o.m. den 16 februari 2012

Juristen Britt-Marie Jönson fr.o.m. den 16 februari 2012

Numera justitiesekreteraren Chris Stattin Larsson fr.o.m. den 16 februari 2012 t.o.m. den 10 mars 2013

Numera sektionschefen Annette Norman fr.o.m. den 16 februari 2012

Numera ämnesrådet Göran Olsson fr.o.m. den 16 februari 2012 t.o.m. den 24 augusti 2014 (för Försvarsmakten) och fr.o.m. den 25 augusti 2014 (för Försvarsdepartementet)

Chefsjuristen Bertil Persson fr.o.m. den 16 februari 2012

Rättssakkunniga Mats Rundström fr.o.m. den 16 februari 2012

Chefsjuristen Anders Sjöborg fr.o.m. den 16 februari 2012

Numera biträdande säkerhetspolischefen Johan Sjöö fr.o.m. den 16 februari 2012

Kanslichefen Eva Melander Tell fr.o.m. den 16 februari 2012 t.o.m. den 25 september 2012

Juristen Thomas Wallander fr.o.m. den 16 februari 2012

Rättssakkunniga Stefan Jansson fr.o.m. den 16 april 2012 t.o.m. den 30 november 2013

Numera justitiesekreteraren Emily Alfvén Nickson fr.o.m. den 26 september 2012 t.o.m. den 19 mars 2013

Rättssakkunniga Evelina Säfwe fr.o.m. den 11 mars 2013 t.o.m. den 5 maj 2014

Enhetschefen Ulrika Söderqvist fr.o.m. den 20 mars 2013 t.o.m. den 30 september 2013 och fr.o.m. den 20 oktober 2014

Numera säkerhetsskyddschefen Jens Johanson fr.o.m. den 22 maj 2013

Numera rådmannen Patrik Skogh fr.o.m. den 1 oktober 2013 t.o.m. den 19 oktober 2014

Kanslirådet Ida Wettervik fr.o.m. den 1 november 2013

Rättssakkunniga Izla Staifo fr.o.m. den 6 maj 2014 t.o.m. den 24 augusti 2014

Översten Roger Nordh fr.o.m. den 20 oktober 2014

Innehåll

Sammanfattning

Förslag

Vi föreslår att säkerhetsskyddslagen ersätts av en ny lag. Även den nya lagen bör benämnas säkerhetsskyddslag. En ny lag ska svara mot de förändrade kraven på säkerhetsskyddet, bl.a. avseende utvecklingen på informationsteknikområdet, en ökad internationell samverkan, en ökad sårbarhet i samhällsviktiga funktioner och att säkerhetskänslig verksamhet i allt större omfattning bedrivs i enskild regi.

En bredare ansats för lagen innebär bl.a. att tillgänglighets- och riktighetsaspekterna av information och it-system lyfts fram. På detta sätt vidgas tillämpningsområdet till att ge ett skydd för informationstillgångar i samhällsviktig verksamhet som inte behöver ett skydd från ett konfidentialitetsperspektiv.

Den nya lagen ska medge ett nyanserat säkerhetsskydd som bygger på fyra informationssäkerhetsklasser av internationell modell. Informationssäkerhetsklasserna påverkar utformningen av säkerhetsskyddsåtgärderna informationssäkerhet, fysisk säkerhet och personalsäkerhet. Säkerhetsskyddsanalysen får en central roll och ska leda till slutsatser om hur säkerhetsskyddet i en verksamhet bör utformas. Vad verksamhetsansvaret innebär i fråga om säkerhetsskydd förtydligas.

Lagen ska på ett tydligare sätt än i dag ge stöd för internationella säkerhetsskyddsåtaganden och internationell samverkan, bl.a. genom möjligheten att utfärda säkerhetsintyg för personer och leverantörer.

Uppdraget

Ett huvudsyfte med uppdraget är att modernisera regleringen och att bättre anpassa den till det som krävs för att skydda verksamhet som har betydelse för Sveriges säkerhet och till de krav det internationella samarbetet ställer.

Bakgrund

Den gällande regleringen

Säkerhetsskydd ska i den omfattning som behövs finnas vid verksamhet hos staten, kommunerna och landstingen, hos juridiska personer som staten, kommunerna eller landstingen utövar ett rättsligt bestämmande inflytande över samt hos enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Säkerhetsskyddet ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet), att obehöriga får tillträde till platser där de kan få tillgång till sådana uppgifter eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning) samt att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning). Säkerhetsskyddet ska även i övrigt förebygga terrorism.

Säkerhetsskyddslagen innehåller också bestämmelser om skyldighet att i vissa fall teckna säkerhetsskyddsavtal vid anlitande av leverantörer samt om utbildning, kontroll och tillsyn. Närmare bestämmelser om säkerhetsskydd finns i den till lagen hörande säkerhetsskyddsförordningen.

Närliggande reglering

Av betydelse för säkerhetsskyddet är bl.a. reglering avseende luftfartsskydd, hamnskydd och sjöfartsskydd, reglering om kärnteknisk verksamhet och strålskydd, skydd för landskapsinformation och reglering avseende samhällsskydd och beredskap. Vidare finns ett nära

samband mellan säkerhetsskyddslagstiftningen och reglerna om upphandling på försvars- och säkerhetsområdet.

Folkrättsliga förpliktelser avseende säkerhetsskydd

Sveriges internationella säkerhetsskyddsåtaganden har ökat markant, bl.a. när det gäller generella säkerhetsskyddsöverenskommelser med andra stater och mellanfolkliga organisationer.

Syftet med en generell säkerhetsskyddsöverenskommelse är att två eller flera länder (eller mellanfolkliga organisationer) på ett säkert sätt ska kunna utbyta uppgifter som berör nationell säkerhet.

Av internationella åtaganden följer att det ska finnas ett utpekat organ som har ett nationellt ansvar för säkerhetsskyddsfrågor och som är kontaktorganisation i internationella säkerhetsskyddsärenden.

Myndigheter med uppgifter enligt säkerhetsskyddslagstiftningen

Säkerhetspolisen och Försvarsmakten har ett särskilt ansvar för säkerhetsskyddet, bl.a. genom att myndigheterna har det huvudsakliga ansvaret för tillsyn och tillämpningsföreskrifter. Därutöver har bl.a. Affärsverket svenska kraftnät, Post- och telestyrelsen och Transportstyrelsen fått ansvar för att i fråga om vissa enskilda verksamheter besluta om placering i säkerhetsklass och registerkontroll samt kontrollera säkerhetsskyddet.

Säkerhets- och integritetsskyddsnämnden prövar om uppgifter som kommer fram vid registerkontroll ska lämnas ut för säkerhetsprövning.

Försvarets materielverk får under vissa omständigheter ingå avtal om säkerhetsskydd med företag, om det behövs för att företaget ska kunna delta i internationella uppdrag.

Internationell utblick

Vi har studerat regelverken i Danmark, Finland, Nederländerna, Norge och Tjeckien.

Hot och förändringsfaktorer

Begreppet rikets säkerhet har kommit att förknippas med framför allt militära förhållanden. Samtidigt har utvecklingen gått mot att andra för samhället viktiga verksamheter fått en allt större betydelse från säkerhetsskyddssynpunkt. Främmande staters underrättelseverksamhet har breddats mot forskning och utveckling inom civila områden samt mot politiska frågor och information som rör samhällsviktiga system. Elektroniska angrepp betraktas som ett av de allvarligare hoten. Samtidigt kvarstår underrättelsehotet mot militära förhållanden och mot information av betydelse för försvaret av Sverige. Den ökade koncentrationen till ett fåtal företag som tillhandahåller tjänster till myndigheter särskilt på it-området och som därmed får tillgång till stora mängder information kan medföra en ökad sårbarhet.

Våra överväganden

Utgångspunkter för en reformerad säkerhetsskyddslagstiftning

En reformerad säkerhetsskyddslagstiftning bör i vissa delar bygga på tidigare reglering. Vi anser att syftet med lagstiftningen ska vara att säkerställa ett tillräckligt skydd för det som är mest skyddsvärt för nationen, att den ska vara verksamhetsorienterad, att den ska ge ett förebyggande skydd mot i huvudsak antagonistiska hot, att den ska omfatta samverkande säkerhetsskyddsåtgärder för information, personer och verksamhet, samt att den nuvarande organisatoriska indelningen avseende bl.a. verkställighetsföreskrifter och tillsyn bör finnas kvar.

Säkerhetsskyddslagen behöver dock *utvecklas* när det gäller Sveriges internationella åtaganden på säkerhetsskyddsområdet och informationssäkerhetsperspektiven tillgänglighet och riktighet. Vidare behöver lagen *förtydligas* avseende att den ska tillämpas i såväl allmän som enskild verksamhet. Det innebär att våra överväganden inriktas på att klargöra lagens skyddsintressen och dess tillämpningsområde. Sammantaget medför det behov av en justerad beskrivning av lagens syfte och av en delvis förändrad systematik.

Lagens syfte

Den nuvarande lagen är uppbyggd utifrån begreppen rikets säkerhet och skydd mot terrorism. Vi har sett behov av att ompröva också den delen av lagstiftningen. En utgångspunkt har varit att skydd mot terrorism, som snarare hör till frågan *mot vad* behövs ett skydd, inte bör ingå i en beskrivning av vad som ska skyddas.

Rikets säkerhet är en för säkerhetsskyddet lämplig avgränsning. Vi delar den uppfattning om innebörden av begreppet som regeringen gett uttryck för vid översynen av spioneribestämmelsen, nämligen att skyddsvärda verksamheter kan finnas inom fler samhällsområden än tidigare.

Vi delar också uppfattningen att *Sveriges säkerhet* är en lämpligare benämning. Vi har övervägt om tillämpningsområdet kan göras tydligare genom någon form av komplettande skrivning, t.ex. en exemplifiering av olika slag av civila och militära verksamheter eller genom en hänvisning till övriga vitala säkerhetsintressen. Sådana lösningar kan dock riskera att få en motsatt effekt än den avsedda. Vi har därför stannat vid att det skyddsvärda området ska beskrivas som *verksamhet av betydelse för Sveriges säkerhet*.

Sverige har ingått överenskommelser om säkerhetsskydd med andra stater och mellanfolkliga organisationer. Det är därför viktigt med en större tydlighet om de krav på säkerhetsskydd som sådana åtaganden innebär. Vi föreslår därför att säkerhetsskyddslagens tillämpningsområde ska omfatta även verksamhet som avses i ett för Sverige förpliktande åtagande om säkerhetsskydd (*internationellt säkerhetsskyddsåtagande*).

Som en samlande benämning för dessa huvudkomponenter i säkerhetsskyddslagen föreslår vi *säkerhetskänslig verksamhet.* Innebörden av detta för lagen centrala begrepp är således verksamhet av betydelse för Sveriges säkerhet samt verksamhet som omfattas av ett internationellt säkerhetsskyddsåtagande.

I fråga om vad lagen ska skydda *mot* har vi gjort bedömningen att det är bra med en fortsatt tydlighet om att säkerhetsskydd främst handlar om skydd mot antagonistiska hot bl.a. spioneri, sabotage och terroristbrott.

Det skydd som avser annat obehörigt röjande, ändrande, otillgängliggörande eller förstörande av uppgifter som är säkerhetskänsliga bör även i fortsättningen komma till uttryck i

bestämmelsen om vad säkerhetsskyddslagen ska skydda mot. Vi föreslår att det skyddet ska omfatta också uppgifter som ska skyddas enligt internationella säkerhetsskyddsåtaganden.

Säkerhetskänslig verksamhet – två huvudsakliga inriktningar

I dag utgår säkerhetsskyddslagen från att behov av säkerhetsskydd främst handlar om skydd av hemliga uppgifter. Kopplingen till offentlighets- och sekretesslagen kan ge intryck av att säkerhetsskydd främst är en angelägenhet för myndigheter och andra offentliga organ för vilka den lagen är tillämplig. Därutöver handlar det om ett säkerhetsskydd med inriktning att skydda mot terrorism för flygplatser och byggnader, anläggningar m.m. som enligt skyddslagen är skyddsobjekt. Sådana avgränsningar är i dag för snäva och medför eller riskerar att medföra att t.ex. verksamheter som är av betydelse för att upprätthålla grundläggande samhällsfunktioner faller utanför tillämpningsområdet. Ett första steg är en ändrad systematik som bl.a. tydligare innefattar sådan säkerhetskänslig verksamhet som bedrivs hos enskilda. Vi föreslår att beskrivningen av säkerhetsskyddet ska utgå från två huvudsakliga inriktningar.

Säkerhetsskyddet ska inriktas mot verksamhet som innebär *hantering av säkerhetsskyddsklassificerade uppgifter.* Det ska innefatta skydd av uppgifter som är av betydelse för Sveriges säkerhet eller som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande och som till sin natur är sådana uppgifter som avses i bestämmelser om sekretess. Det innebär således en vidare ram än enligt den nuvarande lagen som utgår från begreppet hemliga uppgifter.

Därutöver ska säkerhetsskyddet inriktas mot verksamheter som av annan anledning behöver ett säkerhetsskydd (*i övrigt säkerhetskänslig verksamhet*). Det motsvarar delvis vad som i dag skyddas inom ramen för skydd mot terrorism, dvs. i huvudsak verksamhet vid skyddsobjekt, flygplatser och vissa verksamheter som ska skyddas enligt folkrättsliga åtaganden om luftfartsskydd, hamnskydd och sjöfartsskydd. Det skyddsvärda området bör inte avgränsas genom regleringen om skyddsobjekt, utan ska utformas så att det även kan innefatta annan säkerhetskänslig verksamhet, t.ex. hantering av it-system eller sammanställningar av uppgifter som är

av central betydelse för ett fungerande samhälle eller verksamhet som behöver skyddas på den grunden att den kan utnyttjas för att skada nationen, t.ex. vissa verksamheter inom det kärntekniska området.

Vad ska skyddas – säkerhetsskyddsanalys

Svaret på frågan vilka tillgångar och funktioner i verksamheter som behöver säkerhetsskydd varierar över tid och kommer därför att behöva omprövas kontinuerligt. Frågan måste bl.a. därför besvaras på verksamhetsnivå.

Säkerhetsskyddsanalysens centrala funktion för säkerhetsskyddet behöver bl.a. därför lyftas fram. En bestämmelse om att den som är ansvarig för säkerhetskänslig verksamhet ska se till att behovet av säkerhetsskydd för den egna verksamheten utreds bör därför tas in i lagen.

Genom säkerhetsskyddsanalysen ska säkerhetsskyddsklassificerade uppgifter och vad som i övrigt behöver ett säkerhetsskydd identifieras samt säkerhetshot och potentiella konsekvenser, sårbarheter och behovet av säkerhetsskyddsåtgärder bedömas. Analysen ska ligga till grund för planeringen av verksamhetens säkerhetsskydd.

I det bredare arbetet med att stärka skyddet av samhällsviktig verksamhet och kritisk infrastruktur utförs risk- och sårbarhetsanalyser. Säkerhetsskyddsanalysen bör så långt som möjligt samordnas med sådana analyser.

Ett tydligare verksamhetsansvar

Vi föreslår att regleringen av för vilka verksamheter lagen gäller förenklas. Vi ser inget behov av någon uppdelning mellan företagsformer över vilket det allmänna har ett rättsligt bestämmande inflytande och företagsformer där ett sådant inflytande inte finns. Lagen ska därför gälla för verksamhet hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet eller omfattas av ett internationellt säkerhetsskyddsåtagande (säkerhetskänslig verksamhet).

I dag finns inte i säkerhetsskyddslagen någon bestämmelse som sammanfattar vad som är följden av att lagen är tillämplig. Vi före-

slår därför att det i lagen uttrycks att den som ansvarar för en säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd, se till att säkerhetsskyddsåtgärder vidtas, kontrollera att bestämmelserna om säkerhetsskydd följs samt lämna uppgifter som följer av viss angiven rapporteringsskyldighet till utsedda tillsynsmyndigheter.

Ett system av samverkande säkerhetsskyddsåtgärder

Samverkande säkerhetsskyddsåtgärder

Vi anser att indelningen i tre säkerhetsskyddsåtgärder ska bestå i en ny lag. De tre säkerhetsskyddsåtgärderna, som bör benämnas informationssäkerhet, fysisk säkerhet och personalsäkerhet, samverkar och utgör ett sammanhållet system för skydd av säkerhetskänslig verksamhet. Säkerhetsskyddsåtgärderna kan kombineras på olika sätt för att optimera skyddseffekten. Ett sådant synsätt leder till ett balanserat och kostnadseffektivt säkerhetsskydd. Grunden för vilka säkerhetsskyddsåtgärder som ska vidtas läggs i säkerhetsskyddsanalysen, och dessa åtgärder ska sedan konkretiseras i en säkerhetsskyddsplan.

Säkerhetsskyddsklassificerade uppgifter

Säkerhetsskyddsklassificerade uppgifter ska delas in i fyra informationssäkerhetsklasser efter den skada som kan uppstå om uppgifterna röjs. De fyra klasserna ska benämnas kvalificerat hemlig, hemlig, konfidentiell och begränsad. Indelningen i informationssäkerhetsklasser är grunden för utformningen av den del av säkerhetsskyddsåtgärderna informationssäkerhet, fysisk säkerhet och personalsäkerhet som tar sikte på skyddet av säkerhetsskyddsklassificerade uppgifter.

En bestämmelse om indelning av säkerhetsskyddsklassificerade uppgifter ska finnas i säkerhetsskyddslagen eftersom denna indelning är av central betydelse för hur säkerhetsskyddet ska utformas.

Informationssäkerhet

Enligt vårt förslag ska säkerhetsskyddsåtgärden informationssäkerhet vara uppdelad i två moment. Det första tar sikte på skyddet av säkerhetsskyddsklassificerade uppgifter för att förebygga att uppgifterna röjs, ändras, görs otillgängliga eller förstörs. I informationssäkerhetssammanhang brukar man tala om skydd för konfidentialitet, riktighet och tillgänglighet.

I det andra momentet är inriktningen att åtgärderna ska förebygga skadlig inverkan på informationstillgångar som *annars* är av betydelse för säkerhetskänslig verksamhet. I detta fall är det därför enbart riktighets- och tillgänglighetshänsyn som gör sig gällande. Med informationstillgångar avses information och informationssystem i vid bemärkelse, dvs. uppgifter, handlingar och tekniska system som används för att i olika avseenden elektroniskt kommunicera och i övrigt behandla uppgifter.

Informationssäkerhet innebär åtgärder av olika slag för att skydda information som är av betydelse för säkerhetskänslig verksamhet. Sådan information förekommer i olika miljöer och verksamheter och hanteras och används på flera olika sätt. Därför måste säkerhetsskyddsåtgärderna anpassas till de skiftande förutsättningarna. Uppgifternas form saknar i sammanhanget betydelse, och åtgärderna måste avse uppgifterna som sådana dvs. såväl uppgifter på papper som elektroniskt lagrade och kommunicerade uppgifter samt uppgifter som kan läsas ut ur t.ex. bilder eller materiel.

Fysisk säkerhet

Enligt vårt förslag ska fysisk säkerhet innefatta sådana säkerhetsskyddsåtgärder som ska förebygga dels att obehöriga får tillträde till områden, byggnader, andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där i övrigt säkerhetskänslig verksamhet bedrivs, dels skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt. Den nya benämningen svarar bättre mot åtgärderna än den nuvarande benämningen tillträdesbegränsning.

Personalsäkerhet

Syftet med personalsäkerhet

Vi föreslår att syftet med säkerhetsskyddsåtgärden *personalsäkerhet* ska anges vara dels att förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av annan anledning är säkerhetskänslig (*säkerhetsprövning*), dels att säkerställa att de som deltar i säkerhetskänslig verksamhet har en tillräcklig kunskap om säkerhetsskydd (*utbildning i säkerhetsskydd*).

En övergång till säkerhetsklarering?

Enligt direktiven ska vi överväga en förändring av nuvarande säkerhetsprövning mot ett system med inslag av säkerhetsklarering. Redovisningen i direktiven utgår i det avseendet från de förändringar som samarbetet med andra länder och mellanfolkliga organisationer påkallar.

Erfarenheter som kan dras utifrån den internationella utblicken visar att i fråga om klarering likheterna med den svenska modellen är större än olikheterna. Det handlar överlag mer om formella skillnader än om skillnader i sak. Systemen för klarering i de länder vi har studerat skiljer sig dessutom sinsemellan åt i flera avseenden.

Vid en jämförelse med den svenska säkerhetsprövningen är vårt intryck att underlagen i klareringsmodellerna i högre grad är mer summariska och inte sällan bygger på enbart uppgifter om tidigare brottslighet. Som vi ser det innebär vidare en ordning med ett klareringsförfarande ett avsteg från den viktiga principen om ett verksamhetsanpassat säkerhetsskydd. Att prövningen ska anpassas till den specifika befattningen är angeläget inte enbart utifrån behovet av ett för den ifrågavarande verksamheten väl anpassat säkerhetsskydd utan också för den som prövningen avser.

Sammantaget har det inte för skyddet av verksamhet som har betydelse för Sveriges säkerhet kommit fram några påtagliga behov av ett intygsförfarande. Behoven hör i stället samman med utlandstjänstgöring och liknande. Det finns mervärden i nuvarande system

som i viss utsträckning kan behöva förstärkas men som i stället kan riskera att försvagas vid en övergång till ett klareringssystem.

För att tillgodose krav som följer av internationella säkerhetsskyddsåtaganden behöver grunderna för och underlaget vid säkerhetsprövningen ansluta till det sätt att klassificera information i en fyrgradig skala som vi har föreslagit. En sådan anpassning kan åstadkommas genom en justering av grunderna för placering av anställningar i säkerhetsklass. Det finns vidare behov av en reglering som tydligt ger stöd för att utfärda internationellt sett inom säkerhetsskyddsområdet accepterade intyg. Sådana förändringar kan genomföras också inom ramen för nuvarande system för säkerhetsprövning (se vidare nedan under rubriken Internationell samverkan).

Vi har alltså kommit fram till att säkerhetsprövningen inte bör utvecklas mot ett s.k. klareringssystem. En sådan förändring behövs inte för att kunna uppfylla krav som följer av internationella säkerhetsskyddsåtaganden och är inte heller av annan anledning att föredra.

Säkerhetsprövning

Vad som ska bedömas inom ramen för säkerhetsprövningen är liksom i dag pålitlighet och lojalitet. Av förarbeten till gällande säkerhetsskyddslag framgår att det innebär ett behov av att utreda och ta ställning till om t.ex. missbruk av olika slag eller förbindelser med andra länder innebär att den kontrollerade kan löpa en särskild risk att utsättas för påtryckningar. Det kan innebära att det är nödvändigt att ställa frågor om personliga förhållanden som kan vara känsliga för den som kontrollen avser. Vi föreslår att det i lagtexten tydligt anges att säkerhetsprövningen innebär att omständigheter som kan antas innebära sårbarheter i säkerhetshänseende ska beaktas.

Säkerhetsskyddslagens bestämmelser om säkerhetsprövning bör i stora delar föras över till en reformerad säkerhetsskyddslag. I vissa avseenden har vi sett behov av förtydliganden. Vårt förslag innebär att det också av lagen tydligare framgår att prövningen förutsätter en grundutredning som, i den utsträckning som följer av bestämmelserna om placering i säkerhetsklass, ska kompletteras med

registerkontroll och särskild personutredning. Med grundutredning avses således bl.a. intervju eller annan form av uppgiftsinhämtning.

Vidare föreslår vi att det av lagtexten tydligt ska framgå att säkerhetsprövningen innebär krav på uppföljning under hela den tid deltagandet i den säkerhetskänsliga verksamheten pågår.

Placering i säkerhetsklass

Bestämmelserna om placering av anställningar i säkerhetsklass anpassas till förslaget om en övergång från skydd av hemliga uppgifter till skydd av säkerhetsskyddsklassificerade uppgifter och till förslaget om att skyddsnivån för sådana uppgifter ska bestämmas av uppgiftens informationssäkerhetsklass.

Att den berörde får del av säkerhetsskyddsklassificerade uppgifter som klassificerats som kvalificerat hemliga, hemliga eller konfidentiella ska styra placeringen i säkerhetsklass. Om uppgifter på en högre skyddsnivå förekommer endast i mindre omfattning, ska dock anställningen placeras i nästa lägre klass.

Bestämmelserna om placering i säkerhetsklass utvidgas till att omfatta även anställningar i verksamhet som, även om den inte innebär hantering av säkerhetsskyddsklassificerade uppgifter, är säkerhetskänslig (i övrigt säkerhetskänslig verksamhet). Den nya grunden för placering i säkerhetsklass innebär att den registerkontroll som i dag görs med stöd av 14 § säkerhetsskyddslagen (skydd mot terrorism) inordnas i systemet med säkerhetsklassplaceringar.

Att den anställde till följd av sitt deltagande i verksamheten har möjlighet att orsaka synnerligen allvarlig skada, allvarlig skada eller en inte obetydlig skada för Sveriges säkerhet ska styra placeringen i säkerhetsklass.

Medborgarskapskravet tas bort

Vi har kommit fram till att svenskt medborgarskap inte ska vara ett behörighetsgrundande krav för att inneha en säkerhetsklassad anställning hos staten, kommuner eller landsting och att det kravet således inte ska föras över till en reformerad säkerhetsskyddslag. Det innebär dock inte att avsaknaden av svenskt medborgarskap är

utan betydelse. Den omständigheten att en person saknar svenskt medborgarskap får i stället, på samma sätt som t.ex. innehav av annat medborgarskap jämte ett svenskt, närmare utredas och vägas in vid säkerhetsprövningen.

Ett uttryckligt krav på restriktivitet vid placering i säkerhetsklass

Ett krav på restriktiv tillämpning i fråga om placering av anställningar i säkerhetsklass ska införas i säkerhetsskyddslagen. Av en sådan bestämmelse ska framgå att den som beslutar om placering av en anställning i säkerhetsklass ska noga pröva behovet och att sådan placering får göras endast om skyddsbehovet inte kan tillgodoses på något annat sätt.

Utlämnande av uppgifter som kommit fram vid registerkontroll

Den nuvarande ordningen där uppgifter efter registerkontroll får lämnas ut endast efter en relevansprövning av Säkerhets- och integritetsskyddsnämnden bör inte ändras.

Vem ska besluta om placering i säkerhetsklass?

Behörigheten att besluta om placering av anställningar i säkerhetsklass ska bygga på nuvarande beslutsordning där regeringen, med undantag för riksdagens förvaltningsområde, ytterst har beslutanderätten men kan överlåta den till myndigheter, kommuner och landsting och, om det finns särskilda skäl, vissa företag.

I huvudsak ska endast den som beslutar om placering i säkerhetsklass ha behörighet att från Säkerhetspolisen få uppgifter vid registerkontroll.

Ansvaret för säkerhetsprövningen

Den verksamhet som avser att anställa någon eller på annat sätt låta någon delta i säkerhetskänslig verksamhet ansvarar för säkerhetsprövningen och avgör självständigt om personen är lämplig från säkerhetssynpunkt. En delvis avvikande ordning gäller på vissa

områden bl.a. i fråga om verksamhet som omfattas av krav på luftfartsskydd och för leverantörer där villkoren för säkerhetsskyddet bestäms i ett säkerhetsskyddsavtal.

Skyddet för uppgifter om enskildas personliga förhållanden

Säkerhetsprövningen kan innebära att för den enskilde synnerligen känsliga uppgifter hämtas in av den presumtive arbetsgivaren eller den som annars ska göra säkerhetsprövningen. Det är därför viktigt att det finns ett skydd för att uppgifterna inte används för annat ändamål än det avsedda. Vår bedömning är att skyddet i dag inte i alla avseenden är tillräckligt. Vi föreslår därför en ändring i offentlighets- och sekretesslagen och en, i fråga om enskild verksamhet, kompletterade tystnadspliktsbestämmelse i säkerhetsskyddslagen.

Säkerhetsskyddad upphandling

Säkerhetsskyddad upphandling med säkerhetsskyddsavtal bör behållas i en ny lagstiftning. Bestämmelserna om säkerhetsskyddad upphandling och säkerhetsskyddsavtal ska gälla för upphandlingar eller ingående av kontrakt där det förekommer information i informationssäkerhetsklassen konfidentiell eller däröver, eller som i övrigt avser säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet. Skälet till det är att kraven på att säkerhetsskyddad upphandling genomförs ska korrespondera mot andra krav på säkerhetsskydd.

I säkerhetsskyddsavtalen ska villkor anges för hur krav på säkerhetsskydd ska tillgodoses av leverantören.

Även fortsättningsvis bör säkerhetsskyddsavtal ingås av staten, kommuner och landsting, men vi anser att andra som har behov av sådana avtal bör kunna begära detta hos en myndighet som regeringen bestämmer, i första hand en säkerhetsskyddsstödjande myndighet. Om det finns särskilda skäl, bör en enskild kunna ingå säkerhetsskyddsavtal.

Internationell samverkan

Vi föreslår att Försvarsmakten får i uppgift att vara nationell säkerhetsmyndighet. Försvarsmakten ska dock, i fråga om andra ärenden än sådana som rör registerkontroll och säkerhetsintyg för person, till Säkerhetspolisen lämna över ärenden som främst rör Säkerhetspolisens tillsynsområde. Vi föreslår också att Försvarets materielverk får i uppgift att vara nationell industrisäkerhetsmyndighet. Försvarsmakten och Försvarets materielverk bör ges rätt att utfärda föreskrifter för respektive ansvarsområden.

Säkerhetsintyg för *person* får utfärdas om behov av sådant intyg finns vid internationell samverkan avseende säkerhetskänslig verksamhet, eller om intyget kan underlätta för en person som har hemvist i Sverige att delta i en verksamhet som en annan stat eller en mellanfolklig organisation bedömer vara i behov av säkerhetsskydd.

Säkerhetsintyg för *leverantör* får utfärdas om behov av sådant intyg finns vid internationell samverkan avseende säkerhetskänslig verksamhet, eller om intyget kan underlätta för en leverantör som har sitt säte i Sverige att delta i en verksamhet som en annan stat eller en mellanfolklig organisation bedömer vara i behov av säkerhetsskydd.

Gemensamt för båda slagen av intyg är att dessa i princip får utfärdas endast om deltagandet avser verksamhet i eller för en stat eller mellanfolklig organisation som omfattas av ett internationellt säkerhetsskyddsåtagande.

Tillsyn, föreskrifter och rapportering

Det finns brister som i vissa fall är allvarliga vad gäller att uppfylla säkerhetsskyddslagens bestämmelser och intentioner. I några avseenden beror det på förhållanden som inte går att påverka genom en reformerad säkerhetsskyddslagstiftning. Vad i övrigt gäller bristerna i säkerhetsskyddet är det vår bedömning att de i en relativt stor utsträckning kan relateras till otydlig lagstiftning och bristfällig kunskap om hur lagstiftningens krav påverkar och kan tillgodoses i den egna verksamheten. Tillsyn kan endast i begränsad omfattning påverka sådana brister.

Vår bedömning är att tillsynen bör bedrivas under i huvudsak samma former som i dag. Behovet av råd och stöd är framträdande särskilt i fråga om enskilda som bedriver säkerhetskänslig verksamhet. Tillräckliga skäl föreligger för närvarande inte att föreslå en så genomgripande förändring av tillsynens inriktning och genomförande som sanktioner skulle medföra. Frågan bör dock följas upp när en reformerad säkerhetsskyddslag har varit i kraft en tid.

I fråga om organisationen av tillsynen föreslår vi bl.a. ett förenklat samrådsförfarande för de inblandade myndigheterna. Säkerhetspolisen och Försvarsmakten som har det huvudsakliga ansvaret för tillsynen av säkerhetsskyddet kan då också arbeta mer effektivt med tillsynen. Vi föreslår också att Myndigheten för samhällsskydd och beredskap tar över det tillsynsansvar som länsstyrelserna har gentemot vissa enskilda verksamheter samt även Säkerhetspolisens tillsynsansvar för kommuner och landsting.

Rätten att meddela föreskrifter bör i huvudsak vara densamma som i nuvarande säkerhetsskyddslagstiftning. Det innebär att föreskriftsrätten fördelas främst mellan Säkerhetspolisen och Försvarsmakten.

I fråga om rapportering föreslår vi bl.a. att myndigheter och andra som säkerhetsskyddslagstiftningen gäller för och som får kännedom om säkerhetshotande verksamhet av allvarlig karaktär eller misstänker sådan verksamhet ska vara skyldiga att rapportera förhållandet till Säkerhetspolisen eller Försvarsmakten. Det kan t.ex. vara fråga om incidenter där angreppen är av kvalificerad art eller tyder på en systematisk och målinriktad strategi från en aktör. Vidare torde angrepp som samtidigt riktas mot flera verksamheter ofta vara allvarliga.

Övriga frågor

Tystnadsplikt för den som deltar i säkerhetskänslig verksamhet

Det behövs sekretesskydd för uppgifter som är av betydelse för Sveriges säkerhet när sådana uppgifter förekommer i enskild verksamhet. Vi föreslår att en tystnadspliktsbestämmelse införs i säkerhetsskyddslagen. Tystnadsplikten ska gälla också förhållanden som omfattas av ett för Sverige förpliktande åtagande om säkerhetsskydd. En förutsättning för tystnadsplikten ska vara att anställningen eller deltagandet placeras i säkerhetsklass.

Säkerhetsskyddet i riksdagen och Regeringskansliet

Riksdagen och dess myndigheter och Regeringskansliet omfattas i en begränsad utsträckning av säkerhetsskyddslagstiftningen. Den ordningen ska i sak föras över till en reformerad säkerhetsskyddslag. Den föreslagna bestämmelsen om krav på informationssäkerhetsklassificering kommer att vara central för bl.a. bestämmelser om placering av anställda i säkerhetsklass. Vi föreslår därför att även den bestämmelsen ska gälla för de nämnda organen.

Summary

Proposals

We propose that the Protective Security Act be replaced by a new act. The new act should also be called the Protective Security Act. The new act should correspond to the changed requirements concerning protective security, including developments in the area of information technology, increased international cooperation, the increased vulnerability of vital public services and the fact that security-sensitive activities are increasingly being conducted by private actors.

A broader approach for the new act means highlighting the availability and integrity aspects of information and IT systems. In this way, the scope of application will be broadened to provide protection for information assets in vital public activities that do not need protection from a confidentiality perspective.

The new act will grant nuanced protective security based on four information security classifications conforming to an international model. The information security classifications influence the design of the protective security areas: information security, physical security and personnel security. Protective security analysis will play a key role and lead to conclusions on how protective security in an organisation should be designed. The meaning of organisations bearing responsibility for the protective security will also become clarified.

The act should be clearer than it currently is in providing support for international protective security measures and international cooperation, by introducing, for example, the possibility of issuing security certificates for individuals and contractors.

Remit

One of the main purposes of the remit is to modernise regulations and better adapt them to the requirements for the protection of activities that are important for Sweden's security and to the requirements resulting from international cooperation.

Background

Current regulations

To the extent required, there must be protective security for the activities of central government, the municipalities and the county councils, for legal persons over which central government, the municipalities and county councils have a legally decisive influence, and for private actors, if their activities are important for the security of the realm or need special protection against terrorism. The aim of protective security is to prevent classified information concerning the security of the realm from being improperly disclosed, amended or destroyed (information security), to prevent unauthorised persons from gaining admission to places where they may have access to such information or where activities are undertaken that are important for the security of the realm (access restrictions), and to prevent persons who are not reliable from a security perspective from taking part in activities that are important for the security of the realm (security investigation). Protective security is also intended to prevent terrorism in other ways.

The Protective Security Act also contains provisions on the obligation in some cases to enter into classified contracts when engaging contractors, and on training, checks and supervision. More detailed provisions on protective security are contained in the act associated with the Protective Security Ordinance.

Related regulations

Regulations concerning aviation security, port security and maritime security, regulations on nuclear technology activities and radiation protection, protection of geographic information and regulations concerning civil contingencies are all relevant to protective security. Moreover, there is a close link between protective security legislation and the rules on procurement in the area of defence and security.

International law obligations concerning protective security

Sweden's international protective security commitments have increased significantly in terms of general security agreements agreed with other states and international organisations.

The purpose of a general security agreement is for two or more countries (or international organisations) to be able to exchange information concerning national security in a secure manner.

It follows from international commitments that there must be a designated body that has national responsibility for protective security issues and is the contact organisation in international protective security matters (*National Security Authority*).

Government agencies with responsibilities under the protective security legislation

The Swedish Security Service and the Swedish Armed Forces have particular responsibility for protective security, being the agencies with the main responsibility for supervision and application regulations. In addition, Affärsverket svenska kraftnät (the Swedish national grid), the Swedish Post and Telecom Authority and the Swedish Transport Agency have been given responsibility – in matters concerning certain private organisations – for making decisions on individuals' security classifications and record checks, and for monitoring protective security.

The Swedish Commission on Security and Integrity Protection checks whether information emerging from record checks should be disclosed for security investigations.

The Defence Materiel Administration may under certain circumstances enter into protective security contracts with companies if this is necessary for the company to be able to take part in international assignments.

International survey

We have studied the regulatory frameworks in the Czech Republic, Denmark, Finland, the Netherlands and Norway.

Threats and change factors

The term 'security of the realm' has come to be associated mainly with military defence. At the same time, the trend has shifted towards other activities that are important to society becoming increasingly significant from a protective security perspective. The intelligence activities of foreign states have broadened to encompass research and development in civilian areas, and political issues and information concerning vital public systems. Electronic attacks are considered to be one of the most serious threats. However, the intelligence threat to military defence and to information that is important for Sweden's defence remains. The increased confinement to a small number of companies that provide government agencies with services – particularly in the area of IT – and that thus have access to large amounts of information may lead to greater vulnerability.

Our deliberations

Starting points for reformed protective security legislation

Reformed protective security legislation should in certain regards be based on earlier regulations. We consider that the purpose of the legislation is to ensure that there is sufficient protection for that which is most worthy of protection for the nation; that it should be activity-oriented; that it should provide preventive protection, primarily against antagonistic threats; that it should cover combined protective security measures for information, persons

and activities; and also that the current organisational division regarding implementation regulations and supervision should remain in place.

However, the Protective Security Act needs to be *developed* in terms of Sweden's international commitments in the area of protective security and the information security perspectives of availability and integrity. Moreover, there needs to be *greater clarification* about the act being applicable to both public and private activities. This means that our deliberations have focused on clarifying the act's protective interests and scope of application. All of this combined means that there is a need to revise the description of the purpose of the act and partly amend the classifications.

Purpose of the act

The current act is based on the terms 'security of the realm' and 'protection against terrorism'. We have identified a need to review this part of the legislation as well. One basic point was that protection against terrorism – which is more a matter of what we need protection *against* – should not be included in a description of what it is that needs protection.

The security of the realm is an appropriate definition for protective security. We share the view of the meaning of the term expressed by the Government in its review of the provision on espionage, i.e. that activities worthy of protection may be conducted in more areas of society than was previously the case.

We also share the view that *Sweden's security* is a more appropriate term. We have considered whether the scope of application can be made clearer through some form of supplementary text, providing examples of various kinds of civilian and military activities, for example, or through a reference to other vital security interests. However, such solutions can risk having the opposite effect to the desired one. We have therefore concluded that the area worthy of protection should be described as *activities of importance for Sweden's security*.

There are protective security commitments that Sweden is bound by in relation to other states and international organisations.

It is therefore important to have greater clarity concerning the protective security requirements that follow from such commitments. We therefore propose that the scope of application of the Protective Security Act should also cover activities included in a protective security commitment that is binding for Sweden (*international security commitment*).

We propose the term *'security-sensitive activities'* as an umbrella term for these main components of the Protective Security Act. The meaning of this term, which is central to the act, is therefore activities of importance for Sweden's security and activities included in an international protective security commitment.

When it comes to what the act should protect *against*, we consider that it is good to have continued clarity over the fact that protective security is primarily a matter of protection against antagonistic threats, including espionage, sabotage and terrorist offences.

The protection that covers other unauthorised disclosure, amendment, blocking or destruction of security-sensitive information should continue to be reflected in the provision on what the Protective Security Act is to protect against. We propose that this protection also cover information that is to be protected under international protective security commitments.

Security-sensitive activities – two main focuses

The Protective Security Act is currently based on the idea that protective security needs are primarily about protecting secret information. The link to the Public Access to Information and Secrecy Act may give the impression that protective security is primarily a matter for government agencies and other public bodies to which the act is applicable. Furthermore, this protective security focuses on protection against terrorism for airports and buildings, facilities, etc. that have protected status under the Protective Security Act. Such definitions are now too narrow and result in – or risk resulting in – activities that are important for upholding fundamental public services falling outside the scope of application. A first step is to amend the classifications so that they more clearly encompass the kind of security-sensitive activities carried out by

private actors. We propose that the description of protective security take its cue from two main focuses.

Protective security should focus on activities that involve *the handling of classified information.* This should encompass the protection of information that is of importance for Sweden's security or that should be protected under an international protective security commitment, and that is information of the kind covered by provisions on secrecy. This therefore means a wider framework than the current act, which is based on the term 'secret information'.

In addition, protective security should focus on activities that need protective security for some other reason (*other security-sensitive activities).* This corresponds in part to that which is currently protected within the framework of protection against terrorism, i.e. essentially activities conducted at facilities with protected status, airports and certain activities that must be protected under international law commitments on aviation security, port security and maritime security. The area worthy of protection should not be demarcated through regulations on facilities with protected status; rather, it should be defined in such a way that it can also include other security-sensitive activities, such as the handling of IT systems or the compilation of information that is of vital importance to a functioning society, or activities that need to be protected on the grounds that they could be exploited to harm the nation, e.g. certain activities within the area of nuclear technology.

What should be protected – protective security analysis

The answer to the question of what assets and functions in organisations need protective security varies over time and will therefore need to be reviewed continuously. For this reason, and others, the question should be addressed at organisation level.

This is one reason why there is a need to highlight the key role of protective security analysis in protective security. A provision should therefore be included in the act whereby any person responsible for security-sensitive activities is to ensure that the

need for protective security in their own organisation is investigated.

Protective secuirty analysis is to enable the identification of classified information and anything else that needs protective security, and the assessment of security threats and potential consequences, vulnerability and the need for protective security measures. This analysis should form the basis of plans for protective security for that particular organisation.

In broader efforts to strengthen the protection of activities vital to society and critical infrastructure, risk and vulnerability analyses are conducted. Protective security analysis should, as far as possible, be coordinated with such analyses.

Clearer responsibility for organisations

We propose the simplification of the regulations on which activities the law should apply to. We do not consider there to be a need for any distinction between company forms over which the public sector has a legally decisive influence and company forms over which there is no such influence. The act should therefore apply to the activities of central government, municipalities, county councils and private actors that are of importance for Sweden's security or are covered by an international protective security commitment (security-sensitive activity).

The current Protective Security Act contains no provision summarising the implications of being subject to the act. We therefore propose that the act state that any person responsible for a security-sensitive activity is to investigate the need for protective security, ensure that protective security measures are taken, monitor to ensure that the provisions on protective security are being followed and provide information in line with certain specified reporting obligations to the designated supervisory authorities.

A system of combined protective security areas

Combined protective security areas

We consider that the classification into three protective security areas should remain in a new act. The three protective security areas – which should be termed 'information security', 'physical security' and 'personnel security' – interact and make up a coherent system for the protection of security-sensitive activities. The protective security measures can be combined in various ways to optimise the protective effect. Such an approach leads to balanced and cost-effective protective security. The grounds on which protective security measures should be taken are laid out in the protective security analysis, and these measures should then be clarified in a protective security plan.

Classified information

Classified information should be divided into four information security classifications based on the harm that could be caused if the information were disclosed. The four classifications should be termed *kvalificerat hemlig*, *hemlig*, *konfidentiell* and *begränsad* (equivalent to top secret, secret, confidential and restricted). The division into security classifications forms the basis for the design of the parts of the protective security areas (information security, physical security and personnel security) that aims to protect classified information.

A provision on the classification of classified information should be included in the Protective Security Act as this classification is crucial for how protective security is designed.

Information security

Under our proposal, the protective security area *information security* should be divided into two parts. The first focuses on the protection of classified information to prevent the information being disclosed, amended, made unavailable or destroyed. In information security contexts, this is often described as confidentiality, integrity and availability.

The second specifies that the measures are to prevent adverse effects on information assets that would *in some other respects* be of importance for security-sensitive activities. In this case, it is therefore only the integrity and availability considerations that apply. 'Information assets' refers to information and information systems in a broad sense, i.e. information, documents and technical systems that are used in various ways to communicate information electronically and handle information in general.

Information security encompasses measures of various kinds intended to protect information that is of importance to security-sensitive activities. Such information appears in various environments and activities and is handled and used in various different ways. Protective security measures must therefore be adapted to the changing circumstances. The form that the information takes is not relevant in this context, and the measures must concern information as such, i.e. information on paper and information stored electronically, communicated information and information that can be gleaned from images or other material, for example.

Physical security

Under our proposal, the protective security area *physical security* should be divided into two parts. The first focuses on preventing unauthorised persons from gaining admission to areas, facilities, buildings or objects where they may have access to classified information or where in other respects security-sensitive activities are conducted, and to prevent adverse effects on such areas, facilities, buildings or objects. The new term corresponds to the measures better than the current term 'access restrictions'.

Personnel security

The purpose of personnel security

We propose that the purpose of the protective security area *personnel security* be stated as being to prevent persons who are not reliable from a security perspective from taking part in activities

where they may have access to classified information or in activities that for some other reason are security-sensitive (*security investigation*), and to ensure that those who take part in security-sensitive activities have sufficient knowledge of protective security (*protective security training*).

A transition to security clearance?

Under the terms of reference, we are to consider a transition from the current security investigation system towards a system with elements of security clearance. The description in the terms of reference is based in this respect on the changes that are required as a result of cooperation with other countries and international organisations.

Experience that can be gleaned from the international survey shows that when it comes to clearance, the similarities with the Swedish model are greater than the differences. Overall, these are purely formal differences rather than differences in substance. The clearance systems in the countries we have studied also differ among themselves in several respects.

When comparing these with the Swedish security investigation system, our impression is that the background material in the clearance models is more summary and is often based only on information concerning previous offences. In our view, a system with a clearance procedure would also be a departure from the important principle of protective security tailored to specific activities. Tailoring the investigation to the specific position is important, not only in view of the need for well-tailored protective security for the activity in question, but also for the person who is the subject of the investigation.

On balance, no tangible needs have come to light that would require the introduction of a certification procedure for the protection of activities that are of importance for Sweden's security. Instead, the needs that exist are associated with foreign postings and similar. There is added value in the current system, which may need to be strengthened to some extent, but which may risk being weakened in the event of a transition to a clearance system.

To meet the requirements that follow from international protective security commitments, the basis and background material for a security investigation need to tally with the method of classifying information on a four-grade scale, as we have proposed. Such an adaptation can be achieved by adjusting the grounds for classifying positions in security classes. Moreover, there is a need for a framework that provides clear support for issuing certificates that are accepted internationally in the area of protective security. Such changes can also be made within the framework of the current system of security investigation (more details below under the heading 'International cooperation').

We have concluded, therefore, that the security investigation system should not be developed into a clearance system. Such a change is not necessary to be able to meet the requirements that follow from international protective security commitments, nor is it preferable for any other reason.

Security investigations

As is the case today, security investigations should assess reliability and loyalty. The legislative history of the current Protective Security Act states that this involves a need to investigate and determine whether, for example, various forms of substance abuse or links with other countries mean that the person under investigation runs a particular risk of being subjected to pressure. This may mean that it is necessary to ask questions about personal circumstances that may be sensitive for the person under investigation. We propose that the legislative text clearly state that the security investigation involves considering circumstances that may result in vulnerability from a security perspective.

The provisions of the Protective Security Act on security investigations should for the most part be transferred to a reformed Protective Security Act. In some respects we have identified a need for clarification. Under our proposal, the act would more clearly state that the security investigation requires basic screening, which – to the extent that follows from the provisions on classification in security classes – is to be supplemented by record checks and a special personal screening.

The basic screening thus involves interviews and other forms of information-gathering.

Moreover, we propose that the legislative text clearly state that the security investigation involves requirements concerning follow-up during the entire time in which the person is taking part in security-sensitive activities.

Security classification

The provisions on the security classification of positions are adapted to the proposal on a transition from the protection of secret information to the protection of classified information, and to the proposal on the level of protection for such information being determined by which information security class the information belongs to.

The fact that the person concerned has access to information that has been classified as top secret, secret or confidential should determine their security classification. If small amounts of information from a higher level of protection are accessible, the position is to be classified in the next security class down.

The provisions on security classification will be broadened to also cover positions in activities that are security-sensitive (other security-sensitive activities), even if they do not involve dealing with classified information. The new basis for classifying positions in a security class means that the record checks that are currently carried out pursuant to Section 14 of the Protective Security Act (protection against terrorism) are categorised in the system of security classifications.

The fact that the employee, as a result of taking part in the activity, has the opportunity to cause particularly serious damage, serious damage or significant damage to Sweden's security is to be a determining factor when selecting the security class.

Removal of the citizenship requirement

We have concluded that Swedish citizenship should not be an eligibility requirement for holding a security-classified position within central government, municipalities or county councils, and

that the requirement should thus not be carried over to a reformed Protective Security Act. However, this does not mean that a lack of Swedish citizenship is insignificant. The fact that a person does not have Swedish citizenship may instead be investigated more closely and considered in the security investigation in the same way that it would, for example, for persons who have another citizenship alongside Swedish citizenship.

An explicit requirement for restrictiveness when selecting security class

A restrictiveness requirement for the security classification of positions should be introduced in the Protective Security Act. Such a provision should state that the person who determines the security classification of a position should carefully consider the need for this, and that such classification may only be undertaken if the needs for protection cannot be met in any other way.

Disclosure of information emerging from record checks

The current system in which information emerging from record checks may only be disclosed following a relevance test by the Swedish Commission on Security and Integrity Protection should not be changed.

Who should determine security classification?

The authority to determine the security classification of positions should be based on the current decision-making system, whereby – with the exception of the Riksdag's administrative area – the Government has ultimate decision-making power but can delegate this to government agencies, municipalities and county councils and, if there are special grounds, certain companies.

Essentially, only the person who determines security classification should have the authority to receive information from the Swedish Security Service's record checks.

Responsibility for security investigations

An organisation planning to employ someone or in some other way allow someone to take part in security-sensitive activities is responsible for the security investigation and determines independently whether or not the person is suitable from a security perspective. A partially different system applies in certain areas, such as activities covered by the aviation protective security requirements and for contractors for whom the terms and conditions of protective security are laid down in a classified contract.

Protecting information about an individual's personal circumstances

The security investigation may involve information that is particularly sensitive for the individual being gathered by the prospective employer or by anyone else carrying out the security investigation. It is therefore important that there is protection in place so that the information is not used for purposes other than those intended. In our assessment, the current level of protection is not sufficient in all respects. We therefore propose an amendment to the Public Access to Information and Secrecy Act and a supplementary provision in the Protective Security Act on the duty of secrecy regarding private actors.

Security-protected procurement

Security-protected procurement involving classified contracts should be retained in the new legislation. The provisions on security-protected procurement and classified contracts should be applicable to procurement processes or contracts involving information in the confidential security class at the lowest, or information that in other respects concerns security-sensitive activities of corresponding importance for Sweden's security. The reason for this is that the security-protected procurement requirement should correspond to other protective security requirements.

Classified contracts should contain the terms and conditions for how protective security requirements are to be met by the contractor.

In the future, too, classified contracts should be entered into by central government, municipalities and county councils, but we consider that other parties that need such contracts should be able to request them from a government agency designated by the Government, preferably an agency responsible for protective security. If there are special grounds, it should be possible for a private actor to enter into classified contracts.

International cooperation

We propose that the Swedish Armed Forces be given the role of National Security Authority. However, the Swedish Armed Forces should leave other matters than such concerning record checks and security certificates for individuals to the Swedish Security Service, that primarily concern the Swedish Security Service's area of supervision. We also propose that the Defence Materiel Administration be given the role of Designated Security Authorith. The Swedish Armed Forces and the Defence Materiel Administration should be given the right to issue regulations for their respective areas of responsibility.

Security certificates for *personnel* may be issued if there is a need for such a certificate for international cooperation concerning security-sensitive activities, or if such a certificate can make it easier for a person who has their habitual residence in Sweden to take part in activities that another state or international organisation considers to be in need of protective security.

Security certificates for *facilities* may be issued if there is a need for such a certificate for international cooperation concerning security-sensitive activities, or if such a certificate can make it easier for a contractor that has its headquarters in Sweden to take part in activities that another state or international organisation considers to be in need of protective security.

A common requirement of both types of certificate is that they may only be issued if they are for participation in activities in or for a state or international organisation that is covered by an international protective security commitment.

Supervision, regulations and reporting

In some cases there are serious shortcomings in terms of compliance with the provisions and intentions of the Protective Security Act. In some respects, this is due to circumstances that cannot be influenced by reforming the protective security legislation. In other respects, we consider that the shortcomings in protective security may to some extent be related to unclear legislation and deficient knowledge about how the requirements contained in the legislation influence an organisation and can be met by it. Supervision can only influence such shortcomings to a limited extent.

In our view, supervision should be undertaken in largely the same way as today. The need for advice and support is clear, particularly for private actors conducting security-sensitive activities. There are currently not sufficient grounds for proposing such a comprehensive change in the direction and implementation of supervision that sanctions would represent. However, the issue should be followed up once a reformed Protective Security Act has been in force for some time.

Regarding how supervision is organised, we propose, among other things, simplifications to the consultation procedure for the government agencies involved. The Swedish Security Service and the Swedish Armed Forces that have the main responsibility for supervising protective security will then be able to carry out their supervisory duties more effectively and efficiently. We also propose that the Swedish Civil Contingencies Agency take over the supervisory responsibility currently held by the county administrative boards vis-à-vis certain private activities, as well as the Swedish Security Service's supervisory responsibility for municipalities and county councils.

The right to issue regulations should largely remain the same as in the current protective security legislation. This means that the right to issue regulations would be distributed primarily between the Swedish Security Service and the Swedish Armed Forces.

With regard to reporting, we propose that government agencies and other actors that are covered by the protective security legislation and that learn of activities that are a serious threat to security or that suspect that such activities are taking place should

be obliged to report this to the Swedish Security Service or the Swedish Armed Forces. This may involve incidents in which attacks are of a sophisticated nature or point to a systematic and targeted strategy on the part of an actor. Furthermore, attacks that target several activities simultaneously are likely to be serious.

Other matters

Duty of secrecy for persons taking part in security-sensitive activities

Secrecy protection is necessary for information that is of importance for Sweden's security when such information is found in private activities. We propose that the duty of secrecy provision be introduced in the Protective Security Act. The duty of secrecy should also apply to circumstances covered by a protective security commitment that is binding for Sweden. One prerequisite for the duty of secrecy should be that the position or the participation in an activity has a security classification.

Protective security in the Riksdag and the Government Offices

The Riksdag and its agencies and the Government Offices are covered to a limited extent by the protective security legislation. This system should in principle be carried over into a reformed Protective Security Act. The proposed provision on the requirement for information security classification will be central to provisions on the classification of employees in security classes, among other things. We therefore propose that this provision also apply to the above-mentioned bodies.

1 Författningsförslag

1.1 Förslag till säkerhetsskyddslag

Härigenom föreskrivs följande.

1 kap. Lagens syfte och tillämpningsområde samt definitioner

Lagens syfte och tillämpningsområde

1 § Syftet med denna lag är att säkerställa säkerhetsskyddet för verksamheter hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet, eller som omfattas av ett för Sverige i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd.

Lagen ska även i övrigt ge stöd för internationell samverkan på säkerhetsskyddsområdet.

Definitioner

2 § Med *internationellt säkerhetsskyddsåtagande* avses ett för Sverige, i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd.

3 § Med *säkerhetskänslig verksamhet* avses sådan verksamhet hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet eller omfattas av ett internationellt säkerhetsskyddsåtagande.

4 § Med *säkerhetsskyddsklassificerad uppgift* avses en uppgift som rör säkerhetskänslig verksamhet och som av den anledningen omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess, om uppgiften i stället förekommit i en verksamhet där bestämmelser om sekretess i offentlighets- och sekretesslagen gäller.

5 § Med *säkerhetsskydd* avses

1. skydd mot spionerі, sabotage, terroristbrott och andra brott som kan hota säkerhetskänslig verksamhet, samt
2. skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.

2 kap. Allmänna bestämmelser om säkerhetsskydd

Säkerhetsskyddsåtgärder

1 § Säkerhetsskyddet ska särskilt genom

1. *informationssäkerhet* förebygga dels att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, dels skadlig inverkan på andra informationstillgångar som avser säkerhetskänslig verksamhet,
2. *fysisk säkerhet* förebygga dels att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där verksamhet som av annan anledning är säkerhetskänslig bedrivs, dels skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt, och
3. *personalsäkerhet* förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av annan anledning är säkerhetskänslig (*säkerhetsprövning*) samt säkerställa att de som deltar i säkerhetskänslig verksamhet har en tillräcklig kunskap om säkerhetsskydd (*utbildning i säkerhetsskydd*).

Skyldigheter för den som är ansvarig för en säkerhetskänslig verksamhet

2 § Den som är ansvarig för en säkerhetskänslig verksamhet ska se till att

1. behovet av säkerhetsskydd utreds (*säkerhetsskyddsanalys*),
2. säkerhetsskyddsåtgärder enligt 1 § planeras och vidtas för att säkerställa det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter, samt i fråga om säkerhetsskyddsklassificerade uppgifter också är anpassat till uppgifternas informationssäkerhetsklass enligt 3 §,
3. säkerhetsskyddet kontrolleras, och
4. att sådan anmälnings- och upplysningsskyldighet som följer av förordning som har meddelats med stöd av denna lag fullgörs.

Så långt det är möjligt ska säkerhetsskyddsåtgärderna utformas så att de inte medför skada eller annan olägenhet för andra allmänna eller enskilda intressen.

Informationssäkerhetsklasser

3 § Säkerhetsskyddsklassificerade uppgifter ska utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet delas in i en informationssäkerhetsklass enligt följande

1. *Kvalificerat hemlig* vid en synnerligen allvarlig skada,
2. *Hemlig* vid en allvarlig skada,
3. *Konfidentiell* vid en inte obetydlig skada, eller
4. *Begränsad* vid en ringa skada.

Säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande ska, om de inte redan av annan stat eller mellanfolklig organisation har klassificerats, på motsvarande sätt delas in en informationssäkerhetsklass enligt första stycket utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation.

Säkerhetsskyddsavtal

4 § Vid upphandling eller ingående av ett avtal avseende varor, tjänster eller byggentreprenader där det förekommer säkerhetsskyddsklassificerade uppgifter i informationssäkerhetsklassen konfidentiell eller däröver, eller som i övrigt avser säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, ska villkor anges i ett säkerhetsskyddsavtal för hur krav på säkerhetsskydd enligt 2 § ska tillgodoses av leverantören.

Den som ingått ett säkerhetsskyddsavtal med en leverantör ska också kontrollera att de angivna villkoren om säkerhetsskydd följs och se till att sådan anmälningsskyldighet som avses i 2 § första stycket 4 fullgörs.

5 § Ett säkerhetsskyddsavtal enligt 4 § får, om det inte finns särskilda skäl, ingås endast av staten, kommuner eller landsting.

Om en upphandlande verksamhet i enlighet med första stycket inte själv får ingå ett säkerhetsskyddsavtal, ska en ansökan om ingående av säkerhetsskyddsavtal göras till den myndighet som regeringen bestämmer.

Undantag från bestämmelser om säkerhetsskydd

6 § För riksdagen och dess myndigheter gäller endast bestämmelserna om informationssäkerhetsklasser, säkerhetsprövning och säkerhetsintyg. I övrigt gäller lagen (2006:128) om säkerhetsskydd för riksdagen och dess myndigheter.

7 § Regeringen får i fråga om Regeringskansliet förordna om undantag från andra bestämmelser i lagen än sådana som gäller informationssäkerhetsklasser, säkerhetsprövning och säkerhetsintyg.

Särskilda bestämmelser om statsministerns tjänstebostäder

8 § I lagen (2014:514) om ansvar för vissa säkerhetsfrågor vid statsministerns tjänstebostäder finns särskilda bestämmelser om ansvar för fysisk säkerhet och om samrådsskyldighet inför att säkerhets-

skyddsavtal ska träffas och inför beslut om placering i säkerhetsklass.

Skyddsobjekt

9 § Bestämmelser om förbud mot tillträde till vissa byggnader, andra anläggningar, områden och andra objekt finns i skyddslagen (2010:305).

3 kap. Säkerhetsprövning

Vem som ska säkerhetsprövas

1 § Den som genom anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas. Säkerhetsprövning ska dock inte göras när det gäller

1. ledamöter av regeringen, av Europaparlamentet, av riksdagen eller av kommun- och landstingsfullmäktige, eller
2. andra uppdrag som offentliga försvarare eller ombud inför domstol än sådana som avser offentligt ombud enligt 27 kap. 27 § rättegångsbalken eller integritetsskyddsombud enligt 6 § lagen (2009:966) om Försvarsunderrättelsedomstol.

Säkerhetsprövningens syfte och dess innehåll

2 § Säkerhetsprövningen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas i denna lag och i övrigt pålitlig från säkerhetssynpunkt. Vid säkerhetsprövningen ska beaktas sådana omständigheter som kan antas innebära sårbarheter i säkerhetshänseende.

3 § En inledande säkerhetsprövning ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas. Prövningen ska innefatta en grundutredning samt registerkontroll och särskild personutredning i den omfattning som anges i 6, 7 och 10 §§. Om det finns särskilda skäl, får den inledande säkerhetsprövningen göras mindre omfattande.

Säkerhetsprövningen ska därefter följas upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.

Säkerhetsklasser

4 § En anställning eller ett annat deltagande i säkerhetskänslig verksamhet ska placeras i säkerhetsklass enligt följande.

1. *Säkerhetsklass 1*, om den anställde eller den som på annat sätt deltar i verksamheten i en omfattning som inte är ringa får del av uppgifter i informationssäkerhetsklassen kvalificerat hemlig, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka synnerligen allvarlig skada för Sveriges säkerhet.

2. *Säkerhetsklass 2*, om den anställde eller den som på annat sätt deltar i verksamheten i en omfattning som inte är ringa får del av uppgifter i informationssäkerhetsklassen hemlig eller i ringa omfattning får del av uppgifter i informationssäkerhetsklassen kvalificerat hemlig, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka allvarlig skada för Sveriges säkerhet.

3. *Säkerhetsklass 3*, om den anställde eller den som på annat sätt deltar i verksamheten får del av uppgifter i informationssäkerhetsklassen konfidentiell eller i ringa omfattning får del av uppgifter i informationssäkerhetsklassen hemlig, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka en inte obetydlig skada för Sveriges säkerhet.

En anställning eller ett annat deltagande i säkerhetskänslig verksamhet ska också i andra fall än sådana som följer av första stycket placeras i en säkerhetsklass som motsvarar de krav på säkerhetsprövning som följer av ett internationellt säkerhetsskyddsåtagande.

En anställning eller ett annat deltagande får placeras i säkerhetsklass endast om behovet av säkerhetsskydd inte kan tillgodoses på annat sätt.

Vem som beslutar om placering i säkerhetsklass

5 § Riksdagen och dess myndigheter beslutar om placering i säkerhetsklass såvitt avser riksdagens förvaltningsområde.

I övrigt beslutar regeringen om placering i säkerhetsklass. Regeringen får föreskriva att myndigheter och andra för vilka bestämmelserna om säkerhetsprövning gäller beslutar om placering i säkerhetsklass. Denna beslutanderätt får tilldelas enskilda endast om det finns särskilda skäl.

Registerkontroll

6 § Med registerkontroll avses i denna lag att uppgifter i den omfattning som följer av 12 § hämtas från register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller lagen (2010:362) om polisens allmänna spaningsregister. Med registerkontroll avses också att uppgifter som behandlas med stöd av polisdatalagen (2010:361) hämtas in.

7 § Registerkontroll ska göras om anställningen eller deltagandet i verksamheten har placerats i säkerhetsklass.

Vid registerkontroll enligt första stycket ska också uppgifter enligt 6 § löpande hämtas in under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.

8 § Om det finns särskilda skäl, får registerkontroll av någon som ska delta i en säkerhetskänslig verksamhet göras utan föregående placering i säkerhetsklass. Föreskrifter om detta meddelas av regeringen, utom såvitt gäller riksdagen och dess myndigheter.

9 § Bestämmelser om registerkontroll finns också i 4 kap. om internationell säkerhetsskyddssamverkan och säkerhetsintyg.

Särskild personutredning

10 § En särskild personutredning ska göras vid registerkontroll som avser anställning eller annat deltagande i verksamhet, om anställningen eller deltagandet i verksamheten har placerats i säkerhetsklass 1 eller 2. Utredningen ska omfatta en undersökning av den kontrollerades ekonomiska förhållanden. I övrigt ska utredningen ha den omfattning som behövs.

Krav på samtycke

11 § Registerkontroll och särskild personutredning får göras endast om den som säkerhetsprövningen gäller har lämnat sitt samtycke. Samtycket ska anses gälla också kontroller och utredningar under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.

Utlämnande av uppgifter

12 § Säkerhets- och integritetsskyddsnämnden beslutar om uppgifter som kommit fram vid registerkontroll och särskild personutredning ska lämnas ut för säkerhetsprövning. Utlämnande av uppgifter får omfatta,

1. för säkerhetsklass 1 eller 2: uppgifter om den kontrollerade som finns i något av de register som anges i 6 § eller som behandlas med stöd av polisdatalagen (2010:361). Om det är oundgängligen nödvändigt, får också motsvarande uppgifter om den kontrollerades make eller sambo lämnas ut, eller
2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret och misstankeregistret samt uppgifter som behandlas hos Säkerhetspolisen med stöd av polisdatalagen.

Om det finns synnerliga skäl, får utlämnandet omfatta även andra uppgifter än sådana som avses i första stycket.

En uppgift som har kommit fram vid registerkontroll eller särskild personutredning får lämnas ut för säkerhetsprövning endast om den i det enskilda fallet kan antas ha betydelse för prövningen av den kontrollerades pålitlighet från säkerhetssynpunkt.

13 § Innan en uppgift lämnas ut för säkerhetsprövning ska den som uppgiften avser ges tillfälle att yttra sig över uppgiften. Detta gäller dock inte om uppgiften omfattas av sekretess i förhållande till den enskilde enligt någon annan bestämmelse i offentlighets- och sekretesslagen (2009:400) än 35 kap. 3 §.

Även om uppgiften omfattas av sådan sekretess, ska den som uppgiften avser ges tillfälle att yttra sig innan uppgiften lämnas ut, om hans eller hennes intresse av att få yttra sig skäligen bör ha företräde framför det intresse som sekretessen ska skydda.

Bedömning vid säkerhetsprövning

14 § Säkerhetsprövningen innebär en bedömning enligt 2 § av en persons lämplighet för att delta i en säkerhetskänslig verksamhet. Bedömningen ska utgå från uppgifter som kommit fram vid genomförandet av grundutredningen och den kännedom som i övrigt finns om den som ska prövas, uppgifter som har lämnats ut efter registerkontroll och särskild personutredning, arten av den verksamhet för vilken prövningen görs samt omständigheterna i övrigt.

Bedömningen görs av den som beslutar om anställning eller annat deltagande i den säkerhetskänsliga verksamheten. Har någon annan ett avgörande bestämmande över den prövades lämplighet att delta i den säkerhetskänsliga verksamheten, gör dock denne den slutliga bedömningen.

Om det finns anledning till det, ska en tidigare gjord bedömning avseende en persons lämplighet för att delta i den säkerhetskänsliga verksamheten omprövas.

4 kap. Internationell säkerhetsskyddssamverkan och säkerhetsintyg

Nationell säkerhetsmyndighet

1 § Den som regeringen bestämmer ska fullgöra uppgiften som nationell säkerhetsmyndighet och nationell industrisäkerhetsmyndighet i enlighet med internationella säkerhetsskyddsåtaganden.

Säkerhetsintyg

2 § Ett säkerhetsintyg får utfärdas för personer och leverantörer när en annan stat eller mellanfolklig organisation ansökt om sådant underlag, om

1. behov av sådant intyg finns vid internationell samverkan avseende säkerhetskänslig verksamhet enligt denna lag, eller
2. intyget, utöver vad som följer av punkten 1, kan underlätta för en person som har hemvist i Sverige eller för en leverantör med säte i Sverige att delta i en verksamhet som en annan stat eller en mellanfolklig organisation bedömer vara i behov av säkerhetsskydd.

Ett intyg enligt första stycket får utfärdas endast om deltagandet avser verksamhet i eller för en stat eller mellanfolklig organisation som omfattas av ett internationellt säkerhetsskyddsåtagande. Om det finns särskilda skäl, får regeringen besluta om undantag från kravet på ett internationellt säkerhetsskyddsåtagande.

3 § En säkerhetsprövning som innefattar registerkontroll enligt 3 kap. 6 § får göras, om det behövs för att ett säkerhetsintyg ska kunna utfärdas. Vid sådan registerkontroll får också en särskild personutredning enligt 3 kap. 10 § göras.

4 § Vid ärenden om säkerhetsintyg gäller bestämmelserna om säkerhetsprövning i 3 kap. 2, 6, 10–13 §§ samt 14 § första stycket.

Registerkontroll på ansökan av en annan stat eller mellanfolklig organisation

5 § Registerkontroll enligt 3 kap. 6 § får göras när en annan stat eller mellanfolklig organisation ansökt om sådant underlag, om

1. den person som ansökan gäller har eller har haft hemvist i Sverige, och
2. personen genom anställning eller på annat sätt ska delta i en verksamhet där det för deltagandet gäller regler om registerkontroll vid säkerhetsprövning som motsvarar reglerna i denna lag.

Vid registerkontroll enligt första stycket får också en särskild personutredning enligt 3 kap. 10 § göras.

6 § Vid ärenden enligt 5 § gäller bestämmelserna om registerkontroll, särskild personutredning och samtycke i 3 kap. 6 och 10–13 §§.

Vem som beslutar om registerkontroll och utfärdar intyg

7 § Den nationella säkerhetsmyndigheten beslutar om registerkontroll enligt 3 och 5 §§ samt utfärdar intyg enligt 2 § och lämnar underlag enligt 5 §.

Om en registerkontroll föranleds av ett ärende om säkerhetsintyg för leverantör, beslutar i stället den nationella industri-

säkerhetsmyndigheten om registerkontrollen och utfärdar intyg enligt 2 §.

5 kap. Övriga bestämmelser

Tystnadsplikt

1 § Den som med stöd av denna lag har fått del av uppgifter om någon annans personliga förhållanden får inte obehörigen röja eller utnyttja dessa uppgifter.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

2 § Den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet enligt denna lag får inte obehörigen röja eller utnyttja säkerhetsskyddsklassificerade uppgifter. Tystnadsplikten gäller om anställningen eller deltagandet placerats i säkerhetsklass enligt 3 kap. 4 §.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Sekretessbrytande bestämmelse

3 § Sekretess hindrar inte att den nationella säkerhetsmyndigheten enligt 4 kap. 1 § i ett ärende om underlag för säkerhetsprövning enligt 4 kap. 5 § till en utländsk myndighet eller en mellanfolklig organisation lämnar ut en uppgift som har kommit fram vid registerkontroll eller särskild personutredning, om det står klart att ett sådant utlämnande är förenligt med svenska intressen.

Tillsyn

4 § Den som regeringen bestämmer ska utföra tillsyn över säkerhetsskyddet hos myndigheter och andra som lagen gäller för samt hos leverantörer som har träffat ett säkerhetsskyddsavtal.

Föreskrifter om verkställighet

5 § Regeringen eller den myndighet som regeringen bestämmer meddelar de närmare föreskrifter som behövs för lagens tillämpning.

---

1. Denna lag träder i kraft den 1 januari 2017.

2. Genom lagen upphävs säkerhetsskyddslagen (1996:627).

3. En anställning eller annat deltagande som enligt säkerhetsskyddslagen (1996:627) placerats i säkerhetsklass 1–3 ska motsvara en placering enligt 3 kap. 4 § i säkerhetsklass 1–3. En registerkontroll med stöd av 14 § säkerhetsskyddslagen ska i den utsträckning regeringen föreskriver motsvara ett beslut om placering i säkerhetsklass 3.

1.2 Förslag till lag om ändring i polislagen (1984:387)

Härigenom föreskrivs att 3 § polislagen (1984:387) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 §	
Till Säkerhetspolisens uppgifter hör att	
1. förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott,	
2. utreda och beivra sådana brott som anges i 1 eller som följer av 5,	
3. fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,	
4. fullgöra uppgifter enligt säkerhetsskyddslagen *(1996:627)*,	4. fullgöra uppgifter enligt säkerhetsskyddslagen *(2017:xx)*,
5. leda annan polisverksamhet om regeringen föreskriver det och i övrigt bedriva sådan verksamhet som framgår av lag eller förordning eller som regeringen uppdragit åt Säkerhetspolisen att i särskilda hänseenden ansvara för.	
När Säkerhetspolisen leder polisverksamhet enligt första stycket ska det som i lag eller annan författning föreskrivs om Polismyndigheten i tillämpliga delar gälla Säkerhetspolisen.	

Denna lag träder i kraft den 1 januari 2017.

1.3 Förslag till lag om ändring i elberedskapslagen (1997:288)

Härigenom föreskrivs att 2 § elberedskapslagen (1997:288) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §	
Beredskapslagring av bränsle som används för elproduktion omfattas av lagen endast i fråga om rätt till ersättning enligt 10 §. Särskilda bestämmelser om beredskapslagring finns i lagen (2012:806) om beredskapslagring av olja.	
I skyddslagen (2010:305) och i säkerhetsskyddslagen *(1996:627)* finns bestämmelser om tillträdesbegränsning.	I skyddslagen (2010:305) och i säkerhetsskyddslagen *(2017:xx)* finns bestämmelser om tillträdesbegränsning *och fysisk säkerhet*.

Denna lag träder i kraft den 1 januari 2017.

1.4 Förslag till lag om ändring i lagen (1998:938) om behandling av personuppgifter om totalförsvarspliktiga

Härigenom föreskrivs att 9 § lagen (1998:938) om behandling av personuppgifter om totalförsvarspliktiga ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 §	
I automatiserat register över totalförsvarspliktiga får endast följande personuppgifter föras in:	
1. personnummer eller samordningsnummer, namn, adress, telefonnummer och folkbokföringsort,	
2. hinder för genomförande av utredning som avses i 3 § första stycket, för utbildning eller för krigsplacering eller annat ianspråktagande av den registrerade för totalförsvarets räkning,	
3. boende- och familjeförhållanden samt försörjning, om uppgiften behövs för att Totalförsvarets rekryteringsmyndighet ska kunna fullgöra sina åligganden i fråga om förmåner till totalförsvarspliktiga,	
4. utbildning, anställning, kunskaper, färdigheter, anlag och intressen som har betydelse för bedömningen av den registrerades användbarhet inom totalförsvaret,	
5. fysisk och psykisk hälsa och förmåga jämte de uppgifter som ligger till grund för bedömningen härav,	
6. om den registrerade är svensk medborgare eller inte,	
7. utgången i mål om ansvar för brott mot totalförsvarsplikten,	
8. att den registrerade har dömts till påföljd för brott som framgår av uppgift ur belastningsregistret som Totalförsvarets rekryteringsmyndighet fått del av,	
9. att den registrerade genomgått säkerhetsprövning enligt säkerhetsskyddslagen *(1996:627)*, vilken säkerhetsklass prövningen avsett och resultatet av denna,	9. att den registrerade genomgått säkerhetsprövning enligt säkerhetsskyddslagen *(2017:xx)*, vilken säkerhetsklass prövningen avsett och resultatet av denna,

10. vad som bestämts vid inskrivningen enligt lagen (1994:1809) om totalförsvarsplikt eller lagen (1994:1810) om möjlighet för kvinnor att fullgöra värnplikt eller civilplikt med längre grundutbildning,

11. krigsplacering, annat ianspråktagande av den registrerade för totalförsvaret eller särskild uppgift som han eller hon ska utföra vid höjd beredskap,

12. tjänstgöring inom totalförsvaret samt betyg, vitsord, förordnanden och utmärkelser som är att hänföra till denna, samt

13. personliga förhållanden i övrigt som åberopas av den registrerade, om de rör hans eller hennes tjänstgöring inom totalförsvaret.

Andra känsliga personuppgifter än sådana uppgifter som rör hälsa eller religiös övertygelse får inte föras in i ett automatiserat register över totalförsvarspliktiga. Uppgifter om religiös övertygelse får endast registreras om den registrerade har lämnat sitt uttryckliga samtycke till att uppgifterna behandlas i registret och de rör hans eller hennes tjänstgöring inom totalförsvaret.

Denna lag träder i kraft den 1 januari 2017.

1.5 Förslag till lag om ändring i lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter

Härigenom föreskrivs att 7, 8 och 10 §§ lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
7 §	
För riksdagen och de myndigheter som avses i 1 § finns bestämmelser om säkerhetsprövning i säkerhetsskyddslagen (*1996:627*).	För riksdagen och de myndigheter som avses i 1 § finns bestämmelser om *informationssäkerhetsklass*, säkerhetsprövning *och säkerhetsintyg* i säkerhetsskyddslagen (*2017:xx*).
8 §	
När en myndighet som lagen gäller för avser att begära in anbud eller träffa avtal om upphandling där det förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess, *skall* myndigheten träffa ett skriftligt avtal (säkerhetsskyddsavtal) med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet.	När en myndighet som lagen gäller för avser att begära in anbud eller träffa avtal om upphandling där det förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess, *ska* myndigheten träffa ett skriftligt avtal (säkerhetsskyddsavtal) med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet.
Om säkerhetsskyddslagen *(1996:627)* gäller för anbudsgivaren eller leverantören på grund av *1 § 2 eller 3* i den lagen, kan anbudsgivarens eller leverantörens skyldigheter enligt lagen inte göras mindre långt-	Om säkerhetsskyddslagen *(2017:xx)* gäller för anbudsgivaren eller leverantören på grund av *1 kap. 1 §* i den lagen, kan anbudsgivarens eller leverantörens skyldigheter enligt lagen inte göras mindre långt-

gående genom villkoren i säkerhetsskyddsavtalet.	gående genom villkoren i säkerhetsskyddsavtalet.
	10 §
Av 7 § lagen (2011:745) med instruktion för Riksdagsförvaltningen framgår att Riksdagsförvaltningen får meddela föreskrifter inom sitt verksamhetsområde.	
Övriga myndigheter som avses i 1 § får meddela de närmare föreskrifter inom sitt verksamhetsområde som behövs för tillämpning av	
1. denna lag och	
2. säkerhetsskyddslagens *(1996:627)* bestämmelser om säkerhetsprövning.	2. säkerhetsskyddslagens *(2017:xx)* bestämmelser om *informationssäkerhetsklass*, säkerhetsprövning och *säkerhetsintyg.*

Denna lag träder i kraft den 1 januari 2017.

1.6 Förslag till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

Härigenom föreskrivs att 1 kap. 10 § lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
10 §	
Uppgifter om en person får behandlas för de ändamål som anges i 9 § endast om	
1. uppgifterna ger grundad anledning att anta att personen har utövat eller kan komma att utöva verksamhet som innefattar brott som kan hota rikets säkerhet eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning,	
2. uppgifterna ger grundad anledning att anta att personen har utövat eller kan komma att utöva underrättelseverksamhet riktad mot Försvarsmakten och dess säkerhetsintressen,	
3. uppgifterna ger grundad anledning att anta att personen utövar annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften *skall* behandlas,	3. uppgifterna ger grundad anledning att anta att personen utövar annan säkerhetshotande verksamhet än som avses i 1 och som innefattar brott eller åsidosättande av åligganden i anställning hos Försvarsmakten, och det finns särskilda skäl till att uppgiften *ska* behandlas,
4. personen har lämnat uppgifter om säkerhetshotande verksamhet och personuppgifterna är nödvändiga för att bedöma personens trovärdighet, eller	
5. uppgifterna avser information som har framkommit i	5. uppgifterna avser information som har framkommit i

samband med att en person har genomgått registerkontroll eller särskild personutredning enligt säkerhetsskyddslagen *(1996:627)*.

Uppgifter om en person *skall* förses med upplysning om på vilken av de i första stycket angivna grunderna uppgiften behandlas.

Om behandlingen av en personuppgift föranleds av något annat än antagande om att personen har utövat eller kommer att utöva brottslig verksamhet *skall* det särskilt anges att personen inte är misstänkt för brottslig verksamhet, om det inte på annat sätt klart framgår att sådan misstanke inte finns. Uppgifter om en person som inte heller kan antas ha utövat eller komma att utöva annan säkerhetshotande verksamhet *skall* förses med en särskild upplysning om detta, om det inte på annat sätt klart framgår att sådant antagande inte finns.

Uppgifter om en person som avses i första stycket 1–3 *skall* förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

samband med att en person har genomgått registerkontroll eller särskild personutredning enligt säkerhetsskyddslagen *(2017:xx)*.

Uppgifter om en person *ska* förses med upplysning om på vilken av de i första stycket angivna grunderna uppgiften behandlas.

Om behandlingen av en personuppgift föranleds av något annat än antagande om att personen har utövat eller kommer att utöva brottslig verksamhet *ska* det särskilt anges att personen inte är misstänkt för brottslig verksamhet, om det inte på annat sätt klart framgår att sådan misstanke inte finns. Uppgifter om en person som inte heller kan antas ha utövat eller komma att utöva annan säkerhetshotande verksamhet *ska* förses med en särskild upplysning om detta, om det inte på annat sätt klart framgår att sådant antagande inte finns.

Uppgifter om en person som avses i första stycket 1–3 *ska* förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

---

1. Denna lag träder i kraft den 1 januari 2017.

2. Föreskriften i 1 kap. 10 § första stycket 5 ska tillämpas även i fråga om registerkontroll eller särskild personutredning enligt säkerhetsskyddslagen (1996:627).

1.7 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 35 kap. 1, 3 och 10 §§ offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

35 kap.

1 §

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,

2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott

3. angelägenhet som avser *registerkontroll och särskild personutredning* enligt säkerhetsskyddslagen *(1996:627)*,	3. angelägenhet som avser säkerhetsskyddslagen *(2017:xx)*,

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. Statens medieråds verksamhet att biträda Justitiekanslern, allmän åklagare eller Polismyndigheten i brottmål,

6. register som förs av Polismyndigheten enligt 4 kap. polisdatalagen (2010:361) eller som annars behandlas med stöd av de bestämmelserna eller uppgifter som behandlas av Säkerhetspolisen med stöd av 5 kap. samma lag,

7. register som förs enligt lagen (1998:621) om misstankeregister,

8. register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,

9. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

10. register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas där med stöd av samma lag, eller

11. register som förs enligt lagen (2010:362) om polisens allmänna spaningsregister.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

3 §

Sekretess gäller i verksamhet som avser förande av eller uttag ur register enligt lagen (1998:620) om belastningsregister för uppgift i registret. I fråga om utlämnande av sådan uppgift gäller vad som är föreskrivet i den lagen och i säkerhetsskyddslagen *(1996:627)* samt i förordningar som har meddelats med stöd av dessa lagar.

Sekretess gäller i verksamhet som avser förande av eller uttag ur register enligt lagen (1998:620) om belastningsregister för uppgift i registret. I fråga om utlämnande av sådan uppgift gäller vad som är föreskrivet i den lagen och i säkerhetsskyddslagen *(2017:xx)* samt i förordningar som har meddelats med stöd av dessa lagar.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Bestämmelserna i 10 och 12 kap. gäller inte i fråga om sekretessen enligt denna paragraf.

10 §

Sekretessen enligt 1 § hindrar inte att en uppgift lämnas ut

1. till en enskild enligt vad som föreskrivs i lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

2. till en enskild enligt vad som föreskrivs i säkerhetsskyddslagen *(1996:627)* samt i förordning som har meddelats med stöd i den lagen,

2. till en enskild enligt vad som föreskrivs i säkerhetsskyddslagen *(2017:xx)* samt i förordning som har meddelats med stöd i den lagen,

3. enligt vad som föreskrivs i

– lagen (1998:621) om misstankeregister,

– polisdatalagen (2010:361),

– lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar,

– lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet,

– kustbevakningsdatalagen (2012:145),

– förordningar som har stöd i dessa lagar, eller

4. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.

---

1. Denna lag träder i kraft den 1 januari 2017.

2. För angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627) gäller 35 kap. 1 § första stycket 3 i sin äldre lydelse.

1.8 Förslag till lag om ändring i polisdatalagen (2010:361)

Härigenom föreskrivs att 5 kap. 2 § polisdatalagen (2010:361) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

5 kap.

1 §

Personuppgifter får behandlas i Säkerhetspolisens brottsbekämpande verksamhet om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

a) brott mot rikets säkerhet,

b) terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott,

c) brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, eller

d) tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,

2. utreda eller beivra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,

3. fullgöra uppgifter i samband med personskydd,

4. fullgöra uppgifter enligt säkerhetsskyddslagen *(1996:627)*,

4. fullgöra uppgifter enligt säkerhetsskyddslagen *(2017:xx)*,

5. fullgöra förpliktelser som följer av internationella åtaganden, eller

6. lämna tekniskt biträde till Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket

---

Denna lag träder i kraft den 1 januari 2017.

1.9 Förslag till lag om ändring av lagen (2010:1767) om geografisk miljöinformation

Härigenom föreskrivs att 15 § lagen (2010:1767) om geografisk miljöinformation ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

15 §

Bestämmelser om

1. behandling av personuppgifter finns i personuppgiftslagen (1998:204),

2. behandling av personuppgifter i fastighetsregistret finns i lagen (2000:224) om fastighetsregister,

3. krav på tillstånd för upprättande av databaser med landskapsinformation samt för spridning av kartor och andra sammanställningar av landskapsinformation finns i lagen (1993:1742) om skydd för landskapsinformation,

4. säkerhetsskydd finns i säkerhetsskyddslagen *(1996:627)*, och	4. säkerhetsskydd finns i säkerhetsskyddslagen *(2017:xx)*, och

5. upphovsrätt finns i lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk.

I fråga om behandling av personuppgifter enligt denna lag gäller inte 2 § personuppgiftslagen (1998:204).

Denna lag träder i kraft den 1 januari 2017.

1.10 Förslag till lag om ändring i lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet

Härigenom föreskrivs att 2 kap. 22 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet ska följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 kap.
	22 §
Med säkerhetsskyddsklassificerade uppgifter avses information och material oavsett form, karaktär eller överföringsteknik som omfattas av krav på en viss säkerhetsnivå eller en viss skyddsnivå och som med hänsyn till *rikets* säkerhet enligt lagar och andra författningar måste skyddas mot intrång, förstörelse, avlägsnande, spridning, förlust eller åtkomst av någon obehörig person, eller någon annan typ av risk.	Med säkerhetsskyddsklassificerade uppgifter avses *i denna lag* information och material oavsett form, karaktär eller överföringsteknik som omfattas av krav på en viss säkerhetsnivå eller en viss skyddsnivå och som med hänsyn till *Sveriges* säkerhet enligt lagar och andra författningar måste skyddas mot intrång, förstörelse, avlägsnande, spridning, förlust eller åtkomst av någon obehörig person, eller någon annan typ av risk. *För skydd av säkerhetsskyddsklassificerade uppgifter finns bestämmelser i säkerhetsskyddslagen (2017:xx).*

Denna lag träder i kraft den 1 januari 2017.

1.11 Förslag till lag om ändring i lagen (2014:514) om ansvar för vissa säkerhetsfrågor vid statsministerns tjänstebostäder

Härigenom föreskrivs att 1, 2, 4 och 5 §§ lagen (2014:514) om ansvar för vissa säkerhetsfrågor vid statsministerns tjänstebostäder ska följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Denna lag innehåller särskilda bestämmelser som rör verksamheten vid och skyddet för egendom som används som tjänstebostad för statsministern. Bestämmelserna utgör kompletteringar till och undantag från säkerhetsskyddslagen *(1996:627)* och skyddslagen (2010:305).	Denna lag innehåller särskilda bestämmelser som rör verksamheten vid och skyddet för egendom som används som tjänstebostad för statsministern. Bestämmelserna utgör kompletteringar till och undantag från säkerhetsskyddslagen (*2017:xx*) och skyddslagen (2010:305).
2 §	
Säkerhetspolisen har det ansvar för *tillträdesbegränsning* som anges i *7 § 2* säkerhetsskyddslagen *(1996:627)* vid egendom som används som tjänstebostad för statsministern.	Säkerhetspolisen har det ansvar för *fysisk säkerhet* som anges i *2 kap. 1 § 2* säkerhetsskyddslagen *(2017:xx)* vid egendom som används som tjänstebostad för statsministern.
Inför att *tillträdesbegränsande åtgärder* vidtas ska Säkerhetspolisen samråda med den eller de myndigheter som förvaltar egendomen och som berörs av åtgärden. När det gäller *tillträdesbegränsande åtgärder* som är av större betydelse ska Säkerhetspolisen även samråda	Inför att *åtgärder avseende fysisk säkerhet* vidtas ska Säkerhetspolisen samråda med den eller de myndigheter som förvaltar egendomen och som berörs av åtgärden. När det gäller *åtgärder avseende fysisk säkerhet* som är av större betydelse ska Säkerhetspolisen även

med Regeringskansliet.	samråda med Regeringskansliet.
4 §	
Inför att säkerhetsskyddsavtal ska träffas enligt *8 §* säkerhetsskyddslagen *(1996:627)* med anledning av upphandling till egendom som används som tjänstebostad för statsministern ska den upphandlande myndigheten samråda med Säkerhetspolisen.	Inför att säkerhetsskyddsavtal ska träffas enligt *2 kap. 4 §* säkerhetsskyddslagen *(2017:xx)* med anledning av upphandling till egendom som används som tjänstebostad för statsministern ska den upphandlande myndigheten samråda med Säkerhetspolisen
5 §	
Inför beslut om placering i säkerhetsklass enligt *17 §* säkerhetsskyddslagen *(1996:627)* av anställningar eller annat deltagande i verksamheten vid egendom som används som tjänstebostad för statsministern ska den som bedriver verksamheten samråda med Säkerhetspolisen.	Inför beslut om placering i säkerhetsklass enligt *3 kap. 4 §* säkerhetsskyddslagen *(2017:xx)* av anställningar eller annat deltagande i verksamheten vid egendom som används som tjänstebostad för statsministern ska den som bedriver verksamheten samråda med Säkerhetspolisen.

Denna lag träder i kraft den 1 januari 2017.

1.12 Förslag till säkerhetsskyddsförordning

Härigenom föreskrivs följande.

1 kap. Tillämpningsområde och definitioner

Tillämpningsområde

1 § I denna förordning finns kompletterande föreskrifter om säkerhetsskydd enligt säkerhetsskyddslagen (2017:xx). Begrepp och uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen.

Föreskrifterna gäller inte för riksdagen och dess myndigheter.

2 § För Regeringskansliet gäller endast bestämmelser om informationssäkerhetsklasser, säkerhetsskyddsavtal, säkerhetsprövning och säkerhetsintyg i säkerhetsskyddslagen (2017:xx) samt bestämmelser om säkerhetsskyddsavtal, säkerhetsprövning och säkerhetsintyg i denna förordning.

För sådana kommittéer och särskilda utredare som avses i kommittéförordningen (1976:119) gäller endast bestämmelser om informationssäkerhetsklasser, säkerhetsprövning och säkerhetsintyg i säkerhetsskyddslagen samt bestämmelser om säkerhetsprövning och säkerhetsintyg i denna förordning.

3 § Vad som i denna förordning föreskrivs om myndigheter gäller också vid säkerhetskänslig verksamhet som bedrivs i annan form hos staten, kommuner, landsting och enskilda.

Definitioner

4 § Med *säkerhetsskyddsstödjande myndighet* avses en myndighet som, för det verksamhetsområde som anges i andra stycket, har uppgifter enligt denna förordning i fråga om ingående av säkerhetsskyddsavtal, beslut om placering i säkerhetsklass, rådgivning och tillsyn avseende bolag, föreningar, stiftelser och enskilda näringsidkare som bedriver säkerhetskänslig verksamhet.

Säkerhetsskyddsstödjande myndighet är

1. Affärsverket svenska kraftnät för elförsörjningsverksamhet,

2. Transportstyrelsen för civil flygtransportverksamhet och verksamhet som i övrigt är av betydelse för luftfartsskydd, eller av betydelse för hamnskydd och sjöfartsskydd,

3. Post- och telestyrelsen för verksamhet som avser elektronisk kommunikation, och

4. Myndigheten för samhällsskydd och beredskap för andra säkerhetskänsliga verksamheter än sådana som anges i 1–3.

Myndigheten för samhällsskydd och beredskap är dessutom säkerhetsskyddstödjande myndighet för kommuner och landsting när det gäller rådgivning och tillsyn.

5 § Staten, en eller flera kommuner eller landsting ska anses utöva ett *rättsligt bestämmande inflytande* över ett aktiebolag, handelsbolag, en förening eller en stiftelse, om den eller de ensamma eller tillsammans

1. äger aktier i ett aktiebolag eller andelar i en ekonomisk förening med fler än hälften av samtliga röster i bolaget eller föreningen eller på något annat sätt förfogar över så många röster i bolaget eller föreningen,

2. har rätt att utse eller avsätta fler än hälften av ledamöterna i styrelsen för ett aktiebolag, en förening eller en stiftelse, eller

3. utgör samtliga obegränsat ansvariga bolagsmän i ett handelsbolag.

Vid tillämpningen av 1–3 ska inflytande anses vara utövat av staten, om inflytandet utövas av en juridisk person över vilken staten bestämmer på det sätt som anges i punkterna. Motsvarande gäller i fråga om kommuner och landsting.

6 § Med *säkerhetsskyddsklassificerad handling* avses handling som innehåller säkerhetsskyddsklassificerad uppgift enligt 1 kap. 4 § säkerhetsskyddslagen (2017:xx).

7 § Med *it-system* avses ett system av sammansatt mjuk- och hårdvara som behandlar information.

2 kap. Allmänna bestämmelser om säkerhetsskydd

Säkerhetsskyddsanalys och säkerhetsskyddsplanering

1 § Bestämmelser om säkerhetsskyddsanalys finns i 2 kap. 2 § säkerhetsskyddslagen (2017:xx). Genom sådan analys ska säkerhetsskyddsklassificerade uppgifter och vad som i övrigt behöver ett säkerhetsskydd identifieras samt säkerhetshot och potentiella konsekvenser, sårbarheter och behovet av säkerhetsskyddsåtgärder bedömas.

Säkerhetsskyddsanalysen ska ligga till grund för planeringen av verksamhetens säkerhetsskydd. Analysen ska dokumenteras och hållas uppdaterad.

2 § Vid verksamhet som förordningen gäller för ska det, om det inte är uppenbart obehövligt, finnas en säkerhetsskyddschef som utövar kontroll över säkerhetsskyddet och i övrigt ansvarar för att skyldigheter som följer av 2 kap. 2 och 4 §§ säkerhetsskyddslagen (2017:xx) fullgörs.

Ingående av säkerhetsskyddsavtal

3 § Sveriges Radio Aktiebolag, Sveriges Televison Aktiebolag, Teracom Aktiebolag och Teracom Boxer Group Aktiebolag får ingå säkerhetsskyddsavtal när det gäller den egna verksamheten.

En ansökan enligt 2 kap. 4 § säkerhetsskyddslagen (2017:xx) om ingående av säkerhetsskyddsavtal från en upphandlande verksamhet som inte själv får ingå sådant avtal ska i fråga om

1. bolag, föreningar och stiftelser där en myndighet som anges i bilagan till denna förordning, en kommun eller ett landsting utövar ett rättsligt bestämmande inflytande göras till den som utövar sådant bestämmande inflytande, och
2. i övrigt till den säkerhetsskyddsstödjande myndigheten.

4 § Vid förhandlingar om sådana säkerhetsskyddsavtal som avses i 2 kap. 4 § säkerhetsskyddslagen (2017:xx) företräds det allmänna av den myndighet, kommun eller landsting som avser att begära in anbud eller träffa avtal eller som uppdrar åt annan att begära in anbud eller träffa avtal.

Säkerhetsskyddsavtal vid behov av underlag för säkerhetsintyg

5 § Den nationella industrisäkerhetsmyndigheten enligt 8 kap. 1 § får träffa avtal om säkerhetsskydd med en leverantör, om det behövs för att utfärda säkerhetsintyg enligt 4 kap. 2 § säkerhetsskyddslagen (2017:xx).

Anmälan om ingående eller upphörande av säkerhetsskyddsavtal

6 § Den som ingår ett säkerhetsskyddsavtal enligt 2 kap. 4 § säkerhetsskyddslagen (2017:xx) eller 5 § ska anmäla det till Säkerhetspolisen. Om avtalet upphör vid annan tidpunkt än vad som anges i avtalet, ska också upphörandet av avtalet anmälas till Säkerhetspolisen.

I fråga om sådana säkerhetsskyddsavtal som avses i 5 § ska anmälan enligt första stycket göras också till den nationella säkerhetsmyndigheten enligt 8 kap. 1 §.

Överlåtelse av säkerhetskänslig verksamhet

7 § En myndighet eller annan som planerar att i en betydande omfattning överlåta säkerhetskänslig verksamhet ska anmäla det till den myndighet som enligt 9 kap. 9 eller 10 § ska utföra tillsyn.

8 § När säkerhetskänslig verksamhet överlåts till en enskild ska den överlåtande parten upplysa om att säkerhetsskyddslagen (2017:xx) gäller för verksamheten. En sådan upplysning ska innehålla en erinran om de skyldigheter som enligt 2 kap. 2 och 4 §§ säkerhetsskyddslagen gäller för den som är ansvarig för en säkerhetskänslig verksamhet.

3 kap. Säkerhetsskyddsklassificerade uppgifter

Anteckning om informationssäkerhetsklass

1 § En säkerhetsskyddsklassificerad handling ska märkas så att de framgår vilken informationssäkerhetsklass uppgifterna i handlingen har. Om handlingen innehåller uppgifter med olika informations-

säkerhetsklass, ska den högsta informationssäkerhetsklassen avgöra vilken märkning handlingen ska ha.

Om en säkerhetsskyddsklassificerad handling kan antas komma att lämnas över till utländska myndigheter eller leverantörer, ska den förses med en markering om ursprungsland.

Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter

2 § Om inte något annat följer av bestämmelser i lag, är endast den behörig att ta del av säkerhetsskyddsklassificerade uppgifter som

1. bedöms pålitlig från säkerhetssynpunkt,
2. har tillräckliga kunskaper om säkerhetsskydd, och
3. behöver uppgifterna för sitt arbete eller annat deltagande i den verksamhet där de säkerhetsskyddsklassificerade uppgifterna förekommer.

3 § Den som tillåts ta del av säkerhetsskyddsklassificerade uppgifter ska upplysas om räckvidden och innebörden av den sekretess och tystnadsplikt som följer av offentlighets- och sekretesslagen (2009:400) eller 5 kap. 2 § säkerhetsskyddslagen (2017:xx).

Skydd för säkerhetsskyddsklassificerade uppgifter som lämnas till en utländsk myndighet eller mellanfolklig organisation

4 § Säkerhetsskyddsklassificerade uppgifter som lämnas till en utländsk myndighet eller en mellanfolklig organisation ska omfattas av ett internationellt säkerhetsskyddsåtagande hos den mottagande myndigheten eller organisationen, om det inte finns särskilda skäl för att sådana uppgifter ändå kan lämnas.

I 8 kap. 3 § offentlighets- och sekretesslagen (2009:400) samt i förordningen (2010:649) om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet finns det bestämmelser om när uppgifter som omfattas av sekretess får lämnas till en utländsk myndighet eller en mellanfolklig organisation.

4 kap. Informationssäkerhet

1 § Den som avser att inrätta ett it-system som ska användas för säkerhetskänslig verksamhet ska analysera vilka krav på skydd som finns och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses.

2 § Innan ett it-system, som kan förutses komma att behandla säkerhetsskyddklassificerade uppgifter i informationssäkerhetsklassen konfidentiell eller däröver inrättas eller i väsentliga avseenden förändras ska myndigheten eller den som förordningen i övrigt gäller för skriftligen samråda med Säkerhetspolisen. Om myndigheten hör till Försvarsmaktens tillsynsområde enligt 9 kap. 9 § 1, ska den i stället samråda med Försvarsmakten.

Vad som anges i första stycket gäller även i fråga om it-system som är av motsvarande betydelse för Sveriges säkerhet, även om de inte behandlar säkerhetsskyddsklassificerade uppgifter.

3 § Ett it-system som av flera personer ska användas för behandling av säkerhetsskyddsklassificerade uppgifter ska vara försett med funktioner för behörighetskontroll, registrering av händelser i systemet som är av betydelse för säkerheten, skydd mot obehörig avlyssning, intrångsskydd, skydd mot skadlig kod samt skydd mot röjande signaler.

Ett it-system enligt första stycket får inte tas i drift förrän det har ackrediterats av den för vars verksamhet systemet inrättas.

Säkerhetspolisen får föreskriva eller besluta om undantag från kravet i första stycket. Om det gäller verksamhet som hör till Försvarsmaktens tillsynsområde enligt 9 kap. 9 § 1, får i stället Försvarsmakten föreskriva eller besluta om sådant undantag.

4 § Myndigheter och andra som förordningen gäller för ska, innan de behandlar säkerhetsskyddsklassificerade uppgifter i ett it-system utanför deras kontroll, försäkra sig om att det för uppgifterna där finns ett tillräckligt säkerhetsskydd.

Om säkerhetsskyddsklassificerade uppgifter ska kommuniceras och skyddas med hjälp av kryptografiska funktioner, ska dessa ha godkänts av Försvarsmakten.

Säkerhetspolisen får föreskriva eller besluta om undantag från kravet i andra stycket utom då kravet följer av ett internationellt säkerhetsskyddsåtagande. Om det gäller verksamhet som hör till Försvarsmaktens tillsynsområde enligt 9 kap. 9 § 1, får i stället Försvarsmakten föreskriva eller besluta om sådant undantag.

5 § För försändelser till utlandet med säkerhetsskyddsklassificerade handlingar, som innehåller uppgifter i informationssäkerhetsklassen konfidentiell eller däröver, ska Utrikesdepartementets kurirförbindelser anlitas.

Säkerhetspolisen får föreskriva eller besluta om undantag från kravet i första stycket. Om det gäller verksamhet som hör till Försvarsmaktens tillsynsområde enligt 9 kap. 9 § 1, får i stället Försvarsmakten föreskriva eller besluta om sådant undantag.

6 § Säkerhetsskyddsklassificerade handlingar som märkts som kvalificerat hemliga ska inventeras minst en gång per år. Säkerhetsskyddsklassificerade handlingar som märkts som hemliga eller konfidentiella ska inventeras i den omfattning som anges i Säkerhetspolisen föreskrifter eller, om det gäller verksamhet som hör till Försvarsmaktens tillsynsområde enligt 9 kap. 9 § 1, Försvarsmaktens föreskrifter.

Kravet på inventering gäller inte för handlingar som är arkiverade.

5 kap. Personalsäkerhet

Genomförandet av säkerhetsprövningen

1 § Med grundutredning enligt 3 kap. 3 § säkerhetsskyddslagen (2017:xx) avses en utredning om personliga förhållanden av betydelse för säkerhetsprövningen. Den ska avse bland annat betyg, intyg, referenser samt uppgifter som den som prövningen avser har lämnat. Identitetskontroll ska göras, om det inte är obehövligt.

2 § I 7 kap. 1 och 3–14 §§ finns bestämmelser om registerkontroll och särskild personutredning som föranleds av ett beslut om placering i säkerhetsklass. Ansökan om registerkontroll och särskild personutredning ska inte göras om det redan mot bak-

grund av vad som kommit fram vid grundutredningen står klart att det är olämpligt att den som prövningen avser deltar i den säkerhetskänsliga verksamheten.

3 § Av 6 kap. 1 och 3 §§ och 7 kap. 5 § följer att en myndighet i vissa fall ska besluta om placering i säkerhetsklass och vid Säkerhetspolisen ansöka om registerkontroll i fråga om någon som inte ska anlitas i den egna verksamheten. Myndigheten ska inte bedöma uppgifter som lämnas ut vid sådan kontroll utan endast redovisa resultatet till den verksamhet som berörs. Det gäller dock inte om det följer av 3 kap. 14 § andra stycket säkerhetsskyddslagen (2017:xx) att myndigheten ska göra den slutliga bedömningen i fråga om säkerhetsprövningen. I sådana fall ska myndigheten, om inte särskilda skäl talar emot det, samråda med den berörda arbetsgivaren.

Dokumentation av säkerhetsprövning

4 § Säkerhetsprövningen ska dokumenteras.

Utbildning i säkerhetsskydd

5 § Den som är ansvarig för en säkerhetskänslig verksamhet ska se till att den som ska anställas eller på annat sätt delta i verksamheten får utbildning i säkerhetsskydd i den utsträckning som behövs. Behovet av utbildning ska följas upp under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.

6 kap. Beslut om placering i säkerhetsklass

1 § Kommuner, landsting och de myndigheter som anges i bilagan till denna förordning beslutar om

1. placering i säkerhetsklass 2 och 3 i fråga om anställning eller annat deltagande i den egna verksamheten och hos bolag, föreningar och stiftelser som de utövar ett rättsligt bestämmande inflytande över, samt

2. placering i säkerhetsklass i fråga om anställning eller uppdrag hos en leverantör med vilken de har ingått säkerhetsskyddsavtal enligt 2 kap. 4 § säkerhetsskyddslagen (2017:xx).

Utöver vad som följer av första stycket beslutar Regeringskansliet också om placering i säkerhetsklass 2 och 3 i fråga om anställning eller annat deltagande i sådan verksamhet som avses i 1 § kommittéförordningen (1998:1474).

2 § Sveriges Radio Aktiebolag, Sveriges Televison Aktiebolag, Teracom Aktiebolag och Teracom Boxer Group Aktiebolag beslutar om placering i säkerhetsklass 2 och 3 i fråga om anställning eller annat deltagande i den egna verksamheten.

3 § I andra fall än de som anges i 1 och 2 §§ beslutar den säkerhetsskyddsstödjande myndigheten om placering i säkerhetsklass 2 och 3 i fråga om anställning eller annat deltagande i verksamhet hos bolag, föreningar, stiftelser och enskilda näringsidkare enligt de ansvarsområden som anges i 1 kap. 4 §.

4 § Om en kommun, ett landsting eller en sådan myndighet som anges i 1 § eller 3 § bedömer att det finns behov av att placera en anställning eller annat deltagande i säkerhetsklass 1, ska myndigheten, kommunen eller landstinget begära att regeringen beslutar om sådan placering. Motsvarande gäller för bolag som anges i 2 §.

7 kap. Registerkontroll

Registerkontroll vid placering i säkerhetsklass

1 § Av ett beslut om att en anställning eller annat deltagande i säkerhetskänslig verksamhet ska placeras i säkerhetsklass följer att säkerhetsprövning vid sådan anställning eller sådant deltagande ska omfatta registerkontroll i enlighet med 3 kap. 6 § säkerhetsskyddslagen (2017:xx). Av ett sådant beslut följer också att en särskild personutredning ska göras vid registerkontrollen i den utsträckning som anges i 3 kap. 10 § säkerhetsskyddslagen.

Registerkontroll utan placering i säkerhetsklass

2 § Registerkontroll av den som ska delta i säkerhetskänslig verksamhet får göras utan placering i säkerhetsklass om det finns särskilda skäl. Regeringen beslutar om sådan registerkontroll.

Vid större evenemang, statsbesök eller andra liknade händelser får regeringen överlåta åt Säkerhetspolisen att besluta om sådan registerkontroll.

Närmare förutsättningar för registerkontroll

3 § Registerkontroll får göras endast om den som säkerhetsprövningen avser kan antas komma att anställas eller på annat sätt delta i den aktuella verksamheten. Om det finns synnerliga skäl, får kontroll göras utan ett sådant antagande.

4 § Registerkontroll vid anställning eller deltagande som placerats i säkerhetsklass 1 eller 2 ska göras på nytt, om det finns anledning till det.

Utförande av registerkontroll

5 § Säkerhetspolisen ska utföra registerkontroll efter ansökan från den som beslutat om placering i säkerhetsklass eller från sådant bolag som avses i 6 § eller från den som i annat fall beslutat om registerkontroll.

När regeringen beslutat om placering i säkerhetsklass ska, om inte annat anges i beslutet, kontrollen utföras efter ansökan från den som beslutar om placering i säkerhetsklass 2 och 3.

6 § Om det finns särskilda skäl, får en säkerhetsskyddsstödjande myndighet besluta att ett bolag med anledning av ett beslut om placering i säkerhetsklass får ansöka vid Säkerhetspolisen om registerkontroll.

7 § Till en ansökan om registerkontroll ska bifogas uppgift om lämnat samtycke enligt 3 kap. 11 § säkerhetsskyddslagen (2017:xx) och uppgift om placering i säkerhetsklass eller, om register-

kontrollen inte föranleds av ett beslut om placering i säkerhetsklass, beslut om registerkontroll. Om registerkontrollen avser anställning eller annat deltagande i verksamhet som har placerats i säkerhetsklass 1 eller 2, ska också ett skriftligt underlag bifogas där den som kontrollen avser har lämnat uppgifter om sina personliga förhållanden.

8 § Säkerhetspolisens uppgift att utföra registerkontrollen innefattar också uppgiften att göra en särskild personutredning enligt 3 kap. 10 § säkerhetsskyddslagen. När det gäller en anställning eller annat deltagande i verksamhet som har placerats i säkerhetsklass 1 ska sådan utredning omfatta även andra personliga förhållanden än de ekonomiska, om det inte är obehövligt. Om det finns särskilda skäl, ska också en utredning som avser anställningar och annat deltagande i verksamhet som har placerats i säkerhetsklass 2 omfatta sådana förhållanden.

9 § När den särskilda personutredningen avser anställningar och annat deltagande i verksamhet som har placerats i säkerhetsklass 1, ska Säkerhetspolisen hålla ett personligt samtal med den som prövningen gäller. Ett sådant samtal får dock underlåtas, om det står klart att det inte behövs.

Ett personligt samtal ska, om det behövs, hållas också när utredningen avser anställningar och annat deltagande i verksamhet som har placerats i säkerhetsklass 2.

Handläggningen av frågan om utlämnande av uppgifter

10 § Om det vid registerkontrollen kommer fram uppgifter som antas kunna vara av betydelse för säkerhetsprövningen, ska Säkerhetspolisen underställa Säkerhets- och integritetsskyddsnämnden frågan om uppgifter ska lämnas ut enligt 3 kap. 12 § säkerhetsskyddslagen (2017:xx).

11 § Säkerhets- och integritetsskyddsnämnden ska avgöra om den som en uppgift avser ska ges tillfälle att yttra sig över uppgiften enligt 3 kap. 13 § säkerhetsskyddslagen (2017:xx). Säkerhets- och integritetsskyddsnämnden ska vid sin prövning av denna fråga

överväga om ett personligt samtal bör hållas med den kontrollerade. Om Säkerhets- och integritetsskyddsnämnden finner att den som uppgiften avser ska ges tillfälle att yttra sig över uppgiften eller att ett personligt samtal ska hållas med denne, ska nämnden uppdra åt Säkerhetspolisen att inhämta yttrande eller hålla personligt samtal med den kontrollerade. Yttranden som kommit in till Säkerhetspolisen och uppgifter som kommit fram vid personligt samtal ska redovisas för Säkerhets- och integritetsskyddsnämnden.

12 § En uppgift som efter beslut av Säkerhets- och integritetsskyddsnämnden ska lämnas ut för säkerhetsprövning får inte åtföljas av något annat yttrande än en förtydligande kommentar till uppgiften.

13 § Det får inte framgå av svaret på en ansökan om registerkontroll att det finns en uppgift om den kontrollerade som inte lämnas ut.

Avanmälan

14 § Vid upphörande av en anställning eller annat deltagande som föranlett placering i säkerhetsklass eller vid en omplacering till en lägre säkerhetsklass ska verksamhetens säkerhetsskyddschef skyndsamt anmäla till Säkerhetspolisen att registerkontrollen ska avslutas eller anpassas till den lägre säkerhetsklassen. Sådan avanmälan ska göras också om ett deltagande i den säkerhetskänsliga verksamheten inte längre är aktuellt.

8 kap. Internationell samverkan och säkerhetsintyg

1 § Försvarsmakten ska vara nationell säkerhetsmyndighet och Försvarets materielverk nationell industrisäkerhetsmyndighet enligt 4 kap. 1 § säkerhetsskyddslagen (2017:xx).

Försvarsmakten ska, i fråga om andra ärenden än sådana som avses i 4 kap. 2 och 5 §§ säkerhetsskyddslagen, till Säkerhetspolisen lämna över ärenden som rör främst Säkerhetspolisens tillsynsområde enligt 9 kap. 9 § 2. Innan sådant överlämnade ska Försvarsmakten samråda med Säkerhetspolisen. Försvarsmakten och

Säkerhetspolisen får komma överens om att ärendet ska handläggas av Försvarsmakten.

2 § Om en person eller en leverantör ansöker om ett säkerhetsintyg enligt 4 kap. 2 § säkerhetsskyddslagen (2017:xx), får en tidigare gjord säkerhetsprövning eller ett tidigare träffat säkerhetsskyddsavtal i den utsträckning som är lämpligt läggas till grund för utfärdande av ett sådant intyg. Föreskrifter om detta meddelas av Försvarsmakten och Försvarets materielverk i den utsträckning som följer av 9 kap. 2 och 3 §§.

3 § Bestämmelserna i 5 och 7 kap. gäller i tillämpliga delar vid ärenden enligt 4 kap. 2 och 5 §§ säkerhetsskyddslagen (2017:xx).

9 kap. Föreskrifter, rådgivning och tillsyn

Föreskrifter

1 § Säkerhetspolisen får meddela närmare föreskrifter om verkställigheten av säkerhetsskyddslagen (2017:xx) i fråga om förfarandet vid registerkontroll, om inte annat följer av 2 och 3 §§.

2 § Försvarsmakten får meddela närmare föreskrifter om verkställigheten av säkerhetsskyddslagen (2017:xx) i fråga om internationella säkerhetsskyddsåtaganden, utfärdande av säkerhetsintyg för personer enligt 4 kap. 2 § säkerhetsskyddslagen, registerkontroll enligt 4 kap. 5 § säkerhetsskyddslagen, samt om kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet. Försvarsmakten ska innan sådana föreskrifter meddelas samråda med Säkerhetspolisen.

3 § Försvarets materielverk får meddela närmare föreskrifter om verkställigheten av säkerhetsskyddslagen (2017:xx) i fråga om utfärdande av säkerhetsintyg för leverantörer enligt 4 kap. 2 § säkerhetsskyddslagen. Försvarets materielverk ska innan sådana föreskrifter meddelas samråda med Försvarsmakten och Säkerhetspolisen.

4 § Utöver vad som följer av 1–3 §§ får Säkerhetspolisen, med undantag av Försvarsmaktens tillsynsområde enligt 9 § 1, meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (2017:xx). Säkerhetspolisen ska innan sådana föreskrifter meddelas samråda med Försvarsmakten. Motsvarande gäller i fråga om föreskrifter enligt 4 kap. 3–6 §§.

Försvarsmakten får, utöver vad som följer av 1–3 §§, meddela föreskrifter för sitt tillsynsområde. Försvarsmakten ska innan sådana föreskrifter meddelas samråda med Säkerhetspolisen. Motsvarande gäller i fråga om föreskrifter enligt 4 kap. 3–6 §§.

5 § En säkerhetsskyddsstödjande myndighet får för sitt ansvarsområde enligt 1 kap. 4 § meddela föreskrifter som kompletterar föreskrifter meddelade av Säkerhetspolisen, Försvarsmakten och Försvarets materielverk med stöd av 1–4 §§. Om det inte är obehövligt, ska myndigheterna innan sådana föreskrifter meddelas samråda med Säkerhetspolisen, Försvarsmakten och Försvarets materielverk.

6 § Myndigheter för vilka säkerhetsskyddslagen (2017:xx) gäller ska meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen i fråga om säkerhetsskyddet för sin egen verksamhet, om det inte är obehövligt. En myndighet ska innan sådana föreskrifter meddelas samråda med Säkerhetspolisen. Om myndigheten omfattas av Försvarsmaktens tillsynsområde enligt 9 § 1, ska den i stället samråda med Försvarsmakten.

Rådgivning

7 § Säkerhetspolisen och Försvarsmakten ska på begäran lämna råd om säkerhetsskydd till Regeringskansliet, riksdagen och dess myndigheter samt till Justitiekanslern. Sådan rådgivning ska samordnas av Säkerhetspolisen.

8 § De säkerhetsskyddsstödjande myndigheterna ska inom sina respektive ansvarsområden lämna råd i fråga om skyldigheter som följer av säkerhetsskyddslagen (2017:xx).

Tillsyn

9 § Tillsyn över säkerhetsskyddet ska utföras av

1. Försvarsmakten när det gäller Fortifikationsverket och Försvarshögskolan samt de myndigheter som hör till Försvarsdepartementet,
2. Säkerhetspolisen när det gäller övriga myndigheter utom Justitiekanslern, och
3. de säkerhetsskyddsstödjande myndigheterna enligt de ansvarsområden som följer av 1 kap. 4 §.

Tillsyn enligt första stycket får avse även verksamhet som omfattas av ett säkerhetsskyddsavtal samt verksamhet hos bolag, föreningar och stiftelser som den verksamhet som tillsynen avser utövar ett rättsligt bestämmande inflytande över. Om inte särskilda skäl talar emot, ska tillsynen utföras i samråd med den avtalsslutande myndigheten, kommunen eller landstinget.

10 § Utöver vad som följer av 9 § andra stycket får tillsyn över bolag, föreningar, stiftelser och enskilda näringsidkare utföras också av Säkerhetspolisen och Försvarsmakten. Säkerhetspolisen får även utföra tillsyn över kommuner och landsting. Om inte särskilda skäl talar emot det, ska tillsynen utföras i samråd med den myndighet som ska utföra tillsyn enligt 9 § 3.

Säkerhetspolisen får besluta att myndigheten ska utföra tillsynen över en leverantör som har uppdrag för flera myndigheter, kommuner eller landsting och där leverantörens samlade uppdrag är av stor betydelse för Sveriges säkerhet.

10 kap. Övriga bestämmelser

Anmälan vid röjande av en säkerhetsskyddsklassificerad uppgift

1 § Om en säkerhetsskyddsklassificerad uppgift i informationssäkerhetsklassen konfidentiell eller däröver kan ha röjts, ska det skyndsamt anmälas till Säkerhetspolisen Om sådan uppgift omfattas av ett internationellt säkerhetsskyddsåtagande eller om det gäller en verksamhet som hör till Försvarsmaktens tillsynsområde enligt 9 kap. 9 § 1, ska anmälan göras också till Försvarsmakten.

Anmälan vid allvarlig säkerhetshotande verksamhet

2 § Om myndigheter och andra som förordningen gäller för får kännedom om allvarlig säkerhetshotande verksamhet eller misstänker sådan verksamhet ska de skyndsamt rapportera förhållandet till den myndighet som enligt 9 kap. 9 eller 10 §§ ska utföra tillsyn. Om en sådan rapport lämnas till en annan myndighet än Säkerhetspolisen eller Försvarsmakten, ska den mottagande myndigheten skyndsamt informera Säkerhetspolisen.

Anmälan om brister i säkerhetsskyddet

3 § Om det vid utövande av tillsyn över säkerhetsskyddet konstateras allvarliga brister som trots påpekanden inte rättas till, ska Säkerhetspolisen eller Försvarsmakten anmäla förhållandet till regeringen. Det gäller dock inte brister hos sådana enskilda där villkoren för säkerhetsskyddet angetts i ett säkerhetsskyddsavtal.

Om sådana brister i säkerhetsskyddet som anges i första stycket konstaterats av annan myndighet än Säkerhetspolisen eller Försvarsmakten, ska myndigheten informera Säkerhetspolisen. Om bristerna gäller verksamhet som omfattas av ett internationellt säkerhetsskyddsåtagande, ska myndigheten också informera Försvarsmakten.

Överklagande

4 § Beslut enligt denna förordning får inte överklagas.

Ikraftträdande och övergångsbestämmelser

1. Denna förordning träder i kraft den 1 januari 2017.

2. Genom förordningen upphävs säkerhetsskyddsförordningen (1996:633).

3. Ett beslut om registerkontroll enligt 26 eller 27 § säkerhetsskyddsförordningen (1996:633) ska, om inte annat beslutas, motsvara ett beslut om placering i säkerhetsklass 3 enligt 3 kap. 4 § första stycket 3 säkerhetsskyddslagen (2017:xx).

4. Föreskriften i 3 kap. 1 § gäller inte handlingar som är arkiverade. I fråga om andra handlingar och som märkts enligt föreskrifter som meddelats med stöd av säkerhetsskyddslagen (1996:627) ska föreskriften i 3 kap. 1 § tillämpas först den 1 januari 2020.

5. Säkerhetsskyddsklassificerade uppgifter får utan hinder av bestämmelsen i 3 kap. 4 § lämnas ut till en utländsk myndighet eller mellanfolklig organisation till utgången av 2019 utan att omfattas av ett internationellt säkerhetsskyddsåtagande hos den mottagande myndigheten eller organisationen.

Bilaga

Följande statliga myndigheter beslutar om placering i säkerhetsklasser i enlighet med vad som anges i 6 kap. 1 §.

Affärsverket svenska kraftnät,
Arbetsförmedlingen
Arbetsgivarverket,
Arbetsmiljöverket,
Brottsförebyggande rådet,
Datainspektionen,
Domstolsverket,
E-hälsomyndigheten,
Ekobrottsmyndigheten,
Ekonomistyrningsverket,
E-legitimationsnämnden
Elsäkerhetsverket,
Energimarknadsinspektionen,
Exportkreditnämnden,
Finansinspektionen,
Folke Bernadotteakademin,
Folkhälsomyndigheten,
Fortifikationsverket,
Försvarets materielverk,
Försvarets radioanstalt,
Försvarsexportmyndigheten,
Försvarshögskolan,
Försvarsmakten,
Försvarsunderrättelsedomstolen,
Försäkringskassan,
Granskningsnämnden för försvarsuppfinningar,
Havs- och vattenmyndigheten,
Inspektionen för strategiska produkter,
Justitiekanslern,
Konkurrensverket,
Kriminalvården,
Kronofogdemyndigheten,
Kustbevakningen,
Lantmäteriet,

Luftfartsverket,
Läkemedelsverket,
länsstyrelserna,
Migrationsverket,
Myndigheten för samhällsskydd och beredskap,
Myndigheten för tillväxtpolitiska utvärderingar och analyser,
Naturvårdsverket,
Patent- och registreringsverket
Pensionsmyndigheten,
Polismyndigheten
Post- och telestyrelsen,
Regeringskansliet,
Riksarkivet,
Riksgäldskontoret,
Rymdstyrelsen,
Sjöfartsverket,
Skatteverket
Socialstyrelsen,
Statens energimyndighet
Statens fastighetsverk,
Statens haverikommission,
Statens inspektion för försvarsunderrättelseverksamheten,
Statens jordbruksverk,
Statens livsmedelsverk,
Statens servicecenter,
Statens tjänstepensionsverk,
Statens veterinärmedicinska anstalt,
Statens överklagandenämnd,
Statistiska centralbyrån,
Statskontoret,
Strålsäkerhetsmyndigheten,
Styrelsen för internationellt utvecklingssamarbete,
Sveriges geologiska undersökning,
Sveriges lantbruksuniversitet,
Sveriges meteorologiska och hydrologiska institut,
Säkerhets- och integritetsskyddsnämnden,
Säkerhetspolisen
Totalförsvarets forskningsinstitut,
Totalförsvarets rekryteringsmyndighet,

Trafikverket,
Transportstyrelsen,
Tullverket,
Valmyndigheten, och
Åklagarmyndigheten.

1.13 Förslag till förordning om ändring i förordningen (1989:149) om bevakningsföretag m.m.

Härigenom föreskrivs att 10 § förordningen (1989:149) om bevakningsföretag m.m. ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	10 §
För godkännandemyndighetens prövning av en persons laglydnad och medborgerliga pålitlighet *skall* uppgifter som avses i 21 § 2 säkerhetsskyddslagen (1996:627) inhämtas. Därvid *skall 19*, *24–26* och *28 §§* säkerhetsskyddslagen och *29*, *31–33* och *43 §§* säkerhetsskyddsförordningen *(1996:633)* tillämpas.	För godkännandemyndighetens prövning av en persons laglydnad och medborgerliga pålitlighet *ska* uppgifter som avses i *3 kap. 12 § första stycket 2* säkerhetsskyddslagen *(2017:xx)* inhämtas. Därvid *ska* 3 kap. *11 §*, *12 § tredje stycket* och *13 §* säkerhetsskyddslagen och *7 kap. 5 § första stycket*, *11–13 §§* och 9 *kap. 1 §* säkerhetsskyddsförordningen *(2017:xx)* tillämpas.

Avser prövningen en person som inte redan är anlitad av ett bevakningsföretag, inhämtar dock myndigheten uppgifter ur belastningsregistret och misstankeregistret genom direktåtkomst enligt 20 § förordningen (1999:1134) om belastningsregister och 7 § förordningen (1999:1135) om misstankeregister.

Denna förordning träder i kraft den 1 januari 2017.

1.14 Förslag till förordning om ändring i förordningen (1996:1515) med instruktion för Regeringskansliet

Härigenom föreskrivs att 20 § förordningen (1996:1515) med instruktion för Regeringskansliet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
20 §	
Regeringskansliet ska	
1. utse Sveriges ombud och andra representanter vid förhandlingar med annan stat eller vid förhandlingar med och möten inom internationella organisationer,	
2. utse Sveriges representanter i det löpande arbetet inom Europeiska unionens råd samt föreslå och utse Sveriges representanter i kommittéer under Europeiska kommissionen,	
3. besvara formella underrättelser från kommissionen och i övrigt upplysa kommissionen om hur Sverige har uppfyllt de förpliktelser som följer av Sveriges medlemskap i unionen,	
4. bestämma vem som ska delta i arbetet inom Ständiga representanternas kommitté,	
5. besvara motiverade yttranden från kommissionen,	
6. anmäla förslag till författningar i enlighet med informationsförfaranden som följer av Sveriges medlemskap i unionen eller av andra internationella överenskommelser.	
7. avge svenska svar och kommentarer inom förfaranden som följer av Sveriges medlemskap i unionen eller av andra internationella överenskommelser,	7. avge svenska svar och kommentarer inom förfaranden som följer av Sveriges medlemskap i unionen eller av andra internationella överenskommelser, *och*
8. vara den nationella säkerhetsmyndighet som ansvarar för att upprätthålla säkerheten för sekretessbelagda uppgifter enligt Europeiska rådets säkerhetsföreskrifter samt enligt Sveriges åta-	8. besvara en utländsk begäran om inspektion, utvärderingsbesök eller observationsflygning som följer av åtaganden inom Organisationen för säkerhet och sam-

ganden om detta i överenskommelser med Västeuropeiska unionen och Nato inom ramen för samarbetet Partnerskap för fred, och

9. besvara en utländsk begäran om inspektion, utvärderingsbesök eller observationsflygning som följer av åtaganden inom Organisationen för säkerhet och samarbete i Europa (OSSE) enligt Wiendokumentet om förtroende- och säkerhetsskapande åtgärder den 30 november 2011 och fördraget om observationsflygningar den 24 mars 1992.

Denna förordning träder i kraft den 1 januari 2017.

1.15 Förslag till förordning om ändring i förordningen (2001:590) om behandling av uppgifter i Kronofogdemyndighetens verksamhet

Härigenom föreskrivs att 8 § förordningen (2001:590) om behandling av uppgifter i Kronofogdemyndighetens verksamhet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	8 §
På begäran av Säkerhetspolisen *skall* lämnas ut uppgifter som avses i 2 kap. 5 § 1–7 lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet om uppgifterna avser en person som förekommer i ett ärende om särskild personutredning enligt *18 §* säkerhetsskyddslagen *(1996:627)*.	På begäran av Säkerhetspolisen *ska* lämnas ut uppgifter som avses i 2 kap. 5 § 1–7 lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet om uppgifterna avser en person som förekommer i ett ärende om särskild personutredning enligt *3 kap. 10 §* säkerhetsskyddslagen *(2017:xx)*.

Denna förordning träder i kraft den 1 januari 2017.

1.16 Förslag till förordning om ändring i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden

Härigenom föreskrivs att 2 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §	
Myndigheten har till uppgift att i ärenden om registerkontroll enligt säkerhetsskyddslagen (1996:627) pröva frågor om utlämnande av uppgifter	Myndigheten har till uppgift att i ärenden om registerkontroll enligt säkerhetsskyddslagen *(2017:xx)* pröva frågor om utlämnande av uppgifter

1. från register som omfattas av lagen (1998:620) om belastningsregistret,
2. från register som omfattas av lagen (1998:621) om misstankeregistret,
3. från register som omfattas av lagen (2010:362) om polisens allmänna spaningsregister, och
4. som behandlas med stöd av polisdatalagen (2010:361).

Myndigheten ska pröva frågor om utlämnande av uppgifter även i sådana fall som avses i 10 § förordningen (1989:149) om bevakningsföretag m.m. och 7 § skyddsförordningen (2010:523).

Denna förordning träder i kraft den 1 januari 2017.

1.17 Förslag till förordning om ändring i förordningen (2007:1164) för Försvarshögskolan

Härigenom föreskrivs att 1 kap. 2 § och 4 kap. 3 § förordningen (2007:1164) för Försvarshögskolan ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §	
Försvarshögskolans hantering av säkerhetsskyddsfrågor regleras i säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633).	Försvarshögskolans hantering av säkerhetsskyddsfrågor regleras i säkerhetsskyddslagen *(2017:xx)* och säkerhetsskyddsförordningen *(2017:xx)*.
4 kap.	
3 §	
För att kunna bli antagen till en utbildning som leder till officersexamen som anges i bilagan till denna förordning krävs, utöver vad som gäller för grundläggande behörighet enligt 7 kap. 5, 6 och 24 §§ högskoleförordningen (1993:100), att sökanden	
1. är svensk medborgare,	
2. har fullgjort militär grundutbildning enligt lagen (1994:1809) om totalförsvarsplikt eller motsvarande militär utbildning,	
3. har genomgått säkerhetsprövning och uppfyller kraven enligt säkerhetsskyddslagen (*1996:627*) och säkerhetsskyddsförordningen (*1996:633*), och	3. har genomgått säkerhetsprövning och uppfyller kraven enligt säkerhetsskyddslagen *(2017:xx)* och säkerhetsskyddsförordningen *(2017:xx)*, och
4. har av Försvarshögskolan bedömts lämplig för utbildningen.	
Försvarshögskolan får meddela närmare föreskrifter om det krav som anges i första stycket 4.	

Denna förordning träder i kraft den 1 januari 2017.

1.18 Förslag till förordning om ändring i förordningen (2007:1244) om konsekvensutredning vid regelgivning

Härigenom föreskrivs att 2 § förordningen (2007:1244) om konsekvensutredning vid regelgivning (2007:1164) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §	
Förordningen ska inte tillämpas på	
1. föreskrifter som uteslutande rör verksamheten inom myndigheten,	
2. föreskrifter om sådana avgifter som omfattas av samrådsskyldigheten enligt 7 § avgiftsförordningen (1992:191),	
3. föreskrifter för utrikesförvaltningen, och	
4. föreskrifter som meddelas med stöd av säkerhetsskyddsförordningen *(1996:633)* eller på allmänna råd till den förordningen.	4. föreskrifter som meddelas med stöd av säkerhetsskyddsförordningen *(2017:xx)* eller på allmänna råd till den förordningen.

Denna förordning träder i kraft den 1 januari 2017.

1.19 Förslag till förordning om ändring i förordningen (2007:1266) med instruktion för Försvarsmakten

Härigenom föreskrivs i fråga om förordningen (2007:1266) med instruktion för Försvarsmakten

dels att 33 § ska upphöra att gälla,

dels att 26 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	26 §
Till Försvarsmaktens förslag om anställning och placering på befattning ska fogas	
– meritförteckning,	
– uppgift om att säkerhetsprövning gjorts enligt säkerhetsskyddslagen *(1996:627)* och säkerhetsskyddsförordningen *(1996:633)*, och	– uppgift om att säkerhetsprövning gjorts enligt säkerhetsskyddslagen *(2017:xx)* och säkerhetsskyddsförordningen *(2017:xx)*, och
– betyg och intyg över tjänstgöring under de senaste fem åren samt de handlingar i övrigt som Försvarsmakten vill åberopa.	

Denna förordning träder i kraft den 1 januari 2017.

1.20 Förslag till förordning om ändring i officersförordningen (2007:1268)

Härigenom föreskrivs att 9 § officersförordningen (2007:1268) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 §	
För att bli antagen till grundläggande officersutbildning inom Försvarsmakten krävs att en sökande	
1. är svensk medborgare,	
2. har fullgjort militär grundutbildning enligt lagen (1994:1809) om totalförsvarsplikt eller annan motsvarande militär utbildning eller tjänstgöring,	
3. har genomgått säkerhetsprövning och uppfyller kraven enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633), och	3. har genomgått säkerhetsprövning och uppfyller kraven enligt säkerhetsskyddslagen *(2017:xx)* och säkerhetsskyddsförordningen *(2017:xx)*, och
4. uppfyller särskilda krav.	
Försvarsmakten får meddela föreskrifter i fråga om sådan annan motsvarande militär utbildning eller tjänstgöring som avses i första stycket 2 och de särskilda krav som en sökande ska uppfylla enligt första stycket 4.	

Denna förordning träder i kraft den 1 januari 2017.

1.21 Förslag till förordning om ändring i skyddsförordningen (2010:523)

Härigenom föreskrivs att 7 och 8 §§ skyddsförordningen (2010:523) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
7 §	
Vid länsstyrelsens och Försvarsmaktens prövning av en persons laglydnad och medborgerliga pålitlighet ska uppgifter som avses i *21 § 2* säkerhetsskyddslagen *(1996:627)* inhämtas.	Vid länsstyrelsens och Försvarsmaktens prövning av en persons laglydnad och medborgerliga pålitlighet ska uppgifter som avses i *3 kap. 12 § första stycket 2* säkerhetsskyddslagen *(2017:xx)* inhämtas.
Vid prövningen ska *19*, *24–26* och *28 §§* säkerhetsskyddslagen och *29*, *31–33* och *43 §§* säkerhetsskyddsförordningen *(1996:633)* tillämpas.	Vid prövningen ska *3 kap. 11 §*, *12 § tredje stycket och 13 §* säkerhetsskyddslagen och *7 kap. 5 § första stycket*, *11–13 §§* och *9 kap. 1 §* säkerhetsskyddsförordningen *(2017:xx)* tillämpas.

Andra stycket gäller inte när länsstyrelsen inhämtar uppgifter ur belastningsregistret och misstankeregistret genom direktåtkomst enligt 20 § förordningen (1999:1134) om belastningsregister eller 7 § förordningen (1999:1135) om misstankeregister.

8 §	
Om en persons laglydnad och medborgerliga pålitlighet redan har prövats enligt lagen (1974:191) om bevakningsföretag eller säkerhetsskyddslagen *(1996:627)*, får länsstyrelsen eller Försvarsmakten vid godkännandeprövningen låta bli att inhämta de uppgifter som anges	Om en persons laglydnad och medborgerliga pålitlighet redan har prövats enligt lagen (1974:191) om bevakningsföretag eller säkerhetsskyddslagen *(2017:xx)*, får länsstyrelsen eller Försvarsmakten vid godkännandeprövningen låta bli att inhämta de uppgifter som anges

i 7 §, om det står klart att någon ytterligare kontroll inte behövs.	i 7 §, om det står klart att någon ytterligare kontroll inte behövs.

Denna förordning träder i kraft den 1 januari 2017.

1.22 Förordning om ändring i förordningen (2014:1103) med instruktion för Säkerhetspolisen

Härigenom föreskrivs att 6 § förordningen (2014:1103) med instruktion för Säkerhetspolisen ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 §
Säkerhetspolisen får, utöver vad som följer av *47 §* säkerhetsskyddsförordningen *(1996:633)*, ge råd om säkerhetsskydd. Säkerhetspolisen får även i övrigt ge råd för att förebygga brott mot rikets säkerhet eller andra särskilt viktiga samhällsintressen.	Säkerhetspolisen får, utöver vad som följer av *9 kap. 7 §* säkerhetsskyddsförordningen *(2017:xx)*, ge råd om säkerhetsskydd. Säkerhetspolisen får även i övrigt ge råd för att förebygga brott mot rikets säkerhet eller andra särskilt viktiga samhällsintressen.

Denna förordning träder i kraft den 1 januari 2017.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Enligt direktiven (se bilaga 1) ska utredningen se över säkerhetsskyddslagstiftningen. Syftet med uppdraget är främst att bättre anpassa lagstiftningen till det som krävs för att skydda verksamhet som har betydelse för rikets säkerhet och till de krav som det internationella samarbetet ställer.

I uppdraget ingår bl.a. att

- analysera vilka verksamheter som är av betydelse för rikets säkerhet eller som behöver skyddas mot terrorism och därför är i behov av säkerhetsskydd,
- föreslå hur reglerna om informationssäkerhet, som en del av säkerhetsskyddet, bör vara utformade,
- analysera vilka förändringar som kan behövas för att bättre anpassa lagstiftningen till de krav på säkerhetsskydd som ställs i det internationella samarbetet,
- analysera hur ett system med säkerhetsklarering kan utformas för svenska förhållanden,
- bedöma inom vilka verksamheter registerkontroll till skydd mot terrorism bör få ske,
- analysera behovet av förändringar av bestämmelserna om säkerhetsskyddad upphandling,
- ta ställning till om kravet på svenskt medborgarskap i säkerhetsskyddslagen bör förändras och
- utarbeta nödvändiga författningsförslag.

I direktiven anges vidare ett antal områden som utredningen ska ägna särskild uppmärksamhet. De områden som nämns är säkerhetsskyddets syfte, informationssäkerhet, säkerhetsprövning, registerkontroll till skydd mot terrorism, säkerhetsskyddad upphandling och industrisäkerhetsskydd, medborgarskapskravet och tillsyn.

2.2 Utredningsarbetet

Utredningen har haft såväl möten som mer informella kontakter med experterna.

Utredningen har också haft informella möten och kontakter med bl.a. företrädare för Affärsverket svenska kraftnät, Försvarsmakten, Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Regeringskansliet, riksdagen, Säkerhetspolisen och Säkerhets- och integritetsskyddsnämnden. Det har också förekommit kontakter med vissa intresseorganisationer och enskilda företag, bl.a. Näringslivets Säkerhetsdelegation, Säkerhets- och Försvarsföretagen och Vattenfall Aktiebolag.

Vidare har informella möten och kontakter förekommit mellan utredningen och företrädare för ett flertal utredningar, bl.a. Utredningen om förstärkt skydd mot främmande makts underrättelseverksamhet (Ju 2010:13), Utredningen om översyn av de statliga insatserna för dammsäkerhet (N 2011:05), Utredningen om skydd för geografisk information (Fö 2012:02), Utredningen om registerutdrag i arbetslivet (A 2013:04) och Utredningen NISU 2014 (Fö 2013:04).

Det ingår i utredningsuppdraget att redovisa de regler och förfaranden som gäller i några med Sverige jämförbara länder, i första hand de nordiska och några länder inom EU som tillämpar ett system med säkerhetsklarering. Vi har valt att anlägga ett något vidare perspektiv för den internationella utblicken. Utredningen har därför sökt information om systemen för säkerhetsskydd i Danmark, Finland, Nederländerna, Norge och Tjeckien. Vi har inte studerat Islands lagstiftning på området.

Arbetet har bedrivits främst genom undersökning av lagstiftning och i förekommande fall förarbeten samt övrig information

från officiella webbplatser. Denna undersökning har kompletterats med besök vid de nationella säkerhetsmyndigheterna med i förhand lämnade skriftliga frågor till företrädare för myndigheterna.

2.3 Betänkandets disposition

Betänkandet består av 24 kapitel. Kapitel 3–9 är bakgrundskapitel som beskriver gällande ordning och förändringsbehoven. I de kapitlen beskriver vi säkerhetsskyddslagstiftningen, skyddsintressen, närliggande reglering, folkrättsliga förpliktelser avseende säkerhetsskydd, myndigheter med uppgifter enligt säkerhetsskyddslagstiftningen, regleringen om säkerhetsskydd i bl.a. de nordiska länderna, samt hoten och de huvudsakliga förändringsfaktorerna.

Kapitel 10–22 är övervägandekapitel där vi redogör för våra bedömningar och förslag. Kapitel 10–12 inleder den delen av betänkandet med utgångspunkter för en reformerad säkerhetsskyddslag, lagens syfte samt dess inriktning. De överväganden och förslag som redovisas i de kapitlen utgör en grund för de frågor som behandlas i de efterföljande kapitlen. Kapitel 13–15 tar upp vad som ska skyddas, säkerhetsskyddsanalys, verksamhetsansvar samt systemet med säkerhetsskyddsåtgärder med olika inriktning. Därefter följer kapitel 16–19 som närmare behandlar säkerhetsskyddsåtgärderna informationssäkerhet, fysisk säkerhet och personalsäkerhet samt, avslutningsvis, säkerhetsskyddad upphandling. Kapitel 20 behandlar frågor om internationell samverkan på säkerhetsskyddsområdet och kapitel 21 tillsyn, föreskrifter och rapportering. I kapitel 22 har vi samlat några frågor som innehållsmässigt inte passar i övriga kapitel, t.ex. om tystnadsplikt.

Kapitel 23 beskriver konsekvenserna av förslagen och frågor om ikraftträdande. Kapitel 24 innehåller en författningskommentar till författningsförslagen i kapitel 1.

3 Säkerhetsskyddslagstiftningen

I det här kapitlet ges en översiktlig redogörelse för regleringen om säkerhetsskydd, både i ett historiskt perspektiv (avsnitt 3.1 och 3.2) och enligt gällande rätt (avsnitt 3.3). I fråga om gällande rätt finns vidare i kapitel 4 om skyddsintressen en redogörelse för reglering som har särskild relevans för säkerhetsskyddslagen. En samlad beskrivning av de uppgifter som bl.a. Säkerhetspolisen, Försvarsmakten, Affärsverket svenska kraftnät, Post- och telestyrelsen och Transportstyrelsen har enligt säkerhetsskyddsförordningen finns i kapitel 7. I anslutning till utredningens överväganden lämnas också i vissa avseenden en mer utförlig beskrivning av gällande ordning.

Det bör också tilläggas att det finns flera lagar och förordningar och även internationella konventioner och EU-rättsakter som innehåller bestämmelser som syftar till att tillförsäkra vissa samhällsområden och verksamheter ett säkerhetsskydd, eller till att från ett vidare säkerhetsperspektiv mer generellt verka för ett skydd av vissa för samhället viktiga verksamheter. I kapitel 5 finns en redogörelse för sådan närliggande reglering.

3.1 Äldre rätt

Personalkontrollkungörelsen

Ett system för personalkontroll växte fram under andra världskriget och därefter. Personalkontrollkungörelsen (1969:446), kom till efter förslag av den parlamentariska nämnden med anledning av Wennerströmaffären.[1]

[1] Parlamentariska nämnden i Wennerströmaffären, betänkandet Handläggningen av säkerhetsfrågor (SOU 1968:4).

Reglerna i personalkontrollkungörelsen innebar i huvudsak att personalkontroll fick göras avseende vissa befattningshavare vid de organ som angavs i kungörelsen, företrädesvis statliga myndigheter med uppgifter av betydelse för totalförsvaret men också vissa företag. Endast den som innehade eller skulle tillträda en tjänst som var placerad i s.k. skyddsklass fick kontrolleras. Antalet skyddsklasser var då, liksom nu, tre och benämnda som 1A, 1B och 2, där 1A var den högsta klassen. Vilka tjänster som skulle placeras i skyddsklass bestämdes av regeringen eller, när det gällde skyddsklass 2, efter regeringens bemyndigande av vederbörande myndighet. Uppgifter i samband med personalkontroll hämtades ur bl.a. polisens person- och belastningsregister och Säkerhetspolisens register. Rikspolisstyrelsens styrelse avgjorde vilka uppgifter som skulle lämnas ut. I kungörelsen fanns vidare föreskrifter som innebar att den kontrollerade, med vissa begränsningar, skulle beredas tillfälle att yttra sig innan beslut fattades om att lämna ut uppgifter från registren. Prövningen av den kontrollerades lämplighet från säkerhetssynpunkt gjordes av den myndighet som beslutat om kontroll.

Förordningen om säkerhetsskyddet vid statliga myndigheter

För att åstadkomma ett skydd inom statliga myndigheter i syfte att förhindra att obehöriga fick del av information av betydelse för totalförsvaret eller landets säkerhet i övrigt utfärdades förordningen (1981:421) om säkerhetsskyddet vid statliga myndigheter. Enligt förordningen var det varje statlig myndighets ansvar att se till att det fanns ett tillfredsställande säkerhetsskydd inom myndighetens verksamhetsområde. Säkerhetsskyddet omfattade enligt förordningen sekretesskydd, tillträdesskydd, infiltrationsskydd, information och kontroll. Förordningen innehöll inte några detaljerade regler för hur säkerhetsskyddet skulle vara utformat. Rikspolisstyrelsen och myndigheten Överbefälhavaren hade till uppgift att utfärda närmare bestämmelser och att kontrollera att bestämmelserna följdes. Förordningen var inte tillämplig på kommuner och landsting och inte heller för riksdagen och dess myndigheter eller för Regeringskansliet. För att skapa motsvarande skydd för riksdagens verksamhet tillkom, efter mönster från förordningen om säkerhetsskyddet för statliga myndigheter, lagen (1983:953)

om säkerhetsskydd i riksdagen.[2] Också för Regeringskansliet, som i princip inte omfattades av förordningen om säkerhetsskyddet vid statliga myndigheter, beslutades särskilda föreskrifter.

3.2 Bakgrunden till nuvarande säkerhetsskyddslag

SÄPO-kommittén

I november 1987 tillkallades en parlamentarisk kommitté, SÄPO-kommittén, med uppgift att bl.a. se över personalkontrollförfarandet. Syftet med översynen var både att öka kontrollens effektivitet och att stärka den enskildes rättssäkerhet i samband med kontrollen.

Kommittén lade i sitt slutbetänkande Säkerhetspolisens arbetsmetoder, personalkontroll och meddelarfrihet (SOU 1990:51) fram förslag till en lag om personalkontroll. Kommittén underströk i betänkandet att den inte hade funnit anledning att ändra den grundläggande inriktningen av personalkontrollen. Lagförslaget byggde därför i väsentliga delar på reglerna i personalkontrollkungörelsen. Att ge reglerna om personalkontroll lagform ansågs inte nödvändigt av konstitutionella skäl, men kommittén ansåg det ändå lämpligt att föreslå en sådan ordning med hänsyn till reglernas betydelse för den enskilde.

Till de sakliga nyheterna i kommitténs förslag hörde att kontroll skulle kunna genomföras inte bara som dittills av personer med insyn i sekretessbelagda uppgifter utan också till skydd mot terroristaktioner.

Kommittén föreslog också en förändring i fråga om skyddsklassindelningen och begränsningen beträffande möjligheterna att lämna ut uppgifter ur Säkerhetspolisens register i samband med kontrollen. Beslut om att lämna ut uppgifter borde fattas av en från polisen fristående nämnd. Också förändringar i fråga om partsinsynen föreslogs.

Betänkandet remissbehandlades. De flesta remissinstanserna tillstyrkte förslaget om personalkontrollen eller lämnade det utan erinran. Försvarets materielverk framförde dock invändningar mot

[2] Lagen har senare ersatts av lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter, se vidare avsnitt 3.3.

förslaget att göra det omöjligt att lämna ut uppgifter ur Säkerhetspolisens register vid kontroll avseende skyddsklass 2. Enligt Försvarets materielverk skulle begränsningen träffa en stor del av de kontroller som utfördes inom försvarsindustrins område och skulle därmed på ett oacceptabelt sätt innebära ett försvagat skydd. Begränsningen skulle, menade Försvarets materielverk, innebära svårigheter när det gällde samarbetet med utländsk försvarsindustri. Även Justitiekanslern ansåg det fel att inte kunna utnyttja uppgifter i Säkerhetspolisens register i de fall detta behövdes.

Översyn av personalkontrollförfarandet

SÄPO-kommitténs förslag och de synpunkter som framfördes under remissförfarandet ledde fram till en översyn av personalkontrollförfarandet (dir. 1993:81). Departementschefen konstaterade i direktiven att SÄPO-kommitténs förslag byggde på en lämplig balans mellan kontrollbehovet och hänsynen till den personliga integriteten, men att det samtidigt kunde resas allvarliga invändningar mot bl.a. förslagen att ta bort möjligheterna att lämna ut uppgifter från SÄPO-registret vid kontroll i skyddsklass 2. Departementschefen menade att förslaget i praktiken i många fall skulle betyda att uppgifter om samröre med politiska extremistorganisationer eller kontakter med terrorister eller utländska spionorganisationer inte fick lämnas ut vid prövning av om en person är lämplig att få en säkerhetskänslig befattning. Det skulle medföra en väsentlig försvagning av skyddet mot säkerhetshotande verksamhet. Till detta kom att Sveriges ansökan om medlemskap i EG hade förändrat förutsättningarna för bedömningen av SÄPO-kommitténs förslag.

Departementschefen konstaterade att många länder i Västeuropa tillämpar ett system som bygger på s.k. *security clearance*, säkerhetsklarering. Enligt departementschefen var det inte realistiskt att Sverige skulle behålla ett personkontrollsystem som i viktiga avseenden skiljde sig från vad som allmänt gäller hos andra EG-länder. Målet för utredningens uppdrag var enligt direktiven att redovisa ett förslag till en lag om personalkontroll som bygger på s.k. säkerhetsklarering.

Enligt direktiven hade utredningen i uppgift att se till att såväl kontrollintresset som integritets- och rättssäkerhetsintresset kom att tillgodoses i den nya lagen om personalkontroll. Utredningen fick också i uppgift att komplettera den föreslagna lagen med förslag till föreskrifter i förordningsform.

Tilläggsdirektiv om översyn av personalkontrollförfarandet

Genom tilläggsdirektiv (dir. 1993:123) fick utredningen för översyn av personalkontrollförfarandet i särskilt uppdrag att se över frågan om att lagreglera säkerhetsskyddet hos myndigheter m.m.

Bakgrunden till tilläggsdirektiven var att Rikspolisstyrelsen och Överbefälhavaren i en gemensam skrivelse till regeringen hade framfört att förordningen om säkerhetsskyddet vid statliga myndigheter borde arbetas om och ges formen av lag. I skrivelsen framhölls särskilt att kommunerna, som viktiga totalförsvarsmyndigheter, borde omfattas av regleringen och att regleringen därför krävde lagform.

Rikspolisstyrelsen och Överbefälhavaren menade också att säkerhetsskyddet i den gällande förordningen i stort sett var koncentrerat till uppgifter som omfattades av försvarssekretess och att frågan om en utvidgning av begreppet säkerhetsskydd borde analyseras.

Statsrådet anförde i direktiven att hon var av uppfattningen att förordningen om säkerhetsskyddet vid statliga myndigheter behövde ses över och att en sådan översyn i första hand borde inriktas på en lagreglering, bl.a. med hänsyn till att det borde utredas på vilket sätt vissa enskilda skulle omfattas av en ny reglering om säkerhetsskydd. Som exempel nämndes företag som omfattades av regelverk om upphandling och enskilda organ som utan att det rörde sig om upphandlingsavtal bedrev verksamhet inom totalförsvaret. I översynen ingick inte att ta ställning till säkerhetsskyddet hos regering och riksdag.

Säkerhetsskyddsutredningens förslag och propositionen 1995/95:129 Säkerhetsskydd

Säkerhetsskyddsutredningen, lämnade i sitt betänkande Säkerhetsskydd (SOU 1994:149) förslag till en säkerhetsskyddslag och en säkerhetsskyddsförordning.

Säkerhetsskyddsutredningens förslag kom i allt väsentligt att läggas till grund för regeringens förslag till säkerhetsskyddslag[3] som senare antogs av riksdagen. Också bestämmelserna i säkerhetsskyddsförordningen utgår i allt väsentligt från utredningens förslag.

I fråga om lagens tillämplighet för enskilda la säkerhetsskyddsutredningen fram ett i förhållande till propositionen avvikande förslag. Utredningens förslag som fick kritik under remissförfarandet, innebar att säkerhetsskyddslagen skulle bli tillämplig på andra företag än de offentligt ägda företagen endast när ett säkerhetsskyddsavtal hade träffats mellan företaget och det allmänna. Regeringens förslag innebar i stället att lagen gjordes direkt tillämplig även för sådana verksamheter.

I fråga om en övergång till ett klareringssystem gjordes bedömningen att en övergång till ett sådant system inte var motiverat.[4] Därvid framfördes att det förhållandet att ett skriftligt intyg utfärdas är en skillnad av mer formell än saklig karaktär och att ett internationellt utbyte skulle underlättas om en säkerhetsprövning som innehåller en registerkontroll dokumenteras. På grundval av sådan dokumentation skulle sedan en säkerhetsklarering kunna utfärdas, om en framställning om detta görs av en annan stat.

Säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633) trädde i kraft den 1 juli 1996. Författningarna ersatte därmed personalkontrollkungörelsen och förordningen om säkerhetsskyddet vid statliga myndigheter.

[3] Prop. 1995/95:129 Säkerhetsskydd
[4] Prop. 1995/96:129, s. 39.

3.3 Gällande rätt – 1996 års säkerhetsskyddslagstiftning

3.3.1 Säkerhetsskyddslagens syfte, tillämpningsområde och huvudsakliga innehåll

Syfte

Syftet med säkerhetsskyddslagen framgår av bestämmelserna om lagens tillämpningsområde (1 §), om vad som avses med säkerhetsskydd (6 §) samt om vad säkerhetsskyddet genom de olika säkerhetsskyddsåtgärderna ska förebygga (7 §).

Av 1 § 3 som anger lagens tillämpningsområde i fråga om enskilda kan utläsas att lagen tar sikte på verksamhet som är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Ledning i fråga om mot vad ett skydd behövs finns i 6 §. I paragrafen anges att med säkerhetsskydd avses

1. skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet,
2. skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet, och
3. skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet.

I 7 § anges närmare vad säkerhetsskyddet ska syfta till genom bestämmelser om de tre inriktningarna för säkerhetsskyddsåtgärder. I paragrafen anges att säkerhetsskyddet ska förebygga

1. att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen, röjs, ändras eller förstörs (informationssäkerhet),
2. att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som omfattas av sekretess och som rör rikets säkerhet eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning), och

3. att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning).

Paragrafen avslutas med ett tillägg om att säkerhetsskyddet även i övrigt ska förebygga mot terrorism. Säkerhetsskydd med sådan inriktning är i vart fall i fråga om kontroll av personal i hög grad kopplat till bestämmelserna om skyddsobjekt i skyddslagen (2010:305).

Begreppet rikets säkerhet

Begreppet rikets säkerhet är centralt i säkerhetsskyddslagen. I förarbetena konstateras att det inte finns någon legaldefinition av begreppet. Till ledning i fråga om innebörden av rikets säkerhet i säkerhetsskyddslagen framhålls bl.a. följande i förarbetena.[5]

Rikets säkerhet kan omfatta såväl den yttre säkerheten till skydd för Sveriges försvarsförmåga, politiska oberoende och territoriella suveränitet som den inre säkerheten till skydd för Sveriges demokratiska statsskick. Skyddet för den yttre säkerheten tar i första hand sikte på totalförsvaret, dvs. den verksamhet som behövs för att förbereda Sverige för krig. Ett hot mot rikets yttre säkerhet anses dock kunna förekomma, även om det inte hotar totalförsvaret. Skyddet av rikets yttre säkerhet anses omfatta uppgifter och förhållanden av rent militär betydelse eller av betydelse för totalförsvaret i övrigt och andra uppgifter som har betydelse för rikets nationella oberoende. I lagen (1992:1403) om totalförsvar och höjd beredskap definieras totalförsvarsbegreppet som den verksamhet som behövs för att förbereda Sverige för krig.

Också rikets inre säkerhet kan vara hotad utan att totalförsvaret berörs. Angrepp på det demokratiska statsskicket kan förekomma från grupperingar utan förbindelse med främmande makt. Det kan också vara fråga om försök att ta över den politiska makten genom våld eller att använda våld, hot eller tvång mot statsledningen i syfte att påverka politikens utformning. Försök att systematiskt

[5] Prop. 1995/96:129, s. 22 f.

hindra medborgarna från att utnyttja sina demokratiska fri- och rättigheter räknas också till hoten mot rikets inre säkerhet.

Tillämpningsområde

Säkerhetsskyddslagen är direkt tillämplig för såväl myndigheter, kommuner och landsting som verksamhet som bedrivs i olika företagsformer. Vilka verksamheter som lagen gäller för anges i 1 § säkerhetsskyddslagen. Bestämmelsen innehåller bl.a. ett moment som särskiljer aktiebolag, handelsbolag, föreningar och stiftelser över vilka det allmänna har ett rättsligt bestämmande inflytande. Vid myndigheter, kommuner och landsting samt vid företagsformer där det allmänna har ett rättsligt bestämmande inflytande gäller säkerhetsskyddslagen enligt ordalydelsen generellt medan den för enskilda (dvs. företagsformer där det allmänna inte utövar något rättsligt bestämmande inflytande) gäller om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Vad som i sammanhanget avses med rättsligt bestämmande inflytande definieras i lagens 4 §.

Säkerhetsskyddslagen gäller endast i viss angiven utsträckning för riksdagen och dess myndigheter och för Regeringskansliet (se 2 och 32 §§ säkerhetsskyddslagen och 2 § säkerhetsskyddsförordningen). Det handlar bl.a. om bestämmelserna om placering i säkerhetsklass och om registerkontroll. Säkerhetsskyddsförordningen gäller inte för riksdagen och endast i begränsad utsträckning för Regeringskansliet (1 och 2 §§ säkerhetsskyddsförordningen). Vad gäller riksdagen finns det bestämmelser om säkerhetsskydd även i lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter. Den lagen, som kompletteras med föreskrifter, har säkerhetsskyddslagen som förebild. För Regeringskansliet gäller på motsvarande sätt även föreskrifter om säkerhetsskyddet i Regeringskansliet (RKF 1998:16).

Vilket säkerhetsskydd behövs i en verksamhet som lagen gäller för?

I fråga om säkerhetsskyddets omfattning anges i lagens 5 § att i verksamhet där lagen gäller ska det säkerhetsskydd finnas som behövs med hänsyn till verksamhetens art, omfattning och övriga

omständigheter. Vidare erinras om att säkerhetsskyddet ska utformas med beaktande av enskildas rätt att enligt tryckfrihetsförordningen ta del av allmänna handlingar.

I 5 § säkerhetsskyddsförordningen finns en bestämmelse om säkerhetsanalys som ställer krav på att myndigheter och andra som förordningen gäller för ska undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism.

I 30 § säkerhetsskyddslagen finns en bestämmelse om intern kontroll (se avsnitt 3.3.6).

I fråga om de olika säkerhetsskyddsåtgärderna innehåller lagen nästan uteslutande bestämmelser om säkerhetsprövning. Det har sin förklaring i att säkerhetsprövning innebär åtgärder i form av bl.a. registerkontroll som i stor utsträckning förutsätter en reglering i lag. I fråga om informationssäkerhet och tillträdesbegränsning finns närmare bestämmelser i säkerhetsskyddsförordningen och i tillämpningsföreskrifter. Motsvarande gäller även för det närmare förfarandet vid säkerhetsprövning och registerkontroll. För att kunna ge en sammantagen bild av vad som gäller i fråga om de olika säkerhetsskyddsåtgärderna är det lämpligt att i ett sammanhang redogöra för bestämmelser i lag och förordning och i viss utsträckning även i myndighetsföreskrifter (se vidare avsnitten 3.3.2–3.3.4).

Övriga bestämmelser om säkerhetsskydd

Säkerhetsskyddslagen innehåller också bestämmelser om säkerhetsskyddad upphandling (säkerhetsskyddsavtal), intern kontroll och utbildning samt bestämmelser om föreskrifter och tillsyn. Vi redogör för de bestämmelserna i avsnitten 3.3.5–3.3.7 där vi samtidigt behandlar den reglering som i de avseendena finns i säkerhetsskyddsförordningen.

I säkerhetsskyddslagen och säkerhetsskyddsförordningen finns även vissa bestämmelser som tar sikte på internationell samverkan (se vidare avsnitt 3.3.8).

3.3.2 Informationssäkerhet

Vad innebär informationssäkerhet?

I säkerhetsskyddsåtgärden *informationssäkerhet* ingår förebyggande av att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen, röjs, ändras eller förstörs, oavsett om det sker uppsåtligen eller av oaktsamhet. Dessa uppgifter definieras i 4 § säkerhetsskyddsförordningen som *hemliga uppgifter.* Där definieras även *hemlig handling* som en handling som innehåller hemliga uppgifter. Regleringen i fråga om informationssäkerhet består till stor del av bestämmelser i säkerhetsskyddsförordningen och i tillämpningsföreskrifter som rör hantering av hemliga uppgifter och hemliga handlingar.

Behörighet till hemliga uppgifter

I 7 § säkerhetsskyddsförordningen anges tre kriterier som måste vara uppfyllda för att någon ska få ta del av hemliga uppgifter. För det första ska personen bedömas som pålitlig från säkerhetssynpunkt. Det innebär som huvudregel att personen är säkerhetsprövad och efter prövningen bedömd som pålitlig. För det andra krävs tillräckliga kunskaper om säkerhetsskydd för att kunna hantera de hemliga uppgifterna på ett säkert sätt. För det tredje krävs att personen behöver uppgifterna för sitt arbete.

Anmälan vid röjd uppgift

Om en hemlig handling kan ha röjts ska det skyndsamt anmälas till Säkerhetspolisen under förutsättning att röjandet kan antas medföra men för rikets säkerhet som inte enbart är ringa (10 § säkerhetsskyddsförordningen). Skälen till bestämmelsen är dels att kunna utreda det eventuella straffrättsliga ansvaret för röjandet, dels att kunna vidta åtgärder för att minska skadan i det enskilda fallet och om möjligt minska risken för framtida röjande.

It-säkerhet

I 12 och 13 §§ säkerhetsskyddsförordningen finns bestämmelser som tar sikte på skyddet för hemliga uppgifter i it-system och vid kommunicering av uppgifterna. I bestämmelserna regleras bl.a. att en myndighet innan den inrättar ett it-system[6] som kan skada totalförsvaret ska samråda med Försvarsmakten eller i vissa fall Säkerhetspolisen, att ett system för hemliga uppgifter som ska användas av flera personer ska godkännas från säkerhetssynpunkt innan det tas i drift och att hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten.

Tillämpningsföreskrifter

Informationssäkerheten inklusive it-säkerhet regleras mer i detalj i Säkerhetspolisens och Försvarsmaktens tillämpningsföreskrifter. Bestämmelserna syftar till att hemliga uppgifter och handlingar ska hanteras på ett betryggande sätt.

I avsnitt 16.4 finns en beskrivning över åtgärder inom informationssäkerheten.

3.3.3 Tillträdesbegränsning

Vad avses med tillträdesbegränsning?

Med tillträdesbegränsning avses ett fysiskt skydd för att hindra obehöriga att få tillträde till platser där de kan få tillgång till hemliga uppgifter eller där det pågår verksamhet av betydelse för rikets säkerhet. Tillträdesbegränsning ska även förebygga terrorism. Tillträdesbegränsning i säkerhetsskyddslagstiftningen har ett nära samband med reglerna om förbud mot tillträde i skyddslagen (2010:305) och ett beslut om skyddsobjekt kan sägas vara en kvalificerad form av tillträdesbegränsning. Tillträdesbegränsning enligt säkerhetsskyddslagen ålägger dem som omfattas av reglerna att pröva i vilken utsträckning en tillträdesbegränsning är påkallad och

[6] I författningstexten används den något ålderdomliga skrivningen ”register som ska föras med hjälp av automatisk databehandling”.

att i förekommande fall utforma begränsningen på ett tillfredsställande sätt.[7]

Tillträdesbegränsningen kan utformas på olika sätt. Sådana åtgärder ska dock enligt 10 § säkerhetsskyddslagen utformas så att den enskildes rätt att röra sig fritt inte inskränks mer än nödvändigt.

Åtgärder för tillträdesbegränsning

Tillträdesbegränsningen kan hindra, fördröja och förvarna om obehörigt tillträde till platser där säkerhetskänslig verksamhet bedrivs eller där hemliga uppgifter bearbetas eller förvaras. Tillträdesbegränsning kan ske t.ex. genom utfärdande och tillkännagivande av tillträdesförbud, passerkontroll, byggnadstekniska åtgärder, bevakningstekniska hjälpmedel, larmanordningar och bevakning. I Säkerhetspolisens och Försvarsmaktens tillämpningsföreskrifter finns detaljerade bestämmelser om hur tillträdesbegränsningen ska utformas. I avsnitt 17.4 finns en förteckning över åtgärder för bl.a. tillträdesbegränsning.

3.3.4 Säkerhetsprövning

När gäller krav på säkerhetsprövning?

Säkerhetsprövning ska göras innan en person genom anställning eller på något annat sätt deltar i verksamhet som har betydelse för rikets säkerhet eller anlitas för uppgifter som är viktiga för skyddet mot terrorism (11 § säkerhetsskyddslagen). Säkerhetsprövning förutsätter inte placering i säkerhetsklass enligt 17 § säkerhetsskyddslagen. Däremot är sådana i säkerhetsprövningen ingående kvalificerade moment som registerkontroll och särskild personutredning förbehållna situationer där det är fråga om anställning eller annat deltagande som placerats i en säkerhetsklass. Också bestämmelser om verksamheter som särskilt behöver skyddas mot terrorism ger stöd för registerkontroll som ett led i en säkerhetsprövning.

[7] Prop. 1995/96:129, s. 77 och Säkerhetspolisens handbok Säkerhetsskydd – en vägledning, 2010, s. 34.

Vad ska bedömas?

Vad som ska bedömas inom ramen för säkerhetsprövningen framgår av 7 och 11 §§ säkerhetsskyddslagen. I 7 § 3 nämns pålitlighet från säkerhetssynpunkt. I 11 § anges att prövningen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas av säkerhetsskyddslagen och i övrigt pålitlig från säkerhetssynpunkt. Av författningskommentaren till 7 § 3 framgår bl.a. att pålitlighetsbedömningen ska innefatta inte bara en bedömning av om det finns en risk för att personen i fråga kan göra sig skyldig till spionerieller dylikt utan också av risken för att bli utsatt för olika påtryckningar eller risker för att den enskilde genom slarv eller på annat oavsiktligt sätt röjer sekretessbelagda uppgifter.

Prövningsunderlaget

I 27 § säkerhetsskyddslagen anges att säkerhetsprövningen ska grundas på den kunskap som finns om den som prövas, de uppgifter som (för det fall att sådan kontroll och utredning ska göras) kommit fram vid registerkontroll och särskild personutredning, arten av den verksamhet för vilken prövningen görs samt omständigheterna i övrigt. Vidare framgår av 14 § säkerhetsskyddsförordningen att prövningen innebär kontroll av betyg, intyg och referenser och även en identitetskontroll.

När ska registerkontroll göras?

I vilken utsträckning registerkontroll och särskild personutredning ska användas vid säkerhetsprövning styrs, förutom vad avser skydd mot terrorism, av bestämmelserna om placering i säkerhetsklass i 17 § säkerhetsskyddslagen. Säkerhetsklasserna är tre till antalet. Placeringen bestäms av en kombination av två faktorer; i vilken omfattning den berörde kan få del av sekretessbelagda uppgifter och om det är fråga av uppgifter av *synnerlig betydelse* för rikets säkerhet eller uppgifter av *betydelse* för rikets säkerhet. I fråga om placering i säkerhetsklass 3 gäller ett uttryckligt krav på skada av viss storlek (men för rikets säkerhet som inte är ringa) om uppgifterna röjs för obehöriga.

Om det finns särskilda skäl får också registerkontroll göras för att skydda mot terrorism (14 § säkerhetsskyddslagen). Den närmare regleringen i det avseendet finns i 26–27 a § säkerhetsskyddsförordningen. Det anges särskilt att sådan kontroll får göras endast om skyddsbehovet inte kan tillgodoses på annat sätt. Bestämmelserna innebär att en registerkontroll för detta syfte får göras i fråga om den som ska anställas eller på annat sätt delta i verksamhet vid bl.a. civila flygplatser, flygstationer och flygpassagerarterminaler, statschefens residens och bostäder, statsministerns bostäder, anläggningar inom elförsörjningen som är skyddsobjekt, Regeringskansliets byggnader och vissa andra skyddsobjekt enligt skyddslagen. Registerkontroll får göras också beträffande de personer som ska förordnas enligt 16 § (lagen (2004:487) om sjöfartsskydd eller 4 kap. 3 § lagen (2006:1209) om hamnskydd samt av den som ska anställas eller på annat sätt delta i verksamhet som har betydelse för luftfartsskyddet, om det följer av en internationell överenskommelse som Sverige tillträtt eller av en bindande EU-rättsakt på området för luftfartsskydd att säkerhetsprövningen ska omfatta registerkontroll.

Vad innebär registerkontroll?

Med registerkontroll avses enligt 12 § säkerhetsskyddslagen att uppgifter hämtas från ett register som omfattats av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller lagen (2010:362) om polisens allmänna spaningsregister samt att uppgifter som behandlas med stöd av polisdatalagen (2010:361) hämtas in. Av 18 § säkerhetsskyddslagen framgår i vilka fall en särskild personutredning ska göras vid registerkontroll. Närmare bestämmelser om sådan utredning finns i 34–37 §§ säkerhetsskyddsförordningen.

Det krävs att den som ska kontrolleras ger sitt samtycke innan någon registerkontroll genomförs (19 § säkerhetsskyddslagen). I säkerhetsskyddslagens 21–23 §§ anges vilka uppgifter om den kontrollerade och vissa till den kontrollerade närstående som ett utlämnande får omfatta. Tidigare innebar registerkontroll i fråga om skydd mot terrorism att endast uppgifter om vissa angivna

brott fick lämnas ut. Genom ändringar i säkerhetsskyddslagen gäller numera inte någon sådan begränsning.[8]

Uppgifter som kommer fram vid registerkontroll och särskild personutredning får lämnas ut för säkerhetsprövning endast om de kan antas ha betydelse för prövningen av den kontrollerades pålitlighet från säkerhetssynpunkt (24 § säkerhetsskyddslagen). Bedömningen av vilka uppgifter som har en sådan relevans för säkerhetsprövningen görs av Säkerhets- och integritetsskyddsnämnden (31 § säkerhetsskyddsförordningen). Det finns krav på att den berörde ska få tillfälle att yttra sig över uppgifter som kommit fram vid en kontroll innan uppgifterna lämnas ut för säkerhetsprövning (25 § säkerhetsskyddslagen). Undantag gäller för uppgift som omfattas av sekretess i förhållande till den enskilde. I fråga om prövningen av de utlämnade uppgifterna anges i 27 § säkerhetsskyddslagen att den som bestämmer om registerkontroll avgör självständigt om den person som prövas ska få anlitas.

Beslut om placering i säkerhetsklass och om registerkontroll

Vilka som har behörighet att besluta om placering i säkerhetsklass och om registerkontroll framgår av 20 § säkerhetsskyddslagen i kombination med 18–22 och 26 a–27 a §§ säkerhetsskyddsförordningen samt av bilagan till den förordningen. Bestämmelserna innebär sammanfattningsvis att regeringen, med undantag för riksdagens förvaltningsområde, ytterst har beslutanderätten men kan överlåta den åt myndigheter, kommuner och landsting och, om det finns särskilda skäl, vissa företag. Regeringen har överlåtit i princip all beslutanderätt, med undantag för framför allt beslut om placering i säkerhetsklass 1, till myndigheter, kommuner och landsting samt till några få bolag där starka oberoendehänsyn gör sig gällande, bl.a. Sveriges Radio Aktiebolag. I övrigt är det vissa utsedda myndigheter (Affärsverket svenska kraftnät, Transportstyrelsen, Post- och telestyrelsen eller någon av länsstyrelserna) som beslutar om placering i säkerhetsklass och om registerkontroll i fråga om anställning eller annat deltagande i enskild verksamhet. En närmare redogörelse för myndigheternas beslutanderätt i detta avseende finns i kapitel 7.

[8] Prop. 2005/06:137 Ändringar i säkerhetsskyddslagen m.m.

3.3.5 Säkerhetsskyddad upphandling

När ska en säkerhetsskyddad upphandling göras?

Av 8 § första stycket säkerhetsskyddslagen följer att när staten avser att begära in anbud eller träffa avtal om upphandling där det förekommer hemliga uppgifter ska staten träffa ett skriftligt avtal (säkerhetsskyddsavtal) med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet. Detsamma gäller för kommuner och landsting. Vad som ska gälla för anbudsgivare och leverantörer i frågan om säkerhetsskydd regleras i säkerhetsskyddsavtalet och anpassas efter behovet i varje enskilt fall.

Bestämmelserna om säkerhetsskyddad upphandling gäller inte för bolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande. Bestämmelserna gäller inte heller för enskilda som omfattas av säkerhetsskyddslagen.

Vad innebär ett säkerhetsskyddsavtal?

Att ett säkerhetsavtal har slutits innebär inte att säkerhetsskyddslagen blir tillämplig på anbudsgivarens eller leverantörens verksamhet, utan vad som ska gälla i fråga om säkerhetsskydd regleras i avtalet. Om säkerhetsskyddslagen av något annat skäl är tillämplig på anbudsgivaren eller leverantören, t.ex. på grund av att denna bedriver verksamhet av betydelse för rikets säkerhet, kan åliggandena enligt lagen inte inskränkas genom avtalet (8 § andra stycket säkerhetsskyddslagen).

Syftet med säkerhetsskyddsavtalet är att skyddet för hemliga uppgifter ska vara detsamma oberoende av i vilken verksamhet dessa förekommer.

Vad regleras i säkerhetsskyddsavtalen?

I avtalen regleras hur anbudsgivaren ska utforma sitt säkerhetsskydd avseende informationssäkerhet, tillträdesbegränsning och säkerhetsprövning. Avtalen kan också innehålla villkor om bl.a. säkerhetsskyddsorganisation, utbildning och information, kontroll,

vite, säkerhetsskyddsinstruktion och säkerhetsplan.[9] Säkerhetsskyddsavtalet är som huvudregel kopplat till affärsavtalet genom att det sistnämnda görs beroende av att åliggandena i säkerhetsskyddsavtalet följs av leverantören.

3.3.6 Intern utbildning och kontroll

Myndigheter och andra som lagen gäller för ska se till att personalen får utbildning i frågor om säkerhetsskydd och att säkerhetsskyddet kontrolleras (30 § säkerhetsskyddslagen).

Av förarbetena[10] framgår att en förutsättning för ett effektivt säkerhetsskydd är att all personal får grundläggande utbildning i ämnet. I första hand gäller det de som direkt befattar sig med sekretessbelagda uppgifter eller har sin arbetsplats på ett känsligt område. Det betonas dock att grundläggande kunskaper bör finnas hos samtliga medarbetare på en arbetsplats som omfattas av säkerhetsskyddet.

Syftet med den interna kontrollen är att se till att bestämmelserna om säkerhetsskydd efterlevs vid den egna myndigheten och att skyddsnivån är jämn och hög.

3.3.7 Tillsyn, föreskrifter och anmälan till regeringen

Tillsyn

I 31 § säkerhetsskyddslagen anges att regeringen föreskriver vem som ska kontrollera säkerhetsskyddet hos myndigheter och andra som lagen gäller för samt hos anbudsgivare och leverantörer som har träffat ett säkerhetsskyddsavtal. Därutöver anges att staten, kommuner och landsting ska se till att det finns ett tillfredsställande säkerhetsskydd hos de bolag, föreningar och stiftelser över vilka de utövar ett rättsligt bestämmande inflytande samt hos anbudsgivare och leverantörer med vilka de har träffat ett säkerhetsskyddsavtal.

[9] Försvarsmaktens Handbok Säkerhetsskyddad upphandling med säkerhetsskyddsavtal, 2010 års utgåva (M7739-352025), s. 31.
[10] Prop. 1995/96:129 s. 29.

Säkerhetspolisen och Försvarsmakten utför tillsyn av myndigheter enligt den fördelning av ansvaret som anges i 39 § säkerhetsskyddsförordningen. Säkerhetspolisen ska också utföra tillsyn över kommuner och landsting (3 § och 39 § 2 säkerhetsskyddsförordningen). När det gäller bolag, föreningar, stiftelser och enskilda näringsidkare utövas kontrollen av Affärsverket svenska kraftnät för elförsörjningsverksamhet, Post- och telestyrelsen för verksamhet som avser elektronisk kommunikation, Transportstyrelsen för flygtransportverksamhet och i övrigt länsstyrelsen (19 § andra stycket och 40 § säkerhetsskyddsförordningen). Även på dessa områden kan dock säkerhetsskyddet kontrolleras av Säkerhetspolisen och Försvarsmakten. Kontrollen ska i så fall utföras i samråd med den primärt ansvariga myndigheten (42 § säkerhetsskyddsförordningen)

Föreskriftsrätt

I 33 § säkerhetsskyddslagen anges att regeringen eller den myndighet som regeringen utser meddelar de närmare föreskrifter som behövs för lagens tillämpning. Bestämmelser om föreskriftsrätt finns i 43–45 §§ säkerhetsskyddsförordningen. Av 43 och 44 §§ framgår att Säkerhetspolisen får meddela närmare föreskrifter i fråga om förfarandet vid registerkontroll och att Säkerhetspolisen och Försvarsmakten i övrigt får meddela föreskrifter för sina respektive tillsynområden.

Övriga myndigheters föreskrifträtt regleras i 45 §. där det anges att myndigheterna ska meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen i fråga om säkerhetsskyddet inom sina verksamhetsområden, om det inte är uppenbart obehövligt. Vidare finns bestämmelser om samråd och om att föreskrifterna får avvika från föreskrifter meddelade av Säkerhetspolisen eller Försvarsmakten endast om det har medgivits.

Anmälan till regeringen

Bestämmelser om anmälan till regeringen finns i 48 och 49 §§ säkerhetsskyddsförordningen. Sådan anmälan ska göras, om det vid utövandet av tillsyn över säkerhetsskyddet konstateras brister som,

trots påpekanden, inte rättas till eller om det vid säkerhetsprövning hos en statlig myndighet kommer fram att en person som redan är anställd vid myndigheten måste anses olämplig från säkerhetssynpunkt för sin befattning.

3.3.8 Internationell samverkan

Det finns några bestämmelser i säkerhetsskyddslagen och säkerhetsskyddsförordningen som tar sikte på internationell samverkan. Det gäller dels 15 § säkerhetsskyddslagen om registerkontroll efter ansökan från annan stat eller mellanfolklig organisation, dels 17 § säkerhetsskyddsförordningen om säkerhetsskyddsavtal vid internationellt samarbete om utveckling och produktion av försvarsmateriel. Bestämmelserna och dess bakgrund beskrivs i kapitel 20.

4 Skyddsintressen

I de följande avsnitten redogör vi översiktligt för reglering som har särskild relevans för säkerhetsskyddslagen.

Säkerhetsskyddets övergripande syfte är att förebygga spionerі, sabotage och andra brott som hotar rikets säkerhet samt terroristbrott, även om brotten inte hotar rikets säkerhet. I avsnitt 4.1 redogör vi för straffbestämmelser avseende bl.a. dessa brott.

Vidare är säkerhetsskyddslagen i hög grad uppbyggd kring behovet av åtgärder för att skydda hanteringen av hemliga uppgifter, dvs. uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL, och som rör rikets säkerhet. I avsnitt 4.2 redogör vi för bestämmelser om sekretess som kan utgöra grund för att hanteringen av uppgifterna omfattas av krav på säkerhetsskydd.

I fråga om säkerhetsskyddsåtgärder till skydd mot terrorism finns en nära koppling till bestämmelserna om skyddsobjekt i skyddslagen (2010:305). I avsnitt 4.3 redogör vi för de bestämmelserna.

4.1 Brott som säkerhetsskyddet ska skydda mot

4.1.1 Spionerі och annan olovlig underrättelseverksamhet

Ett förstärkt skydd mot främmande makts underrättelseverksamhet

Kapitel 19 i brottsbalken (Om brott mot Sveriges säkerhet) handlar om brott som innebär olika slag av angrepp mot svenska staten vilka främjar utländska intressen. Sedan den 1 juli 2014 gäller en ändrad lydelse för flera av de centrala straffbestämmelserna och

också en ny straffbestämmelse om olovlig underrättelseverksamhet mot Sverige.[1] Ändringarna i kapitlet (som också har en ny lydelse av kapitelrubriken) innebär skärpningar i den reglering som bl.a. rör skydd mot främmande makts underrättelseverksamhet. I lagstiftningsärendet behandlades innebörden av begreppet rikets säkerhet som i bl.a. den nya lydelsen av spioneribestämmelsen kom att ersättas av *Sveriges säkerhet*.

Spioneri

I 19 kap. 5 respektive 6 § brottsbalken finns bestämmelser om straff för spioneri och grovt spioneri. Detta brott har som föremål för gärningen vissa uppgifter om försvarsverk, vapen, förråd, import, export, tillverkningssätt, underhandlingar, beslut eller något förhållande i övrigt, vars uppenbarande för främmande makt kan medföra *men för Sveriges säkerhet*. Denna beskrivning av vilket men (skada) som uppgiftens uppenbarande kan ha är ny. Före lagändringen 2014 var motsvarande lydelse; *men för totalförsvaret eller eljest för rikets säkerhet*.

I fråga om spioneribestämmelsens tillämpningsområde gjorde regeringen bedömningen att vilka förhållanden som är av betydelse för Sveriges säkerhet – och i vilka fall men-rekvisitet är uppfyllt – är delvis avhängigt hur samhället är ordnat samt beroende av hotens karaktär och nationens medel för att möta dessa.[2] Regeringen anförde vidare att utvecklingen har fört med sig att uppgifter som är skyddsvärda med hänsyn till Sveriges säkerhet i dag kan finnas inom fler områden än tidigare. Det betonades vidare att för frågan om straffansvar det inte är avgörande inom vilket samhällsområde den aktuella uppgiften finns och att spioneribestämmelsen således kan träffa även underrättelseverksamhet som riktar sig mot t.ex. företag, politiska företrädare och universitet, om uppgifterna rör sådana förhållanden som det kan skada Sveriges säkerhet att en främmande makt känner till.

Regeringen anförde också att tillämpningsområdet inte bör begränsas till uppgifter rörande förhållanden av hemlig natur. En

[1] Se SFS 2014:383 som föranletts av riksdagens beslut med anledning av Prop. 2013/14:51 Förstärkt skydd mot främmande makts underrättelseverksamhet.
[2] a. prop., s. 39.

sådan ändrad ordning, som förordats av Svenska advokatsamfundet, ansåg regeringen kunna innebära att i och för sig straffvärda förfaranden som kan skada skyddsintresset faller utanför tillämpningsområdet, t.ex. när det är fråga om uppgifter som hanteras i verksamheter som inte lyder under offentlighets- och sekretesslagen eller vid sammanställningar av öppna uppgifter.[3]

Slopandet av den tidigare hänvisningen i men-villkoret till ”totalförsvaret” motiverades på följande sätt:[4]

> Men-rekvisitet innebär att spioneribestämmelsen endast är tillämplig på uppgifter som rör förhållanden av sådan betydelse att dess uppenbarande för främmande makt kan skada Sveriges säkerhet. Det är alltså inte tillräckligt för straffansvar att ett förfarande kan skada totalförsvaret utan att samtidigt innebära en potentiell skada för Sveriges säkerhet. Trots det nämns i dag totalförsvaret särskilt i samband med men-rekvisitet. Utredningen har föreslagit att rekvisitet ”totalförsvaret” ska tas bort från bestämmelsen. Begreppet omfattar både militär och civil verksamhet som behövs för att förbereda Sverige för krig. Totalförsvarshänsyn spelar av uppenbara skäl en viktig roll vid bedömningen av om en uppgift är av betydelse för Sveriges säkerhet. Som utredningen har konstaterat fyller emellertid rekvisitet ”totalförsvaret” inte någon självständig funktion för straffbestämmelsens tillämpning.

Vid revisionen behölls exempelförteckningen i straffbestämmelsen. Utredningen om förstärkt skydd mot främmande makts underrättelseverksamhet hade i sitt betänkande (SOU 2012:95) föreslagit att den exemplifierande uppräkningen av uppgifter skulle utgå ur lagtexten. Flera remissinstanser ställde sig tveksamma till förslaget och menade att en sådan ändring skulle medföra en osäkerhet om tillämpningsområdet. Regeringen instämde i kritiken och ansåg att exemplifieringen borde kvarstå. Samtidigt betonade regeringen att uppräkningen inte är uttömmande och att det varken är möjligt eller lämpligt att lämna en uttömmande uppräkning av dessa uppgifter i paragrafen eller att närmare ringa in de verksamhetsområden där de kan finnas. Regeringen anförde vidare att det känsliga kunskapsområde som spioneribestämmelsen är avsedd att skydda inte är konstant utan påverkas av samhällsutvecklingen och att därmed en viss osäkerhet är oundviklig i detta avseende.

[3] I tidigare förarbeten till spioneribestämmelsen har framhållits att systematiskt insamlande av uppgifter, vilka var och en för sig är ofarliga, kan vara menligt för Sveriges säkerhet när de sammanställs. Det kan t.ex. gälla uppgifter om trafiken i en viss hamn.
[4] a. prop., s.41.

Obehörig befattning med och vårdslöshet med hemlig uppgift

I 19 kap. 7 och 8 §§ brottsbalken finns bestämmelser om straff för obehörig befattning med hemlig uppgift. Vid revisionen år 2014 förenklades brottsbeskrivningen. Brottet skiljer sig från spioneri på så sätt att straffansvar inte förutsätter att gärningsmannens syfte varit att gå främmande makt tillhanda men väl att det varit fråga om uppgifter rörande förhållanden av hemlig natur.

I 19 kap. 9 § brottsbalken finns bestämmelser om straff för vårdslöshet med hemlig uppgift. Brottet är ett oaktsamhetsbrott. I övrigt är rekvisiten desamma som vid brottet obehörig befattning med hemlig uppgift.

Olovlig underrättelseverksamhet mot Sverige

Enligt den nya bestämmelsen om olovlig underrättelseverksamhet mot Sverige i 19 kap. 10 § brottsbalken träffas den som ”hemligen eller med användande av svikliga medel antingen bedriver verksamhet vars syfte är anskaffande av uppgifter om förhållanden vars uppenbarande för främmande makt kan medföra men för Sveriges säkerhet eller medverkar till sådan verksamhet mer än tillfälligt” av straffansvar. Bestämmelsen har motiverats med att det i betydande omfattning förekommer att främmande makt bedriver oönskad underrättelseverksamhet i Sverige som syftar till att komma över uppgifter som är känsliga med hänsyn till Sveriges säkerhet. Det utmärkande för sådan underrättelseverksamhet är att den sker dolt och med användande av svikliga medel, till skillnad från den legitima underrättelseverksamheten som kännetecknas av att den sker öppet och i andra former.

Olovlig underrättelseverksamhet mot främmande makt m.m.

Vid ändringarna år 2014 flyttades med viss revision den bestämmelse om olovlig underrättelseverksamhet som tidigare fanns i 19 kap. 10 § första stycket brottsbalken till en ny paragraf, 10 a §. Bestämmelsen anger att den som, för att gå främmande makt tillhanda, här i landet antingen bedriver verksamhet vars syfte är anskaffande av uppgifter om förhållanden vars uppenbarande för

den främmande makten kan medföra men för annan främmande makts säkerhet eller medverkar till sådan verksamhet mer än tillfälligt, döms för olovlig underrättelseverksamhet mot främmande makt. Vid revisionen gjordes en språklig förenkling. Den bestod i att ”militära förhållanden” inte längre särskilt anges i bestämmelsen. Därmed blir, menade man i förarbetena, det tydligare att straffbestämmelsen tar sikte på verksamhet som är inriktad på att komma över uppgifter om sådana förhållanden som det kan skada den främmande makten att en annan främmande makt känner till, oavsett om det är fråga om militära eller andra förhållanden.

Bestämmelser om underrättelseverksamhet mot person (s.k. flyktingspionage) som tidigare fanns i 19 kap. 10 § andra stycket finns numera i en ny paragraf (10 b).

Andra straffbestämmelser i 19 kap. brottsbalken

I 19 kap. brottsbalken finns vidare bestämmelser om straff för bl.a. högförräderi, trolöshet vid förhandling med främmande stat, olovlig värvning, tagande av utländskt understöd och olovlig underrättelseverksamhet mot person. Den närmare innebörden av dessa bestämmelser utvecklas inte här.

4.1.2 Sabotage och andra brott i brottsbalken som kan hota rikets säkerhet

Sabotage m.m.

I 13 kap. brottsbalken finns straffbestämmelser avseende allmänfarliga brott. Vissa av dessa brott (bl.a. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, sabotage, grovt sabotage, kapning, sjö- eller luftfartssabotage och flygplatssabotage) anses beroende på syftet med brottet utgöra brott mot rikets säkerhet. Flera av de gärningar som beskrivs i 13 kap. brottsbalken (bl.a. sabotage, kapning och sjö- och luftfartssabotage, spridande av gift eller smitta) ska i stället under vissa förutsättningar utgöra terroristbrott (se avsnitt 4.1.3).

Bestämmelser om straff för *sabotage och grovt sabotage* finns i 13 kap. 4 och 5 §§ brottsbalken. Sabotage föreligger bl.a. när någon förstör eller skadar egendom som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning eller förvaltning eller för upprätthållande av allmän ordning och säkerhet i riket. Bestämmelsen omfattar även skadegörelse eller annan åtgärd som allvarligt stör eller hindrar den allmänna samfärdseln eller användningen av telegraf, telefon, radio eller dylikt allmänt hjälpmedel eller av anläggning för allmänhetens förseende med vatten, ljus, värme och kraft.

Uppror m.m.

I 18 kap. brottsbalken finns bestämmelser till skydd för rikets inre säkerhet. I 1 § stadgas om straff för *uppror* när någon företar handling i uppsåt att med vapenmakt eller annars med våldsamma medel omstörta statsskicket eller för att framtvinga eller hindra åtgärd eller beslut av statschefen, regeringen, riksdagen eller högsta domarmakten.

4 § handlar om *olovlig kårverksamhet*, som består i att bilda eller delta i sådan organisation som lätt kan utvecklas till sådant maktmedel som militär trupp eller polisstyrka.

Den som utövar olaga tvång eller olaga hot för att påverka den allmänna åsiktsbildningen kan enligt 5 § dömas för *brott mot medborgerlig frihet*.

Tjänstefel och brott mot tystnadsplikt

I 20 kap. 1 § brottsbalken finns bestämmelser om straff för tjänstefel. Brottet innebär att någon uppsåtligen eller av oaktsamhet vid myndighetsutövning genom handling eller underlåtenhet åsidosätter vad som gäller för uppgiften.

Bestämmelser om *brott mot tystnadsplikt* finns i 20 kap. 3 § brottsbalken. Där anges att den som röjer en uppgift, som han eller hon är skyldig att hemlighålla enligt lag eller annan författning eller enligt förordnande eller förbehåll som har meddelats med stöd av lag eller annan författning, eller som olovligen utnyttjar en sådan uppgift, om inte gärningen annars är belagd med straff, ska dömas

för brott mot tystnadsplikt. Bestämmelsen är i första hand en till offentlighets- och sekretesslagen kopplad sanktionsbestämmelse.

Andra straffbestämmelser i brottsbalken som kan vara relevanta för säkerhetsskyddet

Ytterligare ett antal straffbestämmelser i brottsbalken kan beroende på omständigheterna ha betydelse för säkerhetsskyddet, även om bestämmelserna inte direkt pekar ut rikets säkerhet som det intresse som ska tillgodoses genom straffsanktionerna. Både tillgreppsbrott och trolöshetsbrott (t.ex. stöld och förskingring) i 8 respektive 10 kap. brottsbalken kan utgöra angrepp mot rikets säkerhet.

Bland brotten mot frihet och frid i 4 kap. brottsbalken kan nämnas 6 § andra stycket om olaga intrång. Bestämmelsen syftar till att skydda lokaler där människor arbetar eller annars vistas. Genom bestämmelsen ges stöd för att kunna avvisa eller avhysa obehöriga personer från myndigheters och företags lokaler. I 4 kap. finns också bestämmelser om brytande av post- och telehemlighet, intrång i förvar, olovlig avlyssning och dataintrång (8–9 a och 9 c §§). Även dessa brott kan beröra förhållanden av betydelse för rikets säkerhet.

4.1.3 Terroristbrott

Till följd av EU:s rambeslut om terrorism infördes det särskilda terroristbrottet i 2 § lagen (2003:148) om straff för terroristbrott.[5] Straffbestämmelsen är konstruerad på så sätt att ett kvalificerande rekvisit gäller för att vissa uppräknade brott ska anses vara terroristbrott. Det kvalificerande rekvisitet ställer upp krav på att gärningen allvarligt kan skada en stat eller mellanstatlig organisation och att avsikten med gärningen är att

[5] Prop. 2002/03:38 Straffansvar för terroristbrott, bet. 2002/03:JuU12, rskr. 2002/03:148 EGTL164/2002. s. 3.

1. injaga allvarlig fruktan hos en befolkning eller befolkningsgrupp,
2. otillbörligen tvinga offentliga organ eller en mellanstatlig organisation att vidta eller att avstå från attvidta en åtgärd, eller
3. allvarligt destabilisera eller förstöra grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturer i en stat eller i en mellanstatlig organisation.

De gärningar som kan utgöra terroristbrott räknas upp i lagens 3 §, och är bl.a. mord, dråp, grov misshandel, människorov, olaga frihetsberövande, grov skadegörelse, mordbrand och grov mordbrand, allmänfarlig ödeläggelse, sabotage och grovt sabotage, kapning och sjö- eller luftfartssabotage, flygplatssabotage och spridande av gift eller smitta.

4.2 Offentlighets- och sekretesslagen

Allmänt om offentlighet och sekretess

Reglerna i offentlighets- och sekretesslagen gäller i första hand myndigheters verksamhet men de gäller även hos bl.a. kommunala bolag och stiftelser samt hos vissa utpekade organ (2 kap. 1, 3 och 4 §§). Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnade av en allmän handling eller på något annat sätt (3 kap. 1 §). Det saknar således betydelse om uppgiften dokumenterats i en allmän handling, i en handling som inte är allmän eller om den inte alls har dokumenterats. Det innebär att iakttagelser av objekt också kan omfattas.

Kopplingen mellan säkerhetsskyddslagen och offentlighets- och sekretesslagen

Som framgår av redovisningen av säkerhetsskyddslagen i kapitel 3 är säkerhetsskyddslagen i hög grad uppbyggd kring behovet av åtgärder för att skydda hanteringen av hemliga uppgifter. Med hemlig uppgift avses en uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet (4 § 1

säkerhetsskyddsförordningen). Bestämmelserna om informationssäkerhet tar sikte på hemliga uppgifter (7 § 1 säkerhetsskyddslagen). Också bestämmelser om placering i säkerhetsklass (17 § säkerhetsskyddslagen) utgår från att en anställd eller den som annars deltar i verksamheten får del av hemliga uppgifter.[6] Säkerhetsskyddsförordningen innehåller bestämmelser om hantering av hemlig handling, dvs. en handling som innehåller hemlig uppgift. En hemlig handling kan vara en allmän handling, en intern handling, en minnesanteckning eller ett koncept som innehåller hemliga uppgifter. Även lagringsmedier och annat liknande arbetsmaterial är att jämställa med hemliga handlingar, om de innehåller hemliga uppgifter.

I offentlighets- och sekretesslagen är det främst den s.k. försvarssekretessen i 15 kap. 2 § som avser förhållanden av betydelse för rikets säkerhet. Det finns andra sekretessbestämmelser där det primära skyddsintresset är ett annat men som samtidigt kan avse förhållanden som i vissa fall kan vara av betydelse även för rikets säkerhet. Det gäller för utrikessekretessen i 15 kap. 1 §, och förundersökningssekretessen i 18 kap. 1 §. Men även andra bestämmelser om sekretess i 18 kap. kan ge ledning om vilka slag av förhållanden som kan vara är av betydelse för rikets säkerhet. I det följande beskrivs nämnda sekretessbestämmelser.

Försvarssekretess

En särskild betydelse i sammanhanget har bestämmelsen om försvarssekretess i 15 kap. 2 § OSL. De villkor som gäller för att försvarssekretessen ska vara tillämplig är dels att en uppgift ska röra verksamhet, planläggning eller annan förberedelse för att försvara landet eller i övrigt röra totalförsvaret, dels att uppgiften – om den röjs – kan skada landets försvar eller på annat sätt vålla fara för rikets säkerhet. För att en uppgift ska rymmas i sekretessområdet krävs att ett röjande av uppgiften innebär en minskad förmåga att försvara landet (avser främst det militära försvaret)

[6] I säkerhetsskyddslagen används uttrycket *rör* rikets säkerhet i 6 § om säkerhetsskydd medan det i 17 § om säkerhetsklasser talas om *betydelse för* rikets säkerhet. Förarbetena till säkerhetsskyddslagen ger ingen ledning huruvida någon skillnad i sak är avsedd.

eller minskade möjligheter att uthärda ett krig (till exempel försörjningsfrågor).

Om det kan antas att ett röjande av en uppgift leder till att Sverige får minskad försvarsförmåga, försvarsvilja eller eliminerar eller minskar effekten av ett framtaget försvarssystem, så anses ett sådant röjande skada landets försvar. En sådan uppgift omfattas således av försvarssekretess.

Försvarssekretess kan t.ex. i fråga om Försvarsmakten vara tillämplig i såväl nationell som internationell verksamhet. Uppgifter inom det civila försvaret kan också omfattas av försvarssekretess om uppgifterna rör verksamhet som behövs för att förbereda det civila samhället för krig. I det civila försvaret ingår samhällsviktig infrastruktur som t.ex. elförsörjning, vattenförsörjning, telekommunikation, hälso- och sjukvård, radio och tv.

Uppgifter som omfattas av försvarssekretess rör alltid rikets säkerhet. Sådana uppgifter ska således ges ett säkerhetsskydd.

Utrikessekretess

Utrikessekretess enligt 15 kap 1 § OSL gäller först och främst uppgifter som rör Sveriges förbindelser med annan stat. Exempel på sådana förbindelser är Sveriges utrikespolitiska förbindelser, handelsförbindelser och kulturella förbindelser.

Bestämmelsen om utrikessekretess har sin största betydelse för regeringen, Regeringskansliet och utrikesrepresentationen, men den kan också aktualiseras i annan verksamhet.

För att sekretess ska gälla för en uppgift krävs att ett röjande av uppgiften kan antas störa Sveriges mellanfolkliga förbindelser eller på annat sätt skada landet. Skadan ska vara väsentlig och mindre missnöjen eller störningar i förbindelserna räcker inte för sekretess.

Uppgifter som omfattas av utrikessekretess kan ha betydelse för rikets säkerhet och är då hemliga uppgifter. Uppgifter som omfattas av utrikessekretess bedöms sällan röra rikets säkerhet. Sådana uppgifter kan dock förekomma t.ex. vid förberedelser för försvaret av Sverige som inbegriper stöd från andra stater eller mellanfolkliga organisationer.

Bestämmelser i 18 kap. offentlighets- och sekretesslagen

I 18 kap. OSL finns bestämmelser främst till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. Beroende på omständigheterna kan uppgifter som skyddas genom dessa bestämmelser anses röra rikets säkerhet. Det kan också vara så att uppgifterna omfattas av sekretess med stöd av bestämmelserna om försvarssekretess eller utrikessekretess.

Enligt 18 kap. 1 § OSL gäller sekretess för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Sekretess gäller, under motsvarande förutsättningar, för bl.a. uppgift som hänför sig till annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

I 18 kap. OSL finns också sekretessbestämmelser till skydd för bl.a. underrättelseverksamhet (2 §), kvalificerade skyddsidentiteter (5 §) säkerhets- eller bevakningsåtgärd (8 §), chiffer och kod (9 §), upplysning som kan användas i syfte att åstadkomma kärnsprängning eller spridning av kärnvapen (12 §) och risk- och sårbarhetsanalyser (13 §). Flera av bestämmelserna har tillkommit eller materiellt sätt ändrats sedan säkerhetsskyddslagen infördes. Det kan finnas anledning att redogöra för bestämmelserna som avser säkerhets- eller bevakningsåtgärd, chiffer och kod och om risk- och sårbarhetsanalyser.

I fråga om *säkerhets- och bevakningsåtgärd* gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser

1. byggnader eller andra anläggningar, lokaler eller inventarier,
2. tillverkning, förvaring, utlämning eller transport av pengar eller andra värdeföremål samt transport eller förvaring av vapen, ammunition, sprängämnen, klyvbart material eller radioaktiva ämnen,

3. telekommunikation eller system för automatiserad behandling av information,
4. behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling,
5. den civila luftfarten eller den civila sjöfarten,
6. transporter på land av farligt gods, eller
7. hamnskydd.

Det handlar således om sekretess för olika brottsförebyggande åtgärder som i huvudsak hänför sig till annan verksamhet än polisens. Vissa av åtgärderna syftar endast indirekt till att förebygga brott. För sekretess krävs att det vid en prövning ska kunna antas, att ett röjande av uppgiften motverkar syftet med säkerhets- eller bevakningsåtgärden. Innebörden av vissa av punkterna finns anledning att beröra.

Första punkten avser byggnader eller andra anläggningar, lokaler eller inventarier. Med anläggningar avses bl.a. kulvertsystem, upplag och uppställningsplatser. Det är således inte enbart utrymmen med en omslutningsyta (huskropp, berganläggning eller motsvarande) som omfattas utan även öppna inhägnade ytor. Säkerhets- eller bevakningsåtgärder för byggnader, anläggningar och lokaler avser utformningen av tillträdesbegränsning som ska hindra att obehöriga får tillträde till utrymmen eller att upptäcka obehöriga. Dessa åtgärder kan även syfta till att hindra eller upptäcka avlyssning. Exempel på säkerhets- eller bevakningsåtgärder är byggnadstekniska åtgärder (mekaniskt inbrottsskydd), teknisk bevakning (inbrottslarm, passerkontroll och övervakningssystem) och manuell bevakning. Byggnadsritningar och projekteringshandlingar för exempelvis inbrottslarm som kartlägger säkerhetsåtgärder eller säkerhetsbrister är också sådana uppgifter som kan omfattas av den aktuella bestämmelsen. Sekretessen kan även gälla uppgifter om instruktioner och tjänstgöringslistor som rör bevakningen.

Tredje punkten avser telekommunikation med vilket avses överföring av meddelanden med telefoni, tråd, radio eller liknande metod. Syftet med att skydda telekommunikationer är att hindra brott mot rikets säkerhet samt sabotage eller brytande av post-

eller telehemlighet. Sekretessbestämmelsen syftar även till att skydda data- och telekommunikationer för att t.ex. hindra brott mot rikets säkerhet. Sekretessen avser uppgifter som rör skyddet för telekommunikation som, om de röjs, kan leda till att syftet med säkerhetsåtgärderna motverkas. Uppgifterna kan avse såväl fysiska som logiska företeelser. Exempel på uppgifter som kan omfattas av sekretessen är frekvenser och sändningsmetoder för radiokommunikation, adressinformation i tele- och datakommunikationsnätverk t.ex. IP-adresser. Uppgifter som lämnar eller kan bidra till upplysning om säkerhetsåtgärder i ett it-system omfattas också av bestämmelsens tredje punkt. Säkerhetsåtgärder behöver inte enbart vara av teknisk natur utan kan även röra administrativa rutiner som utgör en del av säkerhetsåtgärderna i ett it-system, exempelvis rutiner för manuell analys av säkerhetsloggar. Det är inte enbart de säkerhetsåtgärder som syftar till att säkerställa sekretessen för uppgifterna i ett it-system som omfattas av sekretess. Även de säkerhetsåtgärder som säkerställer tillgänglighet i ett it-system omfattas av sekretess, om ett röjande av uppgifterna kan antas motverka syftet med säkerhetsåtgärden. Ytterligare ett exempel är ett it-system som är avsett för offentliga uppgifter och som behöver skyddas mot obehörig ändring. Sekretessbestämmelsen kan således avse andra säkerhetsåtgärder än de som ska säkerställa sekretessen för uppgifter i ett it-system.

Fjärde punkten avser arrangemang och fördelning av behörighetskoder och behörighetsnycklar. Detta kan exempelvis omfatta användarens och administratörers lösenord till it-system, personliga koder till aktiva kort eller s.k. privata nycklar för autentisering. Även lösenord till utrustning som ingår i it-system och som ordinarie användare normalt inte har åtkomst till (kommunikationsutrustning) omfattas av sekretessen.

I fråga om *chiffer och kod* gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod, om det kan antas att syftet med metoden motverkas om uppgiften röjs och metoden har till syfte att

1. underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts, eller
2. göra det möjligt att kontrollera om data i elektronisk form har förvanskats.

I fråga om *risk- och sårbarhetsanalyser* gäller sekretess för uppgift som hänför sig till en myndighets verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida krissituationer, planering och förberedelser inför sådana situationer eller hantering av sådana situationer, om det kan antas att det allmännas möjligheter att förebygga och hantera fredstida kriser motverkas om uppgiften röjs. Bestämmelsen kom till för att skydda känsliga uppgifter som kan komma fram i samband med risk- och sårbarhetsanalyser, som t.ex. resonemang som förs när helhetsbilden skärskådas och analyseras. Som exempel anges också att det kan vara fråga om gränssättande faktorer för samhällets krishanteringsförmåga, förbättringsåtgärder som vägs mot varandra, grunder för nedprioriteringar, detaljer om var reaktionstiden är lång och var möjligheten att upptäcka en incident är låg m.m.[7]

4.3 Skyddsobjekt enligt skyddslagen

Kopplingen mellan säkerhetsskyddslagen och skyddslagen

Det finns bl.a. i fråga om säkerhetsskyddsåtgärder till skydd mot terrorism en nära koppling till bestämmelserna om skyddsobjekt i skyddslagen.[8] Ett beslut om skyddsobjekt innebär att obehöriga inte har tillträde till skyddsobjektet. Nedan redogör vi för bestämmelser i skyddslagen som anger förutsättningar för att utse skyddsobjekt. I kapitel 17 återkommer vi till regleringen i skyddslagen. Där behandlas närmare bl.a. förhållandet mellan bestämmelser om tillträdesförbud avseende skyddsobjekt och bestämmelser om tillträdesbegränsning enligt säkerhetsskyddslagen.

En moderniserad skyddslag

Skyddslagen trädde i kraft den 1 juli 2010 och ersatte då lagen (1990:217) om skydd för samhällsviktiga anläggningar m.m. Lagen ger, liksom sin föregångare, rättsliga förutsättningar för ett kvalificerat skydd för vissa byggnader, andra anläggningar och

[7] Prop. 2004/05:5 Vårt framtida försvar, s. 260.
[8] Se 26 och 27 §§ säkerhetsskyddsförordningen.

områden samt militära fartyg och luftfartyg (skyddsobjekt). Skyddslagen innebär i förhållande till den tidigare lagen på området ett vidgat fokus i fråga om fredstida viktiga samhällsfunktioner Nya möjliga skyddsobjekt är byggnader, andra anläggningar och områden som används eller är avsedda för Sveriges försörjning med sedlar och mynt, verksamhet till upprätthållande av allmän ordning och säkerhet samt verksamhet som bedrivs inom kriminalvården. De tidigare militära skyddsområdena har avskaffats. En ny möjlighet att besluta att vissa vattenområden ska vara skyddsobjekt har införts som en kompensatorisk åtgärd.

I likhet med vad som gällde enligt den tidigare lagen ska skyddslagen kunna ge ett särskilt skydd mot hot i form av sabotage, terroristbrott enligt 2 § lagen om straff för terroristbrott, spionerisamt röjande i andra fall av hemliga uppgifter som rör totalförsvaret (skyddsändamål). Skyddsändamålen har vidare utvidgas till att omfatta även skydd mot angrepp i form av grovt rån.

Ett beslut om skyddsobjekt innebär att obehöriga inte har tillträde till skyddsobjektet. Liksom tidigare skyddas ett skyddsobjekt genom fysiskt bevakningsskydd vilket bl.a. utgörs av bevakningspersonal med särskilda befogenheter. Genom särskilt beslut kan tillträdesförbudet förenas med ett förbud mot att göra avbildningar, beskrivningar eller mätningar av eller inom skyddsobjektet. Såväl tillträdesförbudet som i förekommande fall avbildningsförbudet är straffsanktionerat.

I förarbetena till skyddslagen lämnar regeringen sin syn på möjligheterna att ge lagen ett vidare tillämpningsområde för att kunna omfatta bl.a. it-system.[9]

> Vid bedömningen av vad som kan vara ett möjligt skyddsobjekt har man att titta på verksamheten när det gäller hot och risker kopplade till lagens skyddsändamål. Det handlar då typiskt sett om hotets art och styrkan i hotet samt konsekvensbilden, dvs. de verkningar i ett enskilt fall på samhällets funktionalitet som ett angrepp skulle leda till.
>
> Till detta kommer att skyddet av ett skyddsobjekt, vilket även tidigare har konstaterats, fortsättningsvis bör upprätthållas genom olika typer av bevakningsåtgärder. Det är då ofrånkomligt, av praktiska skäl, att skyddet knyts till anläggningar, byggnader eller områden i syfte att säkerställa en verksamhet som bedrivs. Det innebär att skyddet bör ha en verklig betydelse och vara lämpat för en viss verksamhet. Här kan påpekas att det finns många verksamheter dit allmänheten generellt

[9] Prop. 2009/10:87 Skyddslagen, s. 32 f.

sett inte har rätt till tillträde även om dessa inte är skyddsobjekt, t.ex. verksamhet som bedrivs av privata företag. Vidare är de befogenheter som måste tillkomma bevakningspersonalen för att skyddet ska vara effektivt så pass långtgående att det, sett utifrån grundlagsfästa intressen och rättssäkerhet, inte är lämpligt att lagen utvidgas mer än absolut nödvändigt.

Det sagda innebär bl.a. att en utvidgning som medför att nya breda kategorier av verksamheter, som i sin tur kan antas omfatta ett mycket stort antal byggnader m.m., som utgångspunkt inte bör tillföras i en ny lag. Inte heller är det generellt möjligt att genom bevakning skydda hela system, framförallt inte de som är av icke-fysisk karaktär. Regeringen menar därför att t.ex. it-system eller elektroniska system som sådana, inte är lämpliga eller möjliga som skyddsobjekt.

Skyddsobjekt

Förutsättningarna för vad som ska kunna beslutas vara skyddsobjekt framgår uttömmande av 4–6 §§ skyddslagen.[10] 4 § innehåller en uppräkning över byggnader, anläggningar och områden vilka huvudsakligen används för civila ändamål och som kan beslutas vara skyddsobjekt. Uppräkningen omfattar

1. statschefens och tronföljarens residens och bostäder samt statsministerns bostäder,
2. byggnader, andra anläggningar och områden som staten har äganderätt eller nyttjanderätt till och som disponeras av riksdagen eller riksdagsförvaltningen,
3. byggnader och andra anläggningar som staten, en kommun eller ett landsting har äganderätt eller nyttjanderätt till och som används eller är avsedda för att leda eller styra statlig eller kommunal verksamhet,
4. byggnader, andra anläggningar och områden som används eller är avsedda för ledning av räddningstjänsten eller totalförsvarets civila delar i övrigt eller för fredstida krishantering, energiförsörjning, vattenförsörjning, elektroniska kommunikationer, transporter eller försvarsindustriella ändamål, och

[10] 6 § gäller endast om Sverige befinner sig i krig eller krigsfara eller om det råder andra utomordentliga förhållanden som är föranledda av krig.

5. byggnader, andra anläggningar och områden som används eller är avsedda för verksamhet som innefattar upprätthållande av allmän ordning och säkerhet, verksamhet inom kriminalvården eller Sveriges försörjning med sedlar och mynt.

I förarbetena[11] konstateras att, när det gäller beslutande statliga och kommunala församlingar, t.ex. riksdagens kammare och kommunfullmäktige, principen om förhandlingsoffentlighet innebär att utrymmet för ett skyddsobjektsarrangemang blir mycket begränsat.[12] Det framhålls att det bör främst vara byggnader m.m. av central betydelse eller som av någon annan anledning har ett särskilt skyddsbehov som kan komma i fråga som skyddsobjekt. Angående punkten 4 som innehåller en uppräkning av byggnader m.m. där det utförs eller kan utföras sådan verksamhet som är av central betydelse för att bevara samhällets grundläggande förmåga på ett tillfredställande sätt påpekas att vissa i den då gällande lagen förekommande uttryck har bytts ut i moderniserande syfte. I somliga fall har detta medfört att kretsen för vad som kan beslutas vara skyddsobjekt utvidgats något.

Införandet av begreppet elektroniska kommunikationer innebär en anpassning till utvecklingen i samhället när det gäller datakommunikationer och annan it-användning och följaktligen en utvidgning av möjliga skyddsobjekt. Ett exempel på detta är möjligheten att förklara anläggningar som ingår i det centrala radiokommunikationssystemet Rakel som skyddsobjekt. Med begreppet elektroniska kommunikationer täcks också in nya företeelser av den tekniska utvecklingen på området i framtiden. Det betonas dock att även om begreppet kan verka omfattande, måste beaktas att skyddsobjektsförklaring kan göras endast för att ge skydd mot de antagonistiska hot som är lagstiftningens skyddsändamål och att ett beslut om skyddsobjekt kan omfatta endast konkreta ting i form av anläggningar och områden, dvs. byggnader och andra anläggningar, kommunikationsnät, noder och installationer bl.a. för sändning och mottagning (t.ex. master o. dyl.).[13]

[11] a. prop., s. 88 f.
[12] Det bör noteras att det finns särskilda lagar om säkerhetskontroll vid sådana sammanträden.
[13] a. prop., s. 112.

Vad avser kriminalvårdens verksamhet anges att det bör, mot bakgrund av lagens skyddsändamål som anges i 1 §, framför allt vara de kriminalvårdsanstalter och häkten med behov av särskilt hög grad av säkerhet som kan komma i fråga som skyddsobjekt. Vidare anges att med byggnader, andra anläggningar och områden som används eller är avsedda för Sveriges försörjning med sedlar och mynt avses Riksbankens inrättningar, samt depåer för kontantförvaring och uppräkningscentraler och motsvarande.

I 5 § anges olika byggnader, anläggningar och områden eller objekt vilka används för verksamhet främst inom Försvarsmakten, Försvarets materielverk och Försvarets radioanstalt och som kan beslutas vara skyddsobjekt. I förhållande till vad som gällde tidigare kan även områden där följder av t.ex. prov- och försöksverksamhet kan inträffa omfattas samt också övningsverksamhet för andra militära ändamål än övningar i samband med utbildning för fredsfrämjande verksamhet. Det kan t.ex. röra sig om utländska förband som övar under subarktiska förhållanden.

5 Närliggande reglering

Det här kapitlet innehåller en översiktlig redogörelse för till säkerhetsskyddslagen närliggande reglering. I det inledande avsnittet (avsnitt 5.1) berör vi regleringen inom områdena luftfartsskydd, hamnskydd och sjöfartsskydd. Därefter kommer vi in på reglering om kärnteknisk verksamhet och strålskydd (avsnitt 5.2) och om skydd för landskapsinformation (avsnitt 5.3). Avslutningsvis redovisar vi reglering om samhällsskydd och beredskap (avsnitt 5.4). I fråga om den nämnda regleringen finns i vissa avseenden en närmare redovisning i anslutning till våra överväganden.

Det finns också ett nära samband mellan lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet och säkerhetsskyddslagen. Det sambandet redovisas i anslutning till våra överväganden om säkerhetsskyddad upphandling i kapitel 19. Det bör också noteras att en annan närliggande lag, skyddslagen (2010:305), redan har tagits upp i avsnitt 4.3. Åtgärder enligt skyddslagen berörs även vidare i kapitel 17.

5.1 Luftfartsskydd, hamnskydd och sjöfartsskydd

Luftfartsskydd

Lagen (2004:1100) om luftfartsskydd kompletterar Europaparlamentets och rådets förordning (EG) nr 2320/2002 av den 16 december 2002 om införandet av gemensamma skyddsregler för den civila luftfarten. Förordningen och dess bilaga innefattar en rad bestämmelser som anger krav för säkerheten på flygplatser. Kraven avser bl.a. säkerhetskontroller av personal, av luftfartyg, av passagerare och av föremål.

Inom luftfartsområdet finns också internationella konventioner som Sverige är bunden av, bl.a. den s.k. Chicagokonventionen.

Flertalet svenska flygplatser är skyddsobjekt, i vart fall vad gäller delar av anläggningarna. Det förhållandet medför att också skyddslagen gäller.

I 26 § 2 säkerhetsskyddsförordningen finns bestämmelser om registerkontroll enligt 14 § säkerhetsskyddslagen (skydd mot terrorism) i fråga om den som ska anställas eller på annat sätt delta i verksamhet som har betydelse för luftfartsskyddet, om det följer av en internationell överenskommelse som Sverige tillträtt eller av en bindande EU-rättsakt på området för luftfartsskydd att säkerhetsprövningen ska omfatta registerkontroll. Bestämmelsen är ett komplement till övriga bestämmelser om registerkontroll till skydd mot terrorism som innefattar bl.a. civila flygplatser, flygstationer, flygpassagerarterminaler och anläggningar inom flygtrafiktjänsten (26 § och 27 § 1 och 7 säkerhetsskyddsförordningen).

Hamnskydd och sjöfartsskydd

Lagen (2006:1209) om hamnskydd kompletterar Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar. Med hamnskydd avses åtgärder som ska vidtas i hamnar i syfte att skydda människor, infrastruktur och utrustning i hamnarna mot allvarliga brott. För själva hamnanläggningarna ska dock inte lagen om hamnskydd tillämpas, utan i stället lagen om sjöfartsskydd (se nedan). Inte heller ska lagen om hamnskydd tillämpas på militära hamnanläggningar.

I likhet med lagen om hamnskydd kompletterar lagen (2004:487) om sjöfartsskydd den ovan nämnda EG-förordningen. Medan lagen om hamnskydd avser skyddet i hamnar, avser lagen om sjöfartsskydd skyddet för fartyg och för själva hamnanläggningarna. Båda lagarna har bestämmelser om bl.a. skyddsnivåer, administrativa åtgärder och tillsyn. Bestämmelserna om tillträdesbegränsning och om tvångsmedel liknar i stora delar vad som gäller enligt lagen om luftfartsskydd. Bestämmelserna ska verka preventivt, och tillämpningen förutsätter inte att det förekommer miss-

tanke om brott. Av de båda lagarna följer att det gäller förbud mot tillträde till hamnar, hamnanläggningar och fartyg, om det genom stängsel eller skyltar eller på annat liknande sätt står klart att allmänheten inte har tillträde.

Av 26 § säkerhetsskyddsförordningen framgår att registerkontroll får göras med anledning av ett förordnande enligt 16 § lagen om sjöfartsskydd eller 4 kap. 3 § lagen om hamnskydd.

5.2 Kärnteknisk verksamhet och strålskydd

Lagen (1984:3) om kärnteknisk verksamhet är inriktad på att ta till vara säkerheten vid den kärntekniska verksamheten och se till att Sverige uppfyller sina åtaganden på icke-spridningsområdet. I lagen anges bl.a. att säkerheten vid kärnteknisk verksamhet ska upprätthållas genom att de åtgärder vidtas som krävs för att förebygga fel i utrustning, felaktig funktion hos utrustning, felaktigt handlande, sabotage eller annat som kan leda till en radiologisk olycka, och förhindra olovlig befattning med kärnämne eller kärnavfall. Lagen innehåller också de centrala bestämmelserna som rör omhändertagande och slutförvaring av kärnavfall och använt kärnbränsle.

Strålskyddslagen (1988:220) och den till lagen hörande förordningen syftar till att skydda människor, djur och miljön från skadliga effekter till följd av såväl joniserande som icke-joniserande strålning. Strålskyddslagen är en allmän skyddslag som täcker i princip alla verksamheter där det finns strålskyddsaspekter. Lagen tillvaratar således även viktiga skyddsintressen vid verksamhet på kärnenergiområdet.

Lagstiftningen avseende kärnteknisk verksamhet och strålskydd är föremål för översyn. Utredningen om en samordnad reglering på kärnteknik- och strålskyddsområdet har i sitt slutbetänkande Strålsäkerhet – gällande rätt i ny form (SOU 2011:18) förslagit en sammanhållen reglering. Betänkandet har remissbehandlats och förslaget bereds inom Regeringskansliet.

Strålsäkerhetsmyndigheten har på uppdrag av regeringen lämnat en rapport i januari 2012 om Översyn av tillståndshavarnas och samhällets förmåga att skydda kärntekniska anläggningar och transporter av kärnämnen mot antagonistiska hot (SSM 2010-2632). Förslagen avser i viss del även ändringar i säkerhetsskydds-

förordningen. Sammanfattningsvis föreslås att ansvaret för tillsyn av säkerhetsskyddet vid kärnkraftverk och registerkontroll i fråga om personal vid kärnkraftverk flyttas från Affärsverket svenska kraftnät och länsstyrelserna till Strålsäkerhetsmyndigheten. Därutöver föreslås också att kretsen som omfattas av registerkontroll vidgas. Förslagen i denna del berör således frågor som omfattas av våra direktiv.

5.3 Skydd för landskapsinformation

Bestämmelser om förbud mot fotografering och andra mätningar finns i lagen (1993:1742) om skydd för landskapsinformation och den till lagen hörande förordningen. Lagen – som tillkommit i syfte att värna om rikets säkerhet vad gäller insamling, lagring, bearbetning och presentation av information rörande förhållanden på marken m.m. – innehåller bestämmelser om dels krav på tillstånd för sjömätning, för fotografering och liknande registrering från luftfartyg samt för upprättande av databaser med landskapsinformation, dels tillståndskrav för spridning av flygbilder, kartor och andra sammanställningar av landskapsinformation.

Lagen definierar landskapsinformation som lägesbestämd information om förhållandena på och under markytan samt på och under sjö- och havsbotten. Lagen innehåller straffbestämmelser för den som uppsåtligen eller av oaktsamhet utan de tillstånd som krävs utför sjömätning, flygfotografering eller inrättar en databas med landskapsinformation över svenskt territorium eller sprider flygbilder, kartor eller andra otillåtna sammanställningar av landskapsinformation.

Regleringen har nyligen setts över av Utredningen om skydd för geografisk information som föreslagit att den nuvarande regleringen ersätts med ny lag och förordning om skydd för geografisk information. Av utredningens betänkande (SOU 2013:51) framgår att det även fortsättningsvis ska krävas tillstånd för sjömätning inom Sveriges sjöterritorium, med undantag för bl.a. sjömätning i insjöar, vattendrag och kanaler. Utredningen föreslår att sjömätning i ringa omfattning undantas från tillståndskravet. Det föreslås vidare att tillståndskravet för inrättande av databas för lagring av geografisk information slopas. Tillstånd för spridning ska alltjämt

krävas för sjögeografisk information, men tillståndskravet begränsas till att gälla information som avser de områden inom vilka det krävs tillstånd för sjömätning och enbart för information som rör förhållanden i ett visst vattenområde. För landgeografisk information föreslås att tillståndskravet begränsas till att gälla enbart information som har hämtats in från luftfartyg genom fotografering eller liknande registrering. Utredningens förslag har remissbehandlats och bereds inom Regeringskansliet.

5.4 Reglering om samhällsskydd och beredskap

Totalförsvar och höjd beredskap

Lagen (1992:1403) om totalförsvar och höjd beredskap innehåller bestämmelser om totalförsvaret och anger vad som gäller vid höjd beredskap. Totalförsvarsbegreppet togs in i lagen om höjd beredskap efter beslut av riksdagen i samband med behandlingen av regeringens proposition Totalförsvar i förnyelse – etapp 2 (se prop. 1996/97:4 s. 54 ff.). Totalförsvar är den verksamhet som behövs för att förbereda Sverige för krig och består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar). För att stärka landets försvarsförmåga kan beredskapen höjas. Höjd beredskap är antingen skärpt beredskap eller högsta beredskap. Under högsta beredskap är totalförsvar all samhällsverksamhet som då ska bedrivas.

Krisberedskap och höjd beredskap m.m.

Förordningen (2006:942) om krisberedskap och höjd beredskap syftar till att statliga myndigheter genom sin verksamhet ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap. Bestämmelserna i förordningen ska tillämpas endast om inte annat föreskrivs i lag eller förordning (2 § andra stycket). Varje myndighet är enligt förordningen skyldig att genomföra risk- och sårbarhetsanalyser. Kommuner och landsting ska genomföra motsvarande arbete enligt lagen (2006:544) om kommuners och lands-

tings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

Konkret syftar arbetet till att öka medvetenheten och kunskapen hos beslutsfattare samt verksamhetsansvariga om vilka hot och risker som finns inom det egna verksamhetsområdet. En väsentlig del av arbetet är att samla information.

I förordningen regleras också vilka myndigheter som ska ha säkra kryptografiska funktioner och Myndighetens för samhällsskydd och beredskap beslutanderätt över vilka företag som ska få tillgång till säkra kryptografiska funktioner respektive avtal om tilldelning med kommuner och organisationer som har behov av kryptografiska funktioner.

I fråga om informationssäkerhet anges att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt och att behovet av säkra ledningssystem särskilt ska beaktas. Myndigheten för samhällsskydd och beredskap har också meddelat föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).[1] Enligt föreskrifterna ska statliga myndigheter tillämpa ett ledningssystem för informationssäkerhet. Föreskrifterna innebär bl.a. krav på att myndigheter ska klassificera sin information, identifiera och hantera risker samt fortlöpande utvärdera och förbättra sin säkerhet. Arbetet ska bedrivas enligt etablerade informationssäkerhetsstandarder. Föreskrifterna gäller inte för Försvarsmakten.

Lagen om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap ställer krav på bl.a. en plan för hantering av extraordinära händelser och på att genomföra risk- och sårbarhetsanalyser som underlag för denna plan. Vidare anges att Myndigheten för samhällsskydd och beredskap får meddela föreskrifter för analyserna, på samma sätt som för de risk- och sårbarhetsanalyser som ska göras av statliga myndigheter enligt förordningen om krisberedskap och höjd beredskap. Myndigheten har meddelat sådana föreskrifter (MSBFS 2010:6 och 2010:7).

[1] Föreskrifterna har beslutats med stöd av 34 § förordningen om krisberedskap och höjd beredskap.

Elberedskap

Elberedskapslagen (1997:288) innehåller bestämmelser om skyldighet att vidta beredskapsåtgärder inom elsektorn. Bestämmelserna gäller för den som bedriver produktion av el, handel med el eller sådan överföring av el som sker med stöd av nätkoncession enligt 2 kap. 1 § ellagen (1997:857). Med beredskapsåtgärder avses åtgärder som behövs för att förebygga, motstå och hantera sådana störningar i elförsörjningen som kan medföra svåra påfrestningar på samhället. Lagen tar sikte på åtgärder för att förhindra störningar på grund av av händelser av exceptionell karaktär såsom krig, terrorhandlingar och sabotage. Genom en lagändring som trädde i kraft den 1 juli 2012 har man frångått det tidigare kravet på att åtgärderna ska säkerställa elförsörjningen när landet är i höjd beredskap. Lagen har därigenom fått ett vidare tillämpningsområde.

Elektronisk kommunikation

Genom lagen (2003:389) om elektronisk kommunikation genomfördes den EG-rättsliga regleringen på området för elektronisk kommunikation. Lagen gäller för den som tillhandahåller allmänt tillgängliga elektroniska kommunikationsnät och kommunikationstjänster. Exempel på nät är telenät, kabel-tv-nät och bredbandsnät och exempel på kommunikationstjänster är fast telefoni, mobiltelefoni och internetanslutning. Lagen om elektronisk kommunikation är en central reglering från informationssäkerhetssynpunkt. I lagen finns bl.a. krav som syftar till att förhindra driftavbrott och att abonnentuppgifter eller andra uppgifter som behandlas vid elektronisk kommunikation sprids till obehöriga. Lagen omfattar dock inte innehållet i meddelanden som överförs med tjänsterna eller i näten.

I lagen anges att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. Syftet med bestämmelserna är att bidra till effektiva och säkra elektroniska kommunikationer samt att skapa en grundläggande säkerhetsnivå för dessa. Med driftsäkerhet avses främst upp-

rätthållande av funktion och tillgänglighet men även uthållighet vid extraordinära händelser i fredstid.

Det finns i lagen även bestämmelser om skyldighet att rapportera störningar eller avbrott av betydande omfattning. Post- och telestyrelsen är tillsynsmyndighet för lagen och har bl.a. beslutat föreskrifter som preciserar kraven på driftssäkerhet, rapportering av störningar och avbrott samt skyddsåtgärder för uppgifter som behandlas i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål.

EU-rättslig reglering om identifiering av europeisk kritisk infrastruktur

Från EU-nivå kan på detta område noteras rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av och klassificering som europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EPCIP). Myndigheten för samhällsskydd och beredskap har på uppdrag av regeringen redovisat strategier med fokus på skydd av samhällsviktiga verksamheter och viktiga samhällsfunktioner (se vidare avsnitt 13.1).

Transport av farligt gods

Syftet med lagen (2006:263) om transport av farligt gods är att förebygga, förhindra och begränsa att transporter av farligt gods eller obehörigt förfarande med godset orsakar skador på liv, hälsa, miljö eller egendom.

Den som transporterar farligt gods eller lämnar farligt gods till någon annan för transport ska vidta de skyddsåtgärder och de försiktighetsmått i övrigt som behövs för att förebygga, hindra eller begränsa att godset, genom transporten eller genom obehörigt förfarande med godset på land, orsakar sådana skador på liv, hälsa, miljö eller egendom som beror på godsets farliga egenskaper.

Skydd mot allvarliga kemikalieolyckor

Efter en allvarlig och uppmärksammad olycka i staden Seveso i Italien 1976, där dioxiner släpptes ut som förorenade mark och förgiftade ett stort antal människor påbörjades ett arbete inom EU som ledde fram det s.k. Svesesodirektivet. Det har sedan kompletteras med Seveso II- och Seveso III-direktiven. Direktiven är i svensk rätt genomförda[2] genom bl.a. lagen (1999:381) om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor (Sevesolagen) och den till lagen hörande förordningen.

Sevesolagen innehåller bl.a. bestämmelser om verksamhetsutövarens skyldigheter och informationsansvar. I Sevesoförordningen anges bl.a. vad som ska kategoriseras som farliga ämnen och tröskelvärden för sådana ämnen. Reglerna i Sevesolagstiftningen tillämpas för verksamheter där farliga ämnen vid ett och samma tillfälle förekommer i vissa mängder. Verksamheter som omfattas av Sevesolagstiftningen är i de flesta fall att betrakta som farlig verksamhet enligt lagen (2003:778) om skydd mot olyckor.

Myndigheten för samhällsskydd och beredskap är central tillsynsmyndighet för verksamhet som faller under Sevesolagen och Sevesoförordningen. Även Naturvårdsverket, Arbetsmiljöverket, länsstyrelserna och kommunerna har tillsynsansvar inom olika områden.

Dammsäkerhet

En samlad reglering av frågor om dammsäkerhet har nyligen införts i miljöbalken (26 kap.). Regleringen i miljöbalken kompletteras av förordningen (2014:214) om dammsäkerhet. Regelverket syftar till att förebygga dammbrott, stödja utvecklingen av dammsäkerhetsarbetet hos dammägarna samt stärka tillsynen av dammsäkerheten. Regleringen innebär i huvudsak följande.

De dammar som finns i Sverige ska klassificeras utifrån en bedömning av ett eventuellt dammhaveris sammanlagda samhälleliga konsekvenser. Beroende på konsekvenserna av ett dammhaveri ska en damm klassificeras i dammsäkerhetsklass A, B, eller C.

[2] Lagstiftningsarbete pågår i Regeringskansliet med anledning av Seveso III-direktivet som ska vara genomfört i medlemsstaterna senast 1 juni 2015.

I klass A klassificeras dammar där ett dammhaveri kan leda till så allvarliga konsekvenser att det leder till en nationell kris.

En damminnehavare ska upprätta en konsekvensutredning där en bedömning görs av de konsekvenser som ett dammhaveri kan medföra. Utredningen ska ges in till länsstyrelsen som på grundval av utredningen fattar beslut om dammsäkerhetsklass. En damminnehavare ska utföra egenkontroll på grundval av ett säkerhetsledningssystem som fastställs av damminnehavaren.

Sprängämnesprekursorer

Europaparlamentets och rådets förordning (EU) nr 98/2013 av den 15 januari 2013 om saluföring och användning av sprängämnesprekursorer har trätt i kraft och är till alla delar bindande och direkt tillämplig i Sverige. Förordningen ska tillämpas från och med den 2 september 2014. I lagen (2014:799) om sprängämnesprekursorer finns till förordningen komplettarande bestämmelser.

Krisberedskap i det centrala betalningssystemet

Utredningen om stärkt krisberedskap i det centrala betalningssystemet har i betänkandet med samma namn (SOU 2011:78) lämnat förslag om bl.a. en lag om krisberedskap i det centrala betalningssystemet. Betänkandet har remitterats och förslaget bereds inom Regeringskansliet.

Den föreslagna lagen anges syfta till att förebygga uppkomsten av allvarliga störningar i det centrala betalningssystemet, och om sådana störningar inträffar säkerställa en tillfredsställande funktion så att följderna av störningarna begränsas, samt att clearing och avveckling av alla transaktioner inom det centrala betalningssystemet kan ske inom utlovad tid. Lagförslaget innehåller bestämmelser med grundläggande säkerhetsnivåer. De säkerhetskrav som enligt förslaget bör ställas på det centrala betalningssystemet bör utformas som en kombination av funktionskrav på detta system och krav på de tekniska system – externa och interna – som det centrala betalningssystemet är beroende av. Riksbanken får i den föreslagna lagen uppgiften att genomföra en årlig risk- och sårbarhetsanalys i syfte att identifiera kriser som kan drabba det centrala betalnings-

systemet. Utredningen konstaterar att viktiga system inom det centrala betalningssystemet är RIX-systemet för stora betalningar, Bankgirocentralens betalningssystem för massbetalningar, Euroclear Swedens VPC-system där transaktioner från aktie- och räntemarknaden clearas och avvecklas samt Nasdaq OMX Derivatives Markets som är central motpart för standardiserade derivatkontrakt. Andra viktiga aktörer inom det centrala betalningssystemet är Riksgäldskontoret samt de fyra storbankerna.

I lagförslagets 10 § uttrycks ett särskilt krav på aktörernas tekniska lösningar och system. Enligt författningskommentaren till förslaget avses t.ex. de it-system som är helt centrala för aktörernas förmåga att fullgöra sina uppgifter i det centrala betalningssystemet. Informationssäkerhet, såväl utformningen av de tekniska lösningarna och systemen som handhavandet av dessa, omfattas av kravet. Enligt författningskommentaren till förslaget innebär det vidare att det finns möjlighet att ställa krav på t.ex. informationssäkerhetsstandard, incidentrapportering, säkerhetsklassning av tjänster och utbildning av personal hos de aktörer som omfattas av lagens bestämmelser. I betänkandet hänvisas till säkerhetsskyddslagens bestämmelser om säkerhetsprövning. Det anges därvid bl.a. att personer som innehar nyckelfunktioner inom det centrala betalningssystemet bör genomgå säkerhetsprövning.

6 Folkrättsliga förpliktelser avseende säkerhetsskydd

Under 1990-talet förändrades svensk försvars- och säkerhetspolitik på ett påtagligt sätt. Kalla krigets slut innebar att Sverige på ett annat sätt än tidigare kunde delta i internationella säkerhetsfrämjande åtgärder och försvarssamarbeten med en bibehållen alliansfrihet. Medlemskapet i Natos partnerskap för fred (PFF) 1994 och medlemskapet i Europeiska Unionen 1995 påverkade naturligtvis detta förhållande. 1995 ställdes också svensk militär trupp för första gången under Nato-ledning. Genom medlemskapen i EU och PFF öppnades det för en ökad samverkan med andra länder på bl.a. försvarsmaterielområdet. EU:s och Natos utvidgning gjorde att utvecklingen blev likartad i många länder i Europa.

Behovet av att i dessa samarbeten utbyta uppgifter som är skyddsvärda från ett nationellt (försvars-)perspektiv medförde krav på att på ett bindande sätt komma överens om ändamålsenliga skyddsåtgärder som garanterar ursprungslandets eller organisationens information när den hanteras av andra länder. Sverige hade sedan tidigare generella säkerhetsskyddsavtal med några länder, men nu accelererade behovet av sådana lösningar. Vidare ökade säkerhetsarbetet inom internationella organisationer vilket ledde till moderniserade säkerhetsföreskrifter för medlemsstaterna.

I det här kapitlet beskrivs Sveriges folkrättsliga förpliktelser dels avseende generella säkerhetsskyddsavtal (avsnitt 6.1), dels i förhållande till EU (avsnitt 6.2). Slutligen redovisas nationella funktioner i det internationella säkerhetsskyddsarbetet (avsnitt 6.3).

6.1 Generella säkerhetsskyddsavtal

Ett stort antal generella säkerhetsskyddsavtal har ingåtts

Sverige har under de senaste årtiondena ingått bilaterala överenskommelser om säkerhetsskydd, s.k. generella säkerhetsskyddsavtal (GSA), med ett trettiotal länder. Även vissa multilaterala säkerhetsskyddsavtal, bl.a. ett avtal mellan de nordiska länderna har ingåtts. Säkerhetsskyddsavtalen med Nato, Västeuropeiska unionen (WEU)[1] och Europeiska rymdbyrån (ESA) liksom avtalet mellan EU:s medlemsländer om skydd för säkerhetsskyddsklassificerade uppgifter[2] kan också sägas vara säkerhetsskyddsavtal, även om dessa till sin konstruktion skiljer sig något från de bilaterala säkerhetsskyddsavtalen. Det äldsta nu gällande bilaterala säkerhetsskyddsavtalet är ett avtal med Tyskland från 1969.

Säkerhetsskyddsavtalen har utvecklats över tiden från att avse enbart försvarshemliga uppgifter i försvarsmaterielsamarbeten till att numera avse hemliga uppgifter i säkerhetsskyddslagstiftningens mening från ett mer övergripande nationellt perspektiv. Fortfarande är det dock så att avtalens tillämpning, åtminstone de bilaterala, till övervägande del berör försvarssektorn och mer explicit internationella försvarsmaterielsamarbeten, internationella militära insatser, försvarsunderrättelseutbyte, internationellt försvarssamarbete och samarbeten inom försvars- och säkerhetsforskningen. Utvecklingen kan dock på sikt medföra en tillämpning av avtalen för andra typer av samarbeten som rör t.ex. internationell terroristbekämpning och internationella rymdfrågor.

Varför behövs ett generellt säkerhetsskyddsavtal?

Det övergripande syftet med ett generellt säkerhetsskyddsavtal är att två eller flera länder (eller mellanfolkliga organisationer) på ett säkert sätt ska kunna utbyta uppgifter som berör nationell säkerhet. Behovet av att utbyta information har sin grund i olika former av samarbeten mellan länderna eller organisationerna. Uppgifterna har vanligtvis ett högt skyddsvärde och ges därför ett skydd enligt

[1] Detta avtal är obsolet eftersom WEU har upphört per den 30 juni 2011.
[2] Avtalet har ännu inte trätt i kraft.

nationell lagstiftning. I Sverige omfattas sådana uppgifter normalt av sekretess och utgör även *hemliga uppgifter* enligt säkerhetsskyddslagstiftningen.

Grunden för att lämna över uppgifter som omfattas av sekretess till utländska myndigheter och mellanfolkliga organisationer finns i 8 kap. 3 § offentlighets- och sekretesslagen (2009:400), OSL. Huvudregeln i bestämmelsen är att en uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen inte får lämnas ut till en utländsk myndighet eller en mellanfolklig organisation. Bestämmelsen innehåller två undantag från denna huvudregel, nämligen dels när det finns en föreskrift om utlämnande i lag eller förordning, dels en möjlighet för en myndighet att under vissa angivna förutsättningar besluta om ett utlämnande av uppgifter.

Ett exempel på en sådan föreskrift som avses i bestämmelsen är förordningen (2010:649) om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet. Enligt den förordningen får Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut i vissa fall delge uppgifter som omfattas av 15 kap. 2 § OSL (försvarssekretess) till en utländsk myndighet som deltar i ett samarbete inom Försvarsdepartementets verksamhetsområde. Detta under förutsättning att samarbetet följer av en internationell överenskommelse som avses i 10 kap. 1 § eller 10 kap. 2 § regeringsformen. Ett krav är att delgivningen enligt den beslutande myndigheten är nödvändig för att genomföra samarbetet. Vidare får uppgifter av synnerlig betydelse för rikets säkerhet inte lämnas ut och inte heller uppgifter som kan ge underlag för att utveckla motmedel mot Sveriges försvarssystem.

Enligt det andra undantaget i 8 kap. 3 § OSL får en uppgift under vissa förutsättningar lämnas till en utländsk myndighet, om uppgiften i motsvarande situation skulle få lämnas till en svensk myndighet. Skälet till denna begränsning är att det inte får förekomma att uppgifter som omfattas av sekretess lämnas till en utländsk myndighet, om en svensk myndighet i motsvarande läge inte skulle kunna ha fått uppgifterna. Ett ytterligare krav är att det dessutom enligt den utlämnande myndigheten står klart att utlämnandet är förenligt med svenska intressen. Vid en sådan prövning får det intresse som sekretessen ska skydda vägas mot andra intressen som t.ex. vikten av ett internationellt samarbete. Prövningen

kan ibland behöva genomföras i samråd med Utrikesdepartementet (10 kap. 8 § regeringsformen).

Bestämmelsen medför i sig inte någon förpliktelse att lämna uppgift utan ger enbart förutsättningar för när en uppgift som omfattas av sekretess *får* lämnas till en utländsk myndighet eller en mellanfolklig organisation.

I författningstexten anges att uppgifterna *lämnas ut*[3] till en utländsk myndighet. Med detta menas inte att uppgifternas offentliggörs på ett sådant sätt som avses i 2 kap. tryckfrihetsförordningen eller i 6 kap. OSL. Tvärtom är tanken att sekretessen ska kvarstå hos mottagaren men med stöd av en nationell lagstiftning som motsvarar offentlighets- och sekretesslagen. Hos den svenska avsändande myndigheten kvarstår sekretessen oförändrad.

Som framgår av beskrivningen finns det i svensk rätt inga krav på att det ska finnas ett bindande generellt säkerhetsskyddsavtal mellan Sverige och ett land eller mellanfolklig organisation som ska erhålla uppgifter som omfattas av sekretess. I bedömningen rörande *svenskt intresse* torde frågan om hur ett mottagande land (eller organisation) avser att skydda uppgifterna vara av betydelse – särskilt om uppgifterna rör rikets säkerhet. Ett sådant intresse kan dock teoretiskt få vika mot andra intressen som t.ex. de samhällsekonomiska fördelar som ett utlämnande kan medföra. Däremot är ett generellt säkerhetsskyddsavtal den enda möjligheten att med bindande verkan reglera att uppgifter som i Sverige omfattas av sekretess och rör rikets säkerhet hanteras på ett säkert sätt av ett annat land eller en mellanfolklig organisation när sådana uppgifter överlämnas.

Problematiken kring begreppet hemlig uppgift

Nuvarande säkerhetsskyddslagstiftning är som tidigare beskrivits uppbyggd kring begreppet *hemlig uppgift* vilket definieras som uppgifter som omfattas av sekretess och dessutom är av betydelse för rikets säkerhet.[4] I internationella sammanhang och vid förhandling av säkerhetsskyddsavtal brukar det engelska begreppet *classified*

[3] Se formuleringen i 3 kap. 8 § 2 st. OSL och i 1 § förordningen (2010:649) om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet.
[4] 4 § 1 säkerhetsskyddsförordningen, se vidare kapitel 3.

information användas i en generisk betydelse som refererar till ländernas nationella lagstiftning på området och dess motsvarande begrepp.

I Sverige motsvaras begreppet närmast av begreppet hemlig uppgift, men genom detta begrepps konstruktion begränsas tillämpningen till att avse enbart sådana uppgifter som rör rikets, dvs. Sveriges, säkerhet. Då syftet med säkerhetsskyddsavtalen är att ge ett skydd för även ett annat lands skyddsvärda uppgifter (som inte med nödvändighet rör Sveriges säkerhet) innebär det att nuvarande säkerhetsskyddslagstiftning inte på ett tillfredsställande sätt medger ett säkerhetsskydd för utländska uppgifter i Sverige. Begreppet hemlig uppgift är således alltför snävt för att vara ändamålsenligt i denna typ av avtal. I andra länder innefattar vanligen den nationella motsvarigheten till hemliga uppgifter även sådana uppgifter som landet har erhållit från ett annat land eller en mellanfolklig organisation och som omfattas av ett för landet folkrättsligt åtagande.[5] Svårigheten att tillämpa begreppet *classified information* i svensk rätt illustreras av att det i de gällande säkerhetsskyddsavtalen i sin svenska lydelse översatts som omväxlande hemlig, sekretessbelagd, klassificerad och säkerhetsskyddsklassificerad uppgift.

Problematiken kring säkerhetsskyddsavtal och principen om upphovslandets medgivande

Säkerhetsskyddsavtalens konstruktion innebär i regel att två eller flera parter ömsesidigt åtar sig att skydda uppgifter som utbyts mellan parterna. Med parter avses i dessa sammanhang stater eller mellanfolkliga organisationer. Skyddet ansluter i stor grad till säkerhetsskyddslagstiftningens säkerhetsskyddsåtgärder, vilket även överensstämmer med de flesta länders säkerhetsskyddsreglering. Säkerhetsskyddsavtalen medför i sig ingen skyldighet att lämna ut hemliga uppgifter till den andra parten.

Avtalen innehåller emellertid ofta begränsningar av hur information som erhållits från ett land får användas av det mottagande landet. En vanligt förekommande princip är att det behövs ett skriftligt medgivande för att uppgifter ska få lämnas

[5] Se bl.a. 11 § i den norska sikkerhetsloven (1998-03-20 nr. 10) och 2 § 2 i den finska lagen om internationella förpliktelser om informationssäkerhet (24.6.2004/588).

vidare, offentliggöras eller omklassificeras. Principen brukar på engelska benämnas *originator control.* Att denna princip, som snarast är att betrakta som en sekretessförbindelse, förekommer i avtal om säkerhetsskydd kan delvis förklaras med att den avgränsning mellan sekretess och säkerhetsskydd som finns i svensk rätt sällan är lika tydlig i andra länders rättssystem. Även i Sverige är dock sekretessen en förutsättning för säkerhetsskydd, vilket även för svensk del motiverar förekomsten av sådana bestämmelser i avtalen.

Avtalsvillkor om *originator control* kan medföra vissa komplikationer. Bestämmelser om sekretess utgör undantag från offentlighetsprincipen, och offentlighets- och sekretesslagstiftningen reglerar uttömmande under vilka förutsättningar uppgifter – oavsett om de omfattas av ett säkerhetsskyddsavtal eller inte – omfattas av sekretess. Andra bestämmelser än sådana som har stöd i denna lagstiftning är således oförenliga med svensk rätt. Sådana avtalsvillkor är dock inte ovanliga i olika slag av internationella avtal som Sverige ingår.

Enligt en relativt ny bestämmelse[6] i 15 kap. 1 a § OSL gäller sekretess för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation. Sekretessen gäller, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. Detta innebär ett visst stöd för att uppfylla förpliktelser om sekretess i internationella överenskommelser under förutsättning att bestämmelsens villkor är uppfyllda.

Problematiken kring avtalsvillkor om sekretess är dock främst teoretisk när det gäller säkerhetsskyddsöverenskommelser. Bestämmelsen om utrikessekretess i 15 kap. 1 § OSL torde i stort sett i samtliga fall vara tillämplig på det slag av uppgifter som överenskommelserna avser, eftersom ett otillåtet röjande av uppgifterna från svensk sida i strid med en folkrättslig förpliktelse måste kunna antas störa Sveriges förbindelser med landet i fråga. Att uppgifterna dessutom är skyddsvärda utifrån landets nationella säkerhet ger ytterligare stöd för en sådan tolkning.

[6] Prop. 2012/13:192 Sekretess i det internationella samarbetet.

I moderna säkerhetsskyddsavtal har man från svensk sida med viss framgång lyckats undvika skrivningar om upphovslandets samtycke genom att i stället använda formuleringar om en skyldighet att vidta alla rättsliga åtgärder för att förhindra ett utlämnande. I andra fall har man i förhandlingarna lyckats få med en formulering om konsultation i stället för samtycke. I åtminstone två kända fall[7] har det från svensk sida ansetts nödvändigt att göra en unilateral deklaration där principen om upprättande parts samtycke beskrivs utifrån ett svenskt rättsläge.

I praktiken bör de olika lösningarna inte innebära någon större skillnad eftersom parterna och då även Sverige med stöd av avtalet förväntar sig ett fullgott skydd för de uppgifter som lämnas ut till det andra landet. Som beskrivits ovan bör utrikessekretessen väl tillgodose detta krav.

Svårigheten att tillämpa nuvarande säkerhetsskyddslagstiftning på uppgifterna är därför ett större problem än sekretessfrågan. I den utsträckning som uppgifter som omfattas av avtalen är av betydelse även för rikets säkerhet omfattas informationen av säkerhetsskyddslagen. I praktiken har så ofta varit fallet men motsatsen skulle även kunna inträffa.

Innehållet i säkerhetsskyddsavtal

Som tidigare nämnts så är syftet med säkerhetsskyddsavtalen att parterna ömsesidigt ska ge ett skydd för varandras skyddsvärda information. Detta innebär att avtalsvillkoren i huvudsak berör hur sådan information ska hanteras i olika situationer. Centralt i avtalen är en jämförelsetabell i vilken parternas märkning av den skyddsvärda informationen förtecknas och jämförs.

Vidare finns det bestämmelser som reglerar behörigheten till informationen vilket motsvarar behörighetskraven i 7 § säkerhetsskyddsförordningen. Som tidigare nämnts är det även vanligt med begränsningar i användandet av informationen i form av en sekretessförpliktelse. Utöver dessa centrala delar finns normalt bestämmelser om industrisäkerhet, rutiner vid besök samt vilka åtgärder som ska vidtas när uppgifter från den andra parten

[7] Se säkerhetsskyddsavtalen med WEU (SÖ 2004:59) och ESA (SÖ 2004:60).

kan ha röjts för obehöriga. Slutligen är det vanligt med en upplysningsbestämmelse om vilka myndigheter hos parterna som är behöriga att hantera frågor som rör tillämpningen av avtalet.

Det beskrivna avtalsinnehållet gäller för moderna bilaterala säkerhetsskyddsavtal. Äldre avtal har ibland en annan systematik. Detsamma gäller för avtal med mellanfolkliga organisationer som t.ex. Sveriges säkerhetsskyddsavtal med Nato, WEU och ESA. De sistnämnda saknar t.ex. en jämförelsetabell över parternas märkning av skyddsvärda uppgifter och är också mer kortfattade än de bilaterala avtalen.

Genomförande av säkerhetsskyddsavtal i svensk rätt

Säkerhetsskyddsavtal ingås av regeringen och träder för svensk del i regel i kraft vid undertecknandet. Avtalet är en traktat i Wienkonventionens[8] mening och är därför folkrättsligt bindande för Sverige. Avtalen får tolkas utifrån gällande rätt. I övrigt ansvarar regeringen för att nödvändiga åtgärder för avtalets genomförande och implementering.

6.2 Reglering inom EU avseende säkerhetsskydd

2001 års säkerhetsbestämmelser för rådet respektive kommissionen

Under 2001 beslutades säkerhetsbestämmelser för rådet respektive kommissionen. Bland EU:s medlemsstater fanns det dock delade meningar om dessa säkerhetsbestämmelser kunde anses vara förpliktande för medlemsstaterna. Problemet låg i författningarnas rättsgrund. Rådets säkerhetsbestämmelser antogs med stöd av artikel 207.3 i fördraget om upprättandet av europeiska gemenskapen,[9] enligt vilken rådet i sin arbetsordning ska utarbeta villkoren för allmänhetens tillgång till rådets handlingar. Dessa säkerhetsbestämmelser gällde enligt artikel 2.2 i bestämmelserna enbart för rådet och de decentraliserade EU-myndigheterna och omfattade därför inte alla EU-byråer och organ. I säkerhets-

[8] Wienkonventionen om traktaträtten, SÖ 1975:1.
[9] Numera fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

bestämmelserna ingick det emellertid också bestämmelser som var riktade mot medlemsstaterna. En del medlemsstater, bl.a. Finland, genomförde bestämmelserna i nationell lagstiftning, medan andra medlemsstater som t.ex. Sverige ansåg att bestämmelserna som avsåg medlemsstaterna snarast var vägledande.

Nya bestämmelser och ett mellanstatligt säkerhetsskyddsavtal tas fram

Coreper godkände 2007 ett mandat (dok. 14762/07) enligt vilket Europeiska unionen bör bereda en enhetlig och heltäckande allmän ram för skydd av säkerhetsskyddsklassificerade uppgifter inom EU. Strävan var att förenkla och uppdatera bestämmelserna om säkerhetsskyddsklassificerade uppgifter mot bakgrund av god internationell praxis. Utifrån mandatet började rådets säkerhetskommitté (*Council Security Committee*, *CSC*) se över säkerhetsbestämmelserna och kom fram till att genom rådets säkerhetsbestämmelser rådets institutioner, men inte medlemsstaterna, kan förpliktas att skydda säkerhetsskyddsklassificerade EU-uppgifter. Det var därför nödvändigt med andra åtgärder utöver säkerhetsbestämmelserna för att skyddet av säkerhetsskyddsklassificerade EU-uppgifter skulle vara heltäckande. Vidare fanns det en vilja att förbättra skyddet i medlemsstaterna av säkerhetsskyddsklassificerade uppgifter som EU erhållit från internationella organisationer och tredjeländer. Som ett nytt element ville man upprätta ett system för att skydda nationella säkerhetsskyddsklassificerade uppgifter som utbyts medlemsstater emellan i EU:s intresse. För att uppfylla dessa målsättningar föreslog Frankrike att ett avtal skulle ingås mellan EU:s medlemsstater, församlade i rådet, om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i *Europeiska unionens intresse*. Starten för detta arbete skedde i februari 2008 i Stockholm genom att Utrikesdepartementet bjöd in representanter från medlemsstaterna att delta i en diskussion om möjliga lösningar.

Begreppet *Europeiska unionens intresse* definieras inte. I praktiken kommer därför medlemsstaterna att själva avgöra i vilka fall som de utbyter nationellt säkerhetsskyddsklassificerade uppgifter inom ramen för avtalet.

Rådets nya säkerhetsbestämmelser

Med rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter fastställs grundläggande principer och miniminormer för säkerhet för att skydda säkerhetsskyddsklassificerade EU-uppgifter. Dessa grundläggande principer och miniminormer ska gälla för rådet och rådets generalsekretariat och iakttas av medlemsstaterna i enlighet med deras nationella lagar och andra författningar. I praktiken möjliggör detta att nationell lagstiftning tillämpas, förutsatt att miniminormerna för rådets säkerhetsbestämmelser iakttas. Rådets nya säkerhetsbestämmelser syftar till att göra bestämmelserna enklare och användarvänligare samt till att eliminera otydligheter i de äldre bestämmelserna. Avsikten är att hanteringen av säkerhetsrisker samtidigt ska bli bättre.

Beslutet om rådets nya säkerhetsbestämmelser omfattar 18 artiklar, sex bilagor och fyra tillägg. Beslutet innehåller bl.a. bestämmelser om tillämpningsområde, definitioner och säkerhetsskyddsklassificering, regler för säkerhetsskyddsklassificeringen, personalsäkerhet, fysisk säkerhet, administrativ säkerhet, informationssystemssäkerhet, och industrisäkerhet. Vidare finns det bestämmelser om utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater och internationella organisationer samt om överträdelse av säkerhetsbestämmelserna.

Bilagorna rör personalsäkerhet, fysisk säkerhet, hantering av säkerhetsskyddsklassificerade uppgifter, skydd av säkerhetsskyddsklassificerade EU-uppgifter som hanteras i kommunikations- och informationssystem, industrisäkerhet och utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater och internationella organisationer. Tilläggen innehåller definitioner, en jämförelsetabell över medlemsstaternas informationssäkerhetsklassificering, en förteckning över nationella säkerhetsmyndigheter samt en förteckning över förkortningar.

Det multilaterala säkerhetsskyddsavtalets syfte

Syftet med avtalet mellan Europeiska unionens medlemsstater om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse är att ålägga medlemsstaterna att följa

rådets säkerhetsbestämmelser. Avtalet förutsätter att parterna vidtar alla lämpliga åtgärder i enlighet med sina respektive nationella lagar och andra författningar för att säkerställa att den säkerhetsnivå som ges säkerhetsskyddsklassificerade uppgifter når upp till minst kraven i Rådets säkerhetsbestämmelser. Därmed är det avtalets målsättning att skyddet av säkerhetsskyddsklassificerade EU-uppgifter och uppgifter som EU har mottagit från tredjeländer på detta sätt ska bli bättre i medlemsstaterna.

En vidare målsättning är att upprätta ett system för skydd av nationella säkerhetsskyddsklassificerade uppgifter som utbyts i EU:s intresse när medlemsstaterna inte sinsemellan har ingått bilaterala informationssäkerhetsavtal. Ambitionen är att avtalet ska utgöra en enhetlig reglering av säkerhetsskyddsklassificerade EU-uppgifter inom EU.

Innehållet i det multilaterala säkerhetsskyddsavtalet

Enligt artikel 3.1 i avtalet ska parterna vidta alla lämpliga åtgärder i enlighet med sina respektive lagar och andra författningar för att säkerställa att den säkerhetsnivå som ges säkerhetsklassificerade uppgifter som omfattas av avtalet är likvärdig med den som ges enligt rådets säkerhetsbestämmelser. I fråga om principen om upphovsmannens medgivande anges dock i artikel 3.2 att ingenting i avtalet ska påverka parternas nationella lagar och andra författningar när det gäller allmänhetens tillgång till handlingar, skyddet för personuppgifter eller skyddet av säkerhetsskyddsklassificerade uppgifter (se avsnitt 6.1). Denna skrivning kom till som en kompromiss efter krav från främst Storbritannien och Sverige utifrån nationella krav på offentlighet.

I artikel 5 i avtalet finns bestämmelser om säkerhetsklarering. Bland annat föreskrivs att endast personer som genomgått lämplig säkerhetsklarering eller som på annat sätt i kraft av sina arbetsuppgifter vederbörligen bemyndigats i enlighet med nationell lagstiftning får ges tillgång till säkerhetsskyddsklassificerade uppgifter på nivån EU CONFIDENTIAL eller högre. I avtalet finns också bestämmelser t.ex. om ändring av säkerhetsskyddsklassificeringsnivåer.

Inom ramen för avtalet får medlemsstaterna erkänna andra medlemsstaters säkerhetsprövning av personal och säkerhetskontroll av anläggningar. Ett sådant förfarande är avsett att underlätta för företag i medlemsstaterna att delta i säkerhetsskyddsklassificerade projekt i andra EU-länder. Medlemsstaterna kan på begäran och i enlighet med nationell lagstiftning bistå varandra vid säkerhetsutredningar i samband med säkerhetsgodkännande.

Avtalet träder i kraft när samtliga medlemsstater slutfört de interna förfaranden som är nödvändiga för att avtalet ska kunna träda i kraft.

6.3 Nationella funktioner i det internationella säkerhetsskyddsarbetet

Något om termerna

I huvudelen av Sveriges internationella säkerhetsskyddsåtaganden finns krav på en samverkansfunktion som vanligtvis benämns *National Security Authority* (NSA[10]). Ursprunget till denna funktion torde ha varit relativt tidiga säkerhetsbestämmelser i Nato som föreskrev att varje medlemsland skulle utpeka en myndighet som hade ett nationellt ansvar för säkerhetsskyddsfrågor och som dessutom skulle vara kontaktorganisation i internationella säkerhetsskyddsärenden inom Nato. Modellen började därefter även användas bilateralt mellan Natos medlemsländer som begrepp för den eller de myndigheter som parterna i generella säkerhetsskyddsavtal (GSA) utpekar som kontaktorganisationer. Även begreppet *Designated Security Authority* (DSA) har sitt ursprung i Nato och det används för att beskriva den nationella myndighet som i ett land har det praktiska säkerhetsansvaret med fokus på industrisäkerhetsfrågor i internationella säkerhetskänsliga materielprojekt.

Utöver dessa roller, som får anses vara de mest centrala funktionerna, har ytterligare specialiserade roller växt fram. En sådan roll är *National Communication Security Authority*[11] (NCSA) som rör internationella krypto- och signalskyddsfrågor samt de därtill

[10] Akronymen NSA används även av den amerikanska signalspaningsmyndigheten *National Security Agency*. Den har inga likheter med NSA-funktionen i detta sammanhang.
[11] Inom EU används i stället begreppet *Crypto Approval Authority, CAA*.

hörande funktionerna *Key Production Authority* (KPA) och *National Distribution Authority* (NDA), vilka är kopplade till produktion och distribution av signalskyddsnycklar. *Information Assurance Authority* (IAA) är en funktion som representerar ett land från ett it-säkerhetsperspektiv, särskilt i frågor som rör ackreditering och säkerhetsgodkännanden kring internationella säkerhetskänsliga informationssystem. *Tempest Authority* (TA), slutligen, hanterar frågor om krav på skydd mot röjande signaler (RÖS).

Eftersom många medlemsstater i Nato även är EU-medlemmar blev det naturligt att huvuddelen av begreppen kom att användas i EU:s säkerhetsarbete där arbetet leds av medlemsstaternas NSA-funktioner tillsammans med säkerhetskontoret i generalsekretariatet i Europeiska unionens råd. Begreppen har även inarbetats i många länders lagstiftning. Ofta är huvuddelen eller samtliga av rollerna kopplade till samma organisation.

Nuvarande ordning

Enligt EU:s och Natos säkerhetsbestämmelser[12] är en NSA en myndighet (eller myndighetsfunktion) som har ett nationellt ansvar för skyddet av säkerhetsskyddsklassificerade uppgifter och att bedöma hoten mot dessa uppgifter, att utfärda bestämmelser om skyddet av informationen samt att utföra tillsyn över myndigheter som hanterar sådan information. Myndigheten ska vidare utgöra ett rådgivande organ till myndigheter som hanterar den säkerhetsskyddsklassificerade informationen och samordna nationella register för att kunna redovisa en spårbarhet när det gäller hantering av informationen. I arbetsuppgifterna ingår även att delta i internationella arbetsgrupper på säkerhetsskyddsområdet och att representera säkerhetsskyddsfunktionen i internationell samverkan. De flesta länderna i Nato och EU har lagt denna uppgift på militära eller civila säkerhetstjänster eller ibland skapat särskilda säkerhetsskyddsmyndigheter med NSA-rollen som utgångspunkt.

[12] Rådets beslut av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2013/488/EU) samt Security within the North Atlantic Treaty Organisation (Nato), C-M(2002)49.

I Sverige ansvarar Utrikesdepartementet för NSA-funktionen gentemot EU och Nato samt även gentemot WEU som dock torde vara obsolet i dag. När det gäller NSA-rollen i förhållande till ESA så innehar Utrikesdepartementet även denna roll utan att detta har formaliserats i författningstext. I ett regeringsbeslut[13] från 2003 uppdrog regeringen åt ett antal myndigheter, bl.a. Försvarsmakten och Säkerhetspolisen, att ställa expertis till förfogande för det arbete som NSA-funktionen vid Regeringskansliet (Utrikesdepartementet) ska utföra.

För bilateral samverkan är Försvarsmakten utpekad som NSA-funktion. Denna roll grundar sig inte på någon författningsreglering utan följer av bestämmelser i de generella säkerhetsskyddsavtal som Sverige har ingått med ett trettiotal länder. I en skrivelse från Utrikesdepartementet till Europeiska unionens råd 2007 meddelades att säkerhetskontoret vid den militära underrättelse- och säkerhetstjänsten har rollerna som NCSA och NDA i Sverige.[14]

Det finns bestämmelser i nuvarande säkerhetsskyddslagstiftning som behandlar internationella relationer, bl.a. när det gäller - Säkerhetspolisens uppgift att svara på begäran om registerkontroll från andra länder. Detta är en typisk NSA-uppgift internationellt sett. Vidare är Försvarets materielverks möjlighet att genomföra säkerhetsskyddad upphandling med säkerhetsskyddsavtal med företag för som ska delta i internationella säkerhetskänsliga projekt som rör utveckling eller produktion av försvarsmateriel, en typisk DSA-uppgift.[15] Försvarsmakten och Säkerhetspolisen har bemyndigats att meddela föreskrifter och att utöva tillsyn vilket är uppgifter som normalt hör till en NSA-funktion.

Regeringskansliets NSA-roll är reglerad i förordningen (1996:1515) med instruktion för Regeringskansliet. Enligt den ska Regeringskansliet vara den nationella säkerhetsmyndighet som ansvarar för att upprätthålla säkerheten för sekretessbelagda uppgifter enligt Europeiska rådets säkerhetsföreskrifter samt enligt Sveriges åtaganden om detta i överenskommelser med Västeuro-

[13] Uppdrag att biträda den nationella säkerhetsmyndigheten (NSA), UD2003/126/SSSB, 2003-03-06.
[14] Response from Sweden concerning identification of NDA and NCSA, Utrikesdepartementet 2007-05-11, A19E.
[15] 17 § säkerhetsskyddsförordningen.

peiska unionen och Nato inom ramen för samarbetet Partnerskap för fred.[16] Enligt Regeringskansliets arbetsordning ska chefen för Utrikesdepartementet besluta i dessa ärenden.[17] Det framgår dock inte närmare i dessa bestämmelser hur uppgiften ska lösas.

Försvarsmakten bemyndigas regelbundet i regeringsbeslut att förhandla generella säkerhetsskyddsavtal med andra länder. Det anges inte uttryckligen att Försvarsmakten gör detta i sin NSA-roll, men uppgiften tillkommer NSA-funktioner i andra länder, och motparten i avtalsförhandlingarna har uteslutande varit respektive lands NSA. Efter avrapportering beslutar regeringen att avtalen ska ingås. I avtalen regleras hur samverkan ska genomföras mellan parternas NSA-funktioner och vilka ärenden som dessa funktioner ska hantera.

Vid minst ett tillfälle har frågan om vilka myndigheter som skulle vara NSA och DSA varit föremål för diskussion. Det gällde förhandlingen om ett säkerhetsskyddsavtal med USA med anledning av ett säkerhetsforskningssamarbete mellan Sverige och USA. I det fallet utfärdade Försvarsdepartementet en instruktion att Försvarsmakten skulle vara nationell säkerhetsmyndighet och Försvarets materielverk verkställande säkerhetsmyndighet i det aktuella fallet.[18]

Internationell utblick[19]

Som tidigare beskrivits är NSA-rollen i många länder kopplad till nationella säkerhetstjänster eller civila eller militära underrättelse- och säkerhetstjänster. Så är fallet i t.ex. Nederländerna, Polen, Spanien och Tyskland. Andra länder som t.ex. Frankrike, Italien och Storbritannien har inrättat en särskild säkerhetsmyndighet under premiärministerns kansli. Ytterligare en grupp länder har inrättat en särskild säkerhetsskyddsmyndighet med Natos och EU:s bestämmelser som grund. Till dessa länder hör Bulgarien, Norge, Slovakien, Slovenien, Tjeckien och Ungern.

---

[16] 20 § 8 förordningen (1996:1515) med instruktion för Regeringskansliet.
[17] 5 § 8 Regeringskansliets föreskrifter om ändring i Regeringskansliets föreskrifter med arbetsordning för Regeringskansliet (RKF 2014:2).
[18] Utpekande av NSA och DSA inom säkerhetsforskningsavtal med USA, Fö2007/2637/MIL, 2007-11-15.
[19] En mer omfattande internationell utblick finns i kapitel 8.

I Danmark är funktionen delad mellan *Forsvarets Efterrettningstjenste* (FE) och på Politiets Efterrettningstjenste (PET). FE har även rollen som SAA och NCSA. Danmark deltar inte i verksamhet som rör EU:s försvarspolitik. Genom att den största delen av EU:s säkerhetsskyddsklassificerade information hanteras inom den gemensamma säkerhets- och försvarspolitiken är FE:s roll när det gäller säkerhetsarbetet inom EU ytterst begränsad. FE fokuserar därför främst på säkerhetssamarbetet inom Nato och bilateralt.

I Finland är Utrikesministeriet utpekad som NSA. Rollen gäller såväl NSA-funktionen bilateralt som gentemot mellanfolkliga organisationer. NSA-funktionen lyder under statssekreteraren och består av ett kansli. En stor del av arbetet samordnas med stöd från Skyddspolisen, Huvudstabens utredningsavdelning och Försvarsministeriet vilka även aktivt deltar i NSA-arbetet. Dessa är formellt utpekade som DSA. Finland är det enda landet som inte använder begreppet DSA för en myndighet som utpekats särskilt för industrisäkerhetsfrågor. Vidare är Kommunikationsverket utpekat som NCSA.

I Norge är *Nasjonal Sikkerhetsmyndighet* utpekad som NSA och fungerar även som DSA, NCSA och SAA. Myndigheten har såväl ett nationellt som ett internationellt ansvar för säkerhetsskyddsfrågor.

7 Myndigheter med uppgifter enligt säkerhetsskyddslagstiftningen

Vissa myndigheter har särskilda uppgifter i fråga om säkerhetsskydd. Det gäller framför allt Säkerhetspolisen och Försvarsmakten som har det huvudsakliga ansvaret för att utföra tillsyn och meddela tillämpningsföreskrifter (se avsnitt 7.1.1 och 7.1.2).

Vidare fyller Säkerhets- och integritetsskyddsnämnden en viktig funktion för skyddet av enskildas integritet vid säkerhetsprövning (se avsnitt 7.1.3).

Försvarets materielverk har vissa uppgifter i fråga om säkerhetsskyddsavtal som syftar till att underlätta för leverantörer som ska delta i ett internationellt samarbete på försvarsmaterielområdet (se avsnitt 7.1.4).[1]

Några myndigheter har ett sektorsbestämt ansvar för att i fråga om säkerhetskänslig verksamhet hos vissa bolag, föreningar och stiftelser och enskilda verksamhetsutövare besluta om placering i säkerhetsklasser och registerkontroll och för att kontrollera säkerhetsskyddet (se avsnitt 7.2).

Därutöver finns ett antal myndigheterna och samarbetsorgan som inte har något i säkerhetsskyddslagstiftningen utpekat ansvar men som har uppgifter och verksamhet som det i sammanhanget ändå finns anledning att redovisa (se avsnitt 7.3 och 7.4).

[1] I fråga uppgifter till följd av internationella säkerhetsskyddsåtaganden se även redovisningen i kapitel 6.

7.1 Myndigheter med särskilt ansvar

7.1.1 Säkerhetspolisen

Den 1 januari 2015 blev Säkerhetspolisen en egen myndighet från att tidigare ha varit en del av Rikspolisstyrelsen. Säkerhetspolisen har till uppgift att skydda Sveriges demokratiska system, medborgarnas fri- och rättigheter och den nationella säkerheten. Säkerhetspolisens verksamhet kan i huvudsak delas in i fem områden (kontraspionage, kontraterrorism, författningsskydd, säkerhetsskydd och personskydd).

Säkerhetspolisen ansvarar enligt 3 § förordningen (2014:1103) med instruktion för Säkerhetspolisen för att förebygga, förhindra och upptäcka brottslig verksamhet samt utreda och beivra bl.a. brott mot rikets säkerhet och brott mot lagen (2003:148) om straff för terroristbrott. Säkerhetspolisen ansvarar också för personskyddet av den centrala statsledningen. Säkerhetspolisen får, utöver vad som följer av 47 § säkerhetsskyddsförordningen, ge råd om säkerhetsskydd. Säkerhetspolisen får även i övrigt ge råd för att förebygga brott mot rikets säkerhet eller andra särskilt viktiga samhällsintressen. Säkerhetspolisen får även efter medgivande av regeringen i särskilda fall bedriva uppdragsverksamhet när det gäller säkerhetsskydd och annat säkerhetsarbete.

Säkerhetspolisen ska vidare enligt 18 § i sin instruktion tillhandahålla Registerkontrolldelegationen vid Säkerhets- och Integritetsskyddsnämnden sammanträdes- och kontorslokaler, kanslistöd och föredragande.

Av säkerhetsskyddsförordningen framgår att Säkerhetspolisen har flera olika funktioner när det gäller säkerhetsskyddet. Om en hemlig uppgift kan ha röjts, ska det skyndsamt anmälas till Säkerhetspolisen, om röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa (10 §). Vidare ska en myndighet som avser att inrätta ett register som ska föras med hjälp av automatisk databehandling innehållande uppgifter av betydelse för rikets säkerhet i vissa fall samråda med Säkerhetspolisen (12 §). Säkerhetspolisen ska också besluta om registerkontroll när en framställan om det har gjorts från en annan stat eller en mellanfolklig organisation (22 §).

Säkerhetspolisen beslutar vidare om registerkontroll av person till skydd mot terrorism såvitt avser verksamhet vid statschefens och tronföljarens residens och bostäder samt statsministerns bostäder och statens egendom Harpsund (26 § och 27 § 2). I det sammanhanget kan även nämnas att Säkerhetspolisen har vissa uppgifter enligt lagen (2014:514) om ansvar för vissa säkerhetsfrågor vid statsministerns tjänstebostäder. Ytterligare uppgifter enligt säkerhetsskyddsförordningen följer av att regeringen kan överlåta åt Säkerhetspolisen att besluta om registerkontroll vid större evenemang, statsbesök eller andra liknande händelser som särskilt behöver skyddas mot terrorism (26 a §).

Vidare ska den som har beslutat om registerkontroll göra en framställan om utlämnande av uppgifter hos Säkerhetspolisen som bereder ärendet inför beslut av Säkerhets- och integritetsskyddsnämnden (29 §). Det innefattar också att Säkerhetspolisen ska göra en särskild personutredning i de fall en anställning eller annat deltagande i verksamhet har placerats i säkerhetsklass 1 eller 2 och när framställan om registerkontroll har gjorts av en annan stat eller mellanfolklig organisation (34 §). Säkerhetspolisen ska också när det gäller placeringar i säkerhetsklass 1 hålla ett personligt samtal med den som säkerhetsprövningen gäller och till Säkerhets- och integritetsskyddsnämnden därefter redovisa de uppgifter som kommit fram (36 och 37 §§).

Säkerhetspolisen kontrollerar säkerhetsskyddet vid myndigheter utom de myndigheter som hör till Försvarsdepartementet och Fortifikationsverket, Försvarshögskolan samt Justitiekanslern (39 §).[2] Säkerhetspolisen kan även utföra kontroll av säkerhetsskyddet hos sådana bolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande samt enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism, eller enskilda som omfattas av ett säkerhetsskyddsavtal. Kontrollen ska i dessa fall utföras i samråd med de myndigheter som enligt 31 § säkerhetsskyddslagen eller 40 eller 41 § säkerhetsskyddsförordningen primärt ska kontrollera säkerhetsskyddet i dessa fall (42 §).

[2] 39 § säkerhetsskyddsförordningen återspeglar ännu inte den ändring i förordningen (1996:1515) med instruktion för Regeringskansliet som gäller från den 1 januari 2015 och som innebär att Myndigheten för samhällsskydd och beredskap och Statens haverikommission numera hör till Justitiedepartementet.

Säkerhetspolisen får meddela närmare föreskrifter om verkställigheten av säkerhetsskyddslagen i fråga om förfarandet vid registerkontroll samt meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (43 och 44 §§). Säkerhetspolisen ska på begäran lämna råd om säkerhetsskydd till Regeringskansliet, riksdagen och dess myndigheter samt Justitiekanslern (47 §).

Rikspolisstyrelsen har beslutat föreskrifter och allmänna råd om säkerhetsskydd (RPSFS 2010:03). Denna föreskriftsrätt ankommer sedan den 1 januari 2015 på Säkerhetspolisen.

7.1.2 Försvarsmakten

Försvarsmakten är en statlig myndighet med ansvar för att upprätthålla och utveckla ett militärt försvar. Försvarsmakten ska enligt 2 § förordningen (2007:1266) med instruktion för Försvarsmakten kunna försvara Sverige och främja svensk säkerhet genom insatser nationellt och internationellt. Vidare ska Försvarsmakten kunna upptäcka och avvisa kränkningar av det svenska territoriet samt värna Sveriges suveräna rättigheter och nationella intressen utanför det svenska territoriet. Försvarsmakten ska kunna lämna stöd till civil verksamhet. Enligt 3 b § förordningen med instruktion för Försvarsmakten ska Försvarsmakten bl.a. särskilt bedriva verksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet, leda och bedriva militär säkerhetstjänst samt leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information.

Liksom när det gäller Säkerhetspolisen har Försvarsmakten enligt säkerhetsskyddsförordningen flera olika funktioner när det gäller säkerhetsskyddet. Som exempel kan nämnas att en myndighet som avser att inrätta ett register som ska föras med hjälp av automatisk databehandling innehållande uppgifter av betydelse för rikets säkerhet i vissa fall ska samråda med Försvarsmakten (12 §). Enligt 26 § och 27 § 4 säkerhetsskyddsförordningen beslutar Försvarsmakten om registerkontroll till skydd mot terrorism för sådana skyddsobjekt som avses i 5 § 1 skyddslagen (2010:305) och som huvudsakligen disponeras av Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt för militära fartyg och luft-

fartyg som avses i nämnda bestämmelse i skyddslagen och för sådana skyddsobjekt som avses i 5 § 4 skyddslagen.

Av 39 § säkerhetsskyddsförordningen framgår att Försvarsmakten ska kontrollera säkerhetsskyddet när det gäller Fortifikationsverket och Försvarshögskolan samt de myndigheter som hör till Försvarsdepartementet utom Statens haverikommission.[3]

Av 42 § säkerhetsskyddsförordningen framgår vidare att Försvarsmakten kan kontrollera säkerhetsskyddet hos sådana bolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande samt enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism, eller enskilda som omfattas av ett säkerhetsskyddsavtal. Kontrollen ska i dessa fall utföras i samråd med de myndigheter som enligt 31 § säkerhetsskyddslagen eller 40 eller 41 § säkerhetsskyddsförordningen primärt ska kontrollera säkerhetsskyddet i dessa fall.

Enligt 44 § säkerhetsskyddsförordningen får Försvarsmakten meddela närmare föreskrifter om verkställigheten av säkerhetsskyddslagen för sitt tillsynsområde. Försvarsmakten har beslutat föreskrifter om säkerhetsskydd (FFS 2003:7). Huvudelen av Försvarsmaktens uppgifter enligt säkerhetsskyddsförordningen hanteras av den militära underrättelse- och säkerhetstjänsten (MUST).

MUST är en del av myndigheten Försvarsmakten. MUST har dock en särställning på ett sådant sätt att dess uppdragsgivare är såväl regeringen och Regeringskansliet (Försvarsdepartementet) som Försvarsmakten. Chefen för MUST rapporterar därför även direkt till regeringen i vissa ärenden.

Den militära säkerhetstjänstens uppgift är att tillvarata de säkerhetsintressen som främst berör Försvarsmakten och dess tillsynsområde enligt säkerhetsskyddslagstiftningen samt att samverka rörande skyddet av rikets säkerhet och skydd mot terrorism med Säkerhetspolisen. Den militära säkerhetstjänsten består av säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst, där signalskyddstjänsten är att anse som en säkerhetsskyddsangelägenhet.

[3] Avseende utformningen av 39 §, se not 1.

Säkerhetsunderrättelsetjänstens uppgift är att klarlägga, förhindra och försvåra den säkerhetshotande verksamhetens mål, medel och metoder. Säkerhetsskyddstjänsten inklusive signalskyddstjänsten syftar till att förhindra eller motverka den säkerhetshotande verksamheten mot Sverige eller mot insatta förband och insatser i andra länder.

Chefen för MUST ska även leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information samt förhandla internationella säkerhetsskyddsavtal. Vid MUST finns Försvarsmaktens nationella säkerhetsmyndighetsfunktion (NSA) och den nationella kryptogodkännandefunktionen (CAA/NCSA). Dessa funktioner har beskrivits i avsnitt 6.3.

7.1.3 Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden är en statlig myndighet som har tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter. Nämnden har också tillsyn över polisens behandling av personuppgifter. Nämnden ska bidra till att värna rättssäkerheten och skyddet för den personliga integriteten i de verksamheter som nämnden har tillsyn över. Myndigheten leds av en nämnd.

Vid sidan av nämnden finns det två andra beslutsorgan inom myndigheten. Det ena beslutar i frågor om utlämnande av uppgifter från olika register vid registerkontroll enligt säkerhetsskyddslagen (Registerkontrolldelegationen) och det andra beslutar i ärenden om kvalificerade skyddsidentiteter (Skyddsregistreringsdelegationen).

Kanslistödet för Registerkontrolldelegationen tillhandahålls av Säkerhetspolisen med stöd av 4 § förordningen med instruktion för Säkerhetspolisen.

Registerkontrolldelegationens uppgift att pröva frågor om utlämnande av uppgifter från vissa register till myndigheter som begärt kontroll framgår av 21 och 23 §§ säkerhetsskyddslagen, 29–32 §§ säkerhetsskyddsförordningen samt av förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

När uppgifter om en omfrågad person förekommer i registren görs alltid en individuell bedömning huruvida uppgifterna kan antas ha betydelse för prövning av den kontrollerades pålitlighet ur säkerhetssynpunkt (relevansbedömning) och därmed kan lämnas ut för säkerhetsprövning.

Registerkontrolldelegationen ska, om en uppgift kommit fram som delegationen funnit anledning att lämna ut, ge den som uppgiften avser tillfälle att yttra sig. Undantag gäller för uppgift som omfattas av sekretess i förhållande till den enskilde.

7.1.4 Försvarets materielverk

Försvarets materielverk har enligt 1 § förordningen (2007:854) med instruktion för Försvarets materielverk till uppgift att på uppdrag av Försvarsmakten vidmakthålla, destruera och kassera varor samt upphandla byggentreprenader, varor och tjänster. Försvarets materielverk ska på uppdrag av Försvarsmakten även tillhandhålla logistik i form av service-, förråds- och verkstadstjänster. Försvarets materielverk ska vidare biträda Försvarsmakten i materielförsörjnings- och logistikförsörjningsplanering samt med materielsystemkunskap.

Försvarets materielverks enhet för säkerhetsskydd är den del inom Försvarets materielverk som ser till att samarbeten inom materielområdet med nationella och internationella myndigheter och företag omfattas av ett fullgott säkerhetsskydd. Försvarets materielverk har ett särskilt ansvar att enligt 17 § säkerhetsskyddsförordningen träffa avtal med svenska företag om det behövs för internationellt försvarssamarbete.

Sveriges Certifieringsorgan för it-säkerhet (CSEC) är en självständig enhet inom Försvarets materielverk som etablerades efter ett regeringsbeslut 2002. CSEC verkar som Sveriges nationella certifieringsorgan för it-säkerhet i produkter och system enligt standarden *Common Criteria* (CC), en internationell standard som används för att ställa krav på it-säkerhet och för opartisk granskning av it-säkerhet. CC har utvecklats i nära samarbete mellan flera länders säkerhetsmyndigheter och erkänns internationellt av världens ledande länder inom it-säkerhet. CC anses obligatoriskt för itprodukter i kritiska infrastrukturer i flera länder och tillämpas

inom flera olika sektorer, exempelvis försvar, finans, sjukvård, transport och kommunikation.

7.2 Myndigheter med sektorsansvar

7.2.1 Vad ansvaret innebär

I 40 § säkerhetsskyddsförordningen finns bestämmelser om kontroll av säkerhetsskyddet hos bolag, föreningar, stiftelser och enskilda över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande (1 § 2 säkerhetsskyddslagen) samt enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism (1 § 3 säkerhetsskyddslagen). Denna kontroll ska utföras av vissa i 19 § andra stycket säkerhetsskyddsförordningen utpekade myndigheter. Dessa myndigheter får också, vid sidan av den föreskriftsrätt som gäller för Säkerhetspolisen och Försvarsmakten enligt 43 och 44 §§ säkerhetsskyddsförordningen, meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen i fråga om säkerhetsskyddet inom sina verksamhetsområden (45 § säkerhetsskyddsförordningen). Myndigheter har också i uppgift att, med vissa undantag, för nämnda verksamheter besluta om placering i säkerhetsklass 2 och 3 och om registerkontroll till följd av sådan placering (se 19 § andra stycket säkerhetsskyddsförordningen) samt även registerkontroll skydd mot terrorism i fråga om bl.a. personal som deltar i verksamhet vid flygplatser och vissa skyddsobjekt (se 14 § säkerhetsskyddslagen samt 26 och 27 §§ säkerhetsskyddsförordningen). Myndigheterna och deras ansvarsområden i fråga om de uppgifter som här har redovisats beskrivs i de följande avsnitten 7.2.2–7.2.4.

7.2.2 Affärsverket svenska kraftnät

Affärsverket svenska kraftnät (Svenska kraftnät) är ett statligt affärsverk med uppgift att förvalta och utveckla Sveriges stamnät för elkraft som omfattar ledningar, stationer och utlandsförbindelser.

Svenska kraftnäts uppgifter anges i 1–5 §§ förordningen (2007:1119) med instruktion för Affärsverket svenska kraftnät.

Svenska kraftnät har bl.a. systemansvaret för el och ser till att det kontinuerligt råder balans mellan inmatad och uttagen el. Svenska kraftnät är vidare säkerhetsskyddsmyndighet för elföretagen, elberedskapsmyndighet och utövar tillsynsledning över dammsäkerheten i landet.

Svenska kraftnät beslutar enligt 26 § och 27 § 5 säkerhetsskyddsförordningen om registerkontroll av personer som ska anställas eller på annat sätt delta i verksamhet vid sådana anläggningar inom elförsörjningen som är skyddsobjekt, t.ex. vid kärnkraftverk. För elförsörjningsverksamhet beslutar Svenska Kraftnät även enligt 19 § andra stycket 1 och 20 § säkerhetsskyddsförordningen i vissa fall om placering i säkerhetsklass 2 och 3 samt registerkontroll.

7.2.3 Transportstyrelsen

Transportstyrelsen är en statlig myndighet som enligt 1 § förordningen (2008:1300) med instruktion för Transportstyrelsen har till huvuduppgift att svara för regelgivning, tillståndsprövning och tillsyn inom transportområdet.

Transportstyrelsen beslutar om registerkontroll till skydd mot terrorism enligt 26 samt 27–27 a §§ säkerhetsskyddsförordningen. Enligt 27 § 1 säkerhetsskyddsförordningen beslutar Transportstyrelsen om registerkontroll för personer som ska anställas eller på annat sätt delta i verksamhet vid civila flygplatser, flygstationer och flygpassagerarterminaler. Transportstyrelsen beslutar vidare enligt 26 § 1 och 27 a § andra stycket säkerhetsskyddsförordningen om registerkontroll av personer som ska anställas eller på annat sätt ska delta i verksamhet som har betydelse för luftfartsskyddet, om det följer av en internationell överenskommelse som Sverige tillträtt eller av en bindande EU-rättsakt på området luftfartsskydd, att säkerhetsprövningen ska omfatta registerkontroll. För flygtransportverksamhet beslutar Transportstyrelsen också enligt 19 § andra stycket 2 och 20 § säkerhetsskyddsförordningen i vissa fall om placering i säkerhetsklass 2 och 3 samt registerkontroll.

7.2.4 Post- och telestyrelsen

Post- och telestyrelsen är en statlig myndighet som bevakar områdena elektronisk kommunikation och post i Sverige. Begreppet elektronisk kommunikation innefattar telekommunikationer, it och radio. Post- och telestyrelsen är tillsynsmyndighet enligt lagen (2003:389) om elektronisk kommunikation.

Post- och telestyrelsens arbete med säker kommunikation innefattar bl.a. arbete med robust och driftsäker kommunikation. Av Post- och telestyrelsens föreskrifter framgår bl.a. att operatörerna ska förebygga avbrott och störningar genom att genomföra riskanalyser, hantera risker samt planera för att kunna hantera avbrott och störningar som kan inträffa.

Post- och telestyrelsen beslutar med stöd 26 § och 27 § 6 säkerhetsskyddsförordningen om registerkontroll av personer som ska anställas eller på annat sätt delta i verksamhet vid sådana anläggningar som används eller som är avsedda för elektronisk kommunikation och som är skyddsobjekt. För verksamhet som avser elektronisk kommunikation beslutar Post- och telestyrelsen också enligt 19 § andra stycket 3 och 20 § säkerhetsskyddsförordningen i vissa fall om placering i säkerhetsklass 2 och 3 samt registerkontroll.

7.2.5 Länsstyrelserna

I varje län finns enligt 1 § förordningen (2007:825) med länsstyrelseinstruktion en länsstyrelse som ansvarar för den statliga förvaltningen i länet. Länsstyrelsen ska vidare ansvara för de tillsynsuppgifter som riksdagen eller regeringen har ålagt den.

Länsstyrelsen i det län där skyddsobjektet finns beslutar med stöd av 26 § och 27 § 8 säkerhetsskyddsförordningen om registerkontroll av personer som ska anställas eller på annat sätt delta i verksamhet vid vissa skyddsobjekt. För andra verksamheter än sådana som avses i 19 § andra stycket 1–3 säkerhetsskyddsförordningen (dvs. de verksamheter som hör till Svenska kraftnäts, Post- och telestyrelsen eller Transportstyrelsens ansvarsområde) beslutar länsstyrelsen också enligt 19 § andra stycket 4 och 20 § säkerhetsskyddsförordningen i vissa fall om placering i säkerhetsklass 2 och 3 samt registerkontroll.

7.3 Övriga särskilt berörda myndigheter

7.3.1 Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap är en statlig myndighet som enligt 1 § i sin instruktion (2008:1002) har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning någon annan myndighet inte har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris.

Myndigheten ska i samverkan med myndigheter, kommuner, landsting, organisationer och företag identifiera och analysera sådana sårbarheter, hot och risker i samhället som kan anses vara särskilt allvarliga. Myndigheten ska vidare tillsammans med de ansvariga myndigheterna genomföra en övergripande planering av åtgärder som bör vidtas. Myndigheten ska värdera, sammanställa och rapportera resultatet av arbetet till regeringen. Myndigheten meddelar föreskrifter om risk- och sårbarhetsanalyser för kommuner och landsting samt för statliga myndigheter. Myndigheten ska införa, förvalta och utveckla radiokommunikationssystemet för skydd och säkerhet (Rakel-systemet).

Myndigheten för samhällsskydd och beredskap har vidare till uppgift att stödja och samordna arbetet med samhällets informationssäkerhet samt att analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. I myndigheten ingår CERT-SE, som är Sveriges nationella *Computer Emergency Response Team* med uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter. Inom ramen för detta ansvar ska Myndigheten för samhällsskydd och beredskap samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet och vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder.

Den 1 februari 2010 trädde myndighetens föreskrifter om statliga myndigheters informationssäkerhet i kraft.[4] Enligt föreskrifterna ska statliga myndigheter tillämpa ett ledningssystem för in-

[4] Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet, MSBFS 2009:10.

formationssäkerhet (LIS). Det innebär bl.a. krav på att myndigheter ska klassificera sin information, identifiera och hantera risker samt fortlöpande utvärdera och förbättra sin säkerhet. Arbetet ska bedrivas enligt etablerade informationssäkerhetsstandarder. Myndigheten för samhällsskydd och beredskap har även utfärdat föreskrifter om civila myndigheters kryptoberedskap under och utanför ordinarie kontorstid.[5]

7.3.2 Försvarets radioanstalt

Försvarets radioanstalt är en statlig myndighet som enligt 1 § i sin instruktion (2007:937) har till uppgift att bl.a. bedriva signalspaning.

Signalspaningen vid Försvarets radioanstalt riktas mot vissa utländska förhållanden. Det kan till exempel handla om säkerhetsläget och aktörer i områden där det finns svensk trupp, spridning av massförstörelsevapen, internationell terrorism och it-angrepp mot känsliga informationssystem i Sverige.

All signalspaning görs på uppdrag av regeringen, Regeringskansliet, Försvarsmakten, Polismyndigheten och Säkerhetspolisen.

Enligt 4 § förordningen med instruktion för Försvarets radioanstalt ska myndigheten ha teknisk kompetens inom informationssäkerhetsområdet och stödja statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Stödet kan bestå i bl.a. penetrationstester, kartläggning av nätverk och teknisk rådgivning om hur informationssäkerheten kan förbättras i de berörda verksamheterna. Tjänster inom informationssäkerhet beställs främst av statliga myndigheter och statligt ägda bolag.

7.3.3 Totalförsvarets forskningsinstitut

Totalförsvarets forskningsinstitut är en huvudsakligen uppdragsstyrd myndighet vars verksamhet bidrar till det militära försvarets

[5] Myndigheten för samhällsskydd och beredskaps föreskrifter om civila myndigheters kryptoberedskap, MSBFS 2009:11.

utveckling och samhällets säkerhet samt utgör ett stöd till Regeringskansliet i bl.a. vissa forsknings- och utredningsfrågor.

Enligt förordningen (2007:861) med instruktion för Totalförsvarets forskningsinstitut har myndigheten till uppgift att bedriva forskning, metod- och teknikutveckling samt utredningsarbete för totalförsvaret och till stöd för nedrustning, icke-spridning och internationell säkerhet. Myndigheten får även i övrigt bedriva forskning, metod- och teknikutveckling samt utredningsarbete. Totalförsvarets forskningsinstitut ska verka för att försvarsforskningen kommer till nytta även utanför totalförsvaret.

Totalförsvarets forskningsinstituts uppgift att bedriva försvarsunderrättelseverksamhet ska fullgöras genom analyser av information som inhämtats från offentliga informationskällor eller som lämnats av uppdragsgivare.

Totalförsvarets forskningsinstitut ska vidare särskilt verka för samverkan mellan militär och civil forskning samt mellan nationell och internationell forskning och ska på uppdrag av Försvarsexportmyndigheten bedriva exportrelaterad verksamhet inom försvarssektorn.

Försvarsmakten och Försvarets materielverk är Totalförsvarets forskningsinstituts huvudkunder, men myndigheten har även uppdrag från civila myndigheter och näringslivet.

7.3.4 Fortifikationsverket

Fortifikationsverket är en statlig myndighet som ansvarar för att förvalta Sveriges försvarsfastigheter. Verket har också till uppgift att bistå samhället med kunskap om skyddsteknik och säkerhet. Fortifikationsverkets uppdrag anges i förordningen (2007:758) med instruktion för Fortifikationsverket.

Fortifikationsverket utför skydds- och sårbarhetsanalyser för andra myndigheter och företag, med fokus på skydd av värden i byggnader och anläggningar. Verket har bl.a. tagit fram ett praktiskt arbetssätt för att identifiera värden och hot, analysera befintligt skydd samt utföra riskanalyser för anläggningar med särskilda skyddskrav. Målet är att optimera skyddsåtgärderna mot angrepp av varierande art mot anläggningen och konsekvenserna av sådana angrepp.

7.4 Samverkan mellan olika myndigheter m.fl.

Samverkansrådet mot terrorism

Samverkansrådet mot terrorism är ett samarbete mellan 13 myndigheter som syftar till att stärka Sveriges förmåga att motverka terrorism. Till Samverkansrådet hör ett antal arbetsgrupper. En av arbetsgrupperna, Nationellt centrum för terrorhotbedömning (NCT), är permanent. I NCT finns representanter för Försvarets radioanstalt, Försvarsmakten (MUST), och Säkerhetspolisen. Uppgifterna för det permanenta NCT är att göra strategiska terrorhotbedömningar på kort och lång sikt mot Sverige och svenska intressen. NCT ska även producera strategiska analyser av händelser, trender och omvärldsutveckling med koppling till terrorism som berör eller kan komma att beröra Sverige och svenska intressen.

Samverkansforumet Nationell samverkan till skydd mot allvarliga it-hot

Samverkansforumet Nationell samverkan till skydd mot allvarliga it-hot (NSIT) är en ny samverkansform mellan Säkerhetspolisen, Försvarsmakten (MUST) och Försvarets radioanstalt. NSIT ska framför allt bedöma hot och sårbarheter när det gäller allvarliga it-angrepp mot våra mest skyddsvärda nationella civila och militära intressen. Målet med NSIT är bl.a. att skapa effektivare informationsöverföring och kunskapsöverföring mellan NSIT-myndigheterna och ett effektivt operativt användande av de kvalificerade nationella it-säkerhetskompetenserna som myndigheterna har.

Nationella telesamverkansgruppen

Nationella telesamverkansgruppen (NTSG), som bildades 2005, är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället. Kriteriet för medlemskap i NTSG är att operatören eller organisationen har egen teknisk utrustning, kunskaper eller resurser som påverkar Sveriges kritiska infrastruktur för elektronisk kommunikation. I NTSG ingår ComHem, Hi3G, IP-Only, Netnod, Skanova, Stokab, Svenska

Kraftnät, Svenska Stadsnätsföreningen, TDC, Tele2, Telenor, TeliaSonera, Teracom, Trafikverket, ICT, Försvarsmakten, Myndigheten för samhällsskydd och beredskap samt Post- och telestyrelsen.

Samverkansgruppen för informationssäkerhet

Samverkansgruppen för informationssäkerhet (SAMFI) är en grupp bestående av myndigheter med särskilda uppgifter inom området informationssäkerhet. Förutom Myndigheten för samhällsskydd och beredskap, som är ansvarig för SAMFI, ingår i samverkansgruppen Försvarsmakten (MUST), Försvarets materielverk (CSEC), Försvarets radioanstalt, Post- och telestyrelsen samt Polismyndigheten och Säkerhetspolisen i samverkan. SAMFI ska verka för säkra informationstillgångar i samhället avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet samt genom informationsutbyte och samverkan stödja de medverkande myndigheternas arbete avseende samhällets informationssäkerhet. Myndigheten för samhällsskydd och beredskap har i samverkan med SAMFI-myndigheterna samt andra myndigheter och organisationer tagit fram ett metodstöd för verksamheters informationssäkerhetsarbete. Metodstödet ska fungera som ett stöd till alla typer av organisationer som ska införa och tillämpa LIS med utgångspunkt i internationella standarder i ISO 27000-serien.

8 Internationell utblick

Det ingår i utredningsuppdraget att redovisa de regler och förfaranden som gäller i några med Sverige jämförbara länder, i första hand de nordiska och några länder inom EU som tillämpar ett system med säkerhetsklarering. Utredningen har därför sökt information om systemen i Danmark, Finland, Nederländerna, Norge och Tjeckien. Nederländerna är ett land som är väletablerat ur ett säkerhetsskyddsperspektiv och har gott internationellt renommé på området. Tjeckien är särskilt intressant för att lagstiftningen på området är relativt ny och anpassad för internationella åtaganden. Båda dessa länder har även intressanta lösningar när det gäller säkerhetsklarering och hur den nationella säkerhetstjänsten organiserats.

Arbetet har bedrivits främst genom undersökning av lagstiftning och i förekommande fall förarbeten samt övrig information från officiella webbplatser. Denna undersökning har kompletterats med besök vid de nationella säkerhetsmyndigheterna med i förhand lämnade skriftliga frågor till företrädare för myndigheterna. Skrivelserna har varit ställda direkt till berörda tjänstemän och de svar dessa lämnat representerar således inte någon formell ståndpunkt från de berörda ländernas sida. Vad gäller materialinsamlingen i övrigt bör beaktas att materialet funnits tillgängligt på originalspråk, i något fall kompletterat av mer eller mindre officiella översättningar till engelska.

8.1 De nordiska länderna

8.1.1 Allmänt om de nordiska länderna

Det är naturligt att inledningsvis redovisa vad som gäller i de nordiska länderna med tanke på de likheter som finns mellan Sverige och de övriga nordiska länderna. På detta område har det dock visat sig att de författningstekniska konstruktionerna skiljer sig markant mellan länderna. I Danmark regleras säkerhetsskyddsfrågorna i ett *sikkerhedscirkulære* dvs. närmast på normnivån förordning. Detta liknar lösningen i Finland där informationssäkerhetsfrågorna är reglerade i förordningen om informationssäkerheten inom statsförvaltningen. I Finland finns det dock även två separata lagar av betydelse, nämligen en säkerhetsutredningslag (motsvarar säkerhetsprövning i Sverige) samt en lag om internationella förpliktelser som gäller informationssäkerhet som reglerar Finlands folkrättsliga förpliktelser på informationssäkerhetsområdet. Norge, slutligen, har en *sikkerhetslov* där samtliga bestämmelser om säkerhetsskydd finns samlade vilket liknar den svenska säkerhetsskyddslagen (1996:627).

Vi har inte studerat Islands lagstiftning på området.

8.1.2 Danmark

Allmänt om säkerhetsskydd i Danmark

I Danmark regleras säkerhetsskyddet i ett *sikkerhedscirkulære*[1] som rör skyddet av såväl dansk skyddsvärd information som sådan information från Nato, EU och WEU samt från andra organisationer och länder som Danmark har internationella avtal med (däribland Sverige). Cirkuläret gäller för statsministeriet, men det förutsätts att cirkuläret tillämpas även av övriga ministerier. Cirkulärets innehåll kan göras tillämpligt på enskilda genom avtal.

Politiets Efterretningstjenste (PET) och *Forsvarets Efterretningstjenste* (FE) är de två myndigheter som har huvudansvaret för säkerhetsskydd i Danmark. Verksamheterna styrs av lagen om PET

[1] Statsministeriets *Cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelseinteresse i øvrigt*, CIR nr. 10338 af 17/12/2014.

(LOV nr. 604 af 12/06/2013) respektive lagen om FE (LOV nr. 602 af 12/06/2013).

Huvuddragen i regleringen

Säkerhetscirkuläret innehåller bestämmelser om PET:s och FE:s uppgifter, klassificering av information, informations- och dokumentsäkerhet, behörighet till klassificerad information, it-säkerhet, destruktion av klassificerad information, personalsäkerhet och fysisk säkerhet, rådgivning och tillsyn. I Danmark har Statsministeriet en sådan samordnande roll i statsförvaltningen att cirkuläret anses vara tillämpligt även för övriga ministerier och deras myndigheter. Det är dock inte tillämpligt på enskilda och inte heller på kommuner och regioner. De fyra största kommunerna tillämpar cirkuläret på frivillig basis vilket har haft påverkan på övriga kommuner och regioner som också använder cirkuläret i praktiken.

Cirkuläret är detaljerat och innehåller bestämmelser som direkt kan tillämpas av de som cirkuläret gäller för, men det finns även ett krav att myndigheter ska utforma närmare föreskrifter om tillämpningen i den egna verksamheten. I försvarssektorn gäller Försvarskommandots bestämmelser för militär säkerhetstjänst.[2] Dessa bestämmelser är ett omfattande dokument som närmast kan liknas vid en handbok i säkerhetstjänst.

Cirkulärets primära fokus är skyddet av klassificerad information, men det innehåller även ett fåtal bestämmelser som tar sikte på ”information av säkerhetsmässigt skyddsintresse i övrigt.” Denna del av regelverket är inte ytterligare utvecklat utan ger enbart en möjlighet för myndigheter att genom föreskrifter tillämpa skyddet för annan information i den egna verksamheten. Cirkuläret har ett informationssäkerhetsperspektiv och ger inte något skydd för säkerhetskänslig verksamhet i övrigt.

Informationsklassificeringen bygger som i många andra länder på en fyragradig skala med klasserna (i fallande ordning) *yderst hemmeligt*, *hemmeligt*, *fortroligt* och *til tjenstebrug*. I anslutning till begreppen anges deras motsvarigheter i Nato och EU inom parentes. Det som avgör klassificeringens nivå är den skada som ett

[2] Försvarskommandots bestämmelser för militär säkerhetstjänst, FKOBST 358.1.

olovligt röjande kan innebära. Det är upprättaren som avgör hur informationen ska klassificeras. Behörigheten till den klassificerade informationen styrs av att det ska finnas ett behov att ta del av uppgifterna, samt att mottagaren av informationen ska vara säkerhetsgodkänd och ha fått utbildning i de regler som styr hanteringen av informationen. Informationssystem som hanterar klassificerad information på nivån *fortroligt* eller över ska godkännas av den nationella it-säkerhetsmyndigheten. Denna roll har FE, utom för Justitieministeriets område där i stället PET har denna roll.

När det gäller säkerhetsprövning (på danska *sikkerhedsundersøgelse*) styrs processen av bestämmelser i både säkerhetscirkuläret och i lagarna om PET och FE. Enligt förarbetena[3] till de sistnämnda lagarna krävs samtycke av såväl den prövade som av närstående till den prövade. Prövningen görs mot den högsta nivå av klassificerad information som den prövade kan komma att få del av. En registerkontroll utgör grunden i en säkerhetsprövning och är det enda momentet för prövning mot anställningar eller annat deltagande i de två lägre nivåerna (*til tjenstebrug* och *fortroligt*). Prövningen i de två högre nivåerna kompletteras med inhämtning av information om den prövade hos referenspersoner och eventuella tidigare arbetsgivare, och därefter görs en värdering utifrån inhämtade upplysningar från skatteväsendet. Om det anses nödvändigt kallas den prövade till samtal för att hantera eventuella oklarheter. Inom Försvarsministeriets område genomförs säkerhetssamtal med samtliga prövade som ska säkerhetsgodkännas mot nivån *yderst hemmeligt*. När det gäller anställning vid PET eller FE kompletteras säkerhetsprövningen med en säkerhetsintervju som innefattar psykologiska aspekter.

PET gör vid registerkontrollen en viss relevansprövning av eventuella förekommande registeruppgifter, men i övrigt lämnas samtliga uppgifter till den anställande myndigheten för prövning. PET ger inte någon rekommendation till beslut utan det ankommer helt och hållet på den anställande myndigheten att avgöra relevansen och fatta beslut om anställningen. PET redovisar de grunder och den praxis som PET har för anställning vid den egna myndigheten och denna praxis följs i stor omfattning även av andra myndigheter. Prövningen ska visa att personen har en ”obestridd loja-

[3] Lovforslag nr. L 161 Folketinget 2012-13 respektive nr. L 163 Folketinget 201-13.

litet” samt en sådan personlighet som inte ger några tvivel om personens pålitlighet avseende hanteringen av klassificerad information. Om myndigheten fattar ett positivt beslut, anses personen vara säkerhetsgodkänd.

Ett sådant godkännande kan ligga till grund för ett säkerhetsintyg för person om det behövs i internationella sammanhang. Ett intyg gäller bara för den aktuella anställningen och kan inte användas för annat bruk. Inom Försvarsdepartementets område utfärdas alltid intyg (eller säkerhetscertifikat) för nivån *yderst hemmeligt* och i övrigt vid behov. Om intyg utfärdas motsvarar giltighetstiden säkerhetsgodkännandets giltighetstid (högst fem år för *yderst hemmeligt* och tio år för övriga).

Det finns i säkerhetscirkuläret ett krav att den som är säkerhetsgodkänd ska utbildas i relevanta bestämmelser som rör hantering av klassificerad information och om innehållet i vissa straffrättsliga bestämmelser.

Säkerhetsprövningen anses vara pågående under hela anställningstiden, och uppgifter som tillförs kriminalregistret efter det att en person har blivit säkerhetsgodkänd lämnas med automatik ut från PET till den anställande myndigheten.

Industrisäkerheten är inte lagreglerad, men det finns i säkerhetscirkuläret en bestämmelse om att den nationella säkerhetsmyndigheten kan ingå avtal om områdessäkerhetsgodkännande (vilket motsvarar *Facility Security Clearance*), och FE:s säkerhetsgodkännande av verksamheter är beskrivet i förarbetena till lagen om FE.

I lagarna om PET och FE finns dessutom bestämmelser om när behandling av uppgifter om juridiska personer är tillåten. FE genomför således säkerhetsgodkännande av privata verksamheter med stöd av lagen om FE, säkerhetscirkuläret och Försvarskommandots säkerhetsbestämmelser. Enbart verksamheter som har blivit säkerhetsgodkända kan få uppdrag som innebär tillgång till klassificerad information. Kraven på säkerhetsskydd regleras i avtal mellan den upphandlande myndigheten och uppdragstagaren och avtalet ligger sedan till grund för säkerhetsprövning av den personal som kan komma att få tillgång till klassificerad information. PET har i princip samma möjligheter för den civila sektorn, men ännu har det inte förekommit att verksamheter utanför Försvarsministeriets verksamhetsområde har haft behov av säkerhets-

godkännande. Ett säkerhetsgodkännande kan ligga till grund för säkerhetsintyg för leverantör om det behövs för internationell samverkan. Dessa utfärdas av FE i egenskap av industrisäkerhetsmyndighet (DSA).

Utmärkande detaljer i regleringen

Det danska regelverket skiljer sig från det svenska genom att bestämmelser om säkerhetsskydd i huvudsak återfinns i ett cirkulär (motsvarande förordning). Bestämmelser som kräver lagform finns i de lagar som styr verksamheten vid PET och FE generellt, t.ex. i vilka fall personuppgifter får hanteras.

Säkerhetsprövningen och säkerhetsgodkännande av leverantörer är tillämpligt på samtliga nivåer, dvs. från nivån *til tjenstebrug* och uppåt. Detta skiljer sig från många andra länder och krav i internationella regelverk där den lägsta nivån ofta undantas.

Ansvarsuppdelningen mellan PET och FE liknar i huvudsak motsvarande ansvarsfördelning mellan Säkerhetspolisen och Försvarsmakten i Sverige.

8.1.3 Finland

Allmänt om säkerhetsskydd i Finland

I Finland är regleringen på säkerhetsskyddsområdet uppdelad på flera författningar. Informationssäkerheten regleras i förordningen om informationssäkerheten inom statsförvaltningen[4] som bygger på ett normgivningsbemyndigande i lagen om offentlighet i myndigheternas verksamhet.[5] Finlands folkrättsliga åtaganden på säkerhetsskyddsområdet hanteras i en separat lag om internationella förpliktelser som gäller informationssäkerhet[6] i vilken det finns bestämmelser om informationssäkerhet och om olika myndigheters ansvar i internationell samverkan på säkerhetsskyddsområdet. Slutligen regleras säkerhetsprövningsfrågorna i en separat

[4] Förordning om informationssäkerheten inom statsförvaltningen, 681/2010.
[5] Lag om offentlighet i myndigheternas verksamhet, 621/1999.
[6] Lag om internationella förpliktelser som gäller informationssäkerhet, 588/2004.

säkerhetsutredningslag.[7] Den sistnämnda lagen trädde den ikraft den 1 januari 2015 och ersatte den tidigare lagen om säkerhetsutredningar. Lagstiftningsarbetet har pågått sedan 2008, och de huvudsakliga reformbehoven har varit att förtydliga under vilka omständigheter en säkerhetsutredning får göras, effektivisera arbetsformerna, utveckla industrisäkerheten samt att ge en ökad öppenhet i utredningsförfarandet.

Skyddspolisen, som motsvarar Säkerhetspolisen i Sverige, har ett övergripande ansvar för det nationella säkerhetsskyddsarbetet utom vad avser det finska försvaret där Huvudstaben i stället ansvarar för direktiv inom den egna verksamheten.

Huvuddragen i regleringen

Informationssäkerheten regleras främst i förordningen om informationssäkerheten inom statsförvaltningen som bygger på ett normgivningsbemyndigande i lagen om offentlighet i myndigheternas verksamhet. Finansministeriet är ansvarigt ministerium för att styra statsförvaltningens informationsförvaltning, och inom ramen för den uppgiften ligger även ett ansvar för informationssäkerhet. Finansministeriet har inte någon direkt föreskriftsrätt eller tillsyn över informationssäkerheten men har inrättat en ledningsgrupp för datasäkerheten i statsförvaltningen (VAHTI) som ett organ för samarbete inom området informationssäkerhet. VAHTI har gett ut en anvisning om verkställighet av förordningen om informationssäkerheten inom statsförvaltningen. Förordningen definierar informationssäkerhet som ”administrativa, tekniska och andra åtgärder och arrangemang som genomförs för iakttagande av sekretessen och åtkomstbegränsningarna samt säkerställandet av uppgifternas tillgänglighet, integritet och användbarhet.” När det gäller klassificering av handlingar ställer förordningen inte några bindande krav, men handlingar *kan* klassificeras i skyddsnivåer enligt en fyrgradig skala som bygger på den skada som ett obehörigt avslöjande av informationen kan innebära. Skyddsnivå I är den högsta klassificeringen och skyddsnivå IV den lägsta och dessa styr sedan hanteringskraven för informationen i fråga. Vidare finns det i

[7] Säkerhetsutredningslag, 726/2014.

förordningen kompletterande bestämmelser som gäller om informationen kan orsaka skada för bl.a. internationella relationer, statens säkerhet eller försvaret. I dessa fall kan skyddsnivåmärkningen kompletteras eller ersättas av en säkerhetsklassificering. Denna följer skyddsnivåindelningen men nivåerna benämns i stället (i fallande ordning) *ytterst hemlig, hemlig, konfidentiell* och *begränsad tillgång*. Inte heller i detta fall ställer förordningen något bindande krav utan ger endast en möjlighet för myndigheterna att utföra en sådan klassificering som beskrivs, under förutsättning att kriterierna för klassificering är uppfyllda. Förordningen avslutas med ett antal bestämmelser som reglerar hanteringen av klassificerade handlingar.

Informationssäkerheten avseende Finlands internationella åtaganden regleras i lagen om internationella förpliktelser som gäller informationssäkerhetsområdet. Denna lag reglerar hur olika myndigheter, säkerhetsmyndigheterna,[8] ska samverka i det internationella samarbetet avseende informationssäkerhet. Vidare innehåller lagen en bestämmelse om en obligatorisk märkning för det som i lagen definieras som särskilt känsligt informationsmaterial.[9] Lagen innehåller också bestämmelser om säkerhetsåtgärder, säkerhetsutredningar, internationella inspektioner, utredning om informationsförluster och avslutningsvis straffbestämmelser. De sistnämnda hänvisar till den finska strafflagens bestämmelser om sekretessbrott och brott mot tjänstehemlighet vilka båda närmast motsvarar brott mot tystnadsplikten i svensk rätt.

Säkerhetsprövning i svensk rätt motsvaras i Finland av begreppet säkerhetsutredning. Till skillnad från svensk rätt regleras säkerhetsprövning i en separat lagstiftning, säkerhetsutredningslagen. Lagen har som syfte att främja möjligheterna att förebygga verksamhet som kan medföra skada för statens säkerhet, försvaret, Finlands internationella förbindelser, den allmänna säkerheten eller något annat med dessa jämförbart allmänt intresse eller enskilda

[8] Utrikesministeriet är Finlands nationella säkerhetsmyndighet vid uppfyllandet av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben, skyddspolisen och Kommunikationsverket är sådana utsedda säkerhetsmyndigheter som avses i internationella förpliktelser som gäller informationssäkerhet.

[9] Med *särskilt känsligt informationsmaterial* avses sådana sekretessbelagda handlingar och material samt sådan information som kan fås ur dem samt sådana handlingar och material som producerats utifrån dessa handlingar och material samt denna information och som har säkerhetsklassificerats enligt en internationell förpliktelse som gäller informationssäkerhet.

ekonomiska intressen av synnerligen stor betydelse eller säkerhetsarrangemang för skyddet av dessa intressen.[10] Säkerhetsutredningar kan genomföras som normal, omfattande eller begränsad utredning. Den normala utredningen utgör huvudregeln och ett ärende om en säkerhetsutredning initieras av en arbetsgivare eller uppdragsgivare som kan vara t.ex. en statlig myndighet, ett statligt affärsverk eller en privat sammanslutning.

Skyddspolisen beslutar om en säkerhetsutredning ska göras, om inte sökanden hör till Försvarsmakten då i stället huvudstaben fattar beslut. En säkerhetsutredning förutsätter samtycke från den som utredningen gäller och får bygga enbart på registeruppgifter ur i lagen uppräknade register. En omfattande utredning får göras om en person

- i sina arbetsuppgifter får rätt att annat än tillfälligt hantera klassificerade handlingar på skyddsnivå I eller II,
- sköter sådana uppgifter där han eller hon genom att röja sekretessbelagda uppgifter eller begå någon annan lagstridig gärning kan skada statens säkerhet, försvaret eller Finlands internationella förbindelser,
- behöver ett intyg över säkerhetsutredning av person på grund av en internationell förpliktelse som gäller informationssäkerhet, eller
- ska kunna utses till uppdrag inom en internationell organisation eller ett internationellt organ.

En omfattande utredning innehåller förutom registeruppgifter även uppgifter om näringsverksamhet, ekonomisk ställning och familje-, bostads- och anställningsförhållanden och får, om det är absolut nödvändigt, utsträckas till att avse närstående.

En begränsad säkerhetsutredning får göras i ett stort antal fall t.ex. när personer får rätt att hantera myndighetshandlingar på skyddsnivåerna III och IV, får permanent tillträde till vissa myndigheters lokaler eller områden som är stängda för allmänheten, får tillträde till skyddade lokaler på flygplatser eller i hamnar eller del-

[10] 1 kap. 1 § säkerhetsutredningslagen.

tar i transport av kärnämnen. En begränsad utredning avser registerutdrag ur ett fåtal register.

Ett beslut, t.ex. rörande utfärdande av säkerhetsintyg, i ett ärende som gäller en säkerhetsutredning kan överklagas under vissa förutsättningar hos förvaltningsdomstol. En behörig myndighets beslut genom vilket den vägrat göra en säkerhetsutredning får dock inte överklagas genom besvär. Ett beslut som gäller utfärdande och återkallelse av ett intyg över säkerhetsutredning får överklagas av den som ansökt om säkerhetsutredning och av den som utredningen gäller. En myndighet vars beslut förvaltningsdomstolen har upphävt eller ändrat får för att bevara en enhetlig tillämpning av lagen överklaga förvaltningsdomstolens beslut.

Ett centralt mål för lagreformen har varit att effektivisera den övergripande säkerheten genom att främja företagssäkerheten och utveckla säkerhetsskyddet inom statsförvaltningen. Målet har även varit att få lagstiftningen i Finland att motsvara internationell praxis samt att göra utredningsförfarandet hos olika myndigheter enhetligt och öppnare.

Utmärkande detaljer i regleringen

Det finska regelverket är uppdelat på ett sådant sätt som var fallet i Sverige före säkerhetsskyddslagens tillkomst. Säkerhetsprövningen, eller infiltrationsskyddet som det då benämndes, reglerades i personalkontrollkungörelsen från 1969 medan säkerhetsskyddet i övrigt reglerades i 1981 års säkerhetsskyddsförordning. Vidare är det finska regelverket inte så tydligt avseende tillsyn och föreskrifter, även om Finansministeriet har ett visst övergripande ansvar för det nationella informationssäkerhetsarbetet.

När det gäller säkerhetsklareringen skiljer sig förfarandet från säkerhetsprövning i Sverige genom att klareringen i huvudsak bygger på registeruppgifter. Även om den nya lagen innehåller bestämmelser om kompletterande intervjuer, kommer troligen ändå klareringen fortsättningsvis i huvudsak bygga på uppgifter ur register.

8.1.4 Norge

Allmänt om säkerhetsskydd i Norge

I Norge består regleringen av säkerhetsskydd av *lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)*[11] med tillhörande förordningar. Lagen trädde i kraft i juli 2001 och har därefter vid två tillfällen genomgått mindre ändringar. Den norska regleringen liknar i stora delar den svenska regleringen. Sikkerhetsloven med tillhörande förordningar gäller inte för Stortinget och dess organ.[12] Syftet med sikkerhetsloven är att skapa förutsättningar för att effektivt motverka hot mot rikets självständighet och säkerhet samt hot mot andra vitala nationella säkerhetsintressen. Bedömningen görs med utgångspunkt i den skada som kan inträffa om skyddsvärd information blir känd för obehöriga. I lagens inledande bestämmelser understryks därutöver bl.a. vikten av att tillvarata den enskildes rättssäkerhet. Lagen med tillhörande föreskrifter anger minimikrav för skydd av information och objekt av betydelse för rikets eller allierades säkerhet samt andra vitala nationella säkerhetsintressen. Begreppet vitala nationella säkerhetsintressen omfattar bl.a. kritisk infrastruktur och andra kritiska samhällsfunktioner.[13] Regelverket innehåller bestämmelser om förebyggande åtgärder mot förberedelse till, försök till och genomförande av spionerі, sabotage och terrorhandlingar.

Den norska regeringen har tagit initiativ till en översyn av sikkerhetsloven med anledning av dels att förutsättningarna för informationssäkerhet har förändrats, dels att ingen översyn har gjorts av lagen i sin helhet sedan den trädde i kraft 2001.

I Norge finns en nationell säkerhetsmyndighet, *Nasjonal sikkerhetsmyndighet (NSM)*.[14] Myndigheten bildades 2003 och sorterar under Försvarsdepartementet. NSM rapporterar dock till Justitiedepartementet[15] avseende den civila sektorn. Myndighetens verksamhet innefattar även Norges nationella centrum för hantering av

[11] Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven, LOV 1998-03-20 nr 10).
[12] Vilket är jämförbart med säkerhetsskyddslagen där riksdagen i stor utsträckning har undantagits från lagens bestämmelser.
[13] Elförsörjning, elektronisk kommunikation, vatten- och avlopp, transporter samt olja- och gasförsörjning är exempel på kritisk infrastruktur.
[14] NSM har rollerna som NSA, NCSA, NDA, SAA och TA i Norge. Angående dessa funktioner se avsitt 6.3.
[15] *Justis- og beredskapsdepartementet (JD)*.

allvarliga incidenter mot samhällsviktig infrastruktur och information (NorCERT) vilket i Sverige motsvaras av CERT-SE (på Myndigheten för samhällsskydd och beredskap). NSM har en nationell tillsyn över säkerhetsskyddet och även föreskriftsrätt.

Huvuddragen i regleringen

Sikkerhetsloven innehåller bestämmelser om informationssäkerhet, objektsäkerhet, personalsäkerhet och industrisäkerhet. Syftet med *informationssäkerheten* är att skydda känsliga uppgifter som är ”av betydelse för Norges eller dess allierades säkerhet, förhållandet till främmande makter eller andra vitala nationella säkerhetsintressen.”

Lagens bestämmelser om informationssäkerhet tar sikte på säkerhetsgradering, skyldighet att skydda säkerhetsklassad information, godkännande av informationssystem, kryptosäkerhet, övervakning av informationssystem och tekniska säkerhetsundersökningar.[16] Säkerhetsgraderingen innebär att skyddsvärd information placeras i någon av de fyra säkerhetsgraderna (i fallande ordning) *strengt hemmelig, hemmelig, konfidensielt,* och *begrenset*. Avgörande för vilken säkerhetsgrad informationen ska placeras i är den skada som kan uppstå om informationen röjs. Lagen föreskriver ett bindande skydd för uppgifter som omfattas av internationella åtaganden.[17] En säkerhetsgradering är giltig i 30 år om inget annat anges. Om tiden för behov av skydd är väsentligt kortare, ska i stället en tidsbegränsad värdering övervägas.

När det gäller *personalsäkerhet* tillämpas ett tvåstegsförfarande. Det inleds med en säkerhetsklarering och åtföljs av en s.k. auktorisation.[18] Beslut om auktorisation fattas av den anställande myndigheten och är nödvändigt för anställningar där känsliga uppgifter på nivån *konfidensiellt* eller högre kan komma att hanteras. Säkerhetsklareringen utgår från säkerhetsgraderingen av information. Vilken nivå den enskilde ska klareras för avgörs därmed av graderingen av den skyddsvärda information som personen kan komma att hantera. Anställningar där endast hantering av information i den lägsta

[16] Här avses inte tekniska säkerhetsundersökningar, s.k. TSU, i svensk mening utan snarare säkerhetsgodkännande av informationssystem (ackrediteringsgranskning).
[17] Norge har ingått avtal bl.a. med de nordiska länderna, Nato och EU.
[18] Auktorisation är ett beslut om godkännande som en person har från verksamhetens chef för att få tillgång till säkerhetsklassad information.

graderingen kan komma i fråga kräver inte klarering men dock ett beslut om auktorisation. Ett särskilt förfarande, s.k. säkerhetsorientering, gäller för personer som genom sina arbetsuppgifter under enbart en begränsad tid kan komma i kontakt med skyddsvärd information på låg nivå. Ett exempel på en sådan personalkategori är lokalvårdspersonal.

Även andra myndigheter, angivna referenser och tidigare arbetsgivare kan kontaktas inom ramen för säkerhetsklareringen, men det är något som görs mycket sällan. Trots ordalydelsen i lagen tycks underlaget för säkerhetsklareringen i huvudsak vara begränsat till en registerkontroll. Vid klarering av utländska medborgare görs bl.a. en bedömning av vederbörandes anknytning till hemlandet och till Norge. I samband med en lagändring[19] uttalades dock att ändringen inte innebär någon huvudregel om att utländska medborgare ska ges klarering, utan i de fall ett utländskt medborgarskap ger upphov till särskilda problem från säkerhetssynpunkt ska detta beaktas. En klarering gäller för all statlig verksamhet under fem år vilket skiljer sig från det svenska systemet där säkerhetsprövningen är kopplad till anställningen. För värnpliktiga är en klarering giltig i endast två år. Klareringsmyndigheterna är de olika departementen och ett stort antal myndigheter som har fått denna uppgift delegerad från respektive departement. För närvarande finns det 42 klareringsmyndigheter. Försvarssektorn hanterar det största antalet klareringar.

Genom mängden klareringsmyndigheter är förfarandet delvis likt det svenska systemet där anställningsmyndigheten står för säkerhetsprövningen, men systemet är också förhållandevis svåröverskådligt. NSM är av uppfattningen att antalet klareringsmyndigheter skulle behöva minskas betydligt. Det finns också ett stort spann avseende antalet klareringar som de olika myndigheterna hanterar. Vissa myndigheter hanterar flera tusen klareringar per år och andra endast ett fåtal. I fråga om klarering ansvarar NSM framför allt för registerkontroll (motsvarande Säkerhetspolisens uppgift i Sverige). Undantag gäller för den högsta klassen där NSM också är klareringsmyndighet. Det finns möjlighet att överklaga ett negativt klareringsbeslut (se nedan under rubriken Utmärkande detaljer i lagstiftningen).

[19] 22 § Sikkerhetsloven, som ändrades genom lag av den 17 juni 2005 nr. 81.

I Sikkerhetsloven finns det även bestämmelser om *objektsäkerhet*. Detta kan jämföras med Sverige där objektssäkerhet i huvudsak regleras i skyddslagen (2010:305). Objekt som i enlighet med den norska lagen bedöms vara skyddsvärda klassificeras som viktiga, kritiska eller mycket kritiska.[20] Lagen ställer också funktionella krav på hur de skyddsvärda objekten ska skyddas. En svårighet som NSM har pekat på är vilken roll myndigheten ska ha i klassificeringen av objekt och hur klassificeringen ska bli likvärdig mellan olika samhällssektorer.

När det gäller *industrisäkerhet* så finns bestämmelser om detta i lagens avsnitt om säkerhetsgraderade upphandlingar.[21] För att företag och andra leverantörer ska få arbeta med uppdrag där säkerhetskänslig information på nivån *konfidensielt* eller högre kan komma att hanteras ställs krav på att leverantörer ska vara säkerhetsklarerade genom en leverantörsklarering. Till skillnad från klarering av personer är leverantörsklareringen giltig endast för ett särskilt uppdrag. För klarering av leverantörer är NSM ensam klareringsmyndighet. Myndigheten utfärdar cirka 100 leverantörsklareringar årligen och trenden är uppåtgående. En del av de gjorda klareringarna avser emellertid samma företag på grund av att klareringen är uppdragsspecifik.

Utmärkande detaljer i regleringen

Den norska *sikkerhetlovens* syfte är att ge ett skydd för ”rikets eller allierades säkerhet samt andra vitala nationella säkerhetsintressen” vilket innebär är ett vidare tillämpningsområde än säkerhetsskyddslagen.

När det gäller objektsäkerhet i lagstiftningen så skiljer sig även detta från säkerhetsskyddslagen. I Sverige regleras dessa frågor delvis i skyddslagen, även om bedömningskriterierna och analysen kring objekten inte är lika tydligt beskrivna. Reglerna om objektssäkerhet ansluter till reglerna om tillträdesbegränsning.

I *sikkerhetsloven* finns det bestämmelser om överklagande av säkerhetsklarering. Överklagade ärenden prövas av klareringsmyndigheten med NSM som överinstans. För ärenden där NSM varit

[20] På norska *viktig*, *kritisk* och *meget kritisk*.
[21] På norska *sikkerhetsgraderte anskaffelser*.

klareringsmyndighet är i stället Försvarsdepartementet överinstans. Ett delvis gynnande beslut kan inte överklagas. Det är endast möjligt att få lagligheten av ett beslut prövat (laglighetsprövning).[22]

Sikkerhetsloven innehåller bestämmelser om kryptosäkerhet som endast delvis finns reglerat i säkerhetsskyddslagstiftningen.

8.2 Övriga länder

8.2.1 Nederländerna

Allmänt om säkerhetsskydd i Nederländerna

Grunden för att skydda information i Nederländerna finns i 1951 års lag om skydd för statshemligheter.[23] Vidare finns det grundläggande bestämmelser om säkerhetsskydd och säkerhetsprövning i 2002 års lag om underrättelse- och säkerhetstjänsterna och utöver det en särskild säkerhetsundersökningslag från 1996 (motsvarande säkerhetsprövning i Sverige). Det finns kompletterande föreskrifter i form av förordningar om informationssäkerhet, säkerhetsskyddsfunktioner och kommunikationssäkerhet.

I Nederländerna finns det två nationella säkerhetsmyndigheter – AIVD[24] och MIVD[25]. AIVD är den allmänna underrättelse- och säkerhetstjänsten och den har ett övergripande nationellt ansvar för bl.a. säkerhetsskyddsfrågor. AIVD ingår i inrikesministeriet. MIVD är den militära underrättelse- och säkerhetstjänsten vars ansvar omfattar försvarsministeriets verksamhetsområde. Båda är informellt utsedda[26] som NSA, och AIVD har den samordnande rollen. De två tjänsternas uppgifter och befogenheter beskrivs i den ovan nämnda lagen om underrättelse- och säkerhetstjänsterna. Tjänsternas uppgifter avseende informationssäkerhet och klarering är enbart översiktligt beskrivna i lag.

[22] Denna princip gäller bl.a. i Norge generellt för förvaltningens beslut.
[23] På holländska: *Wet van 5 April 1951, houdende nadere voorzieningen met betrekking tot de bescherming van gegevens, waarvan de geheimhouding door het belang van de Staat wordt geboden*.
[24] *Algemene Inlichtingen- en Veiligheidsdienst*, Allmänna underrättelse- och säkerhetstjänsten.
[25] *Militaire Inlichtingen- en Veiligheidsdienst*, Militära underrättelse och säkerhetstjänsten.
[26] Detta tycks ha skett genom brevväxling under 1950-talet mellan premiärministern och CVD – en föregångare till AIVD.

Huvuddragen i regleringen

Lagen om skydd för statshemligheter är tämligen kortfattad och innehåller inte några egentliga bestämmelser om säkerhetsskydd. Den kan principiellt närmast jämföras med offentlighets- och sekretesslagen (2009:400) så till vida att den ger grunden för konfidentialitetsskyddet för uppgifter som hanteras av det allmänna. Vidare inne-håller den nederländska underrättelse- och säkerhetslagen[27] allmänt formulerade bestämmelser om vilka uppgifter AIVD har avseende säkerhetsskydd. Slutligen finns det bestämmelser om säkerhetsklarering i den särskilda säkerhetsundersökningslagen där det nederländska klareringsförfarandet regleras.

När det gäller *informationssäkerhet* är den huvudsakliga regleringen samlad i två författningar på förordningsnivå. Den ena från 2007 rör informationssäkerhet i allmänhet. I den läggs ansvaret på verksamheter i statsförvaltningen för att ta fram en informationssäkerhetspolicy och att värdera informationstillgångar utifrån perspektiven tillgänglighet, riktighet och sekretess. Bestämmelserna innehåller inte några konkreta säkerhetsskyddskrav. Förordningen kompletteras av ytterligare en förordning från 2013 som tar sikte på skyddet av uppgifter vars röjande kan medföra ett men för landets säkerhet (konfidentialitet). I denna förordning definieras en informationsklassificering i fyra nivåer utifrån det men som ett röjande av informationen kan medföra – *zeer geheim*, *geheim*, *konfidentieel* och *vertrouwelijk* (i fallande ordning). Därefter finns bestämmelser om vilka säkerhetsskyddsåtgärder som är tillämpliga för information på de olika nivåerna i fråga om säkerhetsanalys, skydd för utländska uppgifter samt åtgärder då uppgifter kan ha röjts. Förordningen innehåller även en bilaga med konkreta säkerhetsskyddsåtgärder för de olika nivåerna uppställt i tabellform. Bland åtgärderna finns behörighetsregler, fysiskt skydd, it-säkerhet och kommunikationssäkerhet.

Säkerhetsklareringen är som nämnt reglerad i en särskild lag om säkerhetsundersökning från 1996. Strukturen liknar därmed den i Finland och i viss mån Danmark med separata författningar avseende informationssäkerhet och säkerhetsklarering. Lagens

[27] WET van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten, 2002).

huvudsakliga innehåll rör genomförandet av säkerhetsklarering för befattningar som får tillgång till skyddsvärda uppgifter. För den lägsta informationsnivån (*vertrouwelijk*) krävs dock inte någon klarering utan enbart en allmän säkerhetsbedömning. Säkerhetsklareringen är indelad i tre nivåer (A, B och C). Nivå A avser befattningar som kräver behörighet till den högsta informationssäkerhetsnivån (*zeer geheim*). Lagen innehåller också bestämmelser för klarering av personer som behöver tillträde till flygplatser, även om dessa inte ska hantera känslig information. Bestämmelsen motsvarar närmast 14 § säkerhetsskyddslagen (skydd mot terrorism) som dock är vidare till sin tillämpning. I Nederländerna har en utvidgning av denna bestämmelse diskuterats bl.a. till att omfatta även personal vid hamnar. Även om Nederländerna tillämpar ett system med säkerhetsklarering, är bestämmelserna strikt knutna till befattning. Det åligger varje ministerium[28] att avgöra vilka befattningar inom den egna organisationen som kräver placering i säkerhetsklass, och det är enbart personer som avses att placeras på sådana befattningar som kan säkerhetsklareras.

Klareringsförfarandet inleds med vad som beskrivs som en administrativ utredning. Med utgångspunkt från ett frågeformulär kontrollerar AIVD den sökandes ekonomi och eventuell förekomst i polis- och belastningsregister. Uppgifterna avgränsas till de senaste åtta åren alternativt tio åren för den högsta klassen. En lagakraftvunnen dom som inneburit mer än 20 dagars fängelse, 40 dagars samhällstjänst eller 1 000 euro i böter medför med automatik att en klarering inte kan utfärdas. Om personen under en längre tid varit bosatt utomlands, görs kontroll med det aktuella landets säkerhetstjänst i de fall som det finns ett etablerat samarbete mellan Nederländerna och detta land. Svårigheter i att kontrollera den som har varit bosatt utomlands kan innebära att en klarering inte kan utfärdas. I klass B och C avgörs normalt ärendet enbart på dessa uppgifter. I klass A (och undantagsvis även i klass B) görs också referenstagning och intervjuer med den sökande. En intressant detalj är att AIVD alltid försöker att göra intervjuerna i den sökandes hem med syftet att få en mer naturlig dialog.

[28] Eftersom Nederländerna har ett ministeriesystem ingår även de underliggande myndigheterna i respektive ministerium, vilket medför att bestämmelsen tar sikte på hela statsförvaltningen.

Säkerhetsklareringen avslutas med ett intyg om att det inte finns några hinder för placering.[29] Ett negativt besked kan överklagas av den enskilde. Ärendet går först till en oberoende stiftelse – CAOP – som efter att ha hört parterna utfärdar ett icke-bindande förslag till beslut. Är den sökande inte nöjd med resultatet, kan beslutet från AIVD överklagas till domstol.[30]

Industrisäkerheten är liksom säkerhetsprövningen centrerade till utfärdandet av intyg – i detta fall avseende leverantörsklarering. Verksamheten är uppdelad på ett sådant sätt att MIVD ansvarar för leverantörsklareringarna från ett nationellt perspektiv och AIVD ansvarar för internationella intyg på förfrågan från andra länder och mellanfolkliga organisationer. Skälet till denna uppdelning uppges vara att leverantörsklareringarna till en övervägande del traditionellt har rört försvarsindustrin. Klareringen är projektspecifik och avslutas när ett projekt avslutas. Klareringen innebär att personer vid det aktuella företaget kan säkerhetsklareras och att företagets lokaler och anläggningar anses ha sådan säkerhet att klassificerad information kan hanteras där. MIVD har gett ut en anvisning i industrisäkerhet (2006) som riktar sig till företag som ska klareras.[31]

Utmärkande detaljer i regleringen

Säkerhetsklareringen i Nederländerna har detaljer i genomförandet som saknar motsvarighet i Sverige och i de övriga länderna som utredningen har studerat. För det första genomförs intervjuer i säkerhetsprövningen företrädesvis i den sökandes hem. Detta ger enligt uppgift till utredningen en mera avspänd miljö och även en större möjlighet att upptäcka eventuella sårbarheter. För det andra har säkerhetsklareringsintyget ett särskiljande drag. De flesta länder har intyg som specificerar en persons pålitlighet att hantera klassificerade handlingar upp till en viss nivå. I Nederländerna intygas i stället att det under klareringen inte har kommit fram några uppgifter som *motsäger* att den prövade är pålitlig att ta del av klassificerade handlingar upp till en viss nivå. Formuleringen tydliggör

[29] På nederländska ”*verklaring van geen bezwaar*”.
[30] Hur personklareringarna går till beskrivs vidare i avsnitt 18.4.
[31] ”*Algemene Beveiligingseisen voor Defensieopdrachten 2006*” (ABDO 2006).

att en pålitlighetsbedömning, oavsett ambitionsnivå, innefattar ett visst mått av osäkerhet.

8.2.2 Tjeckien

Allmänt om säkerhetsskydd i Tjeckien

Säkerhetsskyddet i Tjeckien regleras främst i lagen nr. 412 av den 21 september 2005 om skydd av klassificerad information.[32] Syftet med säkerhetsskyddet är att skydda information och verksamheter som är av betydelse för tjeckiska säkerhetsintressen. Tjeckien har sedan 1998 en central nationell säkerhetsmyndighet, *Národní bezpečnostní úřad* (NBÚ). Myndigheten har ansvar för säkerhetsskyddsfrågor såväl nationellt som i förhållande till andra länder och mellanfolkliga organisationer. Vi myndigheten finns huvuddelen av de funktioner som anges i internationella säkerhetsskyddsåtaganden. NBÚ har en stark ställning i Tjeckien och har befogenhet att utfärda böter för myndigheter som på olika sätt inte följer säkerhetslagstiftningen.

Huvuddragen i regleringen

Regleringen om säkerhetsskydd består av den nämnda lagen om skydd av klassificerad information och en rad tillhörande förordningar. Lagstiftningen har justerats vid ett par tillfällen. Detaljnivån i regleringen är genomgående hög och enbart lagen omfattar drygt 70 sidor. Lagens definition av vad som är föremål för lagstiftningen är förhållandevis vid och utgår från tjeckiska nationella intressen. Dessa specificeras till att upprätthålla grundlagarna, suveräniteten och den territoriella integriteten, att säkerställa intern ordning och säkerhet, att bevara internationella åtaganden och försvar, att skydda landets ekonomi och skydd av liv och hälsa. Genom hänvisningen till internationella åtaganden klargörs att regleringen ger ett skydd även för uppgifter som har klassificerats av annan stat eller mellanfolklig organisation. Lagen kompletteras

[32] På tjeckiska ”*zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti*”.

med en förordning som ämnesvis anger vilket slag av information som kan vara klassificerad samt på vilken nivå.

Den tjeckiska regleringen om säkerhetsskydd är, vilket tycks vara ett gemensamt drag i flera länder, tydligt uppbyggd utifrån behovet att skydda klassificerad information. En skillnad i förhållande till den svenska säkerhetsskyddslagen är avsaknaden av bestämmelser som riktar in lagstiftningen på skydd mot vissa antagonistiska hot. I stället ligger fokus på den skada som kan uppstå vid ett röjande av viss information samt vilka åtgärder som ska vidtas för att uppnå ett skydd för informationen.

Centralt när det gäller *informationssäkerhet* är att den klassificerade informationen indelas i en fyrgradig skala (i fallande ordning) *Přísně tajné, Tajné, Důvěrné och Vyhrazené* (i svensk översättning strängt hemligt, hemligt, konfidentiellt respektive restriktivt) utifrån en bedömning av den skada som kan uppkomma vid obehörigt röjande eller missbruk av informationen i fråga. Informationssäkerhetsbestämmelserna är uppdelade på olika kapitel som avser administrativ säkerhet, it- och kommunikationssäkerhet samt kryptografiskt skydd. Även kapitlet om fysisk säkerhet har som syfte att ge ett skydd för klassificerad information i byggnader och anläggningar.

Med *säkerhetsklarering* avses i den tjeckiska lagstiftningen förfarandet som syftar till att ge en fysisk person behörighet till klassificerad information. Förfarandet avslutas med att ett intyg om säkerhetsklarering utfärdas eller nekas. På den lägsta nivån (*Vyhrazené*) behövs inte någon klarering, men för behörighet till sådan information finns det ett grundläggande krav på att personen ska ha fyllt 18 år och ha full rättshandlingsförmåga. För de högre nivåerna ställs krav på tjeckiskt medborgarskap eller medborgarskap i en EU-medlemsstat eller i ett Natoland. Vidare ställs det krav på att personen är lämplig och pålitlig ur ett säkerhetsperspektiv. En person anses som lämplig om han eller hon inte har några personliga problem som kan påverka förmågan att upprätthålla sekretessen i hantering av information vilket t.ex. en sjukdom anses kunna göra. För lämplighetsbedömningen finns en möjlighet att förordna s.k. allmänna experter som läkare och psykologer vilka kan genomföra undersökningar och meddela utlåtanden. För att anses som pålitlig krävs att personen inte anses utgöra någon säkerhetsrisk. Som säkerhetsrisker anses personer som allvarligt

eller vid upprepade tillfällen har deltagit i verksamhet som hotar tjeckiska säkerhetsintressen eller som har deltagit i, eller på annat sätt stöttat, verksamhet som utgjort ett kränkande av mänskliga rättigheter. Lagen innehåller en riklig uppräkning på vad som kan ligga till grund för att en person kan anses utgöra en säkerhetsrisk. För den näst lägsta nivån (*Důvěrné*) ska händelser under den senaste tioårsperioden beaktas, för den näst högsta nivån (*Tajné*) händelser under de senaste 15 åren och för den högsta nivån (*Přísně tajné*) händelser under de senaste 20 åren. Om den sökande inte fyllt 15 år vid periodens början, gäller i stället den tid som gått från det att den sökande har fyllt 15 år fram till tiden för ansökan. Systemet för säkerhetsklarering i Tjeckien påminner om de i Norge och Nederländerna med såväl skriftliga som muntliga inslag, men med ett något större utrymme att genomföra samtal och intervjuer inom ramen för säkerhetsklareringen. Från den näst högsta nivån och uppåt görs det även en utredning som genomförs av landets polis- och säkerhetstjänster vilka är skyldiga att delge NBÚ sådan information som kan vara till nackdel för den enskilde. Ett negativt beslut om säkerhetsklarering kan överklagas. Det första steget är att NBÚ kan ompröva beslutet. Om myndigheten inte ändrar beslutet, går ärendet vidare till allmän domstol. NBÚ har dock lyft fram att denna process både är resurskrävande och leder till att rättstillämpningen är otydlig och kan ge olika besked i principiellt liknande fall. Det tjeckiska systemet tillåter såväl laglighets- som lämplighetsprövning.

När det gäller *industrisäkerhet* så fordras en giltig leverantörsklarering för företag som behöver få tillgång till information på den näst lägsta nivån och högre. För företag som endast kommer i kontakt med information på den lägsta nivån krävs ingen säkerhetsklarering utan det räcker med att företaget gör en anmälan till NBÚ. Företagsklareringar giltiga i maximalt nio år (för den näst lägsta nivån). Vid bedömningen om ett företag ska ges klarering tas hänsyn till företagets ekonomiska situation, förmåga att hantera och säkra klassificerad information och företagets säkerhetsmässiga pålitlighet. NBÚ ska neka klarering om företaget ägnat sig åt eller stöttat verksamhet som hotar tjeckiska säkerhetsintressen eller som strider mot mänskliga rättigheter. När det gäller industrisäkerhet har tjeckiska företag rätt att ansöka om klarering utan att det finns något affärsavtal som kräver detta. Det finns dock ett krav på att

minst en anställd på det aktuella företaget ska vara säkerhetsklarerad. Det tas för intäkt för att företaget bedriver någon verksamhet som är säkerhetskänslig. I praktiken är det dock förhållandevis enkelt att kringgå detta krav vilket har medfört att en hel del företag har en klarering utan att något egentligt behov finns. Att personklareringen måste vara på lägst samma nivå som den sökta företagsklareringen försvårar dock ett kringgående för de högre nivåerna. Det förekommer att företag i sin marknadsföring anger att de har en företagsklarering. NBÚ har mot denna bakgrund uttryckt att det vore önskvärt med en tydligare begränsning av företagsklareringarna, t.ex. genom en koppling till affärsavtal som innebär att leverantören får tillgång till klassificerad information. NBÚ tar ut en mindre avgift för företagsklareringar, men syftet med avgiften är något oklart eftersom den varken täcker de verkliga omkostnaderna eller verkar fungera avhållande gentemot företagen.

Utmärkande detaljer i regleringen

Den tjeckiska lagstiftningen utmärker sig i jämförelse med andra länder genom den stora samstämmigheten med EU:s och Natos säkerhetsregelverk. Detta redovisades vara en medveten strategi och möjligt för ett land som relativt sent blivit medlem i såväl EU som Nato. Lagstiftningen har en relativt vid definition av nationell säkerhet (vilken bygger på definitionerna i de olika internationella regelverken). Man har dock försökt att i någon mån snäva in begreppet genom att författningsreglera vilken information som ska klassificeras och på vilken nivå.

9 Hoten och de huvudsakliga förändringsfaktorerna

I direktiven och även i Säkerhetspolisens förstudierapport[1] betonas att hoten mot rikets säkerhet har förändrats sedan den tid då nu gällande säkerhetsskyddslagstiftning tillkom.

Även om begreppet rikets säkerhet inte är reserverat för förhållanden som har betydelse för totalförsvaret, har det i hög grad kommit att förknippas med framför allt militära förhållanden. Samtidigt har utvecklingen gått mot att andra för samhället viktiga verksamheter fått en allt större betydelse från säkerhetsskyddssynpunkt. Ett uttryck för detta är den förändring som hoten genomgått under de senaste tio åren. I förarbetena till säkerhetsskyddslagen konstaterades att hoten mot Sverige förändrats efter det kalla krigets slut. Trots det gjordes bedömningen att det nya säkerhetspolitiska läget inte hade inneburit några radikala förändringar av förutsättningarna för en ny säkerhetsskyddsreglering.[2] Det nya regelverket utarbetades mot den bakgrunden.

Sedan säkerhetsskyddslagen trädde i kraft har hoten mot rikets säkerhet ytterligare förändrats. Främmande staters underrättelseverksamhet har de senaste decennierna breddats mot forskning och utveckling inom civila områden samt mot politiska frågor och information som rör samhällsviktiga system. Elektroniska angrepp i olika former betraktas som ett av de allvarligare hoten. Antalet it-angrepp ökar i omfattning och blir allt mera riktade och sofistikerade. Samtidigt kvarstår underrättelsehotet mot militära förhållanden och mot information av betydelse för försvaret av Sverige,

[1] Säkerhetspolisens Förstudierapport Översyn av säkerhetsskyddslagen (AD001-8770-09).
[2] Säkerhetsskyddsutredningens betänkande Säkerhetsskydd (SOU 1994:149), s. 14 f.

något som blivit tydligt genom det försämrade säkerhetsläget i Östersjöregionen under 2014.

Sveriges uppfattning om säkerhetsläget nationellt och internationellt, hoten samt inriktningen på Sveriges försvar är frågor som påverkar synen på vad som är av betydelse för rikets säkerhet. Det kan i sin tur bidra till att ge en uppfattning om vilka verksamheter som är i behov av säkerhetsskydd. Lagstiftningen måste vara utformad så att den har förutsättningar att stå sig över tid och innehålla ett visst mått av flexibilitet så att den även kan möta morgondagens hot.

De förändringsfaktorer som tas upp i Säkerhetspolisens förstudierapport och i direktiven är i flera avseenden inte unika för Sverige utan gör sig gällande på motsvarande sätt i vår omvärld. Ytterligare faktorer att beakta är koncentrationen av uppdrag och tjänster på it-området till ett fåtal företag. Denna ökade koncentration till ett fåtal företag som tillhandahåller tjänster till myndigheter särskilt på it-området och som därmed får tillgång till stora mängder information kan medföra en ökad sårbarhet. Den samlade informationen kan bli mycket omfattande och kräver därför särskilda hänsyn från säkerhetsskyddssynpunkt.

I det här kapitlet tar vi avstamp i Sveriges nuvarande säkerhetspolitik (avsnitt 9.1). Därefter (i avsnitt 9.2) redogör vi för hoten mot Sverige som de bedöms i dag. Även om hotbilden inte nödvändigtvis ska ha en direkt påverkan på lagens utformning, är den ändå viktig för att avgöra vilka slag av hot som en ny lag ska ge ett skydd mot. Vidare redogör vi för hur vi ser på samhällsutvecklingen och de därmed sammanhängande förändringsfaktorer som bör påverka utformningen av lagen (avsnitt 9.3). Avslutningsvis ger vi några sammanfattande reflektioner över vad som bör styra innehållet och utformningen av en ny säkerhetsskyddslagstiftning (avsnitt 9.4).

9.1 Sveriges säkerhetspolitik

Som framgår av det följande har regeringen i olika sammanhang gett uttryck för den förändrade säkerhetspolitiken.[3]

Europa präglas i dag av ömsesidiga beroenden. Säkerhetspolitiska möjligheter och utmaningar som Sverige ställs inför delas i hög utsträckning av övriga Europa. Det går inte att föreställa sig en militär konflikt i vårt närområde som enbart skulle påverka ett land. Samarbetet inom EU intar en särställning i svensk utrikes- och säkerhetspolitik. Sambandet mellan Sveriges säkerhetspolitik och europapolitiken är uppenbar. Sveriges säkerhet stärks genom europeisk integration. Regeringen menar att det ligger i Sveriges intresse att genom nära samarbete stärka medlemsstaternas gemensamma säkerhet samtidigt som EU, genom att vara en effektiv säkerhetspolitisk aktör, kan verka för en fredlig och demokratisk utveckling i omvärlden.

Sveriges säkerhet byggs solidariskt tillsammans med andra. Hot mot fred och säkerhet avvärjs i gemenskap och samverkan med andra länder och organisationer. Medlemskapet i EU innebär att Sverige ingår i en politisk allians, där medlemsländer inte har försvarsförpliktelser i förhållande till varandra, men tar ett solidariskt ansvar för Europas säkerhet.

Sverige kommer inte att förhålla sig passivt om en katastrof eller ett angrepp skulle drabba ett annat medlemsland eller nordiskt land. Det förväntas att dessa länder agerar på samma sätt om Sverige drabbas. Sverige bör därför ha förmågan att kunna ge och ta emot militärt stöd. Målet för det militära försvaret ska vara att enskilt och tillsammans med andra, inom och utom landet, försvara Sverige och främja vår säkerhet.

Sveriges säkerhetspolitik utgår från en bred syn på säkerhet. Ett enskilt militärt väpnat angrepp direkt mot Sverige är osannolikt under överskådlig tid. Kriser och incidenter som även inbegriper militära maktmedel kan dock inte uteslutas i vår region och på längre sikt kan militära angreppshot likväl aldrig uteslutas. Utmaningar och hot mot Sveriges säkerhet är i dag föränderliga, gränslösa och komplexa. Tidigare syn på säkerhet utgick från stater och

[3] Detta avsnitt härrör från information om Sveriges säkerhetspolitik på regeringens webbplats, www.regeringen.se, den 27 februari 2015. Texten baseras på regeringens utrikesdeklarationer samt prop. 2008/09:140 Ett användbart försvar.

en militär hotbild. I ett vidgat säkerhetsbegrepp inryms även icke-militära hot och icke-statliga aktörer. Individens, vid sidan av staters, rättigheter och säkerhet ges stor betydelse.

Gränsöverskridande samarbete, handel och integration främjar en positiv utveckling i stora delar av världen. Globalisering kan dock också innebära ökad sårbarhet genom att enskilda händelser snabbt kan få regionala eller globala återverkningar. I detta ligger en ökad sårbarhet mot säkerhetshot som terrorism, spridning av massförstörelsevapen, organiserad brottslighet, pandemier och miljökatastrofer.

Dagens hot och utmaningar är i hög grad gränsöverskridande. Säkerhet uppnås därför gemensamt och genom nära samarbete med andra länder. Sverige är en aktiv och solidarisk partner i arbetet för stabilitet och säkerhet i Europa och omvärlden. Sveriges bidrag till krishanteringsinsatser under EU:s, FN:s och Nato:s ledning leder till ökad säkerhet.

Vidare är även en stark transatlantisk länk av vital betydelse för Sveriges och hela Europas stabilitet och säkerhet. Nato är en central aktör för europeisk säkerhet och integration samt för internationell krishantering. Sveriges samarbete med Nato och USA är ett uttryck för viljan att vara en del av och stärka den transatlantiska säkerhetspolitiska gemenskapen.

För Sverige är säkerheten och samarbetet i vårt närområde av särskild betydelse. Det nordiska samarbetet inom det säkerhetspolitiska området fördjupas och utvidgas. Det ligger i Sveriges intresse att åstadkomma effektiva samverkanslösningar och ett fördjupat samarbete med de nordiska länderna. Norden har i sammanhanget också ett utvecklat samarbete med Estland, Lettland och Litauen. Regeringen ser detta som ett komplement till och en naturlig utveckling av de europeiska och euroatlantiska samarbetena. Nordiskt försvarssamarbete är inte ett självständigt säkerhetspolitiskt alternativ.

Ryssland är Sveriges största grannland och en central säkerhetspolitisk aktör i vårt närområde, Europa och den större omvärlden. Rysslands partnerskap med EU och samverkan med Nato, liksom dess integration i den globala ekonomin, är av stor säkerhetspolitisk betydelse för Östersjöregionen och hela Europa.

9.2 De aktuella hoten mot Sverige

Hotens betydelse

Som framgår av föregående avsnitt har svensk säkerhets- och försvarspolitik förändrats under senare år. Hur stort hotet är värderas emellertid inte. Vi har därför inhämtat särskild information om bl.a. aktuella hot och tendenser från Säkerhetspolisen och Försvarsmakten. Utredningen har också tagit del av annan relevant information som publicerats på Säkerhetspolisens, Försvarsmaktens och Försvarets radioanstalts webbplatser på internet.

Som vi har anfört i inledningen till detta kapitel får hoten inte bli någon allenarådande styrning av hur en säkerhetsskyddslag bör utformas. Tvärtom bör en sådan lag för att kunna vara ändamålsenlig och relevant under en längre tid vara tämligen okänslig för förändringar i hotbilden. Hotbeskrivningen tjänar dock som en viktig redogörelse av vilka slag av hot det kan vara fråga om och således *mot vad* en säkerhetsskyddslag ska ge ett skydd.

Nya hot mot säkerheten

Den nuvarande säkerhetsskyddslagstiftningen kom till i en brytningstid. Det bedömdes att det nya säkerhetspolitiska läget inte hade inneburit några radikala förändringar av förutsättningarna för en ny säkerhetsskyddsreglering, och det nya regelverket utarbetades mot den bakgrunden. Utredningen[4] som föregick den nuvarande säkerhetsskyddslagstiftningen var primärt inriktad på regleringstekniska frågor rörande personalkontroll. Genom tilläggsdirektiv[5] kom utredningens uppdrag att omfatta även en översyn av förordningen (1981:421) om säkerhetsskyddet vid statliga myndigheter. Någon mer ingående analys av vilka behov i övrigt som fanns av en säkerhetsskyddsreglering gjordes inte (se vidare avsnitt 3.2).

Säkerhetsskyddslagen är i första hand inriktad på att skydda rikets säkerhet. Även om begreppet rikets säkerhet inte är reserverat för förhållanden som har betydelse för totalförsvaret, har det i hög grad kommit att förknippas med det och framför allt då med

[4] Säkerhetsskyddsutredningen (SOU 1994:149).
[5] Dir. 1993:123.

militära förhållanden. Samtidigt har utvecklingen gått mot att även andra samhällsviktiga verksamheter fått en allt större betydelse från säkerhetsskyddssynpunkt. Även om ett militärt angreppshot inte kan uteslutas på längre sikt, görs numera en annan bedömning av hoten mot säkerheten i Sverige.

Aktuella hot

De hot som i dag bedöms kunna få konsekvenser för Sveriges säkerhet är alltså av delvis annan karaktär än tidigare. Numera utgörs hoten av t.ex. internationell terrorism, andra typer av grov internationell brottslighet, spridning av massförstörelsevapen samt framställning och transport av vapen, komponenter och teknologi.

Civila verksamheter har på ett helt annat sätt än tidigare kommit att stå i fokus. Främmande staters underrättelseverksamhet har breddats mot forskning och utveckling inom civila områden samt mot politiska frågor och information som rör samhällsviktiga system. Utvecklingen med utflyttning av väsentliga funktioner i samhällsviktig verksamhet till utlandet, t.ex. inom energiförsörjningen, har också inneburit att sårbarheten har förändrats. Elektroniska angrepp i olika former har kommit att bli ett av de allvarligaste hoten.

Informationsteknikens utveckling ger ökade möjligheter till att subversivt påverka den dagliga informationsbilden för samhällets invånare. Det finns exempel på att främmande makts underrättelsetjänster har förmåga att automatiserat och i stor omfattning påverka innehållet i sociala media. Enligt *Säkerhetspolisen* pågår i dag politisk, ekonomisk, militär och teknisk-vetenskaplig underrättelseverksamhet samt flyktingspionage. Målen som främmande makts underrättelsetjänster visat intresse för är bl.a. statsledningen, myndigheter, försvar, forskning och industri samt oppositionella och utländska intressen. Underrättelseinhämtningen sker med hjälp av mänskliga källor, elektroniska angrepp, signalspaning, flyg- och satellitspaning, öppna källor m.fl. metoder. Säkerhetspolisen anser att ett av de i dag allvarligaste tekniska inhämtningshoten utgörs av elektroniska angrepp. Det är framför allt de tre miljöfaktorerna digitalisering, globalisering och outsourcing som påverkar riskbilden och som underlättar eller skapar nya förutsättningar för

hot. När det gäller terrorism konstaterar Säkerhetspolisen, utifrån andra länders erfarenheter att det finns exempel på såväl attentatsplanering och genomförda attentat som hot mot transporter, rättsväsende och annan myndighetsutövning. Hoten emanerar framför allt från våldsfrämjande islamister.

Enligt *Försvarsmakten* utgörs de potentiella hoten mot Sverige och Försvarsmakten numera i allt större utsträckning av annan säkerhetshotande verksamhet än konventionella stridskrafter. Försvarsmakten har sedan några år tillbaka noterat ett ökat intresse från främmande makts underrättelsetjänst riktat mot svensk försvarsförmåga, försvarspolitik, forskning och teknikutveckling samt Sveriges förhållanden till andra nationer och organisationer. Den tekniska utvecklingen i form av bl.a. dator- och nätverksattacker för att utnyttja samhällets beroende av informationsteknologi för att åstadkomma skada på såväl civila som militära kritiska funktioner gör Försvarsmakten sårbar för t.ex. sabotage. Privatiseringen av traditionellt sett statliga verksamheter i kombination med Försvarsmaktens ökade nyttjande av civil teknik och privatägd infrastruktur ger främmande makt nya möjligheter att inhämta information om och påverka nationella skyddsvärden av strategisk betydelse. Främmande underrättelseaktörers möjlighet att inhämta information som i Sverige betraktas som öppen kan också utgöra underlag i militär planering mot svenska mål. Hotet avseende terrorism riktad mot Försvarsmakten har ökat på senare tid. Enligt Försvarsmakten påverkas terrorhotbilden av Försvarsmaktens verksamhet, t.ex. i samband med internationella insatser, och våldsfrämjande islamistiska aktörer har sannolikt avsikten att angripa mål i Sverige eller att attackera svenska intressen utomlands.

På informationssäkerhetsområdet konstaterar *Försvarets radioanstalt* att det finns ett reellt hot mot Sverige och svenska intressen. Enligt Försvarets radioanstalt utförs it-angrepp ständigt, och de kommer från resursstarka och kunniga aktörer som har uttalade mål och syften med sina angrepp. Det kan vara underrättelseinhämtning, ekonomisk brottslighet, industrispionage och olika former av påverkan. Försvarets radioanstalt anser att det finns kunskap om hur informationsteknik kan användas för att orsaka skada och att denna kunskap är ett växande hot. Hotet riktar sig främst mot samhällsviktig verksamhet och kritisk infrastruktur. Många terrorgrupper har etablerat sin närvaro på internet. It-angreppen

blir alltmer sofistikerade och riktade. Antagonistiska aktörer utnyttjar samhällets sårbarheter på ett systematiskt sätt. Enligt Försvarets radioanstalt beror dock hotbilden också på omvärldshändelser och på hur Sverige och svenska medborgare agerar i olika sammanhang.

9.3 Förändringsfaktorerna

9.3.1 Informationstekniken

Allmänt

Sedan säkerhetsskyddslagen trädde i kraft har informationstekniken och användningen av den genomgått en betydande utveckling. Bland annat internet har radikalt förändrat förutsättningarna för informationssäkerhetsarbetet. Informationstekniken genomsyrar i dag i stort sett alla aspekter av samhällsviktiga verksamheter, och fungerande it-system är nödvändiga för att t.ex. styrning av el- och vattenförsörjning samt kommunikationssystem ska fungera.

När säkerhetsskyddslagen infördes förekom sekretessbelagda uppgifter som rörde rikets säkerhet främst i pappersdokument. Numera hanteras mycket stora informationsmängder, såväl öppna som hemliga, i it-system. En rad verksamheter, både hos det allmänna och inom näringslivet, är helt beroende av digitala system för bl.a. styrning, reglering och övervakning. Eftersom bestämmelserna om informationssäkerhet i säkerhetsskyddslagen är inriktade uteslutande på att skydda uppgifter som omfattas av sekretess och som rör rikets säkerhet ger lagen små möjligheter att vidta åtgärder för att skydda it-systemen som sådana. Ett behov av att skydda systemen är i dag påtagligt inom vissa för samhället kritiska sektorer bl.a. elförsörjningen.

Teknikutvecklingen och it-samhället innebär också i andra avseenden ändrade förutsättningar för säkerhetsskyddet. Som exempel kan nämnas möjligheter till ett flexibelt arbetssätt med mobila kontorslösningar i form av bärbara datorer, smarta mobiltelefoner och s.k. molntjänster vilket försvårar arbetet med säkerhetsskyddsåtgärder. Tillgången till och öppenheten kring stora mängder av information på t.ex. myndigheters webbplatser kan ge användaren

nya möjligheter att söka och sammanställa denna information på ett sätt som skulle kunna få konsekvenser för säkerhetsskyddet.

Även internationaliseringen har påverkat förutsättningarna för informationssäkerheten. Det gäller t.ex. i samband med utflyttning av verksamhet till utlandet, bl.a. inom energiförsörjningen.

Behovet av en god informationssäkerhet

Lite förenklat kan sägas att digitaliseringen tog fart samtidigt som säkerhetsskyddslagen trädde i kraft. Det var först vid mitten av 1990-talet som internet slog igenom på allvar i Sverige och antalet internetuppkopplingar började öka. Härefter har det skett en enorm utveckling på it-området och Sverige är i dag en ledande it-nation. Förutom att it har stor betydelse för svensk ekonomi bidrar den till att förbättra och förenkla tillvaron för alla; medborgare, företag, organisationer och offentlig sektor. Utvecklingen går snabbt, och digitaliseringen förändrar och påverkar alla delar av samhället. Informationstekniken gör det möjligt att bl.a. lagra stora mängder information och kunskap som snabbt, även globalt, kan göras tillgänglig för alla. Den utbredda digitaliseringen, främst av viktiga samhällsfunktioner, medför effektivitetsvinster och en ökad öppenhet, tillgänglighet och insyn. Samtidigt medför digitaliseringen en påtagligt ökad sårbarhet för störningar och avbrott. Den ökade öppenheten medför t.ex. större risk för att aktörer med antagonistiska avsikter utnyttjar de möjligheter som den brett åtkomliga informationen ger för hot och angrepp. Öppenheten kräver också att den information som görs tillgänglig inte kan förvanskas. Skyddet av de egna informationstillgångarna blir därför en grundläggande fråga för snart sagt varje privatperson och för större aktörer i många fall en ren överlevnadsfråga. Det är därför av grundläggande betydelse att infrastrukturen med väl fungerande elektroniska kommunikationer är tillgänglig, robust och säker.

Informationssäkerhetsområdet blir allt viktigare i takt med den tekniska utvecklingen och de sårbarheter som härmed skapas. En av informationssäkerhetsområdets stora utmaningar är att tekniken ofta utvecklas betydligt snabbare än säkerhetsarbetet. Den snabba utvecklingen på it-området i kombination med myndigheternas ökande nyttjande av civil teknik och privatägd infrastruktur medför

att myndigheternas egna tekniska kompetens minskar. Bristande kontroll över vilka it-produkter som tas in i svensk infrastruktur kan ge nya möjligheter för olika aktörer att inhämta information om och påverka nationella skyddsintressen och tillgångar av strategisk betydelse.

I dag betraktar de flesta länder informationssäkerhet som en stor nationell utmaning, och informationssäkerhet inklusive cybersäkerhet anses vara av såväl strategisk som utrikespolitisk och säkerhetspolitisk betydelse.

En storskalig it-incident bedöms i dag kunna få allvarliga konsekvenser såväl för ekonomisk som för samhällsviktig verksamhet och kritisk infrastruktur. På grund av samhällets ökade it-beroende är sannolikheten stor att samhällsviktiga system som finansiella system, ledningscentraler för trafiksystem, administrativa och medicinska system inom sjukvården, digitala kontrollsystem för el och vatten samt elektroniska kommunikationer drabbas.

Informationssäkerhet kräver i dag en helhetssyn eftersom det är ett komplext och gränsöverskridande område, såväl geografiskt som vad avser bl.a. teknik, administration, ekonomi och juridik. Den internationella dimensionen är också påtaglig. Dels för att informationsinfrastrukturen i dag är sammanflätad och korsar nationsgränser, dels därför att många privata företag som driver och äger infrastrukturen är verksamma i flera länder. Störningar i informationssystem kan snabbt röra sig mellan nationell och internationell nivå.

Lagring av stora mängder uppgifter i digitala system har ökat kraftigt och fortsätter öka närmast lavinartat i takt med ökade tekniska möjligheter och ökade ambitioner i samhället. Sammanställningar över t.ex. känsliga anläggningar och objekt kan snabbt och enkelt tas fram genom effektiva sökmotorer. Effekten av detta kan bli att uppgifter, som var för sig inte är skyddsvärda, i aggregerad form kan komma att utgöra en stor sårbarhet.

Vissa verksamheter tillhandahåller så väsentliga tjänster att, om deras funktionalitet kraftigt reduceras eller upphör, såväl den enskildes hälsa och liv som möjligheten att värna samhällets grundläggande värden riskeras. Som exempel på verksamheter som levererar tjänster som krävs för ett fungerande samhälle kan nämnas energiförsörjningen, elektronisk kommunikation, vattenförsörjning, hälso- och sjukvård samt betalningsväsendet. Flera av dessa

viktiga funktioner styrs och övervakas numera med hjälp av avancerade it-system. Beroendeförhållanden är en viktig orsak till att samhällsviktiga verksamheter är sårbara. Kritiska beroendeförhållanden uppstår i de fall då funktionen i en samhällsviktig verksamhet kräver att en annan verksamhet fungerar där denna saknar alternativ. Ett exempel på ett sådant förhållande är beroendet mellan el och elektroniska kommunikationer.

Ett annat problem som kan liknas vid ett beroendeförhållande är att det finns en pågående koncentration av it-drift till ett litet antal stora leverantörer som skapar nya sårbarheter i samhället. En incident i april 2013, då en operatör hade ett stort nätverksfel som bl.a. drabbade ett kommunikationsnät inom vård och omsorg medförde även konsekvenser för medieföretag, kommuner och andra myndigheter. En incident vid ett it-driftleverantör i november 2011,[6] då företaget drabbades av ett tekniskt fel kom att få konsekvenser för cirka 50 av företagets kunder inom såväl privat som offentlig sektor. Dessa exempel visar tydligt på problemet med koncentration och ömsesidiga beroenden. När ett tekniskt fel inträffar kan det påverka flera delar av samhället samtidigt och konsekvenserna kan därför bli svåra att överblicka.

Ett ytterligare exempel som illustrerar problematiken med beroendeförhållanden och koncentration är att Försvarsmakten i högre utsträckning än tidigare har kommit att förlita sig på samma kritiska infrastruktur och samhällsfunktioner som landet i övrigt. Detta gör Försvarsmakten till vissa delar lika sårbar för sabotage som övriga samhället.

Myndigheternas arbete på informationssäkerhetsområdet

Det bedrivs i dag ett brett nationellt, men också internationellt, arbete med informationssäkerhet där många aktörer samverkar.[7] Bland annat analyserar och utreder Säkerhetspolisen de allvarliga elektroniska angrepp som drabbat och drabbar de samhällsviktiga verksamheterna. Även den militära underrättelse- och säkerhets-

[6] Myndigheten för samhällsskydd och beredskaps rapport Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter – En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011.
[7] Se även avsnitt 7.4.

tjänsten (MUST) har särskilda kunskaper om och tillgång till unik information på informationssäkerhetsområdet.

Flera myndigheter är verksamma inom informationssäkerhetsområdet med stöd av även andra författningar än säkerhetsskyddslagen. Särskilt kan nämnas Myndigheten för samhällsskydd och beredskap som har i uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet. Myndigheten ska svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Myndigheten beslutar också om vissa andra myndigheters och företags tillgång till säkra kryptografiska funktioner.

9.3.2 Avreglering och konkurrensutsättning av samhällsviktig verksamhet

Avregleringarna på 1990-talet, då bl.a. el- och telekommunikationsmarknaderna avreglerades, ledde till förändrade ansvarsförhållanden för flera samhällsviktiga verksamheter. Avregleringen hade inte hunnit få något större genomslag när säkerhetsskyddslagstiftningen utformades. I dag finns en övervägande del av de verksamheter som är viktiga för det svenska samhällets funktionalitet inte under direkt statligt inflytande. Verksamheten drivs och förvaltas i stället av privata företag. Även utländskt ägande eller inflytande är numera en realitet inom samhällsviktiga verksamheter. För de företag som driver och förvaltar verksamheter som är viktiga för samhällets funktionalitet finns prioriteringar som t.ex. ägarstyrning, vinstintressen och kostnadsbesparingar som kan komma att stå i motsats till säkerhetsarbete. Sådana prioriteringar kan hämma eller rent av motverka det interna säkerhetsskyddsarbetet.

Av effektivitetsskäl och ekonomiska skäl väljer eller åtminstone överväger många verksamheter i dag åtgärder som outsourcing och offshoring när det gäller utveckling eller hantering av säkerhetskänsliga it-system.

Outsourcing, eller utkontraktering av tjänster, är när en extern aktör utför utvecklings-, underhålls- eller driftsarbete av system. Outsourcing kan ofta innebära att flera kunders system och information blandas samman i fysiska datasystem vilket innebär att olika kunders data kan hamna i samma lagringsmiljöer, routrar och brandväggar. Av kostnadsskäl väljer leverantören inte sällan lös-

ningar som leder till att system förs samman och virtualiseras. Det innebär att en kunds externa webbserver kan placeras på samma server som en annan kunds interna databasserver vilket kan medföra en ökad risk då en störning i ett kundsystem kan orsaka störningar även i andra kunders system. Vilka rättigheter personalen har att komma åt kunders information, hur stor omsättning leverantören har på sin personal och i vilken utsträckning man använder sig av konsulter är frågor som kunden, dvs. myndigheten eller företaget inte har någon insyn i eller kontroll över när det gäller outsourcing. Som nämnts inledningsvis i detta kapitel kan outsourcing, när en stor mängd information från olika myndigheter och företag hamnar hos en enda leverantör, riskera att bli en central punkt för t.ex. andra länders underrättelseinhämtning.

Offshoring är när outsourcing sker till en aktör i ett annat land. För svenska myndigheter innebär offshoring att svenska staten riskerar en sämre kontroll över samhällsviktiga system eftersom möjligheterna att säkerhetspröva personal och utnyttja svenska kontrollinstrument är mycket begränsade när verksamheten bedrivs i utlandet. Det är dessutom svårare för svenska myndigheter att bedöma hoten i de länder till vilka man har utkontrakterat verksamhet. Om det internationella säkerhetsläget förändras, vilket kan gå snabbt, saknas i värsta fall såväl kompetens som kapacitet och tid för att kunna flytta hem verksamheten till Sverige.

I takt med avregleringar och konkurrensutsättningar av offentlig verksamhet har det område inom vilket säkerhetsskyddsregelverket inte är tillämpbart kommit att öka alltmer.

9.3.3 Internationaliseringen

Allmänt

Globaliseringen och det ökade internationella samarbetet har medfört att gränserna för vad som är att hänföra till rikets inre respektive rikets yttre säkerhet har ändrats, liksom att begreppet nationell säkerhet har utvidgats. Vidare deltar Sverige i stor omfattning i internationella samarbeten för fred och säkerhet där känsliga uppgifter utbyts mellan länder och mellanfolkliga organisationer.

Effekten av globaliseringen avspeglas också på hotsidan. Dagens hot är gränsöverskridande och uppvisar en stor komplexitet genom att angreppen utförs genom medverkan från aktörer i olika länder.

En annan effekt av internationaliseringen är den reglering som utarbetas inom främst EU och som Sverige aktivt medverkar till att utforma och som syftar till att motverka allvarliga hot och risker inom olika sektorer.

En ökad internationell samverkan

Sambandet mellan skyddet av Sveriges säkerhet och skyddet av säkerhetsintressen hänförliga till andra stater och mellanfolkliga organisationer har förstärkts sedan säkerhetsskyddslagen infördes. Det är i dag i förhållande till säkerhetsintressen i omvärlden svårare att dra en gräns för vad som utgör svenska säkerhetsintressen. Sveriges säkerhet byggs solidariskt tillsammans med andra länder med gemensamma demokratiska värderingar, och vår säkerhet stärks genom förtroendeskapande åtgärder, genom gemensam krishantering samt genom aktiva och trovärdiga bidrag till nordisk, europeisk och global säkerhet. Landets säkerhet kan inte värnas enbart vid vår gräns, och en ökad samverkan med andra länder innebär bättre förutsättningar att hantera utmaningar och hot innan de når vårt eget territorium.

Ett närmare samarbete med andra stater och mellanfolkliga organisationer har medfört att det skyddsvärda området i dag i större utsträckning innefattar uppgifter som inte direkt berör svenska säkerhetsintressen. Behovet av att skydda hanteringen av uppgifter kan, t.ex. i samband med internationella militära insatser omfatta uppgifter som primärt rör en annan stats, EU:s eller annan mellanfolklig organisations säkerhetsintressen.

Den ökade samverkan med andra länder har vidare inneburit ett växande behov av att anpassa säkerhetsskyddet till åtaganden som följer av folkrättsliga förpliktelser. Sverige har bl.a. ingått generella säkerhetsskyddsavtal (GSA) med ett trettiotal länder. Tillämpningen av avtalen berör till övervägande del försvarssektorn och mer explicit internationella försvarsmaterielsamarbeten, internationella militära insatser och internationellt försvarssamarbete. Säkerhetsskyddsavtalen har dock utvecklats över tiden från att avse

enbart försvarshemliga uppgifter i försvarssektorn till att numera avse hemliga uppgifter i säkerhetsskyddslagstiftningens mening (respektive utländska motsvarigheter) i ett mer övergripande nationellt perspektiv. Säkerhetsskyddsavtal har också ingåtts med flera mellanfolkliga organisationer bl.a. Nato. Avtalen innebär ett ömsesidigt åtagande att skydda hemliga uppgifter som utbyts mellan avtalsparterna.[8]

Det finns en klar överlappning mellan för nationen övergripande säkerhetsintressen och näringslivets intressen av säkerhetsskydd inom det försvars- och säkerhetsrelaterade området. Som regeringen har framhållit[9] är det ett väsentligt säkerhetsintresse att materielförsörjningen inom försvaret, t.ex. i samarbete med andra länder och organisationer, kan garanteras. Det intensifierade internationella samarbetet både inom försvarssektorn och inom den civila sektorn medför behov av anpassning till internationellt gångbara säkerhetsskyddsåtgärder.

9.3.4 Ett bredare arbete för att stärka säkerheten i samhället

Framväxten av närliggande reglering

Det breda arbetet med samhällets skydd och beredskap hos myndigheter, kommuner och landsting har tagit fart under senare år. Det gäller inte bara informationssäkerhet. Hot, risker och sårbarheter av olika slag samt kritiska beroenden ska identifieras och värderas. Inom den privata sektorn finns andra starka incitament än lagstiftning (t.ex. konkurrens och skydd av företagshemligheter) som driver på det interna säkerhetsarbetet.

Vid tiden för säkerhetsskyddslagens tillkomst var sektors- och ämnesspecifik reglering på säkerhetsområdet inte så vanlig. Åtgärder mot allvarliga säkerhetshot vidtas dock numera i allt större utsträckning med utgångspunkt i olika regelverk, såväl övergripande som sektorsvisa, som ställer krav på skyddsåtgärder. Sådana närliggande regelverk har i en stor utsträckning arbetats fram inom EU eller i andra internationella sammanhang.[10]

[8] För en mer utförlig beskrivning av internationella säkerhetsskyddsavtal och reglering till skydd för uppgifter, se kapitel 6.
[9] Prop. 2010/11:150 Upphandling på försvars- och säkerhetsområdet Del 1, s. 130.
[10] Se vidare kapitel 5 om närliggande reglering.

Säkerhet är dock i sig ett brett begrepp som relaterar till behovet av att skydda mot hot av olika slag, såväl aktörs- som miljöbetingade. Säkerhet i sin bredaste bemärkelse tar sikte på att förebygga och hantera hot som kan innefatta risker för såväl olyckor, naturfenomen, oavsiktligt handlande som antagonistiska hot, dvs. ett avsiktligt handlande. I andra sammanhang relateras begreppet säkerhet till ett skydd som är inriktat mot hot av ett visst slag, t.ex. olyckor och oavsiktligt handlande respektive antagonistiska hot.

I det engelska språket finns en distinktion mellan ”safety” och ”security”. Det förstnämnda begreppet tar sikte på skydd mot olyckor, naturfenomen och oavsiktligt handlande medan ”security”, är tydligt kopplat till skydd mot någon form av antagonistiskt hot. Svenska språket har inte någon motsvarande distinktion vilket också återspeglas i regleringar som avser säkerhet i dess olika bemärkelser. För säkerhetsskyddslagen som tar sikte på att skydda Sveriges säkerhet mot antagonistiska hot används det centrala uttrycket säkerhetsskydd.

I vissa avseenden kan ett säkerhetsskydd ge skydd även i ett ”safetyperspektiv”. Sådan samverkande effekt finns t.ex. vid anskaffning av robust elektronisk kommunikation. Med robusthet menas i detta sammanhang förmågan att motstå störningar och avbrott samt förmågan att minimera konsekvenserna om de ändå inträffar. Tillgång till reservsystem och alternativa driftmiljöer är åtgärder med avseende på robusthet. För andra skyddsåtgärder t.ex. byggnadstekniska åtgärder kan gälla att de ger skydd endast mot ett mer specifikt slag av hot, t.ex. skydd mot miljöpåverkan och naturfenomen. Sådana åtgärder saknar därför relevans för säkerhetsskyddet.

Informationssamhället och förhållandet mellan ”safety” och ”security”

En avgörande skillnad mellan säkerhet i bemärkelserna ”safety” respektive ”security” är utgångspunkterna för hur ett effektivt skydd kan uppnås. För skyddsåtgärder som vidtas från ett ”safetyperspektiv” är den naturliga utgångspunkten öppenhet kring åtgärderna. Öppenheten kring t.ex. placering av kritiska funktioner i en verksamhet kan vara en förutsättning för ett effektivt skydd mot oavsiktlig påverkan. I fråga om skyddsåtgärder som vidtas från ett

”securityperspektiv” är utgångspunkten ofta den motsatta. Öppenhet kring skyddsåtgärder är i regel kontraproduktivt. Att öppet tala om sårbarheter inom området "safety" kan få en oönskad påverkan på "security-området”. Vidare kan öppen information när den digitaliseras delas och spridas på ett sätt som inte går att kontrollera. En särskild utmaning i dag är därför att uppnå ett effektivt skydd i samhällsviktiga verksamheter, t.ex. kritiska funktioner inom elförsörjningen som behöver skyddas mot såväl olyckor och naturkatastrofer som mot antagonistiska hot. Detsamma gäller för skydd avseende potentiellt skadegenerande verksamhet inom t.ex. kärnkraftsindustrin.

Det finns i dag ett flertal regelverk – bl.a. utarbetade inom EU och i andra internationella sammanhang – som syftar till att motverka allvarliga hot och risker inom olika sektorer. Det har framför allt ur ett ”safetyperspektiv” vuxit fram en tämligen omfattande EU-rättslig reglering som tar sikte på att skydda mot olika former av potentiellt skadegenererande verksamheter. Sverige har t.ex. genom lagen (2010:1767) och förordningen (2010:1770) om geografisk miljöinformation genomfört det s.k. Inspiredirektivet.[11] Lagstiftningen syftar till att etablera en fungerande infrastruktur för tillgång till och utbyte av geografisk information som är användbar för verksamheter och åtgärder som kan påverka människors hälsa eller miljön (geografisk miljöinformation). Myndigheter, kommuner och vissa enskilda organ som har geografisk miljöinformation och informationshanteringstjänster ska medverka i det nya systemet genom att göra informationen och tjänsterna tillgängliga för allmänheten samt dela information med andra myndigheter, kommuner och enskilda organ som fullgör offentliga förvaltningsuppgifter som kan ha betydelse för miljön. Lantmäteriet har getts i uppgift att samordna den svenska infrastrukturen för tillgång till och utbyte av geografisk miljöinformation samt utveckla en portal på internet, den så kallade Geodataportalen.

Under arbetet med lagstiftningen om geografisk miljöinformation anförde Försvarsmakten att lagstiftningen riskerade att undergräva det skydd som bestämmelserna om sekretess och skydd för

[11] Europaparlamentets och rådets direktiv 2007/2/EG av den 14 mars 2007 om upprättande av en infrastruktur för rumslig information i Europeiska gemenskapen, EUT L 108, 25.4.2007, s. 1 (Celex 32007L0002).

landskapsinformation gett olika typer av information som omfattas av den föreslagna lagstiftningen. Säkerhetspolisen framförde liknande synpunkter. Regeringens bedömning var dock att skyddet för landskapsinformationen inte undergrävdes utan konstaterade att merparten av den geografiska miljöinformation som omfattas av lagen utgör landskapsinformation och att de informationsansvariga därför måste ha tillstånd enligt lagen (1993:1742) om landskapsinformation för att få tillgängliggöra informationen.[12] I 15 § lagen om geografisk miljöinformation fördes in en hänvisning till bl.a. säkerhetsskyddslagen och lagen om skydd för landskapsinformation.[13]

Lagstiftningsärendet illustrerar de intressekonflikter som i dagens informationssamhälle kan finnas i fråga om krav på öppenhet från ett ”safetyperspektiv” och krav på hemlighållande från ett ”securityperspektiv”. Ett exempel på hur en sådan konflikt kan lösas är portalen Ledningskollen (en webbtjänst som underlättar kommunikation mellan ägare av nedgrävd infrastruktur i form av olika ledningar och de som har ett berättigat behov av att veta var dessa finns) som med hänvisning till ”safety-kravet” ska ge information och underlag utan att stå i motsättning till kravet på hemlighållande av sekretessbelagd information från ett ”securityperspektiv”.

9.4 Sammanfattande reflektioner

Som vi återkommer till i kapitel 10–12 tar den första huvudfrågan som anges i utredningens direktiv – att bättre anpassa lagstiftningen till det som krävs för att skydda verksamhet som har betydelse för rikets säkerhet – sikte på det primära syftet med säkerhetsskyddet. Reformbehovet av säkerhetsskyddslagstiftningen ger därmed upphov till flera frågor. Först och främst den mer övergripande frågan *vad* som ska skyddas, och den därmed korresponderande frågan *mot vad* ett skydd behövs. Vidare de anslutande frågorna *hur* skyddet ska säkerställas, dvs. frågan om säkerhetsskyddsåtgärdernas tillämpningsområde och innehåll, samt *av vem*

[12] Prop. 2009/10:224 Ett sammanhängande system för geografisk miljöinformation, s. 71 f.
[13] En redogörelse för lagen om skydd för landskapsinformation finns i avsnitt 5.3 och en redogörelse för relevanta sekretessbestämmelser i avsnitt 4.2.

nödvändiga säkerhetsskyddsåtgärder ska vidtas. Samtliga dessa frågor berörs av de ändrade förutsättningarna för säkerhetsskyddet som vi redogjort för.

Säkerhetsskyddslagen är i första hand inriktad på att skydda rikets säkerhet. Vid säkerhetsskyddslagens tillkomst var det huvudsakliga syftet, skyddet av rikets säkerhet, i hög grad förknippat med framför allt militära förhållanden. Med hänsyn till att utvecklingen gått mot att andra samhällsviktiga verksamheter har fått en allt större betydelse från säkerhetssynpunkt har frågan *vad* som ska skyddas hamnat i förgrunden. Hoten mot rikets säkerhet har förändrats, säkerhetsbegreppet har vidgats och dagens säkerhetspolitiska hot, eller hot som kan få säkerhetspolitiska konsekvenser, är i många avseenden annorlunda än de hot som var aktuella vid lagens tillkomst. Utländska underrättelsetjänsters intresse riktar sig numera i större utsträckning mot forskning och utveckling inom civila områden samt mot information om samhällsviktiga system. Samtidigt kvarstår dock underrättelsehotet mot militära förhållanden.

Även den ökade internationaliseringen och Sveriges omfattande internationella samarbete har inneburit förändringar och påverkar svaret på frågan *vad* som ska skyddas.

Att hoten mot rikets säkerhet har förändrats innebär också att svaret på frågan *mot vad* behövs ett säkerhetsskydd har kommit att påverkas. Till skillnad mot tidigare är dagens hot ofta gränsöverskridande, icke-militära och utgår inte sällan från icke-statliga aktörer. Som exempel kan nämnas internationell terrorism. Sedan säkerhetsskyddslagens införande har hotet från terrorism blivit allt mer påtagligt. Terrorismen har också förändrats. Tidigare handlade det främst om mindre politiskt extrema organisationer som agerade mot enskilda statsmakter, och drivkraften var ofta nationella konflikter. I dag är de flesta terroraktörer transnationellt organiserade, och de uppfattar sina motståndare i form av kulturer eller världsomspännande konspirationer. Det gör att terrorism i dag inte bara berör det land där ett attentat sker. Vidare har globaliseringen och revolutionen inom informationsteknologin ändrat förutsättningarna för terrorism. Inom EU utgör förebyggande, skydd, efterspaning och beredskap de fyra centrala områdena i EU:s strategi för kampen mot terrorism. EU prioriterar såväl förebyggande och bekämpande av terroristhandlingar som

skydd av infrastruktur och av medborgarna. Ett annat av de allra allvarligaste hoten i dag utgörs av elektroniska angrepp i olika former. Frågan *mot vad* behövs ett säkerhetsskydd har också kommit att påverkas av lagstiftning som tillkommit efter säkerhetsskyddslagens ikraftträdande och som, genom sitt liknande eller delvis liknande syfte att motverka allvarliga hot och risker inom olika sektorer, i många avseenden tangerar säkerhetsskyddet.

Även svaret på frågan *hur* skyddet ska säkerställas har kommit att ändras i förhållande till vad som gällde vid säkerhetsskyddslagens tillkomst. Tillämpningsområdet för de olika säkerhetsskyddsåtgärderna förutsätter enligt den gällande lagstiftningen i stor utsträckning hantering av sekretessbelagda uppgifter. Säkerhetsskyddsåtgärden informationssäkerhet, som tidigare benämndes sekretesskydd, tar uteslutande sikte på att förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Med hänsyn till informationsteknikens utveckling ställs numera helt andra krav på säkerhetsskyddet. I dag hanteras merparten av uppgifter, såväl sådana som omfattas av krav på sekretess som andra uppgifter som rör säkerhetskänslig verksamhet, i it-system. Dessa system hanterar mycket stora informationsmängder, såväl öppna som hemliga. Eftersom säkerhetsskyddsåtgärderna i stor utsträckning förutsätter hantering av sekretessbelagda uppgifter omfattas således inte systemen som sådana av krav på säkerhetsskydd. Förutsättningarna för informationssäkerheten har också påverkats av internationaliseringen. Som ett resultat av avregleringen har viktiga funktioner inom elsektorn kommit att flyttas till utlandet. Likaså har det blivit vanligt med åtgärder som outsourcing och offshoring när det gäller utveckling eller hantering av säkerhetskänsliga it-system.

När det gäller informationssäkerhet bedrivs i dag ett arbete på bred front med att stärka samhällets informationssäkerhet. Detta innebär att ett stort antal myndigheter m.fl. arbetar med informationssäkerhetsfrågor, dock utifrån andra utgångspunkter än att betrakta informationssäkerheten som en säkerhetsskyddsangelägenhet. Att informationssäkerhetsarbetet bedrivs utifrån diverse utgångspunkter med stöd av olika författningar kan ge upphov till tveksamheter för tillämpande myndigheter och övriga om vad det

är som särskilt gäller för informationssäkerhet på säkerhetsskyddsområdet.

En annan effekt av it-utvecklingen är att den har medfört att säkerhetsskyddsåtgärder avseende informationssäkerhet och fysisk säkerhet alltmer har kommit att vävas samman. Ett exempel på detta är utökade möjligheter för medarbetare att utföra sitt arbete från annat ställe än den fysiska arbetsplatsen medför ändrade förutsättningar för tillträdesskyddet.

Även när det gäller säkerhetsprövning har förutsättningarna ändrats. På samma sätt som för krav på säkerhetsskydd avseende informationssäkerhet förutsätter säkerhetsprövning, med undantag för bestämmelserna om säkerhetsprövning till skydd mot terrorism, hantering av vissa sekretessbelagda uppgifter. Bland annat avregleringen av offentlig verksamhet som därmed övergått till privata aktörer och som således inte omfattas av offentlighets- och sekretesslagen, har kommit att påverka tillämpningsområdet för säkerhetsprövningen.

En annan väsentlig förändring är intensifieringen av det internationella samarbetet såväl stater emellan som inom näringslivet. Med anledning av det ökande internationella samarbetet ställs numera allt oftare krav på säkerhetsskyddsåtgärder som villkor för att få delta i olika internationella samarbeten. Säkerhetsskyddslagens avsaknad av reglering om utfärdande av intyg över en utförd säkerhetsprövning kan göra det svårare för svenskar att delta i säkerhetskänslig verksamhet utomlands.

Svaret på frågan *av vem* nödvändiga säkerhetsskyddsåtgärder ska vidtas har också kommit att påverkas. De ändrade förutsättningarna för säkerhetsskyddet har bl.a. inneburit att fler enskilda aktörer än tidigare i större utsträckning berörs av lagstiftningen. Numera ägnar sig betydligt fler aktörer än tidigare åt säkerhetskänslig verksamhet. It-utvecklingen och den ökande användningen och beroendet av it har medfört att många privata aktörer, t.ex. it-konsultföretag som sköter driften av viktiga it-system för styrning, reglering och övervakning samt företag som levererar sådana it-system, numera bedriver sådan verksamhet och hanterar sådana uppgifter som är i behov av ett säkerhetsskydd.

Dessa förändrade förutsättningar kan vid ett första påseende verka överväldigande. Förvisso är förändringsfaktorerna utmanande för vårt arbete, men samtidigt har vi en befintlig lagstiftning

som åtminstone i vissa delar synes vara ändamålsenlig även i dag och som därför bör finnas också i en kommande lag. I det följande kapitlet redovisar vi våra överväganden kring vilka delar av nuvarande lagstiftning som bör kvarstå i en ny säkerhetsskyddslag och vilka delar som behöver utvecklas.

10 Utgångspunkter för en reformerad säkerhetsskyddslag

Det övergripande syftet med utredningen är enligt direktiven att anpassa lagstiftningen

- till det som krävs för att skydda verksamhet som har betydelse för rikets säkerhet från allvarliga konsekvenser till följd av antagonistiska hot, och
- till de krav som det internationella samarbetet ställer.

Vi ska analysera frågor som hur informationssäkerheten bör vara utformad, om ett system med säkerhetsklarering kan ersätta nuvarande säkerhetsprövning och hur skyddet mot terrorism bör utformas i säkerhetsskyddslagstiftningen. Direktiven anger också att vi ska föreslå hur systemet med säkerhetsskyddad upphandling bör vara utformat för att vara enkelt att tillämpa och samtidigt anpassat för internationell samverkan och om kravet på svenskt medborgarskap för säkerhetsklassad anställning vid staten, en kommun eller ett landsting bör bestå. Slutligen ska tillsynen och den därmed sammanhängande frågan om eventuella sanktioner utredas.

I detta kapitel behandlar vi inledningsvis (avsnitt 10.1) vilka delar av nuvarande lagstiftning som vi ser som ändamålsenliga redan i dag och som därför bör behållas i en ny lag. Därefter redovisar vi vilka delar som bör förtydligas, utvecklas eller ändras för att möta direktivens krav (avsnitt 10.2).

10.1 En utgångspunkt i nuvarande reglering

En säkerhetsskyddslagstiftning bör så till vida bygga på tidigare reglering

att den ska säkerställa ett tillräckligt skydd för det som är mest skyddsvärt för nationen,

att den ska vara verksamhetsorienterad,

att den ska ge ett förebyggande skydd mot i huvudsak antagonistiska hot,

att den ska omfatta samverkande säkerhetsskyddsåtgärder för information, personer och verksamhet, och

att den ska utgå från nuvarande organisatoriska indelningen avseende bl.a. verkställighetsföreskrifter och tillsyn.

Även om våra direktiv och förstudier, departementspromemorior och skrivelser pekar på viktiga förändringsbehov, finns det delar av lagstiftningen som fungerar bra och är ändamålsenliga. Dessa delar bör naturligtvis behållas. I de följande delavsnitten utvecklas de principer, syften och strukturer som vi anser bör finnas kvar i en ny reglering.

10.1.1 Ett säkerhetsskydd för det mest skyddsvärda

Säkerhetsskyddslagen bör även fortsättningsvis i huvudsak ta sikte på de för Sverige viktigaste verksamheterna och funktionerna.

Annan närliggande reglering innehåller bestämmelser om åtgärder som liknar säkerhetsskydd, men det bör inte påverka säkerhetsskyddslagens tillämpningsområde.

Ett kvalificerat skyddsbehov

Även fortsättningsvis bör lagen begränsas till att ge ett säkerhetsskydd för det som är mest betydelsefullt för nationen och där en skada, förlust eller begränsning kan få allvarliga konsekvenser för landet. Skälet till det är att säkerhetsskyddsåtgärderna – informationssäkerhet, tillträdesbegränsning och säkerhetsprövning – inne-

bär intrång i enskildas privatliv, ger ökade kostnader och kan medföra negativa konsekvenser för effektivitet och administration. Det bör därför krävas ett kvalificerat skyddsbehov utifrån för samhället fundamentalt viktiga funktioner för att åtgärder enligt säkerhetsskyddslagstiftningen ska vara motiverade. Dessa funktioner kan, trots kravet på nationell betydelse, finnas i en regional eller till och med i en lokal kontext. Dagens säkerhetspolitiska situation och Sveriges internationella säkerhetssamarbeten innebär att även Sveriges internationella verksamhet och folkrättsliga åtaganden har nationell betydelse. Det bör återspeglas i lagstiftningen som därför behöver förtydligas och utvecklas. Frågan behandlas i avsnitt 10.2.1.

Den utveckling som har beskrivits i kapitel 9 innebär att behovet av säkerhetsskydd och andra former av skydd har utsträckts till att omfatta fler verksamheter än tidigare. Denna utveckling kan komma att fortsätta. Det är därför angeläget att lagstiftningen är utformad så att den kan omfatta nya verksamheter och skydda mot hot av olika karaktär, och att den därmed står sig över tiden. Med hänsyn till detta bör inte aktuella hot eller vilka verksamheter som i dag är av nationell betydelse ges någon avgörande betydelse för hur lagstiftningen utformas. Lagstiftningen bör i stället utformas med hänsyn tagen till en mer schematisk och relativt tidsobestämd hotbild och, precis som nu, ge ett skydd för de för landet allra viktigaste samhällsfunktionerna.

Även verksamheter och funktioner som med ett sådant synsätt inte täcks av säkerhetsskyddslagen kan ha skyddsbehov. Detta får tillgodoses genom annan reglering. För att illustrera detta kan nämnas att information hos myndigheter träffas av de föreskrifter om statliga myndigheters informationssäkerhet som Myndigheten för samhällsskydd och beredskap har meddelat.[1] Bestämmelserna gäller även för information som inte omfattas av säkerhetsskyddslagstiftningen.

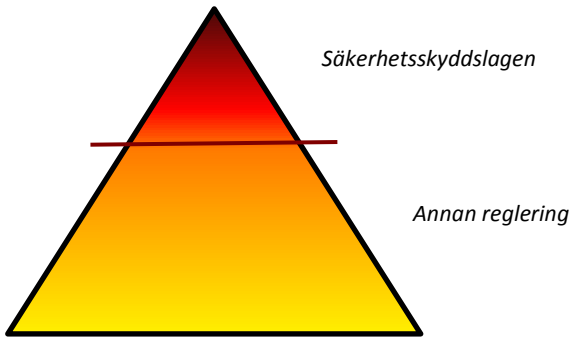
Inte sällan kan det finnas goda skäl för en verksamhet att välja att anlägga ett vidare perspektiv i fråga om säkerhetsarbetets syfte och omfattning. Enligt t.ex. Försvarsmaktens beskrivning av myndighetens säkerhetstjänst ingår, förutom det som omfattas av

[1] MSBFS 2009:10 med stöd av 34 § förordningen (2006:942) om krisberedskap och höjd beredskap, se avsnitt 5.4.

säkerhetsskydd, även t.ex. skydd av egendom av stort ekonomiskt värde, och skyddsåtgärderna syftar också till att avvärja ett bredare spektrum av hot. Åtgärderna kan avse t.ex. bevakning för att skydda it- och kommunikationsutrustning mot stöld eller åverkan. Det kan också handla om utbildning för att motverka att anställda och uppdragstagare genom oaktsamhet eller bristande kunskap skadar tillgångar i verksamheten, även om de inte är av betydelse för rikets säkerhet eller behöver skyddas mot terrorism. Åtgärder med sådan inriktning omfattas inte av säkerhetsskyddslagen, men de kan ändå med fördel samordnas med säkerhetsskyddsåtgärder, inte minst av kostnads- och effektivitetsskäl.

Avgränsningen kan symboliseras av en pyramid av skyddsvärda intressen där enbart den översta delen av pyramiden omfattas av säkerhetsskyddslagen.

Fig. 1 Principskiss över säkerhetsskyddslagstiftningens avgränsning



Källa: utredningens figur

Motstående intressen

Säkerhetsskydd innebär som nämnts en avvägning mellan å ena sidan behovet av ett skydd för de för nationen viktigaste funktionerna och å andra sidan ökade kostnader, ökad administration, möjliga öppenhets- och effektivitetsförluster och intrång i enskildas personliga integritet. Avvägningen innebär att denna lagstiftning måste utformas med beaktande av behovs- och proportionalitetsprinciper där varje åtgärd prövas mot de motstående intressena, och att andra mindre ingripande åtgärder för att uppnå ett skydd över-

vägs. Hänsyn till behov av säkerhetsskyddsåtgärder kan för en verksamhet innebära en jämkning av effektivitetskrav som ställts upp för verksamheten. Krav på tillträdesbegränsning kan medföra bl.a. behov av system för att kontrollera och övervaka inpassering av anställda och besökare till anläggningar och lokaler. Krav på säkerhetsprövning av personal kan innebära begränsningar i fråga om val av personal, inskränkningar i den personliga integriteten och en mindre effektiv rekryterings- och bemanningsprocess. En god informationssäkerhet är i allmänhet ett angeläget intresse för en verksamhet, men samtidigt kan de krav på förhöjd informationssäkerhet som säkerhetsskyddet medför innebära krav på kostsamma specialanpassade säkerhetsfunktioner, medföra oönskad informationsbegränsning och hindra eller begränsa kostnadsbesparingar.

Regleringen i Europakonventionen till skydd för de mänskliga rättigheterna och de medborgerliga friheterna samt 2 kap. regeringsformen medför att frågan om intrånget i den personliga integriteten kan motiveras av lagens skyddsbehov är särskilt viktig. Säkerhetsprövningen i allmänhet och registerkontrollen i synnerhet medför ett betydande ingrepp i den personliga integriteten som måste vara noggrant avvägt mot det behov som åtgärden ska tillgodose.[2]

Det är utifrån nämnda avvägningar som en lagstiftning om säkerhetsskydd bör utformas. Samtidigt är det viktigt att de skyddsvärden som verkligen behöver ett säkerhetsskydd också får det och att andra motstående intressen inte motverkar skyddsnivån när behovet väl är bedömt. Säkerhetsanalysen är central i detta sammanhang och den behandlas vidare i kapitel 13. Vidare är det viktigt att lagstiftningen medger en viss flexibilitet på ett sådant sätt att lagen även kan möta förändringar utifrån samhällsutvecklingen och en förändrad hotbild.

[2] Frågan om denna avvägning behandlas vidare i avsnitt 18.8.

Närliggande reglering

Säkerhetsskyddslagstiftningen är inte den enda reglering som ger ett skydd för samhällsviktig verksamhet, utan även närliggande reglering måste beaktas. I kapitel 5 har vi redogjort för ett antal regleringar som har en koppling till säkerhetsskyddslagstiftningen. Bland dessa kan nämnas de olika kris- och beredskapsförfattningarna samt skyddslagstiftningar för kärnteknisk verksamhet, luftfart, sjöfart, hamnar, transport av farligt gods och skydd för landskapsinformation. Skyddslagen (2010:305) ansluter nära till säkerhetsskyddslagen genom hänvisningen till säkerhetsskyddsåtgärden tillträdesbegränsning. Dessa regleringar måste därför ses som ett system där olika regelverk samverkar i olika situationer.

Merparten av de ovan nämnda skyddsregleringarna har tillkommit eller ändrats efter säkerhetsskyddslagens tillkomst. I viss utsträckning handlar det om lagar och förordningar som genomför eller kompletterar EU-rättslig reglering. Inte sällan har lagstiftningen arbetats fram främst från ett ”safety-perspektiv”, dvs. att den utgår främst från behovet att skydda mot andra hot än antagonistiska, även om gränsdragningen inte alltid är så tydlig (ang. distinktionen mellan *safety* och *security* se avsnitt 9.3.4).

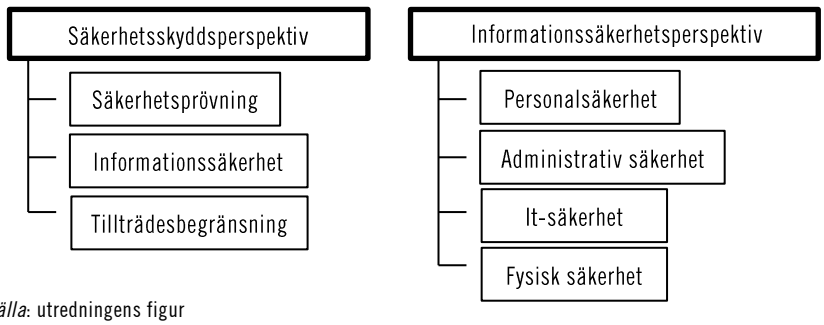
Vi har ställt oss frågan om lagens tillämpningsområde, dvs. vilka verksamheter som bör omfattas av krav på säkerhetsskydd, ska påverkas av att det finns reglering som i olika avseenden tangerar säkerhetsskyddslagen, t.ex. reglering som ställer krav avseende fysiskt skydd och informationssäkerhet. Vi har kommit fram till att så inte bör vara fallet. Säkerhetsskyddslagen fyller en viktig funktion som sektorsövergripande reglering som på lång sikt ska förebygga för nationen påtagliga konsekvenser av antagonistisk verksamhet. De olika regleringarna på området ska därför tillämpas parallellt och i samverkan beroende på situationen och verksamhetens art. Säkerhetsskyddslagstiftningen ska dock kunna tillämpas även fristående från annan lagstiftning. Sammanfattningsvis kan vad som i förhållande till närliggande reglering utmärker säkerhetsskyddslagen beskrivas genom de tre nyckelkomponenterna långsiktigt förebyggande åtgärder, skydd mot antagonistiska hot och nationell dimension.

10.1.2 Verksamhetsorienterad eller informationsorienterad lagstiftning

Lagstiftningen bör även fortsättningsvis vara verksamhetsorienterad. Alternativet – att lagstiftningen görs informationsorienterad vilket är vanligt i andra länder – riskerar att göra den snävare än vad som är ändamålsenligt.

Som den internationella utblicken har visat har många länder och även internationella organisationer ett regelverk som utgår från en viss typ av känslig information och hur den ska skyddas. Med ett sådant perspektiv blir säkerhetsskyddsåtgärder som i Sverige benämns som säkerhetsprövning och tillträdesbegränsning snarare metoder för att skydda information än självständiga funktioner i säkerhetsskyddet. Även den internationella standarden för ledning av informationssäkerhet (LIS, SS-ISO/IEC 27000-serien) har ett sådant perspektiv. Nuvarande säkerhetsskyddslagstiftning skiljer sig från denna indelning genom att säkerhetsprövning och tillträdesbegränsning är *parallella* delområden till informationssäkerheten. Den ordningen illustreras i figuren nedan.

Fig. 2 Olika perspektiv på skydd



Källa: utredningens figur

Frågan är om det med tanke på den internationella jämförelsen finns skäl att överge nuvarande struktur till förmån för en struktur som fokuserar på informationssäkerhet.

Lagstiftningen ska även fortsättningsvis ge ett skydd för landets viktigaste säkerhetsintressen. I dessa skyddsintressen finns som en betydande delmängd information som – om den röjs, ändras, görs

otillgänglig eller förstörs – kan orsaka skada för landet på olika sätt. Det förekommer dock även andra skyddsvärda tillgångar som t.ex. kommunikationer och anläggningar för el- och vattenförsörjning. Vidare finns det verksamheter och materiel som har ett högt skyddsbehov genom att de kan orsaka stor skada i händerna på obehöriga, t.ex. radioaktivt material, sprängämnesprekursorer och vapensystem. Dessa skyddsvärda tillgångar låter sig inte alltid inordnas under rubriken information. Som vi beskriver i nästa avsnitt omfattar lagen skydd mot antagonistiska hot som sabotage och terrorism som sällan, åtminstone direkt, riktas mot information. Vi bedömer därför att ett informationssäkerhetsperspektiv skulle vara alltför snävt för att kunna ge ett relevant skydd för det som lagstiftningen bör skydda. Vi har därför valt att behålla verksamhetsperspektivet i förslaget till ny säkerhetsskyddslag.

Genom att lagen föreslås ha ett vidare perspektiv ser vi inte några hinder mot att den internationella standarden för ledning av informationssäkerhet tillämpas inom ramen för lagstiftningen. Vi ser heller inga problem med att utifrån ett bibehållet säkerhetsskyddsperspektiv uppfylla internationella förpliktelser på området.

10.1.3 Mot vad ska lagen ge ett skydd?

Lagstiftningen bör även fortsättningsvis ge ett skydd mot antagonistiska hot som t.ex. spioneri, sabotage och terroristbrott.

Säkerhetsskyddslagen har som syfte att ge ett skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet. Lagen ska också ge ett skydd mot terroristbrott. På samma sätt som när det gäller frågan om *vad* som ska skyddas finns det anledning att föra resonemang om en avgränsning i fråga om *mot* vilka hot som en säkerhetsskyddslag ska skydda. Säkerhetsskydd innebär som tidigare har beskrivits vissa olägenheter. Det finns goda skäl att begränsa lagen till att avse sådana hot som på grund av sin karaktär kan motivera och stå i proportion till sådana negativa effekter. Sammantaget innebär det att skyddet även fortsättningsvis bör riktas mot antagonistiska hot. Hoten kan dock uppstå utan någon *direkt* koppling till de brott som räknas upp, och det bör därför även fortsättningsvis ges ett skydd mot oaktsamhet och andra

åtgärder än brottsliga som kan leda till konsekvenser för rikets säkerhet eller utgöra ett led i, eller förstadium till, antagonistisk verksamhet. Detta utvecklas närmare i avsnitt 11.5. När det gäller terroristbrott saknas det skäl att låta detta hot ha en särställning på ett sådant sätt som det har i nuvarande lagstiftning. Detta utvecklas närmare i avsnitt 10.2.3.

10.1.4 Vilka säkerhetsskyddsåtgärder bör lagen innehålla?

De nuvarande säkerhetsskyddsåtgärderna informationssäkerhet, tillträdesbegränsning och säkerhetsprövning behålls. Benämningarna bör dock ses över.

Säkerhetsskyddslagen delar in säkerhetsskyddsåtgärderna i tre huvudområden – informationssäkerhet, tillträdesbegränsning och säkerhetsprövning. Därutöver anges utbildning och kontroll som delar av säkerhetsskyddet. Som tidigare nämnts bör en säkerhetsskyddslag även fortsättningsvis ha ett verksamhetsperspektiv. Med detta synsätt bör även åtgärderna indelas på samma sätt som i dag. Om lagen i stället skulle få ett informationssäkerhetsperspektiv, skulle tillträdesbegränsningen och säkerhetsprövningen ha blivit delar av informationssäkerheten. Som nämnts skulle ett sådant förhållningssätt inte vara ändamålsenligt. Benämningarna av åtgärderna behöver ses över. Den frågan behandlas i avsnitt 15.1.

10.1.5 Organisatoriska frågor

Ansvaret för tillsyn av säkerhetsskyddet och för att meddela verkställighetsföreskrifter till lagstiftningen bör även fortsättningsvis vara uppdelat på i huvudsak Försvarsmakten, Säkerhetspolisen och de s.k. sektorsmyndigheterna. De sistnämnda myndigheterna bör i stället benämnas *säkerhetsskyddsstödjande myndigheter*. Ansvaret bör dock förtydligas.

Säkerhetspolisen och Försvarsmakten

Nuvarande lagstiftning utgår från ett decentraliserat ansvar där den som leder en verksamhet ansvarar för säkerhetsskyddet i denna. Regelverket bygger på att säkerhetsskyddslagen och säkerhetsskyddsförordningen kompletteras med tillämpningsföreskrifter för bl.a. hur säkerhetsskyddsåtgärderna ska utföras. Uppdelningen av tillsyn och normgivning på i huvudsak Försvarsmakten och Säkerhetspolisen (tidigare Rikspolisstyrelsen) bygger på en historisk ansvarsfördelning mellan myndigheterna som riktar sig mot försvarsrelaterad respektive civil verksamhet. Mot denna ordning kan man naturligtvis ha invändningar. Samarbetet mellan myndigheterna fungerar dock bra, och fram till 2004 uppvisade de båda myndigheternas tillämpningsföreskrifter stora likheter. Skillnaderna därefter har i huvudsak berott på att Försvarsmakten, mot bakgrund av Sveriges internationella åtaganden, införde fyra informationssäkerhetsklasser. I avsnitt 15.3 föreslås att krav på en sådan indelning ska införas i lagen, varför denna diskrepans i tillämpningsföreskrifterna försvinner. Systemet med en delad föreskriftsrätt ger en viss flexibilitet genom att den relativt homogena grupp av myndigheter som Försvarsmaktens föreskrifter gäller för kan behöva mer detaljerade bestämmelser om säkerhetsskydd som kanske inte passar för annan verksamhet. Det underlag som har redovisats för utredningen från olika myndigheter har heller inte innehållit några uppgifter om att nuvarande uppdelning skulle vara till någon nackdel. Försvarsmakten och Säkerhetspolisen har dessutom de resurser och den kompetens som krävs för att lösa dessa uppgifter. Nuvarande ordning bör därför behållas.

Den 1 januari 2015 genomfördes en omorganisation av polisen som bl.a. innebär att Säkerhetspolisen får ställning som fristående myndighet. Detta innebär i sin tur att Säkerhetspolisen formellt har övertagit frågor som rör säkerhetsskydd från Rikspolisstyrelsen. I praktiken innebär det ingen förändring eftersom dessa frågor redan har hanterats vid Säkerhetspolisen.

Säkerhetsskyddsstödjande myndigheter

Affärsverket svenska kraftnät, Post- och telestyrelsen, Transportstyrelsen och länsstyrelserna har uppgifter i fråga om bl.a. beslut om placering i säkerhetsklass och kontroll av säkerhetsskyddet i förhållande till vissa enskilda som bedriver säkerhetskänslig verksamhet. I dag är det vanligt att de myndigheterna i säkerhetsskyddssammanhang benämns sektorsansvariga myndigheter. Den benämningen förekommer bl.a. i våra direktiv.

Vi ser behov av att kunna använda en sammanfattande benämning för dessa myndigheter också i den till lagen hörande förordningen. Det har dock med fog, bl.a. från Transportstyrelsen, framförts att det är olyckligt att i författningstexten använda uttrycket sektorsanvariga myndigheter. Någon självklar benämning finns inte. Ett alternativ vi stannat för är *säkerhetsskyddsstödjande myndighet*. Vi föreslår vidare i avsnitt 18.10 och 21.2.4 att Myndigheten för samhällsskydd och beredskap ska ta över de uppgifter länsstyrelserna har som säkerhetsskyddsstödjande myndighet samt att även, vad gäller rådgivning och tillsyn, vara säkerhetsskyddsstödjande myndighet för kommuner och landsting.

Även de säkerhetsskyddsstödjande myndigheternas roll bör behållas och även förstärkas och förtydligas något.

De organisatoriska frågorna behandlas närmare i kapitel 18, 19 och 21 om personalsäkerhet, säkerhetsskyddad upphandling samt tillsyn, föreskrifter och rapportering.

10.2 Ett utvecklat och förtydligat regelverk

Säkerhetsskyddslagen behöver utvecklas och förtydligas. Den behöver *utvecklas* när det gäller Sveriges internationella åtaganden på säkerhetsskyddsområdet och informationssäkerhetsperspektiven tillgänglighet och riktighet. Vidare behöver den *förtydligas* avseende att lagen ska tillämpas i såväl allmän som enskild verksamhet. Det innebär att våra överväganden inriktas på att klargöra lagens skyddsintressen och att klargöra lagens tillämpningsområde.

Detta sammantaget medför behov av en justerad beskrivning av lagens syfte och av en delvis förändrad systematik.

Som redovisats tidigare är det viktigt att bygga vidare på de delar av nuvarande lagstiftning som fungerar bra. Vissa delar behöver dock utvecklas eller förtydligas för att lagen ska möta kraven i våra direktiv. I detta avsnitt behandlas inledningsvis behovet att utveckla lagens skyddsintressen. Det innefattar folkrättsliga åtaganden på säkerhetsskyddsområdet, internationell samverkan och att lagen bör träffa både uppgifter och verksamhet som är av säkerhetskänslig betydelse. Därefter behandlas lagens tillämpningsområde avseende myndigheter och enskilda. Avslutningsvis tar vi upp behovet av en tydligare syftesbeskrivning och hur våra förändringsförslag påverkar lagens systematik.

10.2.1 Lagens utökade skyddsintressen och andra närliggande intressen

Lagen bör ge ett skydd inte bara för s.k. *hemliga uppgifter* utan även för uppgifter som omfattas av ett folkrättsligt åtagande om säkerhetsskydd. Lagen bör även uppfylla krav på andra säkerhetsskyddsåtgärder som följer av åtaganden inom t.ex. luft- och sjöfartsskydd.

Lagen bör omfatta både verksamhet och uppgifter. Information bör inte ges ett skydd enbart från ett konfidentialitetsperspektiv utan även avseende informationssäkerhetsperspektiven tillgänglighet och riktighet.

Lagen bör innehålla bestämmelser om formerna för internationell samverkan på säkerhetsskyddsområdet vilket bl.a. innefattar bestämmelser om säkerhetsintyg för personer och leverantörer.

Folkrättsliga åtaganden

Nuvarande säkerhetsskyddslagstiftning fokuserar på skyddet av *hemliga uppgifter*, dvs. uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL, och som rör rikets säkerhet. Samtidigt har Sverige ingått ett betydande antal överenskommelser som innebär ett folkrättsligt åtagande att ge ett skydd för klassificerad information från andra länder och inter-

nationella organisationer (se kapitel 6). I den mån som denna information är av betydelse även för rikets säkerhet, t.ex. när informationen rör försvarsmateriel som har utvecklats i samarbete med ett annat land, omfattas informationen av lagstiftningen. I praktiken är det därför ofta så att informationen ändå träffas av säkerhetsskyddslagstiftningens krav. Den ökade internationaliseringen på försvars- och säkerhetsområdet liksom utvecklingen mot andra internationella samarbetsområden innefattar dock ett informationsutbyte där även uppgifter som inte täcks av lagstiftningen behöver skyddas. Detta medför att det kan uppstå en situation där uppgifter som täcks av ett folkrättsligt åtagande inte omfattas av säkerhetsskyddslagen. Detta är naturligtvis olyckligt. Sverige omfattas även av andra folkrättsliga åtaganden som rör säkerhetsskydd, t.ex. konventioner om luft- och sjöfartsskydd samt EU-rättslig reglering. Dessa är ofta genomförda i svensk rätt genom den närliggande lagstiftning som har redovisats i kapitel 5, men det är ändamålsenligt att denna typ av åtaganden också täcks av en ny säkerhetsskyddslag eftersom åtagandena även rör säkerhetsskydd.

Av denna anledning behöver lagen kompletteras för att ge ett explicit skydd för verksamhet som avses i ett för Sverige, i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd (internationellt säkerhetsskyddsåtagande).

Verksamhet och uppgifter

Även om nuvarande lagstiftning överlag har ett verksamhetsperspektiv, så är skyddet för verksamhet starkt förknippat med skyddet mot terrorism, medan lagen i övrigt främst avser skydd för hemliga uppgifter. Denna uppdelning är inte ändamålsenlig. Samhällsviktig verksamhet behöver skyddas mot samtliga i lagen uppräknade antagonistiska hot och inte bara mot terrorism. Det kan röra sig om försvarets installationer, eller om ledningscentraler, distributionsnät för elkraft eller informationssystem för drift och övervakning av dricksvattenproduktion. Information är ofta en av de viktigare tillgångarna i en verksamhet, och denna kan behöva olika skydd beroende på verksamhetens art. Det är t.ex. inte säkert

att ett skydd mot röjande av informationen alltid är relevant. Detta utvecklas i det följande.

Aspekter på informationssäkerheten

I nuvarande säkerhetsskyddslagstiftning har skyddet av information ett snävt konfidentialitetsperspektiv som innebär ett skydd mot obehörigt röjande av uppgifter. Visserligen finns det en bestämmelse om att tillgänglighets- och riktighetsaspekter för *hemliga* uppgifter ska beaktas, men denna bestämmelse träffar enbart uppgifter som redan har ett skyddsbehov från ett konfidentialitetsperspektiv.

Utvecklingen på informationsområdet och det därmed ökade teknikberoendet har medfört en ökad sårbarhet för informationssystem i för samhället vitala verksamheter. Inte sällan är det dock andra krav än konfidentialitetskrav som står i fokus. Detta kan illustreras med att ett avbrott, dvs. ett *tillgänglighetsproblem*, i övervakningssystemen i ett kärnkraftverk skulle kunna få katastrofala följder. Detsamma gäller för en felfunktion, dvs. ett *riktighetsproblem*, i styrkommandon för dammluckor i ett större vattenkraftverk. Karaktäristiskt för dessa båda exempel är att konfidentialitetsaspekten för uppgifterna i systemen inte är påtaglig.

Det finns därför ett behov av ett vidare perspektiv när det gäller skyddet av uppgifter som – om de röjs, ändras, görs otillgängliga eller förstörs – kan medföra skada på för landet viktiga intressen (se vidare kapitel 16). En sådan utvidgning påverkar även lagens systematik och utformningen av personalsäkerheten och den fysiska säkerheten.

Internationell samverkan

De internationella åtagandena på säkerhetsskyddsområdet hänger samman med en ökad internationell samverkan. Det kan gynna en utveckling mot att svenska medborgare och företag i ökad omfattning kan delta i säkerhetskänslig verksamhet i andra länder och internationella organisationer. De flesta internationella överenskommelser på säkerhetsskyddsområdet innehåller bestämmelser som utgår från ett ömsesidigt förtroende för parternas nationella

säkerhetsskyddslagstiftning. Bestämmelserna innebär att ett lands säkerhetsbedömningar avseende personer med hemvist i landet, respektive leverantörer med säte där, godtas av den andra parten. För att det ska vara möjligt krävs mekanismer för hur en part ska kommunicera bedömningen till den andra parten. För detta ändamål är det brukligt att använda sig av säkerhetsintyg avseende personer och leverantörer. Många överenskommelser har även detaljerade beskrivningar av hur sådana intyg ska utformas.

I nuvarande lagstiftning saknas explicita bestämmelser om intygsförfarandet. Det har lett till en osäkerhet i tillämpningen och i förlängningen till ett sämre läge för personer bosatta i Sverige och svenska företag att kunna delta i säkerhetskänslig verksamhet utomlands. En ny säkerhetsskyddslagstiftning bör därför ha tydliga bestämmelser om under vilka förutsättningar som sådana intyg kan utfärdas och vem som utfärdar dem. Även avseende den internationella samverkan i övrigt bör uppgiftsfördelningen mellan myndigheter göras tydlig. Frågorna behandlas vidare i kapitel 20.

10.2.2 För vem ska lagen gälla?

Säkerhetsskyddslagen bör även fortsättningsvis gälla i såväl allmän som enskild verksamhet. Den grundläggande principen bör vara att skyddet för det skyddsvärda bör vara detsamma oavsett i vilken verksamhet det förekommer. Lagen behöver förtydligas i detta avseende så att den principen får bättre genomslag.

Som vi behandlat tidigare bör säkerhetsskyddslagens huvudsakliga funktion vara att säkerställa ett säkerhetsskydd, dvs. ett skydd mot antagonistiska hot, för de verksamheter som är allra mest skyddsvärda för nationen. Från säkerhetsskyddslagens tillämpningsområde bör därför inte vissa sektorer eller verksamhetsområden undantas. Tillämpningsområdet bör i stället vara så heltäckande som möjligt. Vilka verksamheter som säkerhetsskyddslagen ska gälla för bör som vi betonat tidigare avgöras utifrån en bedömning av vilken betydelse verksamheten har och hur denna bör skyddas. Den grundläggande principen bör på samma sätt som i dag vara att skyddet ska vara likvärdigt oavsett om det handlar om allmän eller enskild verksamhet.

När det gäller lagens tillämplighet hos enskilda finns det behov av ett förtydligande. Nuvarande lagstiftning definierar begreppet *hemlig uppgift*[3] som en uppgift som omfattas av offentlighets- och sekretesslagen och som rör rikets säkerhet. Definitionen är problematisk i verksamheter som inte omfattas av lagen, t.ex. enskilda och statliga bolag, trots att säkerhetsskyddslagstiftningen är tillämplig även för dessa. Genom att definitionen innehåller ett krav på att uppgiften omfattas av offentlighets- och sekretesslagen, verkar följden bli att det inte kan förekomma några hemliga uppgifter i sådana verksamheter, trots att det kan förekomma uppgifter som till *sin natur* rör rikets säkerhet. En sådan insnävning kan knappast ha varit avsedd med tanke på hur bestämmelserna om säkerhetsskyddslagens tillämpningsområde är utformade.[4] Behovet av ett förtydligande i det avseendet behandlas i avsnitt 12.2.

10.2.3 Lagens syfte och en delvis ny systematik

Det behöver förutsättningslöst övervägas såväl hur lagens syfte bör beskrivas som hur lagen systematiskt bör vara uppbyggd.

Säkerhetsskyddslagen innehåller i dag inte någon uttrycklig syftesbestämmelse. Syftet med lagen framgår i stället indirekt genom en kombination av bestämmelser om lagens tillämpningsområde och om säkerhetsskydd. Vilka verksamheter som lagen avser framgår av det angivna tillämpningsområdet i fråga om enskilda i lagens 1 § 3. Där anges att lagen gäller vid verksamhet hos enskilda, *om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism*. Lagens 6 § ger svar på frågan mot vad ett skydd behövs. Bestämmelsen anger bl.a. att säkerhetsskyddet ska förebygga spioneri, sabotage och andra brott som kan hota rikets säkerhet samt terroristbrott, även om brotten inte hotar rikets säkerhet.

Begreppet *rikets säkerhet*, som säkerhetsskyddslagstiftningen primärt är uppbyggd kring, har kommit att bli starkt förknippat med försvarsrelaterade förhållanden och skydd mot ett obehörigt

[3] 4 § 1 säkerhetsskyddsförordningen.
[4] 1–4 §§ säkerhetsskyddslagen.

röjande av för nationen känsliga uppgifter. Rikets säkerhet kan därför i flera avseenden tolkas alltför snävt. Det kan bl.a. bidra till att säkerhetsskyddet inte alltid uppfattas som en angelägenhet för civila verksamheter i enskild regi som är av stor vikt i ett fungerande samhälle. Vidare medför säkerhetsskyddslagens bestämmelser om skydd mot terrorism oklarheter. Det gäller bl.a. vilka förhållanden som formuleringarna ”verksamheter som särskilt behöver skyddas mot terrorism” och ”även om brotten inte hotar rikets säkerhet” i 1 och 3 §§ säkerhetsskyddslagen tar sikte på. I fråga om terrorism ser vi behov av en tydligare åtskillnad mellan *vad* lagen ska skydda och *mot vad* det skyddsvärda ska skyddas. Terroristbrott bör därför vara *ett* av de antagonistiska hot som lagen ska skydda mot och inte ha någon särställning i det avseendet. Våra direktiv utgår, vid beskrivningen av vad som bör omfattas av bestämmelser om säkerhetsskydd i en reformerad säkerhetsskyddslag, från den *nuvarande* terminologin och systematiken (se t.ex. direktiven s. 5). Av de skäl som redovisats ser vi emellertid behov av att förutsättningslöst överväga såväl hur lagens syfte bör beskrivas som hur lagen systematiskt bör vara uppbyggd.

10.2.4 En ny säkerhetsskyddslag

Förslag: Den nuvarande säkerhetsskyddslagen ersätts med en ny lag. Även den nya lagen bör benämnas säkerhetsskyddslag.

I det här kapitlet har vi dels utifrån nuvarande säkerhetsskyddslag redovisat några utgångspunkter som även en reformerad lagstiftning bör bygga på, dels redogjort för hur vi i stora drag ser på reformbehovet. Det handlar bl.a. om att tydliggöra och utveckla säkerhetsskyddslagens tillämpningsområde. Det gäller dels krav på säkerhetsskydd som följer av folkrättsliga förpliktelser, dels lagens tillämplighet avseende t.ex. elförsörjning, elektronisk kommunikation och andra samhällsviktiga verksamheter. De utgångspunkterna för reformbehovet behöver beaktas bl.a. i fråga om beskrivningen av lagens syfte och lagens systematiska uppbyggnad.

Nuvarande systematik bygger på skyddet av uppgifter från ett snävt konfidentialitetsperspektiv. Med hänsyn till de reformbehov som redovisats, bör systematiken i stället utgå från ett skydd av

uppgifter från ett bredare perspektiv samt tydligare inkludera skydd för andra slag av säkerhetskänslig verksamhet. Terrorismen blir med en sådan systematik en delmängd av de i huvudsak antagonistiska hot som lagen ska skydda mot.

Vissa delar av den nuvarande säkerhetsskyddslagstiftningen bör behållas, medan andra delar bör ändras, utvecklas eller förtydligas. Sammantaget innebär våra förslag en modernisering och i vissa avseenden förändrad systematik när det gäller säkerhetsskyddslagstiftningen. Det faller sig därför naturligt att lagen ersätts av en ny lag med tillhörande förordning. Benämningen säkerhetsskyddslag bör kvarstå.

11 Lagens syfte

I kapitel 10 har vi redovisat hur vi i stora drag ser på reformbehovet. Några av de utgångspunkter vi i det avseendet redogjort för har särskild relevans för beskrivningen av säkerhetsskyddslagens syfte. Av väsentlig betydelse är att lagen även i fortsättningen primärt bör ta sikte på verksamheter där ett antagonistiskt angrepp kan leda till allvarliga konsekvenser för nationen.[1] Tillämpningsområdet bör således också i fortsättningen avgränsas till verksamheter som vid en värdering av dess betydelse från ett nationellt säkerhetsperspektiv når upp till en särskilt hög nivå. Säkerhetsskyddslagen bör därför ta sikte på de för nationen mest skyddsvärda verksamheterna. Det gäller såväl i allmän som enskild verksamhet och med inriktning mot såväl försvarsverksamhet i traditionell bemärkelse som civil verksamhet. Frågan är då hur detta ska uttryckas i lagtexten.

En grundläggande fråga är om begreppet rikets säkerhet är tillräckligt brett för att även fortsättningsvis användas i en beskrivning av vilka verksamheter som omfattas av säkerhetsskyddslagen.

Som nämnts tidigare ser vi behov av en förändring vad gäller det förhållandet att det skyddsvärda området delvis beskrivs genom en hänvisning till verksamheter som särskilt behöver skyddas mot terrorism. Någon ändring i sak är inte avsedd utan det är fråga om att åstadkomma en mer logisk konstruktion av säkerhetsskyddslagen (se vidare kapitel 12). Detta förhållande behöver beaktas vid övervägandena om hur det skyddsvärda området ska beskrivas.

Kapitlet inleds med en bakgrundsbeskrivning i avsnitt 11.1. Våra överväganden och förslag redovisas därefter i avsnitt 11.2–5.

[1] Behovet av ett förtydligande i fråga om internationella åtaganden behandlas först i avsnitt 11.3.

11.1 Rikets säkerhet och förändringar på andra rättsområden

Förändringar inom rättsområden som säkerhetsskyddslagen anknyter till

Säkerhetsskyddslagens syfte och tillämpningsområde anknyter till vissa i sammanhanget relevanta straff- respektive sekretessbestämmelser samt bestämmelser om skyddsobjekt (se avsnitt 3.3.1 och kap. 4). Den reglering som säkerhetsskyddslagen anknyter till har setts över och ändrats i flera avseenden sedan säkerhetsskyddslagen infördes. I det följande tar vi översiktligt upp hur utvecklingen på dessa rättsområden kan ha betydelse för frågan om hur det för nationen, från ett säkerhetsskyddsperspektiv, skyddsvärda området ska beskrivas. För en närmare redovisning av de lagstiftningsärenden och lagbestämmelser som nämns i detta sammanhang hänvisas till kapitel 4.

Offentlighets- och sekretesslagen – bestämmelser som kan överlappa försvarssekretessen

I offentlighets- och sekretesslagen (2009:400), OSL, är det främst den s.k. försvarssekretessen i 15 kap. 2 § som avser förhållanden av betydelse för rikets säkerhet. Det är viktigt att notera att försvarssekretessen inte är begränsad till militära förhållanden. Det finns även andra bestämmelser om sekretess där det primära skyddsintresset är ett annat men som samtidigt kan avse uppgifter som i vissa fall är av betydelse för rikets säkerhet. De materiella ändringarna av sekretesslagstiftningen som här är av betydelse har medfört att det i dag finns fler och mer detaljerade sekretessbestämmelser som kan ge ytterligare vägledning i fråga om förhållanden som, också utanför försvarssektorn, kan vara relevanta att skydda med hänsyn till rikets säkerhet. Sekretessbestämmelser i 18 kap. i fråga om t.ex. säkerhets- och bevakningsåtgärder, chiffer och kod och risk- och sårbarhetsanalyser kan således samtidigt träffa uppgifter som rör rikets säkerhet.

Skyddslagen – ett vidgat fokus i fråga om civil verksamhet

Skyddslagen (2010:305) innebär i förhållande till den tidigare lagen på området ett vidgat fokus i fråga om fredstida viktiga samhällsfunktioner. Ett avgörande skäl för denna inriktning är enligt förarbetena[2] att samhället generellt sett har blivit väsentligt mera sårbart än tidigare. Det framhålls därvid att det är en sårbarhet som inte behöver hänga samman med militära eller direkta säkerhetspolitiska förhållanden men som ändå utsätter samhället för risker och påfrestningar på grundläggande samhällsfunktioner.

Möjliga nya skyddsobjekt är bl.a. byggnader, andra anläggningar och områden som används eller är avsedda för verksamhet som innefattar upprätthållande av allmän ordning och säkerhet, verksamhet inom kriminalvården eller Sveriges försörjning med sedlar och mynt.

En fortsatt utgångspunkt i begreppet rikets säkerhet för straffbestämmelserna i 19 kap. brottsbalken

Lagstiftningen i 19 kap. brottsbalken som syftar till att skydda riket mot främmande makts underrättelseverksamhet har nyligen setts över och ändrats.[3] På samma sätt som i våra direktiv grundades reformbehovet i stor utsträckning på de förändringar som den allmänna samhällsutvecklingen inneburit t.ex. genom den tekniska utvecklingen och en intensifierad globalisering. En central fråga var hur straffbestämmelserna har stått sig i ljuset av samhällsutvecklingen. Av särskilt intresse är därför övervägandena i fråga om en fortsatt utgångspunkt i begreppet rikets säkerhet för straffbestämmelserna i 19 kap. brottsbalken.

I den proposition som låg till grund för ändringarna i 19 kap. brottsbalken konstateras[4] att, även om begreppet saknar en legaldefinition, det har en relativt intakt och entydig betydelsekärna. Den anges kunna sammanfattas som skyddet för Sveriges oberoende – i betydelsen självständighet och suveränitet – och

[2] Prop. 2009/10:87 Skydd för samhällsviktig verksamhet, s. 25 f.
[3] Till följd av antagandet av Prop. 2013/14:51 Förstärkt skydd mot främmande makts underrättelseverksamhet, har ändringar gjorts i 19 kap. brottsbalken. Lagändringarna som trädde i kraft 2014-07-01 redovisas i avsnitt 4.1.1.
[4] Prop. 2013/14:51 s. 20.

bestånd och innefattar en rätt till okränkta landsgränser, ett bevarande av det svenska självstyret och det demokratiska statsskicket samt av nationens grundläggande funktionalitet. Det framhålls därvid att rikets säkerhet således inte enbart tar sikte på skyddet av det fysiska territoriet. Det avser också hävdandet av Sveriges suveränitet, vilket innebär att Sverige ska kunna bruka sin exklusiva frihet under det folkrättsliga regelverket för att självständigt utöva statens funktioner, vad avser såväl statens inre som yttre förbindelser. Vidare anförs att, trots att det finns en etablerad definition av begreppet, det är förknippat med viss osäkerhet och att det hänger åtminstone delvis samman med att de förhållanden som är av betydelse för rikets säkerhet kan förändras över tiden, bl.a. i takt med samhällsutvecklingen. Regeringen utvecklar det resonemanget på följande sätt.

> Tidigare var begreppet starkt förknippat med Försvarsmaktens verksamhet, eftersom det främsta hotet mot rikets säkerhet ansågs vara ett militärt angrepp. I dag är samhället och hotbilden mer komplex och föränderlig, vilket i sin tur har fört med sig att uppgifter hänförliga till förhållanden inom andra samhällssektorer kan vara av betydelse för rikets säkerhet. Vidare har den ökade internationaliseringen, och framför allt ett ökat internationellt samarbete inom det försvars- och säkerhetspolitiska området, inneburit att Sverige är mer beroende av sina relationer till andra länder för att i vissa lägen kunna upprätthålla skyddet för rikets säkerhet.
>
> Ibland hänvisas till ett lands yttre respektive inre säkerhet. I allmänhet avses då med den yttre säkerheten landets oberoende i förhållande till andra länder och med den inre säkerheten den inre sammanhållningen, samhällsordningen samt vitala politiska och ekonomiska funktioner. Utvecklingen har inneburit att det i vart fall i nu aktuellt sammanhang är svårare och mindre relevant att göra en sådan uppdelning. Som framgått omfattar begreppet rikets säkerhet förhållanden som kan hänföras både till den yttre och till den inre säkerheten.

I det betänkande som låg till grund för propositionen resoneras utförligare kring de konsekvenser som samhällsutvecklingen medfört i fråga om vad som behöver skyddas av hänsyn till rikets säkerhet.[5] Det konstateras därvid att vi i dag är mer beroende av olika samhällsfunktioner för att upprätthålla en fungerande vardag och att samhällsutvecklingen har inneburit ett ökat antal kontaktytor och att antalet kommunikationssätt har ökat kraftigt liksom till-

[5] Betänkandet Spioneri och annan olovlig underrättelseverksamhet (SOU 2012:95), s. 165 f.

gången till information och takten i vilken den produceras och konsumeras. Att utvecklingen har fört med sig att uppgifter som rör andra förhållanden än enbart vårt militära försvar i traditionell bemärkelse är skyddsvärda exemplifieras med förhållanden som är hänförliga till Sveriges beroende av och samarbete med andra länder liksom förhållanden som rör grundläggande samhällsfunktioner som kommunikationsnät och annan infrastruktur.

I fråga om tillämpningen av spioneribestämmelsen framhålls i betänkandet att tillgängliga rättsfall och övrig utredning inte ger uttryck för att spioneribestämmelsen tillämpats enbart när det varit fråga om uppgifter rörande det militära försvaret.[6] Det hänvisas i det sammanhanget till det s.k. Ericsson-målet[7] där det var fråga om bl.a. tillverkningssätt och konstruktion av produkter inom telekommunikationsområdet.

I den nämnda propositionen konstaterade regeringen att begreppet rikets säkerhet har en tillräckligt klar och tydlig innebörd samt är väl etablerat i praxis. Regeringens slutsats var därför att begreppet även i framtiden bör tjäna som utgångspunkt för straffbestämmelserna i 19 kap. brottsbalken. Ur språklig synvinkel ansåg dock regeringen att uttrycket *riket* är ålderdomligt och att det därför skulle bytas ut till *Sverige*, eller *landet*, i kapitelrubriken till 19 kap. och i lagtexten.

En tydligare definition av terrorism

När säkerhetsskyddslagen infördes fanns ingen definition av terrorism i straffrätten. Terrorism brukade beskrivas som våld eller hot om våld för politiska syften. Begreppet terrorism har därefter fått en mer distinkt innebörd genom att det särskilda terroristbrottet infördes till följd av EU:s rambeslut om skydd mot terrorism.[8] Begreppet terrorism i säkerhetsskyddslagen är i dag detsamma som terroristbrott enligt lagen (2003:148) om straff för terroristbrott.[9] Straffbestämmelsen består av två delar; dels ett kvalificerande

[6] a. bet. s.188f.
[7] Svea hovrätts dom den 20 oktober 2003 i mål B 5221-03.
[8] Prop. 2002/03:38 Straffansvar för terroristbrott, bet. 2002/03:JuU12, rskr. 2002/03:148 EGTL164/2002. s. 3.
[9] Se 6 § 3 säkerhetsskyddslagen som hänvisar till terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott.

rekvisit, dels en brottskatalog som upptar gärningar som ska bedömas som terroristbrott om det kvalificerande rekvisitet är uppfyllt. Det förutsätts att handlingen objektivt är sådan att den genom sin art eller sitt sammanhang allvarligt kan skada ett land eller en internationell organisation. En annan förutsättning är att handlingen begåtts i syfte att injaga allvarlig fruktan hos en befolkning, eller otillbörligen tvinga offentliga organ eller en internationell organisation att utföra eller avstå från att utföra en handling, eller allvarligt destabilisera eller förstöra de grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturerna i ett land eller i en internationell organisation. Innebörden av uttrycket *kunna allvarligt skada* är inte närmare utvecklad i rambeslutet. I den nämnda propositionen anges att det, bl.a. mot bakgrund av rambeslutets syfte och de rådsuttalanden som gjorts i samband med dess antagande, får anses innebära att gärningen ska kunna utgöra en svår påfrestning på samhället eller på en mellanstatlig organisation. Det anges naturligtvis omfatta gärningar som allvarligt kan skada de grundläggande strukturerna för ett demokratiskt samhälle som grunderna och formerna för statsskicket eller rättsordningen. Det framhålls vidare att rekvisitet emellertid inte är begränsat till gärningar som kan hota de grundläggande strukturerna i en stat eller som är av sådan omfattning att de kan få landsomfattande konsekvenser. Rekvisitet anges därför också innefatta gärningar som i övrigt kan allvarligt skada ett väsentligt allmänintresse eller orsaka allvarliga störningar i en stats samhällsfunktioner eller försörjningsmöjligheter. Enligt uttalandena omfattar det viktiga infrastruktursystem som allmänna kommunikationsnät och kommunikationsmedel, el- och vattenförsörjning, telekommunikationer, hälso- och sjukvård, radio och TV men även viktiga försörjningsgrenar och industrier samt handelsplatser såsom börser. Slutligen anges det också inrymma sådana för medborgarna väsentliga gemensamma intressen som värnandet av det öppna och säkra samhället.

11.2 En fortsatt utgångspunkt i begreppet rikets säkerhet

Bedömning: Begreppet rikets säkerhet som tar sikte på förhållanden av grundläggande betydelse för Sverige som möjligheterna att hävda landets oberoende i olika avseenden, är tillräckligt för att sammantaget beskriva de för nationen från ett säkerhetsskyddsperspektiv primärt skyddsvärda verksamheterna. Utan att någon ändring i sak är avsedd behöver därför inte det nuvarande tillägget om verksamheter som särskilt behöver ett skydd mot terrorism föras över till en ny säkerhetsskyddslag.

Förslag: Benämningen rikets säkerhet ska ersättas med *Sveriges säkerhet* vilket endast är en språklig ändring.

Är begreppet rikets säkerhet tillräckligt brett också i fråga om krav på säkerhetsskydd?

Överväganden som gjorts i andra sammanhang i fråga om för nationen särskilt skyddsvärda intressen och verksamheter är av stor betydelse för hur det skyddsvärda bör beskrivas i en reformerad säkerhetsskyddslag. Av särskild relevans är regeringens uttalanden vid översynen av spioneribestämmelsen. Den i det sammanhanget lämnade beskrivningen av innebörden av rikets säkerhet stämmer väl in på en allmänt hållen beskrivning av de skyddsintressen och de olika slag av verksamheter, såväl försvarsinriktade i en mer traditionell bemärkelse som civila, som vi anser är av intresse också från ett säkerhetsskyddsperspektiv. Vi instämmer i slutsatsen att begreppets innebörd måste bedömas i ljuset av samhällsutvecklingen vilket medför ett fokus på skydd av grundläggande samhällsfunktioner. En vidgning mot den civila sektorn är också ett framträdande drag i den nu gällande skyddslagen. Också i fråga om sekretess av hänsyn till rikets säkerhet kan en viss breddning av tillämpningsområdet skönjas. Att det i andra sammanhang tydliggörs att såväl försvarsinriktade som civila verksamheter kan ha betydelse för rikets säkerhet bör också påverka hur begreppet uppfattas i en säkerhetsskyddskontext.

Det bör i sammanhanget betonas att även om civila verksamheter inom olika samhällssektorer har fått en ökad betydelse för upprätthållandet av grundläggande samhällsfunktioner (och ytterst rikets säkerhet), så innebär det på intet sätt att den militära verksamhetens betydelse samtidigt skulle ha minskat. Det är snarare så, vilket vi också tagit upp i kapitel 9, att förändringar och instabilitet i vår relativt nära omvärld samtidigt medfört att det militära försvaret har fått en förnyad betydelse för rikets säkerhet.

Beskrivningen av säkerhetsskyddslagens tillämpningsområde utgår i dag inte enbart från begreppet rikets säkerhet utan också från skrivningar om verksamheter som *särskilt behöver skyddas mot terrorism*. Vår uppfattning är att tillägget om terrorism i beskrivningen av lagens tillämpningsområde medför en otydlighet i förhållande till begreppet rikets säkerhet. I propositionen till säkerhetsskyddslagen finns resonemang om att terroristbrott, oavsett om de utgör ett hot mot rikets säkerhet eller inte, innebär ett angrepp på de demokratiska spelreglerna i samhället och att skydd mot terrorism i vart fall kan anses ligga nära värnet om rikets säkerhet.[10] Som vi redogjort för har terrorism i säkerhetsskyddslagen i dag en mer distinkt betydelse. En fråga som har uppkommit är om det numera behövs en åtskillnad mellan verksamheter av betydelse för rikets säkerhet och verksamheter som särskilt behöver skyddas mot terrorism. Någon närmare analys av hur de intressen som terroristbrottet avser att skydda förhåller sig till begreppet rikets säkerhet redovisades inte i samband med att lagen om terroristbrott infördes. Vi ser det inte som meningsfullt att fördjupa oss i den frågan. Däremot anser vi oss ändå kunna dra slutsatsen att begreppet rikets säkerhet i princip bör vara tillräckligt för att täcka in även sådana särskilt skyddsvärda verksamheter som bestämmelserna om säkerhetsskydd till skydd mot terrorism tar sikte på. Det handlar i stor utsträckning om verksamheter som är skyddsobjekt enligt skyddslagen vilket redan det i regel innebär en koppling till rikets säkerhet.

Sammantaget har vi kommit fram till att begreppet rikets säkerhet omfattar sådana övergripande nationella intressen och samhällsvärden som också en reformerad säkerhetsskyddslag bör ta sikte på att skydda. Genom att ordet *rikets* bytts ut mot *Sveriges* i 19 kap.

[10] Prop. 1995/96:129 Säkerhetsskydd, s. 25.

brottsbalken framstår också begreppet som mer tidsenligt. Som vi tidigare har berört och som utvecklas i avsnitt 12.1 behöver också en reformerad säkerhetsskyddslag delvis utgå från bestämmelser om sekretess med hänsyn till rikets säkerhet. Sammantaget talar det för att rikets säkerhet, efter en språklig justering till *Sveriges säkerhet*, också i fortsättningen används vid en beskrivning av vilka verksamheter som omfattas av säkerhetsskyddslagen. Vi har ändå, vilket vi kommer in på i det följande, vissa betänkligheter med att i en beskrivning av säkerhetsskyddslagens syfte använda enbart uttrycket Sveriges säkerhet.

En risk för att tillämpningsområdet tolkas för snävt

Vi har i avsnitt 10.2 beskrivit att en viktig utgångspunkt för reformbehovet är att utveckla lagen för att bl.a. ge ett tydligare utrymme för säkerhetsskydd av andra anledningar än skydd mot obehörigt röjande av uppgifter. Med anledning av den inriktningen för reformbehovet ser vi vissa problem med att använda uttrycket Sveriges säkerhet. Det kan förefalla motsägelsefullt eftersom vi samtidigt har kommit fram till slutsatsen att begreppet Sveriges säkerhet, med utgångspunkt från bl.a. förarbetena till spionaribestämmelsen, har en tillräcklig bredd. Det problematiska är dock just att begreppet är centralt i annan lagstiftning där orsaken till skyddsbehoven kan sägas vara snävare. I fråga om sekretess handlar det uteslutande om ett skydd mot att uppgifterna röjs. Också straffbestämmelsen om spionaeri tar sikte på skydd av uppgifters innehåll även om den inte är begränsad till vare sig uppgifter som omfattas av sekretess eller förhållanden av hemlig natur. Skyddslagen å sin sida har ett relativt begränsat tillämpningsområde som är inriktat på att begränsa det fysiska tillträdet till vissa anläggningar etc. Att skydda för samhället centrala it-system utifrån behov av att säkerställa informationens tillgänglighet och riktighet ligger således utanför den lagstiftningens tillämpningsområde.

Vi konstaterar således att referensramen genom de grundläggande samhällsvärden som där innefattas i och för sig är tillräckligt bred. Vi ser emellertid samtidigt en risk för att den givna avgränsningen av vilka förhållanden som är skyddsvärda i andra sammanhang kan ha en negativ inverkan på tillämpningen av

säkerhetsskyddslagen. Därigenom skulle en användning av samma begrepp kunna motverka en utveckling av säkerhetsskyddet som tydligare inkluderar förhållanden som behöver skyddas från ett vidare perspektiv. Det gäller inte minst it-system där funktioner med avseende på tillgänglighet eller riktighet, dvs. systemens driftsäkerhet och funktionalitet, är av kritisk betydelse för ett fungerande samhälle.

De betänkligheter vi har inför att också fortsättningsvis behålla rikets/Sveriges säkerhet som enda referensram för tillämpningsområdet för säkerhetsskyddet beror också på att begreppet även används just i straffbestämmelser och bestämmelser om sekretess som innebär andra intresseavvägningar. För lagstiftning av sådant slag kan hänsynen till motstående allmänna och enskilda intressen, som bl.a. den enskildes rättssäkerhet och rätten att ta del av allmänna handlingar, medföra en relativt restriktiv tolkning av vilka förhållanden som faller inom tillämpningsområdet. Vi ser således en risk att en återhållsam tillämpning i dessa sammanhang spiller över på en bedömning av vilka verksamheter som behöver ett säkerhetsskydd. Det riskerar att bidra till att säkerhetsskyddets tillämpningsområde uppfattas som snävare än avsett.

Vidare har begreppet rikets säkerhet i säkerhetsskyddssammanhang starkt kommit att förknippas med militära förhållanden. Såväl Säkerhetspolisen som har tillsynsansvar för säkerhetsskydd på det civila området som flera av de säkerhetsskyddsstödjande myndigheterna,[11] bl.a. Affärsverket svenska kraftnät har påtalat svårigheter med att till alla de verksamheter som har att tillämpa säkerhetsskyddslagen förmedla att rikets säkerhet och säkerhetsskydd inte tar sikte på bara militära förhållanden. Det är därför av värde att regeringen i samband med förändringarna i 19 kap. brottsbalken uttalat stöd för att begreppet måste ses i ljuset av samhällsutvecklingen och betonat att utvecklingen har fört med sig att uppgifter

[11] I direktiven används benämningen sektorsansvariga myndigheter som en samlande benämning för Affärsverket svenska kraftnät, Post- och telestyrelsen, Transportstyrelsen och länsstyrelserna. Som framgår av avsnitt 10.1.5 har vi i stället valt att använda säkerhetsskyddsstödjande myndigheter som en samlande benämning för dessa myndigheter såvitt avser deras funktioner för säkerhetsskyddet. Vi föreslår vidare i avsnitt 18.10 och 21.2.4 att Myndigheten för samhällsskydd och beredskap ska ta över de uppgifter Länsstyrelserna i detta avseende har samt även i vissa avseenden vara säkerhetsskyddsstödjande myndighet för kommuner och landsting.

som är skyddsvärda med hänsyn till Sveriges säkerhet i dag kan finnas inom fler områden än tidigare.

En beskrivning som enbart utgår från Sveriges säkerhet

Som framgått ser vi en risk med att uttrycket Sveriges säkerhet i en säkerhetsskyddskontext framkallar allt för snäva associationer. En fråga som infinner sig är därför om det är lämpligt att i säkerhetsskyddslagen komplettera eller förtydliga uttrycket på något sätt.

Ett alternativ vi har övervägt är att lägga till någon form av exemplifiering av vilka slag av skyddsvärda verksamheter som lagen tar sikte på. En sådan exemplifiering finns t.ex. i straffbestämmelsen om spionerі. Vi har dock kommit till den slutsatsen att det utifrån säkerhetsskyddsbehov är svårt att utforma en exemplifiering som tydliggör utan att uppfattas som uttömmande och som också har förutsättningar att stå sig över tid.

Ett annat alternativ är att komplettera begreppet Sveriges säkerhet med ytterligare något uttryck eller att använda sig av någon form av mer utvecklad beskrivning. Viktigt är dock att en sådan komplettering eller omskrivning inte öppnar upp för en förskjutning till en lägre nivå. Något annat än de verksamheter som i vår pyramidskiss i avsnitt 10.1.1 kan sägas höra till den övre delen av skyddsvärda verksamheter bör inte omfattas av lagens tillämpningsområde. Vi har i fråga om tänkbara kompletterande begrepp som kan uppfylla sådana krav studerat bl.a. den nederländska och den norska lagstiftningen på området.[12] Ett kompletterande uttryck skulle kunna vara *övriga vitala nationella säkerhetsintressen*. Ett förslag på förtydligande omformulering som förts fram är *skyddet av Sveriges vitala nationella säkerhetsintressen*. Mot sådana lösningar kan invändas att ett till *Sveriges säkerhet* kompletterande uttryck eller någon form av förtydligande omformulering kan skapa osäkerhet i fråga om tillämpningsområdet för bl.a. straffbestämmelsen om spionerі där enbart uttrycket Sveriges säkerhet används. Sådana risker kan dock hanteras. Som framförts tidigare sammanfaller inte skyddsperspektiven.

[12] Beträffande lagstiftningen i Nederländerna och Norge se den internationella utblicken i kapitel 8.

En annan invändning som det finns större fog för är att en komplettering för att komma ifrån en snäv tolkning skapar en ny osäkerhet om vad kompletteringen tar sikte på. Erfarenheter som vi tagit del av vid vårt studiebesök i Norge visar dessutom att ett tillägg om *vitala säkerhetsintressen* inte med säkerhet får den följden att tillämpningsområdet uppfattas som mindre snävt.

Sammantaget ser vi det inte som en lämplig lösning att försöka motverka en eventuell alltför snäv tillämpning genom någon form av komplettering till uttrycket Sveriges säkerhet. Vi har därför i våra överväganden stannat vid att det för nationen från säkerhetsskyddshänseende skyddsvärda området enbart ska beskrivas som *verksamheter av betydelse för Sveriges säkerhet*.

Det ska tilläggas att vi ser det som möjligt att lyfta fram tillämpningsområdets bredd genom lagens utformning i övrigt. De gäller bl.a. i fråga om beskrivningen av det närmare syftet med de olika säkerhetsskyddsåtgärderna som tydligare än i dag bör kunna ge uttryck för att säkerhetsskydd är en angelägenhet för betydligt fler verksamheter än de myndigheter som hanterar försvarshemligheter och andra uppgifter som behöver skyddas mot ett röjande. En viktig komponent är därvid en ny uppbyggnad av säkerhetsskyddslagen varigenom skydd av s.k. *hemliga uppgifter* ersätts av *säkerhetsskyddsklassificerade uppgifter* som är ett vidare begrepp och där det också görs tydligt att säkerhetsskydd också är en angelägenhet för verksamheter som, även om de inte hanterar säkerhetsskyddsklassificerade uppgifter, är av betydelse för Sveriges säkerhet eller förbindelser med annan stat eller mellanfolklig organisation (i övrigt säkerhetskänslig verksamhet). Vi återkommer i avsnitt 12.1 till innebörden av begreppet säkerhetsskyddsklassificerade uppgifter och till de två nu nämnda huvudinriktningarna för säkerhetsskyddet. Dessförinnan behandlar vi bl.a. frågan om ett tydligare lagstöd för säkerhetsskydd avseende uppgifter som Sverige i förhållande till annan stat eller mellanfolklig organisation har åtagit sig att skydda.

11.3 Säkerhetsskydd till följd av internationella åtaganden

Förslag: Säkerhetsskyddslagens tillämpningsområde ska omfatta även verksamhet som avses i ett för Sverige, i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd (*internationellt säkerhetsskyddsåtagande*).

Lagen ska även i övrigt ge stöd för internationell samverkan på säkerhetsskyddsområdet.

Internationella säkerhetsskyddsåtaganden

Som vi redogjort för tidigare har sambandet mellan skyddet av Sveriges säkerhet och skyddet av säkerhetsintressen hänförliga till andra stater och mellanfolkliga organisationer förstärkts sedan säkerhetsskyddslagen infördes. Bland annat har medlemskapet i EU medfört att det blir allt svårare att dra en gräns för vad som utgör svenska säkerhetsintressen. Det påverkar också synen på vad som är av betydelse för Sveriges säkerhet.

Ett tydligt stöd för säkerhetsskydd som följer av folkrättsliga förpliktelser är viktigt vid en beskrivning av säkerhetsskyddslagens syfte. Sverige har ingått generella säkerhetsskyddsavtal med ett trettiotal stater. Därutöver finns multilaterala säkerhetsskyddsavtal dels mellan de nordiska länderna, dels mellan EU:s medlemsstater.[13] Säkerhetsskyddsavtal har också ingåtts med flera mellanfolkliga organisationer, bl.a. Nato och ESA. Som vi redogjort för i kapitel 6 innebär avtalen skyldigheter i fråga om säkerhetsskyddsåtgärder och medför också behov av en tydlig reglering för att kunna utfärda säkerhetsintyg för personer och leverantörer som ska delta i verksamhet som omfattas av avtalen. Utöver de gällande säkerhetsskyddsavtalen innebär också för Sverige bindande EU-rättsakter och andra internationella regelverk, inom bl.a. områdena hamnskydd och luftfartsskydd, åtaganden i fråga om säkerhetsskydd. Även om svenska säkerhetsintressen i praktiken t.ex. inom ramen för ett försvarsmaterielprojekt eller utvecklingsprojekt inom rymdområdet ofta kan anses sammanfalla med en annan stats eller

[13] Avtalet mellan EU:s medlemsstater har ännu inte trätt i kraft.

mellanfolklig organisations säkerhetsintressen, är inte enbart en hänvisning till Sveriges säkerhet tillräcklig. Som vi nämnt tidigare i avsnitt 10.2.1 bör säkerhetsskyddslagen därför kompletteras för att tydligare ge stöd för skyddsåtgärder avseende uppgifter som omfattas av internationella säkerhetsskyddsåtaganden.

Vårt förslag är att lagens tillämpningsområde bör anges inkludera verksamhet som omfattas av ett för Sverige i förhållande till annan stat eller mellanfolklig organisation förpliktande åtagande om säkerhetsskydd (*internationellt säkerhetsskyddsåtagande*). Genom ett sådant tillägg ges ett tydligare stöd för säkerhetsskydd avseende uppgifter som Sverige i förhållande till annan stat eller mellanfolklig organisation genom någon form av säkerhetsskyddsavtal har åtagit sig att skydda. Det ger också samtidigt ett tydligare stöd för säkerhetsskyddsåtgärder som följer av EU-rätten och internationella konventioner inom bl.a. luftfartsskyddet t.ex. i fråga om säkerhetsprövningsåtgärder avseende personal vid flygplatser och annan verksamhet av betydelse för luftfartsskyddet.[14]

Internationell samverkan i övrigt på säkerhetsskyddsområdet

Utöver ett tydligare stöd för säkerhetsskyddsåtgärder som är en direkt följd av folkrättsliga förpliktelser bör säkerhetsskyddslagen ge uttryck för behovet av att stödja internationell samverkan i övrigt på säkerhetsskyddsområdet. Till följd av internationella projekt där Sverige eller svenska företag avser att delta såväl inom försvarsmaterielområdet som inom den civila säkerhetssektorn kommer ett fortsatt behov finnas av att ingå nya eller omförhandlade avtal om säkerhetsskydd med andra länder. Som vi återkommer till i kapitel 20 behöver den uppgiften och styrningen av den tydliggöras. Vidare bör det av beskrivningen av lagens syfte framgå att lagen också i övrigt ska ge stöd för internationell säkerhetsskyddssamverkan. En sådan skrivning har också betydelse i andra avseenden. Det finns behov av att bistå andra länder med utredningsunderlag i säkerhetsprövningsärenden och av att kunna ut-

[14] Jfr 26 § första stycket 2 säkerhetsskyddsförordningen som möjliggör registerkontroll i verksamhet som har betydelse för luftfartsskyddet, om det följer av en internationell överenskommelse som Sverige har tillträtt eller av en bindande EU-rättsakt på området för luftfartsskydd att säkerhetsprövningen ska omfatta registerkontroll.

färda säkerhetsintyg för personer och leverantörer. Redan i dag finns vissa bestämmelser i säkerhetsskyddsförordningen och säkerhetsskyddslagen om registerkontroll och ingående av säkerhetsskyddsavtal som är avsedda att kunna användas i samarbetet med andra länder och mellanfolkliga organisationer. Avsikten med bestämmelserna är att ge underlag för säkerhetsintyg som kan underlätta för enskilda och företag att delta i säkerhetskänslig verksamhet i ett annat land eller i en mellanfolklig organisation. Den regleringen behöver som nämnts utvecklas, inte minst för att bättre stämma överens med Sveriges internationella säkerhetsskyddsåtaganden. De förslag vi lämnar i kapitel 20 innebär dock, i linje med de behov som förutsågs redan när säkerhetsskyddslagen infördes ett utrymme för att utfärda säkerhetsintyg också i vissa situationer där den verksamhet som intyget behövs för varken direkt berör Sveriges säkerhet eller en verksamhet som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande. Också behovet av ett mer utvecklat regelverk om sådana underlag och intyg föranleder därför ett tillägg om att lagen även i övrigt ska ge stöd för internationell samverkan på säkerhetsskyddsområdet.

11.4 Säkerhetskänslig verksamhet – en samlande benämning

Förslag: *Säkerhetskänslig verksamhet* förs in i säkerhetsskyddslagen som en samlande benämning för

1. verksamhet av betydelse för Sveriges säkerhet, samt
2. verksamhet som omfattas av ett för Sverige, i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd (dvs. ett internationellt säkerhetsskyddsåtagande).

Som en allmän utgångspunkt har vi kommit fram till att också en reformerad säkerhetsskyddslag bör utgå från skydd av viss *verksamhet*. I fråga om de nationella säkerhetsintressen som säkerhetsskyddslagen tar sikte på har vi föreslagit att tillämpningsområdet ska beskrivas som verksamhet som är av *betydelse för Sveriges säkerhet*. Vidare har vi föreslagit att tillämpningsområdet ska

utsträckas till verksamhet som *omfattas av internationella säkerhetsskyddsåtaganden*.

Lagens skyddsintressen kan lämpligen samlat framgå av en inledande bestämmelse om lagens syfte. För att förenkla regleringen i efterföljande lagbestämmelser och i till lagen anslutande förordning ser vi fördelar med att sammanfatta de skyddsintressen som lagen tar sikte på i ett gemensamt begrepp.

I dag används i säkerhetsskyddsförordningen begreppet *säkerhetskänslig verksamhet*. Det definieras i 4 § 3 säkerhetsskyddsförordningen som verksamhet av betydelse för rikets säkerhet. Termen används mycket sparsamt i säkerhetsskyddsförordningen och verkar inte heller ha kommit att användas vid tillämpningen av säkerhetsskyddslagstiftningen.[15] Mot den bakgrunden anser vi att uttrycket bör kunna ges en vidare innebörd och innefatta lagens skyddsintressen i sin helhet. Med *säkerhetskänslig verksamhet* ska således avses verksamhet av betydelse för Sveriges säkerhet samt verksamhet som ska skyddas med hänsyn till internationella säkerhetsskyddsåtaganden.

11.5 Mot vad ska lagen skydda?

Förslag: Också av en reformerad säkerhetsskyddslag ska det framgå att åtgärder enligt lagen ska skydda mot bl.a. spionerі, sabotage och terroristbrott.

Det skydd som tar sikte på att uppgifter som är säkerhetskänsliga på annat sätt obehörigen röjs, ändras, görs otillgängliga eller förstörs ska även i fortsättningen komma till uttryck i bestämmelsen om vad säkerhetsskyddslagen på ett övergripande plan ska skydda mot. Det skyddet ska omfatta också uppgifter som ska skyddas enligt internationella säkerhetsskyddsåtaganden.

[15] Uttrycket används endast i 29 § säkerhetsskyddsförordningen som innehåller bestämmelser om utlämnade av uppgifter som tillförts polisregister efter det att registerkontroll har gjorts.

Frågan *Mot vad behövs ett skydd?* har vi redan berört i avsnitt 10.2.3. Vi konstaterade där att även en reformerad säkerhetsskyddslag bör vara inriktad mot att genom förebyggande åtgärder skydda verksamheter som är särskilt skyddsvärda för nationen mot antagonistiska hot som spionerі, sabotage och terroristbrott. Vi har ställt oss frågan vilken funktion en bestämmelse som den som i dag finns i 6 § säkerhetsskyddslagen och som övergripande anger vad säkerhetsskyddet ska förebygga egentligen fyller. Av den internationella utblicken framgår att de hot som säkerhetsskyddet ytterst tar sikte på sällan har någon framträdande plats i de studerade regelverken. Inriktningen mot antagonistiska hot framgår i stället av den närmare beskrivningen av de olika säkerhetsskyddsåtgärderna.

Ett alternativ till nuvarande hänvisning till vissa brott kunde vara att tydligt ange vad de olika säkerhetsskyddsåtgärderna ska syfta till. En hänvisning av det slag som finns i dag är i och för sig inte nödvändig. Samtidigt finns det behov av att i förhållande till närliggande reglering med ett mer vidsträckt skyddsperspektiv, t.ex. om samhällsskydd, tydliggöra säkerhetsskyddslagens inriktning på skydd mot antagonistiska hot. Vi anser därför att en bestämmelse som på en övergripande nivå anger *vad* lagen ska skydda mot ändå fyller en funktion.

Säkerhetsskyddet kan beroende på verksamhetens art och omständigheterna i övrigt behöva riktas mot hot avseende brott av skilda slag. I avsnitt 4.1 finns en redogörelse för brott som skyddet kan behöva ta sikte på att förebygga. Liksom i dag ska det i säkerhetsskyddslagen finnas en exemplifiering av för säkerhetsskyddet centrala brott. Terroristbrott, som i dag nämns särskilt (6 § 3 säkerhetsskyddslagen), bör i stället läggas till i den generella exemplifieringen av brott som lagen syftar till att förebygga.

I direktiven framhålls behovet av ett tydligare stöd för att genom säkerhetsskyddsåtgärder skydda t.ex. samhällsviktig verksamhet vars funktionalitet är av betydelse för Sveriges säkerhet mot andra brottsliga angrepp, även om angreppet i det konkreta fallet inte anses kunna hota Sveriges säkerhet. Några exempel lämnas inte i direktiven men det skulle kunna vara fråga om ett skydd mot bl.a. förmögenhetsbrott vars primära syfte inte är att skada samhällsviktiga intressen men som ändå får den följden. Vad som är viktigt att förebygga är således brott som, oavsett motiv, kan innebära allvar-

liga konsekvenser för Sveriges säkerhet. En stöld av datorer i ett luftövervakningssystem kan på ett sådant sätt medföra begränsningar i skyddet av Sveriges territorium trots att detta inte var avsikten med stölden. Också dataintrång, olaga intrång och skadegörelse är tänkbara brott som utan att det är avsikten med brottet kan innebära indirekta följder som hotar Sveriges säkerhet. Frågan är om det av lagen uttryckligen bör framgå att säkerhetsskyddet ska avse även brott som kan få sådana indirekta följder. Att det i säkerhetsskyddslagen anges att lagens syfte är att skydda mot vissa i förhållande till Sveriges säkerhet allvarliga brott bör innefatta också ett skydd mot brott som ger konsekvenser för Sveriges säkerhet. Vi anser att det inte behövs något förtydligande i författningstexten.

I 6 § 2 säkerhetsskyddslagen anges att med säkerhetsskydd avses också skydd i andra fall (än det skydd mot brott som beskrivs i paragrafens första punkt) av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet.[16] Av förarbetena framgår att skyddet ska motverka allt röjande, ändrande och förstörande av sekretessbelagda uppgifter som rör rikets säkerhet, oavsett om det sker uppsåtligen eller av oaktsamhet.[17]

Ytterst handlar det även i detta avseende i huvudsak om att i förlängningen förebygga brott som t.ex. oaktsamt förfarande med hemliga uppgifter kan leda till. Det bör inflikas att digitaliseringen av information medfört att det i dag också handlar om ett skydd mot att uppgifterna görs otillgängliga. Det kan ifrågasättas om det i detta sammanhang särskilt behöver anges att bl.a. röjande av uppgifter i övrigt ska förebyggas. Det skulle kunna vara tillräckligt att detta förhållande i stället framgår av efterföljande bestämmelser om vad de olika säkerhetsskyddsåtgärderna särskilt syftar till. Vi har emellertid kommit fram till att ett sådant förtydligande ändå bör finnas kvar. Om skrivningen i fråga tas bort, skulle det kunna uppfattas som att ett sådant skydd inte längre behövs. Dessutom skulle antagonistiska hot som inte utgör brott, t.ex. avlyssning av trådlös kommunikation, inte omfattas av lagen. Även med hänsyn till förpliktelser som följer av internationella säkerhetsskydds-

[16] S.k. hemliga uppgifter enligt definition i 3 § säkerhetsskyddsförordningen.
[17] Prop. 1995/96:129 Säkerhetsskydd, s. 26 f., se särskilt Lagrådets yttrande s. 129.

åtaganden kan det finnas skäl att vara tydlig i fråga om säkerhetsskyddets omfattning. En bestämmelse som motsvarar den som i dag finns i 6 § 2 säkerhetsskyddslagen bör därför finnas även i en reformerad säkerhetsskyddslag. Som utvecklas i det följande kapitlet bör den dock inte avse hemliga uppgifter utan *säkerhetsskyddsklassificerade uppgifter* för att även innefatta uppgifter som ska skyddas enligt internationella säkerhetsskyddsåtaganden.

12 Säkerhetskänslig verksamhet – två huvudsakliga inriktningar

I det här kapitlet behandlas frågor om den övergripande inriktningen för åtgärder som ska vidtas med stöd av säkerhetsskyddslagen. I dag är säkerhetsskyddslagen i hög grad uppbyggd kring behovet av att från ett konfidentialitetsperspektiv skydda uppgifter av betydelse för rikets säkerhet. Som beskrivits tidigare har den ökade internationaliseringen och samhällsutvecklingen i övrigt medfört att en sådan inriktning kommit att bli för snäv. En viktig utgångspunkt är att en reformerad säkerhetsskyddslag behöver ge ett större utrymme för och vara tydligare vad gäller skydd av uppgifter och andra förhållanden som av annan anledning än konfidentialitetsbehov är av betydelse för Sveriges säkerhet. Vidare behöver lagens uppbyggnad anpassas till att skyddet inte enbart handlar om Sveriges säkerhet utan också ett behov av att uppfylla förpliktelser som kommer till uttryck i internationella säkerhetsskyddsåtaganden (se avsnitt 11.3). I det följande avsnittet redogör vi för hur syftet och tillämpningsområdet för de olika säkerhetsskyddsåtgärderna kan utvecklas genom en ny systematik som utgår från de skyddsbehov som finns i

- verksamheter som innebär hantering av *säkerhetsskyddsklassificerade uppgifter*, och
- verksamheter som av annan anledning är säkerhetskänslig *(i övrigt säkerhetskänslig verksamhet*).

Den första kategorin, som innebär en utvidgning i förhållande till vad som i dag benämns hemliga uppgifter, behandlas vidare i avsnitt 12.2.

Den senare kategorin, som systematiskt ersätter men samtidigt bl.a. inkluderar vad som i dag skyddas inom ramen för skydd mot terrorism, behandlas vidare i avsnitt 12.3.

Dessförinnan utvecklar vi i det följande avsnittet varför en ny systematik behövs och varför beskrivningen av de åtgärder som vidtas med stöd av säkerhetsskyddslagen behöver ha en delvis förändrad ansats.

12.1 En ny systematik

Nuvarande systematik

Säkerhetsskyddet är i dag i hög grad inriktat mot ett skydd för *hemliga uppgifter*. Med hemliga uppgifter avses i säkerhetsskyddslagstiftningen uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL, och som rör rikets säkerhet (4 § 1 säkerhetsskyddsförordningen). Inriktningen mot att skydda hemliga uppgifter är tydlig. Centralt för säkerhetsskyddet är placering av anställningar i säkerhetsklass som, i olika grad, förutsätter att den anställde ska hantera hemliga uppgifter (17 § säkerhetsskyddslagen). Placering i säkerhetsklass är i sin tur i stor utsträckning avgörande för möjligheterna till registerkontroll i samband med säkerhetsprövning (13 § säkerhetsskyddslagen). Också bestämmelserna om informationssäkerhet är inriktade på att skydda hemliga uppgifter (7 § 1 säkerhetsskyddslagen).

Bestämmelserna om säkerhetsskydd med inriktning mot skydd av hemliga uppgifter kompletteras i dag genom bestämmelser om säkerhetsskydd för *verksamheter som särskilt behöver skyddas mot terrorism.* Tillämpningsområdet i fråga om sådant säkerhetsskydd avgränsas, i vart fall i fråga om möjligheter till registerkontroll, i hög grad till verksamhet som bedrivs vid skyddsobjekt enligt skyddslagen (2010:305).

En för snäv avgränsning

Säkerhetsskyddslagen behöver utvecklas för att det faktiska tillämpningsområdet ska bli tydligare och mer ändamålsenligt. I fråga om skyddet av uppgifter från konfidentialitetssynpunkt har vi

i avsnitt 10.2.1 pekat på behovet av en breddning och ett tydliggörande i förhållande till begreppet hemliga uppgifter. Det handlar om tydligare stöd för säkerhetsskyddsåtgärder dels i fråga om uppgifter som ska skyddas enligt säkerhetsskyddsavtal och andra internationella säkerhetsskyddsåtaganden, dels när för nationen känsliga uppgifter hanteras i enskild verksamhet (dvs. verksamheter där bestämmelser om sekretess inte gäller). Utöver de nämnda behoven i fråga om skydd av ”konfidentialitetskänsliga” uppgifter handlar reformbehovet om att den övriga delen av säkerhetsskyddet, dvs. det som i dag hänförs till skydd mot terrorism, behöver få ett mer ändamålsenligt avgränsat tillämpningsområde. Det finns bl.a. behov av att tydligare inkludera informationstillgångar och elektroniska kommunikationssystem som utifrån höga krav på riktighet och tillgänglighet är av kritisk betydelse för ett fungerande samhälle. Ett motsvarande behov finns i fråga om vissa anläggningar eller objekt inom bl.a. kärnkraftsindustrins område som kan utnyttjas för att åstadkomma för nationen allvarliga skadeverkningar. I dessa avseenden är en avgränsning som anknyter till skyddsobjekt enligt skyddslagen inte ändamålsenlig. En grundläggande förutsättning för att något ska kunna vara ett skyddsobjekt är nämligen att det finns behov av ett fysiskt skydd dvs. bevakningsåtgärder eller perimeterskydd av t.ex. en anläggning eller ett område. Det medför bl.a. att it-system, där ett s.k. logiskt skydd är påkallat, inte har ansetts vara lämpliga som skyddsobjekt.[1] Att avgränsningen i fråga om säkerhetsprövning utgörs av verksamhet *vid* skyddsobjektet medför vidare tveksamhet i fråga om vad som gäller för personal som tjänstgör i till skyddsobjektet anslutande verksamhet eller personal som inte rent fysiskt utför sitt arbete vid skyddsobjektet som bl.a. är fallet vid fjärrstyrning av driftsystem. En annan aspekt i fråga om avgränsningen till skyddsobjekt är att tillämpningen av säkerhetsskyddslagen blir avhängig att lagstiftningen om skyddsobjekt fungerar som avsett. Som vi redogjort för i avsnitt 4.3 ger den reformerade skyddslagen stöd för att i större utsträckning skydda samhällsviktiga verksamheter inom den civila sektorn. Skyddsobjekt kan avse såväl offentlig som privat verksamhet. En ansökan från den som driver verksamheten är i princip en

[1] Se vidare avsnitt 4.3 angående överväganden i förarbeten till skyddslagen i fråga om lämpligheten av att utvidga skyddslagen till att kunna omfatta skydd av it-system.

förutsättning för att något ska utgöra skyddsobjekt. Detta medför t.ex. krav på bevakningsåtgärder. Det har bl.a. från Affärsverket svenska kraftnät påtalats att det verkar finnas en tendens att skyddsobjekten inom elförsörjningen blir allt färre och att kostnads- och effektivitetskrav medför att behovet av skyddsåtgärder får stå tillbaka. Den i dag ensidiga inriktningen på verksamhet vid skyddsobjekt behöver mot bakgrund av vad som anförts därför omprövas.

Som vi tidigare har redovisat bör inte heller denna del av säkerhetsskyddet definieras genom hot om terrorism. Skyddet bör i stället vara anpassat till att kunna skydda mot olika slag av antagonistiska hot. En utgångspunkt för vårt förslag till reformerad säkerhetsskyddslag är därför att bestämmelser som ensidigt tar sikte på att skydda mot terrorism inte bör föras över till den nya lagen (se avsnitt 10.2.3). Säkerhetsskyddslagen bör även i fortsättningen gälla i fråga om t.ex. tillträde till säkerhetsområden för flygplatspersonal och för personal vid skyddsobjekt inom elförsörjningen. Den verksamhet som i dag omfattas av krav på säkerhetsskydd genom säkerhetsskyddslagens bestämmelser om verksamheter som behöver ett skydd mot terrorism behöver därför definieras på annat sätt.

Behövs över huvud taget en koppling till bestämmelser om sekretess?

Säkerhetsskyddslagens koppling till bestämmelser om sekretess framhålls bl.a. i våra direktiv som en starkt bidragande orsak till att lagstiftningen i dag inte upplevs som ändamålsenlig. En fråga som vi därför inledningsvis ser behov av att beröra är om det är möjligt och lämpligt att helt frångå säkerhetsskyddslagens nuvarande koppling till bestämmelser om sekretess i offentlighets- och sekretesslagen.

Kopplingen som den ser ut i dag har onekligen brister eftersom den medför att tillämpningsområdet tenderar att bli för snävt i flera avseenden. Å andra sidan innebär hänvisningen till bestämmelser om sekretess som rör rikets säkerhet att en avsevärd delmängd av vad som är mest skyddsvärt för nationen ändå kan avgränsas förhållandevis enkelt och tydligt. I fråga om myndigheter som i stor omfattning hanterar sådana uppgifter har det inte heller kommit

fram några egentliga problem med att, utifrån relevanta bestämmelser om sekretess, identifiera uppgifter som behöver ett säkerhetsskydd. Såvitt vi känner till fungerar konstruktionen med hänvisningen till offentlighets- och sekretesslagen förhållandevis bra även för verksamhet inom ramen för säkerhetsskyddad upphandling. Generellt sett finns det dock i dag brister vad gäller möjligheten att ställa krav på säkerhetsskydd i enskilda verksamheter. Vi återkommer till den frågan i det följande.

Om hänvisningen till offentlighets- och sekretesslagen skulle tas bort, uppstår behov av att på ett annat sätt identifiera uppgifter som behöver omfattas av krav på säkerhetsskydd. Det är svårt att se några egentliga alternativ till den identifiering av känsliga uppgifter som behövs. Jämförelsen med andra länder visar att identifiering och klassificering av känsliga informationstillgångar ofta görs enbart från ett konfidentialitetsperspektiv, dvs. behovet av säkerhetsskydd avgörs utifrån någon form av bedömning av vilka konsekvenser ett röjande av uppgiften skulle få. Sådana bedömningar utgör också i regel grund för vilken nivå som behövs avseende säkerhetsskyddet för uppgiften i fråga. Placering av anställningar i säkerhetsklass enligt säkerhetsskyddslagen avgörs på ett liknande sätt.[2]

Intrycken från utredningens internationella utblick är vidare att identifieringen av vad som är skyddsvärt i regel görs på en verksamhetsnivå också i de studerade länderna. I Tjeckien har man dock genomfört en identifiering och klassificering av känsliga uppgifter på nationell nivå. Vilka slag av uppgifter som avses och deras klassificering framgår av en förordning.[3] Vi ser inga fördelar med en sådan lösning. En sådan nationell identifiering och klassificering, även om den skulle modifieras och bl.a. innefatta en återkommande uppdatering, riskerar att ha en cementerande verkan på vad som ska anses vara särskilt skyddsvärt. Säkerhetspolisen menar också att det varken är möjligt eller önskvärt att utforma en uttömmande lista över vad som identifierats som skyddsvärt för nationen. Det är också vår uppfattning att identifieringen för att vara meningsfull och ändamålsenlig framför allt måste göras på en

[2] Enligt gällande reglering bestäms placeringen i säkerhetsklass dock genom en kombination av nivån på uppgifternas skyddsvärde och omfattningen av uppgifter på en viss nivå.
[3] Se avsnitt 8.2.2.

verksamhetsnivå och också kontinuerligt behöver omprövas och uppdateras. Den säkerhetsskyddsanalys som myndigheter och andra som säkerhetsskyddslagen gäller för ska utföra är en viktig komponent för att säkerhetsskyddet därigenom ska träffa rätt och få en väl avvägd omfattning (se vidare avsnitt 13.2).

Sammanfattningsvis har vi kommit fram till att kopplingen till bestämmelser om sekretess fyller en viktig funktion för att i vart fall delvis kunna identifiera vad som behöver skyddas enligt säkerhetsskyddslagstiftningen och därför bör vara ett centralt inslag också i en reformerad säkerhetsskyddslag (se vidare avsnitt 12.2).

Hantering av säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet

Med utgångspunkt i vad som redovisats ovan har vi kommit fram till att säkerhetsskyddet bör utgå från två huvudsakliga funktioner eller delområden – dels skydd av uppgifter där behovet av skydd framför allt hänger samman med uppgifternas konfidentialitet, dels verksamhet som av andra anledningar behöver omges med ett säkerhetsskydd. Den första kategorin har vi identifierat som verksamhet som innebär *hantering av säkerhetsskyddsklassificerade uppgifter*. Begreppet säkerhetsskyddsklassificerade uppgifter innebär en breddning i förhållande till det nuvarande begreppet hemliga uppgifter på så sätt att såväl uppgifter i enskild verksamhet som uppgifter som ska skyddas enligt internationella säkerhetsskyddsåtaganden tydligare omfattas. Vad begreppet säkerhetsskyddsklassificerade uppgifter tar sikte på utvecklas i avsnitt 12.2.

Den andra funktionen eller delområdet för säkerhetsskyddet kan sägas ta sikte på bl.a. verksamheter vid skyddsobjekt där det behövs ett förstärkt skydd avseende det fysiska tillträdet eller verksamheter där det finns ett nationellt behov av ett förstärkt skydd för informationstillgångar (it-system m.m.) utifrån informationssäkerhetskraven tillgänglighet och riktighet. Delområdet, som vi identifierat som *i övrigt säkerhetskänslig verksamhet*, motsvarar delvis vad som i dag skyddas inom ramen för skydd mot terrorism. Vad som därutöver bör kunna hänföras till sådan verksamhet utvecklas i avsnitt 12.3.

Självfallet kan en verksamhet omfattas av båda de beskrivna kriterierna. I dag är det av viss betydelse om verksamheten endast omfattas av säkerhetsskyddslagen på grund av bestämmelserna om skydd mot terrorism. Det beror på att den grunden inte innebär placering av anställningar i säkerhetsklass. Överlag ger säkerhetsskyddslagstiftningen i dag intryck av att den del av säkerhetsskyddet som inte handlar om hemliga uppgifter närmast ses som ett kompletterande skydd. En sådan ordning bör inte behållas. Som framgår av våra förslag i avsnitt 16.1, 17.1 och 18.1 föreslås syftet med de olika åtgärdsområdena (informationssäkerhet, fysisk säkerhet och personalsäkerhet) beskrivas med utgångspunkt från såväl de skyddsbehov som finns när en verksamhet hanterar säkerhetsskyddsklassificerade uppgifter som de skyddsbehov som finns i verksamheter som av annan anledning är säkerhetskänsliga. Några skillnader i fråga om åtgärder och förfarandet för de två inriktningarna anser vi inte vara motiverade. Det innebär, vilket vi utvecklar i avsnitt 18.6, ett vidare tillämpningsområde för placering i säkerhetsklass. Enligt vårt förslag ska en säkerhetsprövning normalt föregås av ett beslut om att anställningen eller deltagandet i verksamheten ska placeras i säkerhetsklass. Den registerkontroll som i dag görs inom ramen för skydd mot terrorism kommer således enligt vårt förslag att inordnas i det system som gäller för säkerhetsprövning vid placering i säkerhetsklass.

I stället för den systematik som finns i dag, där säkerhetsskyddet utgår från skydd av hemliga uppgifter och kompletteras av ett skydd mot terrorism, bör säkerhetsskyddet således utgå från ett mer övergripande behov av att skydda säkerhetskänslig verksamhet. Därigenom kan säkerhetsskyddslagen ges en vidare ram och ett större mått av flexibilitet.

12.2 Säkerhetsskyddsklassificerade uppgifter

Förslag: Säkerhetsskyddet ska delvis inriktas mot verksamhet som innebär hantering av *säkerhetsskyddsklassificerade uppgifter.* Det ska innefatta skydd av uppgifter som är av betydelse för Sveriges säkerhet eller som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande, och som till sin natur är sådana uppgifter som avses i bestämmelser om sekretess.

Uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen

I det föregående avsnittet har vi redogjort för behovet av att göra något åt den i dag inte ändamålsenliga insnävningen av tillämpningsområdet för säkerhetsskyddet som hänger samman med den nuvarande säkerhetsskyddslagstiftningens hänvisningar till bestämmelser om sekretess som rör rikets säkerhet. Sådana hänvisningar finns i bl.a. 6 § 2 säkerhetsskyddslagen.

Vad gäller hänvisningen till rikets (eller Sveriges) säkerhet har vi redan föreslagit att tillämpningsområdet för säkerhetsskyddslagen uttryckligen ska inkludera också känsliga uppgifter som härrör från annan stat eller mellanfolklig organisation och som Sverige förbundit sig att omge med ett säkerhetsskydd. Sådana uppgifter ska därför omfattas av samma krav på säkerhetsskydd som gäller för uppgifter som mer direkt rör svenska säkerhetsintressen.

Vad gäller hänvisningen till offentlighets- och sekretesslagen medför den en osäkerhet i fråga om krav på säkerhetsskydd när uppgifter som är av betydelse för Sveriges säkerhet (eller som ska skyddas enligt internationella säkerhetsskyddsåtaganden) förekommer i andra verksamheter än sådana där bestämmer om sekretess gäller. Som vi berört redan i våra allmänna utgångspunkter i kapitel 10 är det vår uppfattning att en sådan de facto insnävning mot det allmännas verksamhet knappast kan ha varit tanken. Den nämnda otydligheten i säkerhetsskyddslagen i kombination med att säkerhetskänsliga uppgifter i allt högre grad förekommer i enskild verksamhet medför en allvarlig risk för ett otillräckligt skydd för förhållanden som kan vara av stor betydelse för den nationella säkerheten. Risken för ett otillräckligt skydd finns inte minst i

verksamheter inom t.ex. elförsörjningen där det samtidigt finns starka motstående drivkrafter i fråga om effektivitet och kostnadsminimering. Mot den bakgrunden föreslår vi att det genom en ändrad formulering tydliggörs att referensen till bestämmelser om sekretess är relevant för att avgöra *det slag av uppgifter* det är fråga om men att den inte innebär något krav på att den verksamhet där sådana uppgifter hanteras också inkluderas i tillämpningsområdet för offentlighets- och sekretesslagen. Det bör således vara uppgifternas natur som är bestämmande för krav på säkerhetsskydd.

En i sammanhanget relevant fråga är behovet av ett förstärkt sekretesskydd också när uppgifter av det slag som det här är fråga om hanteras i verksamheter som inte omfattas av krav på sekretess enligt offentlighets- och sekretesslagen. Vårt uppdrag handlar primärt om säkerhetsskydd men frågan har ändå ett så nära samband med säkerhetsskyddet att vi anser att vi bör föreslå en till offentlighets- och sekretesslagen kompletterande bestämmelse om tystnadsplikt. Den frågan behandlas dock först i avsnitt 22.1

Särskilt relevant för vägledning i fråga om vilka uppgifter som till sin natur medför krav på säkerhetsskydd är den s.k. försvarssekretessen i 15 kap. 2 § OSL. Som vi redogjort för i avsnitt 4.2 bör vägledning om vilka förhållanden som är av betydelse för Sveriges säkerhet kunna hämtas också från andra sekretessbestämmelser som delvis överlappar försvarssekretessen. Känsliga uppgifter som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande omfattas i regel av bestämmelser om sekretess i förhållande till annan stat eller mellanfolklig organisation, den s.k. utrikessekretessen i 15 kap. 1 § OSL. Även andra bestämmelser om sekretess kan vara tillämpliga på denna typ av uppgifter, t.ex. försvarssekretessen eller bestämmelsen i 15 kap. 1 a § OSL om sekretess i det internationella samarbetet.

Säkerhetsskyddsklassificerade uppgifter – ett gemensamt begrepp

De uppgifter för vilka krav på säkerhetsskydd ska gälla bör, för att i övriga underlätta lagens systematik och dess tillämpning, sammanfattas i ett gemensamt begrepp. Närmast till hands är *säkerhetsskyddsklassificerade uppgifter* som används bl.a. som översättning av det engelska uttrycket *classified information* i den officiella över-

sättningen av avtalet mellan EU:s medlemstater om skydd av säkerhetsskyddsklassificerade uppgifter. Mot den bakgrunden kom också begreppet att användas i lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet.[4] Det är därför logiskt att samma uttryck används i en ny säkerhetsskyddslag.

Det finns ett nära samband mellan den nämnda upphandlingslagstiftningen och säkerhetsskyddslagen. Upphandlingslagstiftningen på försvars- och säkerhetsområdet förutsätter att det finns författningsstöd för att uppgifterna är skyddsvärda och att det finns förfaranden för att skydda uppgifterna. De ändringar som vi föreslår i fråga om omfattningen av uppgifter som ska skyddas enligt säkerhetsskyddslagen är därför av betydelse för upphandlingsregelverket. Vi återkommer till den frågan i avsnitt 19.4.

12.3 I övrigt säkerhetskänslig verksamhet

Förslag: Utöver skydd av säkerhetsskyddsklassificerade uppgifter ska säkerhetsskyddet inriktas mot verksamheter som av annan anledning behöver ett säkerhetsskydd (*i övrigt säkerhetskänslig verksamhet*). Det motsvarar delvis vad som i dag skyddas inom ramen för skydd mot terrorism, dvs. i huvudsak verksamhet vid skyddsobjekt, flygplatser och vissa verksamheter som ska skyddas enligt folkrättsliga åtaganden om luftfartsskydd, hamnskydd och sjöfartsskydd. Det skyddsvärda området bör dock inte avgränsas genom regleringen om skyddsobjekt utan ska även kunna innefatta annat slag av säkerhetskänslig verksamhet, t.ex. verksamheter som innefattar hantering av itsystem eller av sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle eller verksamhet som behöver skyddas på den grunden att den kan utnyttjas för att skada nationen, t.ex. vissa verksamheter inom det kärntekniska området.

[4] Se vidare avsnitt 19.4.

I det föregående avsnittet om säkerhetsskyddsklassificerade uppgifter har vi behandlat frågor som rör skyddet av sådana känsliga uppgifter som kan identifieras framför allt utifrån behov av att skydda deras konfidentialitet. Därutöver finns som vi redogjort för tidigare verksamhet som är säkerhetskänslig, även om den inte innebär hantering av säkerhetsskyddsklassificerade uppgifter. Som nämnts inledningsvis i detta kapitel har vi identifierat det som *verksamhet som i övrigt är säkerhetskänslig*.

Till skillnad från verksamhet som innebär hantering av säkerhetsskyddsklassificerade uppgifter finns för annat slag av säkerhetskänslig verksamhet inte någon given referensram för att avgöra vad som bör omfattas av krav på säkerhetsskydd. Särskilt i fråga om registerkontroll till skydd mot terrorism enligt 14 § säkerhetsskyddslagen har dock bestämmelser om skyddsobjekt i skyddslagen kommit att fylla en funktion som referensram. Som vi redogjort för tidigare är dock inte regleringen om skyddsobjekt utifrån dagens behov och verklighet i alla delar relevant och ändamålsenlig för att (i förening med säkerhetsskyddsklassificerade uppgifter) avgränsa de verksamheter som är i behov av säkerhetsskydd. Även om det för nationen skyddsvärda området till övervägande del i dag skulle kunna hänföras antingen till hantering av säkerhetsskyddsklassificerade uppgifter enligt vårt förslag i avsnitt 12.2 eller till verksamhet vid skyddsobjekt, finns det verksamheter av central betydelse för nationen som inte självklart kan inkluderas. Det kan t.ex. vara fråga om it-system som styr viktiga samhällsfunktioner eller som hanterar sammanställningar av uppgifter där uppgifternas tillgänglighet eller riktighet är av kritisk betydelse för ett fungerande samhälle. Folkbokföringen är ett exempel.

Vidare bör också vissa verksamheter som innefattar hantering med farliga ämnen som kan utnyttjas för att orsaka förödande skadeverkningar för nationen kunna omfattas. Transporter av kärnavfall och forskningsanläggningar inom kärnindustrin är exempel på sådana verksamheter. Annan sådan verksamhet är samhällets hantering av sprängämnen och ammunition som vid obehörig användning kan medföra stor skada på viktiga samhällsfunktioner. Även om annan lagstiftning, t.ex. strålskyddslagstiftningen, ställer krav på de fysiska skyddsåtgärder som behövs kan säkerhetsskyddslagen behöva kunna tillämpas i fråga om kontroll av anställda och andra som deltar i sådan verksamhet. Vidare före-

kommer det i internationella konventioner och andra folkrättsliga åtaganden som Sverige är bundet av, bl.a. inom EU-rätten, krav på att personal inom t.ex. verksamhet av betydelse för luftfartsskyddet ska genomgå säkerhetsprövning med registerkontroll. Redan i dag finns i säkerhetsskyddsförordningen flera bestämmelser om registerkontroll som kan härledas till folkrättsliga åtaganden i fråga om luftfarts-, sjöfarts- och hamnskydd. Att hänvisa till verksamhet vid skyddsobjekt riskerar således att medföra en för snäv avgränsning. För att lagstiftningen också ska kunna stå sig över tid behöver, bl.a. med hänsyn till folkrättsliga förpliktelser, ett visst bedömningsutrymme finnas i fråga om vad som är att anse som i övrigt säkerhetskänslig verksamhet. Innebörden av det föreslagna centrala begreppet säkerhetskänslig verksamhet med dess referens till Sveriges säkerhet och internationella säkerhetsskyddsåtaganden ger en yttre ram för vilka verksamheter som kan komma i fråga.[5] Någon annan ram bör inte anges. Den slutsatsen leder in på de frågor som vi tar upp i nästa kapitel, nämligen i vilka samhällssektorer säkerhetskänslig verksamhet typiskt sett kan förekomma och säkerhetsskyddsanalysens centrala funktion för att identifiera sådan verksamhet.

[5] Med en sådan avgränsning är det tydligt att kraven på säkerhetsskydd inte omfattar t.ex. gator, torg och idrottsarenor som varken är rimligt eller möjligt att skydda genom säkerhetsskyddsåtgärder.

13 Vad ska skyddas – säkerhetsskyddsanalys

För att i det enskilda fallet bedöma om en tillgång eller en funktion ska betraktas som så skyddsvärd att den ska falla inom ramen för säkerhetsskyddslagen måste den värderas. Utgångspunkten för en sådan värdering bör vara konsekvensdriven. Det är således den möjliga konsekvensen av att tillgången eller funktionen påverkas negativt som ger dess skyddsvärde. Behovet av skydd beror därmed på den konsekvens som ett angrepp kan generera.

Svaret på frågan vilka tillgångar och funktioner i verksamheter som behöver säkerhetsskydd varierar över tid och kommer alltså att behöva omprövas kontinuerligt. Den måste bl.a. därför besvaras på verksamhetsnivå. Det är den ansvarige för en verksamhet som ska bedöma om verksamheten är säkerhetskänslig och, om så är fallet, har att se till att det upprättas en säkerhetsskyddsanalys, att lämpliga säkerhetsskyddsåtgärder vidtas och att säkerhetsskyddet upprätthålls. Dessa åtgärder ingår i säkerhetsplaneringen.

I detta kapitel behandlar vi inledningsvis (i avsnitt 13.1), utan att göra anspråk på att uppräkningen är uttömmande, inom vilka områden som de mest skyddsvärda tillgångarna och funktionerna förekommer. Syftet med redovisningen är att beskriva och i någon mån ringa in vilka verksamheter som lagen är avsedd att träffa. Därefter (i avsnitt 13.2) beskrivs säkerhetsskyddsanalysen som metod för att i en säkerhetskänslig verksamhet identifiera risker och sårbarheter, så att brister i säkerhetsskyddet kan åtgärdas.

Det kan uppstå ett behov av att uppfattningen om vad som är skyddsvärt jämkas mellan liknande verksamheter och samhällssektorer, så att lagstiftningen tillämpas på ett likartat sätt. Här har Säkerhetspolisen och Försvarsmakten en viktig roll att tillsammans

med säkerhetsskyddsstödjande myndigheter[1] och de som tillsynen avser diskutera säkerhetsskyddsanalysernas innehåll för att nå en så enhetlig tillämpning som möjligt.

Det förekommer i annan reglering krav på olika slag av analyser. Exempel på sådana analyser redovisas i avsnitt 13.3. Arbetet med säkerhetsskyddsanalysen kan i många fall samordnas med och dra nytta av dessa andra slag av risk- och sårbarhetsanalyser (avsnitt 13.4). Avslutningsvis (i avsnitt 13.5) behandlar vi frågan om sekretess vad avser säkerhetsskyddsanalyser.

13.1 Inom vilka samhällssektorer finns särskilda skyddsvärda funktioner?

För att kunna identifiera särskilt skyddsvärda funktioner som bör kunna omfattas av säkerhetsskydd har behovsbeskrivningar hämtats in från de myndigheter som är representerade i utredningen och från vissa övriga intressenter. Vi har vidare tagit del av förslag lämnade av andra utredningar och olika myndighetsrapporter som berör frågor som är relevanta för att bedöma vad som bör skyddas inom ramen för en ny säkerhetsskyddslag.

I detta sammanhang kan nämnas den handlingsplan för skydd av samhällsviktig verksamhet som Myndigheten för samhällsskydd och beredskap har tagit fram. Handlingsplanen baseras på den nationella strategi för skydd av samhällsviktig verksamhet som myndigheten redovisade i mars 2011. Inom ramen för arbetet med handlingsplanen har myndigheten tagit fram en vägledning för identifiering av samhällsviktig verksamhet och konsekvensbedömning.[2] Vägledningen utgår bl.a. från elva samhällssektorer inom vilka merparten av den samhällsviktiga verksamheten kan identifie-

[1] I direktiven används benämningen sektorsansvariga myndigheter som en samlande benämning för Affärsverket svenska kraftnät, Post- och telestyrelsen, Transportstyrelsen och länsstyrelserna. Som framgår av avsnitt 10.1.5 har vi i stället valt att använda säkerhetsskyddsstödjande myndigheter som en samlande benämning för dessa myndigheter såvitt avser deras funktioner för säkerhetsskyddet. Vi föreslår vidare i avsnitt 18.10 och 21.2.4 att Myndigheten för samhällsskydd och beredskap ska ta över de uppgifter länsstyrelserna i detta avseende har samt även vara säkerhetsskyddsstödjande myndighet för kommuner och landsting.

[2] Myndigheten för samhällsskydd och beredskaps publikation Att identifiera samhällsviktig verksamhet – En metod för identifiering av samhällsviktig verksamhet och bedömning av tolerabel avbrottstid, publ.nr. MSB620, januari 2014.

ras. Dessa elva samhällssektorer kan vara relevanta också för att identifiera sådana skyddsvärda funktioner som kräver skydd med stöd av säkerhetsskyddslagen.

Myndighetens uppdrag utgår dock från ett för hela samhället, på dess olika nivåer, samlat funktionalitetsperspektiv och inte från de särskilt skyddsvärda funktioner som säkerhetsskyddslagen avser att skydda. De samhällssektorer och de exempel på samhällsviktiga funktioner som anges i vägledningen träffar därmed betydligt bredare och djupare än vad säkerhetsskyddslagen ska skydda. De områden som presenteras nedan bygger därför på myndighetens indelning men är inte identisk med denna.

Här ges exempel på områden, verksamheter och funktioner som är av sådan karaktär att de skulle kunna omfattas av krav på skydd enligt säkerhetsskyddslagen. Gemensamt för flera av områdena är att det inom dessa finns skyddsvärda it-system för bl.a. ledning, styrning, reglering och övervakning av samhällsviktiga funktioner. Dessa it-system karaktäriseras ofta, men inte alltid, av att det är systemens tillgänglighet och informationens riktighet som står i fokus snarare än konfidentialiteten. Vidare är flera av sektorerna ömsesidigt beroende. El- och vattenförsörjning är t.ex. beroende av fungerande elektronisk kommunikation och livsmedelsförsörjningen av fungerande transporter. Bedömningen att det finns skyddsvärda intressen inom en viss samhällssektor innebär naturligtvis inte heller att all verksamhet eller alla tillgångar inom respektive sektor som berörs ska betraktas som tillräckligt skyddsvärda för att träffas av säkerhetsskyddslagen. Det är i verksamheten som tillgångarna måste bedömas. Här har den som utför tillsyn över säkerhetsskyddet i en verksamhet ett ansvar att se till att denna bedömning är balanserad. De angivna exemplen kan dock tjäna som en vägledning för att identifiera skyddsvärda tillgångar inom respektive verksamhetsområde.

Centrala statsledningen

Inom den centrala statsledningen finns flera skyddsvärda funktioner som t.ex. regeringens möjligheter att sköta sina uppgifter. Motsvarande gäller för lednings- och stödfunktioner till den centrala statsförvaltningen. I Regeringskansliet finns på grund av

verksamhetens karaktär information som kan orsaka mycket stor skada om den röjs för obehöriga, förstörs, görs otillgänglig eller obehörigen ändras.

Totalförsvaret

Det svenska försvaret delas in i militärt försvar och civilt försvar som tillsammans utgör totalförsvaret. Med totalförsvar avses all verksamhet som behövs för att förbereda Sverige för krig.[3]

Det militära försvaret innefattar skyddsvärda funktioner som ytterst syftar till att öka Sveriges förmåga att stå emot ett militärt angrepp eller att minska eller förhindra en angripares möjligheter till framgång i ett sådant angrepp på Sverige, och oberoende av mot vilket nationellt svenskt intresse ett sådant angrepp eller hot riktas.

Genom att Försvarsmakten i högre grad än tidigare samarbetar med andra länder inom bl.a. försvarsmaterielområdet, i militär utbildning, i övningar och vid insatser finns behov av att också skydda vissa uppgifter som rör sådan internationell samverkan. Även svensk försvarsindustri är av stor betydelse för svenska försvarets förmåga att utföra sina uppgifter, t.ex. forskning och utveckling samt produktion av militära fordon, fartyg och luftfartyg.

Det civila försvaret ska enligt Försvarsberedningen[4] stödja och samverka med det militära försvaret för att kunna motstå ett väpnat angrepp, hantera samhällskonsekvenser och upprätthålla samhällsviktig verksamhet samt kunna bidra till att återuppbygga och återställa samhällets funktionalitet efter ett sådant angrepp. Planeringen för det civila försvaret ska göras i samverkan med bl.a. de statliga myndigheter, kommuner, landsting, sammanslutningar och näringsidkare som är berörda. Säkrandet av samhällsviktig infrastruktur och behovet av att säkerställa tillräcklig försörjning med strategiska förnödenheter är en viktig del i samhällets samlade beredskap.

[3] 1 § lagen (1992:1403) om totalförsvar och höjd beredskap.
[4] Försvarsberedningens rapport Försvaret av Sverige – Starkare försvar för en osäker tid (Ds 2014:20).

Internationella relationer

För Sveriges utveckling och för vårt oberoende och bestånd finns ett behov av att kunna upprätthålla goda utrikespolitiska förbindelser. Som en del av förutsättningarna för sådana förbindelser ingår förmågan att erbjuda skydd och säkerhet för andra staters och internationella organisationers verksamhet i Sverige. Det kan röra sig om verksamhet kopplad till diplomatiska beskickningar och konsulat samt missioner i Sverige, besök av utländska statsfartyg och statsluftfartyg samt internationella övningar. Vad som är skyddsvärt från ett säkerhetsskyddsperspektiv är i huvudsak förmågan att erbjuda skydd och säkerhet som behövs för att upprätthålla de internationella relationerna. Utrikes- och säkerhetspolitisk verksamhet som rör Sveriges internationella relationer inom t.ex. gemensamt freds- och säkerhetsarbete, rymdfrågor, sanktioner, försvarsexportfrågor och icke-spridningsfrågor har ofta ett högt skyddsvärde.

Rättsväsendet

Funktioner för att upprätthålla lag och ordning och ett fungerande rättsväsende är viktiga ur både ett rättssäkerhetsperspektiv och ett demokratiskt perspektiv. Inom detta område finns olika system och funktioner för att stödja rättsväsendet som kan vara nationella skyddsvärda intressen. Antagonistiska hot mot och otillbörlig påverkan av rättsväsendets funktioner kan, förutom att leda till en felaktig utgång i domar och beslut, på sikt även leda till en minskad tilltro till rättsväsendet som funktion. Som exempel på särskilt skyddsvärd verksamhet kan nämnas Säkerhetspolisens verksamhet att utreda brott mot Sveriges säkerhet.

Skydd mot olyckor

Samhällets förmåga att hantera allvarliga olyckor och angrepp och att begränsa konsekvenserna av dessa omfattar flera skyddsvärda intressen. Det gäller bl.a. samhällets alarmeringstjänst samt räddningstjänstens lednings- och stödfunktioner, som radiokommuni-

kationssystemet Rakel. I vissa fall kan räddningstjänstens insatsplanering ha ett särskilt skyddsvärde.

Hälso- och sjukvård

Antagonistiska aktörers avsikter kan riktas mot t.ex. akutsjukvård, läkemedels- och materielförsörjning samt smittskydd. För att utgöra särskilt skyddsvärda funktioner måste det dock vara fråga om kritisk verksamhet, t.ex. centrala läkemedelslager eller laboratorier som hanterar smittoämnen som vid ett antagonistiskt angrepp kan innebära allvarlig fara för människors liv och hälsa.

Energiförsörjning

Energiförsörjningen intar en särställning bland de områden som redovisas här, eftersom flertalet verksamheter för sin funktion är kritiskt beroende av en fungerande energiförsörjning. I denna sektor bör som särskilt skyddsvärt framhållas system och funktioner som är kritiska för produktion, transmission och distribution av energi i olika former samt elhandel. Annat som kan bedömas vara särskilt skyddsvärt är t.ex. särskilt viktiga delar och anläggningar i elsystemet, driftsfunktioner och datastödssystem, information om anläggningars sårbarheter och kapacitet, funktion och roll i elsystemet, exakta lägesangivningar och vilka skyddsåtgärder som vidtagits.

Det moderna samhället är i allra högsta grad beroende av elektricitet, och ett elavbrott drabbar i stort sett alla verksamheter. Elförsörjningen är i sin tur i hög utsträckning beroende av itsystem och elektroniska kommunikationer för drift, övervakning och styrning.

Kärnkraftsproduktion är en typ av högriskindustri vars skyddsvärde särskilt bör nämnas då den kan vara i hög grad skadegenererande. Den kan i vissa lägen ha stor betydelse i energisystemet. Sådan betydelse kan också vissa dammanläggningar ha i de fall dammen utgör en del av en vattenkraftproduktionsanläggning av nationell betydelse (t.ex. en anläggning som är viktig för dödnäts-

start av det svenska kraftnätet) och då dammen vid ett haveri skulle kunna orsaka allvarlig skada av nationell betydelse.[5]

Vattenförsörjning och avloppshantering

I denna sektor inkluderas vattentäkter, produktionsanläggningar och distributionssystem som behövs för att förse Sverige med dricksvatten samt avloppssystem och avloppshantering.

Dricksvatten är samhällets viktigaste livsmedel. Produktion och distribution av dricksvatten är i hög grad beroende av en vidmakthållen funktionalitet hos industriella informations- och styrsystem vilka styr, kontrollerar och övervakar den fysiska processen. När dricksvattenförsörjningen inte fungerar kan konsekvenserna för samhället bli allvarliga. För att skyddet för dricksvattenförsörjningen eller avloppshanteringen ska bli en säkerhetsskyddsangelägenhet krävs dock att det rör sig om sådana för försörjningen och hanteringen centrala funktioner eller system som vid ett antagonistiskt angrepp skulle få allvarliga nationella konsekvenser.

Annan livsmedelsförsörjning

Livsmedelsförsörjningen omfattar produktion, kontroll, lagerhållning och distribution av livsmedel. I princip samtliga delar av denna sektor har ett stort beroende av strömförsörjning, bl.a. för kyl- och frysmöjligheter, men också av vattenförsörjning och fungerande kommunikationssystem. Särskilt skyddsvärt kan vara t.ex. beredskapsplaner hos de stora matvarudistributörerna.

Elektronisk kommunikation

Vid sidan av elförsörjningen är elektronisk kommunikation avgörande för att kunna upprätthålla skyddsvärda verksamheter och funktioner i samhället. Sektorn innefattar fast och mobil telefoni samt internet, it-kommunikation och radio.

[5] Jämför Mikael Niemi, Fallvatten, Piratförlaget 2012.

Såvitt gäller elektronisk kommunikation kan t.ex. driftledningscentraler och centrala kopplingspunkter med utrustning för trafikutbyte och signalering, större transmissionsnät samt samverkanspunkter för signalspaning vara skyddsvärda funktioner. Även system som hanterar verkställighet av hemlig avlyssning och övervakning av elektronisk kommunikation kan vara skyddsvärda.

Finansiella tjänster

Som exempel kan nämnas funktioner i det centrala finans- och betalningssystemet som är ägnade att upprätthålla fungerande kapitalmarknader, tillförsäkra befolkningen tillgång till nödvändiga betalningsmedel och säkerställa att finansiella transaktioner inte stannar upp eller kommer på avvägar. Dessa funktioner – som vid ett bortfall, direkt eller över tid, skulle innebära en risk eller fara för samhällets funktionalitet eller samhällets grundläggande värden – kan utgöra skyddsvärda intressen.

Ett exempel på ömsesidigt beroende är finanssektorns beroende av elkraft. Det hjälper ju inte att bankernas eller finansinstitutens centrala system står i datorhallar med reservkraft, om betalstationer och uttagsautomater ändå inte kan fungera vid ett elavbrott.

Industri, forskning och utveckling

Produktion som kan hänföras till kritisk infrastruktur och försvarsindustri liksom forskning och utveckling som från ett nationellt perspektiv är viktig för Sverige kan vara särskilt skyddsvärd verksamhet i säkerhetsskyddslagens mening.

Till denna sektor kan hänföras även industriverksamhet som hanterar explosiva ämnen och giftiga material i stor omfattning samt forskningsverksamhet inom t.ex. bakteriologiska områden. Dessa verksamheter kan orsaka förödande följdverkningar för nationen, om de utnyttjas för antagonistisk verksamhet.

Transporter och kommunikation

Denna sektor avser transporter på land, till sjöss eller i luften som kan anses skyddsvärda. Till dessa räknas både själva färdmedlen, viktiga styrsystem och den infrastruktur som behövs för att transporterna ska fungera, t.ex. system för styrning av kritiska järnvägsväxlar och dirigering av trafik i luftrummet. I sammanhanget bör beaktas att transporter är direkt eller indirekt beroende av el, både för själva transporten, för stödfunktioner och för transport av bränsle. Sjö- och luftfart omfattas av internationella konventioner som innefattar krav på säkerhetsskyddsåtgärder.

Folkbokföring och socialförsäkring

I denna sektor ingår t.ex. skatte- och folkbokföringen, socialförsäkringssystemet och länsstyrelsernas och kommunernas förvaltningar. Centrala system kopplade till myndighetsutövning liksom stora system med uppgifter som andra system är beroende av kan ha särskilt skyddsvärt innehåll.

Funktionen hos centrala bas- och informationssystem som stödjer myndigheternas verksamhet, t.ex. det allmänna pensionssystemet samt sjuk- och arbetslöshetsförsäkringen kan vara skyddsvärda. Begränsningar i att få korrekta basuppgifter från systemen eller en längre tid med icke fungerande informationssystem kan allvarligt skada olika former av funktioner.

Övrigt

Ett annat verksamhetsområde är vissa internationella konferenser, politiska högnivåmöten och liknande evenemang (jämför nuvarande reglering i 26 a § säkerhetsskyddsförordningen). Det kan således finnas vissa s.k. symbolvärden i sådan verksamhet som kan medföra att verksamheten kan förutsättas vara ett potentiellt mål för aktörsdrivna hot, t.ex. terrorism. Även andra nationella symbolvärden som rör t.ex. statschefen, regering och riksdag kan behöva skyddas. I första hand hanteras behovet av skydd i dessa fall genom Säkerhetspolisens personskyddsverksamhet. Det kan dock inte uteslutas att säkerhetsskyddet kan behöva säkerställas även

genom t.ex. säkerhetsprövningsåtgärder som vidtas med stöd av säkerhetsskyddslagstiftningen.

Sammanfattande slutsats

Vi har tidigare betonat att säkerhetsskyddslagens krav på säkerhetsskydd omfattar endast den övre delen av en tänkt pyramid innefattande alla de verksamheter som är viktiga i ett fungerande samhälle. De nu redovisade samhällssektorerna kan rymma en mängd skyddsvärda verksamheter eller funktioner som dock inte är tillräckligt skyddsvärda för att omfattas av säkerhetsskyddsregleringen. Även verksamheter eller funktioner som inte bedöms kräva skydd med stöd av säkerhetsskyddslagen kan vara skyddsvärda eller omfattas av krav på skydd. Det finns en mängd olika regleringar som tar sikte på skydd från ett allmänt säkerhetsperspektiv. Vi har tidigare konstaterat att när skyddsvärda intressen har identifierats ska dessa värderas utifrån en konsekvensnivå som innebär en allvarlig nationell påverkan. Vid denna bedömning måste också hänsyn tas till att vad som är att betrakta som skyddsvärt varierar över tid. Frågan vilka funktioner, system eller anläggningar som behöver säkerhetsskydd kommer att behöva omprövas kontinuerligt och måste därför besvaras på verksamhetsnivå. Säkerhetsskyddsanalysens syfte är att ge ett stöd för detta.

13.2 Säkerhetsskyddsanalys

Bedömning och förslag: Säkerhetsskyddsanalysens centrala funktion för säkerhetsskyddet behöver lyftas fram. En bestämmelse om att den som är ansvarig för säkerhetskänslig verksamhet ska se till att behovet av säkerhetsskydd för den egna verksamheten utreds i form av en säkerhetsskyddsanalys bör därför tas in i säkerhetsskyddslagen.

I förordning bör det finnas en bestämmelse om att genom en sådan analys ska säkerhetsskyddsklassificerade uppgifter och vad som i övrigt behöver ett säkerhetsskydd identifieras samt säkerhetshot och potentiella konsekvenser, sårbarheter och behovet av säkerhetsskyddsåtgärder bedömas. Säkerhetsskydds-

analysen ska ligga till grund för planeringen av verksamhetens säkerhetsskydd. Analysen ska dokumenteras och hållas uppdaterad.

Brister och problem

I den nuvarande säkerhetsskyddsförordningen (5 §) finns en bestämmelse om krav på säkerhetsanalys. Enligt bestämmelsen ska myndigheter och andra som säkerhetsskyddsförordningen gäller för undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av undersökningen (säkerhetsanalys) ska dokumenteras.

Flera av de myndigheter som är representerade i utredningen har påtalat vikten av att de som omfattas av säkerhetsskyddsregleringen verkligen gör en säkerhetsanalys och att den görs på ett korrekt och relevant sätt. Säkerhetspolisen har påpekat att man inom ramen för sin tillsynsverksamhet inte sällan konstaterar att det föreligger brister i säkerhetsskyddet och att dessa brister beror på myndighetens ofullständiga säkerhetsanalys. Det kan t.ex. vara fråga om att myndigheten under lång tid underlåtit att genomföra en säkerhetsanalys. Enligt Säkerhetspolisen förekommer vidare att det saknas fastställda processer för hur säkerhetsanalyser ska genomföras och kriterier för när de ska göras.[6] I detta sammanhang kan nämnas resultatet av en av Affärsverket svenska kraftnät genomförd enkätstudie.[7] Mer än 80 procent av de tillfrågade elbolagen som omfattas av säkerhetsskyddslagen uppgav att man inte hade någon aktuell säkerhetsanalys. Mer än 65 procent av bolagen uppgav att de aldrig gjort någon säkerhetsanalys. Cirka 15 procent av de tillfrågade bolagen angav att säkerhetsanalysen var äldre än två år.

[6] Se också Riksrevisionens granskningsrapport, RIR 2014:23 Informationssäkerheten i den civila statsförvaltningen, dnr: 31-2013-1288, överlämnad till riksdagen 2014-11-10. Detta behandlas även i avsnitt 21.1.
[7] Förstudierapport Svenska Kraftnät 2011 – Branschens behov av stöd inom informationssäkerhetsområdet, dnr 2011/1199.

Anledningarna till att man i sin verksamhet inte genomför en säkerhetsanalys är sannolikt flera. En kan vara att man på grund av problem med att definiera och avgränsa det för säkerhetsskyddsregleringen centrala begreppet *rikets säkerhet* bedömer att verksamheten inte omfattas av lagstiftningen.

Ett problem som påtalats särskilt är säkerhetsskyddslagstiftningens starka kopplingar till offentlighets- och sekretesslagen (2009:400), OSL. Dessa kopplingar innebär dels att säkerhetsanalyser över huvud taget inte genomförs i vissa verksamheter, dels att bl.a. it-system som i sig inte innehåller sekretessbelagda uppgifter som rör rikets säkerhet inte omfattas av säkerhetsanalysen. I säkerhetsskyddsförordningens bestämmelse om säkerhetsanalys omnämns endast uppgifter och anläggningar. Även om man implicit kan låta mycket innefattas i begreppet uppgifter, har det framhållits att det är en brist att det inte framgår att säkerhetsanalys bör göras även för it-system, tjänster och andra elektroniska system som kan påverka säkerhetsskyddet.

Överväganden och bedömningar

I nuvarande reglering finns bestämmelsen om säkerhetsanalys i säkerhetsskyddsförordningen. Med hänsyn till att ett åliggande för kommuner och landsting liksom för enskilda kräver stöd i lag bör en bestämmelse om ett utredningskrav tas in i säkerhetsskyddslagen.

Det finns krav i andra regleringar för myndigheter m.fl. att ta fram olika former av risk- och sårbarhetsanalyser ur diverse perspektiv, t.ex. krishanterings-, arbetsmiljö- och finansiella perspektiv (se vidare avsnitt 13.3). Det som är speciellt med säkerhetsskyddsregleringens säkerhetsanalys är att den fokuserar på skydd för de för nationen mest skyddsvärda verksamheterna mot antagonistiska hot och angrepp.

För att skilja säkerhetsskyddsregleringens säkerhetsanalys från andra former av risk- och sårbarhetsanalyser anser vi att termen *säkerhetsskyddsanalys* bör användas. Termen tydliggör att det är säkerhetsskyddet i verksamheten som ska vara föremål för analysen. Syftet med säkerhetsskyddsanalysen är dels att i en verksamhet identifiera de allra känsligaste delverksamheterna, dels att upp-

rätta en handling som dokumenterar de resonemang som leder fram till bedömningen av vad som är skyddsvärt och hur skyddet av detta ska prioriteras.

Det är bedömningarna i säkerhetsskyddsanalysen som ska motivera de säkerhetsskyddsåtgärder som vidtas och säkerställa att de hänger ihop i ett fungerande säkerhetsskyddssystem. Syftet med säkerhetsskyddsanalysen är vidare att tydliggöra vilka typer av hot och sårbarheter de föreslagna säkerhetsskyddsåtgärderna ska skydda mot och vilka negativa konsekvenser ett angrepp kan medföra. I säkerhetsskyddssammanhang är bedömningen av sårbarheten väl så viktig som hotbedömningen. Att bygga upp ett effektivt säkerhetsskydd är en process och ett arbete som pågår under relativt lång tid. Ett hot kan förändras snabbt och det är därför viktigare att fokusera på sårbarheter snarare än hot eftersom sårbarheter i säkerhetsskyddet ökar möjligheten att ett angrepp ska lyckas.

Säkerhetsskyddsanalysen är kärnan i ett väl anpassat säkerhetsskydd. Eftersom säkerhetsskyddsåtgärder potentiellt sett kan vara kostsamma och riskerar att negativt påverka en verksamhets funktionalitet, effektivitet och tillgänglighet är det viktigt att säkerhetsskyddet inte görs mer omfattande än nödvändigt. Hänsyn till den personliga integriteten stryker under detta. En väl genomförd säkerhetsskyddsanalys med bedömning och dokumentation av vad som är skyddsvärt i verksamheten och vilka skyddsåtgärder som är nödvändiga ökar förutsättningarna för att säkerhetsskyddet blir väl avvägt och effektivt.

Säkerhetsskyddsanalysen tydliggör också behovet av sådana säkerhetsskyddsåtgärder som kräver investeringar. Med hänsyn till säkerhetsskyddsanalysens centrala betydelse för säkerhetsskyddet bör ledningen för verksamheten skapa goda förutsättningar för säkerhetsskyddsanalysarbetet.

I detta sammanhang bör påpekas att själva säkerhetsskyddsanalysen i stora delar med hänsyn till sitt innehåll är mycket skyddsvärd. Den kan därför i sig behöva omfattas av ett säkerhetsskydd. Som exempel på mycket skyddsvärt innehåll i säkerhetsskyddsanalysen kan nämnas identifierade sårbarheter. Uppgifter om sårbarheter bör inte spridas till en större krets än nödvändigt. Däremot kan uppgifter om bedömda säkerhetshot (dvs. vilka aktörer som utövar hot, deras kapacitet, intention och möjlighet att

realisera hot) vara nödvändiga för alla anställda att ta del av. Säkerhetsskyddsanalysen är således grunden för planeringen av säkerhetsskyddet i verksamheten. Därför är det viktigt att alla anställda i en skyddsvärd verksamhet, oavsett om de tar del av skyddsvärd information eller inte, förstår behovet av säkerhetsskydd.

13.3 Närmare om innehållet i säkerhetsskyddsanalysen

Allmänt om säkerhetsskyddsanalysen

Omfattningen av den verksamhet som är i behov av säkerhetsskydd skiljer sig mycket åt mellan de myndigheter och övriga som har att tillämpa säkerhetsskyddsregleringen. För vissa kan merparten av verksamheten kräva säkerhetsskydd medan det för andra rör sig om endast en ytterst liten del av verksamheten. Till exempel kan det i vissa fall röra sig om några enstaka handlingar som behöver skyddas. Oberoende av detta anser vi att det finns vissa steg som alltid bör finnas med i säkerhetsskyddsanalysen. Att identifiera och prioritera skyddsvärda tillgångar, bedöma säkerhetshot, sårbarhet och risk samt att utifrån detta prioritera och hantera risker genom bl.a. säkerhetsskyddsåtgärder är sådana steg.[8] Om verksamheten är okomplicerad och av mindre omfattning, kan tillämpningen av de olika stegen förenklas.

Ett viktigt ingångsvärde i en säkerhetsskyddsanalys är en bedömning och dokumentation av vad som är skyddsvärt i verksamheten. Detta kan göras i form av en separat verksamhetsanalys eller som en inledande del av säkerhetsskyddsanalysen. Resultatet av säkerhetsskyddsanalysen är underlag för att prioritera, införa, planera och utvärdera säkerhetsskyddsåtgärder. Dessa åtgärder sammanställs lämpligen i en säkerhetsskyddsplan som kan ange tidsförhållanden, ansvar och kostnader för de olika åtgärderna.

[8] Säkerhetspolisens handbok Säkerhetsskydd – en vägledning, 2010, s. 12–14. Försvarsmakten, Handbok Säkerhetstjänst Grunder, 2013, s. 35 ff.

I det följande beskrivs moment som bör ingå i en god säkerhetsskyddsanalys.

Verksamhetsbeskrivning

Verksamhetsbeskrivningen klargör verksamhetens övergripande uppdrag. Syftet med verksamhetsbeskrivningen är att definiera, tydliggöra och avgränsa vilken verksamhet som analysarbetet avser. Verksamhetsbeskrivningen är ett viktigt ingångsvärde för säkerhetsskyddsanalysen och bidrar till att underlätta identifieringen och prioriteringen av de skyddsvärda tillgångarna i verksamheten. Verksamhetsbeskrivningen kan även utgöra ett separat dokument.

Identifiera det skyddsvärda

Identifieringen av det skyddsvärda är det viktigaste resultatet av säkerhetsskyddsanalysen. Verksamheten måste analyseras mer i detalj för att identifiera skyddsvärd verksamhet, skyddsvärda uppgifter och system samt vilka anställningar som ska placeras i säkerhetsklass. Spårbarheten, dvs. bakgrunden och argumentationen som leder till att något identifieras som skyddsvärt, bör dokumenteras så att man lätt kan gå tillbaka i analysen för att härleda vilka faktorer som legat till grund för olika bedömningar, förslag och beslut. Det kan även vara viktigt att dokumentera resonemang till stöd för vad som inte bedömts vara skyddsvärt.

Konsekvensanalys

Syftet med konsekvensanalysen är att bedöma skyddsvärdet av olika delar av verksamheten. För att kunna analysera vilka konsekvenser som kan uppstå krävs att oönskade händelser och potentiella orsakskedjor som kan påverka det skyddsvärda negativt identifieras.

Syftet med säkerhetsskyddslagen är framför allt att säkerställa ett skydd för verksamheter där påverkan genom ett antagonistiskt angrepp skulle medföra allvarliga konsekvenser för nationen. Vid

värderingen av de negativa konsekvenser som kan uppstå bör frågeställningar om påverkan på ett större antal människors liv eller hälsa besvaras. Det är också viktigt att bedöma hur stort geografiskt område som påverkas samt längden på och tidpunkten för påverkan. Vad som vidare har betydelse är bl.a. om händelsen får allvarliga sociala, ekonomiska eller politiska konsekvenser för samhället och om andra samhällsviktiga verksamheter som t.ex. elförsörjning eller elektronisk kommunikation påverkas allvarligt.

Säkerhetshotbedömning

Syftet med säkerhetshotbedömningen är att klarlägga vilka slag av hot som kan riktas mot verksamheten. Hotbedömningen avser antagonistiska hot, dvs. hot bakom vilket det står en aktör i form av en enskild, grupp, nätverk, organisation, stat etc. med förmåga och avsikt. Den bedömda hotnivån innebär en samlad bedömning av en eller flera aktörers kapacitet, intention och tillfälle att i tid och rum direkt eller indirekt angripa eller på annat sätt medvetet påverka en eller flera identifierade skyddsvärda intressen. För att göra en sådan bedömning kan den enskilde verksamhetsutövaren behöva bistånd med underlag från t.ex. Säkerhetspolisen eller Försvarsmakten. I detta sammanhang kan vissa av underrättelsemyndigheternas årsrapporter och webbplatser tjäna som vägledning.

Den aktuella hotbilden bör inte ges någon avgörande betydelse för hur säkerhetsskyddet utformas. Att följa hotets utveckling och att hålla sig informerad om aktuella hot är dock av betydelse för att kunna värdera om vidtagna åtgärder är tillräckliga. En dimensionerande hotbeskrivning, dvs. en allmän beskrivning av en tänkt hotaktörs förmåga och tillvägagångssätt, bör ligga till grund för dimensioneringen av säkerhetsskyddet.

När man ska värdera hot är det viktigt att tona ner sannolikhetsfrågan eftersom det är i det närmaste omöjligt att med tillförlitlighet göra en sannolikhetsbedömning, dvs. bedöma risken för att ett hot ska realiseras. Hotbeskrivningen bör därför, liksom när det gäller värderingen av skyddsvärda intressen, vara konsekvensdriven.

Det kan dock vara lämpligt att göra relativa bedömningar genom att rangordna möjliga hot mot en viss verksamhet efter hur troliga de bedöms vara i förhållande till varandra.

Sårbarhetsanalys

Analysen syftar till att identifiera de brister och svagheter i skyddet av sådant som bedömts vara det mest skyddsvärda som kan utnyttjas av en tänkt hotaktör och som kan medföra allvarliga konsekvenser. Sårbarhetsanalysen innefattar t.ex. identifiering och besiktning av befintliga skyddsåtgärder och bedömning av hur effektiva existerande skyddsåtgärder är samt identifiering av potentiella sårbarheter. I analysarbetet kan ingå t.ex. mätningar av säkerheten, analys av inträffade incidenter och praktiska tester av skyddet. Det är viktigt att i arbetet med sårbarhetsanalys relatera till den dimensionerande hotbeskrivningen. Ett tecken på sårbarhet är om säkerhetsskyddet inte klarar att hantera det dimensionerande hotet. Sårbarheter i en verksamhet kan uppstå t.ex. dels på grund av organisationens utformning och den teknik som används, dels på grund av brister i det fysiska skyddet och på informationssäkerhetsområdet. Även de personer som arbetar eller på annat sätt deltar i verksamheten kan utgöra potentiella sårbarheter.

Identifiering och värdering av säkerhetsskyddsåtgärder

När det gäller att värdera vilka åtgärder som är mest lämpliga bör beaktas graden av konsekvens, det troligaste tillvägagångssättet för en hotaktör och vilket skydd som redan finns på plats. Vidare måste skyddsåtgärdernas möjligheter att åstadkomma ett verksamt skydd, skyddsåtgärdernas begränsning av verksamhetens huvudsyfte liksom kostnaden för olika åtgärder beaktas. Även skyddet för den personliga integriteten måste beaktas. En väl genomförd säkerhetsskyddsanalys, där behovet av säkerhetsklassade anställningar och säkerhetsprövningar noga har analyserats, kan sannolikt minska risken för bl.a. obefogade registerkontroller och onödiga kostnader. En förutsättning för en registerkontroll är därför en genomförd säkerhetsskyddsanalys.

Sammanfattande reflektioner

Vi anser att det viktigaste resultatet av säkerhetsskyddsanalysen, förutom att utgöra underlag för prioritering, planering, införande och utvärdering av säkerhetsskyddsåtgärder, är bedömningen och dokumentationen av vad som är skyddsvärt i verksamheten. I säkerhetsskyddsanalysen bör också ingå en beskrivning av de hot som säkerhetsskyddet ska vara dimensionerat för att klara.

I likhet med vad som gäller enligt den nuvarande bestämmelsen om säkerhetsanalys anser vi att resultatet av säkerhetsskyddsanalysen ska dokumenteras.

En närliggande fråga till vad säkerhetsskyddsanalysen ska innehålla är på vilket sätt och hur ofta en sådan bör genomföras. Som vi nämnt i inledningen av detta avsnitt skiljer sig omfattningen av den verksamhet som är i behov av säkerhetsskydd mycket åt mellan de myndigheter och övriga som har att tillämpa säkerhetsskyddsregleringen. Vi anser ändå att det i verksamheten bör finnas en tydligt angiven process för hur en säkerhetsskyddsanalys bör genomföras. Det bör påpekas att säkerhetsskyddsanalysarbetet är en del av verksamhetens hela säkerhetsplanering och en kontinuerligt pågående process. I de verksamheter där merparten av verksamheten kräver säkerhetsskydd bör säkerhetsskyddsanalys genomföras oftare än vad som kan vara aktuellt för andra verksamheter där säkerhetsskydd krävs för en mycket liten del av verksamheten. Vi anser att att säkerhetsskyddsanalysen bör uppdateras årligen eller vid behov och att det därför bör föras in en bestämmelse i säkerhetsskyddsförordningen om att säkerhetsskyddsanalysen ska hållas uppdaterad.

13.4 Samordning med andra risk- och sårbarhetsanalyser

Risk- och sårbarhetsanalyser

De flesta verksamheter har i dag krav på sig att genomföra olika typer av risk- och sårbarhetsanalyser. Det bredare arbetet med att stärka samhällets skydd av samhällsviktiga funktioner och anläggningar samt samhällets informationssäkerhet medför att analyserna

ofta är kopplade till särskilda typer av olyckor, kriser, risker och hot. Risk- och sårbarhetsanalysen har till syfte att kartlägga vilka händelser som kan hota verksamheten, vilka konsekvenser händelserna kan få och i vilken mån man klarar av att hantera dem. Det gäller således att identifiera riskerna och bedöma hur sårbar verksamheten är mot dessa. Genom risk- och sårbarhetsanalysen blir det lättare för organisationen att identifiera problem, prioritera dem och vidta adekvata åtgärder i tid.

Alla statliga myndigheter, kommuner och landsting ska genomföra risk- och sårbarhetsanalyser inom sina respektive områden. Förutom att tillgodose egennyttan för den egna organisationen eller verksamheten tillgodoser dessa risk- och sårbarhetsanalyser även behovet av att kunna ge en samlad bild av risker och sårbarheter som finns i samhället i stort.

Nedan redovisas några exempel på regleringar som innehåller bestämmelser med krav på risk- och sårbarhetsanalyser. Utöver dessa finns ett flertal regelverk med krav på olika typer av riskanalyser, bl.a. inom områdena arbetsmiljö, ekonomisk säkerhet och miljöskydd.

Risk- och sårbarhetsanalys enligt förordningen om krisberedskap och höjd beredskap

Enligt 9 § förordningen (2006:942) om krisberedskap och höjd beredskap ska varje myndighet (vissa undantagna, se 3 §) i syfte att stärka sin egen och samhällets krisberedskap årligen analysera om det finns sådan sårbarhet eller sådana hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Myndigheten ska värdera och sammanställa resultatet av arbetet i en risk- och sårbarhetsanalys.

Risk- och sårbarhetsanalysen ska identifiera de största riskerna och sårbarheterna i samhällsviktig verksamhet. Utifrån dessa ska sedan identifieras nödvändiga åtgärder för att uppnå resultatmålen och för att säkerställa de grundläggande säkerhetsnivåerna. Dessa utgör den lägsta nivån av funktionalitet och säkerhet som bör råda oavsett händelse eller påfrestning i samhället.

Risk- och sårbarhetsanalys enligt lagen om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

Av 2 kap. 1 § lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap framgår att kommuner och landsting ska analysera vilka extraordinära händelser i fredstid som kan inträffa i kommunen respektive landstinget och hur dessa händelser kan påverka den egna verksamheten. Resultatet av arbetet ska värderas och sammanställas i en risk- och sårbarhetsanalys.

Av förarbetena till lagen[9] framgår att det viktigaste syftet med att ta fram risk- och sårbarhetsanalyser är att öka medvetandet och kunskapen hos beslutsfattare och verksamhetsansvariga om vilka hot och risker som finns inom det egna verksamhetsområdet. Ett annat viktigt syfte är att få fram ett underlag för planering och genomförande av åtgärder som minskar riskerna och sårbarheten i kommunerna. Arbetet med risk- och sårbarhetsanalyserna är också ett värdefullt stöd i den fysiska planeringen för att kunna hantera en extraordinär händelse. Eftersom kommunerna ansvarar för ett stort antal viktiga samhällsuppgifter som måste kunna upprätthållas även under störda förhållanden behövs risk- och sårbarhetsanalyser även på lokal nivå. De är också ett viktigt underlag för analyserna på läns- och riksnivå och kan bidra till en helhetsbild av vilka risker och sårbarheter som finns i hela samhället.

Riskanalys enligt lagen om skydd mot olyckor

Av lagen (2003:778) om skydd mot olyckor framgår att, vid en anläggning där verksamheten innebär fara för att en olycka ska orsaka allvarliga skador på människor eller miljön, anläggningens ägare eller den som utövar verksamheten på anläggningen är skyldig att analysera riskerna för sådana olyckor (se 2 kap. 4 §).

Enligt förarbetena till lagen[10] bör riskanalysen innehålla bl.a. en beskrivning av möjliga scenarier för sådana olyckor som skulle kunna medföra allvarliga skador på människor eller i miljön. Den

[9] Prop. 2005/06:133 Samverkan vid kris – för ett säkrare samhälle, s. 105 f.
[10] Prop. 2002/03:119 Reformerad räddningstjänstlagstiftning, s. 52.

ska i första hand vara ett underlag för bedömningen av vilken beredskap för effektiva räddningsinsatser som behöver upprätthållas vid anläggningen för att komplettera den kommunala insatsberedskapen. Riskanalysen är vidare ett underlag för kommunens tillsyn över anläggningen.

Risk- och sårbarhetsanalys enligt elberedskapslagen

Elberedskapslagen (1997:288) ändrades den 1 juli 2012. Ändringarna innebar att syftet med den huvudsakliga inriktningen av de elberedskapsåtgärder som ska vidtas enligt lagen har ändrats till att förebygga, motstå och hantera sådana störningar i elförsörjningen som kan medföra svåra påfrestningar på samhället. Man har således frångått kravet på att åtgärderna ska säkerställa elförsörjningen när landet är i höjd beredskap.

Genom ändringen i elberedskapslagen infördes också en skyldighet för den som omfattas av lagen att upprätta en risk- och sårbarhetsanalys avseende säkerheten i den egna verksamheten. Det infördes även en skyldighet för samma aktörer att lämna de uppgifter som behövs för att Affärsverket svenska kraftnät som elberedskapsmyndighet ska kunna upprätta en nationell risk- och sårbarhetsanalys enligt förordningen om krisberedskap och höjd beredskap.

Fördelar med samordning av arbetet med olika analyser

Som framhållits tidigare har de flesta verksamheter i dag krav på sig att genomföra olika typer av risk- och sårbarhetsanalyser. De har därmed redan processer för att ta fram sådana. Inte minst utvecklingen av informationstekniken har inneburit att i princip alla verksamheter, såväl offentliga som enskilda, numera är beroende av informationstillgångar som måste skyddas. För att kunna bedöma säkerhets- och skyddsnivåer för dessa tillgångar krävs att det i verksamheten upprättas olika typer av risk- och sårbarhetsanalyser. En ofullständig eller felaktig säkerhets- eller skyddsnivå kan å ena sidan leda till att organisationen utsätts för en skada som kan få allvarliga konsekvenser. Överdriven säkerhet kan å andra sidan vara verksamhetshämmande och kostnadsdrivande. Arbetet med att

analysera verksamheten utifrån dessa perspektiv är således av stor betydelse för verksamheten. Vi konstaterar att många av de identifieringar, prioriteringar och bedömningar som behöver vidtas i arbetet med säkerhetsskyddsanalysen görs även i andra typer av risk- och sårbarhetsanalyser. Det är angeläget att i arbetet med säkerhetsskyddsanalysen ta vara på den kunskap och de erfarenheter och de resultat som redan finns i organisationen på risk- och sårbarhetsområdet.

Som framgått har regelverken med krav på planer och analyser olika utgångspunkter. Ofta sammanfaller delvis de risker, hot och konsekvenser av händelser som ska analyseras. Arbetet med att ta fram olika typer av t.ex. säkerhets-, risk- och sårbarhetsanalyser tar mycket tid och stora resurser i anspråk. Det är därför viktigt att i möjligaste mån undvika dubbelarbete och i så stor utsträckning som möjligt samordna analysarbetet utifrån flera olika regelverk. En samordning av analysarbetet bidrar också till en bättre helhetssyn på organisationens säkerhetsarbete i stort.

Vi anser att säkerhetsskyddsanalysarbetet så långt som möjligt bör komplettera, relatera till och utnyttja det arbete som bedrivs med att ta fram andra former av risk- och sårbarhetsanalyser i syfte att stärka samhällets skydd av samhällsviktiga funktioner och anläggningar samt samhällets informationssäkerhet. Det är dock viktigt att vara medveten om de olika regelverkens utgångspunkter. Säkerhetsskyddsanalysen ska fokusera på i huvudsak antagonistiska hot och de delar av verksamheten där de allvarligaste konsekvenserna för nationen kan uppstå om sådana hot förverkligas. Detta innebär att, till skillnad från många riskanalyser, säkerhetsskyddsanalysen inte alltid behöver innehålla någon beräkning av sannolikheten för att ett hot ska realiseras (se avsnitt 13.2 under rubriken Säkerhetshotbedömning).

13.5 Säkerhetsskyddsanalys och sekretess

I det allmännas verksamhet

Risk- och sårbarhetsanalyser syftar till att minska samhällets sårbarhet, bl.a. genom att öka myndigheternas förmåga att förutse och hantera fredstida krissituationer. För att uppgifterna inte ska kunna utnyttjas för angrepp mot myndigheter, enskilda eller samhället i

stort är det nödvändigt att i viss utsträckning begränsa insynen i denna verksamhet. I 18 kap. 13 § OSL finns föreskrifter om sekretess för uppgifter i upprättade risk- och sårbarhetsanalyser. Sekretessen gäller endast om det kan antas att det allmännas möjligheter att förebygga eller hantera fredstida kriser skulle motverkas om uppgiften röjs.

Även andra sekretessbestämmelser kan bli tillämpliga på uppgifter i risk- och sårbarhetsanalyser, t.ex. 18 kap. 8 och 9 §§ OSL.

En säkerhetsskyddsanalys innehåller i många fall sådana uppgifter som, om de röjs för obehörig, kan skada totalförsvaret eller rikets säkerhet i övrigt. En genomförd säkerhetsskyddsanalys torde därmed i regel omfattas av sekretess enligt 15 kap. 2 § OSL, s.k. försvarssekretess. Säkerhetsskyddsanalysen kan givetvis även innehålla uppgifter som omfattas av annan sekretess än försvarssekretess. I rättstillämpningen har en säkerhetsskyddsanalys ansetts omfattas av sekretess enligt 15 kap. 2 § OSL.[11]

I enskildas verksamhet

Som redan påpekats bedriver enskilda numera säkerhetskänslig verksamhet i betydligt större omfattning än tidigare. Eftersom säkerhetsskyddslagstiftningen bygger på grundtanken att de intressen lagstiftningen slår vakt om ska ha samma skydd oavsett om verksamheten bedrivs av det allmänna eller av enskilda innebär detta att även enskilda som bedriver säkerhetskänslig verksamhet är skyldiga att upprätta en säkerhetsskyddsanalys. Frågan om hemlighållandet av en sådan utifrån offentlighetsprincipen blir dock i flertalet fall aldrig aktuell eftersom enskilda till skillnad från det

[11] Kammarrättens i Jönköping dom den 7 september 2012 (mål nr 2490-12) - X kommun beslutade att lämna ut handlingen ”Säkerhetsanalys för X kommun” med undantag för uppgifter som sekretessbelagts med stöd av säkerhetsskyddslagen [sic!]. Beslutet motiverades med kommunens ansvar enligt säkerhetsskyddslagen för att skydda den information och de anläggningar som kommunen bedömer vara av betydelse för rikets säkerhet eller som behöver skyddas mot terrorism. Beslutet överklagades. Kammarrätten fann att det i de maskerade delarna av säkerhetsanalysen redovisades allmänna och specifika uppgifter om åtgärder för att skydda anläggningar och övrig infrastruktur av betydelse för att upprätthålla viktiga samhällsfunktioner. Enligt kammarrätten kunde det antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgifterna röjdes. De tillämpliga bestämmelserna i offentlighets- och sekretesslagen tar direkt sikte på att skydda sådana uppgifter som kan utgöra ett hot mot rikets säkerhet. Därmed omfattades de vid utlämnandet uteslutna uppgifterna i handlingen av sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen. Överklagandet avslogs. Domen har vunnit laga kraft.

allmänna normalt inte omfattas av tryckfrihetsförordningen och offentlighets- och sekretesslagen. En säkerhetsskyddsanalys som upprättats i enskild verksamhet kan således inte där bli föremål för sekretessprövning vid en begäran om utlämnande och delges endast till de som är behöriga att ta del av den.

En säkerhetsskyddsanalys innehåller i regel uppgifter som om de röjs kan medföra en skada för Sveriges säkerhet, t.ex. när det gäller beskrivningar av sårbarheter i säkerhetskänslig verksamhet. Därför bör känsliga uppgifter i analysen i stort sett alltid träffas av definitionen av säkerhetsskyddsklassificerade uppgifter (se avsnitt 12.2). Därmed ges ett skydd för sådana uppgifter även i enskildas verksamhet.

14 Ett tydligare verksamhetsansvar

Reformbehovet handlar bl.a. om att förstärka och utveckla sådana viktiga grunddrag i säkerhetsskyddslagstiftningen som att säkerhetsskyddet ska vara detsamma oavsett om verksamheten är allmän eller enskild. Behovet av en ökad tydlighet i fråga om lagens tillämpningsområde föranleder (utöver de förslag vi lämnat i kapitel 12) dels förenklade bestämmelser om vilka verksamheter lagen gäller för, dels en kompletterande bestämmelse som tydligare anger vad verksamhetsansvaret i fråga om säkerhetsskydd innebär. De frågorna behandlas i de följande avsnitten 14.1 och 14.2.

14.1 Verksamheter som lagen gäller för

Förslag: Vilka verksamheter lagen gäller för ska anges på ett enklare sätt. Det ska inte göras någon uppdelning mellan företagsformer över vilket det allmänna har ett rättsligt bestämmande inflytande och företagsformer där ett sådant bestämmande inflytande inte föreligger. Lagen ska därför anges gälla för verksamhet hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet eller omfattas av ett internationellt säkerhetsskyddsåtagande (säkerhetskänslig verksamhet).

Nu gällande ordning

Säkerhetsskyddslagen är direkt tillämplig för såväl myndigheter, kommuner och landsting som verksamhet som bedrivs i olika företagsformer. Vilka verksamheter som lagen gäller för anges i dag på ett förhållandevis omständligt sätt i 1 § säkerhetsskyddslagen.

Bestämmelsen innehåller bl.a. ett moment som särskiljer aktiebolag, handelsbolag, föreningar och stiftelser över vilka det allmänna har ett rättsligt bestämmande inflytande. Vid myndigheter, kommuner och landsting samt vid företagsformer där det allmänna har ett rättsligt bestämmande inflytande gäller säkerhetsskyddslagen enligt ordalydelsen generellt medan den för enskilda (dvs. företagsformer där det allmänna inte utövar något rättsligt bestämmande inflytande) gäller om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Vad som i sammanhanget avses med rättsligt bestämmande inflytande definieras i 4 §. Vilken funktion uppdelningen mellan olika slag av verksamhetsformer fyller för att bestämma lagens tillämpningsområde och varför olika uttryckssätt valts i fråga om lagens tillämplighet framstår som oklart.

Hur kraven på säkerhetsskydd skulle regleras när det är fråga om enskild verksamhet var föremål för överväganden när säkerhetsskyddslagen infördes. Säkerhetsskyddsutredningens förslag[1] byggde på just en åtskillnad mellan företag där det allmänna har ett rättsligt bestämmande inflytande och företag där ett sådant bestämmande inflytande inte finns. För andra än de ”offentligt ägda” företagen skulle lagen bli tillämpligen först sedan den s.k. funktionsansvariga myndigheten enligt beredskapslagstiftningen tagit initiativ till att träffa ett säkerhetsskyddsavtal med det berörda företaget. Den föreslagna metoden avfärdades dock av flera remissinstanser, bl.a. av konstitutionella skäl.[2] Regeringen föreslog i stället att lagen gjordes direkt tillämplig för samtliga företagsformer. Att lagen är tillämplig uttrycks dock i lagen på olika sätt beroende på om det är fråga om myndigheter, kommuner, statliga bolag etc. (1 § 1 och 2) eller enskild verksamhet (1 § 3). För enskild verksamhet anges som nämnts att lagen gäller om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. För myndigheter, kommuner, statliga bolag etc. gäller lagen utan något sådant kvalificeringskrav. Den konstruktionen medför bl.a. krav på myndigheter och statliga bolag att oavsett inriktning på verksamheten göra en dokumenterad säkerhetsanalys enligt 5 § säkerhetsskyddsförordningen. Att kraven på säkerhets-

[1] Betänkandet Säkerhetsskydd (SOU 1994:149), s. 135 ff.
[2] Prop.1995/96:129 Säkerhetsskydd, s. 36 f.

skydd har fått en sådan generell giltighet i den allmänna verksamheten verkar ha motiverats av kommunernas roll i beredskapsplanläggningen.[3]

Förändringsbehovet

I kapitel 10 har vi tagit upp förhållandet mellan bl.a. beredskapsplanläggning och säkerhetsskydd. En viktig utgångspunkt som vi där redovisat är att bl.a. hänsynen till motstående intressen som kostnadseffektivitet och skydd av personlig integritet medför att krav på säkerhetsskyddsåtgärder behöver avgränsas till att gälla för de verksamheter som är mest skyddsvärda från ett nationellt perspektiv. En annan väsentlig avgränsning är att säkerhetsskyddet är inriktat mot i huvudsak antagonistiska hot. Verksamhet som är av betydelse för Sveriges säkerhet är självfallet av särskilt intresse också från ett vidare samhällsskydds- och beredskapsperspektiv. Tillämpningsområdena sammanfaller däremot inte. Inom ramen för det bredare arbetet med att stärka skyddet av samhällsviktig verksamhet och kritisk infrastruktur ska risk- och sårbarhetsanalyser av olika slag alltid utföras av kommuner, landsting och i princip också av samtliga myndigheter (se avsnitt 13.4). Inte bara möjlig skadlig påverkan från ett nationellt perspektiv är väsentlig i det sammanhanget. Också konsekvenser som är begränsade till en regional eller lokal nivå ska beaktas. Skyddet ska också kunna svara mot en bredare hotbild som innefattar t.ex. extrema väderförhållanden och olyckor. Krav på åtgärder i fråga om samhällsskydd och beredskap gäller mot den bakgrunden för samtliga landets kommuner och landsting och i princip samtliga myndigheter. Vi har valt att åskådliggöra sambandet mellan säkerhetsskydd och andra skyddsåtgärder i samhället genom en pyramidskiss (se avsnitt 10.1.1) där de verksamheter som bör omfattas av säkerhetsskyddslagen representerar den översta delen av en pyramid bestående av alla verksamheter som är viktiga för ett fungerande samhälle. Med en sådan utgångspunkt för vad som bör omfattas av lagens tillämpningsområde förefaller det något inkonsekvent att t.ex. samtliga myndigheter och statliga och kommunala bolag – oberoende av vad verk-

[3] Prop. 1995/96:129 s. 29 f.

samheten avser – omfattas av säkerhetsskyddslagstiftningen. En sådan ordning kan också ge intryck av att säkerhetsskydd primärt är en angelägenhet för allmän verksamhet. Beskrivningen av vilka verksamheter som omfattas av lagen bör därför genomgående utgå från ett kvalificeranderekvisit för att träffa endast de verksamheter som behöver ett säkerhetsskydd. Ett enhetligt sätt att ange lagens tillämpningsområde har också den fördelen att den nuvarande rätt svårtillgängliga avgränsningsmetoden, som gör en skillnad mellan olika former av enskild verksamhet utifrån en definition om vad som konstituerar rättsligt bestämmande inflytande, blir överflödig.

Det avgörande för lagens tillämplighet bör således vara om verksamheten är att anse som säkerhetskänslig, dvs. är av betydelse för Sveriges säkerhet eller omfattas av ett internationellt säkerhetsskyddsåtagande. Som vi betonat tidigare tar den definitionen av säkerhetskänslig verksamhet inte sikte på verksamheten i stort, dvs. myndigheten, bolaget etc., utan på de delar av en verksamhet, t.ex. vissa anläggningar eller uppgifter, som är av betydelse för Sveriges säkerhet eller annars behöver ett säkerhetsskydd med hänsyn till ett internationellt säkerhetsskyddsåtagande.

Att kvalificeringskravet gäller lika för alla verksamhetsformer innebär en förenklad ordning där en skyldighet att genomföra en dokumenterad säkerhetsskyddsanalys kommer att föreligga först om verksamheten är säkerhetskänslig enligt lagens definition. För vissa myndigheter etc. bör det vara rätt uppenbart att verksamheten är att anse som säkerhetskänslig. För andra verksamheter kan det vara nödvändigt att utföra någon form av förenklad säkerhetsskyddsanalys för att kunna bedöma om lagen är tillämplig eller inte. I det avseendet är också vägledning från Säkerhetspolisen och Försvarsmakten samt de säkerhetsskyddsstödjande myndigheterna[4] viktigt (se avsnitt 21.1 och 21.2). Som vi betonat tidigare behöver emellertid det primära ansvaret för säkerhetsskyddet, liksom i dag, finnas på en verksamhetsnivå. Vad det ansvaret innebär bör dock

[4] I direktiven används benämningen sektorsansvariga myndigheter som en samlande benämning för Affärsverket svenska kraftnät, Post- och telestyrelsen, Transportstyrelsen och länsstyrelserna. Som framgår av avsnitt 10.1.5 har vi i stället valt att använda säkerhetsskyddsstödjande myndigheter som en samlande benämning för dessa myndigheter såvitt avser deras funktioner för säkerhetsskyddet. Vi föreslår vidare i avsnitt 18.10 och 21.2.4 att Myndigheten för samhällsskydd och beredskap ska ta över de uppgifter länsstyrelserna i detta avseende har samt även, i fråga om tillsyn och rådgivning, vara säkerhetsskyddsstödjande myndighet för kommuner och landsting.

framgå tydligare av regleringen. Den frågan behandlas i det följande.

14.2 Tydligare regler om vilka skyldigheter lagen innebär

Förslag: Följden av att lagen är tillämplig för en verksamhet ska framgå tydligare genom att det i lagen anges att den som ansvarar för en säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd, se till att säkerhetsskyddsåtgärder vidtas, kontrollera att bestämmelserna om säkerhetsskydd följs samt lämna uppgifter som följer av viss rapporteringsskyldighet till utsedda tillsynsmyndigheter.

Säkerhetsskyddslagen innebär skyldigheter i olika avseenden för myndigheter, kommuner, landsting och företag. Skyldigheterna framgår både explicit och indirekt av säkerhetsskyddslagen och den tillhörande förordningen. Kravet på att genomföra en säkerhetsanalys för att identifiera vad som ska omges av ett säkerhetsskydd anges i 5 § säkerhetsskyddsförordningen. Kraven på att vidta säkerhetsskyddsåtgärder framgår däremot endast indirekt av 5 § säkerhetsskyddslagen där det anges att i verksamhet där lagen gäller det säkerhetsskydd ska finnas som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Vad säkerhetsskydd innebär och syftar till framgår av de efterföljande lagbestämmelserna. I lag regleras också krav på att träffa säkerhetsskyddsavtal vid upphandling (8 §), krav på att göra säkerhetsprövning av personal (11 §) samt att utföra intern utbildning och kontroll (30 §). I säkerhetsskyddsförordningen finns bl.a. bestämmelser som närmare reglerar krav på informationssäkerhetsåtgärder (10–13 §§).

Att säkerhetsskyddslagen är tillämplig medför skyldigheter i olika avseenden för myndigheter, kommuner, landsting och enskilda verksamheter. Åligganden för enskilda verksamheter, kommuner och landsting ska ha stöd i lag. Mot den bakgrunden föreslår vi en kompletterande bestämmelse i säkerhetsskyddslagen som anger en grundläggande skyldighet för den som ansvarar för en säkerhetskänslig verksamhet att utreda behovet av säkerhetsskydd

(se avsnitt 13.2), vidta säkerhetsskyddsåtgärder och kontrollera det egna säkerhetsskyddet. I fråga om säkerhetsskyddets nivå och utformning bör det på samma sätt som i dag anpassas till verksamhetens art, omfattning och övriga omständigheter. Dessutom behöver anges att säkerhetsskyddet i fråga om säkerhetsskyddsklassificerade uppgifter ska anpassas till den informationssäkerhetsklass som gäller för uppgiften (se vidare avsnitt 15.3). Vidare bör bestämmelsen ge stöd för skyldigheten att i vissa avseenden lämna uppgifter om säkerhetsskyddet till myndigheter som är utsedda att kontrollera säkerhetsskyddet (se vidare avsnitt 21.4).

Det bör framhållas att det förhållandet att en leverantör har ingått ett avtal om säkerhetsskydd med t.ex. en upphandlande myndighet inte medför att de skyldigheter som lagen anger för den som ansvarar för en verksamhet därmed åligger leverantören. I upphandlingssituationer där t.ex. en myndighet avser att begära in anbud eller träffa avtal med en leverantör bör, som vi återkommer till i kapitel 19, det säkerhetsskydd som behövs för upphandlingen på samma sätt som i dag närmare preciseras och bestämmas genom en skriftlig överenskommelse. I vissa fall kan dock leverantörens verksamhet vara av sådant slag att denne ändå träffas av de skyldigheter som gäller för den som är ansvarig för en säkerhetskänslig verksamhet.

15 Ett system av samverkande säkerhetsskyddsåtgärder

Säkerhetsskydd består av en uppsättning åtgärder för att ge ett skydd för säkerhetskänslig verksamhet. I kapitel 13 har vi redogjort för hur den säkerhetskänsliga verksamheten kan identifieras och om hur hot mot sådan verksamhet kan analyseras och hanteras. Grunden för att kunna vidta relevanta säkerhetsskyddsåtgärder är en väl genomförd säkerhetsskyddsanalys som visar vilken säkerhetskänslig verksamhet som behöver ett säkerhetsskydd och vilka risker och sårbarheter som behöver hanteras i verksamheten. Analysen ligger till grund för en säkerhetsplan där ändamålsenliga säkerhetsskyddsåtgärder kan konkretiseras i tid och rum.

Vi har i kapitel 10 tagit upp att säkerhetsskyddsåtgärderna informationssäkerhet, tillträdesbegränsning och säkerhetsprövning ska kvarstå i en ny lag men att det finns behov av att se över benämningarna. Den frågan behandlas i avsnitt 15.1 och i avsnitt 15.2 redogör vi för hur säkerhetsskyddsåtgärderna inbördes förhåller sig till varandra. I avsnitt 15.3 föreslår vi därefter en indelning av säkerhetsskyddsklassificerade uppgifter i fyra informationssäkerhetsklasser och beskriver hur detta inte bara påverkar informationssäkerheten utan även är av central betydelse för övriga säkerhetsskyddsåtgärder. Avslutningsvis behandlar vi i avsnitt 15.4 förhållandet mellan säkerhetsskyddsåtgärderna och andra motstående allmänna och enskilda intressen.

15.1 Säkerhetsskyddsåtgärderna i en ny säkerhetsskyddslag

Förslag: De tre säkerhetsskyddsåtgärderna ska kvarstå i en ny lag och benämnas informationssäkerhet, fysisk säkerhet och personalsäkerhet.

Dessa säkerhetsskyddsåtgärder samverkar och utgör ett sammanhållet system för skydd av säkerhetskänslig verksamhet.

Delvis nya begrepp

I avsnitt 10.1.4 har vi redovisat att indelningen i tre säkerhetsskyddsåtgärder ska bestå i en ny säkerhetsskyddslag. Skälen till detta är dels att lagen alltjämt bör ha ett verksamhetsperspektiv, dels att nuvarande indelning har fungerat bra och synes vara ändamålsenlig.

Vi föreslår att begreppet *informationssäkerhet* behålls. Begreppet infördes i nuvarande säkerhetsskyddslag som en ersättning för begreppet *sekretesskydd* i 1981 års säkerhetsskyddsförordning. Skälet till förändringen var huvudsakligen utvecklingen på informationsteknikens område.[1] Informationssäkerhet är i dag ett vedertaget begrepp och används förutom i säkerhetsskyddslagstiftningen även i övrigt som ett samlingsbegrepp för skyddsåtgärder för information. Begreppet motsvaras på engelska av *Information Security*. Informationssäkerheten behandlas vidare i kapitel 16 där också innebörden av begreppet utvecklas.

Begreppet *tillträdesbegränsning* infördes i säkerhetsskyddslagen som ersättning för begreppet *tillträdesskydd* i 1981 års säkerhetsskyddsförordning trots att flera remissinstanser invände mot begreppet. Vi anser att begreppet i dag inte svarar fullt ut mot de faktiska åtgärder som behöver vidtas inom ramen för denna säkerhetsskyddsåtgärd. Det första ledet *tillträde* leder tankarna till personer som fysiskt tar sig in i en byggnad eller på ett område. Säkerhetsskyddsåtgärder bör kunna vidtas även mot andra tillvägagångssätt att skada eller på annat sätt obehörigen påverka t.ex. en byggnad eller ett område och verksamheten där. Vidare bör det

[1] Prop. 1995/96:129 Säkerhetsskydd, s. 26.

kunna vidtas säkerhetsskyddsåtgärder mot t.ex. försändelser med skadligt innehåll vilket inte heller är tillträde i ordets rätta betydelse. Vi föreslår därför att begreppet ändras till *fysisk säkerhet* vilket vi anser bättre överensstämmer med de faktiska åtgärderna. Begreppet motsvaras på engelska av *Physical Security*. Den fysiska säkerheten behandlas vidare i kapitel 17.

Begreppet *säkerhetsprövning* ersatte i nuvarande säkerhetsskyddslag det tidigare begreppet *infiltrationsskydd*.[2] Skälen till ändringen var att åtgärderna syftar till mer än att bara ge ett skydd mot infiltration, t.ex. ett skydd mot att personer som av andra anledningar är olämpliga ur säkerhetssynpunkt får del av hemliga uppgifter. När det gäller säkerhetsprövning föreslår vi en mindre systematisk förändring så att säkerhetsprövningen kompletteras med krav på utbildning i säkerhetsskydd och att utbildningens betydelse för säkerhetsskyddet på så sätt förtydligas. Som en ny rubrik på dessa samverkande åtgärder föreslår vi begreppet *personalsäkerhet*. Med denna systematik består alltså personalsäkerheten av delmomenten säkerhetsprövning och utbildning. Mot detta nya begrepp kan invändas att åtgärderna inte avser enbart personal utan även andra personer som deltar i säkerhetskänslig verksamhet. Den absoluta huvuddelen av de som omfattas av denna säkerhetsskyddsåtgärd träffas dock av ordet personal, åtminstone i sin vidaste betydelse. Vi bedömer därför att någon missförståndsrisk inte föreligger, trots att en viss brist i begreppets precision föreligger. Begreppet motsvaras på engelska av *Personnel Security*. Personalsäkerheten behandlas vidare i kapitel 18.

Säkerhetsskyddsåtgärdernas omfattning

Vårt förslag till förändring av lagens systematik medför att en ny lag ska ge ett skydd inte enbart för hemliga uppgifter och mot terrorism. Lagen ska ge ett skydd för säkerhetskänslig verksamhet. Det innefattar ett skydd för såväl säkerhetsskyddsklassificerade uppgifter som för verksamhet som av annan anledning är säkerhetskänslig. I det sistnämnda innefattas skydd mot skadlig påverkan på t.ex. verksamheter som innefattar styrning och hante-

[2] A prop. s. 28.

ring av samhällskritiska it-system, el- och energiförsörjning, sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle eller verksamhet som behöver skyddas på den grunden att den omfattar sådant som kan skada nationen, t.ex. vissa verksamheter inom det kärntekniska området.

En sådan bredare ansats innebär bl.a. att skyddsåtgärderna som i nuvarande säkerhetsskyddslag främst tar sikte på skydd av konfidentialitet för vissa uppgifter i en reformerad lag ska omfatta även tillgängligheten och riktigheten för informationstillgångar där sådan funktionalitet är av betydelse för Sveriges säkerhet. Den fysiska säkerheten som i dag är inriktad mot att förhindra ett obehörigt tillträde för i första hand skydd av hemliga uppgifter eller mot terrorism utvidgas med ett sådant synsätt till att avse även ett skydd mot skadlig påverkan mot säkerhetskänslig verksamhet och mot obehörig åtkomst till t.ex. kärnavfall, vapensystem, smittoämnen och andra farliga verksamheter som hos obehöriga kan utgöra ett hot mot Sveriges säkerhet. I fråga om personalsäkerheten tydliggörs att pålitligheten från säkerhetssynpunkt ska prövas även i fråga om deltagande i annan säkerhetskänslig verksamhet än sådan som rör hantering av säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskyddsåtgärdernas omfattning behandlas vidare i kapitel 16–18.

15.2 Säkerhetsskyddsåtgärdernas inbördes förhållande

Ett system av samverkande åtgärder

Säkerhetsskyddsåtgärderna ska inte ses som tre från varandra isolerade åtgärder utan som delar i ett system för att uppnå ett ändamålsenligt skydd. Säkerhetsskyddsåtgärder inom dessa tre områden ska samverka som en helhet. De olika delarna är beroende av varandra. Säkerhetsskyddsåtgärderna kan i olika situationer kombineras på olika sätt för att optimera skyddseffekten. Ett sådant synsätt leder till ett balanserat och kostnadseffektivt säkerhetsskydd. Grunden för vilka säkerhetsskyddsåtgärder som ska vidtas läggs i säkerhetsskyddsanalysen och dessa åtgärder ska sedan konkretiseras i en säkerhetsskyddsplan. En säkerhetsskyddsplan som leder

till åtgärder enbart inom personalsäkerheten bygger troligtvis i många fall på en felaktigt genomförd analys eftersom den säkerhetskänsliga verksamheten som ligger till grund för t.ex. en säkerhetsklassplacering rimligen måste medföra krav på säkerhetsskyddsåtgärder också avseende informationssäkerhet och fysisk säkerhet. Det saknas därför förutsättningar att uppnå ett tillräckligt säkerhetsskydd utifrån en bedömning som tar sikte på enbart behovet av säkerhetsprövning och som ensidigt fokuserar på möjligheter till registerkontroll. Därtill kommer att säkerhetsprövning och registerkontroll medför ett ingrepp i den personliga integriteten. Därför måste åtgärden vara noggrant bedömd mot det behov som åtgärden ska tillgodose.

Det sagda innebär dock inte att de tre säkerhetsskyddsåtgärderna alltid måste ha samma omfattning. Ett säkerhetsskydd för sådan säkerhetskänslig verksamhet som genom sin natur kan innebära skadlig påverkan på en sådan nivå att det rör Sveriges säkerhet (t.ex. kärnteknisk verksamhet) kanske har en tyngdpunkt på den fysiska säkerheten medan en säkerhetskänslig verksamhet som berör samhällskritisk it-infrastruktur av naturliga skäl har fokus på informationssäkerheten. Dessa exempel kan också belysa att, även när fokus ligger på en av åtgärderna, det inte går att bortse från de övriga säkerhetsskyddsåtgärdernas betydelse. I båda exemplen är även t.ex. personalsäkerhetsåtgärder viktiga inslag i säkerhetsskyddet.

Ett område som tas upp i våra direktiv är säkerhetsskyddsåtgärder vid transporter av farligt gods. Direktiven hänvisar i det avseendet till bl.a. en rapport från Riksrevisionen.[3] Förslagen i rapporten har sedan direktiven beslutades till följd av ett regeringsuppdrag behandlats i en gemensam rapport från Myndigheten för samhällsskydd och beredskap och Transportsstyrelsen.[4] I fråga om säkerhetsskyddsåtgärder hänvisas i rapporten till vårt uppdrag. Myndigheterna konstaterar dock bl.a. att regler om att vissa personer delaktiga i transport av farligt gods ska omfattas av säkerhetsprövning med registerkontroll kan leda till att ett stort

[3] Rapporten Skyddet för farligt gods, RiR 2008:29 (Ju2008/10750/L4, N2008/8857/TE, Fö2008/3701/SSK).
[4] 2013-04-19 Redovisning av uppdrag om att stärka och utveckla transportskyddet vid transport av farligt gods (Regeringsbeslut Fö2012/1989/SSK), Dnr MSB: 2012-5683, Dnr TS: TSG2112-1058.

antal personer träffas av sådan prövning eller kontroll.[5] Det framhålls att de positiva skyddseffekterna noggrant bör relateras till integritetsaspekten och det ökade arbete som krävs för att behandla prövningar och kontroller.

Vi delar dessa uppfattningar och konstaterar att en restriktiv hållning är nödvändig när det gäller att hänföra verksamheter till kategorin i övrigt säkerhetskänslig verksamhet. För sådan verksamhet är det också särskilt viktigt att säkerhetsskyddet består av samverkande åtgärder av olika slag. För säkerhetsprövning behöver särskild restriktivitet iakttas. Säkerhetsprövning kan vara ett komplement avseende vissa nyckelfunktioner inom t.ex. den nämnda transportverksamheten. I övrigt bör fokus ligga på andra säkerhetsskyddsåtgärder avseende fysisk säkerhet och informationssäkerhet och i fråga om utbildningsinsatser inom ramen för personalsäkerheten i stort. Också inom vissa andra områden där det i dag finns stöd för registerkontroll, t.ex. personal vid vissa skyddsobjekt, är det viktigt med en kritisk hållning till denna inriktning av säkerhetsskyddet.

I arbetet med att ta fram lämpliga säkerhetsskyddsåtgärder finns det fördelar med ett konstruktivt tänkande för att kunna åstadkomma ett säkerhetsskydd på ett kostnadseffektivt sätt och med så små ingrepp som möjligt i enskildas integritet och i verksamhetens effektivitet. Om arbetet t.ex. organiseras så att färre får del av säkerhetsskyddsklassificerade uppgifter och att arbetet med dessa uppgifter utförs i särskilda lokaler, kan det göras stora besparingar när det gäller t.ex. byggnadstekniska åtgärder och utformning av informationssystem. Dessutom innebär det att färre personer behöver genomgå säkerhetsprövning. Med en sådan lösning minskas även den samlade sårbarheten.

[5] På sidan 27 i rapporten nämns som exempel att cirka 16 000 förare har intyg att transportera tankar lastade med farligt gods och kan därmed transportera bensin i volymer överstigande 3 000 liter som definieras som farligt gods med hög riskpotential. Dessutom kan ett flertal andra personer än de som Myndigheten för samhällsskydd och beredskap utfärdar intyg för vara delaktiga i transportverksamheten, antingen som förare eller i någon annan befattning.

Säkerhetsskyddsåtgärdernas syfte

Säkerhetsskydd fokuserar på antagonistiska hot mot de delar av en samhällsviktig verksamhet som kan ge upphov till de allvarligaste konsekvenserna om de utsätts för bl.a. spionage, sabotage, terrorism eller andra brott som direkt eller indirekt kan medföra skada för säkerhetskänslig verksamhet. Säkerhetsskyddet har också en viktig funktion i att ge ett skydd för säkerhetsskyddsklassificerade uppgifter mot andra risker än sådana som beror på brott. Exempel på sådana åtgärder är skydd mot avlyssning och åtgärder för att minska utrymmet för misstag, tekniska brister eller annat som kan medföra oavsiktlig skadlig påverkan på informationen. Säkerhetsskydd handlar sammantaget om att bygga ett system av olika komponenter som åstadkommer ett effektivt skydd av det mest skyddsvärda.

Säkerhetsskyddsåtgärder kan ha fyra grundläggande funktioner. Dessa funktioner är att förebygga, upptäcka, fördröja (eller i bästa fall förhindra) samt hantera säkerhetshotande verksamhet. Detta gäller inom alla de områden inom vilket säkerhetsskyddet kan verka – informationssäkerhet, fysisk säkerhet och personalsäkerhet. Ett väl utformat säkerhetsskyddssystem tillhandahåller ett skydd på djupet. Det ger även en tidig förvarning t.ex. genom larm och minimerar skadekonsekvenserna om en komponent i säkerhetsskyddet skulle fallera.

15.3 Informationssäkerhetsklasser – grunden för skydd av säkerhetsskyddsklassificerade uppgifter

Förslag: Säkerhetsskyddsklassificerade uppgifter ska delas in i fyra informationssäkerhetsklasser efter den skada för Sveriges säkerhet som kan uppstå om uppgifterna röjs. De fyra klasserna ska benämnas *kvalificerat hemlig, hemlig, konfidentiell* och *begränsad*. Indelningen i informationssäkerhetsklasser är grunden för utformningen av den del av säkerhetsskyddsåtgärderna informationssäkerhet, fysisk säkerhet och personalsäkerhet som tar sikte på skyddet av säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande ska, om de inte redan

av annan stat eller mellanfolklig organisation har klassificerats, på motsvarande sätt delas in en informationssäkerhetsklass utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation.

En bestämmelse om indelning av säkerhetsskyddsklassificerade uppgifter ska införas i säkerhetsskyddslagen.

Informationsklassificering enligt nuvarande reglering

När säkerhetsskyddslagen infördes konstaterade regeringen att det inte var möjligt att i lagen precist ange på vilken nivå säkerhetsskyddet ska ligga. Enligt regeringen måste de överväganden i fråga om säkerhetsskyddets utformning som görs i en verksamhet där man regelmässigt handlägger frågor av mycket känslig natur skilja sig från dem i en verksamhet där man mer tillfälligt kommer i kontakt med dessa frågor. Regeringen menade att, med den föreslagna lagstiftningens utformning, säkerhetsskyddet i det enskilda fallet ska ha den utformning som krävs med hänsyn till verksamhetens art, omfattning och övriga omständigheter gav utrymme för olika hänsyn och att mer detaljerade bestämmelser kunde meddelas genom tillämpningsföreskrifter.[6]

I säkerhetsskyddslagen finns inga specifika regler om informationsklassificering för uppgifter och handlingar. Genom ett antal bestämmelser i framför allt säkerhetsskyddsförordningen framgår det dock att hemliga uppgifter kan ha en *synnerlig betydelse* för rikets säkerhet[7] samt att ett röjande av en hemlig uppgift kan medföra enbart ett *ringa men*.[8] Till dessa nivåskillnader kopplas olika säkerhetsskyddsåtgärder som t.ex. placering i säkerhetsklass och inventeringsintervall för hemliga handlingar. Det innebär att det finns såväl ett utrymme för, som ett behov av, att klassificera informationen utifrån hur allvarlig en skada kan bli vid ett eventuellt röjande av informationen.

Ett av de områden där lagen behöver utvecklas är när det gäller möjligheterna till internationell samverkan på säkerhetsskydds-

[6] A prop. s. 73 f.
[7] T.ex. i 9 § säkerhetsskyddsförordningen.
[8] T.ex. i 10 § säkerhetsskyddsförordningen.

området. Ett annat utvecklingsområde är att en säkerhetsskyddslag bör ge förutsättningar för ett nyanserat säkerhetsskydd som kan anpassas till verksamhetens behov. Det leder in på frågan om en indelning i fyra informationssäkerhetsklasser efter internationell modell skulle kunna förbättra förutsättningarna för att möta dessa utvecklingsbehov.

Försvarsmyndigheternas klassificeringssystem med fyra nivåer

Försvarsmakten införde 2004 fyra *informationssäkerhetsklasser* i Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd, för tillämpning i Försvarsmakten och vid de myndigheter som Försvarsmakten har föreskriftsrätt över enligt säkerhetsskyddsförordningen. Skälet till detta var att ett system med i praktiken två nivåer – hemligt och kvalificerat hemligt – stod mot de fyra nivåer (på engelska och i fallande ordning *Top Secret*, *Secret*, *Confidential* och *Restricted*) som tillämpas av många länder och mellanfolkliga organisationer. Genom att de två högsta nivåerna i praktiken motsvaras av de svenska nivåerna kvalificerat hemligt respektive hemligt blev konsekvensen att Försvarsmakten och andra myndigheter inom försvarssektorn behövde anlägga ett alltför högt säkerhetsskydd för uppgifter på nivåerna *Confidential* och *Restricted* med ökade kostnader och minskad effektivitet som följd.

Informationssäkerhetklasserna benämns som en kombination av ordet HEMLIG (med versaler) och nivåernas benämning på engelska (i fallande ordning HEMLIG/TOP SECRET, HEMLIG/SECRET, HEMLIG/CONFIDENTIAL och HEMLIG/RESTRICTED).

Enligt Försvarsmakten och andra myndigheter i försvarssektorn har hanteringen av uppgifter i myndigheternas internationella samarbeten härigenom blivit mer ändamålsenlig.

Nackdelar med nuvarande system

Avsaknaden av bestämmelser om en fyranivåindelning på en nationell nivå innebär problem främst i Sveriges relationer till andra länder och mellanfolkliga organisationer. Representanter från andra länder uttrycker ofta en osäkerhet inför att det i Sverige finns två

system för informationsklassificering som enbart beror på vid vilken myndighet informationen hanteras.

Skillnaden kan också göra det svårt för myndigheter m.fl. att bedöma hur den utländska säkerhetsklassificeringen ska förhålla sig till svenska säkerhetsskyddsbestämmelser. När svenska myndigheter i dag får handlingar med skyddsvärt innehåll från andra staters myndigheter eller mellanfolkliga organisationer har dessa handlingar normalt klassificerats enligt den fyragradiga skalan. Sverige förväntas av hänsyn till folkrättsliga förpliktelser hantera handlingarna på ett sätt som innebär att dessa skyddas i motsvarande mån eller åtminstone inte med ett sämre skydd.

Fördelar med fyra klassificeringsnivåer

Ett klassificeringssystem med fyra nivåer ger bättre förutsättningar att nyansera säkerhetsskyddet mera än vad två nivåer medger. Det medför också bättre förutsättningar att undvika ett för högt säkerhetsskydd för uppgifter som av en utländsk avsändare har klassificerats som *Confidential* och *Restricted* eller motsvarande beteckningar på andra språk. Ett klassificeringssystem som bygger på fyra nivåer kommer att medföra att en uppgift som i dag ges ett mer kostnadskrävande säkerhetsskydd än nödvändigt kan klassificeras på en lägre nivå och således ersättas av ett mindre kostsamt säkerhetsskydd.

Både EU[9] och Nato[10] samt en stor del av länderna i Europa och övriga världen använder i dag ett mer utvecklat nivåsystem än i Sverige med fyra klassificeringsnivåer inom såväl militär som civil verksamhet. Den omfattande internationella samverkan som i dag förekommer mellan Sverige och andra länder och mellanfolkliga organisationer har stor betydelse för frågan om hur säkerhetskänslig information bör klassificeras.

En viktig del av utredningens uppdrag är att bättre anpassa säkerhetsskyddslagen till de krav som det internationella arbetet ställer. En fördel med ett säkerhetsskydd som direkt sluter an till

[9] TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL,RESTRIENT UE/EU RESTRICTED.
[10] COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, NATO RESTRICTED.

de klassificeringsnivåer som andra staters myndigheter eller mellanfolkliga organisationer använder är att det underlättar det internationella samarbetet.

Nackdelar med fyra klassificeringsnivåer

En fyragradig indelning av säkerhetsskyddsklassificerade uppgifter är dock inte utan nackdelar. För det första innebär det för den som upprättar en handling som innehåller säkerhetsskyddsklassificerade uppgifter att det krävs en mer detaljerad kunskap om uppgifternas betydelse och deras potentiella skadeeffekt om de röjs, än om indelningen i stället skulle bestå av enbart två nivåer. Detta kräver kunskap och erfarenhet hos den som ska utföra klassificeringen. Det medför att myndigheter med en rådgivande och utbildande roll behöver utveckla stödverktyg och genomföra utbildning för de som i sitt arbete behöver göra sådan klassificering. En annan nackdel är att de två mellannivåerna i internationella regelverk och många nationella lagstiftningar är relativt likartade avseende de skyddsåtgärder som krävs. Det leder in på funderingar om dessa två nivåer skulle kunna slås samman till en.

I tre för Sverige relevanta samarbetsländer – Frankrike, Storbritannien och USA – finns ett nationellt system med enbart tre nivåer. Konstruktionen skiljer sig mellan dessa länder på ett sådant sätt att, något förenklat, Frankrike och USA har avskaffat den lägsta klassen, medan Storbritannien kan sägas ha en nivå i stället för de två mellannivåerna. Detta har medfört att dessa länder måste ha specialbestämmelser för att uppfylla kraven i t.ex. Natos säkerhetsbestämmelser.

Om man väger samman de nackdelar som följer av förslaget att införa fyra informationssäkerhetsklasser mot de fördelar som en fyranivåindelning innebär, talar betydelsen av den internationella anpassningen och möjligheten till nyansering i säkerhetsskyddet ändå för att en fyranivåindelning är det lämpligaste alternativet. Vi anser därför att ett system motsvarande det som används i många andra länder och inom EU och Nato med fyra klassificeringsnivåer ska införas i den nya lagstiftningen. Klassificeringen ska kopplas till vilken skada ett röjande kan innebära.

Fyra informationssäkerhetsklasser – ska svenska uttryck användas?

Vi föreslår alltså att säkerhetsskyddsklassificerade uppgifter ska delas in i fyra informationssäkerhetsklasser motsvarande de internationellt vedertagna klassificeringsnivåerna *Top Secret*, *Secret*, *Confidential* och *Restricted*. En fråga som uppkommer är hur dessa nivåer ska uttryckas i lagstiftningen. Tänkbara alternativ är klassificeringsnivåer på enbart svenska eller engelska eller en kombination av svenska och engelska.

Språklagen (2009:600) innehåller bl.a. bestämmelser om språkanvändning i offentlig verksamhet. Enligt språklagen har det allmänna ett särskilt ansvar för att svenskan används och utvecklas. I lagen slås fast att språket i domstolar, förvaltningsmyndigheter och andra organ som fullgör uppgifter i offentlig verksamhet är svenska.[11] Vidare framgår att myndigheter har ett särskilt ansvar för att svensk terminologi inom deras olika fackområden finns tillgänglig, används och utvecklas. Språklagens krav ska tillämpas så länge det inte finns tillräckligt starka skäl för undantag. Vi konstaterar att merparten av de länder och mellanfolkliga organisationer som använder sig av fyra säkerhetsskyddsklasser använder sig av beteckningar på det egna språket motsvarande de engelska uttrycken *Top Secret*, *Secret*, *Confidential* och *Restricted*. Detta gäller även för de länder som vi särskilt har studerat (se kapitel 8).

Ur språklig synvinkel finns flera tänkbara svenska beteckningar för de fyra föreslagna säkerhetsskyddsnivåerna. Vi anser att det är lämpligast med en anpassad svensk översättning av de engelska begreppen med inspiration hämtad från begreppens benämningar i Danmark, Finland och Norge. De svenska beteckningar som föreslås är, i fallande ordning, *kvalificerat hemlig*, *hemlig, konfidentiell* och *begränsad*.

Kan Försvarsmaktens system för informationsklassificering tjäna som modell?

Inom Försvarsmakten är informationssäkerhetsklass en beteckning på en uppgift som anger vilken förväntad skada eller vilket förväntat men som inträffar om uppgiften röjs. Informationssäkerhets-

[11] 10 § språklagen.

klassen har betydelse för hur uppgifterna ska hanteras för att ett adekvat säkerhetsskydd ska erhållas. En informationssäkerhetsklass anger således inte sekretessen för en uppgift eller en handling utan enbart hur uppgiften eller handlingen ska hanteras för att erhålla rätt skyddsnivå. Till informationssäkerhetsklasserna kopplas specifika åtgärder som också är anpassade till motsvarande lagstiftning i andra länder och till säkerhetsbestämmelser inom EU och Nato. Ett exempel är att en handling som är klassificerad som HEMLIG/TOP SECRET normalt ska förvaras i ett värdeskåp medan en handling på nivån HEMLIG/RESTRICTED kan förvaras i ett låst utrymme utan närmare kravspecificering. På detta sätt har det inom försvarssektorn åstadkommits en kravharmoni med utländska regelverk. Lösningen följer därmed Sveriges internationella säkerhetsskyddsåtaganden. Denna lösning lämpar sig därför som utgångspunkt för att införa fyra informationssäkerhetsklasser i en ny säkerhetsskyddslag.

De fyra informationssäkerhetsklasserna

Placeringen av uppgifter i informationssäkerhetsklass ska alltså styras av den skada för Sveriges säkerhet som kan uppstå om uppgifterna röjs. Placeringen genomförs därmed utifrån en hypotetisk skadebedömning. Där bedöms vilka konsekvenser ett eventuellt röjande av uppgifterna skulle kunna få för de särskilda skyddsintressena i säkerhetsskyddslagen. Genom att man på ett konkret sätt försöker klarlägga vilka konsekvenserna blir kommer det också tydligt att framgå vari skadan består. För att kunna placera en uppgift i rätt informationssäkerhetsklass är det viktigt att uppgiften bedöms på ett konkret och korrekt sätt. Detta kräver relevant sakkunskap av den som gör bedömningen.

I en handling förekommer ibland skyddsvärd information av varierande grad. I ett sådant fall ska det vara den uppgift som, om den röjs, orsakar störst skada som får styra handlingens placering i informationssäkerhetsklass. Om det är praktiskt av något skäl kan även olika delar av en handling ha olika klassificering, men det är fortfarande den högsta nivån som styr hur handlingen ska hanteras.

Ändamålet med indelningen i olika informationssäkerhetsklasser är främst att ge olika uppgifter ett balanserat säkerhetsskydd

med hänsyn till uppgifternas betydelse ur säkerhetssynpunkt. Klassificeringen ska inte göras i större utsträckning och med placering i högre klass än vad som är nödvändigt.

Kvalificerat hemlig

I denna informationssäkerhetsklass placeras uppgifter vars röjande kan medföra synnerligen allvarlig skada för Sveriges säkerhet. De befarade konsekvenserna ska vara synnerligen allvarliga utifrån skadans omfattning eller art och därigenom utgöra ett synnerligen allvarligt hot mot de särskilda skyddsintressen som omfattas av säkerhetsskyddslagen.

Hemlig

I denna informationssäkerhetsklass placeras uppgifter vars röjande kan medföra betydande skada för Sveriges säkerhet. De befarade konsekvenserna ska vara betydande utifrån skadans omfattning eller art och därigenom innebära ett allvarligt hot mot de särskilda skyddsintressen som omfattas av säkerhetsskyddslagen.

Konfidentiell

I denna informationssäkerhetsklass placeras uppgifter vars röjande kan medföra en inte obetydlig skada för Sveriges säkerhet. De befarade konsekvenserna ska inte vara obetydliga utifrån skadans omfattning eller art och därigenom kunna medföra ett hot, om än i begränsad omfattning, mot de särskilda skyddsintressen som omfattas av säkerhetsskyddslagen.

Begränsad

I denna informationssäkerhetsklass placeras uppgifter vars röjande kan medföra endast ringa skada för Sveriges säkerhet. De befarade konsekvenserna ska vara ringa utifrån skadans omfattning eller art och därigenom begränsade till att i mindre omfattning påverka, försvåra, hindra, undergräva, misskreditera eller störa verksamheten

för de särskilda skyddsintressen som omfattas av säkerhetsskyddslagen.

Uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande

Säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande ska även de, om de inte redan av annan stat eller mellanfolklig organisation har klassificerats, på motsvarande sätt delas in i informationssäkerhetsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation.

Normalt sett är säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande redan försedda med en märkning som motsvarar informationssäkerhetsklass i det upprättande landet eller i den mellanfolkliga organisationen. Ofta anges i det internationella säkerhetsskyddsåtagandet att märkningen är en förutsättning för ett åtagande för den mottagande parten att ge uppgifterna erforderligt säkerhetsskydd. Skälet till denna bestämmelse är att det är svårt för den mottagande parten att avgöra vilka skäl som ska ligga till grund för klassificeringen och vilken skada som kan uppkomma för den upprättande parten om uppgiften röjs. En gjord klassificering ska därför alltid godtas.

I vissa internationella samarbeten som t.ex. deltagande i internationella krishanteringsinsatser förekommer det dock att en svensk myndighet upprättar handlingar som innehåller uppgifter som träffas av ett internationellt säkerhetsskyddsåtagande. I dessa fall kan det bli aktuellt att göra en klassificering utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation. Det regelverk som är tillämpligt i det aktuella samarbetet kan utgöra ett stöd vid bedömningen.

Informationssäkerhetsklassernas betydelse för säkerhetsskyddsåtgärderna

Informationssäkerhetsklasserna har naturligtvis betydelse för utformningen av säkerhetsskyddsåtgärder inom informationssäkerheten men de är också av central betydelse för sådana säkerhetsskyddsåtgärder inom fysisk säkerhet och personalsäkerhet där konfidentialitetsaspekten av informationen är styrande. Grunden i ett nyanserat säkerhetsskydd är att en säkerhetsskyddsåtgärd ska vara tillräckligt omfattande – men inte mer – för att balansera den risk som åtgärden ska motverka.

För den del av säkerhetsskyddet som riktar sig mot säkerhetsskyddsklassificerade uppgifter står åtgärderna i direkt proportion mot informationssäkerhetsklassen. Det innebär t.ex. att placering av anställningar i säkerhetsklasser vid säkerhetsprövning som vi beskriver i avsnitt 18.5 i det avseendet utgår från den informationssäkerhetsklass som gäller för uppgifter som den prövade ska ta del av. Ett annat exempel är att styrkan i ett informationssystems säkerhetsfunktioner ska anpassas efter informationssäkerhetsklassen för de uppgifter som systemet ska kunna hantera.

Möjligheterna till nyansering av säkerhetsskyddet utifrån informationssäkerhetsklasserna kommer, åtminstone avseende informationssäkerhet och fysisk säkerhet, till uttryck främst i myndighetsföreskrifter.

15.4 Säkerhetsskyddets utformning och hänsynen till motstående allmänna och enskilda intressen

Förslag: Nuvarande bestämmelser i säkerhetsskyddslagen om att säkerhetsskyddet ska utformas med beaktande av enskildas rätt att enligt tryckfrihetsförordningen ta del av allmänna handlingar (5 § andra stycket) samt att tillträdesbegränsningar ska utformas så att den enskildes rätt att röra sig fritt inte inskränks mer än nödvändigt (10 § första stycket) tas bort.

I stället ska det i en ny lag finnas en generell bestämmelse om att säkerhetsskyddsåtgärderna så långt det är möjligt ska utformas så att de inte medför skada eller annan olägenhet för andra allmänna eller enskilda intressen.

Allmänna utgångspunkter

I säkerhetsskyddslagen finns det bestämmelser som behandlar förhållandet till motstående intressen. Bestämmelserna anger att säkerhetsskyddet ska utformas med beaktande av enskildas rätt att enligt tryckfrihetsförordningen ta del av allmänna handlingar samt att tillträdesbegränsningar ska utformas så att den enskildes rätt att röra sig fritt inte inskränks mer än nödvändigt.

Vår uppfattning är att bestämmelserna i sin nuvarande utformning leder tankarna fel. Det finns enligt oss inte några möjligheter att säkerhetsskyddsåtgärder, varken rättsligt eller faktiskt, i sig skulle kunna innebära inskränkningar i rätten att ta del av allmänna handlingar eller rätten att röra sig fritt här i landet. Denna typ av inskränkningar finns i annan lagstiftning där inskränkningen noggrant har avvägts mot motstående intressen. Offentlighets- och sekretesslagen (2009:400), OSL, och skyddslagen (2010:305) är exempel på sådana lagar.

Nedan redogör vi för hur vi ser på förhållandet mellan sekretess och informationssäkerhetsklasserna och senare förhållandet mellan fysisk säkerhet och rätten att röra sig fritt.

Frågan om restriktivitet när det gäller beslut om inplacering i säkerhetsklass behandlas vidare i avsnitt 18.8.

Förhållande mellan informationssäkerhetsklasserna och offentlighets- och sekretesslagen

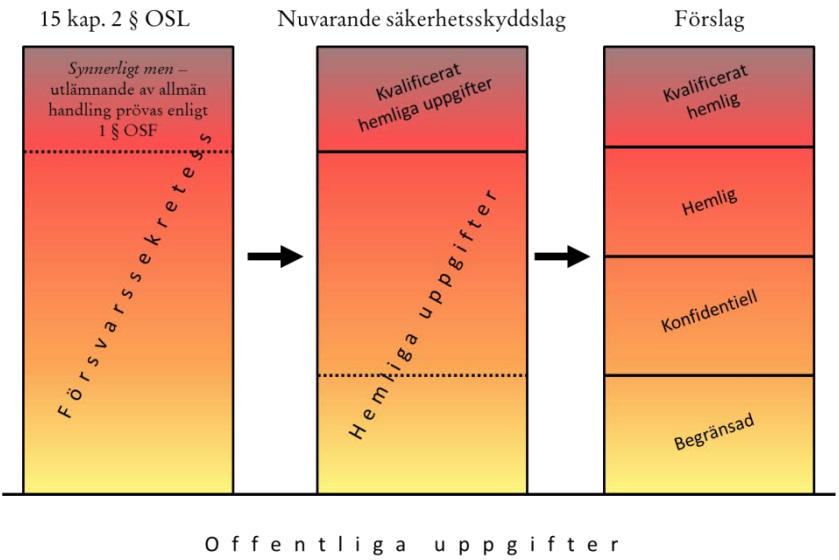
Som vi tidigare redogjort för innebär säkerhetsskyddsklassificerade uppgifter sådana uppgifter som rör säkerhetskänslig verksamhet och av den anledningen omfattas av sekretess enligt offentlighets- och sekretesslagen eller skulle ha omfattats av sekretess, om uppgiften i stället förekommit i en verksamhet där bestämmelser om sekretess i offentlighets- och sekretesslagen gäller.

Det innebär att de fyra informationssäkerhetsklasserna inte utvidgar sekretessen eller inskränker tryckfrihetsförordningens bestämmelser om offentlighet för allmänna handlingar. Detta får i sin tur två viktiga följder. För det första kan offentliga uppgifter aldrig placeras i informationssäkerhetsklass. För det andra inryms hela fyranivåindelningen inom de relevanta sekretessbestämmelsernas skaderekvisit. Det innebär att det är det skaderekvisit som

ställs upp i de aktuella sekretessbestämmelserna som delas in i fyra skadenivåer.

För att belysa detta med ett exempel utgår vi från att en myndighet har en uppgift som är av betydelse för Sveriges säkerhet som om den röjs kan orsaka en ringa skada för landets försvar. Genom att uppgiften kan orsaka skada för landets försvar omfattas den av sekretess enligt 15 kap. 2 § OSL. Genom att den är av betydelse för Sveriges säkerhet uppfyller den kraven för en säkerhetsskyddsklassificerad uppgift som ska placeras i informationssäkerhetsklass. På grund av att den skada som kan uppkomma vid ett röjande av denna uppgift enbart är ringa ska uppgiften placeras i informationssäkerhetsklassen begränsad. I detta exempel är det viktigt att poängtera att, om skadan är så pass ringa att uppgiften inte ens omfattats av sekretess, så utgör heller inte uppgiften en säkerhetsskyddsklassificerad uppgift.

Fig. 1 **Principskiss över förhållandet mellan offentlighets- och sekretesslagen, nuvarande säkerhetsskyddslag och informationssäkerhetsklasserna**



Källa: utredningens figur

Ovanstående figur visar förhållandet mellan offentlighets- och sekretesslagen, nuvarande säkerhetsskyddslag och vårt förslag till ny säkerhetsskyddslag. De tonade staplarna visar att de uppgifter

som omfattas av sekretess enligt i detta fall 15 kap. 2 § OSL (försvarssekretess) inte påverkas i vårt förslag om informationssäkerhetsklasser. Staplarna visar även att de uppgifter som ska ges ett skydd med nuvarande säkerhetsskyddslag, ska skyddas i en ny lag i precis samma omfattning som i dag. Skillnaden är att den tydligare indelningen i fyra informationssäkerhetsklasser medger en nyansering i säkerhetsskyddet som korresponderar mot den skada som ett obehörigt röjande av en uppgift innebär. Uppgifter under staplarna är offentliga.

Förhållande mellan fysisk säkerhet och rätten att röra sig fritt

Bestämmelser om förbud för åtgärder som begränsar rörelsefrihet och innebär andra begränsningar i enskildas grundlagsfästa fri- och rättigheter finns i 2 kap. regeringsformen. Sådana begränsningar kan bara göras genom lag och ska tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningar får förekomma endast i den mån de är nödvändiga med hänsyn till ändamålet och får inte sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen (2 kap. 12 § andra stycket regeringsformen).

När det gäller rätten att röra sig fritt i landet och allemansrättens möjligheter att ha tillgång till naturen regleras detta i 2 kap. 8 och 15 §§ regeringsformen.

Rätten att röra sig fritt är dock inte oinskränkt. Det finns inte någon generell rätt att fritt bereda sig tillträde till byggnader, anläggningar och installationer i allmän eller enskild ägo. Vidare finns det lagstiftning som på olika sätt ytterligare begränsar rätten att röra sig fritt och allemansrättens räckvidd. Skyddslagen är en sådan lag. Den har ett skyddsändamål som delvis överensstämmer med säkerhetsskyddslagens och den innehåller bestämmelser om bl.a. tillträdesförbud. Skyddslagen beskrivs närmare i avsnitt 4.3.

Säkerhetsskyddsåtgärden fysisk säkerhet har inte någon självständig betydelse i det avseendet att den i sig innebär en inskränkning i grundlagsskyddade rättigheter, utan åtgärden handlar om att bl.a. förhindra ett obehörigt tillträde där detta har sin grund i annan lagstiftning, t.ex. skyddslagen. Sådana åtgärder kan vara perimeterskydd i form av stängsel eller andra åtgärder som personell eller teknisk bevakning.

Att i en säkerhetsskyddslag ha en hänvisning till att fysisk säkerhet inte ska utformas så att den enskildes rätt att röra sig fritt inte inskränks mer än nödvändigt leder därmed tankarna fel, eftersom det enligt vår uppfattning inte är möjligt att utforma den fysiska säkerheten på ett sådant sätt.

En sådan bestämmelse fyller dock ett syfte i skyddslagen där ett sådant övervägande behövs när en byggnad, anläggning eller ett område ska bli ett skyddsobjekt enligt ett beslut enligt lagen. En sådan bestämmelse finns i 18 § andra stycket skyddslagen.

En ny mer ändamålsenlig bestämmelse

Med anledning av det som redovisats om säkerhetsskyddets förhållande till grundlagsskyddade fri- och rättigheter föreslår vi att de nuvarande bestämmelserna på detta område i säkerhetsskyddslagen ersätts med en bestämmelse om att säkerhetsskyddet så långt det är möjligt ska utformas så att det inte medför skada eller annan olägenhet för andra allmänna eller enskilda intressen.

Ett sådant mera allmänt hållet åliggande anser vi svarar bättre mot det faktiska behovet när det gäller avvägning av säkerhetsskyddets utformning. En sådan bestämmelse tar på ett tydligare sätt sikte på att bl.a. motverka effektivitetförluster och onödiga kostnader som kan uppkomma till följd av ett obalanserat säkerhetsskydd i såväl allmän som enskild verksamhet. Angående säkerhetsskyddsåtgärder och skyddet av den personliga integriteten se också vårt förslag i avsnitt 18.8.

16 Informationssäkerhet

Information är en central resurs i många verksamheter och så även i verksamheter som är av betydelse för Sveriges säkerhet. Våra direktiv beskriver utvecklingen på informationsområdet sedan nuvarande säkerhetsskyddslag trädde i kraft på följande sätt:

> Sedan säkerhetsskyddslagen trädde i kraft 1996 har informationstekniken och användningen av den genomgått en betydande utveckling. Bland annat internet, som fick sitt egentliga genomslag i mitten på 1990-talet, har i grunden förändrat förutsättningarna för informationssäkerhetsarbetet. Mycket stora informationsmängder, såväl öppen som hemlig, hanteras i it-system. En rad verksamheter, både hos det allmänna och inom näringslivet, är helt beroende av digitala system för bl.a. styrning, reglering och övervakning. Även internationaliseringen har påverkat förutsättningarna för informationssäkerheten. Det gäller exempelvis i samband med utflyttning av verksamhet till utlandet, bl.a. inom energiförsörjningen.

Vi har i avsnitt 9.3.1 redogjort för de förändringsfaktorer avseende utvecklingen på informationsområdet som bör påverka utformningen av en ny säkerhetsskyddslag. I detta kapitel anger vi i avsnitt 16.1 syftet med informationssäkerheten i en ny säkerhetsskyddslag. I avsnitt 16.2 tar vi upp begrepp och benämningar inom området informationssäkerhet. Som vi har beskrivit i kapitel 10 behöver lagen utvecklas från att nästan uteslutande ha varit inriktad på konfidentialiteten för sekretessbelagd information till att ge ett skydd för viss information på ett sådant sätt att brister i antingen konfidentialiteten, tillgängligheten eller riktigheten (eller kombinationer av dessa) motverkas. I avsnitt 16.3 redogör vi för vad som fortsättningsvis bör gälla för behörighet till och delgivning av säkerhetsskyddsklassificerade uppgifter. Slutligen beskriver vi i avsnitt 16.4 vilka säkerhetsskyddsåtgärder som kan vara aktuella för att skydda information med fokus på de åtgärder som bör regleras i förordningsform.

16.1 Vad ska informationssäkerhet syfta till?

Förslag: Syftet med säkerhetsskyddsåtgärden *informationssäkerhet* ska anges vara att förebygga dels att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, dels skadlig inverkan på andra informationstillgångar som avser säkerhetskänslig verksamhet.

I nuvarande säkerhetsskyddslag definieras informationssäkerhet som en säkerhetsskyddsåtgärd för att förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs.

Som vi har beskrivit tidigare är detta alltför snävt med hänsyn till det skyddsbehov som finns för informationstillgångar vars riktighet och tillgänglighet är av betydelse för säkerhetskänslig verksamhet. Det är inte säkert att denna typ av information omfattas av sekretess – tvärtom är fallet snarare det motsatta. Ett exempel på säkerhetskänslig information som normalt inte omfattas av sekretess är driftsinformation för energidistribution. Säkerhetskänsliga informationstillgångar bör därför ges ett skydd oavsett om informationen i dessa omfattas av någon form av sekretess eller inte.

Vi föreslår därför att säkerhetsskyddsåtgärden informationssäkerhet delas upp i två delmoment. Det första tar sikte på skyddet av säkerhetsskyddsklassificerade uppgifter från det perspektivet att åtgärderna ska förebygga att uppgifterna röjs, ändras, görs otillgängliga eller förstörs. I informationssäkerhetssammanhang brukar man tala om skydd för konfidentialitet, riktighet och tillgänglighet. I denna del är det konfidentialitetsperspektivet som är det framträdande.

I det andra momentet anges att åtgärderna ska förebygga skadlig påverkan på informationstillgångar som *annars* är av betydelse för säkerhetskänslig verksamhet. I detta fall är det därför enbart riktighets- och tillgänglighetshänsyn som gör sig gällande.

Med informationstillgångar avses information och informationssystem i vid bemärkelse, dvs. uppgifter, handlingar och tekniska system som används för att i olika avseenden elektroniskt kommunicera och i övrigt behandla uppgifter. Observera att begreppet har en delvis annan och mer långtgående betydelse i den

internationella standarden för ledning av informationssäkerhet (LIS) där även människor ingår i begreppet.

Sammanfattningsvis syftar informationssäkerheten till att tillgodose

- att informationen finns tillgänglig när den behövs,
- att informationen är och förblir riktig,
- att informationen är tillgänglig för endast dem som är behöriga att ta del av den, samt
- att hanteringen av informationen är spårbar.

Den första punkten (tillgänglighet) innebär att informationen ska kunna utnyttjas i förväntad utsträckning och inom önskad tid. Den andra punkten (riktighet) innebär att informationens värde eller innebörd över tiden ska överensstämma med det som informationen är avsedd att avspegla. Den tredje punkten (konfidentialitet/hemlighållande) innebär att endast de som är behöriga ska få ta del av informationen. Den fjärde punkten (spårbarhet) innebär att det ska vara möjligt att i efterhand härleda hur informationen har hanterats, t.ex. vem som har läst en viss uppgift och när läsningen ägde rum.

Dessa fyra aspekter på informationssäkerheten beskrivs i det följande.

Konfidentialitet

Konfidentialitet för uppgifter av betydelse för rikets säkerhet är den bärande principen i nuvarande säkerhetsskyddslagstiftning. Konfidentialitetsaspekten innebär att uppgifter som, om de röjs för obehöriga, kan medföra en skada behöver ett skydd mot ett sådant röjande. I det allmännas verksamhet är konfidentialietsfrågan nära sammanlänkad med bestämmelserna om sekretess i offentlighets- och sekretesslagen (2009:400), OSL, och en materiell bestämmelse om sekretess är också en förutsättning för att på ett meningsfullt sätt vidta åtgärder för att förhindra ett obehörigt röjande av en uppgift.

Konfidentialitetsaspekten har även i vårt förslag till ny säkerhetsskyddslag och säkerhetsskyddsförordning en framträdande position, även om skyddsåtgärderna föreslås omfatta även

riktighets- och tillgänglighetskrav. Det förhållandet beror främst på att säkerhetsskyddsåtgärderna som tar sikte på konfidentialiteten är mer detaljerade och konkreta än beskrivningen av säkerhetsskyddsåtgärder avseende driftsäkerhet, dvs. för att säkerställa riktighet och tillgänglighet. Det beror i sin tur på att åtgärderna i den delen utgår från bl.a. de fyra informationssäkerhetsklasserna och därmed sammanhängande krav i internationella säkerhetsskyddsåtaganden.

Riktighet och tillgänglighet

Riktighets- och tillgänglighetsaspekter kan förekomma i säkerhetskänslig verksamhet där brister i informationens riktighet eller tillgänglighet kan få allvarliga konsekvenser, även om uppgifterna inte omfattas av sekretess. Exempel på detta finns t.ex. i system för styrning och reglering inom energisektorn samt inom verksamhetsområdet telekommunikation. Vi föreslår att informationssäkerheten ska förebygga skadlig inverkan på sådana uppgifter. Riktigheten innebär att informationens värde (t.ex. siffror) eller innebörd (t.ex. ord) över tiden ska överensstämma med det som informationen är avsedd att avspegla. Informationen ska därmed inte obehörigen kunna ändras.

Tillgänglighet innebär att informationen ska kunna utnyttjas i förväntad utsträckning och inom önskad tid. Detta kan uttryckas som att informationen ska ha ett skydd mot att den obehörigen görs otillgänglig eller förstörs.

I dessa fall handlar det inte om att ge informationen ett skydd mot röjande utan snarare att åstadkomma en robusthet i system utifrån de krav på riktighet och tillgänglighet som finns i en verksamhet. Riktighets- och tillgänglighetskrav är svårare att indela i nivåer än när det gäller konfidentialitetskrav. Detta på grund av att kraven kan vara mycket varierande i olika verksamheter och system och svårare att uttrycka i generella termer.

Spårbarhet

Spårbarhet innebär att det ska vara möjligt att i efterhand härleda hur informationen har hanterats, t.ex. vem som har tagit del av en viss uppgift eller ändrat denna och när delgivningen eller ändringen

ägde rum. Spårbarheten är viktigt för att kunna indikera säkerhetshot och incidenter i system.

16.2 Begrepp och benämningar

16.2.1 Informationssäkerhet

Förslag: I avsnitt 15.1 har vi föreslagit att *informationssäkerhet* kvarstår som begrepp i en ny säkerhetsskyddslag. Det finns anledning att utveckla innebörden av det begreppet.

Termen *informationssäkerhet* infördes i 1996 års lagstiftning som en ersättning till det tidigare begreppet *sekretesskydd*. I dag är termen informationssäkerhet allmänt spridd och accepterad, och den används inom skilda verksamheter där kraven och behoven av skydd skiljer sig åt. Termen träffar därför skyddet av olika slag av information hos såväl enskilda som vid myndigheter.

Åtgärder som är förknippade med informationssäkerheten enligt säkerhetsskyddslagen kan inte särskiljas från informationssäkerhet i en vidare bemärkelse. Exempel på detta är skydd mot skadlig kod och användarautentisering som är relevanta åtgärder även för it-system som inte är av betydelse för Sveriges säkerhet. Föreskrifter som meddelas med stöd av lagstiftningen, måste kunna avse informationssäkerheten i stort för de verksamheter som omfattas av säkerhetsskyddslagens krav. Detsamma gäller för tillsyn. En helhetssyn krävs inom detta område och såväl föreskrifter som tillsyn måste kunna omfatta samtliga de relevanta åtgärder som syftar till att ge ett skydd för information.

16.2.2 Informationssäkerhetens beståndsdelar

Informationssäkerhet innebär åtgärder av olika slag för att skydda information som är av betydelse för säkerhetskänslig verksamhet. Sådan information förekommer i olika miljöer och verksamheter och hanteras och används på flera olika sätt. Därför måste säkerhetsskyddsåtgärderna anpassas för att passa för dessa skiftande förutsättningar. Uppgifternas form saknar i sammanhanget betydelse och åtgärderna måste avse såväl uppgifter på papper som

elektroniskt lagrade och kommunicerade uppgifter samt uppgifter som kan läsas ut ur t.ex. bilder eller materiel. Ett angreppssätt är att beskriva informationens livscykel från det att den skapas till det att den upphör eller förstörs och att utifrån denna beskrivning identifiera moment som har betydelse för säkerheten. Dessa moment i informationshanteringen kan skyddas genom administrativa, fysiska eller tekniska säkerhetsskyddsåtgärder eller genom en kombination av dessa. Detta kan illustreras med åtgärden kopiering av säkerhetsskyddsklassificerade handlingar som bör omfattas av såväl administrativa rutiner om hur kopiering får ske som tekniska säkerhetsskyddskrav på lagringsmedia i kopiatorn.

Huvuddelen av dessa åtgärder är av sådan karaktär att de även fortsättningsvis bör kunna beskrivas i tillämpningsföreskrifter. Vissa bestämmelser bör dock meddelas i förordning, eftersom de rör bl.a. förhållandet mellan förvaltningsmyndigheter. Dessa åtgärder beskrivs närmare i avsnitt 16.4.

För att beskriva åtgärdernas karaktär kan de indelas i tre kategorier – administrativ informationssäkerhet, it-säkerhet och kommunikationssäkerhet. Indelningen följer i princip Rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter.[1] Syftet med denna kategorisering är dels att åtgärderna riktar sig mot olika målgrupper, dels att genomförandet av åtgärderna kräver olika typer av kompetens.

Administrativ informationssäkerhet

Till de administrativa informationssäkerhetsåtgärderna hör åtgärder som tar sikte på rutiner, arbetsflöden och arbetsledning. Här kan nämnas bestämmelser om registrering, distribution, kopiering, kvittering och inventering av handlingar som innehåller säkerhetsskyddsklassificerade uppgifter. Ett exempel på en sådan bestämmelse är att handlingar som placerats i informationssäkerhetsklass *konfidentiell* eller högre ska kvitteras av den som tar del av handlingen. En för säkerhetsskyddet central fråga är reglerna om behörighet till säkerhetsskyddsklassificerade uppgifter. Behörighetskriteriet i nuvarande säkerhetsskyddsförordning som innebär att en

[1] Rådets beslut av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2013/488/EU).

person för att vara behörig till hemliga uppgifter ska vara pålitlig från ett säkerhetsperspektiv, ha relevanta kunskaper om säkerhetsskyddet och ha behov av uppgifterna för sin tjänst eller för sitt uppdrag är också en bestämmelse som hör till denna kategori.

It-säkerhet

It-säkerheten innefattar såväl rutiner och handhavanden i och kring informationssystem som tekniska krav på säkerhetsfunktioner i systemen och dess komponenter. För att framför allt säkerställa att tillgängligheten är i enlighet med verksamhetens krav bör alla it-system som används i säkerhetskänslig verksamhet vara föremål för kontinuitetsplanering. Även säkerhetskopiering är en viktig åtgärd som ger ett skydd i termer kring tillgänglighet och riktighet. Till it-säkerheten hör även bestämmelser som rör krav på säkerhetsgodkännande av it-system inför driftsättning.[2] Ett exempel på en säkerhetsskyddsbestämmelse inom it-säkerheten är att lagringsmedia som innehåller säkerhetsklassificerade uppgifter ska förvaras och hanteras på samma sätt som säkerhetsskyddsklassificerade handlingar. Åtgärder som behörighetskontroll och skydd mot obehörig avlyssning är viktiga beståndsdelar av it-säkerheten.

Kommunikationssäkerhet

I dag används termen *signalskydd* för att beskriva det i huvudsak kryptografiska skyddet för information i s.k. signalskyddssystem. Termen leder dock tankarna till en tid då analoga signaler kommunicerades i sambandssystem i form av tal eller telegrafi. Bestämmelser om signalskydd och kryptografiska funktioner förekommer i dag i flera olika författningar. I 3 b § förordningen (2007:1266) med instruktion för Försvarsmakten framgår att Försvarsmakten ska leda och bedriva militär säkerhetstjänst, leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information samt biträda Regeringskansliet i frågor som rör kryptoverksamhet och

[2] 12 § tredje stycket säkerhetsskyddsförordningen.

annan signalskyddsverksamhet. I regleringsbrevet till Försvarsmakten[3] anges att signalskyddet är en ”säkerhetsskydds-angelägenhet”. Genom lydelsen i instruktionen verkar signalskydds-tjänsten vara skild från militär säkerhetstjänst vilket sannolikt inte är avsett. I regleringsbrevet framgår i stället att den militära säkerhetstjänsten består av säkerhetsunderrättelsetjänst, säkerhets-skyddstjänst och signalskyddstjänst. Begreppens inbördes ordning är därmed inte helt tydlig.

Begreppet kommunikationssäkerhet[4] är därför bättre och beskriver på ett bättre sätt vad funktionen avser. Kommunikations-säkerhet syftar i huvudsak till att förhindra eller försvåra avlyssning eller obehörig påverkan av information i kommunikationssystem. Det kryptografiska skyddet har en central roll i kommunikations-säkerheten, och det särskilda kompetensområde som kryptografin tillhör är i sig en för Sverige skyddsvärd strategisk förmåga. Ett exempel på en bestämmelse som tar sikte på kryptografiska funk-tioner är att enbart kommunikationssäkerhetssystem som är god-kända av Försvarsmakten får användas för kommunikation av säkerhetsskyddsklassificerade uppgifter. Kryptografiska funktioner kan användas för även andra säkerhetshöjande åtgärder som identi-fiering, autentisering, signering och verifiering utan att vara en del av kommunikationssäkerheten.

När det gäller regleringen kring signalskydd anser vi att den frå-gan bör utredas vidare och vi lämnar inte några förslag som innebär att begreppet ta bort. Det som ryms inom begreppet i dag sam-manfaller dock med det som en ny säkerhetsskyddslag omfattar. Signalskyddet i sin nuvarande utformning är därmed en del av informationssäkerheten i vårt förslag till säkerhetsskyddslag.

Vi tar dock ett första steg genom att föreslå att Försvarsmak-tens rätt att meddela föreskrifter om signalskyddstjänsten flyttas till säkerhetsskyddsförordningen och omformuleras så att den avser en möjlighet för Försvarsmakten att meddela närmare före-skrifter om verkställigheten av säkerhetsskyddslagen i fråga om kryptografiska funktioner. Detta innefattar såväl kryptografiska funktioner i kommunikationssäkerhet som i annan tillämpning.

[3] Regeringsbeslut 10, bilaga 5, 2013-12-19, Fö2012/2150/MFU (delvis), Fö2013/110/MFI, Fö2013/123/ESL (delvis) m.fl.
[4] Detta motsvarar även den engelska termen *Communication Security* eller förkortat *Comsec*.

16.3 Behörighet och delgivning

Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter

Kriterierna för behörighet till *hemliga uppgifter* regleras i dag i 7 § säkerhetsskyddsförordningen. Dessa innebär att en person ska vara pålitlig från säkerhetssynpunkt, ha kunskap om säkerhetsskyddet och ha behov av uppgifterna för sitt arbete för att en delgivning ska vara tillåten. Kravet på pålitlighet från säkerhetssynpunkt korresponderar mot bestämmelserna om säkerhetsprövning.

Kriterierna motsvarar de som gäller i många andra länder och i mellanfolkliga organisationers säkerhetsbestämmelser och vi ser inte något behov av att ändra dessa kriterier.

Behörigheten till säkerhetsskyddsklassificerade uppgifter styrs av den verksamhet som uppgifterna förekommer i, vilket sammanhänger med att det enbart är i verksamheten som det kan avgöras om en person behöver uppgifterna för sitt arbete. Ett system där en verksamhet styr över behörigheten hos personer i en annan verksamhet torde vara främmande när det gäller relationen mellan fristående myndigheter. I förhållandet mellan myndigheter och leverantörer finns det dock ett stort utrymme för en myndighet att inom ramen för ett uppdrag styra vilka personer hos leverantören som ska ha behörighet till uppgifterna.

I avsnitt 20.4 behandlar vi frågan om s.k. säkerhetsintyg för person som upprättas av en svensk myndighet och innebörden av dessa intyg när det gäller möjligheter för bosatta i Sverige att under vissa förutsättningar kunna delta i det som närmast motsvaras av säkerhetskänslig verksamhet i andra länder eller vid mellanfolkliga organisationer. När det gäller det omvända förhållandet, att utländska medborgare ska delta i säkerhetskänslig verksamhet i Sverige, ska behörighetskriterierna även i dessa fall vara uppfyllda. När det gäller pålitlighetskravet kan detta vara uppfyllt på två sätt – dels genom att en säkerhetsprövning enligt säkerhetsskyddslagen är genomförd, dels genom att en utländsk myndighet eller en mellanfolklig organisation har upprättat ett säkerhetsintyg för den aktuella personen och intyget gäller för den informationssäkerhetsklass som är nödvändig i det specifika fallet. I det sistnämnda alternativet bör en säkerhetsskyddsöverenskommelse med det aktuella landet eller den mellanfolkliga organisationen vara en förutsättning för att ett säkerhetsintyg ska godtas. Skälet till detta är att landets eller organisationens rutiner för prövning av personer från

säkerhetssynpunkt bör vara kända och motsvara det som gäller i Sverige.

I kapitel 20 återkommer vi till frågan om internationella samverkansformer avseende bl.a. säkerhetsintyg.

Sekretess- och tystnadspliktsbevis

I avsnitt 15.3 har vi redogjort för hur sekretessen förhåller sig till säkerhetsskyddsklassificerade uppgifter och att det senare begreppet bygger på att antingen sekretess gäller för uppgifterna eller att dessa skulle ha omfattats av sekretess om uppgifterna i stället förekommit i en verksamhet där bestämmelser om sekretess i offentlighets- och sekretesslagen gäller. Syftet med den föreslagna definitionen är att en uppgift ska vara en säkerhetsskyddsklassificerad uppgift om kriterierna är uppfyllda oberoende av i vilken verksamhet uppgifterna hanteras (se avsnitt 12.2). I avsnitt 22.1 behandlar vi frågan om tystnadsplikt för sådana uppgifter.

Den som tillåts ta del av säkerhetsskyddsklassificerade uppgifter ska upplysas om räckvidden och innebörden av sekretessen eller av tystnadsplikten. Räckvidden av meddelarfriheten och begränsningar i denna, samt en erinran om att ett straffrättsligt ansvar under vissa omständigheter kan uppkomma om uppgifterna röjs för obehöriga, bör ingå i en sådan upplysning.

Sekretessens och tystnadspliktens giltighet är emellertid inte beroende av ett sekretessbevis eller en tystnadspliktsförbindelse. Förbindelsen eller beviset kan nämligen aldrig få någon annan betydelse än att utgöra en bekräftelse på att en person har erinrats om tystnadsplikt och aktuella säkerhetsbestämmelser. Handlingarnas huvudsakliga rättsliga funktion är att i en rättegång eller i ett disciplinärt förfarande tjäna som bevis för att personen har förstått eller bort förstå att han eller hon bröt mot sin tystnadsplikt.

Skyddet när säkerhetsskyddsklassificerade uppgifter lämnas ut till en utländsk myndighet eller mellanfolklig organisation

Säkerhetsskyddsklassificerade uppgifter från Sverige kan lämnas ut till andra länders myndigheter och mellanfolkliga organisationer. I säkerhetsskyddslagen finns det inte några bestämmelser som direkt tar sikte på ett sådant informationsutbyte, även om vissa bestäm-

melser antyder att detta kan vara möjligt. Ett exempel är bestämmelsen i 11 § säkerhetsskyddsförordningen som handlar om anlitande av Utrikesdepartementets kurirförbindelser för försändelser till utlandet.

Det finns författningsbestämmelser som reglerar när uppgifter som omfattas av sekretess får delges utländska myndigheter och mellanfolkliga organisationer. Två sådana bestämmelser är av betydelse i sammanhanget. Den första är 8 kap. 3 § OSL som ger två alternativa möjligheter till sådant utlämnande. Det första fallet är när en föreskrift i lag eller förordning tillåter att uppgifter som omfattas av sekretess lämnas ut. I det andra fallet är ett utlämnande tillåtet när ett sådant hade varit tillåtet till en motsvarande svensk myndighet och det dessutom enligt den utlämnande myndigheten står klart att det ligger i svenskt intresse att uppgiften delges.

Den andra bestämmelsen finns i förordningen (2010:649) om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet. Förordningen gäller för tre myndigheter – Försvarsmakten, Försvarets materielverk och Totalförsvarets forskningsinstitut. Enligt bestämmelsen får en uppgift för vilken sekretess gäller enligt 15 kap. 2 § OSL (försvarssekretessen) lämnas ut till en utländsk myndighet som deltar i ett samarbete inom Försvarsdepartementets verksamhetsområde. I bestämmelsen finns en begränsning som ställer krav på att utlämnandet enligt den utlämnande myndighetens prövning är nödvändigt för att kunna genomföra samarbetet. Vidare får uppgifter som är av synnerlig betydelse för rikets säkerhet eller som kan ge underlag för utveckling av motmedel mot Sveriges försvarssystem inte lämnas ut.

I författningstexten används skrivningen *lämnas ut* men det är inte frågan om ett sådant utlämnande som avses i tryckfrihetsförordningen, dvs. att uppgifterna blir offentliga.

Det finns inte några bestämmelser som tar sikte på vilka krav som kan ställas på mottagaren när det gäller skyddet av uppgifterna som delges. En viktig princip är att skyddet ska vara detsamma oavsett i vilken verksamhet den säkerhetsskyddsklassificerade uppgiften hanteras. Avsaknaden av krav på säkerhetsskydd för uppgifter som delges till bl.a. utländska myndigheter är därför otillfredsställande.

I avsnitt 6.1 har vi beskrivit möjligheten för två länder att ömsesidigt överenskomma om säkerhetsskydd för varandras säkerhets-

skyddsklassificerade uppgifter. Ett sådant internationellt säkerhetsskyddsåtagande binder inte enbart Sverige att ge ett säkerhetsskydd för den andra partens klassificerade uppgifter utan även det motsatta förhållandet. Av det följer att i de fall där det finns sådana överenskommelser har de säkerhetsskyddsklassificerade uppgifter som delges ett betydligt bättre skydd än i de fall där en sådan säkerhetsskyddsöverenskommelse saknas. Vi föreslår därför en bestämmelse i säkerhetsskyddsförordningen som anger att säkerhetsskyddsklassificerade uppgifter som lämnas ut till en utländsk myndighet eller mellanfolklig organisation ska omfattas av ett internationellt säkerhetsskyddsåtagande hos den mottagande myndigheten eller organisationen. En sådan bestämmelse finns även i många andra länder. Det är den utlämnande myndigheten som ska säkerställa att det finns en giltig överenskommelse. Det förutsätts därvid att överenskommelsen är av sådan karaktär att den är folkrättsligt bindande för parterna, dvs. utgör ett traktat i Wienkonventionens mening.[5] Andra typer av överenskommelser som s.k. *Memorandum of Understanding* (MoU) eller projektsäkerhetsavtal är inte tillräckliga. De binder i bästa fall enbart vissa myndigheter hos parterna. Det skydd som följer av sådana överenskommelser är dessutom ofta svagt och underordnat nationell lagstiftning.

Sverige har i dag internationella säkerhetsskyddsöverenskommelser med ett 30-tal länder och mellanfolkliga organisationer, vilket omfattar den absoluta huvuddelen av de länder som vi utbyter skyddsvärda uppgifter med. Nya överenskommelser tillkommer efterhand som behoven uppstår och det pågår ett kontinuerligt arbete med att omförhandla äldre överenskommelser och att förhandla nya. Det kan emellertid undantagsvis uppstå en situation där det finns ett behov av att kunna delge säkerhetsskyddsklassificerade uppgifter till ett annat land även om det inte finns en giltig överenskommelse om säkerhetsskydd. I de fall där det finns särskilda skäl som motiverar att risken för de säkerhetsskyddsklassificerade uppgifterna får stå tillbaka för andra tungt vägande intressen bör det finnas en möjlighet att besluta om undantag från kravet på en säkerhetsskyddsöverenskommelse. Ett sådant fall kan vara när ett för Sverige viktigt internationellt samarbete måste

[5] Wienkonventionen om traktaträtten mellan stater och internationella organisationer eller internationella organisationer sinsemellan av den 21 mars 1986.

påbörjas innan en förhandling om en säkerhetsskyddsöverenskommelse med det aktuella landet har avslutats. Bestämmelsen ska därför kompletteras med en sådan möjlighet. Bestämmelsen kompletteras även med en upplysningshänvisning till ovan nämnda bestämmelser om när uppgifter som omfattas av sekretess får delges till en utländsk myndighet. I en övergångsbestämmelse bör därutöver anges att kravet gäller fullt ut först efter en övergångsperiod.

16.4 Åtgärder inom informationssäkerheten

Anteckning om informationssäkerhetsklass

Krav bör ställas på att en säkerhetsskyddsklassificerad handling märks så att det framgår vilken högsta informationssäkerhetsklass uppgifter i handlingen har. Märkningen gör det tydligt för den som hanterar handlingen vilka krav på säkerhetsskydd som gäller. En bestämmelse om märkning bör finnas i säkerhetsskyddsförordningen. Kravet på märkning gäller oberoende av handlingens form och täcker därför även t.ex. lagringsmedia och handlingar i elektroniskt format. För att kravet inte ska bli onödigt betungande bör handlingar som är arkiverade undantas och i fråga om andra handlingar som redan är märkta bör kravet gälla först efter en övergångsperiod.

Om en säkerhetsskyddsklassificerad handling kan antas komma att lämnas över till utländska myndigheter eller leverantörer, ska den även förses med en markering om ursprungsland. Det finns dock inget som hindrar att en myndighet förser samtliga säkerhetsskyddsklassificerade handlingar med anteckning om ursprungsland eller kompletterar anteckningen med särskilda behörighetsrestriktioner.

I 5 kap. 5 § OSL finns det bestämmelser om s.k. sekretessmarkering. Anteckningen om informationssäkerhetsklass utgör inte en sådan markering och sekretess- och informationssäkerhetsklassmarkering kan således förekomma parallellt eller i kombination. Hur märkningen ska utformas i detalj bör regleras i tillämpningsföreskrifter.

Inventering

Inventering av säkerhetsskyddsklassificerade handlingar och lagringsmedia som innehåller säkerhetsskyddsklassificerade uppgifter är en åtgärd vars syfte är bl.a. att kunna upptäcka om en sådan uppgift kan ha blivit röjd. Kravet på inventering bör kvarstå i en ny förordning, dock enbart för handlingar på nivån konfidentiell och däröver. Ett inventeringsintervall på ett år för kvalificerat hemliga handlingar bör kvarstå i en ny säkerhetsskyddsförordning. För övriga handlingar bör inventeringsintervallet bestämmas i tillämpningsföreskrifter. Handlingar som förvaras i arkiv bör undantas från kravet på inventering eftersom arbetsinsatsen inte står i rimlig proportion till det skydd som åtgärden medför.

Försändelser till utlandet

Bestämmelsen i nuvarande förordning om att Utrikesdepartementets kurirförbindelser i regel ska användas för försändelser till utlandet bör kvarstå i sin nuvarande utformning även i en ny säkerhetsskyddsförordning. Neddragningar i Utrikesdepartementets kurirverksamhet har medfört att behovet av alternativa distributionsmöjligheter har ökat och sannolikt kommer att fortsätta öka i framtiden. Möjligheten att föreskriva eller besluta om undantag från huvudregeln gör andra lösningar möjliga för distribution i de fall där kurirförbindelser inte är möjliga eller lämpliga. Även denna bestämmelse bör därför stå kvar i en ny säkerhetsskyddsförordning.

I många länder och mellanfolkliga organisationer finns särskilda kurirbestämmelser för kurirer som inte omfattas av Wienkonventionen om diplomatiska förbindelser.[6] Även om dessa kurirer inte har något diplomatiskt skydd, kan rutinerna ändå tjäna som förebild för hur föreskrifter på detta område skulle kunna utformas, i syfte att öka flexibiliteten när det gäller försändelser utomlands.

[6] Wienkonventionen om diplomatiska förbindelser av den 18 april 1961.

Konfidentialitet, tillgänglighet och riktighet i it-system

Säkerhetsskyddsanalysen är som betonats tidigare av central betydelse för säkerhetsskyddet. Som komplement till den föreslagna bestämmelsen att bl.a. göra en säkerhetsskyddsanalys och att vidta relevanta säkerhetsskyddsåtgärder föreslår vi en bestämmelse i förordningen om säkerhetsskyddet för it-system. Av bestämmelsen bör framgå att den som avser att inrätta ett it-system som ska användas för säkerhetskänslig verksamhet ska analysera vilka krav på skydd som finns och se till att säkerhetsskyddet utformas så att dessa krav tillgodoses. Syftet med bestämmelsen är att säkerhetsskyddsbehov för ett system tidigt ska identifieras för att på så sätt undvika fördyringar som kan uppstå om sådana behov upptäcks sent i systemutvecklingen.

Aggregering av uppgifter i systemen bör särskilt beaktas. Det innebär att ett it-system som kan förväntas innehålla en omfattande mängd uppgifter på en viss nivå kan behöva ett säkerhetsskydd som är högre än vad nivån som sådan motiverar.

Samråd inför säkerhetsgodkännande

I 12 § första stycket säkerhetsskyddsförordningen finns en bestämmelse som innebär att, innan en myndighet inrättar ett ”register som ska föras med hjälp av automatisk databehandling” och som innehåller vissa slag av uppgifter, myndigheten ska samråda med Försvarsmakten alternativt Säkerhetspolisen. Förutom att bestämmelsen bör moderniseras bör den även kompletteras dels med ett tillägg att ett samråd är nödvändigt även då it-systemet väsentligen förändras, dels med en utvidgning att bestämmelsen avser även system som annars är av betydelse för Sveriges säkerhet, även om de inte behandlar säkerhetsskyddsklassificerade uppgifter.

Samrådet ska ske med Säkerhetspolisen eller, om organisationen hör till Försvarsmaktens tillsynsområde, Försvarsmakten. Samrådet ska vara begränsat till it-system som kan förutses komma att behandla säkerhetsskyddklassificerade uppgifter i informationssäkerhetsklassen konfidentiell eller däröver eller som är av motsvarande betydelse för Sveriges säkerhet. Kvalificeringskravet motiveras av att ett tidskrävande samrådsförfarande inte står i paritet med den skada som t.ex. ett it-system som behandlar uppgifter på nivån begränsad kan medföra. Kravet på ”motsvarande

betydelse” för Sveriges säkerhet gör att it-system som är av ringa betydelse för Sveriges säkerhet inte omfattas av bestämmelsen. Exempel på system av motsvarande betydelse torde vara folkbokföringsregistret och andra it-system som på nationell nivå används för samhällsviktiga funktioner för t.ex. elförsörjning, telekommunikationer, samfärdsel och allmän försäkring.

Ett tidigt samråd kan bl.a. ge värdefull vägledning om hur ett från säkerhetssynpunkt godtagbart system kan utformas på ett kostnadseffektivt sätt. Formerna för samråd och vilka uppgifter ett samrådsförfarande ska omfatta bör kunna regleras i tillämpningsföreskrifter. Samrådet i de fall där systemen ska användas i en internationell miljö bör utformas på ett sådant sätt att det framgår att krav på systemet som följer av internationella säkerhetsskyddsåtaganden har beaktats.

It-säkerhet i fleranvändarsystem

I 12 § andra stycket säkerhetsskyddsförordningen finns en bestämmelse om it-säkerheten i s.k. fleranvändarsystem, dvs. it-system som ska användas av mer än en person. Med sådana system menas dock inte t.ex. fristående datorer som kan användas av flera personer. System som behandlar hemliga uppgifter ska enligt denna bestämmelse vara försett med funktioner för behörighetskontroll och registrering av händelser i systemet som är av betydelse för säkerheten.

Flera av utredningens experter har framfört att fler relevanta krav bör kunna ställas på ett sådant system. Vi föreslår att fleranvändarsystem som hanterar säkerhetsskyddsklassificerade uppgifter ska vara försedda med funktioner för behörighetskontroll, registrering av händelser i systemet som är av betydelse för säkerheten, skydd mot obehörig avlyssning, intrångsskydd, skydd mot skadlig kod samt skydd mot röjande signaler. Kraven kan dock behöva nyanseras, särskilt när det gäller system som innehåller uppgifter i den lägsta informationssäkerhetsklassen. Försvarsmakten och Säkerhetspolisen bör därför kunna föreskriva och besluta om undantag från kraven.

När det gäller it-system som används i säkerhetskänslig verksamhet utan att säkerhetsskyddsklassificerade uppgifter behandlas i dessa bör det inte införas motsvarande krav. Skälet till det är att

kravbilden för dessa system är så olika att detaljerade föreskrifter riskerar att bli svårtillämpade.

Ackreditering av it-system

Enligt 12 § tredje stycket säkerhetsförordningen får vissa it-system som innehåller hemliga uppgifter inte tas i drift förrän det godkänts från säkerhetssynpunkt av den för vars verksamhet systemet inrättas. Det bör även fortsättningsvis finnas en bestämmelse om säkerhetsgodkännande av informationssystem som innehåller säkerhetsskyddsklassificerade uppgifter (s.k. ackreditering). Ackreditering innebär ett godkännande av att ett it-system i en given utformning och konfiguration uppfyller ställda informationssäkerhetskrav och ur den aspekten får tas i drift.

Ackrediteringen har betydelse även för it-system som ska sammanlänkas med internationella it-system. En vanlig rutin är att det i dessa fall utfärdas ett intyg att de säkerhetskrav som gäller för systemet är uppfyllda (på engelska *Statement of Compliance*). Rutiner kring detta beskrivs närmare i avsnitt 20.2.

Kommunikationssäkerhet

Också kravet på kommunikationssäkerhetsskydd i 13 § säkerhetsskyddsförordningen bör föras över till en ny förordning med en modernisering av terminologin men i övrigt med i huvudsak samma betydelse som i dag.

Det innebär att myndigheter och andra som förordningen gäller för, innan de behandlar säkerhetsskyddsklassificerade uppgifter i ett it-system utanför deras kontroll, ska förvissa sig om att det för uppgifterna där finns ett tillräckligt säkerhetsskydd.

Kryptografiska funktioner

Kryptografiska funktioner kan användas inom kommunikationssäkerheten men även i säkerhetslösningar för t.ex. lagring av säkerhetsskyddsklassificerade uppgifter och för autentisering av användare. Bestämmelsen om att kryptografiska funktioner som ska användas i informationssäkerheten ska godkännas av Försvars-

makten bör föras över till en ny förordning. Försvarsmakten och Säkerhetspolisen bör ges möjlighet att föreskriva eller besluta om undantag utom i de fall där kraven följer av ett internationellt säkerhetsskyddsåtagande.

17 Fysisk säkerhet

Detta kapitel rör den säkerhetsskyddsåtgärd som i säkerhetsskyddslagen benämns *tillträdesbegränsning*. En reformerad lag ska ge ett skydd för information av betydelse för säkerhetskänslig verksamhet ur flera aspekter än enbart konfidentialitet. Det innebär att tillträdesbegränsning, som i dag reglerar behörigheten till platser och lokaler, måste utvecklas i samma riktning.

Detta kapitel inleds med en utvecklad förklaring till förslaget i kapitel 15.1 att förändra begreppet tillträdesbegränsning till *fysisk säkerhet* och syftet med åtgärden (avsnitt 17.1). Därefter redovisar vi förhållandet mellan fysiskt säkerhetsskydd och bestämmelser i skyddslagen (2010:305) och hur detta bör uttryckas i en reformerad säkerhetsskyddslag (avsnitt 17.2). Slutligen redovisar vi vilka internationella säkerhetsskyddsåtaganden som påverkar utformningen av den fysiska säkerheten (avsnitt 17.3) samt vilka slag av åtgärder som bör kunna regleras genom tillämpningsföreskrifter (avsnitt 17.4).

17.1 Vad ska fysisk säkerhet syfta till?

Förslag: Med *fysisk säkerhet* ska avses sådana säkerhetsskyddsåtgärder som ska förebygga förebygga dels att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där verksamhet som av annan anledning är säkerhetskänslig bedrivs, dels skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt.

Nuvarande benämning

Vid tillkomsten av nuvarande säkerhetsskyddslag ersattes den tidigare benämningen tillträdesskydd med *tillträdesbegränsning* utan att begreppet ändrades i sak.[1] Benämningen kritiserades av ett flertal remissinstanser på grund av att det ändrade en invand benämning och det framfördes att andra benämningar vore att föredra för det fall att den tidigare benämningen behövde ändras. I andra länder och även i Sverige används begreppet *fysisk säkerhet* (på engelska *Physical Security*) som en beskrivning av bl.a. åtgärder för att förhindra att personer får tillträde till byggnader, områden och anläggningar som de inte är behöriga för. Begreppet är dock vidare än så och avser även ett skydd mot obehöriga fordon och mot att oönskad materiel och oönskade substanser som t.ex. vapen samt sprängoch tändmedel medförs till platser där de kan orsaka skada. Begreppet kan även innefatta åtgärder för att förebygga att försändelser med sjukdomsalstrande organismer eller toxiska ämnen orsakar skada.

I en del av dessa avseenden är begreppet tillträdesbegränsning i den nuvarande säkerhetsskyddslagen för snävt, eftersom det tar sikte på i första hand personer och enbart i syfte att förebygga att obehöriga får tillträde till platser där de kan få tillgång till hemliga uppgifter eller utöva terrorism.[2] Definitionen återspeglar att nuvarande lag i första hand ger ett skydd för uppgifter, och då enbart från ett konfidentialitetsperspektiv.

Förändringsbehoven och syftet med åtgärden

Som vi har beskrivit i avsnitt 10.2.1 behöver lagen utvecklas för att på ett tydligare sätt ge ett skydd för enskild verksamhet samt att uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande skyddas. Dessutom ska informationens skyddsvärde bestämmas inte enbart utifrån ett konfidentialitetsperspektiv utan även utifrån riktighets- och tillgänglighetskrav. Detta förhållande gäller även för säkerhetsskyddsåtgärden tillträdesbegränsning. I en ny säkerhetsskyddslag behövs ett begrepp som tydligare svarar mot

[1] Prop. 1995/96:129 Säkerhetsskydd, s. 27 f.
[2] 7 § första stycket 2 säkerhetsskyddslagen.

behovet av att skydda säkerhetskänslig verksamhet av olika slag. Det nuvarande begreppet behöver därför utvecklas i denna riktning. Vi har översiktligt beskrivit skälen till de nya begreppen i kapitel 15.1.

Ett första förändringsbehov är att det förebyggande skyddet inte ska avse enbart obehörig tillgång till uppgifter som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) utan även sådana uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande. Detta löses genom att det i kapitel 12 definierade begreppet säkerhetsskyddsklassificerade uppgifter täcker båda dessa uppgiftstyper.

Ett andra behov är att förhindra obehörigt tillträde till byggnader m.m. där övrig säkerhetskänslig verksamhet bedrivs, dvs. sådan säkerhetskänslig verksamhet som inte omfattar hantering av säkerhetsskyddsklassificerade uppgifter. Detta bör därför anges specifikt i begreppsdefinitionen.

Slutligen behöver begreppet kompletteras genom ett tillägg som avser ett förebyggande skydd mot skadlig påverkan mot sådana områden, byggnader, anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. Syftet med detta är att åtgärderna ska omfatta även ett förebyggande skydd mot angrepp som sker utifrån eller på distans. Ett exempel på ett sådant angrepp är försändelser med skadebringande verkan som sprängmedel eller sjukdomsalstrande organismer. Ett annat exempel är att med tekniska hjälpmedel obehörigen få insyn i den säkerhetskänsliga verksamheten.

Med anledning av dessa förtydliganden är *fysisk säkerhet* en lämpligare benämning. Begreppet överensstämmer väl med motsvarande begrepp på engelska.

17.2 Koppling till skyddslagen

Skyddslagen

Skyddslagen med tillhörande förordning och tillämpningsföreskrifter ger rättsliga förutsättningar för ett kvalificerat skydd för vissa byggnader, andra anläggningar och områden samt militära fartyg och luftfartyg (skyddsobjekt).

Skyddsändamålen är att ge ett särskilt skydd mot sabotage, terroristbrott enligt 2 § lagen (2003:148) om straff för terrorist-

brott och spioneri samt röjande i andra fall av hemliga uppgifter som rör totalförsvaret. En utgångspunkt för skyddslagstiftningen är att systemet med skyddsobjekt fyller en funktion för skydd mot säkerhetshotande verksamhet. Skyddslagen har ett tydligt fokus på fredstida viktiga samhällsfunktioner utan att för den skull minska betydelsen av försvarsrelaterad verksamhet. Ett avgörande skäl för denna inriktning är enligt regeringen att samhället generellt sett har blivit väsentligt mera sårbart än tidigare.[3] Det är en sårbarhet som inte behöver hänga samman med militära eller direkta säkerhetspolitiska förhållanden men som ändå utsätter samhället för risker och påfrestningar på grundläggande samhällsfunktioner.

Skyddslagens skyddsändamål överensstämmer i stor omfattning med de skyddsändamål som vi föreslår ska gälla för en reformerad säkerhetsskyddslagstiftning. Fokus ligger i de båda lagstiftningarna på ett skydd för den för Sverige mest betydelsefulla verksamheten mot i huvudsak kvalificerade antagonistiska hot.

Skyddet av ett skyddsobjekt genomförs huvudsakligen som ett fysiskt bevakningsskydd genom att med tekniska åtgärder och bevakning ordna ett förstärkt tillträdesskydd. Personalen som ska svara för bevakningen (skyddsvakter) har i lagen getts ett antal befogenheter som är relativt långtgående.[4]

En eventuell följdändring i skyddslagen

Eftersom skyddslagens och säkerhetsskyddslagens skyddsändamål i stor omfattning är desamma kan det finnas skäl att terminologin i de båda lagarna överensstämmer i de fall där detta är möjligt. Lydelsen *hemliga uppgifter som rör totalförsvaret* i skyddslagens bestämmelse om skyddsändamål tycks semantiskt vara en snävare delmängd av de hemliga uppgifter som definieras i säkerhetsskyddsförordningen. Om detta är avsett eller inte framgår inte av motiven. Både skyddslagen och säkerhetsskyddslagen tar sikte på såväl civil som militär verksamhet. Den civila verksamheten har fått en ökande betydelse. Vi har föreslagit att i en ny säkerhetsskyddslag ska begreppet säkerhetsskyddsklassificerad uppgift ersätta hemlig uppgift. Det innebär att även uppgifter som ska skyddas enligt internatio-

[3] Prop. 2009/10:87 Skyddslagen, s. 25 f.
[4] Se även redovisningen av bestämmelser om skyddsobjekt enligt skyddslagen i avsnitt 4.3.

nella säkerhetsskyddsåtaganden omfattas av definitionen (se avsnitt 12.2). Mot bakgrund av vad som anförts kan det finnas anledning att överväga behovet av att en motsvarande ändring i skyddslagen.

Norska sikkerhetslovens bestämmelser om objektssäkerhet

Inom ramen för utredningens internationella utblick har den norska *sikkerhetsloven* beskrivits i avsnitt 8.1.4. Som ett utmärkande drag i denna lag, vilket skiljer sig från nuvarande säkerhetsskyddslag, finns ett kapitel som beskriver *objektsikkerhet*. Detta kapitel innehåller ett åliggande för myndigheter som lagen gäller för att besluta om s.k. *skjermningsverdige objekter*. Det är objekt som är av betydelse för ”säkerhetspolitisk krishantering och försvar av riket, för kritiska civila samhällsfunktioner, för [nationella] symbolvärden eller som kan utgöra en fara för miljön eller befolkningens liv och hälsa.”[5] Dessa objekt ska också klassificeras i kategorierna mycket kritisk, kritisk eller viktig i fallande skala utifrån vilken skada som ett angrepp på objektet kan medföra. Klassificeringen innebär en till varje klass hörande målsättning om hur skyddet ska vara utformat, med en kombination av olika säkerhetsskyddsåtgärder. Lagen ger även en möjlighet att ingå en överenskommelse med en annan stat eller internationell organisation om skydd för utländska objekt i Norge.

Objektssäkerhet i en ny säkerhetsskyddslagstiftning

Vi anser att den norska sikkerhetsloven innehåller bestämmelser om objektssäkerhet som på ett bra sätt skulle kunna tydliggöra förhållandet mellan skydds- och säkerhetsskyddslagen. Sådana bestämmelser skulle dock kunna utformas genom tillämpningsföreskrifter. Vi föreslår därför inte att någon bestämmelse om detta tas in i en ny lag. Däremot är den nuvarande hänvisningen till skyddslagen fortfarande relevant och bör därför kvarstå oförändrad i en ny säkerhetsskyddslag.

[5] 17 § lov (1998-03-20:10) om forebyggende sikkerhetstjenste (sikkerhetsloven). Citatet är översatt från norska.

17.3 Internationella åtaganden avseende fysisk säkerhet

EU-bestämmelser

I rådets beslut av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter[6] finns det bestämmelser om fysiskt säkerhet. Bestämmelserna finns i huvudsak i bilaga II till beslutet och omfattar regler som syftar till att ge ett skydd mot obehörigt tillträde till lokaler där säkerhetsskyddsklassificerade EU-uppgifter hanteras.

Bestämmelserna är således något snävare till sitt syfte än vad vi föreslår för säkerhetsskyddsåtgärden fysisk säkerhet. Bestämmelserna rör krav på riskanalys och ger exempel på olika säkerhetsskyddsåtgärder som kan vidtas, t.ex. perimeterskydd, bevakning och larm. Bestämmelserna indelar också utrymmen där säkerhetsskyddsklassificerade EU-uppgifter kan hanteras, i två kategorier – administrativa respektive säkra utrymmen (på engelska *Administrative Areas* och *Secured Areas*). Till kategorierna kopplas krav som ska vara uppfyllda för att säkerhetsskyddsklassificerade EU-uppgifter ska få hanteras där.

Bestämmelserna är på en sådan detaljnivå att de i Sverige bör kunna genomföras i form av tillämpningsföreskrifter. De myndigheter som ska utfärda tillämpningsföreskrifter till säkerhetsskyddslagen bör söka ledning i de nämnda EU-bestämmelserna för att i den utsträckning det med hänsyn till svenska förhållanden är möjligt följa kraven i bestämmelserna.

Övriga internationella säkerhetsskyddsåtaganden

I kapitel 6 har vi redovisat Sveriges internationella säkerhetsskyddsåtaganden. En inte oväsentlig del av dessa består av i huvudsak bilaterala säkerhetsskyddsöverenskommelser mellan Sverige och ett annat land eller mellanfolklig organisation. Överenskommelserna är vanligtvis utformade på en generell nivå, men avseende den fysiska säkerheten är det vanligt med en artikel med bestämmelser

[6] Rådets beslut av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2013/488/EU).

om hur besök ska genomföras. Besöksbestämmelserna omfattar enbart besök där säkerhetsskyddsklassificerade uppgifter ska utbytas eller delges den andra parten.

Artikelns utformning kan naturligtvis skilja sig åt mellan de olika överenskommelserna, men ett gemensamt krav, och en i sammanhanget internationell vedertagen princip, är att det land vars personal ska besöka det andra landet (eller den mellanfolkliga organisationen) i god tid före mötet ska skicka en besöksbegäran till den mottagande parten (på engelska *Request for Visit*, *RfV*). Denna ska innehålla uppgifter om besökare och deras inplacering i säkerhetsklass, syftet med besöket, vilken plats besöket ska ske på och övriga uppgifter som besöksmottagaren kan behöva. Besöksbegäran ska skickas från en behörig myndighet i det land som besökarna kommer ifrån. Dessa typer av besöksrutiner har sin främsta tillämpning inom ramen för industribesök i säkerhetskänsliga internationella projekt, främst inom försvarsmaterielområdet.

Det är naturligtvis viktigt att Sverige uppfyller kraven i dessa överenskommelser, men kraven är av sådan karaktär att de lämpligen bör regleras i form av tillämpningsföreskrifter.

Det internationella säkerhetsskyddssamarbetet behandlas närmare i kapitel 20.

17.4 Åtgärder för fysisk säkerhet

Allmänt om säkerhetsskyddsåtgärden och regleringen av denna

Säkerhetsskyddet inom den fysiska säkerheten består av ett antal åtgärder som rör bl.a. tillträde, byggnadstekniska åtgärder och bevakning. De flesta av dessa bestämmelser är av sådan karaktär och detaljeringsgrad att de bör finnas i myndighetsföreskrifter. För att tydliggöra den fysiska säkerheten och ge en bild av hur skyddet kan utformas redogör vi nedan för ett antal åtgärder som kan ha sin plats i sådana föreskrifter.

Behörighet och sektionering

För att den fysiska säkerheten ska vara relevant behövs det bestämmelser om vem som ska vara behörig till byggnader, platser och anläggningar samt vilka utrymmen som bör vara tillgängliga för allmänheten och besökare. Ibland kan en sektionering av en byggnad vara ändamålsenlig genom att behörigheten till olika delar av en verksamhet kan vara olika.

Byggnadstekniska åtgärder och områdesskydd

Bland de byggnadstekniska åtgärderna finns perimeterskydd i form av stängsel och staket, grindar, dörrar och portar samt omslutningsytor i form av väggar, golv, tak och fönster. Robustheten i dessa åtgärder kan ofta mätas mot olika typer av standarder och därmed nivåindelas utifrån aktuella hot och betydelsen av det som ska skyddas.

Skydd av viss utrustning och installationer

Även tekniskt skydd, barriärer etc., kan behövas för att ge ett skydd mot viss avgränsad teknisk utrustning som datorer, kommunikationsutrustning och elförsörjning. Viss utrustning kan även behöva förses med exempelvis larm.

Bevakning

Bevakning genomförs som inre och yttre bevakning och syftar dels till att hindra obehöriga, dels till att upptäcka intrångsförsök, incidenter och brister i säkerhetsskyddet. Ibland skiljer man mellan personell bevakning och teknisk bevakning.

Passersystem - nycklar, kort och koder

I stor omfattning styrs det behöriga tillträdet till byggnader, lokaler och områden av antingen elektroniska passersystem eller nycklar. Även biometriska passersystem förekommer där behörigheten

kontrolleras mot en persons unika fysiska karaktär, t.ex. fingeravtryck eller retina. Det behövs en reglering dels om hur tillförlitligheten och robustheten i passersystem ska mätas, dels när det gäller administrativa rutiner för säker hantering av nycklar, passerkort och koder.

Larm och kameraövervakning

För att upptäcka obehörigt tillträde kan larm och kameraövervakning användas. Larm bör terminera i någon form av larmcentral för att åtgärder mot det obehöriga tillträdet ska kunna vidtas. Larmsystemet innefattar sensorer som kan vara volym- och linjedetektorer, kross- och vibrationsdetektorer samt seismiska detektorer. Liksom för passersystem behövs det administrativa bestämmelser om t.ex. kodhantering och vilka åtgärder som ett utlöst larm ska medföra.

Brand, fukt och explosioner

Den fysiska säkerheten ska inte avse enbart skyddet för information ur ett konfidentialitetsperspektiv. När det gäller krav på tillgänglighet och riktighet är det därför viktigt att vidta åtgärder mot antagonistiska säkerhetshot som tar sikte på dessa aspekter. Särskilt it- och kommunikationssystem är sårbara när det gäller t.ex. brand och fukt. Detta kan gälla även för annan säkerhetskänslig verksamhet. Det behövs i dessa fall åtgärder för detektering och skydd som är anpassade mot den aktuella hotbilden och tillgångarnas betydelse.

Detektorer för spräng- och tändmedel, vapen och ammunition, radiosändare och sjukdomsalstrande substanser

Antagonistiska angrepp kan förekomma genom att skadeverkande föremål medförs eller sänds till en verksamhets lokaler eller områden. Beroende på angreppets syfte kan angreppen ta sikte på att förstöra eller undanföra för verksamheten viktiga tillgångar eller att obehörigen inhämta information. En skyddsåtgärd mot denna typ

av antagonistiska hot kan vara att med hjälp av tekniska lösningar upptäcka olika typer av skadeverkande materiel eller ämnen och därigenom förhindra dessa att påverka den säkerhetskänsliga verksamheten. För att förhindra upptagning av ljud eller andra röjande signaler kan utrymmen utformas med elektromagnetisk avskärmning. Lokaler kan också undersökas genom s.k. teknisk säkerhetsundersökning (s.k. TSU) med syfte att upptäcka obehörig teknisk utrustning för ljud- eller bildupptagning.

Kontroll av fordon

Ett fordon kan medföra stora mängder skadeverkande ämnen men även obehöriga personer och otillåten utrustning. För verksamheter där fordon förekommer i anslutning till den säkerhetskänsliga verksamheten bör det därför vidtas åtgärder för att hindra obehöriga fordon och för att kunna upptäcka sådant som inte får medföras i fordonet. Även åtgärder för att förhindra forcering genom användning av fordon kan behöva regleras.

18 Personalsäkerhet

I de föregående kapitlen har vi behandlat informationssäkerhet och fysisk säkerhet. Åtgärder inom dessa områden berör i hög grad anställda och andra som deltar i en säkerhetskänslig verksamhet. Det tredje området för säkerhetsskyddet tar dock på ett mer direkt sätt sikte på att förebygga sårbarheter som kan kopplas samman med anställda och andra som deltar i en säkerhetskänslig verksamhet. I säkerhetsskyddslagen finns i det avseendet bestämmelser om säkerhetsprövning och om utbildning

Direktiven utgår i denna del från två större frågor. För det första handlar det om att underlätta det internationella samarbetet. I det avseendet finns i direktiven en tydlig inriktning mot en anpassning till ett system med s.k. säkerhetsklarering. För det andra handlar det om ett mer ändamålsenligt sätt att avgränsa tillämpningsområdet. I det avseendet tas upp att begränsningen i fråga om säkerhetsklassplacering till anställningar som innebär att den anställde hanterar uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL, innebär ett för snävt tillämpningsområde. Andra frågor som tas upp är bl.a. om kravet på svenskt medborgarskap i säkerhetsskyddslagen bör förändras och om bestämmelserna om registerkontroll vid skydd mot terrorism behöver utvidgas till att avse även bl.a. verksamheter som innebär transporter av farligt gods.

Flera av de förslag vi lämnat tidigare i betänkandet innebär i olika avseenden viktiga moment för förslagen i de följande avsnitten. Det gäller bl.a. förslaget om *skydd av säkerhetskänslig verksamhet*. I begreppet säkerhetskänslig verksamhet ryms dels verksamheter som är av betydelse för Sveriges säkerhet, dels verksamheter som omfattas av internationella säkerhetsskyddsåtaganden. Av grundläggande betydelse för våra överväganden på det här området är förslaget om en förändrad systematik som

innebär dels en övergång från skydd av hemliga uppgifter till ett skydd av *säkerhetsskyddsklassificerade uppgifter*, dels en övergång från ett särskilt skydd mot terrorism till skydd av verksamhet som är säkerhetskänslig av annan anledning än att den innebär hantering av säkerhetsskyddsklassificerade uppgifter *(i övrigt säkerhetskänslig verksamhet)*. Också förslaget om att införa krav på en klassificering (fyra informationssäkerhetsklasser) och anpassning av skyddsnivå utifrån relevant informationssäkerhetsklass är en viktig utgångspunkt för våra överväganden om placering i säkerhetsklass.

De nämnda förslagen innebär att vi redan har behandlat eller delvis behandlat flera av de frågor som i direktiven tas upp i samband med de delområden som närmast berör säkerhetsprövning. Det gäller bl.a. frågan om kopplingen vad gäller placering i säkerhetsklass till bestämmelser om sekretess i offentlighets- och sekretesslagen (se avsnitt 12.2). I avsnitt 15.1 har vi vidare föreslagit att en sammanfattande benämning på de samverkande åtgärderna säkerhetsprövning och utbildning i säkerhetsskydd ska vara *personalsäkerhet*.

De frågor som återstår att behandla i fråga om personalsäkerhet är bl.a. syftet med säkerhetsskyddsåtgärden (avsnitt 18.2) och frågan om en övergång till ett klareringssystem (avsnitt 18.3). Resterande del av kapitlet behandlar frågor som hör samman med säkerhetsprövning. Den delen av kapitlet inleds med frågor om innehållet i och genomförandet av säkerhetsprövningen (avsnitt 18.4). Därefter behandlas grunder för indelning i säkerhetsklass (avsnitt 18.5 och 18.6) och frågan om krav på svenskt medborgarskap vid placering i säkerhetsklass (avsnitt 18.7). Avslutningsvis behandlas några frågor som på olika sätt har koppling till skyddet av den personliga integriteten vid säkerhetsprövning (avsnitt 18.8–18.12).

Utöver de frågor som vi behandlar i det här kapitlet återkommer vi i kapitel 19 till frågor om personalsäkerhet vid säkerhetsskyddad upphandling och i kapitel 20 där vi behandlar frågan om utfärdande av säkerhetsintyg för internationella behov.

Kapitlet inleds med redogörelse för regleringen om säkerhetsprövning och utbildning i säkerhetsskydd och tillämpningen av den.

18.1 Gällande ordning

Regleringen om säkerhetsprövning och utbildning i säkerhetsskydd

Säkerhetsprövning enligt säkerhetsskyddslagen tar sikte på anställda, uppdragstagare och andra som deltar i en säkerhetskänslig verksamhet. Utifrån den nu gällande säkerhetsskyddslagen handlar det om deltagande i verksamheter som är av betydelse för rikets säkerhet eller som särskilt behöver skyddas mot terrorism. Genom en analys ska klarläggas vilka anställningar som medför behov av placering i säkerhetsklass och säkerhetsprövning. Ansvaret för säkerhetsprövningen ligger i regel vid den verksamhet där den kontrollerade ska anställas. När det är fråga om enskild verksamhet är det dock i huvudsak de säkerhetsskyddsstödjande myndigheterna[1] (Affärsverket svenska kraftnät, Transportstyrelsen, Post- och telestyrelsen eller någon av länsstyrelserna) som beslutar om placering i säkerhetsklass och om registerkontroll.

Säkerhetsprövning förutsätter inte placering i säkerhetsklass. Däremot är sådana i säkerhetsprövningen ingående kvalificerade moment som registerkontroll och särskild personutredning förbehållna situationer där det är fråga om anställning eller annat deltagande som placerats i en säkerhetsklass. Också bestämmelser om verksamheter som särskilt behöver skyddas mot terrorism ger stöd för registerkontroll som ett led i en säkerhetsprövning.

I säkerhetsskyddslagen anges också att myndigheter och andra som lagen gäller för ska se till att personalen får utbildning i frågor om säkerhetsskydd.

[1] I direktiven används benämningen sektorsansvariga myndigheter som en samlande benämning för Affärsverket svenska kraftnät, Post- och telestyrelsen, Transportstyrelsen och länsstyrelserna. Som framgår av avsnitt 10.1.5 har vi i stället valt att använda säkerhetsskyddsstödjande myndigheter som en samlande benämning för dessa myndigheter såvitt avser deras funktioner för säkerhetsskyddet. Vi föreslår vidare i avsnitt 18.10 och 21.2.4 att Myndigheten för samhällsskydd och beredskap ska ta över de uppgifter länsstyrelserna i detta avseende har samt även vara säkerhetsskyddsstödjande myndighet för kommuner och landsting. I förhållande till kommuner och landsting är dock uppgiften begränsad till rådgivning och tillsyn.

Närmare om säkerhetsprövning och utbildning i säkerhetsskydd

Avsikten med säkerhetsprövningen är att hämta in ett allsidigt underlag, t.ex. genom samtal med den som prövningen avser och med tidigare arbetsgivare, för att kunna bedöma om personen är lämplig för att delta i den ifrågavarande säkerhetskänsliga verksamheten. Bedömningen, som närmast kan beskrivas som en pålitlighets- och lämplighetsbedömning, ska inte ta sikte bara på att hindra att personer med antagonistiska avsikter deltar i säkerhetskänslig verksamhet. Den bör syfta till att också säkerställa att personer som i säkerhetshänseende är sårbara inte placeras på befattningar där sårbarheten kan påverka personens förmåga och vilja att upprätthålla verksamhetens krav på säkerhetsskydd. Med sårbarhet avses i dessa sammanhang att det finns omständigheter i fråga om livsföring och levnadsbakgrund som gör att en person kan antas riskera att hamna i en intressekonflikt eller bli särskilt utsatt för påtryckningar att lämna ut känsliga uppgifter eller att en person på annat sätt kan befaras äventyra den säkerhetskänsliga verksamheten. I förarbetena till säkerhetsskyddslagen nämns bl.a. dubbla lojaliteter, en ansträngd ekonomisk situation och olika former av missbruk.[2]

Säkerhetsprövning bör inte innebära endast en prövning av en persons pålitlighet i samband med att en anställning påbörjas utan är tänkt att medföra ett uppföljningsansvar som sträcker sig över hela anställningstiden. En viktig del i säkerhetsprövningen kan vara ett avslutningssamtal. Prövningen bör därför kunna beskrivas som en under anställningstiden pågående process. Den bör normalt innefatta någon form av intervju eller annan uppgiftsinhämtning från den som prövningen avser, referenstagning, kontroll av betyg och intyg samt, i den omfattning det föreskrivs, registerkontroll och särskild personutredning. Registerkontrollmomentet innebär också att även uppgifter som efter den inledande prövningen tillförs registren kan komma att lämnas ut för säkerhetsprövning.[3]

[2] Prop. 1995/96.129 Säkerhetsskydd, s. 28 och även Säkerhetsskyddsutredningens betänkande Säkerhetsskydd (SOU 1994:149), avsnitt 8.2.2 Riskfaktorer.
[3] Vilka uppgifter som efter registerkontroll (inkluderat eventuell särskild personutredning) anses vara av relevans för säkerhetsprövningen och därför ska lämnas ut avgörs av Säkerhets- och integritetsskyddsnämnden.

För att förebygga sådana sårbarheter som den s.k. mänskliga faktorn kan utgöra i en verksamhet är också information och utbildning om säkerhetsskydd viktiga delar av säkerhetsskyddet.

Tillämpningen

Det ska tilläggas att det i fråga om tillämpningen av bestämmelserna om säkerhetsprövning och om utbildning i säkerhetsskydd verkar finnas stora variationer mellan olika verksamheter. Säkerhetsprövningen går inte alltid till på det sätt som nu har beskrivits. Det verkar inte vara ovanligt att säkerhetsprövningen så gott som uteslutande består av registerkontroll och att säkerhetsprövningen ses enbart som en åtgärd inför en anställning. Det har också från bl.a. Säkerhetspolisen och Affärsverket svenska kraftnät påtalats omfattande brister i fråga om den grundläggande förutsättningen att behovet av placering i säkerhetsklass och säkerhetsprövning behöver ha ett stöd i en verksamhets säkerhetsskyddsanalys.

Att ambitionsnivån för själva prövningsunderlaget varierar kan i viss mån förklaras av att de anställningar som kan föranleda säkerhetsprövning är av varierande slag. Underlaget behöver självfallet anpassas till den anställning eller det deltagande det är fråga om. Det kan vara tillräckligt med ett mer begränsat underlag när säkerhetsprövningen t.ex. avser en person som behöver ges ett tillträde till vissa mindre känsliga säkerhetsområden på en flygplats. Överlag är vår erfarenhet att variationerna dock snarare beror på att vissa verksamheter tillämpar mer utvecklade metoder för att fastställa behov av och genomföra säkerhetsprövning. Det gäller bl.a. Säkerhetspolisen, Försvarsmakten och flera andra myndigheter inom försvarssektorn. Intressant att notera är att dessa verksamheter framhåller bl.a. att registerkontrollens betydelse för säkerhetsprövningen har minskat, att säkerhetsprövningen förutsätter en kontinuerlig uppföljning och att utbildning som ska visa på behovet av säkerhetsskydd och en acceptans för det är en viktig och kostnadseffektiv del av säkerhetsskyddet.

18.2 Vad ska personalsäkerhet syfta till?

Förslag: Syftet med säkerhetsskyddsåtgärden personalsäkerhet ska anges vara dels att förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de får tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av annan anledning är säkerhetskänslig (*säkerhetsprövning*), dels att säkerställa att de som deltar i säkerhetskänslig verksamhet har en tillräcklig kunskap om säkerhetsskydd (*utbildning i säkerhetsskydd*).

Personalsäkerhet – en ny benämning

Som nämnts i inledningen till kapitlet har vi i avsnitt 15.1 föreslagit en mindre systematisk förändring på så sätt att säkerhetsskyddsåtgärden säkerhetsprövning kompletteras med krav på utbildning i säkerhetsskydd. Därigenom förtydligas utbildningens betydelse för säkerhetsskyddet. Som en sammanfattande benämning på dessa samverkande åtgärder har vi föreslagit personalsäkerhet. Med denna systematik består alltså personalsäkerheten av delmomenten säkerhetsprövning och utbildning i säkerhetsskydd. Syftet med de två delmomentet behandlas i det följande.

En något vidare formulering av syftet med säkerhetsprövning

I 7 § säkerhetsskyddslagen anges bl.a. att syftet med säkerhetsprövning är att förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet. Vidare anges att säkerhetsskyddet även i övrigt ska förebygga terrorism. I 11 § säkerhetsskyddslagen utvecklas innebörden av och förutsättningarna för säkerhetsprövning. Där anges bl.a. att säkerhetsprövning ska göras innan en person genom anställning eller på något annat sätt deltar i verksamhet som har betydelse för rikets säkerhet eller anlitas för uppgifter som är viktiga för skyddet mot terrorism. Det anges vidare att prövningen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas av säkerhetsskyddslagen och i övrigt pålitlig från säkerhetssynpunkt.

Till följd av våra tidigare överväganden i fråga om beskrivningen av lagens syfte och lagens systematiska uppbyggnad behöver syftet med säkerhetsprövning justeras något. Åtgärden behöver följaktligen anpassas till en ny terminologi och därför avse säkerhetskänslig verksamhet i dess helhet. Beskrivningen av syftet med åtgärden bör ansluta till de två huvudsakliga inriktningarna för säkerhetskänslig verksamhet. I en ny säkerhetsskyddslag bör därför syftet med säkerhetsprövning anges vara att förebygga att personer som inte är pålitliga från säkerhetssynpunkt genom anställning eller på annat sätt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av annan anledning är säkerhetskänslig.

Utbildning

I 30 § säkerhetsskyddslagen åläggs myndigheter och andra som lagen gäller för att bl.a. se till att personalen får utbildning i frågor om säkerhetsskydd. På samma sätt som säkerhetsprövning är det fråga om krav på säkerhetsskyddsåtgärder som direkt är inriktade mot att förebygga sådana hot och risker för säkerhetsskyddet som anställda och andra som deltar i verksamheten kan utgöra. Sårbarheter vid t.ex. myndigheter kan inte sällan direkt kopplas samman med anställda som av okunskap, obetänksamhet eller av bekvämlighet inte följer de krav på säkerhetsskydd som gäller för verksamheten. Säkerhetsskyddsåtgärder uppfattas inte sällan som krångliga, tidsödande och begränsande. Det förhållandet blir än mer påtagligt när utvecklingen för att tillgodose säkerhet vid elektronisk kommunikation av olika slag inte är i fas med utvecklingen för att åstadkomma en allt större mobilitet. Utbildnings- och informationsinsatser för att höja kunskapen om verksamhetens säkerhetsskydd och för att öka förståelsen och acceptansen för det är därför en viktig del av säkerhetsskyddet. Myndigheter som har ett väl utvecklat program för att utbilda personalen i säkerhetsskydd har framhållit att det också är en kostnadseffektiv säkerhetsskyddsåtgärd. Självfallet behöver utbildningens omfattning och innehåll samt formerna för den anpassas till det deltagande i säkerhetskänslig verksamhet som det är fråga om. På samma sätt som för säkerhetsprövningen finns det för utbildningskravet ett

uppföljningsansvar som sträcker sig över hela anställningsförhållandet eller den motsvarande tid som deltagandet pågår. Utbildning i säkerhetsskydd kan också underlätta den uppföljande säkerhetsprövningen. Samtal om säkerhetsskydd i samband med utbildning kan ge tillfälle att fånga upp relevanta attitydförändringar hos personer som omfattas av krav på säkerhetsprövning.

Utbildning, inte minst med inriktning på att skapa acceptans för behovet av säkerhetsskydd, är på samma sätt som en väl genomförd säkerhetsprövning således en viktig del av säkerhetsskyddet.

18.3 Behovet av en anpassning till internationella förhållanden

Bedömning: Den nuvarande säkerhetsprövningen bör inte utvecklas mot ett s.k. klareringssystem. För att i fråga om säkerhetsprövning tydligare kunna uppfylla krav som följer av internationella säkerhetsskyddsåtaganden och även i övrigt underlätta internationell samverkan på säkerhetsskyddsområdet behövs det förändringar av nuvarande ordning i följande delar.

1. En anpassning av grunderna för placering i säkerhetsklass till en ordning där säkerhetsskyddets nivå i fråga om säkerhetsskyddsklassificerade uppgifter bestäms utifrån uppgifternas informationssäkerhetsklass.
2. En tydligare reglering avseende säkerhetsintyg som kan jämställas med ett s.k. *personnel security clearance certificate (PSCC)*.

Förändringsbehovet behöver belysas från ett internationellt och nationell perspektiv

Direktiven ger uttryck för behov av en förändring av nuvarande säkerhetsprövning mot ett system med inslag av säkerhetsklarering. Redovisningen i direktiven utgår i det avseendet från de förändringar som samarbetet med andra länder och mellanfolkliga organisationer påkallar. Också behovet av att underlätta för enskilda att få uppdrag i andra länder och mellanfolkliga organisationer där krav

ställs på säkerhetsintyg lyfts fram. En fråga som däremot inte närmare berörs i direktiven är om det också från ett nationellt perspektiv finns fördelar med en ordning som bygger på ett klareringsförfarande. Vi anser att båda dessa perspektiv bör beaktas i fråga om behovet av att förändra nuvarande system.

Inledningsvis behöver därför skillnader och likheter belysas mellan den svenska modellen för säkerhetsprövning och sådana klareringssystem som används bl.a. i andra europiska länder och inom bl.a. EU, Nato och ESA.[4]

På vilket sätt skiljer sig klareringssystemen från nuvarande ordning?

I vårt uppdrag ingår att redovisa hur klareringssystem tillämpas i närliggande länder. Vi har valt att genomföra den internationella utblicken genom att från en något vidare utgångspunkt studera systemen för säkerhetsskydd i några utvalda länder (Finland, Danmark, Nederländerna, Norge och Tjeckien). En landsvis redovisning av bl.a. klareringssystemen i dessa länder finns i kapitel 8. Därutöver har vi mer översiktligt studerat klareringssystem i några andra EU-länder, bl.a. Frankrike, Storbritannien och Ungern. Av betydelse för frågan om en övergång till ett klareringssystem är också bestämmelser om klarering vid mellanfolkliga organisationer, bl.a. EU. I kapitel 6 om folkrättsliga förpliktelser finns en redogörelse för bestämmelser om bl.a. klarering inom EU samt i olika multi- och bilaterala avtal om säkerhetsskydd.

Erfarenheter som kan dras utifrån den internationella utblicken visar framför allt att i fråga om klarering är likheterna med den svenska modellen större än olikheterna. Det handlar överlag mer om formella skillnader än om skillnader i sak. Systemen för klarering i de länder vi har studerat skiljer sig dessutom sinsemellan åt i flera avseenden. Det gäller inte minst organisatoriskt. I Norge finns t.ex. ett stort antal klareringsmyndigheter medan prövningen är centraliserad till en myndighet i Tjeckien. I Nederländerna finns två klareringsmyndigheter med ansvar för civil- respektive försvarsinriktad sektor. I Norge tillämpas dessutom ett tvåstegsförfarande

[4] I avsnittet finns hänvisningar till bl.a. regleringen om säkerhetsskydd i de nordiska länderna och till EU:s bestämmelser om säkerhetsskydd. För fullständiga referenser hänvisas till kapitel 6 och 8.

(klarering av klareringsmyndighet och efterföljande auktorisation på verksamhetsnivå). Vad gäller gemensamma drag i de olika ländernas och mellanfolkliga organisationernas system är det framför allt två områden som är framträdande. Det är också i dessa avseenden som skillnaden mot den svenska säkerhetsprövningen är mest påtaglig. Det handlar för det första om att klareringen utgår från ett system där säkerhetsskyddet för uppgifter ska anpassas till den skyddsnivå (*Top secret*, *Secret*, *Confidential* eller *Restricted*) som bestämts vid en informationsklassificering. Vårt förslag i avsnitt 15.3 innebär krav på en motsvarande klassificering och anpassning av nivå på säkerhetsskyddet, varför den skillnaden inte kommer att kvarstå. För det andra manifesteras klareringen genom att ett intyg utfärdas.

En avgörande skillnad mellan säkerhetsprövning och klarering brukar anses vara att säkerhetsprövningen är kopplad till en anställning medan klareringen är kopplad till en person (se direktiven s. 10). Mot den beskrivningen kan invändas att även i fråga om en klarering finns generellt sett ett nära samband med en specifik befattning. Det är t.ex. i regel endast arbetsgivaren som kan ansöka om klarering. I Nederländerna åligger det varje ministerium att avgöra vilka befattningar inom den egna organisationen som kräver placering i säkerhetsklass, och det är enbart personer som är aktuella för placering på sådana befattningar som kan klareras. Inte i något av de länder vi har studerat är det möjligt för en enskild person att själv ansöka om en klarering. Vilken anställning som aktualiserar klareringen är i hög grad styrande för prövningens omfattning och inriktning. I Nederländerna är det särskilt tydligt hur prövningsunderlaget anpassas till den specifika befattningen.

Själva prövningen uppvisar stora variationer. I Nederländerna är ambitionsnivån i fråga om bedömningsunderlaget överlag hög. Klareringen föregås där bl.a. av omfattande intervjuer i den berördes hemmiljö. Regleringarna i Finland, Norge och Tjeckien ger i och för sig såväl utrymme för som intryck av att klareringen grundas på en helhetsbedömning där omständigheter av olika slag belyses och värderas. I t.ex. den norska motsvarigheten till säkerhetsskyddslagen anges uttryckligen vilka slag av omständigheter som kan vara av relevans för prövningen.[5] Vår uppfattning, efter att ha informe-

[5] 21 §, Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).

rats om tillvägagångssättet i dessa länder, är dock att intervjuer, referenstagning och liknande underlagsinhämtning i praktiken förekommer relativt sällan. Det förefaller i stället vara så att underlaget som klareringen grundar sig på i flertalet fall består endast av en kontroll mot straffregister och liknande. Någon motsvarighet till Säkerhet- och integritetsskyddsnämndens prövning av registeruppgifters relevans finns inte i de studerade länderna, utan i princip alla förekommande registeruppgifter lämnas ut till den myndighet som avgör frågan om klarering.

Det bör också framhållas att inte heller klareringen ger någon självständig rätt att ta del av uppgifter upp till en viss skyddsnivå (se avsnitt 16.3). På samma sätt som enligt 7 § säkerhetsskyddsförordningen förutsätts ett behov av att i tjänsten ta del av känsliga uppgifter. I Norge är det den efterföljande auktorisationen som medför en rätt att, för en viss anställning, ta del av uppgifter upp till en viss skyddsnivå.

Klareringen bygger i huvudsak på en prövning av en persons pålitlighet vid tidpunkten då en anställning påbörjas och gäller sedan i princip under en viss tid. Klareringen gäller alltså i regel för en förutbestämd tidsperiod. Rådets säkerhetsbestämmelser till vilka avtalet mellan EU-länderna om säkerhetsskydd hänvisar anger tio år som en yttersta gräns för en klarering på nivåerna *Secret* och *Confidential* och fem år för nivån *Top secret.* De flesta EU-länder har kortare giltighetstider.

Att klareringen gäller för en viss tid kan, men innebär inte med nödvändighet att godkännandet har giltighet även vid ändrad anställning eller att klareringen i sig underlättar möjligheterna att få andra anställningar som kräver en klarering. I t.ex. Danmark och Nederländerna gäller klareringen enbart för en specifik befattning. I Norge däremot gäller klareringen under fem år för statliga anställningar (för värnpliktiga dock endast under två år). I Finland har man genom den nya säkerhetsutredningslagen frångått den tidigare strikta ändamålsbundenheten vid säkerhetsutredningar. I stället gäller att en ny arbetsgivare i princip måste godta en tidigare säkerhetsprövning. Undantag får göras om det finns särskilda skäl t.ex. om förundersökning har inletts. I Ungern finns en möjlighet, men ingen skyldighet, att överta en tidigare klarering. En klarering behöver inte heller medföra att den som klareringen gäller också själv förfogar över intyget. I t.ex. Norge är det arbetsgivaren som

får intyget, och det får endast för kortare tidsperioder, vid behov i tjänsten, lånas ut till den som intyget avser.

Om kännedom om händelser eller förändrade förhållanden under giltighetstiden medför behov att ompröva bedömningen av pålitligheten, finns i regel förfaranden som ytterst kan leda till att klareringen återkallas. I fråga om nya omständigheter finns inte i något av de länder vi studerat någon direkt motsvarighet till den fortlöpande bevakning av tillkommande registeruppgifter som i Sverige görs inom ramen för säkerhetsprövningen.[6]

Är klarering som modell att föredra framför nuvarande ordning?

En jämförelse mellan det system vi tillämpar och ett klareringssystem försvåras av att klareringssystemen, som framgått ovan, sinsemellan uppvisar stora olikheter. Vidare är tillämpningen av de svenska bestämmelserna om säkerhetsprövning som redovisats i avsnitt 18.1 inte enhetlig, vilket också det försvårar en jämförelse.

Med utgångspunkt i hur bestämmelserna om säkerhetsprövning *bör* tillämpas ser vi, vid en jämförelse med ett klareringssystem, tydliga fördelar med nuvarande ordning. Det gäller framför allt ordningen där prövningen görs av den verksamhet som anställningen eller deltagandet avser. Det kan bli svårare att anpassa prövningen till vad som krävs för en specifik befattning, om prövningen inte görs på en verksamhetsnivå. Överlag är vårt intryck att underlagen i klareringsmodellerna, med undantag av framför allt Nederländerna, i högre grad är mer summariska och inte sällan bygger på enbart uppgifter om tidigare brottslighet. Sådana uppgifter tycks också i större utsträckning ges en självständig betydelse. Även om den helhetsbedömning som förarbetena till säkerhetsskyddslagen ger uttryck för inte fått fullt genomslag, är ändå intrycket att en mer nyanserad prövning överlag görs i Sverige. I det avseendet fyller också ordningen med Säkerhets- och integritetsskyddsnämndens relevansprövning av registeruppgifter en viktig funktion för att skydda den enskildes integritet. Den ordningen förefaller vara mer ändamålsenlig än de begränsade möjligheter till överklagande av klarering som finns i vissa länder. En annan fördel med

[6] En delvis liknande ordning finns i Danmark. Omfattningen av kontrollen är dock mer begränsad.

den svenska modellen är att den genom den verksamhetsnära prövningen ger bättre förutsättningar för en fördjupad personkännedom under den tid som anställningen pågår. Fasen efter den inledande säkerhetsprövningen är viktig för att kunna fånga upp t.ex. förändringar i livssituation och förhållningssätt som är av betydelse för pålitlighet, lojalitet och sårbarhet. Bland annat Säkerhetspolisen och Försvarsmakten, som hör till de verksamheter som utvecklat metoderna för säkerhetsprövning, har framhållit att erfarenheterna visar att från säkerhetssynpunkt det kan vara minst lika viktigt att fokusera på den avslutande fasen av en anställning som på den inledande. Även om klareringssystem också i allmänhet innehåller bestämmelser om uppföljning vid t.ex. ingående av äktenskap eller samboförhållande, ger en ordning med förutbestämda giltighetstider snarare intryck av att själva prövningen är begränsad i tid.

Som vi ser det innebär en ordning med ett klareringsförfarande överlag ett avsteg från den viktiga principen om ett verksamhetsanpassat säkerhetsskydd. Att prövningen ska anpassas till den specifika befattningen är angeläget inte enbart utifrån behovet av ett för verksamheten väl anpassat säkerhetsskydd utan också för den som prövningen avser. En person som inte bedöms lämplig för att delta i ett visst slag av säkerhetskänslig verksamhet kan mycket väl anses vara pålitlig när det gäller en annan säkerhetskänslig verksamhet. Om en gjord säkerhetsprövning ska läggas till grund för en lämplighetsbedömning avseende andra anställningar än den som initierat prövningen, kan det således negativt påverka möjligheterna att delta i annat slag av säkerhetskänslig verksamhet. Självklart kan också situationen vara den omvända. Att prövningen skulle ges giltighet utöver den anställning eller det deltagande som initierat prövningen anser vi inte vara i linje med de inslag i prövningen som framhålls som viktiga. Det gäller bl.a. en tydlig verksamhetsanknytning, en anpassning av prövningsunderlaget till specifik befattning, möjligheten att väga in övriga omständigheter, t.ex. kompensatoriska skyddsåtgärder, och synsättet att den personkännedom som är kärnan i säkerhetsprövningen byggs upp genom samtal etc. under hela anställningsförhållandet. Det kan också med hänsyn till skyddet för den personliga integriteten finnas tveksamheter med en ordning som bygger på att en bedömning i ett säkerhetsprövningsärende får verkan också för framtida anställningar och uppdrag. En annan sak är att erfarenheter från

tidigare anställningar genom referenstagning självfallet är en del av det samlade underlag som ska värderas och vägas in vid en säkerhetsprövning.

Inom vissa sektorer, t.ex. inom kärnkraftsindustrin finns det personalkategorier (bl.a. i samband med underhållsarbete) som regelmässigt utför liknande arbetsuppgifter under korta och återkommande tidsperioder för olika arbets- eller uppdragsgivare. Det förekommer också myndighetsombildningar som medför att såväl uppgifter som den personal som utför dem flyttas från en myndighet till en annan. För sådana situationer skulle ett klareringsförfarande kunna medföra en enklare och mer ändamålsenlig hantering utan att avkall behöver göras på viktiga principer för säkerhetsprövningen. Samtidigt innebär också en ordning där prövningen mynnar ut i ett intyg med viss giltighetstid i sig ytterligare administration. Även i fråga om kortvariga anställningar och personalomflyttningar behövs dessutom en fungerande uppföljande säkerhetsprövning genom bl.a. bevakning av tillkommande registeruppgifter. Att ett klareringssystem skulle underlätta för arbetstagare och arbetsgivare inom vissa sektorer anser vi inte vara ett tillräckligt skäl för att gå över till ett sådant system. Däremot bör regelverket utformas så att det medger en viss flexibilitet i fråga om krav på säkerhetsprövning för att i möjligaste mån undvika upprepad underlagsinhämtning som inte tillför något nytt i sak och som innebär en onödig pålaga för de som deltar i säkerhetskänslig verksamhet. En sådan ordning kan åstadkommas genom bestämmelser om att den inledande säkerhetsprövningen får göras mindre omfattande om det finns särskilda skäl.

Sammantaget har det för skyddet av verksamhet som har betydelse för Sveriges säkerhet inte kommit fram några påtagliga behov av ett intygsförfarande. Behoven hör i stället samman med deltagande i säkerhetskänslig verksamhet i andra länder och vid mellanfolkliga organisationer. Det är vår bedömning att det finns mervärden i nuvarande system som i viss utsträckning kan behöva förstärkas men som i stället kan riskera att försvagas vid en övergång till ett klareringssystem. Ett system som i grunden fungerar bra bör inte heller ändras i onödan. Vi ser inga fördelar med en genomgripande ändring av nuvarande ordning för säkerhetsprövning. Den fråga som därmed inställer sig är hur den internationella anpassning som behövs kan åstadkommas inom ramen för nuvarande system.

Förändringar för att underlätta det internationella arbetet

Det är således framför allt i två avseenden (informationsklassificering och intygsmöjligheter) som skillnaderna mellan klareringssystem och den modell för säkerhetsprövning som tillämpas i Sverige är påtagliga och i en del fall kan medföra olägenheter i det internationella samarbetet.

Det förhållandevis enhetliga sättet att klassificera känsliga uppgifter utifrån en fyrgradig skala är en viktig grundförutsättning i klareringssystemen eftersom nivåerna för de olika säkerhetsskyddsåtgärderna bestäms utifrån informationssäkerhetsklass. Vi har redan föreslagit att uppgifter som ska skyddas genom säkerhetsskydd ska klassificeras på ett liknande sätt i fyra olika nivåer och att säkerhetsskyddet ska anpassas efter informationssäkerhetsklass. För att tillgodose krav som följer av internationella säkerhetsskyddsåtaganden behöver också grunderna för och underlaget vid säkerhetsprövningen ansluta till det sätt att klassificera information som vi har föreslagit. En sådan anpassning kan åstadkommas genom en justering av grunderna för placering av anställningar i säkerhetsklass (se vidare avsnitt 18.5).

Redan när säkerhetsskyddslagen infördes förutsågs behovet av att efter säkerhetsprövning kunna utfärda intyg som i andra länder och i mellanfolkliga organisationer kan godtas som ett s.k. bevis om klarering (PSCC). Det behovet är bakgrunden till kravet på att en godkänd säkerhetsprövning ska dokumenteras (se 38 § säkerhetsskyddsförordningen). För en person som redan har säkerhetsprövats kan således ett intyg redan i dag ordnas. Det finns dock behov av en reglering som tydligt ger stöd för att utfärda sådana intyg. Det är också angeläget med en större enhetlighet och att en sådan utsedd nationell säkerhetsmyndighet som förutses i bl.a. avtalet om säkerhetsskydd mellan EU:s medlemsstater har ett ansvar för förfarandet. Vidare behöver intyg kunna utfärdas också i vissa situationer där någon säkerhetsprövning inte tidigare har gjorts. I det avseendet är nuvarande bestämmelser om registerkontroll efter ansökan av annan stat eller mellanfolklig organisation i 15 § säkerhetsskyddslagen inte ändamålsenligt utformade. En fungerande ordning där intyg ges för internationella behov förutsätter en tydligare författningsreglering och också vissa organisatoriska förändringar. Sådana förändringar bedömer vi dock kan

genomföras också inom ramen för nuvarande system för säkerhetsprövning (se vidare kapitel 20).

Sammanfattningsvis har vi alltså kommit fram till att behovet av en anpassning till internationella förhållanden inte motiverar ett systemskifte utan mycket väl kan tillgodoses inom ramen för nuvarande ordning. Inte heller finns det andra skäl som motiverar att den nuvarande modellen med säkerhetsprövning ersätts av ett klareringssystem. Hur behovet av anpassning till internationella förhållanden ska tillgodoses i fråga om säkerhetsprövning behandlas dels i avsnittet om placering i säkerhetsklass vid hantering av säkerhetsskyddsklassificerade uppgifter (avsnitt 18.5), dels i avsnitt 20.4 där vi behandlar frågor om säkerhetsintyg för internationella behov.

18.4 Närmare om säkerhetsprövning

Förslag: Vad som ska bedömas inom ramen för säkerhetsprövningen är pålitlighet och lojalitet. Det ska därför uttryckligen anges att omständigheter som kan antas innebära sårbarheter i säkerhetshänseende ska beaktas.

Det ska också tydligare framgå att prövningen förutsätter en grundutredning som, i den utsträckning som följer av bestämmelserna om placering i säkerhetsklass, ska kompletteras med registerkontroll och särskild personutredning.

Vidare ska förtydligas att säkerhetsprövningen är en åtgärd som innebär krav på uppföljning under hela den tid deltagande i den säkerhetskänsliga verksamheten pågår.

Ett tydliggörande i fråga om sårbarhet i säkerhetshänseende

Vad som ska bedömas inom ramen för säkerhetsprövningen framgår av 7 och 11 §§ säkerhetsskyddslagen. I 7 § 3 nämns pålitlighet från säkerhetssynpunkt. I 11 § anges att prövningen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas av säkerhetsskyddslagen och i övrigt pålitlig från säkerhetssynpunkt. Av författningskommentaren till 7 § 3 framgår bl.a. att pålitlighetsbedömningen ska innefatta inte bara en bedömning av om det finns

en risk för att personen i fråga kan göra sig skyldig till spionerier eller dylikt utan också av risken för att bli utsatt för olika påtryckningar eller risker för att den enskilde genom slarv eller på annat oavsiktligt sätt röjer sekretessbelagda uppgifter.[7] Av författningskommentaren till 11 § framgår bl.a. att med lojalitetsprövningen avses i första hand en bedömning av om det t.ex. på grund av bindningar med en främmande makt eller en terroristorganisation finns en risk att personen begår brottsliga handlingar.[8] Vidare framhålls att en person kan utgöra en säkerhetsrisk, även om han eller hon i och för sig ställer sig solidarisk med de intressen som lagen ska skydda. Det anges t.ex. kunna vara fallet om han eller hon på grund av sin livsföring eller levnadsbakgrund löper en risk för att bli utsatt för utpressning eller om det finns en risk för att han eller hon oaktsamt avslöjar sekretessbelagd information. Det betonas därvid att säkerhetsprövningen ska omfatta inte endast en bedömning av den prövades lojalitet, utan även av hans eller hennes pålitlighet från säkerhetssynpunkt i övrigt.

En reformerad säkerhetsskyddslag behöver på ett tydligare sätt än nuvarande lag ta höjd för att säkerhetsskydd innefattar mer än att skydda information från ett konfidentialitetsperspektiv. Vad som behöver bedömas inom ramen för säkerhetsprövningen är därför om en person som ska anställas eller på annat sätt delta i verksamheten kan anses vara lämplig att anförtros säkerhetsskyddsklassificerade uppgifter eller ges tillträde eller annan behörighet i fråga om verksamheter och funktioner som är av betydelse för Sveriges säkerhet eller som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande. Det vidare skyddsperspektivet i kombination med att vissa verksamheter i hög grad verkar förlita sig enbart på en registerkontroll ger anledning till att något ytterligare beröra vilka omständigheter som kan vara av relevans vid en säkerhetsprövning.

Ytterst handlar säkerhetsprövning om att bedöma om en person har tillräckliga förutsättningar och personlig förmåga att genom anställning eller på annat sätt delta i en säkerhetskänslig verksamhet. Det är fråga om en bedömning som görs utifrån ett riskreduceringsperspektiv, dvs. i syfte att undvika inte acceptabla risker

[7] Prop. 1995/96:129, s.75.
[8] a prop., s. 78.

i den säkerhetskänsliga verksamheten. Det förutsätter en helhetsbedömning som medför krav på ett allsidigt underlag och på att bedömningen tydligt relateras till verksamheten och anställningen. En bedömning att en person inte är lämplig för ett deltagande kan också bero på att det inte finns möjlighet att få tillräcklig kunskap om levnadsbakgrunden t.ex. när personen under längre perioder har vistats utomlands. Så kan särskilt vara fallet när det är fråga om vistelse i länder med vilka Sverige i det avseendet inte har ett tillräckligt samarbete.

De värdeord som används i bestämmelserna om säkerhetsprövning, dvs. pålitlighet och lojalitet i säkerhetshänseende, är i sig mångfacetterade. Vissa närmare egenskaper kan nämnas som särskilt relevanta.[9] Sådana egenskaper är ärlighet (för att avgöra pålitlighet), oberoende (vilket relaterar till en persons sårbarhet), lojalitet mot arbetsgivare, samhället och demokratiska principer, samt integritet (vilket är en indikation på förmåga till en korrekt tjänsteutövning som präglas av sakkunskap, rättvisa, ärlighet och likabehandling). Indikatorer som på olika sätt kan resa frågetecken i förhållande till de egenskaper som eftersöks kan vara bl.a. olika slag av brottslighet, subversiv verksamhet och anti-demokratiska aktiviteter, missbruk i olika former, ekonomiskt beroende, oönskad påverkan på grund av t.ex. dubbla lojaliteter, behov av att hemlighålla personliga förhållanden, tecken på bristande integritet och risktagande i onormal omfattning.

För att få ett tillräckligt underlag för en säkerhetsprövning framgår av Säkerhetspolisens vägledning om säkerhetsprövning[10] att frågor kan behöva ställas om bl.a. umgänge (den sökandes vänner och eventuella ovänner), tidigare verksamhet (erfarenheter från tidigare anställningar), ekonomi (inkomst, skulder, förmögenhet och boendeform), bisysslor (eventuella andra åtaganden samt uppgifter om företag och verksamhet), personliga egenskaper (den sökandes ambition, samarbetsförmåga, etik, säkerhetsmed-

[9] Den följande redogörelsen bygger i stor utsträckning på ett informationsunderlag från den Nederländska säkerhetsmyndigheten, Personal Conduct and Circumstances Guide, publicerad januari 2010 av General Intelligence and Security Service, (materialet finns tillgängligt under fliken publikationer på webbplatsen www.aivd.nl). Vid en muntlig presentation för utredningen i september 2012 av psykologen Tuula Kareketo under temat *Försvarsmaktens metod för säkerhetsprövning* redogjordes för liknande resonemang.

[10] http://www.sakerhetspolisen.se/sakerhetsskydd/sakerhetsprovning.html 2014-10-22.

vetande och dylikt) samt intressekonflikter (om den sökande kan hamna i en intressekonflikt vid eventuell anställning).

Som framhålls i Säkerhetspolisens vägledning är sådana frågor nödvändiga att ställa, även om de kan uppfattas som integritetskränkande. Det är viktigt att vid säkerhetsprövningen skapa en medvetenhet om vilka faktorer som kan medföra att den sökande hamnar i en utsatt situation och därmed blir sårbar. Personliga förhållanden kan t.ex. utnyttjas i utpressningssyften, och dålig ekonomi kan fresta en person att begå brottsliga handlingar. Vi återkommer till frågan om säkerhetsprövning och integritetsskydd i avsnitt 18.8. I fråga om vilka omständigheter som är relevanta vid säkerhetsprövningen och möjliga indikatorer på sådana omständigheter är det angeläget med en större tydlighet och utförlighet. Ett sådant underlag kan vara av värde för personer som ska genomgå en säkerhetsprövning, för registerkontrolldelegationen vid Säkerhets- och integritetsskyddsnämnen som prövar frågan om registeruppgifters relevans och för arbetsgivare och andra som utför säkerhetsprövningar. En redogörelse av sådant slag bör dock närmast vara en uppgift för tillsynsmyndigheterna.

Något som har framhållits av bl.a. Säkerhetspolisen och Försvarsmakten är att det är särskilt viktigt att säkerhetsprövningen innefattar underlag och bedömning i fråga om sårbarhet. Att en eventuell sårbarhet är viktig att beakta vid säkerhetsprövningen kan utläsas av förarbetena till säkerhetsskyddslagen. Av tydlighetsskäl, och inte minst av integritetsskyddshänsyn, bör det framgå redan av lagtexten att sårbarhet i säkerhetshänseende ska beaktas. Vi föreslår en sådan komplettering av lagens beskrivning av säkerhetsprövningens närmare syfte.

En grundutredning är en viktig del av säkerhetsprövningen

I förarbetena till säkerhetsskyddslagen betonas att säkerhetsprövning förutsätter en helhetsbedömning där omständigheter av olika slag vägs samman. Det ställer krav på ett tillräckligt underlag. Vad som ingår i säkerhetsprövningen regleras i 27 § säkerhetsskyddslagen och 14 § säkerhetsskyddsförordningen. Viktigt att framhålla är att bestämmelserna redan i dag ger uttryck för att registerkontroll kan vara en del i en säkerhetsprövning men på intet sätt ersät-

ter personkännedom och omdömen om den som ska prövas. Vad som gäller för registerkontroll vid säkerhetsprövning återkommer vi till i avsnitt 18.8–18.10.

I de fall registerkontroll enligt säkerhetsskyddslagen medför att uppgifter lämnas ut för säkerhetsprövning, är det viktigt att de utlämnade uppgifterna inte ges en självständig betydelse. Betydelsen av tidigare brottslighet eller brottsmisstanke behöver relateras till vilket slag av deltagande det är fråga om och omständigheterna i övrigt. Omständigheter kring brotten och den prövades inställning till dem är också av relevans. Det kan t.ex. vara av betydelse, för att kunna bedöma ärlighet och pålitlighet, om den prövade redan före registerkontrollen berättat om tidigare brottslighet.

Det viktigaste momentet i den inledande säkerhetsprövningen är den del som syftar till en tillräcklig personkännedom. Viktiga inslag kan, beroende på vilket deltagande det är fråga om, vara någon form av intervju eller annan form av uppgiftslämnande från den som prövningen avser, kontroll av intyg och betyg och inhämtande av referenser. För att ytterligare understryka detta moments betydelse för säkerhetsprövningen, inte minst i förhållande till registerkontrollen, bör den delen av säkerhetsprövningen särskiljas genom benämningen *grundutredning*.

Vad som krävs i fråga om underlag och bedömning behöver i hög grad anpassas till de skilda former av deltagande i säkerhetskänslig verksamhet som kan omfattas av krav på säkerhetsprövning. Det är t.ex. en väsentlig skillnad på vilket underlag som är nödvändigt för att kunna bedöma lämplighet att få del av säkerhetsskyddsklassificerade uppgifter på t.ex. skyddsnivån kvalificerat hemlig jämfört med underlag för att kunna ges tillträde till förhållandevis mindre känsliga säkerhetsområden vid ett skyddsobjekt.

Om det redan av vad som kommit fram vid grundutredningen står klart att den som prövningen avser inte är lämplig för att delta i den säkerhetskänsliga verksamheten, ska självfallet inte någon registerkontroll göras. Det finns anledning att förtydliga detta förhållande i de närmare bestämmelserna om säkerhetsprövning i den till lagen hörande förordningen.

Ett tydligare uppföljningsansvar

Som vi har betonat tidigare är det angeläget att säkerhetsprövning ses som en process som också pågår under den tid som en person har sin anställning eller sitt uppdrag snarare än ett i tiden avgränsat moment. Under anställningstiden handlar det om att skaffa sig en genom t.ex. regelbundna kontakter och uppföljningssamtal fördjupad personkännedom för att kunna fånga upp t.ex. upplevt missnöje med arbetssituationen, kontaktförsök från främmande makt och liknande som kan påverka risk och mottaglighet för utpressning eller omständigheter som tyder på att personen är i riskzonen vad gäller olika former av missbruk. Vid uppföljning av säkerhetsprövningen kan det finnas anledning att lägga särskild vikt vid den avslutande fasen av anställningen och även vid tillfällen som innebär större förändringar av arbetsuppgifterna. Erfarenheter visar att missnöje inte sällan kan vara ett motiv för att lämna information till främmande makt. Det kan också vara av värde att uppmana den som avslutar sin anställning att höra av sig till arbetsgivaren, om den tidigare anställde t.ex. utsätts för försök att etablera kontakt.

Genom ett tillägg i 11 § i den nuvarande säkerhetsskyddslagen har förtydligats att säkerhetsprövning *får* göras, inte bara innan anställningen påbörjas utan även under pågående anställning eller annat pågående deltagande i verksamheten. Den bestämmelsen fördes in i lagen för att tydliggöra att en säkerhetsprövning också kan göras efter påbörjandet av en anställning t.ex. om arbetsuppgifterna förändras, om det blir fråga om arbete i en högre säkerhetsklass än tidigare eller för att uppdatera en tidigare prövning.[11] Tillägget har dock medfört en viss otydlighet i fråga om den kontinuerliga uppföljningen av säkerhetsprövning för vilken ett *ska*-krav bör finnas.

Sammantaget ser vi behov av att arbeta om och vidareutveckla flera av de grundläggande bestämmelserna om säkerhetsprövning för att tydliggöra vad åtgärden innebär bl.a. i fråga om uppföljningsansvar. Det innefattar även det förhållandet att registerkontrollen innebär en kontinuerlig bevakning av uppgifter som tillförs registren efter den inledande säkerhetsprövningen. Det bevakningsförfarandet medför också att det är viktigt att Säkerhets-

[11] Prop. 2005/06:137 Ändringar i säkerhetsskyddslagen m.m., s. 27

polisen får kännedom om när grund för att utföra kontrollen upphör, t.ex. vid avslutad anställning eller för det fall att den kontrollerade inte anställs. Det finns anledning att i den till lagen hörande förordningen ta in en bestämmelse om sådan anmälningsskyldighet.

18.5 Placering i säkerhetsklass vid hantering av säkerhetsskyddsklassificerade uppgifter

Förslag: Bestämmelserna om placering av anställningar i säkerhetsklass anpassas till förslaget om en övergång från skydd av hemliga uppgifter till skydd av säkerhetsskyddsklassificerade uppgifter samt förslaget om att skyddsnivån för sådana uppgifter ska bestämmas av uppgiftens informationssäkerhetsklass. Att den berörde får del av säkerhetsskyddsklassificerade uppgifter som klassificerats som kvalificerat hemliga, hemliga eller konfidentiella ska i princip styra placeringen i säkerhetsklass. Om uppgifter på en högre skyddsnivå förekommer endast i mindre omfattning, ska dock anställningen placeras i nästa lägre klass.

Två huvudsakliga grunder för placering i säkerhetsklass

Ett grundläggande moment i nuvarande ordning för säkerhetsprövning är att befattningar där den som deltar i verksamheten får del av känsliga uppgifter i förväg identifieras och placeras i säkerhetsklass. Ordningen innebär att säkerhetsprövningen i fråga om de kvalificerade momenten registerkontroll och särskild personutredning ovillkorligen knyts till de krav som verksamheten eller befattningen ställer i det enskilda fallet. I förarbetena till säkerhetsskyddslagen framhålls att den ordning som innebär att man i förväg bestämt vilka verksamheter som är aktuella för kontroll och på vilken nivå denna ska ske ger en stadga och fasthet åt systemet. [12] Vi instämmer i den uppfattningen, och befattningar avseende säkerhetskänslig verksamhet bör därför även i fortsättningen

[12] SOU 1994:149, s. 173.

placeras i säkerhetsklass. Vi anser dessutom, vilket vi återkommer till i avsnitt 18.6, att den registerkontroll som i dag görs med stöd av 14 § säkerhetsskyddslagen (skydd mot terrorism) ska inordnas i systemet med säkerhetsklassplacering. En sådan ordning kan i linje med vårt förslag i avsnitt 12.3 åstadkommas genom vidare kriterier för placering i säkerhetsklass. Placering i säkerhetsklass bör således göras inte enbart när det är fråga om ett deltagande i säkerhetskänslig verksamhet där den som deltar kan komma att få del av säkerhetsklassificerade uppgifter. Vi återkommer till övriga kriterier för placering i säkerhetsklass i det efterföljande avsnittet och behandlar nu först placering i säkerhetsklass i situationer där den som ska delta i säkerhetskänslig verksamhet får del av säkerhetsskyddsklassificerade uppgifter.

Övergången från hemliga uppgifter till säkerhetsskyddsklassificerade uppgifter

Grunden för placering i säkerhetsklass är i dag att den anställde (eller den som på annat sätt deltar i verksamheten) i olika stor omfattning får del av hemliga uppgifter, dvs. uppgifter som omfattas av sekretess och som i en varierande grad är av betydelse för rikets säkerhet. Vi har i avsnitt 12.2 föreslagit en övergång från skydd av hemliga uppgifter till skydd av säkerhetsskyddsklassificerade uppgifter. Sammantaget innebär den övergången att kraven på säkerhetsskydd för uppgifter som är av betydelse för Sveriges säkerhet på ett tydligare sätt än i dag gäller såväl när sådana uppgifter förekommer vid myndigheter som när de finns i enskild verksamhet. Dessutom omfattas även uppgifter som ska skyddas enligt ett för Sverige folkrättsligt förpliktande åtagande om säkerhetsskydd. Övergången till säkerhetsskyddsklassificerade uppgifter behöver återspeglas i grunderna för placering av anställningar i säkerhetsklass.

Anpassning till förslaget om klassificering av information

I dag är säkerhetsklasserna tre till antalet. Placeringen bestäms av en kombination av två faktorer; i vilken omfattning den berörde kan få del av sekretessbelagda uppgifter och om det är fråga av

uppgifter av *synnerlig betydelse* för rikets säkerhet eller uppgifter av *betydelse* för rikets säkerhet. I fråga om placering i säkerhetsklass 3 gäller ett uttryckligt krav på skada av viss storlek (men för rikets säkerhet som inte är ringa) om uppgifterna röjs för obehöriga. När det gäller de högre säkerhetsklasserna har inte något motsvarande skaderekvisit ansetts påkallat. Av författningskommentaren till 17 § säkerhetsskyddslagen framgår att skälet till den skillnaden är att det får antas att det alltid föreligger en betydande risk för skada om uppgifter av synnerlig betydelse för rikets säkerhet röjs för obehöriga.[13]

Vi har tidigare föreslagit att säkerhetsskyddsklassificerade uppgifter ska klassificeras utifrån nivåerna kvalificerat hemlig, hemlig, konfidentiell och begränsad samt att nivån på säkerhetsskyddet för sådana uppgifter ska anpassas efter informationssäkerhetsklass. En sådan anpassning av nivån på säkerhetsskyddet är (som vi behandlat tidigare) angelägen inte minst med hänsyn till behovet av en ökad tydlighet i fråga om för Sverige folkrättsligt förpliktande åtaganden om säkerhetsskydd. Det skulle kunna innebära att fler anställningar behöver placeras i en högre säkerhetsklass. Vår bedömning är dock att så inte behöver bli fallet. En konsekvens av den gällande ordningen i fråga om grunder för placering i säkerhetsklass är nämligen att översättningsproblematiken i dag kan leda till placering i en onödigt hög säkerhetsklass. Det utrymme för differentiering som fyra informationssäkerhetsklasser innebär medför goda förutsättningar för en väl avvägd skyddsnivå. En bättre ordning är därför att grunderna för placering i säkerhetsklass, på samma sätt som är vanligt i andra länder, i högre grad än i dag styrs av uppgifternas skyddsnivå. Att fullt ut övergå till en ordning där enbart förekomsten av uppgifter på en viss nivå avgör placering i säkerhetsklass anser vi dock inte vara lämpligt. En sådan ordning skulle kunna medföra att betydligt fler befattningar än i dag skulle behöva placeras i framför allt den högsta säkerhetsklassen enbart på grund av en eventuell förekomst av någon enstaka uppgift på nivån kvalificerat hemlig. En sådan ordning är inte rimlig. Uppgifter i mindre omfattning på t.ex. nivån kvalificerat hemlig ska därför medföra placering i nästa lägre säkerhetsklass.

[13] a. prop., s.81.

Information på nivån *begränsad* bör överhuvudtaget inte föranleda några krav på placering i säkerhetsklass med anledning av det ringa skada som ett röjande kan medföra. Inte heller medför de internationella säkerhetsskyddsåtagandena något krav på att anställda och andra som hanterar uppgifter på nivån *restricted* eller motsvarande ska vara klarerade eller på motsvarande sätt godkända i säkerhetshänseende.

18.6 En ny grund för placering i säkerhetsklass

Förslag: Bestämmelserna om placering i säkerhetsklass utvidgas till att omfatta även befattningar i verksamhet som, även om den inte innebär hantering av säkerhetsskyddsklassificerade uppgifter, är att anse som säkerhetskänslig (i övrigt säkerhetskänslig verksamhet). Den nya grunden för placering i säkerhetsklass innebär att den registerkontroll som i dag görs med stöd av 14 § säkerhetsskyddslagen (skydd mot terrorism) inordnas i systemet med säkerhetsklasser vilket gör systemet mer enhetligt och logiskt.

Att den berörde genom att delta i verksamheten har möjlighet att orsaka synnerligen allvarlig skada, allvarlig skada eller en inte obetydlig skada för Sveriges säkerhet ska i princip styra placeringen i säkerhetsklass. En anställning eller annat deltagande i säkerhetskänslig verksamhet ska dock även placeras i säkerhetsklass, om krav på säkerhetsprövning följer av ett internationellt säkerhetsskyddsåtagande t.ex. i fråga om luftfartsskydd eller hamnskydd.

En kompletterande grund för placering i säkerhetsklass

Nuvarande bestämmelser om säkerhetsprövning gäller också i verksamheter som särskilt behöver skyddas mot terrorism. Däremot gäller inte bestämmelserna om placering av befattningar i säkerhetsklass för sådan verksamhet. Grunden för registerkontroll som ett led i säkerhetsprövning i dessa fall finns i stället i 14 § säkerhetsskyddslagen. Där anges att registerkontroll får göras om det behövs för skyddet mot terrorism och det finns särskilda skäl.

Paragrafen innehåller vidare ett bemyndigande för regeringen att meddela föreskrifter.[14] Sådana föreskrifter om registerkontroll till skydd mot terrorism finns i 26 och 26 a §§ säkerhetsskyddsförordningen. Bestämmelserna innebär i huvudsak att den som kan antas komma att anställas eller på annat sätt delta vid verksamheten vid flygplatser och skyddsobjekt av olika slag får registerkontrolleras. Det anges särskilt att sådan kontroll får göras endast om skyddsbehovet inte kan tillgodoses på annat sätt.

Vi har föreslagit en förändrad systematik för säkerhetsskyddslagen där hanteringen av känsliga uppgifter inte ges någon särställning i säkerhetsskyddshänseende. Förändringen är ett uttryck för att säkerhetsskyddet i en reformerad säkerhetsskyddslag inte enbart är inriktat på att skydda uppgifter från ett konfidentialitetsperspektiv. Den nuvarande inriktningen i fråga om säkerhetsprövning, som i sin tur bygger på den tidigare personalkontrollen, har en tydlig inriktning mot just ett sådant mer begränsat skydd av uppgifter.[15] Ett motiv till att välja en annan ordning för anläggningar och annat som behöver skyddas mot terrorism och att hålla isär de olika slagen av kontroll ansågs vara att det skyddet hade en annan inriktning som påverkade prövningen.[16] Ursprungligen fanns vid s.k. § 14–prövningar en begränsning till uppgifter om vissa slag av brott. Bestämmelsen är dock sedan flera år tillbaka ändrad på så sätt att omfattningen i fråga om vilka uppgifter som får lämnas ut är densamma som vid placering i säkerhetsklass 3.[17]

Som vi nämnt tidigare ser vi inte att det i dag i fråga om genomförandet av säkerhetsprövningen finns behov av att sätta upp någon skiljelinje mellan olika slag av befattningar. Övergången från skydd av verksamheter som särskilt behöver skyddas mot terrorism till skydd av i övrigt säkerhetskänslig verksamhet innebär i fråga om säkerhetsprövning att det inte bara är presumtiva terrorister som prövningen ska fånga upp.

En fördel med ordningen med säkerhetsklassade befattningar är att momentet där befattningar i förväg identifieras ger en stadga åt förfarandet som är viktig från integritetssynpunkt. Det är ett argu-

[14] Bemyndigandet omfattar inte riksdagen och dess myndigheter.
[15] SOU 1994:149, s. 180.
[16] a. bet., s. 183.
[17] Ändrad lydelse av 22 § säkerhetsskyddslagen till följd av riksdagens antagande av Prop. 2005/06:137 Ändringar i säkerhetsskyddslagen m.m.

ment som vi anser vara lika viktigt i fråga om all säkerhetskänslig verksamhet. Det gäller särskilt när den del av säkerhetsskyddet som inte avser säkerhetsskyddsklassificerade uppgifter ges ett mer flexibelt tillämpningsområde.

På samma sätt som för anställningar som innebär hantering av säkerhetsskyddsklassificerade uppgifter bör således anställningar som av annan anledning är av betydelse för Sveriges säkerhet medföra placering i säkerhetsklass. Att ytterligare komplicera säkerhetsklassindelningen genom att skapa nya klasser bedöms inte ge något mervärde. En sådan uppdelning i ytterligare klasser kan också vid den praktiska tillämpningen vara svår att förhålla sig till. En vanligt förekommande situation kan vara att en person som ska ges tillträde till anläggningar som är av betydelse från säkerhetssynpunkt samtidigt kan anses få del av säkerhetsskyddsklassificerade uppgifter om skyddet av anläggningen vilket redan det kan motivera en placering i säkerhetsklass.

Placering utifrån en skadebedömning

För befattningar som innebär hantering av säkerhetsskyddsklassificerade uppgifter kommer säkerhetsklassplaceringen att vara given utifrån den skyddsnivå (kvalificerat hemlig, hemlig eller konfidentiell) som har bestämts vid en informationssäkerhetsklassificering. Vilken grad av skada som en anställd eller någon som på annat sätt ska delta i verksamheten kan orsaka genom att obehörigen röja en uppgift har på så sätt bedömts redan på ett tidigare stadium. För verksamhet som är säkerhetskänslig på annan grund än hantering av säkerhetsskyddsklassificerade uppgifter har inte någon motsvarande formell förtida skadebedömning gjorts. Däremot bör en konsekvensbedömning ha gjorts inom ramen för verksamhetens säkerhetsskyddsanalys. För att kunna bedöma t.ex. vilka it-system som behöver ett säkerhetsskydd är det nödvändigt att bedöma vilka konsekvenser ett angrepp som från ett tillgänglighets- eller riktighetsperspektiv stör viktiga funktioner skulle ha. På liknande sätt behöver konsekvenserna av t.ex. ett terroristangrepp mot en flygplats eller en kärnkraftanläggning bedömas innan säkerhetsskyddsåtgärder vidtas för att i olika avseenden begränsa tillträdet till sådana platser och anläggningar. Eftersom en konsekvens-

bedömning behöver göras redan med anledning av kravet på en säkerhetsskyddsanalys bör tillräckliga förutsättningar finnas för att också utifrån en sådan bedömning avgöra inte bara behovet av säkerhetsskyddsåtgärder i stort utan också behovet av att placera in befattningar i säkerhetsklass.

Ett alternativ till placering i säkerhetsklass utifrån en skadebedömning skulle kunna vara att inordna de nuvarande § 14-prövningarna i säkerhetsklass 3. En sådan lösning är logisk mot bakgrund av att prövningsunderlaget i fråga om registerkontroll har samma omfattning.[18] Samtidigt ser vi behov av möjlighet till en viss differentiering mellan olika slag av deltagande. Det gäller inte minst när utrymme ges för att inkludera även andra verksamheter än de som i dag träffas av regleringen om skydd mot terrorism, t.ex. vissa kritiska delar av för samhället vitala it-system. Gemensamt för personalkategorier som i dag prövas inom ramen för 14 § är i regel någon form av fysiskt tillträde till platser och anläggningar som ansetts behöva skyddas särskilt mot terrorism. Graden av skada som en person till följd av sitt deltagande i en säkerhetskänslig verksamhet har möjlighet att orsaka varierar beroende på anläggning och tillträdesbehörighetens omfattning. Som regelverket är utformat i dag är det i fråga om registerkontroll ingen formell skillnad vad gäller underlag till säkerhetsprövningen avseende t.ex. en person anställd vid en butik på en flygplatsterminal eller någon som, utan att få del av känsliga uppgifter, utför service av SCADA-system[19] som reglerar dammluckor vid en större vattenkraftanläggning av central betydelse för Sveriges energiförsörjning.

En mer ändamålsenlig säkerhetsprövning förutsätter att omfattningen av prövningsunderlaget också i fråga om registerkontroll kan anpassas beroende på vad anställningen eller deltagandet innebär. I linje med vad som föreslås gälla för hantering av säkerhetsskyddsklassificerade uppgifter bör en indelning av de säkerhetsklassade befattningarna som här är i fråga göras utifrån skadenivåerna *synnerligen allvarlig*, *allvarlig* eller *inte obetydlig skada* för Sveriges säkerhet. Det innebär en alternativ grund för placering i säkerhetsklass 1, 2 eller 3. Något formellt krav på en föregående

[18] Jfr 18, 21 § 2 och 22 § säkerhetsskyddslagen.
[19] SCADA står för *Supervisory Control And Data Acquisition* och avser system för styrning och övervakning av bl.a. industriprocesser, energiproduktion och annan processövervakning.

klassificering utifrån en skadebedömning, motsvarande det som föreslås gälla för säkerhetsskyddsklassificerade uppgifter, bör inte gälla avseende anläggningar och liknande som utgör i övrigt säkerhetskänslig verksamhet. Som framhållits tidigare bör dock en sådan skadebedömning ha gjorts vid den säkerhetsskyddsanalys som ska utgöra grunden för verksamhetens säkerhetsskydd. Det bör också i sammanhanget understrykas att ett beslut om placering i säkerhetsklass behöver föregås av en noggrann befattningsanalys eller motsvarande analys av det deltagande det är fråga om. Sådana analyser är nödvändiga inte minst för att av integritetsskyddshänsyn motverka en godtycklighet som kan innebära obefogade kontroller (se vidare vårt förslag i 18.8). Av samma anledning bör inte beslut om placering i säkerhetsklass, annat än i undantagsfall, få fattas av enskilda verksamheter (se vidare avsnitt 18.10).

Vår bedömning är att den registerkontroll som i dag görs med stöd av 14 § säkerhetsskyddslagen bör kunna rymmas inom i första hand säkerhetsklass 3. Utrymmet för att placera anställningar i säkerhetsklass 1 och 2 bör däremot vara begränsat. En placering i en högre säkerhetsklass kan vara motiverad om t.ex. en anställning innebär att en person behöver anförtros tillgång till vissa anläggningar eller system av kritisk betydelse för landets elförsörjning.

Internationella säkerhetsskyddsåtaganden

Förslaget i avsnitt 18.5 om säkerhetsklassplacering av den som får del av säkerhetsskyddsklassificerade uppgifter tillgodoser även krav på säkerhetsskydd som följer av internationella säkerhetsskyddsåtaganden. De internationella säkerhetsskyddsåtagandena avser emellertid inte enbart skydd av uppgifter. Det finns också åtaganden som tar sikte på skydd av anläggningar, objekt och platser bl.a. inom områdena luftfarts-, hamn- och sjöfartskydd. Det finns i dag bestämmelser om registerkontroll av bl.a. den som ska anställas eller på annat sätt delta i verksamhet som har betydelse för luftfartsskyddet, om det följer av en internationell överenskommelse som Sverige tillträtt eller av en bindande EU-rättsakt på området för luftfartsskydd (26 § säkerhetsskyddsförordningen). Också åtaganden i förhållande till mellanfolkliga organisationer t.ex. Nato kan innebära ett behov av att skydda annat än uppgifter.

Merparten av de anställningar som kan aktualisera säkerhetsprövning med anledning av internationella säkerhetsskyddsåtaganden i fråga om t.ex. luftfartsskydd kommer att behöva placeras i säkerhetsklass redan av hänsyn till Sveriges säkerhet. Att därför ha en särskild lösning för situationer där så inte är fallet förefaller inte motiverat. En rimlig ordning bör således kunna vara att också säkerhetsprövning med registerkontroll mot bakgrund av sådana internationella säkerhetsskyddsåtaganden som här är i fråga föregås av en placering i en säkerhetsklass. Av bestämmelsen om placering i säkerhetsklass ska därför framgå att, utöver vad som följer av bestämmelserna om säkerhetsskyddsklassificerade uppgifter, ett deltagande ska placeras i säkerhetsklass, om krav på säkerhetsprövning följer av ett internationellt säkerhetsskyddsåtagande. Vilka krav på säkerhetsskydd som ställs bör avgöra valet av säkerhetsklass. Som anförts tidigare bör det t.ex. i fråga om luftfartsskydd i huvudsak handla om säkerhetsklass 3.

18.7 Medborgarskapskravet i fråga om säkerhetsklassad anställning tas bort

Förslag: Kravet på att en säkerhetsklassad anställning vid staten, en kommun eller ett landsting får innehas endast av den som är svensk medborgare tas bort.

Gällande ordning

En säkerhetsklassad anställning vid staten, en kommun eller ett landsting får i dag innehas endast av den som är svensk medborgare (29 § säkerhetsskyddslagen). Den som utöver svenskt medborgarskap har ett ytterligare medborgarskap anses uppfylla kravet på svenskt medborgarskap.

Regeringen får i enskilda fall medge undantag från kravet. Regeringen prövar i regel ett 30-tal sådana ärenden per år. Ärendena omfattar olika slag av befattningar bl.a. inom elförsörjningen och kriminalvården. Undantag från medborgarskapskravet har medgetts i de allra flesta ärendena.

Direktiven och vårt uppdrag

En fråga som tas upp i våra direktiv är om kravet på svenskt medborgarskap för att inneha en anställning som placerats i säkerhetsklass bör förändras, i vart fall för de lägre säkerhetsskyddsklasserna.

I direktiven konstateras (utan att det utvecklas närmare) att det finns anställningar inom totalförsvaret där medborgarskapet är av väsentlig betydelse. Samtidigt framhålls att kravet på svenskt medborgarskap kan försämra möjligheterna att rekrytera kompetent personal inom verksamheter som har behov av specialistkompetens som inte finns att tillgå här i landet. En annan aspekt som tas upp är att kravet på svenskt medborgarskap kan innebära svårigheter att åstadkomma en jämnare personalsammansättning med avseende på etnisk bakgrund. Kriminalvården nämns som ett exempel på en verksamhet som arbetar aktivt för att öka andelen anställda med utländsk bakgrund samtidigt som en stor del av anställningarna är placerade i säkerhetsklass.

Säkerhetsklassade anställningar förekommer i stor utsträckning inom bl.a. Försvarsmakten, Regeringskansliet och Polismyndigheten. För många av de säkerhetsklassade anställningarna vid dessa myndigheter innebär även annan lagstiftning krav på svenskt medborgarskap. [20] Vårt uppdrag att överväga förändringar av kravet på svenskt medborgarskap avser de krav som följer av säkerhetsskyddslagen. Det innebär att, även om kravet på svenskt medborgarskap förändras i säkerhetsskyddslagen, så kan ändå annan lagstiftning utgöra ett hinder för utländska medborgare att inneha vissa anställningar som i regel föranleder placering i säkerhetsklass. Det gäller t.ex. många befattningar i Försvarsmakten och anställning som polis. För andra befattningar, t.ex. inom kriminalvården, är det endast regleringen om placering i säkerhetsklass som innebär krav på svenskt medborgarskap.

[20] Bestämmelser om krav på svenskt medborgarskap för vissa anställningar finns bl.a. i 11 kap. 11 § och 12 kap. 6 § regeringsformen samt 5 och 6 §§ lagen (1992:260) om offentlig anställning.

Tidigare överväganden avseende krav på svenskt medborgarskap

Medborgarskapets principiella betydelse som krav för vissa anställningar har behandlats av Kommittén om medborgarskap i betänkandet Medborgarskapskrav i svensk lagstiftning (SOU 2000:106). Kommittén tog bl.a. upp att medborgarskapskrav i lagstiftningen i viss utsträckning bygger på förutsättningen att svenska medborgare har förståelse för och känner lojalitet med svenska intressen. Den som är svensk medborgare förutsätts t.ex. dela de allmänna värderingar och den samsyn som råder beträffande övergripande demokratiska principer. Kommittén betonade att det förhållandet att en person är svensk medborgare dock inte är någon garanti för att hon eller han sympatiserar eller är lojal med det staten och demokratin står för och framhöll att det finns åtskilliga nutida exempel på detta, bl.a. fascistiska grupperingar. Kommittén konstaterade också att den etniska bakgrunden är en del av den enskildes identitet och att man därför får räkna med att dubbla lojaliteter kan finnas hos en person, oavsett om denne är svensk medborgare, har dubbelt medborgarskap eller är utländsk medborgare. Mot den bakgrunden framhöll kommittén att i det enskilda fallet medborgarskapet inte är någon bra värdemätare för lojaliteten till ett land. Kommittén kom till slutsatsen att, även om medborgarskapet inte ger några garantier i nämnda avseenden, det ändå framstår som motiverat att på ett mer allmänt plan beakta medborgarskapet som en indikation på att den enskilde är lojal mot Sverige och svenska intressen. Mot den bakgrunden gjorde kommittén bedömningen att hänsynen till rikets säkerhet och förhållandet till andra stater kan motivera att t.ex. vissa statliga anställningar förbehålls svenska medborgare.

Kommitténs uppdrag omfattade även medborgarskapskravet i säkerhetsskyddslagen. I det avseendet kom kommittén till den slutsatsen att det, utifrån tillgången till information som är av synnerlig betydelse för rikets säkerhet, var motiverat att anställningar vid staten eller i kommun eller landsting i säkerhetsklasserna 1 och 2 även i fortsättningen skulle vara förbehållna svenska medborgare. I fråga om säkerhetsklass 3 kom kommittén till slutsatsen att det, på grund av bristfälligt underlag avseende vilka slag av anställningar som omfattas, inte var möjligt att lämna något förslag och att frågan behövde utredas vidare.

Medborgarskapets betydelse i fråga om skyddet mot brottslighet riktad mot statliga intressen behandlades också i lagstiftningsärendet varigenom möjlighet till dubbelt medborgarskap infördes. Av förarbeten till den lagändringen[21] kan utläsas att Säkerhetspolisen och Försvarsmakten framfört att det erfarenhetsmässigt är andra faktorer än ett eventuellt dubbelt medborgarskap som är avgörande för om en person kommer att ägna sig åt sådan brottslig verksamhet som utgör en säkerhetsrisk för ett land. I fråga om erfarenheter från andra länder framhölls att de säkerhetsmässiga aspekterna på dubbelt medborgarskap internationellt inte upplevs som något problem. Mot den bakgrunden konstaterade 1997 års medborgarskapskommitté att det visserligen var så att dubbla lojaliteter och lojalitetskonflikter under vissa förhållanden kunde medföra säkerhetsrisker, men att de farhågor som i olika sammanhang framförts om att dubbelt medborgarskap skulle medföra säkerhetsrisker hade varit överdrivna. Kommittén ansåg att det dubbla medborgarskapet i nämnda avseende hade en synnerligen underordnad betydelse. I den efterföljande propositionen om dubbelt medborgarskap ansåg regeringen att säkerhetsaspekterna inte utgör ett hinder mot att tillåta dubbelt medborgarskap fullt ut.[22]

Krav på svenskt medborgarskap har i stor utsträckning tagits bort i lagstiftningen

Utvecklingen i fråga om behörighet till statliga anställningar har generellt sett gått i riktning mot att begränsa de rättsliga skillnaderna mellan de som är svenska medborgare och den övriga befolkningen. I stället för medborgarskapet har bosättningen fått en ökad betydelse för rättigheter och skyldigheter. En inte obetydlig roll i denna utveckling torde det svenska medlemskapet i EU ha spelat. I och med medlemskapet gäller enligt artikel 18 i Fördraget om Europeiska unionens funktionssätt en likabehandlingsprincip, även kallad icke-diskrimineringsprincipen, som innebär ett förbud mot varje form av diskriminering, direkt eller indirekt, på grund av nationalitet inom fördragets tillämpningsområde. Detta grundläg-

[21] 1997 års medborgarskapskommitté i slutbetänkandet Svenskt medborgarskap (SOU 1999:34), s. 159 ff.
[22] Prop. 1996/2000:147 Lag om svenskt medborgarskap, s. 22 f.

gande förbud kompletteras av mer precist utformade diskrimineringsförbud på olika områden. Undantag finns emellertid från förbudet, t.ex. i fråga om vissa anställningar i staten och andra offentliga organ.

I regeringsformen är huvudregeln att det inte görs någon skillnad mellan svenska medborgare och andra när det gäller behörighet för statliga anställningar. Detta har motiverats dels av intresset att få så kvalificerade innehavare som möjligt av offentliga anställningar, dels av önskemålet om en intensifiering av det mellanfolkliga samarbetet. Tidigare innehöll regeringsformen flera undantag från denna huvudregel. Efter förslag i regeringens proposition 2009/10:80 En reformerad grundlag gjordes ändringar som innebar bl.a. att regeringsformen numera innehåller bestämmelser om medborgarskapskrav endast för de viktigaste anställningarna eller uppdragen hos de högsta statsorganen samt hos organ med funktioner inom ramen för den konstitutionella kontrollen. I övrigt får krav på svenskt medborgarskap för behörighet att inneha en anställning eller utöva ett uppdrag hos staten eller en kommun ställas upp endast i lag eller enligt förutsättningar som anges i lag. I den nämnda propositionen framhöll regeringen även att det krav på svenskt medborgarskap som gäller för ett stort antal statliga anställningar eller andra uppdrag i många fall har vållat olägenheter. [23] I det avseendet hänvisade regeringen till den översyn av krav på svenskt medborgarskap och andra krav relaterade till medborgarskap i lagstiftningen som redovisats i slutbetänkandet från Kommittén om medborgarskapskrav och till remissyttrandena över betänkandet.

Svenskt medborgarskap ska inte vara ett behörighetskrav för säkerhetsklassade anställningar

Som nämnts kom Kommittén om medborgarskap till slutsatsen att medborgarskapet i det enskilda fallet inte är någon bra värdemätare för lojaliteten till ett land men att det på ett mer allmänt plan ändå bör kunna användas som en indikation i det avseendet. Kommitténs bedömning var att medborgarsskapskravet skulle behållas i

[23] Prop. 2009/10:80 En reformerad grundlag, s. 238.

vart fall för de högre säkerhetsklasserna. Ett förhållande vars betydelse inte närmare belystes av kommittén är att säkerhetsprövning enligt säkerhetsskyddslagen ger utrymme för en individuell bedömning av omständigheter som kan påverka en persons lojalitet till Sverige.[24]

Som vi behandlat i avsnitt 18.4 innebär säkerhetsprövning en bedömning av en persons lämplighet för att delta i säkerhetskänslig verksamhet från ett riskreducerings- och helhetsperspektiv. Prövningen ska enligt förarbetena till säkerhetsskyddslagen bestå i en allsidig bedömning varigenom man i möjligaste mån skaffar sig en bild av personens allmänna livssituation och levnadsbakgrund. Det innebär att prövningen i regel förutsätter ett brett beslutsunderlag och att omständigheter av olika slag hänförliga både till den som prövningen avser och till det deltagande som är aktuellt ska vägas samman. En enskild omständighet bör därför i regel inte ha någon självständig betydelse vid säkerhetsprövningen.

Kraven på säkerhetsprövning innebär således att omständigheter av olika slag som kan påverka lojaliteten i säkerhetshänseende alltid ska vägas in. En sådan omständighet kan t.ex. vara ett dubbelt medborgarskap[25] eller andra band till ett annat land eftersom det kan vara en indikation på en lojalitetskonflikt som skulle kunna medföra en särskild sårbarhet vid deltagande i en säkerhetskänslig verksamhet. På samma sätt bör det vara fullt möjligt att också värdera och väga in betydelsen av att en person inte har svenskt medborgarskap. Att svenskt medborgarskap saknas kan, men behöver inte, bero på en kort vistelsetid i Sverige. Att en person har bott utomlands större delen av sitt liv eller under längre perioder kan, beroende på omständigheterna i det enskilda fallet, också innebära påtagliga svårigheter att få fram ett tillräckligt underlag för att kunna göra bedömningen att personen i säkerhetshänseende är lämplig för att delta i en säkerhetskänslig verksamhet. Omständigheter av sådant slag kan och bör beaktas inom ramen för säkerhetsprövningen.

Inom ramen för säkerhetsprövningen kan också olika kompensatoriska åtgärder användas för att reducera eventuella risker och

[24] Den omständigheten vägdes däremot in vid regeringens överväganden om att tillåta dubbelt medborgarskap fullt ut (Prop. 1996/2000:147, s. 22).
[25] Se föregående not.

sårbarheter som kommit fram under säkerhetsprövningen. Det kan handla om att undvika ansvar för arbetsuppgifter där lojalitetskonflikter i förhållande till t.ex. ett annat land kan medföra en särskild utsatthet för eventuella påtryckningar från främmande makt.[26] Självfallet kan det finnas anledning att reducera sådana risker även i fråga om en person som har svenskt medborgarskap.

Att när möjlighet till en mer allsidig prövning finns behålla ett behörighetskrav, som dessutom framhållits inte vara en särskilt tillförlitlig indikator på en persons lojalitet till ett land, framstår som otillfredsställande.

Å andra sidan skulle mot det nu förda resonemanget kunna invändas att medborgarskapskravet ändå fyller en funktion eftersom säkerhetsprövningen, som vi redovisat tidigare, i många verksamheter inte genomförs på ett sätt som innebär en allsidig belysning av levnadssituationen. Ett svenskt medborgarskap representerar åtminstone en formell bindning till Sverige och lojalitet med svenska intressen. Att tillämpningen av bestämmelserna om säkerhetsprövningen i dag har brister skulle kunna vara ett skäl för att inta en försiktig hållning i fråga om att ta bort medborgarskapskravet åtminstone för de högre säkerhetsklasserna. Att av den anledning ha kvar kravet för svenskt medborgarskap vore dock en logisk kullerbytta och skulle dessutom kunna bidra till att cementera en ordning där säkerhetsprövningen inte utförs på det sätt den bör.

Att kravet på svenskt medborgarskap är uppfyllt skulle också kunna felaktigt tas till intäkt för att frågor om bindningar till ett annat land, som kan kännas besvärande att ställa och att utreda, inte behöver tas upp under säkerhetsprövningen. En fråga som kommit upp och som anknyter till detta är om ett slopande av medborgarskapskravet kan ställa arbetsgivare inför risken att anklagas för diskriminering t.ex. i situationer där det inte är möjligt att få fram ett tillförlitligt prövningsunderlag på grund av en tidigare bosättning i från säkerhetssynpunkt tveksamma länder. En sådan risk kan finnas också i andra fall när en person med utländsk härkomst ska säkerhetsprövas. Självfallet måste en säkerhetsprövning i alla avseenden enbart grundas på sakliga skäl.

[26] Jfr regeringens överväganden i a. prop., s. 23.

Vidare gäller kravet på svenskt medborgarskap endast säkerhetsklassade anställningar inom staten, kommuner och landsting. En utländsk medborgare kan således i andra avseenden inneha en anställning eller ett uppdrag i det allmännas verksamhet som omfattas av krav på säkerhetsskydd. Det gäller bl.a. för sådant deltagande i verksamhet som på grund av bestämmelserna i 14 § säkerhetsskyddslagen (skydd mot terrorism) kan föranleda en registerkontroll.

Till följd av att utvecklingen fört med sig att säkerhetskänslig verksamhet i högre grad bedrivs av enskilda och eftersom myndigheter i större utsträckning på mer eller mindre permanent basis behöver använda sig av externa leverantörer framstår i dag en särskild ordning för säkerhetsklassade anställningar i det allmännas verksamhet som mindre ändamålsenlig. Ett belysande exempel är drift och underhåll av it-system. Den nuvarande ordningen innebär att, även om arbetsuppgifterna för en it-tekniker är identiska och innebär samma tillgång till uppgifter som har betydelse för Sveriges säkerhet, så är kravet på svenskt medborgarskap beroende av om det är fråga om en säkerhetsklassad anställning vid en myndighets interna it-avdelning eller hos en extern leverantör som myndigheten anlitar. Visserligen kan göras gällande att myndigheten har en valfrihet i fråga om att lägga ut verksamhet på externa leverantörer och alltså kan välja att undvika sådana situationer. Samtidigt har utvecklingen medfört att också myndigheter vars verksamhet är av betydelse för Sveriges säkerhet i hög grad är beroende av externa leverantörer. Valfriheten i fråga om hur t.ex. myndighetens behov av it-drift ska tillgodoses kan därför i många avseenden i praktiken vara begränsad.

Ett annat exempel på vad gällande ordning i fråga om krav på svenskt medborgarskap innebär kan hämtas från elförsörjningen. För befattningar som avser arbetsuppgifter i fråga om driftcentraler hos Affärsverket svenska kraftnät gäller krav på svenskt medborgarskap, däremot inte för personal vid driftcentraler hos Vattenfall.

Det finns ytterligare argument för att ändra den gällande ordningen. En grundförutsättning för ett väl fungerande säkerhetsskydd är, som vi ser det, att ansvaret för skyddet ligger på en verksamhetsnivå. Mot den bakgrunden kan ordningen där regeringen prövar frågan om medborgarskapets betydelse sättas i fråga också

av andra skäl än den principiella hållningen att regeringen inte bör vara beslutsfattare i förvaltningsärenden. Det argumentet har en särskild bäring i fråga om medborgarskapskravet för den lägre säkerhetsklassen. Till följd av de förändringar vi har föreslagit i tidigare avsnitt om att inordna den nuvarande registerkontrollen till skydd mot terrorism i systemet med säkerhetsklasser skulle antalet sådana ärenden kunna öka avsevärt.

Slutligen innebär den nuvarande ordningen framför allt principiella betänkligheter. Det gäller såväl utländska medborgares möjligheter att komma i fråga för vissa anställningar som de problem som kan uppstå för vissa myndigheter att anställa personer med den kompetens och bakgrund som behövs i verksamheten. I sammanhanget bör framhållas att det är påtagligt att synen på medborgarskap har utvecklats på senare tid. Det visar bl.a. uttalanden i lagstiftningsärenden som medfört möjligheten till dubbelt medborgarskap respektive åtstramning i regeringsformen i fråga om krav på medborgarskap för vissa befattningar.

Sammantaget är det vår bedömning att svenskt medborgarskap inte ska vara ett behörighetsgrundande krav för att inneha en säkerhetsklassad anställning vid staten, kommuner eller landsting.

I sammanhanget ska framhållas att den förändring vi föreslår inte innebär att avsaknaden av svenskt medborgarskap är utan betydelse. Den omständigheten att en person saknar svenskt medborgarskap får i stället, på samma sätt som t.ex. innehav av annat medborgarskap jämte ett svenskt, närmare utredas och vägas in vid säkerhetsprövningen. Eventuella bindningar till annan stat och omfattande vistelser utanför Sverige är omständigheter som alltid bör utredas vid en säkerhetsprövning. Om ett tillräckligt underlag för sådan bakgrundskontroll inte går att få fram, t.ex. då samarbete inte finns med aktuellt lands säkerhetstjänst, är det en omständighet som i sig kan medföra att en person bedöms inte vara lämplig för en säkerhetsklassad anställning.

Argumenten för att ta bort kravet har principiellt sett samma relevans för de anställningar som placerats i en högre som i en lägre säkerhetsklass. Vilken betydelse som bör tillmätas sådana omständigheter som hänger samman med medborgarskapet, anknytningen till Sverige och eventuella bindningar till andra länder måste däremot givetvis i hög grad vara beroende av bl.a. vilken anställning det är fråga om. Generellt sett är också utrymmet för att kunna komma

fram till att en person är lämplig för att delta i säkerhetskänslig verksamhet, även om brister finns i underlaget för bakgrundskontrollen, mindre när det gäller anställningar i de högre säkerhetsklasserna.

Det bör anmärkas att det bland utredningens experter finns delade meningar i denna fråga. Vissa av experterna anser att kravet på svenskt medborgarskap ska finnas kvar. Det har därvid framhållits bl.a. att kravet fyller en viktig principiell funktion och att medborgarskapet, även om det inte innebär några garantier avseende t.ex. lojalitet, medför en formell och tydlig koppling till Sverige, dess statsskick och grundläggande värderingar.

18.8 Ett uttryckligt krav på restriktivitet vid placering i säkerhetsklass

Förslag: Med hänsyn till skyddet av den personliga integriteten ska ett krav på restriktiv tillämpning i fråga om placering av anställningar i säkerhetsklass införas i säkerhetsskyddslagen. Av en sådan bestämmelse ska framgå att den som beslutar om placering av en anställning i säkerhetsklass ska noga pröva behovet och att sådan placering får göras endast om skyddsbehovet inte kan tillgodoses på något annat sätt.

Säkerhetsprövning inom ramen för säkerhetsskyddslagen ska göras när en anställning eller annat deltagande i en säkerhetskänslig verksamhet har placerats i säkerhetsklass men kan även förekomma utan sådan placering. I vilken utsträckning registerkontroll och särskild personutredning ska användas styrs av bestämmelserna om placering i säkerhetsklass. Enligt den nuvarande säkerhetsskyddslagen förekommer också registerkontroll enligt särskilda bestämmelser om skydd mot terrorism. Vårt förslag i avsnitt 18.6 innebär att användning av registerkontroll vid deltagande i säkerhetskänslig verksamhet i princip helt styrs av bestämmelserna om placering i säkerhetsklass. Som vi redovisat tidigare i avsnitt 18.4 kan en säkerhetsprövning innebära att frågor om levnadsbakgrund och levnadssituation som kan uppfattas som integritetskränkande behöver ställas. Genom att systemet med placering i säkerhetsklass får ett vidare tillämpningsområde bör i princip alltid säkerhets-

prövningar som kan föranleda att ett mer omfattande underlag inhämtas (t.ex. genom en intervju) grundas på ett beslut om placering i säkerhetsklass. Någon form av säkerhetsprövning kan emellertid också behöva göras vid ett deltagande i säkerhetskänslig verksamhet som inte föranleder placering i säkerhetsklass, t.ex. vid anställning som medför hantering av säkerhetsskyddsklassificerade uppgifter på nivån begränsad. I de fallen bör självfallet säkerhetsprövningen ha en mer begränsad omfattning, och åtgärder inom ramen för personalsäkerheten bör i de fallen framför allt inriktas på utbildning och information om säkerhetsskydd. I en reformerad säkerhetsskyddslag kommer det därför att från integritetssynpunkt vara av avgörande betydelse om en anställning eller ett deltagande placeras i säkerhetsklass eller inte. Självfallet är det också, liksom tidigare, av betydelse i vilken säkerhetsklass placeringen görs. I fråga om underlaget vid registerskontroll (inklusive särskild personutredning) ser vi inte behov av några förändringar i förhållande till vad som i dag gäller för de olika säkerhetsklasserna.

Vårt förslag om att den nuvarande registerkontrollen till skydd mot terrorism ska inordnas i systemet med säkerhetsklasser medför, även om kärnan på samma sätt som i dag kommer att utgöras av anställningar vid skyddsobjekt och flygplatser, en flexibilitet i fråga om vilka verksamheter som kan omfattas. Som vi framfört tidigare bör inte minst samhällsviktiga it-system och vissa andra verksamheter, t.ex. transporter av kärnavfall som inte omfattas av bestämmelser om skyddsobjekt i skyddslagen (2010:305), kunna bedömas utgöra säkerhetskänslig verksamhet. Som vi betonar i avsnitt 15.2 är det nödvändigt att inta en restriktiv hållning när det gäller säkerhetsprövning för vissa personalintensiva verksamheter t.ex. transporter av farligt gods. En mer generell utvidgning till verksamhetsområden som i dag inte omfattas skulle kunna medföra att ytterligare stora personalgrupper behöver säkerhetsprövas och genomgå bl.a. registerkontroll. Vi ställer oss högst tveksamma till om en sådan ordning kan ge positiva skyddseffekter i sådan grad att det väger upp intrånget i de kontrollerades personliga integritetet och också de kostnader och den ökade administration som sådan kontroll medför. Som vi framhållit tidigare behövs i stället ett ökat fokus på andra säkerhetsskyddsåtgärder avseende informationssäkerhet och fysisk säkerhet.

Det är också vår uppfattning att värdet av en registerkontroll överlag överskattas. Erfarenheterna visar att personer som senare upptäcks vara allvarliga säkerhetsrisker relativt sällan förekommer i brotts- och misstankeregister. Den säkerhetsprövning som följer av ett beslut om placering i säkerhetsklass kan dock vara ett viktigt komplement avseende vissa nyckelfunktioner inom verksamheter som i dag inte omfattas av vare sig bestämmelser om säkerhetsklassplacering eller om registerkontroll till skydd mot terrorism. Ett sådant mer flexibelt utformat tillämpningsområde som vi föreslår ställer samtidigt krav på att behovet av placering i säkerhetsklass noga övervägs.

Även om ramarna för säkerhetsskyddsåtgärder görs mer flexibla än i dag, behöver restriktivitet iakttas vad gäller säkerhetsprövning. Ett grundläggande krav för placering i säkerhetsklass med stöd av den kompletterande grunden är att den som ska delta i verksamheten bedöms kunna (genom den behörighet som deltagandet innebär i fråga om t.ex. tillträdesrätt), ha möjlighet att (direkt eller indirekt) orsaka skada (som inte är obetydlig) för Sveriges säkerhet (se avsnitt 18.6). En sådan bedömning förutsätter att en säkerhetsskyddsanalys har gjorts där t.ex. risker som finns kopplade till anställda och inhyrd personal har identifierats och värderats. I förhållande till vad som i dag gäller i fråga om registerkontroll till skydd mot terrorism medför därför den nya ordningen en större tydlighet i fråga om kopplingen mellan ansökan om registerkontroll och utförd säkerhetsskyddsanalys. En sådan koppling är viktig för att undvika registerkontroller som inte är berättigade.

I dag finns i 27 § säkerhetsskyddsförordningen en erinran om kravet att noga pröva behovet av registerkontroll till skydd mot terrorism och om att kontroll får göras endast om skyddsbehovet inte kan tillgodoses på något annat sätt. Vi anser att en motsvarande begränsande bestämmelse i stället bör finnas i säkerhetsskyddslagen och justeras till att avse behovet av placering i säkerhetsklass.

Ett krav på att skyddsbehovet inte kan tillgodoses på annat sätt har flera dimensioner. Ett grundläggande krav är att verksamheten i möjligaste mån organiseras på ett sådant sätt att t.ex. ensambehörighet av olika slag undviks och att tillträdesrätt till en verksamhets säkerhetsområden och liknande inte görs mer omfattande än vad som är nödvändigt i tjänsten. Vidare innebär det ett krav på

att bedöma om skyddsbehovet kan tillgodoses genom alternativa säkerhetsskyddsåtgärder, dvs. åtgärder med inriktning på informationssäkerhet och fysisk säkerhet eller andra åtgärder inom ramen för personalsäkerheten. De senare kan gälla åtgärder för att höja kunskapen och medvetenheten om säkerhetsrisker och säkerhetsskydd. Det kan också avse en säkerhetsprövning utan de moment som följer av beslutet om placering i säkerhetsklass. Vi ser inte anledning att enbart knyta en sådan bestämmelse till placering i säkerhetsklass när det gäller i övrigt säkerhetskänslig verksamhet, utan den bör ha giltighet även i fråga om deltagande som innebär att den berörde får del av säkerhetsskyddsklassificerade uppgifter. En annan sak är att bestämmelsen får en mer begränsad räckvidd i den sistnämnda situationen på grund av mer i detalj i lag angivna krav på placering i säkerhetsklass. Detsamma gäller i fråga om sådana anställningar där krav på säkerhetsprövning följer av folkrättsliga förpliktelser t.ex. i fråga om luftfartsskydd.

18.9 Prövningen av frågan om att lämna ut uppgifter som kommit fram vid registerkontroll

Bedömning: Den nuvarande ordningen där uppgifter efter registerkontroll får lämnas ut endast efter en relevansprövning av Registerkontrolldelegationen vid Säkerhets- och integritetsskyddsnämnden bör inte ändras.

Relevansprövning

Med registerkontroll avses enligt 12 § säkerhetsskyddslagen att uppgifter hämtas från ett register som omfattats av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller lagen (2010:362) om polisens allmänna spaningsregister samt att uppgifter som behandlas med stöd av polisdatalagen (2010:361) hämtas in. Av 18 § säkerhetsskyddslagen framgår i vilka fall en särskild personutredning ska göras vid registerkontroll. I lagens 21–23 §§ anges vilka uppgifter om den kontrollerade och vissa till den kontrollerade närstående som ett utlämnande får omfatta. Utlämnandet får dock avse endast uppgifter som kan antas

ha betydelse för prövningen av den kontrollerades pålitlighet från säkerhetssynpunkt (24 § säkerhetsskyddslagen). Bedömningen av vilka uppgifter som har en sådan relevans för säkerhetsprövningen görs av Säkerhets- och integritetsskyddsnämnden (31 § säkerhetsskyddsförordningen). Registerkontrolldelegationen vid Säkerhets- och integritetsskyddsnämnden som utför uppgiften föregicks av Registerkontrollnämnden som inrättades för att förstärka skyddet för den personliga integriteten vid säkerhetsprövning.

Delegationens funktion kan beskrivas som ett slags filter för att se till att uppgifter som förekommer i registren och som inte har relevans i säkerhetsprövningsärendet inte lämnas ut för säkerhetsprövning. Den ordningen är således en garant för att arbetsgivare inte får del av fler uppgifter än vad som är nödvändigt för ändamålet. Förfarandet innehåller vidare krav på att uppgifter före utlämnande kommuniceras med den som prövningen avser. Vid sådan kommunicering kan också ett samtal hållas med den berörde. Den som prövningen avser ges således tillfälle att förklara omständigheter kring t.ex. ett brott som han eller hon har dömts för. Kommuniceringen fyller inte endast en informationsfunktion utan kan också medföra bedömningen att t.ex. en uppgift om brott inte har relevans för säkerhetsprövningen och därför inte ska lämnas ut. Det finns en bestämmelse om att det inte får framgå av svaret till den som har beslutat om registerkontrollen att det finns en uppgift om den kontrollerade som inte lämnas ut (33 § säkerhetsskyddsförordningen). Det är vidare den som har beslutat om registerkontrollen som självständigt avgör betydelsen av uppgifter som kommit fram vid registerkontroll och som lämnats ut för säkerhetsprövning (27 § säkerhetsskyddslagen). En uppgift som lämnas ut vid registerkontroll får inte heller åtföljas av något annat yttrande än en förtydligande kommentar till uppgiften (26 § säkerhetsskyddslagen).

Tillämpningen av bestämmelserna om utlämnade av uppgifter visar att endast en mindre del av de uppgifter som förekommer i de register som omfattas av kontrollen lämnas ut för säkerhetsprövning. Av Säkerhets- och integritetsskyddsnämndens årsredovisning för 2014[27] kan utläsas att antalet personer som registerkontrollerades var 75 537. Av dessa förekom 206 personer i Säkerhetspolisens

[27] Säkerhets- och integritetsnämndens årsredovisning för 2014, s. 17 (Dnr. 9-2015).

register, och uppgifter om 21 av dessa personer lämnades ut. Av de kontrollerade personerna förekom 1 801 i misstankeregistret eller belastningsregistret, och uppgifter om 309 av dessa lämnades ut. Utlämningsfrekvensen är ungefär densamma för tidigare år.

I vårt uppdrag ingår att ta ställning till om reglerna om utlämnande av uppgifter bör ändras när det gäller registerkontroll till skydd mot terrorism. I direktiven redogörs för att Registernämnden, vars verksamhet den 1 januari 2008 övertogs av Säkerhets- och integritetsskyddsnämnden, i verksamhetsberättelsen för år 2007[28] har ifrågasatt om bestämmelserna om utlämnande i 24 § säkerhetsskyddslagen fått en alltför restriktiv utformning när det gäller personal som är verksam vid flygplatser eller kärnkraftverk I den nämnda verksamhetsberättelsen redogör nämnden mot bakgrund av den allmänna debatt som varit kring frågan om säkerheten vid kärnkraftverk för att t.ex. uppgifter om brott som kan tyda på alkoholproblem normalt sett inte lämnas ut vid kontroll till skydd mot terrorism och att det förhåller sig på liknande sätt när det gäller kontroll av medarbetare vid flygplatser. Vidare noteras i våra direktiv att även Säkerhetspolisen har framfört invändningar mot regelverket i denna del.

Frågan kommer i en något annan dager mot bakgrund av det förslag vi lämnat om att den nuvarande registerkontrollen till skydd mot terrorism (14 § säkerhetsskyddslagen) ska inordnas i systemet med säkerhetsklasser.

En mer övergripande fråga är dock om det finns anledning att i något avseende ändra förfarandet där uppgifter från bl.a. belastningsregistret lämnas ut för säkerhetsprövning först efter en relevansprövning av Registerkontrolldelegationen vid Säkerhets- och integritetsskyddsnämnden.

Vi anser att den utsållning av uppgifter som görs genom delegationen är en viktig del av skyddet av den personliga integriteten. Samtidigt kan konstateras att filtret är finmaskigt genom att endast en mindre del av de uppgifter som förekommer lämnas ut. Vid kontakter med verksamheter som utför säkerhetsprövningar har vi fått exempel på situationer där man senare fått kännedom om uppgifter om brottmålsdomar som för den aktuella anställningen

[28] Registernämndens verksamhetsberättelse för 2007 (Dnr 95/07), se även skrivelsen Ju2008/1653/L4.

och i ljuset av omständigheterna i övrigt ansetts vara av stor relevans för säkerhetsprövningen. Relevansprövningen i sig förutsätter en god kunskap om de förutsättningar som gäller för verksamheten och anställningen. Det redovisade problemet kan bero på att Registerkontrolldelegationen inte har fått ett tillräckligt underlag från den som ansökt om registerkontrollen. Att underlagen som ges in vid registerkontrollen ibland är bristfälliga är också något som har påtalats vid våra kontakter med delegationen.

Vi har under vårt arbete sett exempel på att säkerhetskänsliga verksamheter, för att kompensera vad som uppfattats som ett bristfälligt underlag, tycks utnyttja enskildas möjlighet att begära ett s.k. eget uttag från belastningsregistret. Det är självfallet ett högst olämpligt oskick. Utredningen om registerutdrag i arbetslivet har för övrigt i sitt betänkande med samma titel (SOU 2014:48) föreslagit att det ska vara förbjudet för arbetsgivare att utan författningsstöd begära att arbetssökande ska visa upp eller lämna över ett utdrag ur belastningsregistret. Förslaget har skickats ut på remiss och bereds för närvarande inom Regeringskansliet.

Det som skiljer registerkontrollen enligt säkerhetsskyddslagen från en författningsreglerad rätt att begära utdrag från belastningsregistret är bl.a. att kontrollen avser fler register. Det innebär att uppgifterna inte avser bara domar utan också brottsmisstankar och anteckningar som förts in av Säkerhetspolisen. Uppgifterna kan också under vissa förutsättningar avse inte bara den som prövas utan också närstående. Vidare pågår registerkontrollen kontinuerligt under hela den tid som deltagandet pågår genom en bevakning av tillkommande uppgifter. Mot den bakgrunden innebär en registerkontroll enligt säkerhetsskyddslagen ett större integritetsintrång än ett utdrag från belastningsregistret. Det gäller inte minst som konsekvenserna av att uppgifter lämnas ut i regel kan vara särskilt besvärande under ett pågående anställningsförhållande. Sammantaget anser vi att ordningen med att uppgifter lämnas ut efter en relevansprövning av Registerkontrolldelegationen vid Säkerhets- och integritetsskyddsnämnden är ett viktigt integritetsskyddande moment i säkerhetsprövningen. Det finns emellertid utrymme för att något förtydliga vad relevansprövningen innebär, både i sak och i fråga om delegationens roll i förhållande till Säkerhetspolisens, dvs. den myndighet som utför registerkontrollen.

Vad först gäller ett förtydligande i sak kan noteras att den aktuella bestämmelsen, dvs. 24 § säkerhetsskyddslagen, anger att uppgifter som har kommit fram vid registerkontroll eller särskild personutredning får lämnas ut för säkerhetsprövning endast om den kan antas ha betydelse för prövningen av den kontrollerades pålitlighet från säkerhetssynpunkt. Som vi tagit upp tidigare innebär en bedömning av pålitlighet från säkerhetssynpunkt i detta sammanhang att omständigheter av olika slag behöver utredas och värdereras. Relevansprövningen tar sikte på samma förhållanden som de som nämns i bestämmelsen om säkerhetsprövningens syfte. I det sammanhaget nämns lojalitet som en del i bedömning av pålitlighet och vi har också föreslagit ett förtydligande om omständigheter som kan innebära sårbarheter i säkerhetshänseende (se avsnitt 18.4). Sådana omständigheter ska således alltid beaktas vid prövningen av vilka uppgifter som ska lämnas ut för säkerhetsprövning.

Säkerhetspolisens och Säkerhets- och integritetsskyddsnämndens uppgifter vid registerkontroll

Vad sedan gäller Registerkontrolldelegationen vid Säkerhets- och integritetsskyddsnämndens roll i förhållande till Säkerhetspolisens i fråga om utlämnade av uppgifter efter registerkontroll kan noteras att nuvarande bestämmelser i säkerhetsskyddsförordningen innehåller vissa oklarheter i fråga om ärendehanteringen. Regleringen i säkerhetsskyddsförordningen ger bl.a. en bild av att samtliga registerkontrollärenden, oavsett utfallet av kontrollen, lämnas över från Säkerhetspolisen till delegationen. Så går det inte till. Det stora flertalet ärenden är sådana där det inte förekommer några uppgifter i registren eller där uppgifterna är av ringa betydelse. I dessa ärenden fattar särskilt förordnade tjänstemän vid Registerkontrolldelegationens kansli, som Säkerhetspolisen tillhandahåller, beslut om att det inte finns några uppgifter att redovisa. Den ordningen bygger på en delegation i nämndens arbetsordning från nämnden till de särskilt förordnade tjänstemännen. I praktiken är det alltså de särskilt förordnade tjänstemännen, som är anställda vid Säkerhetspolisen, som beslutar i utlämnandefrågan i sådana fall. Genom det tillvägagångssättet behöver inte delegationen belastas med ärenden där det är uppenbart att de uppgifter som kommit fram vid

kontrollen inte ska lämnas ut för säkerhetsprövning. Det innebär också att besked om att inga uppgifter finns att redovisa kan ges snabbare än om ärendet skulle beslutas av delegationen som endast sammanträder några gånger i månaden. Den redovisade ordningen är ändamålsenlig och bör framgå redan av författningstexten. Sammantaget bör det därför av lag och förordningstext framgå att ansökan görs till Säkerhetspolisen som sedan utför den faktiska registerkontrollen. I den uppgiften ingår också att i vissa fall göra en särskild personutredning. Om det kommer fram uppgifter som kan antas vara av betydelse för säkerhetsprövningen, ska således frågan om utlämnade av uppgifter för säkerhetsprövning underställas prövning av Säkerhets- och integritetsskyddsnämnden. Kommunicering med den som kontrollen avser av uppgifter som kan komma att lämnas ska tas om hand av Säkerhetspolisen. Om nämnden bedömer att uppgifter ska lämnas ut, är det Säkerhetspolisen som ska kommunicera uppgifterna till arbetsgivaren eller den som annars ska göra säkerhetsprövningen (se avsnitt 18.11).

18.10 Vem ska besluta om placering i säkerhetsklass?

Förslag: Behörigheten att besluta om placering av anställningar i säkerhetsklass ska bygga på nuvarande beslutsordning där regeringen, med undantag för riksdagens förvaltningsområde, ytterst har beslutanderätten men kan överlåta den till myndigheter, kommuner och landsting och, om det finns särskilda skäl, vissa företag.

Regeringen bör i förordning ange att de myndigheter m.fl. som i dag beslutar om registerkontroll enligt 14 § säkerhetsskyddslagen (skydd mot terrorism) i stället ska i en motsvarande utsträckning besluta om placering i säkerhetsklass.

Vissa ändringar bör därvid göras av ansvarsområdena för de säkerhetsskyddsstödjande myndigheterna. Myndigheten för samhällsskydd och beredskap bör tilldelas den beslutanderätt i fråga om säkerhetsskyddet som länsstyrelserna har i dag och Transportsstyrelsens ansvarsområde bör utvidgas till att även avse hamnskydd och sjöfartsskydd.

I förordning bör vidare regleras att Säkerhetspolisen på samma sätt som i dag ska utföra registerkontroll endast efter

ansökan från en myndighet, en kommun, ett landsting eller vissa bolag där starka oberoende hänsyn gör sig gällande (Sveriges Radio Aktiebolag och liknande). Därutöver bör, om det finns särskilda skäl, en säkerhetsskyddsstödjande myndighet efter beslut om placering i säkerhetsklass kunna medge att ett bolag, utan myndighetens medverkan, själv vid Säkerhetspolisen får initiera sådan registerkontroll som följer av beslutet om placering i säkerhetsklass.

Nuvarande ordning i fråga om behörighet att besluta om placering i säkerhetsklass och om registerkontroll är inte helt enkel att utläsa. Vilka som har behörighet att besluta i olika avseenden framgår av 20 § säkerhetsskyddslagen i kombination med 18–22 och 26 a–27 a §§ säkerhetsskyddsförordningen samt av bilagan till den förordningen. Bilagan innehåller en förteckning över de statliga myndigheter som beslutar om placering i säkerhetsklass och om registerkontroll till följd av en sådan placering. Bestämmelserna innebär i korthet att regeringen, med undantag för riksdagens förvaltningsområde, ytterst har beslutanderätten men kan överlåta den åt myndigheter, kommuner och landsting och, om det finns särskilda skäl, vissa företag. Regeringen har med stöd av bemyndigandet överlåtit i princip all beslutanderätt, med undantag för framför allt beslut om placering i säkerhetsklass 1, till myndigheter, kommuner och landsting samt till några få bolag där starka oberoendehänsyn gör sig gällande, bl.a. Sveriges Radio Aktiebolag.

Även om beslutsordningen är svåröverskådlig har inte annat kommit fram än att den i huvudsak är ändamålsenlig.

Förslaget i avsnitt 18.6 om att den nuvarande registerkontrollen till skydd mot terrorism ska inordnas i systemet med placering i säkerhetsklass innebär behov av justeringar i fråga om beslutsordningen. Det förefaller vara en lämplig ordning att myndigheter som i dag beslutar om placering i säkerhetsklass får göra det i den större utsträckning som blir följden av den föreslagna ordningen med en utvidgande grunder för placering i säkerhetsklass. Det innebär t.ex. att Transportstyrelsen, i stället för att besluta om registerkontroll enligt 14 § säkerhetsskyddslagen (skydd mot terrorism), i fråga om de som ska anställas vid flygplatser i motsvarande utsträckning beslutar om placering i säkerhetsklass. I fråga om enskild verksamhet som i dag inte omfattas av bestäm-

melserna om registerkontroll till skydd mot terrorism (eller av bestämmelser om placering i säkerhetsklass) är det lämpligt att de säkerhetsskyddsstödjande myndigheterna bemyndigas att också i de fallen besluta om placering i säkerhetsklass. Vi kommer dock, vilket vi behandlar i avsnitt 21.2.4 att föreslå att Myndigheten för samhällsskydd och beredskap tar över de uppgifter i fråga om tillsyn av säkerhetsskyddet som i dag är fördelat på länsstyrelserna (jfr bl.a. 40 § säkerhetsskyddsförordningen). Det medför att Myndigheten för samhällskydd och beredskap också bör ta över länsstyrelsernas uppgift att för vissa enskilda verksamheter besluta om placering i säkerhetsklass. Vidare bör beslut om säkerhetsklass i fråga om sådan bevakningspersonal som avses i 26 § 1 säkerhetsskyddsförordningen fattas av Transportstyrelsen. I dag beslutar Polismyndigheten om registerkontroll i de fallen.[29] Transportstyrelsen har dock den uppgiften när samma slag av personalkategori förordnas för att tjänstgöra vid flygplatser. Det skulle även kunna röra sig om samma personer med olika tjänstgöringsställen. Mot den bakgrunden förefaller det rimligt att Transportstyrelsen får ett samlat ansvar. En sådan ordning sammanfaller också med det ansvar Tranportstyrelsen har i andra avseenden i fråga om hamnskydd och sjöfartsskydd.[30]

Vi har övervägt om det är lämpligt att i större utsträckning än i dag överlåta till enskilda verksamheter att utan myndighetsmedverkan få till stånd registerkontroll. Vårt förslag om att inordna den nuvarande registerkontrollen till skydd mot terrorism i systemet med säkerhetsklasser innebär i princip att all registerkontroll kommer att ha föregåtts av ett beslut om placering i säkerhetsklass. En sådan ordning där alltså frågan om placering i säkerhetsklass avgörs av en myndighet eller annat allmänt organ skulle kunna kombineras med en ordning där ansökan om sådan registerkontroll, som är en i lag reglerad följd av sådan placering,[31] i större utsträckning får skötas av enskilda verksamheter. Det är möjligt att en sådan ordning är en tillräcklig garanti för att registerkontroller inte används i en omfattning som inte är avsedd. Vi är emellertid tvek-

[29] Se 27 a § säkerhetsskyddsförordningen.
[30] Se 2 § förordningen (2008:1300) med instruktion för Transportstyrelsen.
[31] Eftersom registerkontrollen föregås av ett beslut om placering i säkerhetsklass och det av lag följer att sådan placering medför registerkontroll bör det inte behövas ett särskilt beslut om registerkontroll.

samma till större förändringar av en ordning som bestämts utifrån integritetshänsyn och som innebär att ett offentligt organ bedömer om förutsättningarna för registerkontroll är uppfyllda. Ett förhållande som behöver beaktas är också att bland de myndigheter som ansöker om registerkontroll för en annan verksamhets räkning finns myndigheter som behöver ta del av resultatet från registerkontrollen. Vi återkommer till den frågan i det följande avsnittet.

Vi har dock sett det som ändamålsenligt att ge utrymme för ett mer flexibelt system. Det finns bolag som har stor erfarenhet av och kunnande kring säkerhetsprövning av personal och som bör kunna anförtros uppgiften att även ansvara för registerkontrollen utan att skyddet av enskildas integritet försämras. I sammanhanget kan nämnas att det bland de bolag som i dag, genom särskilt regeringsbeslut eller genom delegation i förordning, har fått möjlighet att själva besluta om registerkontroll förekommer bolag där ordningens förenlighet med förarbetsuttalanden om starka integritets- och oberoendeintressen framstår som tveksam.[32]

En mer flexibel ordning kan åstadkommas genom att införa en möjlighet för de säkerhetsskyddsstödjande myndigheterna (Affärsverket svenska kraftnät etc.) att, om det finns särskilda skäl, efter beslut om placering i säkerhetsklass låta ett bolag ansvara för den efterföljande registerkontrollen.

18.11 Ansvaret för säkerhetsprövningen

Förslag: Den som beslutar om anställning eller annat deltagande i säkerhetskänslig verksamhet ansvarar för säkerhetsprövningen och avgör självständigt om personen kan anses vara lämplig från säkerhetssynpunkt. Om en myndighet har ett avgörande bestämmande över den prövades lämplighet att delta i den säkerhetskänsliga verksamheten vid t.ex. en flygplats eller i fråga om säkerhetsskyddad upphandling, gör dock myndigheten den slutliga bedömningen.

[32] Prop. 1995/96:129 s. 56.

En mer flexibel ordning vad gäller myndighetsmedverkan vid säkerhetsprövning i enskild verksamhet

Som framgått av det föregående avsnittet anser vi att hänsynen till enskildas integritet motiverar att beslut om placering i säkerhetsklass och att vid Säkerhetshetspolisen initiera registerkontroll på samma sätt som i dag i huvudsak ska vara en uppgift för myndigheter eller andra offentliga organ. Den ordningen bör kunna säkerställa att säkerhetsklassplacering och de integritetskränkande moment i säkerhetsprövningen som följer av en sådan placering förbehålls sådana anställningar etc. där sådan kontroll är befogad.

En annan fråga är vem eventuella uppgifter bör lämnas ut till och vem som således bör ha ansvaret för att bedöma den kontrollerades pålitlighet i säkerhetshänseende. Enligt gällande ordning lämnas uppgifterna till den som bestämmer om registerkontrollen. Det medför när det gäller en person som ska anställas i en enskild verksamhet att uppgifternas betydelse för säkerhetsprövningen avgörs av en myndighet i stället för t.ex. arbetsgivaren (se 27 § säkerhetsskyddslagen). Den ordningen innebär, som också noteras i författningskommentaren till nämnda bestämmelse,[33] ett avsteg från grundtanken att säkerhetsprövningen bäst görs av den verksamhet som deltagandet avser. I kommentaren hänvisas till att behovet av ett mer allsidigt underlag för prövningen ändå kan tillgodoses genom bestämmelser om samråd mellan den myndighet som beslutat om kontrollen och arbetsgivaren. Sådana bestämmelser finns i 14 § säkerhetsskyddsförordningen. Ordningen medför dock oklarheter i fråga om vem som ansvarar för att genomföra säkerhetsprövningen och en otydlighet, inte minst i förhållande till den enskilde, om vem som prövar lämpligheten av ett deltagande.

De integritetsskyddshänsyn som ligger till grund för att endast en myndighet eller annat allmänt organ bör ha bestämmanderätt över placering i säkerhetsklass och registerkontroll är inte lika framträdande i frågan om vem som bör pröva utlämnade uppgifters betydelse för säkerhetsprövningen. Det gäller särskilt när ordningen är sådan att utlämnandet av uppgifter föregås av en relevansprövning av Säkerhets- och integritetsskyddsnämnden. Den särskilda relevansprövningen, som i praktiken medför att mer-

[33] Prop. 1995/96:129, s. 87.

parten av de uppgifter som utgör underlag vid registerkontrollen inte lämnas vidare till den som gör säkerhetsprövningen, bör i sig vara tillräckligt för att i detta avseende skydda den kontrollerades integritet. Också vid en jämförelse med andra områden där arbetsgivare har rätt att få del av motsvarande registeruppgifter framstår integritetsskyddet som rimligt väl tillgodosett. Även uppgifter som i övrigt kommer fram vid en säkerhetsprövning, t.ex. genom referenstagning och intervju, kan vara minst lika känsliga för den enskilde som uppgifter som lämnas ut efter registerkontroll. Sådana moment i säkerhetsprövningen utförs i regel av arbetsgivaren.

I sammanhanget bör noteras att den aktuella ordningen med en myndighetsmedverkan motiverats endast av behovet att skydda den enskildes integritet. Principiellt sett bör också enskilda verksamheter ha ett eget tydligt ansvar för att utreda behovet av säkerhetsskydd och vidta de säkerhetsskyddsåtgärder som behövs för att tillgodose behovet. Det stöd i fråga om personalsäkerheten som i vissa fall kan behövas får hanteras inom ramen för tillsynen. Så långt som möjligt bör därför även i enskild verksamhet den ordningen gälla att den som beslutar om anställningen eller deltagandet också har hela ansvaret för säkerhetsprövningen.

Det finns dock områden där principen inte kan tillämpas. Det hänger samman med att den ifrågavarande myndigheten också utifrån resultatet av registerkontrollen ska godkänna ett deltagande i den säkerhetskänsliga verksamheten. Den ordningen gäller inom luftfartsskyddsområdet där den är en följd av internationella konventioner som anger villkor för tillträde till olika slag av behörighetsområden på flygplatser. För sådan personal går säkerhetsprövningen till på så sätt att den verksamhet som ska anställa någon för tjänstgöring vid en flygplats, utifrån uppgifter som kommer fram vid det vi valt att benämna grundutredning, gör en första bedömning av personens lämplighet för att delta i den aktuella säkerhetskänsliga verksamheten. Om personen bedöms lämplig, aktualiseras registerkontroll. I annat fall saknas anledning att gå vidare med en registerkontroll. Så långt överensstämmer förfarandet med vad som i allmänhet gäller. Vad som särskiljer är vad som händer efter registerkontrollen. Om Transportstyrelsen som beslutar om sådan kontroll för verksamhetens räkning får besked om att inga uppgifter finns att lämna ut för säkerhetsprövning, meddelar myndigheten sitt godkännande av säkerhetspröv-

ningen. På grundval av Transportstyrelsens godkännande kan sedan en behörighetshandling utfärdas. Också förfarandet för att utfärda sådana handlingar och innebörden av dem styrs av internationella regelverk. Behörighetshandlingen är en förutsättning för att få tillträde till de områden som behövs för att arbetsuppgifterna ska kunna utföras. Om uppgifter efter registerkontrollen lämnas ut till Transportstyrelsen, behöver således myndigheten göra en bedömning av uppgifternas betydelse för den prövades lämplighet att få tillträde till flygplatsens säkerhetsområden.

En liknande ordning torde gälla på fler områden, t.ex. hamn-, sjöfarts- och strålskydd. Också i fråga om säkerhetsskyddad upphandling avtalas i regel om att leverantörer ansvarar för säkerhetsprövningen men att ett godkännande efter registerkontroll krävs från den upphandlande myndigheten.

Om förfarandet avseende prövningen av ett eventuellt utfall efter registerkontroll justeras för att ge ett tydligare stöd för att enskilda verksamheter självständigt ska kunna svara för säkerhetsprövningen, behöver dock hänsyn tas till den ordning som gäller bl.a. i fråga om luftfartsskydd och liknande samt upphandling. För att tillgodose båda de nämnda aspekterna föreslår vi att det i säkerhetsskyddslagen anges att bedömningen i fråga om säkerhetsprövning görs av den som beslutar om anställningen eller deltagandet i den säkerhetskänsliga verksamheten men att det inte gäller om någon annan ska göra den slutliga bedömningen av om någon får delta i den säkerhetskänsliga verksamheten. I den till lagen hörande förordningen bör framgå att en myndighet som beslutar om placering i säkerhetsklass och som vid Säkerhetspolisen för annan verksamhets räkning ska ansöka om registerkontroll i regel inte ska göra någon bedömning av eventuella uppgifter som lämnas ut utan endast redovisa resultatet till den berörda verksamheten. Det ska dock inte gälla om annat följer av den aktuella lagbestämmelsen. Om myndigheten ska svara för den slutliga bedömningen, bör i regel för det fall att uppgifter lämnas ut myndighetens bedömning föregås av ett samråd med den arbetsgivare som i övrigt ansvarar för säkerhetsprövningen. Uppgifter som lämnas ut vid registerkontroll bör inte ges en självständig betydelse utan bedömas utifrån vad som i övrigt har kommit fram vid säkerhetsprövningen och också relateras till vad arbetsuppgifterna innebär. Det kan också behöva vägas in om ett

deltagande är möjligt efter att andra skyddsåtgärder vidtas t.ex. i syfte att begränsa ensambehörighet till vissa anläggningar eller delar av en anläggning. Det kan dock vara så att möjligheterna till sådana åtgärder är begränsade beroende på arbetsuppgifterna eller arbetsplatsens karaktär eller för att internationella regelverk innebär krav på t.ex. utformning av och tillträde till anläggningens behörighetsområden. Sammantaget finns det i regel anledning för de ifrågavarande myndigheterna att i sådana situationer som här har beskrivits samråda med arbetsgivaren eller den som annars i övriga avseenden ansvarar för säkerhetsprövningen.

18.12 Skyddet för uppgifter om enskildas personliga förhållanden

Förslag: Sekretessen till skydd för enskilds personliga förhållanden för uppgifter som kommer fram vid registerkontroll och särskild personutredning enligt säkerhetsskyddslagen ska utvidgas till att avse även andra uppgifter om enskilds personliga förhållanden som kommer fram vid säkerhetsprövningen.

En motsvarande tystnadsplikt införs i säkerhetsskyddslagen i fråga om säkerhetsprövningsärenden i enskilda verksamheter.

Behovet att utvidga skyddet för uppgifter som kommer fram vid säkerhetsprövning

Ett säkerhetsprövningsärende kan innebära att för den enskilde synnerligen känsliga uppgifter hämtas in av arbetsgivaren eller den som annars ska göra säkerhetsprövningen. Det är därför viktigt att det finns ett skydd för att uppgifterna inte används för annat ändamål än det avsedda.

I 35 kap. 1 § OSL finns en bestämmelse som tar sikte på att skydda uppgifter av detta slag. Vår bedömning är dock att skyddet inte är tillräckligt. Enligt ordalydelsen avser bestämmelsen endast uppgifter som kommer fram vid registerkontroll eller särskild personutredning enligt säkerhetsskyddslagen. Det medför en oklarhet i fråga om skyddet för uppgifter som i övrigt kommer fram vid säkerhetsprövningen t.ex. vid en intervju eller vid kon-

takter med tidigare arbetsgivare. Underlaget i den delen kan innebära tillgång till uppgifter som från integritetssynpunkt kan vara minst lika känsliga som uppgifter som lämnats ut efter registerkontroll. Den aktuella bestämmelsen i offentlighets- och sekretesslagen bör därför ändras så att den avser angelägenhet vid säkerhetsprövning i stället för registerkontroll och särskild personutredning.

Bestämmelser om sekretess i offentlighets- och sekretesslagen gäller endast i det allmännas verksamhet. Säkerhetsprövning eller inhämtande av underlag för sådan prövning kan dock vara en uppgift som utförs även i enskilda verksamheter. Mot den bakgrunden behövs en till offentlighets- och sekretesslagen kompletterande bestämmelse om tystnadsplikt för uppgifter som kommer fram om enskildas personliga förhållanden i säkerhetsprövningsärenden. Vi föreslår att en bestämmelse med sådant innehåll ska föras in i säkerhetsskyddslagen.

En handläggningsfråga

I 28 § säkerhetsskyddslagen finns en bestämmelse som innebär en presumtion för att handlingar som erhållits från Säkerhetspolisen snarast efter beslut med anledning av säkerhetsprövning ska återställas dit om inte Säkerhetspolisen har beslutat annat. Bestämmelsen hade en tidigare motsvarighet i personalkontrollkungörelsen.[34] Säkerhetspolisen har framfört att bestämmelsen inte fyller någon funktion. I förarbetena till säkerhetsskyddslagenkonstateras att underlaget och skälen för beslut i säkerhetsprövningsärendet bör dokumenteras. [35] Resultatet av registerkontrollen delges genom att en promemoria lämnas över. Säkerhetspolisen har upplyst om att sådana promemorior innehåller enbart uppgifter av sådant slag och av sådan omfattning att de också bör dokumenteras av den mottagande verksamheten. Bestämmelsen fyller därför ingen praktisk funktion och behöver inte föras över till en reformerad säkerhetsskyddslag.

[34] Att bestämmelsen fördes in säkerhetsskyddslagen har sin bakgrund i bestämmelser i arkivlagen (1990:782) som innebär att det krävs stöd i lag (eller beslut av kommunfullmäktige) för att en kommun ska få lämna ifrån sig allmänna handlingar i andra situationer än sådana som avser lån.
[35]SOU 1994:149, s. 206.

19 Säkerhetsskyddad upphandling

En viktig utgångspunkt för säkerhetsskyddslagstiftningen att de intressen som lagstiftningen slår vakt om ska ha samma skydd oavsett på vilket sätt och var den säkerhetskänsliga verksamheten bedrivs. Det innebär att i en upphandlingssituation myndighetens hemliga uppgifter ska ges samma säkerhetsskydd hos leverantörer som de har hos myndigheten. När det i en upphandling förekommer hemliga uppgifter har myndigheten ansvaret för att det finns ett fullgott säkerhetsskydd. I 8 § säkerhetsskyddslagen finns bestämmelser om säkerhetsskyddad upphandling med säkerhetsskyddsavtal. Bestämmelserna innebär en skyldighet för myndigheter att i avtal specificera vilka säkerhetsskyddskrav som ska vara uppfyllda av leverantören i det aktuella uppdraget.

Numera förekommer i betydligt större utsträckning än när säkerhetsskyddslagen trädde i kraft att myndigheter och enskilda tar hjälp av externa leverantörer. Det är också vanligt att svenska företag deltar i säkerhetsskyddade upphandlingar utomlands, liksom att utländska leverantörer deltar i motsvarande upphandlingar i Sverige.

Enligt direktiven ska vi analysera behovet av förändringar av säkerhetsskyddslagens bestämmelser om säkerhetsskyddad upphandling, bl.a. avseende möjligheterna att träffa säkerhetsskyddsavtal. Vi ska också bedöma vilka förändringar i övrigt som kan behövas för att bättre anpassa reglerna till de krav som ställs i det internationella samarbetet, bl.a. när det gäller säkerhetsintyg för leverantörer.

Kapitlet inleds med frågan om behovet av en internationell anpassning (avsnitt 19.1). I avsnitt 19.2 behandlar vi sedan säkerhetsskyddsavtal i en reformerad säkerhetsskyddslag. Dessa avtals innehåll och innebörd behandlas närmare i avsnitt 19.3. Avsnitt 19.4 innehåller förslag om hur begreppet *säkerhetsskydds-*

klassificerade uppgifter i lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet ska förhålla sig till samma begrepp i en ny säkerhetsskyddslag. Kapitlet avslutas med avsnitt 19.5 om underrättelse i vissa fall till Säkerhetspolisen.

Frågan om säkerhetsintyg för leverantörer för internationella behov behandlas i avsnitt 20.4. Frågan om tillsyn över leverantörer som omfattas av ett säkerhetsskyddsavtal behandlas i kapitel 21 Tillsyn, föreskrifter och rapportering.

19.1 Behovet av en anpassning till internationella förhållanden

Bedömning: Säkerhetsskyddad upphandling med säkerhetsskyddsavtal bör behållas i en ny lagstiftning. Bestämmelserna om säkerhetsskyddad upphandling bör anpassas till en ny säkerhetsskyddslag vad avser vilka som ska omfattas av bestämmelserna och hur säkerhetsintyg för leverantörer kan utfärdas.

I direktiven framgår det även att vi ska analysera om det är lämpligt att inom detta område övergå till ett s.k. klareringssystem som är vanligt i många andra länder. Beskrivningen i direktiven utgår från de förändringar som samarbetet med andra länder och mellanfolkliga organisationer påkallar. Också behovet av att underlätta för enskilda att få uppdrag i andra länder och hos mellanfolkliga organisationer där krav ställs på säkerhetsintyg lyfts fram.

Konstruktionen med säkerhetsskyddsavtal har överlag fungerat väl i nuvarande lagstiftning, och en praxis har etablerats där den upphandlande enheten i avtalsform ställer relevanta krav på säkerhetsskydd som en leverantör ska uppfylla i det aktuella uppdraget.

Industrisäkerhet och säkerhetsskyddad upphandling har varit ett av fokusområdena i våra diskussioner med företrädare för andra länders säkerhetstjänster. Vi har uppfattat att det nuvarande svenska systemet inte skiljer sig i så stora avseenden som ett första påseende kan ge intryck av. Tvärtom så har den nuvarande ordningen med en avtalskonstruktion goda förutsättningar att utvecklas i den riktning som direktiven anger. Vi har också utgått från de

behov som utredningens experter har framfört och synpunkter om att nuvarande system bör behållas, och vi ser det därför som ändamålsenligt att behålla systemet med säkerhetsskyddad upphandling med säkerhetsskyddsavtal i en ny lagstiftning. Vissa anpassningar bör dock göras för att institutet fullt ut ska passa in i en ny lagstiftning och tillgodose de krav som internationellt samarbete ställer.

En central fråga rör utfärdande av s.k. säkerhetsintyg[1] vilka innebär ett uttalande om en leverantörs möjlighet att hantera säkerhetsskyddsklassificerade uppgifter på en viss nivå. Intygen utfärdas av en behörig myndighet och ger mottagaren upplysningar om mot vilken informationssäkerhetsklass en leverantör har bedömts lämplig. Denna fråga som hör samman med internationell samverkan behandlas i avsnitt 20.4.

19.2 Säkerhetsskyddsavtal

Förslag: Bestämmelserna om säkerhetsskyddad upphandling och säkerhetsskyddsavtal ska gälla för upphandlingar eller ingående av kontrakt där det förekommer säkerhetsskyddsklassificerade uppgifter i informationssäkerhetsklassen konfidentiell eller däröver eller som avser säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

I säkerhetsskyddsavtalen ska på samma sätt som i dag villkor anges för hur krav på säkerhetsskydd ska tillgodoses av leverantören.

Även i fortsättningen bör säkerhetsskyddsavtal ingås av staten, kommuner och landsting, men även att andra som har behov av sådana avtal bör kunna begära detta hos en myndighet som regeringen bestämmer, i första hand en säkerhetsskyddsstödjande myndighet. Om det finns särskilda skäl, bör en enskild kunna ingå säkerhetsskyddsavtal. Föreskrifter om detta kan meddelas av regeringen.

[1] På engelska *Facility Security Clearance Certificate* (*FSCC* eller ibland enbart *FSC*).

Ett utökat tillämpningsområde och ett nytt kvalificeringskrav för säkerhetsskyddad upphandling

En ny säkerhetskyddslag bör inte ge ett skydd bara för säkerhetsskyddsklassificerade uppgifter utan även för säkerhetskänslig verksamhet som är säkerhetskänslig av annan anledning än att den innebär hantering av säkerhetsskyddsklassificerade uppgifter (i övrigt säkerhetskänslig verksamhet). Säkerhetsskyddad upphandling bör därför inte vara tillämpligt enbart om en leverantör ska hantera säkerhetskyddsklassificerade uppgifter utan även om leverantören ska delta i säkerhetskänslig verksamhet i övrigt. Detta kan vara fallet t.ex. på kärnkraftverk och på flygplatser där den säkerhetskänsliga verksamheten enbart i liten omfattning avser säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskyddad upphandling med säkerhetsskyddsavtal kan medföra ökade kostnader. Det är därför nödvändigt att begränsa kravet på att använda sådana avtal till säkerhetskänslig verksamhet där det är befogat av hänsyn till skyddsbehoven. I många länder finns det ingen reglering om industrisäkerhet och säkerhetsskyddsavtal när det gäller uppdrag som innefattar säkerhetsskyddsklassificerade uppgifter i motsvarande informationssäkerhetsklass begränsad. Bestämmelserna tar i stället sikte på säkerhetsskyddsklassificerade uppgifter på nivån konfidentiell och däröver. Vi anser att detta ligger i linje med grundtanken i ett mer nyanserat säkerhetsskydd i en ny säkerhetsskyddslag. Vi föreslår därför att en sådan begränsning ska gälla även i Sverige. En betydande fördel med detta är en internationell harmonisering av institutet. I och med att bestämmelserna om säkerhetsskyddad upphandling föreslås gälla även för i övrigt säkerhetskänslig verksamhet bör en korresponderande begränsningsregel införas som begränsar tillämpligheten till säkerhetskänslig verksamhet av *motsvarande betydelse*. Skälet till detta är att undvika ett resurskrävande avtalsförfarande i de fall där kraven på säkerhetskydd i övrigt är begränsade.

Avgränsningen innebär dock inte att man inte ska ställa krav på säkerhetsskydd i sådana fall där ett uppdrag omfattar uppgifter på enbart nivån begränsad eller som avser säkerhetskänslig verksamhet av motsvarande betydelse. I sådana fall kan man välja att ingå ett säkerhetsskyddsavtal eller ställa upp villkor för säkerhetsskydd i t.ex. affärsavtalet.

En ny bestämmelse om att även enskilda ska omfattas av krav på säkerhetsskyddad upphandling för säkerhetskänslig verksamhet

Enskilda som bedriver säkerhetskänslig verksamhet kan ha ett behov av att anlita leverantörer som hanterar en del av deras säkerhetskänsliga verksamhet. Därmed kan det finnas behov av ett skydd för även denna del av verksamheten. Denna möjlighet saknas i den nuvarande säkerhetsskyddslagen där säkerhetsskyddad upphandling är förbehållet myndigheter, kommuner och landsting. Enligt principen att skyddet för säkerhetsskyddsklassificerade uppgifter eller den i övrigt säkerhetskänsliga verksamheten ska vara detsamma oberoende av var uppgifterna eller verksamheten förekommer bör det alltså vara möjligt att även för enskilda som bedriver säkerhetskänslig verksamhet ställa krav på säkerhetsskydd hos en leverantör. Vi föreslår dock att den enskilde inte själv ingår säkerhetsskyddsavtalet utan att avtalet ingås av staten, företrätt av en myndighet, om det inte föreligger särskilda skäl. Skälet till en sådan lösning är att ett säkerhetsskyddsavtal innebär placering av anställningar och annat deltagande i säkerhetsklass vilket alltid av integritetsskäl i huvudsak bör vara ett myndighetsbeslut (se vidare avsnitt 18.10). För vissa enskilda verksamheter finns det särskilda skäl att frångå den principen. Det rör sig om verksamheter där starka oberoendehänsyn gör sig gällande vilket innefattar t.ex. Sveriges Radio Aktiebolag och Sveriges Television Aktiebolag. Dessa bolag har enligt nuvarande säkerhetsskyddsförordning rätt att själva besluta om placering i säkerhetsklass. Det bör därför finnas en bestämmelse i säkerhetsskyddslagen om att regeringen får meddela föreskrifter om att dessa verksamheter får ingå säkerhetsskyddsavtal för den egna verksamheten.

I övrigt ska enskilda verksamheter framföra behovet av säkerhetsskyddsavtal till den säkerhetsskyddsstödjande myndighet som ansvarar för det aktuella verksamhetsområdet utom när det gäller bolag, föreningar och stiftelser över vilka en myndighet, en kommun eller ett landsting utövar ett rättsligt bestämmande inflytande. I dessa fall ska en ansökan i stället göras till den som utövar det rättsligt bestämmande inflytandet.

Säkerhetsskyddsavtalet bör hänvisa till affärsavtalet och i affärsavtalet bör det framgå att dess giltighet är avhängigt mot att kraven i säkerhetsskyddsavtalet uppfylls.

Förslaget är dock inte invändningsfritt och några av utredningens experter har ställt sig tveksamma till det. Förslaget innebär en trepartskonstruktion där säkerhetsskyddsavtalet mellan en säkerhetsskyddsstödjande myndighet och en leverantör inte hänger samman med en affärsmässig relation. Denna relation finns i stället mellan leverantören och den enskilde. Genom att affärsavtalets giltighet ska villkoras med en kravuppfyllnad av säkerhetsskyddsavtalet kan det uppstå situationer där de tre parterna är oense om villkor i säkerhetsskyddsavtalet är uppfyllda eller inte. Vidare förutsätter konstruktionen att den enskilda näringsidkaren som önskar ingå ett säkerhetsskyddsavtal med en leverantör i vissa fall kan behöva lämna uppgifter om affärsavtalet till en myndighet där uppgifterna kan bli offentliga. Det sistnämnda torde dock inte innebära något större problem i och med att sådana uppgifter som behövs sällan är känsliga. Vidare kan säkerhetsskyddsavtalen standardiseras genom föreskrifter och att de säkerhetsskyddsstödjande myndigheternas roll därigenom blir att enbart granska att säkerhetsskyddsavtalen innehåller de uppgifter som krävs.

Ett alternativ som vi har övervägt är att i stället låta enskilda själva ingå säkerhetsskyddsavtal med den begränsningen att besluten om placering i säkerhetsklass och registerkontrollerna hanteras av den säkerhetsskyddsstödjande myndigheten. En sådan lösning minskar statens kontroll över säkerhetsskyddsavtalen, men kan samtidigt uppväga de negativa effekter som vårt förslag kan medföra.

Vi har dock stannat vid att föreslå att det är den säkerhetsskyddsstödjande myndigheten som ska träffa säkerhetsskyddsavtalet.

Genomföra säkerhetsskyddad upphandling åt annan – säkerhetsskyddsanvaret kvarstår

Under vissa förutsättningar finns det en möjlighet för en myndighet att uppdra åt en annan myndighet att upphandla varor och tjänster för den förstnämndas räkning. Ett exempel på sådana uppdrag är att Försvarets materielverk genomför upphandlingar och

ingår avtal på uppdrag av Försvarsmakten.[2] När Försvarsmaktens logistikfunktion överfördes från Försvarsmakten till Försvarets materielverk 2014 uppmärksammades ett antal fall där ansvaret för bl.a. de säkerhetsskyddade upphandlingarna genom organisationsändringen kom att hamna på Försvarets materielverk, trots att de tjänster som upphandlades skulle utföras för Försvarsmaktens räkning. Detta innebar att ansvaret för säkerhetsskyddet kom att förskjutas från den verksamhet som egentligen borde ha haft kvar säkerhetsskyddsansvaret. Utvecklingen kan gå åt samma håll inom flera områden.

Det är därför viktigt att tydliggöra att säkerhetsskyddsansvaret hänger samman med ansvaret för den säkerhetskänsliga verksamheten och att detta förhållande kvarstår även i en upphandlingssituation. Därför föreslår vi en justering i nuvarande 15 § säkerhetsskyddsförordningen på ett sådant sätt att det blir tydligt att säkerhetsskyddsansvaret kvarstår hos den som ansvarar för verksamheten även om någon annan begär in anbud eller träffar avtal för den förstnämndas räkning.

Säkerhetsskyddad upphandling med utländska leverantörer

I kapitel 20 behandlar vi internationell samverkan på säkerhetsskyddsområdet och för svenska leverantörers möjligheter att delta i upphandlingar i andra länder och hos mellanfolkliga organisationer. Systematiskt passar det bättre att här ta upp det omvända förhållandet, dvs. när utländska leverantörer deltar i säkerhetsskyddade upphandlingar som genomförs av svenska upphandlande enheter.

Huvudregeln är att samma förutsättningar gäller för utländska leverantörer som för svenska, nämligen att dessa ska vara lämpliga från säkerhetssynpunkt för det aktuella uppdraget. Förfarandet skiljer sig därmed inte från en säkerhetsskyddad upphandling med svenska leverantörer och nationaliteten på leverantörerna saknar i princip betydelse.

Det kan dock ibland av flera skäl vara svårt att få in tillräckligt underlag för att kunna bedöma en utländsk leverantörs lämplighet från ett säkerhetsperspektiv. För det första kan det innebära prak-

[2] Stödet för detta finns i 1 § förordningen (2007:854) med instruktion för Försvarets materielverk.

tiska svårigheter att bedöma om leverantören har lokaler och anläggningar som är lämpliga från säkerhetssynpunkt och som uppfyller de krav på t.ex. fysisk säkerhet och infrastruktur för informationssäkerhet som uppdraget ställer. Vidare kan det föreligga en osäkerhet om vilka rättsliga förutsättningar som finns i det aktuella landet för skydd av de säkerhetsskyddsklassificerade uppgifter eller den i övrigt säkerhetskänsliga verksamheten som leverantören ska hantera i uppdraget. Slutligen kan ett annat land även ha en annan hotbild än Sverige och ha internationella relationer som kan påverka säkerheten för ett uppdrag eller en entreprenad. I de fall där överväganden avseende dessa faktorer, vilket kan göras inom ramen för en säkerhetsskyddsanalys, leder till en bedömning att ett ändamålsenligt säkerhetsskydd kan åstadkommas i det aktuella uppdraget finns det inget som hindrar att en leverantör med säte i utlandet anlitas.

För att underlätta anlitande av utländska leverantörer finns ett antal mekanismer. I Sveriges internationella säkerhetsskyddsöverenskommelser framgår det oftast att parterna ska följa den säkerhetsbedömning avseende leverantörer som den andra partens behöriga myndigheter har genomfört. Vanligtvis bekräftas denna bedömning i ett säkerhetsintyg för leverantör i vilket det framgår mot vilken informationssäkerhetsklass som en bedömning av säkerhetsskyddet har gjorts. I dessa fall ska normalt inte någon ytterligare prövning av leverantören göras av den upphandlande enheten. Undantagsvis kan dock ytterligare prövning behövas, t.ex. när det förekommer uppgifter om en leverantör som kan påverka bedömningen. Samverkan i ärenden som rör säkerhetsintyg görs av de aktuella ländernas behöriga myndigheter, vanligtvis den nationella säkerhetsmyndigheten eller den nationella industrisäkerhetsmyndigheten. Även i dessa fall ska ett säkerhetsskyddsavtal tecknas mellan den upphandlande enheten och leverantören med samma innehåll som om det varit fråga om en svensk leverantör. Viss anpassning av avtalet kan dock behöva göras på grund av den omständigheten att leverantören har sitt säte utanför Sverige.

Säkerhetsprövningen av företagets ledning, styrelseledamöter och anställda som kan antas delta i den säkerhetskänsliga verksamheten kan genomföras på det sätt som gäller för personer bosatta i Sverige eller, vilket är att föredra för personer bosatta utomlands, genom säkerhetsintyg för person (på engelska *Personal Security Clearance, PSC*) som utfärdas av det aktuella landets behöriga

myndigheter. Fördelarna med det sistnämnda alternativet är att säkerhetsmyndigheterna i det land där personalen är bosatt har större möjligheter att inhämta underlag av betydelse för säkerhetsprövningen.

De bestämmelser som ska tillämpas vid säkerhetsskyddade upphandlingar med utländska leverantörer bör kunna meddelas i form av tillämpningsföreskrifter. Säkerhetsintygen behandlas vidare i avsnitt 20.4.

19.3 Närmare om säkerhetsskyddsavtalens innehåll

Allmänt om säkerhetsskyddsavtalens innehåll

Det huvudsakliga syftet med ett säkerhetsskyddsavtal är att reglera de säkerhetsskyddsåtgärder som behövs för den säkerhetskänsliga verksamhet som omfattas av ett kontrakt avseende varor, tjänster eller byggentreprenader. Bland säkerhetsskyddsåtgärderna ingår att avtalet utgör en grund för att besluta om vilka anställningar och annat deltagande hos leverantören som ska placeras i säkerhetsklass.

Säkerhetsskyddsavtalen och upphandlingskontrakten

I en upphandling ställs naturligtvis krav på det som ska upphandlas, dvs. kontraktsföremålet. Dessa krav är i huvudsak inte lagreglerade. Kraven måste dock framför allt vara relevanta och proportionella i förhållande till det som ska upphandlas. När det gäller de krav som kan ställas på leverantören är dessa mestadels lagreglerade för att inte vara diskriminerande leverantörer emellan. Lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS) innehåller bestämmelser som möjliggör för den upphandlande myndigheten eller enheten att ställa krav på leverantören som går längre än vad de normala upphandlingsreglerna tillåter, särskilt i fråga om förmåga att skydda säkerhetsskyddsklassificerade uppgifter.

Enligt 7 kap. 13 § LUFS får en upphandlande myndighet eller enhet kräva att en leverantör uppfyller vissa krav för att skydda säkerhetsskyddsklassificerade uppgifter som myndigheten eller enheten överlämnar under upphandlingsförfarandet. Den upphandlande myndigheten eller enheten får också kräva att en leverantör

ska säkerställa att dess underleverantörer uppfyller sådana krav. Av 7 kap. 14 § LUFS framgår att den upphandlande myndigheten eller enheten i upphandlingsdokumenten (annonsen, förfrågningsunderlaget, det beskrivande dokumentet eller de kompletterande handlingarna) ska precisera alla de åtgärder och krav som är nödvändiga för att trygga säkerheten för säkerhetsskyddsklassificerade uppgifter när det gäller kontrakt som innehåller, inbegriper eller kräver sådana uppgifter.

Av 7 kap. 15 § LUFS framgår att en upphandlande myndighet eller enhet får kräva att anbuden innehåller dels utfästelser från underleverantörerna om att de på lämpligt sätt kommer att skydda säkerhetsskyddsklassificerade uppgifter som de har tillgång till eller som de kommer att få kännedom om under genomförandet av kontraktet och efter det att kontraktet har genomförts eller upphört att gälla, dels information och utfästelser om information om underleverantörerna för att det ska kunna fastställas att de har den kapacitet som krävs för att kunna skydda säkerhetsskyddsklassificerade uppgifter. En upphandlande myndighet eller enhet får kräva att anbuden även innehåller annat för att trygga säkerheten för information.

För att visa sin kapacitet när det gäller kontrakt som inbegriper, kräver eller innehåller säkerhetsskyddsklassificerade uppgifter får leverantören enligt 12 kap. 11 § LUFS använda bevis om förmågan att behandla, lagra och överföra sådana uppgifter på den skyddsnivå som krävs av den upphandlande myndigheten eller enheten. Enligt 12 kap. 12 § LUFS får bevis ges genom ett system för granskning av säkerhetsskyddet. En upphandlande myndighet eller enhet får ge leverantörer som ännu inte har granskats genom ett sådant system en förlängd tidsfrist för att säkerhetsskyddet ska kunna granskas. Den upphandlande myndigheten eller enheten ska i så fall i annonsen om upphandling ange att den möjligheten finns och tidsfristen för att ordna det.

Ett sådant system för granskning av säkerhetsskyddet kan enligt vår bedömning t.ex. utgöras av att den upphandlande enheten genomför ett säkerhetsskyddsbesök hos leverantören för att kunna specificera inom vilka områden säkerhetsskyddet eventuellt måste förbättras. Besöket bör följas upp med en undersökning att de föreslagna åtgärderna har vidtagits innan leverantören kommer i fråga för att delta i upphandlingen.

Att och i viss mån hur kraven på skyddet för säkerhetsskyddsklassificerade uppgifter ska uppfyllas vid en upphandling måste till följd av upphandlingsregleringen finnas med i anbudet och i upphandlingskontraktet. I grunden är denna typ av uppgifter sådana som ett säkerhetsskyddsavtal ska innehålla. De två avtalen kan enligt vår bedömning knytas till varandra genom ett villkor i upphandlingskontraktet att säkerhetsskyddsavtalet ska uppfyllas. I fråga om en försvars- och säkerhetsupphandling ska dock understrykas att det inte går att ställa längre gående krav i ett säkerhetsskyddsavtal än vad upphandlingsreglerna och upphandlingskontraktet medger. Säkerhetsskyddsavtalet kan därför sägas komplettera och precisera upphandlingskontraktet inom ramen för det senare. Det kommer därför att uppstå frågor om hur de två avtalen förhåller sig till varandra och om vad som ska ingå i upphandlingskontraktet i förhållande till vad som ska ingå i säkerhetsskyddsavtalet.

En särskild problematik kan uppstå när de som tecknar upphandlingskontraktet inte är desamma som de som är ansvariga för säkerhetsskyddsavtalet. Säkerhetsskyddsorganisationen kan vara placerad på annat håll än kontraktsparterna i upphandlingen. Det kan gälla både på köpar- och säljarsidan. Det förutsätts att de olika organisationerna ändå kommunicerar med varandra på vardera sidan. I dessa fall gäller nämligen, liksom då avtalsparterna är desamma för de båda avtalen, att några tillkommande krav som inte ryms inom ramen för upphandlingskontraktet inte kan ställas i säkerhetsskyddsavtalet. Med andra ord kan säkerhetsskyddsavtalet inte ändra innehållet i eller de krav som bestämts ska gälla för upphandlingen. Det kan förstås samtidigt vara så att det inte går att vara fullständigt öppen med detaljerna i säkerhetsskyddsfrågor i upphandlingskontraktet. Sådana kanske lämpligen hör hemma i säkerhetsskyddsavtalet eller i den detaljstyrning som den säkerhetsansvariga myndigheten löpande gör efter att avtal tecknats med viss leverantör. Detaljstyrningen måste dock alltid hålla sig inom de krav som ställts i upphandlingen, t.ex. genom säkerhetsskyddsavtalet och eventuell instruktion som bilagts. Vilket innehåll de olika delarna ska ha beror på vad som upphandlas och vilket säkerhetsskydd som behövs. Ett vanligt förekommande krav är placering i säkerhetsklass för personal som ska utföra vissa tjänster. Detta är ett exempel på ett krav som bör finnas med i upphandlingen. Sammanfattningsvis innebär detta att det är viktigt att den från säkerhetsskyddssynpunkt kravställande myndigheten

tydliggör sina krav och samverkar med den upphandlande myndigheten i ett tidigt skede så att den upphandlande myndigheten får möjlighet att ställa adekvata krav avseende säkerhetsskydd i det underlag som tas fram inför upphandlingen.

19.4 Säkerhetsskyddsklassificerade uppgifter i lagen om upphandling på försvars- och säkerhetsområdet (LUFS) och i en ny säkerhetsskyddslag

Förslag: Definitionen av *säkerhetsskyddsklassificerade uppgifter* i 2 kap. 22 § lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet ska ändras något i språkligt hänseende med anledning av tillkomsten av en ny säkerhetsskyddslag, bl.a. när det gäller begreppet *Sveriges säkerhet.* Bestämmelsen ska kompletteras med en hänvisning till att det i säkerhetsskyddslagen finns bestämmelser om skydd för säkerhetsskyddsklassificerade uppgifter.

Begreppet säkerhetsskyddsklassificerade uppgifter i LUFS

Artikel 1.8 i det s.k. LUFS-direktivet[3] definierar *sekretessbelagd information*[4] som ”all information och allt material oavsett dess form, karaktär eller överföringsteknik, som omfattas av krav på en viss säkerhetsnivå eller en viss skyddsnivå och som med hänsyn till den nationella säkerheten och enligt den berörda medlemsstatens gällande lagar och andra författningar måste skyddas mot intrång, förstörelse, avlägsnande, spridning, förlust eller åtkomst av någon obehörig person, eller någon annan typ av risk.”

I propositionen 2010/11:150 Upphandling på försvars- och säkerhetsområdet diskuterades direktivets definition av *sekretessbelagd information*. För att undvika en sammanblandning med offentlighets- och sekretesslagen (2009:400) ansåg regeringen att

[3] Direktiv om samordning av förfarandena vid tilldelning av vissa kontrakt för byggentreprenader, varor och tjänster av upphandlande myndigheter och enheter på försvars- och säkerhetsområdet (2009/81/EG).
[4] Sekretessbelagd information används här som svensk översättning av engelskans *Classified Information*.

detta begrepp inte borde ligga till grund för lagstiftning. I stället föreslog regeringen begreppet *säkerhetsskyddsklassificerade uppgifter* med motiveringen att detta kommit till användning i EU:s regelverk för skydd av uppgifter av säkerhetskänslig karaktär som utväxlas inom unionen. Regeringen hänvisade också till det multilaterala avtal som numera har slutits mellan medlemsstaterna om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse.[5] För att begreppen vid genomförandet av direktivet skulle korrespondera med begreppsbildningen på säkerhetsskyddsområdet och med det europeiska säkerhetsskyddssystem som arbetas fram, ansåg regeringen att begreppet säkerhetsskyddsklassificerade uppgifter var lämpligare än sekretessbelagd information. Regeringen ansåg vidare att definitionen borde vara direktivnära och därför ges samma omfattning som i artikel 1.8. Regeringen konstaterade även att säkerhetsskyddslagen är en sådan nationell lag som direktivet närmast tar sikte på, men att informationssäkerheten i denna lag har en något snävare innebörd än vad som avses i direktivet. I propositionen nämns även den då förestående utredningen om säkerhetsskyddslagen och att begreppsbildningen borde ingå i denna översyn.

Kan en ny säkerhetsskyddslag innebära en sådan nationell lagstiftning som LUFS-direktivet avser?

Begreppet säkerhetsskyddsklassificerade uppgifter tar i LUFS-direktivet sin utgångspunkt i sådan *nationell* lagstiftning i medlemsstaterna som föreskriver ett skydd för uppgifter av betydelse för den nationella säkerheten. Definitionen bör ses mot bakgrund av skälen i direktivets inledning (skäl 20) som anger att ”[u]pphandlingar på försvars- och säkerhetsområdet [ofta] innehåller […] sekretessbelagda[6] uppgifter som obehöriga av säkerhetsskäl inte får ges tillgång till enligt medlemsstaternas gällande lagar och andra författningar.” I skälen anges vidare att ”[p]å det militära området finns det i medlemsstaterna system för att klassificera dessa uppgifter av militära skäl. Vad gäller det icke-militära säkerhetsområdet skiljer sig medlemsstaternas praxis i fall där annan information

[5] UF2009/86882/SSSB.
[6] Härmed avses den officiella översättningen. För en tydligare beskrivning och med ledning av regeringens överväganden bör ordet *sekretessbelagda* utläsas *säkerhetsskyddsklassificerade.*

måste skyddas på liknande sätt. Det är därför lämpligt att använda ett koncept som beaktar medlemsstaternas skiljande praxis och som gör det möjligt att täcka in både det militära och det icke-militära området." Direktivet nämner på flera ställen att en harmonisering mellan medlemsstaternas lagstiftning till skydd för nationell säkerhet vore önskvärd, men att en avsaknad av sådan harmonisering medför att direktivet måste kunna tillämpas inom den variation som de olika medlemsstaternas lagstiftning på området innebär.

När det gäller genomförandet av LUFS-direktivet i svensk rätt innebar den nuvarande säkerhetsskyddslagstiftningen med sitt begränsade tillämpningsområde att den inte fullt ut lämpade sig att koppla till LUFS som en sådan nationell lagstiftning som LUFS-direktivet hänvisar till. Säkerhetsskyddslagens *hemliga uppgifter* var därmed ett olämpligt begrepp att använda i definitionen av säkerhetsskyddsklassificerade uppgifter i LUFS. Detta innebar att en annan konstruktion fick användas med en egen definition av säkerhetsskyddsklassificerade uppgifter i LUFS som på ett mer allmänt sätt hänvisar till andra författningars krav på skydd för sådana uppgifter.

I kapitel 12 har vi redogjort för en ny systematik som innebär att det som en ny säkerhetsskyddslag ska skydda omfattar mer än hemliga uppgifter i nuvarande säkerhetsskyddslag. Vi föreslår att begreppet *säkerhetsskyddsklassificerade uppgifter* införs som en benämning på sådana uppgifter som är av betydelse för Sveriges säkerhet *eller* som ska ges ett skydd enligt ett internationellt säkerhetsskyddsåtagande, och som till sin natur är en sådan uppgift som avses i bestämmelser om sekretess i offentlighets- och sekretesslagen. Begreppet anknyter till engelskans *Classified Information* vilket även används i den engelska versionen av LUFS-direktivet. Ett exempel på ett internationellt säkerhetsskyddsåtagande är det ovan nämnda avtalet mellan EU:s medlemsstater om skydd för säkerhetsskyddsklassificerade uppgifter inom EU. Även i detta fall används säkerhetsskyddsklassificerade uppgifter som svensk översättning av *Classified Information.*

Vi föreslår även att en ny säkerhetsskyddslag utformas på ett sådant sätt att det tydliggörs att den omfattar såväl civil som militär verksamhet, även om detta gäller även för nuvarande säkerhetsskyddslag. Sammantaget finns det alltså förutsättningar för att en ny säkerhetsskyddslag skulle kunna utgöra en sådan nationell lagstiftning som avses i LUFS-direktivet.

Analys av innebörden av en begreppsharmoni

Under vår internationella utblick konstaterade vi att den finska lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) i sin första paragraf har en hänvisning till den finska lagen om offentlig försvars- och säkerhetsupphandling (1531/2011) vilken genomför LUFS-direktivet i finsk rätt. Denna sistnämnda lag definierar *säkerhetsklassificerad handling* som ”en handling eller uppgifter i en handling som i enlighet med lag eller en bestämmelse som utfärdats med stöd av lag har försetts med en anteckning om säkerhetsklass.” Bestämmelser om ”anteckning om säkerhetsklass” finns i lagen om internationella förpliktelser som gäller informationssäkerhet. Genom denna konstruktion fås en samstämmighet mellan säkerhetsklassificeringen enligt finsk säkerhetslagstiftning och den finska lagen om offentlig försvars- och säkerhetsupphandling.

Vi har i kapitel 10 redogjort för olika perspektiv på säkerhetsskydd där en utgångspunkt i informationssäkerheten är vanligt förekommande i andra länders lagstiftning och även i internationella regelverk. Vi har där konstaterat att det för svensk del ändå är mest ändamålsenligt att en ny säkerhetsskyddslag liksom tidigare är verksamhetsorienterad, framför allt för att säkerhetsskydd ska kunna omfatta säkerhetskänslig verksamhet som inte rör information, t.ex. kärnteknisk verksamhet. Att en svensk lagstiftning i det avseendet har ett vidare perspektiv än LUFS-direktivet anser vi inte vara problematiskt utifrån en lösning där begreppet säkerhetsskyddsklassificerade uppgifter är samstämmiga i båda lagstiftningarna. I vårt förslag till en ny säkerhetsskyddslag är begreppet centralt på ett sådant sätt att det har en direkt betydelse för vilka säkerhetsskyddsåtgärder som kan vidtas. Därför blir en ny säkerhetsskyddslags bestämmelser om säkerhetsskyddsåtgärder som personalsäkerhet och fysisk säkerhet tillämpliga i upphandlingssituationer med krav på informationssäkerhet på ett sådant sätt som LUFS-direktivet förutsätter. Det torde därför inte finnas någon risk att för upphandlingen viktiga säkerhetsskyddsåtgärder inte kan vidtas.

Kan en begreppsharmoni innebära en otillåten inskränkning av LUFS-direktivets tillämpning i svensk rätt

LUFS-direktivets införande i svensk rätt innebär att begreppet säkerhetsskyddsklassificerade uppgifter har definierats som ”information och material oavsett form, karaktär eller överföringsteknik som omfattas av krav på en viss säkerhetsnivå eller en viss skyddsnivå och som med hänsyn till rikets säkerhet enligt lagar och andra författningar måste skyddas mot intrång, förstörelse, avlägsnande, spridning, förlust eller åtkomst av någon obehörig person, eller någon annan typ av risk.” Definitionen har stor likhet med definitionen i direktivet. Frågan är om begreppet i LUFS kan ändras till att i stället hänvisa till begreppets definition i en ny säkerhetsskyddslag, utan att en sådan ändring innebär en inskränkning av LUFS-direktivets tillämpningsområde. En inskränkning skulle i värsta fall kunna innebära att Sverige gör sig skyldig till fördragsbrott. Frågan måste därför analyseras noggrant.

Begreppet i sin nuvarande utformning i LUFS kan delas upp i fyra huvudmoment:

- Informationens form,
- krav på skyddsnivå,
- betydelsen för rikets säkerhet, samt
- mot vad informationen ska ges ett skydd.

Definitionens fyra olika moment behandlas i det följande. I vårt förslag till säkerhetsskyddslag görs inte någon skillnad på hur den information som lagen tar sikte på är beskaffad. Säkerhetsskyddsklassificerade uppgifter kan därför förekomma i pappersdokument, i elektronisk form och i uppgifter som innefattas i, eller kan utläsas av, material i olika former. Det som ska ges ett skydd är informationen som sådan, oavsett form. Detta ska ses mot definitionen i LUFS-direktivet där det anges att *informationens form*, karaktär och överföringsteknik saknar betydelse, vilket måste anses ha samma innebörd som i vårt förslag till säkerhetsskyddslag.

Kravet på *skyddsnivå* i definitionen tas om hand av säkerhetsskyddslagstiftningen som helhet genom att lagens huvudsyfte är att reglera ett sådant (säkerhets)skydd som LUFS-direktivet torde

avse. Skyddsnivåerna kommer till uttryck i såväl säkerhetsskyddslagen som i tillämpningsföreskrifter till denna lag.

I avsnitt 11.2 föreslår vi att begreppet *rikets säkerhet* ändras till Sveriges säkerhet. Skälet till detta är främst språkligt. Begreppet har även nyligen ändrats på ett sådant sätt i spioneribrottet, 19 kap. 5 § brottsbalken.[7] Säkerhetsskyddslagens och LUFS avgränsning är därmed samstämmiga i det avseendet, även om lydelsen skiljer sig åt.

Frågan om *mot vad* den säkerhetskänsliga verksamheten ska ges ett skydd behandlas i avsnitt 11.5. I första hand ska en ny lag ge ett skydd mot antagonistiska brott som direkt eller indirekt kan hota säkerhetskänslig verksamhet. När det gäller säkerhetsskyddsklassificerade uppgifter föreslås att det liksom i nuvarande säkerhetsskyddslag också ges ett skydd i andra fall (än mot brott) för sådana uppgifter. Av förarbetena till nuvarande lag framgår att skyddet ska motverka allt röjande, ändrande och förstörande av sekretessbelagda uppgifter som rör rikets säkerhet, oavsett om det sker uppsåtligen eller av oaktsamhet.[8] Detta gäller oförändrat även i vårt förslag till en ny lag. Denna omfattning av skyddet måste anses täcka de hot mot informationen som anges i LUFS-direktivet.

Utifrån denna analys hade det kunnat övervägas om definitionen i LUFS skulle ersättas med enbart en hänvisning till definitionen av säkerhetsskyddsklassificerade uppgifter i vårt förslag till ny säkerhetsskyddslag. Detta vore av tydlighetsskäl en bra lösning. Det bör dock analyseras vidare om en sådan ändring på ett otillåtet sätt skulle kunna inskränka tillämpningen av LUFS. Vi föreslår därför en smärre språklig ändring i LUFS definition av säkerhetsskyddsklassificerade uppgifter samt en hänvisning i definitionen om att det finns bestämmelser om skydd för säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddslagen.

[7] Prop. 2013/14:51 Förstärkt skydd mot främmande makts underrättelseverksamhet.
[8] Prop. 1995/96:129 Säkerhetsskydd, s. 26 f. och särskilt Lagrådets yttrande s. 129.

19.5 Underrättelse till Säkerhetspolisen

En tydligare uppföljning av företag som omfattas av säkerhetsskyddsavtal

Det finns inget som hindrar att en leverantör har säkerhetsskyddsavtal med flera kommuner, landsting och statliga myndigheter. Det kan, genom att säkerhetsskyddsavtalen är kopplade till uppdrag, även finnas leverantörer som har flera säkerhetsskyddsavtal med samma myndighet. Följden av detta är att det hos en leverantör kan förekomma säkerhetsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet i en relativt stor omfattning. I säkerhetsskyddslagstiftningen finns förvisso en skyldighet för de som ingår ett säkerhetsskyddsavtal att anmäla detta till Säkerhetspolisen liksom även när ett sådant avtal upphör.[9] Uppgifterna om gällande säkerhetsskyddsavtal som på detta sätt rapporteras till Säkerhetspolisen har hittills inte varit föremål för sammanställning eller analys. Det är sannolikt att en analys av leverantörernas samlade uppdrag skulle ge upplysningar om att betydande mängder av säkerhetsskyddsklassificerade uppgifter kan förekomma hos vissa leverantörer och att säkerhetsskyddet, som är anpassat till respektive uppdrag, vid en samlad bedömning är otillräckligt. En sådan leverantör har troligtvis även en högre hotbild än leverantörer med enbart enstaka uppgifter.

Anmälan och avanmälan

Myndigheter ska som redovisats ovan underrätta Säkerhetspolisen om säkerhetsskyddsavtal som träffats och om säkerhetsskyddsavtal som har upphört. För att kravet ska bli tydligare och för att det ska gälla alla som ingår ett säkerhetsskyddsavtal föreslår vi att en bestämmelse med ett sådant krav tas in i förordning i stället för att som nu meddelas i tillämpningsföreskrifter. Förordningens bestämmelser om sådan rapportering ska gälla även för enskilda, kommuner och landsting genom en generell bestämmelse om rapportering i vårt förslag till säkerhetsskyddslag (se kapitel 14).

Säkerhetspolisen bör i föreskrifter närmare reglera hur rapporteringen ska gå till och vilka uppgifter rapporteringen ska innehålla.

[9] 7 kap. 8 § Rikspolisstyrelsens föreskrifter om säkerhetsskydd, RPSFS 2010:03.

20 Internationell samverkan

En ny säkerhetsskyddslagstiftning ska inte enbart tillvarata behovet av ett skydd för säkerhetskänslig verksamhet i Sverige utan även kunna tillämpas vid samarbeten med andra länder och mellanfolkliga organisationer. Vidare ska lagstiftningen enligt direktiven ge stöd för de folkrättsliga förpliktelser på säkerhetsskyddsområdet som följer av internationella överenskommelser och EU-rätten.

Regeringen har ansvaret för Sveriges relationer med andra stater och med mellanfolkliga organisationer. Till följd av den svenska förvaltningsmodellen är en stor del av arbetet med detta – formellt eller de facto – delegerat till olika förvaltningsmyndigheter. En mer allmän princip för arbetsfördelningen mellan regeringen och Regeringskansliet å ena sidan och förvaltningsmyndigheterna å den andra är numera att operativa uppgifter så långt det är möjligt ska delegeras till och utföras av förvaltningsmyndigheter. Detta gäller i princip även på det område som vi här intresserar oss för.

Strukturen på våra internationella relationer präglas numera i hög grad av vårt medlemskap i EU och av arbetet där. I det arbetet har regeringen också en skyldighet att samråda med riksdagen genom dess EU-nämnd. Likväl bedrivs en mycket stor del av Sveriges EU-arbete av förvaltningsmyndigheternas personal, låt vara då formellt som företrädare inte för den egna myndigheten utan för Sverige och i vissa fall med mer eller mindre uttryckliga instruktioner från Regeringskansliet.[1] Myndigheterna har sin lydnadsplikt men agerar i många sammanhang fristående också i internationella sammanhang.

I allt väsentligt fungerar Sveriges internationella samarbete på området för säkerhetsskydd väl. De personer från Regerings-

[1] Se t.ex. betänkandet Styra och ställa – förslag till en effektivare statsförvaltning (SOU 2008:118), avsnitt 2.3.

kansliet och myndigheterna som är engagerade i arbetet har i regel hög kompetens och Sverige har gott anseende såväl multilateralt – EU, NATO, ESA m.fl. – som bilateralt. Vi har också åtskilliga internationella avtal och andra överenskommelser som är adekvata och relevanta och som tjänar oss väl.

Här finns emellertid också naturligtvis en viss förbättringspotential.

Sveriges medverkan i vissa internationella fora, främst inom EU-strukturen, är inte tillräckligt väl fokuserad vad gäller vare sig vilka sammanhang vi ska delta i eller var i den nationella strukturen uppgiften ska ligga. En del frågor av operativ natur hanteras i Regeringskansliet (UD) i stället för i en förvaltningsmyndighet vilket skulle te sig lämpligare, både principiellt och praktiskt. Över huvud taget ter sig arbetsfördelningen ibland snarare slumpartad än genomtänkt. Visserligen finns en bestämmelse i instruktionen för Regeringskansliet som pekar ut UD som svensk nationell säkerhetsmyndighet, men det är ändå i många sammanhang oklart vilka vägar och kanaler som ska begagnas för kontakter mellan våra internationella samarbetspartners och den svenska administrationen. Våra internationella förpliktelser medför krav på att detta ska vara så tydligt som möjligt och att en nationell säkerhetsmyndighet ska pekas ut.

För att ytterligare underlätta och tydliggöra internationellt samarbete på säkerhetsskyddsområdet måste ställning tas till vilka kanaler som ska användas för internationella säkerhetsskyddsfrågor mellan å ena sidan Sverige och å andra sidan andra länder och mellanfolkliga organisationer samt vilka uppgifter som vissa myndigheter bör ha i detta avseende.

I detta kapitel beskrivs vilka uppgifter en nationell säkerhetsmyndighetsfunktion bör ha och vilka krav som dessa uppgifter ställer (avsnitt 20.1). Därefter följer en beskrivning av övriga samverkansfunktioner för industrisäkerhet, informationssäkring och kryptografisk säkerhet (avsnitt 20.2). Efter det följer en analys av vid vilken eller vilka myndigheter funktionerna bör finnas och förslag avseende detta (avsnitt 20.3). Avslutningsvis redovisas hur utfärdandet av säkerhetsintyg för personer och leverantörer bör regleras (avsnitt 20.4). Frågan om rapportering i fall då en uppgift som omfattas av ett internationellt säkerhetsskyddsåtagande kan ha röjts behandlas i avsnitt 21.4.

20.1 Uppgifter för en nationell säkerhetsmyndighet, m.m.

I för Sverige bindande internationella säkerhetsskyddsåtaganden finns bestämmelser om Sveriges internationella funktioner inom säkerhetsskyddsområdet. Den huvudsakliga funktionen är en *nationell säkerhetsmyndighet* (på engelska *National Security Authority*, vanligtvis förkortat *NSA*[2]). Trots namnet avses inte en myndighet i svensk betydelse utan snarare en myndighetsunktion, även om inget hindrar att en myndighet organiseras med denna funktion som huvudsaklig uppgift (som i t.ex. Norge och Tjeckien).

Den nationella säkerhetsmyndighetens ansvar beskrivs på ett likartat sätt i Rådets säkerhetsbestämmelser[3] och i Sveriges åtaganden gentemot Nato. I artikel 6 i det administrativa avtalet med Nato[4] anges att den svenska nationella säkerhetsmyndigheten ska försäkra att säkerhetsåtgärder genomförs och övervaka skyddet av säkerhetsskyddsklassificerad information som Sverige har fått från Nato. Av Sveriges avtal med Nato från 1994[5] framgår också att den nationella säkerhetsmyndigheten förväntas ha ett ansvar liknande det som Natos säkerhetskontor har för Natos verksamhet (*Nato Office of Security*). På liknande sätt framgår det i Rådets säkerhetsbestämmelser[6] att EU:s medlemsstater bör utse en nationell säkerhetsmyndighet som är ansvarig för säkerhetsarrangemang så att åtgärder vidtas för skyddet av säkerhetsskyddsklassificerade EU-uppgifter.

EU:s och Natos regelverk beskriver den nationella säkerhetsmyndighetens ansvarsområden. Där nämns bl.a. att skyddet av säkerhetsskyddsklassificerade uppgifter ska upprätthållas, att säkerhetsfrågor som rör skydd av säkerhetsskyddsklassificerade uppgifter ska samordnas med övriga nationella myndigheter och att funktionen ska vara registreringsenhet för handlingar i den högsta informationssäkerhetsklassen. Vidare ska säkerhetsintyg för perso-

[2] Det är viktigt att notera att denna förkortning inte har något att göra med den amerikanska signalspaningsmyndigheten *National Security Agency*, som förkortas på samma sätt.
[3] Rådets beslut av den 23 september 2013 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter, 2013/488/EU.
[4] Administrative Arrangement for the Handling and Protection of Nato Classified Information Provided to Sweden, 2012-06-14 (överenskommelsen är inte publicerad i SÖ).
[5] Security Agreement between the Government of Sweden and the North Atlantic Treaty Organization, 1994-09-06 (överenskommelsen är inte publicerad i SÖ).
[6] 2013/488/EU, Artikel 16.3 a.

ner som ska ges tillgång till uppgifter på en viss informationssäkerhetsklass kunna utfärdas och ansökningar om säkerhetsintyg för personer och leverantörer hanteras.

Till dessa uppgifter kommer sådana som verksamheten förutsätter, som att representera Sverige när det gäller internationella säkerhetsskyddsfrågor, att förhandla internationella säkerhetsskyddsöverenskommelser med andra länder och mellanfolkliga organisationer och att hantera och skyndsamt rapportera informationsförluster och säkerhetshändelser som rör uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande.

Den nationella säkerhetsfunktionen ska även vara kontaktpunkt gentemot EU och Nato för information om regeländringar som medlemsstaten förväntas ta hänsyn till och delta i olika internationella arbetsgrupper, däribland Rådets säkerhetskommitté.[7]

Funktionen nationell säkerhetsmyndighet förekommer även i ett antal internationella åtaganden som exempelvis i säkerhetsskyddsöverenskommelsen rörande samarbetet inom Europeiska rymdorganet (ESA)[8] samt i bilaterala säkerhetsskyddsöverenskommelser. Även om dess roll i dessa överenskommelser, särskilt i de sistnämnda, vanligen inte är lika tydligt beskriven som i EU:s och Natos regelverk, så får det antas att det är liknande uppgifter som följer av dessa överenskommelser. Så tillämpas överenskommelserna också av EU:s och Natos medlemsstater.

20.2 Funktioner för informationssäkring, kryptografisk säkerhet och industrisäkerhet

Specialiserade funktioner

Enligt Rådets säkerhetsbestämmelser ska medlemsstaterna utse funktioner för informationssäkring[9], för skydd mot s.k. röjande signaler[10] samt för godkännande och distribution av kryptografisk

[7] 2013/488/EU, artikel 17.2.
[8] Avtal mellan de stater som är parter i konventionen om upprättande av ett europeiskt rymdorgan och Europeiska rymdorganet om skydd och utbyte av klassificerad information (SÖ 2004:60).
[9] Den svenska officiella översättningen av *Information Assurance*.
[10] Röjande signaler, normalt förkortat RÖS, är en beteckning på de elektromagnetiska fält som genereras av elektriska apparater och vissa ledningar. Dessa fält kan uppfångas med olika typer av mottagare och därmed kan informationen röjas.

materiel. Vidare kan medlemsstaterna ha en utsedd säkerhetsmyndighet för industrisäkerhetsfrågor (på engelska *Designated Security Authority, DSA*).

Informationssäkring

I bilaga IV till Rådets säkerhetsbestämmelser beskrivs att medlemsstaterna ska bl.a. utveckla strategier och säkerhetsriktlinjer för informationssäkring och övervaka hur ändamålsenliga och relevanta dessa är, skydda och administrera teknisk information som rör kryptoprodukter, samordna utbildning i informationssäkring och samråda med systemleverantörer, säkerhetsaktörer och företrädare för användare när det gäller säkerhetsstrategier och säkerhetsriktlinjer för informationssäkring.

Uppgifterna är av huvudsakligen teknisk natur och kopplade till it- och kommunikationssystem som är avsedda för säkerhetsskyddsklassificerade uppgifter. Under senare tid har cybersäkerhetsfrågorna fått en allt större internationell betydelse. När det gäller begreppet cybersäkerhet och hur frågor kring denna verksamhet ska hanteras är utredningen NISU 2014[11] av särskilt intresse. Utredningen ska överlämna sitt betänkande senast den 1 mars 2015 och utredarens förslag kan i vissa avseenden få betydelse även för innehållet i en ny säkerhetsskyddslag, särskilt när det gäller organisatoriska frågor.

I Sverige där ansvaret för it-säkerhetsfrågorna är decentraliserat till fristående myndigheter och verksamheter blir funktionen, utöver det som följer av bestämmelser om tillsyn och rätt att meddela föreskrifter, snarast en rådgivande och samordnande funktion. En uppgift är att utfärda intyg om att nationella it-system som ska anslutas till internationella system uppfyller de säkerhetskrav som fastställts för systemet. Detta torde kunna bygga på rapportering från den verksamhet som berörs av systemet och det samrådsförfarande som krävs när en myndighet överväger att inrätta ett it-system inom ramen för sin säkerhetskänsliga verksamhet (se vidare avsnitt 16.4). Ett beslut om ackreditering kan också ingå i underlaget till ett sådant intyg.

[11] Direktiv 2013:110 Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system.

Godkännande och distribution av kryptografisk materiel

Att utforma ett skydd för uppgifter med kryptografiska funktioner kräver en särskild teknisk kompetens på området. De flesta av EU:s medlemsstater har därför valt att samla denna kompetens till ett utpekat nationellt organ som i Rådets säkerhetsbestämmelser benämns myndighet för godkännande av krypto (eng. *Crypto Approval Authority, CAA*[12]). Den kryptogodkännande myndigheten ska ansvara för att kryptoprodukter överensstämmer med nationell kryptopolicy och i de fall som det är relevant även Rådets kryptopolicy. Den ska godkänna kryptoprodukter för att skydda säkerhetsskyddsklassificerade EU-uppgifter i deras driftsmiljö upp till en fastställd säkerhetsskyddsklassificeringsnivå. Från denna myndighet kan uppgifterna att distribuera kryptografisk materiel särskiljas till ett särskilt organ som då har uppgiften att förvalta och redovisa sådan materiel som används för kryptering av säkerhetsskyddsklassificerade uppgifter, säkerställa att lämpliga förfaranden följs och att kanaler upprättas för redovisning, säker hantering, förvaring och distribution av kryptomaterial.

I sammanhanget kan nämnas att Sverige har en lång tradition av hög kompetens på kryptoområdet och för närvarande är ett av sex länder inom EU som av Rådet fått förtroende att andrapartsevaluera[13] kryptografiska produkter som utvecklas i andra medlemsstater (AQUA[14]).

En kryptogodkännande myndighet har i uppgift att representera Sverige i internationella kryptografiska samarbeten och meddela föreskrifter om hantering av kryptografisk materiel. Den ska också förhandla bilaterala och multilaterala överenskommelser om kommunikationssäkerhet och skydd för kryptografisk materiel samt i tillämpliga fall vara nyckelproduktionsmyndighet och nationell nyckeldistributionsmyndighet i internationella samarbeten.

[12] Inom Nato används begreppet *National Communication Security Authority, NCSA*
[13] En andrapartsevaluering innebär i detta fall att ett utsett lands kryptogodkännande myndighet utvärderar en kryptografisk funktion som har utvecklats i ett annat land.
[14] AQUA står för *Appropriately Qualified Authority*. För att bli ett s.k. AQUA-land ställs mycket höga krav på kompetens inom kryptoområdet.

Industrisäkerhet

I vissa medlemsstater är industrisäkerhetsfrågorna en del av den nationella säkerhetsmyndighetens ansvar och i dessa fall finns det ingen särskilt utpekad industrisäkerhetsfunktion.

Om det inrättas en separat industrisäkerhetsmyndighet, bör den ha i uppgift att förhandla bilaterala och multilaterala projektsäkerhetsöverenskommelser, kunna intyga säkerheten hos leverantörer som hanterar eller avser att hantera uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande eller som avser att delta i internationella upphandlingar som innebär tillgång till sådana uppgifter, utfärda säkerhetsintyg för leverantörer och deras personal när det behövs för internationellt samarbete eller internationella upphandlingar, administrera internationell besöksbegäran (på engelska s.k. *Request for Visit, RfV*) för besök inom ramen för internationella projekt och utöva tillsyn av leverantörer som hanterar uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande.

20.3 Organisatoriska frågor och överväganden

Förslag: Den myndighet som regeringen bestämmer ska pekas ut som nationell säkerhetsmyndighet och nationell industrisäkerhetsmyndighet.

Regeringen bör i förordning ange Försvarsmakten som nationell säkerhetsmyndighet. Försvarsmakten ska dock om det är lämpligt, i fråga om andra ärenden än sådana som rör registerkontroll och säkerhetsintyg för person, till Säkerhetspolisen lämna över ärenden som främst rör Säkerhetspolisens tillsynsområde.

Regeringen bör i förordning ge Försvarets materielverk i uppgift att vara nationell industrisäkerhetsmyndighet.

I ett fåtal överordnade samarbetsstrukturer, t.ex. när det gäller att representera Sverige i EU:s säkerhetskommitté och i ställningstaganden inför möten i rådet, bör Regeringskansliet mera direkt kunna leda verksamheten. Detta fordrar ingen särskild reglering utan kan lösas under hand mellan Regeringskansliet och respektive myndighet.

Instruktioner till Försvarsmakten, Säkerhetspolisen och Försvarets materielverk bör, i den mån sådana behövs, hanteras genom sedvanlig gemensam beredning i Regeringskansliet.

Försvarsmakten och Försvarets materielverk bör i förordning ges rätt att utfärda föreskrifter för respektive ansvarsområden.

Nuvarande ordning

I Sverige ansvarar Utrikesdepartementet för den nationella säkerhetsmyndighetsfunktionen gentemot EU och Nato och gentemot västeuropeiska försvarsunionen (WEU).[15] Även när det gäller Sveriges förhållande till ESA så har Utrikesdepartementet denna roll. En stor del av uppgifterna löses genom stöd från andra myndigheter.

För bilateral samverkan är Försvarsmakten utpekad att fullgöra uppgiften som nationell säkerhetsmyndighet. Denna uppgift grundar sig inte på någon författningsreglering utan följer av bestämmelser i de generella säkerhetsskyddsöverenskommelser som Sverige har ingått med ett trettiotal länder.

Försvarets materielverk har möjlighet att genomföra säkerhetsskyddad upphandling med säkerhetsskyddsavtal med företag som ska delta i internationella säkerhetskänsliga projekt som rör utveckling eller produktion av försvarsmateriel. Detta utgör en delmängd av de uppgifter som kan ankomma på en industrisäkerhetsmyndighet utan att detta har formulerats så.[16]

Avseende funktionen som nationell kryptogodkännande myndighet anges Försvarsmakten som sådan myndighet i en skrivelse från Utrikesdepartementet till Europeiska unionens råd 2007.

Den nuvarande ordningen beskrivs mer utförligt i avsnitt 6.3. Sammanfattningsvis är ordningen på detta område endast i någon mån formaliserad. Det innebär en otydlighet i fråga om ansvarsförhållanden vilket försvårar samordning, styrning och uppföljning av verksamheten.

[15] 20 § 8 förordningen (1996:1515) med instruktion för Regeringskansliet. Eftersom WEU har upphört 2011 torde även funktionen som nationell säkerhetsmyndighet gentemot WEU vara avslutad.

[16] Den enda konkreta bestämmelsen är 17 § säkerhetsskyddsförordningen som ger Försvarets materielverk en möjlighet att i vissa fall ingå avtal med leverantörer om det behövs för deltagande i internationell verksamhet.

Styrande principer för en nationell säkerhetsmyndighet

Konstruktionen av en nationell säkerhetsmyndighetsfunktion måste anpassas till svenska förhållanden och utgå från nuvarande organisatoriska förutsättningar och från de principer som finns i statsförvaltningen. Samtidigt måste de folkrättsliga kraven på funktionen beaktas och internationell samverkan underlättas.

År 2014 var ungefär 15–20 personer engagerade i den nationella säkerhetsmyndighetsfunktionen i varierande omfattning. Antalet årsarbetskrafter är väsentligt lägre. Till detta kommer att ett rationellt nyttjande av resurser som redan finns avseende t.ex. tillsyn och utfärdande av tillämpningsföreskrifter kan ge samordningsvinster som reducerar behovet av resurser för verksamheten.

Vi ser inte behov av mera dramatiska förändringar av hur Sverige ska organisera och hantera det internationella samarbetet rörande säkerhetsskydd. Vissa justeringar bör dock göras.

Den svenska förvaltningsmodellen med relativt sett små ministerier och fristående förvaltningsmyndigheter som finns utanför ministerierna och till vilka uppgifter i stor utsträckning delegeras ger andra förutsättningar än de som gäller i resten av EU utom Finland. Det ter sig i vårt system inte ändamålsenligt att fullt ut samla alla funktioner på ett ställe, utan de bör snarare fördelas så vitt möjligt på samma sätt som motsvarande nationella funktioner, låt vara att onödig splittring bör undvikas. Våra internationella partners ska så enkelt som möjligt kunna orientera sig i vårt system och lätt kunna identifiera korrekta ingångar. Uppgifterna bör fördelas på så få myndigheter som möjligt med en utpekad myndighet som huvudansvarig för funktionen. Regleringen kring funktionen bör hållas så enkel som möjligt och med utgångspunkt från säkerhetsskyddslagstiftningen. Detaljerade bestämmelser om hur funktionen ska utövas bör inte krävas.

Det står vidare klart att alltför mycket, däribland mer operativa uppgifter, hanteras av Regeringskansliet, visserligen med bistånd från förvaltningsmyndigheterna. Ambitionen bör vara att från Regeringskansliet föra ut allt som inte oundgängligen måste utföras där.

Det finns också skäl att tro att vårt deltagande i multilaterala samarbetsstrukturer bör kunna fokuseras mer.

Alternativa lösningar

Ett alternativ är att en ny nationell säkerhetsskyddsmyndighet inrättas enligt norsk modell, som innebär att en ny myndighet ansvarar för säkerhetsskyddet nationellt och internationellt. Till denna myndighet överförs huvuddelen av den säkerhetsskyddskompetens som i dag finns hos Säkerhetspolisen och i Försvarsmakten. I myndigheten samlas samtliga internationella funktioner (för informationssäkring, krypto och industrisäkerhet). Tillsyn och föreskriftsrätt avseende säkerhetsskydd skulle i detta alternativ överföras till den nya myndigheten. Det vore olämpligt och skulle skapa oklarhet och besvärliga gränsdragningsproblem att ha olika ansvarsfördelning för nationella och internationella säkerhetsskyddsfrågor. Detta alternativ bör därför bygga på att ansvaret för samtliga säkerhetsskyddsfrågor förs över till en ny myndighet. Ett ytterligare skäl till det är att de uppgifter som ankommer enbart på den nationella säkerhetsmyndigheten inte är så omfattande att de skulle kunna motivera en helt ny myndighet. Alternativet med en helt ny myndighet för nationella och internationella säkerhetsskyddsfrågor skulle innebära genomgripande förändringar i fråga om t.ex. tillsyn och tillämpningsföreskrifter i förhållande till vad som gäller i dag.

Vi anser att det inte är ett bra alternativ att inrätta en ny myndighet. En fråga som tas upp i våra direktiv – den om övergång till ett klareringssystem – hade möjligen kunnat motivera mer genomgripande organisatoriska förändringar. Våra överväganden i den delen som innebär att nuvarande system i huvudsak behålls gör dock att vi inte ser några behov av sådana organisatoriska förändringar som möjligen skulle ha behövts i ett renodlat klareringssystem (se vidare i avsnitt 10.1.5 och 18.3). Utredningen har vidare hämtat in behovsbeskrivningar från utredningens experter och även vissa intressenter utanför expertkretsen, bl.a. Näringslivets säkerhetsdelegation. Något behov av att genomgripande organisatoriska förändringar har inte kommit fram. Härtill kommer att våra direktiv och den förstudie som föregick direktiven utgår från att nuvarande ansvarsfördelning i fråga om säkerhetsskydd mellan Säkerhetspolisen och Försvarsmakten bör bibehållas. Sammanfattningsvis kan man säga att den nuvarande uppdelningen av säkerhetsskydds-

frågorna mellan Säkerhetspolisen och Försvarsmakten fungerar bra och bör finnas kvar i en reformerad säkerhetsskyddslag.

Ett annat alternativ är att hela den nationella säkerhetsmyndighetsfunktionen placeras i Regeringskansliet. Alternativet är dock inte lämpligt. För det första är ärendena som funktionen ska hantera i stor utsträckning operativa och av förvaltningskaraktär. Vidare krävs i så fall en uppdelning av internationella och nationella säkerhetsskyddsfrågor. Alternativet kräver även ett omfattande stöd från flera förvaltningsmyndigheter vilket kan innebära komplicerad samordning och resursfördelning i ärenden där det ställs krav på snabb hantering. Slutligen kompliceras frågorna om tillsyn och tillämpningsföreskrifter av en sådan lösning eftersom dessa uppgifter svårligen kan lösas av Regeringskansliet.

Ett tredje alternativ är att funktionen placeras hos Säkerhetspolisen. Huvudskälet för denna lösning skulle vara att myndigheten har det övergripande säkerhetsskyddsansvaret i Sverige. Liknande lösningar finns i Tyskland och Nederländerna (civila säkerhetstjänster, dock utan polisiära befogenheter). Säkerhetspolisen har ett ansvar för säkerhetsskyddsfrågor när det gäller tillsyn av och föreskrifter om säkerhetsskyddet. Myndigheten har därför resurser och kompetens kring tillsyn och normgivning på säkerhetsskyddsområdet.

En omständighet som talar emot en sådan lösning är att ärendenas karaktär i stor utsträckning kommer att kräva samverkan med Försvarsmakten och myndigheter inom Försvarsmaktens tillsynsområde. Detta gäller en stor delmängd av ärendena. Ett annat skäl som talar emot detta alternativ är att Säkerhetspolisens internationella samverkan huvudsakligen är inriktad mot underrättelsesamarbete och inte säkerhetsskydd. Slutligen skulle hanteringen av säkerhetsintyg för person medföra oönskade konsekvenser från ett integritetsperspektiv som utvecklas närmare nedan under avsnitt 20.4.2).

Ett fjärde alternativ är att funktionen, med undantag för vad som fortsatt bör hanteras i Regeringskansliet, placeras i Försvarsmakten. Detta överensstämmer med nuvarande ordning avseende den tillsyn och föreskriftsrätt som Försvarsmakten har över myndigheter inom försvarssektorn. Vid myndigheten finns det redan i dag en nationell säkerhetsmyndighetsfunktion för bilaterala samarbeten. Där finns också kompetens och resurser för att genomföra

förhandlingar om internationella säkerhetsskyddsöverenskommelser och genom detta även kompetens att representera Sverige. Vidare finns vid myndigheten kompetens kring internationella kryptofrågor, och myndigheten utövar redan i dag rollen som nationell kryptogodkännande myndighet med internationell representation i olika kryptosamarbeten, t.ex. AQUA. Med detta sammanhänger även kompetens kring informationssäkring och cybersäkerhet och dess tillämpning i internationella miljöer. Vidare rör de internationella säkerhetsskyddsärendenas karaktär fortfarande ofta försvarssektorn, även om en förskjutning mot civila ärenden sker.[17] Myndigheten har internt utvecklat ett regelverk som stöd för internationella åtaganden på säkerhetsskyddsområdet vilket torde kunna användas vid framtagande av tillämpningsföreskrifter för även andra myndigheter.[18] Försvarsmakten utövar i dag tillsyn av säkerhetsskyddet vid vissa utpekade myndigheter vilka hanterar en stor del av de säkerhetsskyddsklassificerade uppgifterna som omfattas av internationella säkerhetsskyddsåtaganden. Försvarsmakten utfärdar även huvuddelen av säkerhetsintygen för person (på engelska *Personnel Security Clearance Certificate*, *PSCC*) och har rutiner och administrativt stöd för detta. Myndigheten kan också i den nationella säkerhetsmyndighetsfunktionen dra nytta av, och även utveckla, redan etablerade samarbeten med andra länders underrättelse- och säkerhetstjänster. Slutligen hanterar Försvarsmakten regelmässigt ärenden av säkerhetspolitisk betydelse vilket har medfört att Försvarsmakten har utvecklat sina arbetsmetoder så att frågor av politisk betydelse snabbt kan rapporteras till regeringen. Det kan tillämpas även på uppgiften som nationell säkerhetsmyndighet.

Vi föreslår mot denna bakgrund att Försvarsmakten får i uppdrag att vara nationell säkerhetsmyndighet. Försvarsmakten behöver för ett sådant uppdrag liksom i dag regeringens bemyndigande att förhandla internationella överenskommelser och även instruktioner för hur förhandlingar och samarbeten ska bedrivas.

[17] Vi har inte kunnat finna tydliga data som visar i vilken utsträckning denna förskjutning sker. Troligtvis finns det ett stort mörkertal, eftersom hanteringen av de civila internationella säkerhetsfrågorna inte är tydligt reglerad.
[18] Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

Förslaget är dock inte utan nackdelar. Som vi har beskrivit berör frågorna inte enbart försvarssektorn, och tendensen går mot att fler civila internationella samarbetsprojekt berörs av säkerhetsskyddskrav, inte minst inom rymdsektorn och inom civil säkerhetsforskning. Detta innebär att, för det fall att denna typ av uppgifter skulle handläggas av Försvarsmakten, den principiella uppdelningen i civilt och försvarsrelaterat säkerhetsskydd mellan Säkerhetspolisen och Försvarsmakten frångås. För att förhindra detta bör det i uppdragsformuleringen till Försvarsmakten göras ett tillägg att ärenden som rör främst Säkerhetspolisens tillsynsområde ska överlämnas dit. Detta medför förvisso att även Säkerhetspolisen behöver avsätta resurser för att hantera vissa internationella säkerhetsskyddsärenden. Den internationella kommunikationen bör dock av tydlighetsskäl även för dessa fall ske med den nationella säkerhetsmyndigheten som kontaktpunkt.

En ytterligare svårighet är förhållandet mellan Försvarsmakten och Regeringskansliet avseende tillsyn och föreskrifter. Regeringskansliet är i vårt förslag undantaget från de delar av säkerhetsskyddslagstiftningen som inte rör informationssäkerhetsklasser, säkerhetsprövning och säkerhetsintyg. Det innebär att Regeringskansliet internt måste säkerställa att internationella säkerhetsskyddsåtaganden implementeras i Regeringskansliet och att säkerhetsskyddet kontrolleras. Detta utvecklas nedan under avsnittet om internationella säkerhetsskyddsåtaganden i Regeringskansliet.

En tredje nackdel med förslaget är att det kan ifrågasättas om sådana ärenden som skulle kunna vara utrikespolitiskt känsliga bör hanteras av en förvaltningsmyndighet. Även om denna typ av ärenden bedöms som ovanliga så förekommer ändå sådana. Detta motiverar att ett fåtal uppgifter även i fortsättningen bör finnas i Regeringskansliet. Vi återkommer till hur uppgiftsfördelningen bör vara ordnad mellan den nationella säkerhetsmyndigheten, Regeringskansliet och regeringen.

Vi anser att regeringen i förordning bör ge Försvarsmakten i uppgift att vara nationell säkerhetsmyndighet vilket även innefattar funktioner för informationssäkring och kryptografisk säkerhet.

Några av experterna har framfört invändningar mot förslaget bl.a. med hänvisning till att rollen som nationell säkerhetsmyndighet inte hör till Försvarsmaktens kärnverksamhet. Vissa

motförslag har förts fram som innebär en fortsatt uppdelning av funktionen mellan en eller flera förvaltningsmyndigheter (Försvarsmakten och Säkerhetspolisen) och Regeringskansliet (Utrikesdepartementet). Vi ser dock inte att sådana lösningar har fler fördelar – eller färre nackdelar – än vårt förslag.

En nationell industrisäkerhetsmyndighet

Genom att uppdraget att vara nationell säkerhetsmyndighet föreslås ges till Försvarsmakten bör detta uppdrag kunna innefatta rollerna som rör informationssäkring och kryptofrågor. Däremot bör inte Försvarsmakten ha något övergripande ansvar för internationella säkerhetsfrågor som rör industrisäkerhet och leverantörer. Denna uppgift finns i dag åtminstone delvis hos Försvarets materielverk, även om ansvaret och uppgiften är otydligt formulerad. Vid myndigheten finns kompetens kring förhandling av projektsäkerhetsavtal och av att vara kravställare på internationella materielprojekt. Vidare hanteras vid myndigheten ärenden som rör säkerhetsintyg för personer och leverantörer, och det finns upparbetade rutiner för internationell besökshantering och den administration som krävs för detta. Slutligen utövar myndigheten tillsyn över leverantörer och meddelar säkerhetsbestämmelser för dessa med stöd av de säkerhetsskyddsavtal som myndigheten träffar med leverantörerna. Myndigheten är således redan väl förberedd för att utvecklas till en formell nationell industrisäkerhetsmyndighet.

Vi anser att Försvarets materielverk mot den bakgrunden bör få i uppgift att vara nationell industrisäkerhetsmyndighet.[19] Regeringen bör därför i förordning ge Försvarets materielverk detta uppdrag.

Regeringskansliets roll i vissa ärendetyper

Det finns naturligtvis legitima invändningar mot att peka ut Försvarsmakten respektive Försvarets materielverk i funktionerna som nationell säkerhetsmyndighet respektive nationell industri-

[19] Samma slutsats kan utläsas i promemorian Några frågor om säkerhetsprövning inför utlandsverksamhet, m.m. (Ds 2006:20).

säkerhetsmyndighet och därmed i viss mån i praktiken begränsa Regeringskansliets hantering av dessa funktioner. En sådan invändning som förts fram under vårt arbete är att funktionerna, i vart fall den som nationell säkerhetsmyndighet, är av karaktären att verksamheten till stora delar bör ligga på Regeringskansliet. Skälet skulle vara att vissa uppgifter, t.ex. att företräda Sverige i Rådets säkerhetskommitté, löpande kräver (utrikes)politiska bedömningar och ställningstaganden som bäst görs av tjänstemän i Regeringskansliet. Det framhålls också att andra medlemsstater representeras av tjänstemän från respektive ministerium.

I sammanhanget bör då påpekas att den svenska förvaltningsmodellen medför att det som hos oss är förvaltningsmyndigheter med en fristående ställning i andra medlemsstater svarar mot delar av ministerierna. Svenska förvaltningsmyndigheter är vidare underställda och har lydnadsplikt i förhållande till regeringen utom så vitt avser vad som faller under 12 kap. 2 § regeringsformen som knappast aktualiseras här.

Regeringskansliets uppgift är ”att bereda regeringsärenden” och ”att biträda regeringen och statsråden i deras verksamhet i övrigt” (7 kap. 1 § regeringsformen). Vi kan konstatera att själva regeringen så gott som aldrig har befattat sig med de frågor som ankommer på funktionen som nationell säkerhetsmyndighet eller nationell industrisäkerhetsmyndighet. Det tycks så gott som uteslutande ha rört sig om att ge vissa bemyndiganden att förhandla säkerhetsavtal med andra stater, en funktion som rimligen ska ligga kvar på regeringen, oavsett om andra uppgifter flyttas till förvaltningsmyndighet. Det är i stället tjänstemän i Regeringskansliet och i vissa myndigheter som fullgjort nu aktuella funktioner utan att beslut av regeringen aktualiserats. Denna iakttagelse – att regeringen inte annat än undantagsvis befattar sig med ärendena – talar mot att placera funktionerna i Regeringskansliet.

Rent allmänt gäller enligt den svenska förvaltningsmodellen att regeringen har fullt ansvar för förvaltningsmyndigheternas verksamhet och goda möjligheter att kräva ut lydnadsplikten, utom så vitt avser vad som faller under 12 kap. 2 § regeringsformen. Vidare kan verksamheten styras genom adekvata instruktioner, och det finns även andra metoder. Man får dessutom förutsätta att berörda förvaltningsmyndigheter håller nära kontakt med Regeringskansliet i dessa ärenden liksom i andra och vid behov efterfrågar instruk-

tioner och vägledning. För såväl Försvarsmakten som Försvarets materielverk torde detta inte innebära några svårigheter.

Sammantaget finner vi alltså att invändningarna mot att lägga huvuddelen av verksamheten för nu berörda funktioner på förvaltningsmyndigheter får stå tillbaka.

Detta innebär emellertid inte att regeringens ansvar för och Regeringskansliets befattning med frågorna skulle upphöra. För det första består kraven avseende t.ex. ledning, styrning och uppföljning av verksamheten och är dessutom i stället särskilt stora i samband med att organiseringen justeras. För det andra bör Regeringskansliet – beroende på dagordningarnas innehåll – även framgent kunna delta i vissa sammanhang, t.ex. i rådets säkerhetskommitté. Även vissa andra ärenden som berör EU-samarbetet som t.ex. svensk hållning i Coreper och annoteringar till EU-nämnden måste hanteras i Regeringskansliet.

Det är inte meningsfullt att försöka mer i detalj beskriva i vilka sammanhang Regeringskansliet ska leda Sveriges medverkan. Försvarsmakten respektive Försvarets materielverk bör i sina instruktioner pekas ut att sköta respektive funktioner. I dessa myndigheters löpande kontakter med Regeringskansliet får under hand klaras ut hur Regeringskansliets medverkan bör vara beskaffad. Försvarsmaktens respektive Försvarets materielverks deltagande är dock viktigt av kontinuitetsskäl även när Regeringskansliet leder Sveriges medverkan.

Med hjälp av det sinnrika systemet för gemensam beredning får säkerställas att olika berörda delar av Regeringskansliet – fler än Försvarsdepartementet och Utrikesdepartementet – får den befattning med verksamheten som är motiverad.

Över huvud taget förutsätter ett framgångsrikt internationellt samarbete, på detta område liksom på andra, nära kontakter och samverkan mellan Regeringskansliet och förvaltningsmyndigheterna och en löpande diskussion om hur den konkreta arbetsfördelningen ska se ut. Ytterst är det naturligtvis regeringen som får avgöra var gränserna ska dras.

Internationella säkerhetsskyddsåtaganden i Regeringskansliet

Även internt berörs Regeringskansliet av den nationella säkerhetsmyndighetsfunktionen och de internationella åtagandena på säkerhetsskyddsområdet. I och med att vi föreslår att Regeringskansliet inte omfattas av stora delar av lagstiftningen behöver Regeringskansliet ordna det egna säkerhetsskyddet så att det uppfyller Sveriges internationella säkerhetsskyddsåtaganden. Detta bör i så stor utsträckning som möjligt följa tillämpningen vid förvaltningsmyndigheterna. Huvudansvaret för att uppfylla kraven i de internationella säkerhetsskyddsåtagandena bör ankomma på samma enhet som ansvarar för säkerhetsskyddet i övrigt i Regeringskansliet, t.ex. avseende meddelande av interna säkerhetsföreskrifter och kontroll av säkerhetsskyddet. Enheten med sådant ansvar bör regelbundet samverka med den nationella säkerhetsmyndigheten och enheten i Regeringskansliet som leder denna och begära stöd när det är lämpligt. För att korrespondera med bl.a. det sistnämnda föreslår vi ett åliggande i förordning för Försvarsmakten och Säkerhetspolisen att lämna råd om säkerhetsskydd till bl.a. Regeringskansliet.

20.4 Utfärdande av säkerhetsintyg

20.4.1 Allmänt om säkerhetsintyg

Som nämnts ovan i avsnitt 20.1 finns det krav i för Sverige folkrättsligt bindande säkerhetsskyddsåtaganden att en behörig svensk myndighet kan utfärda säkerhetsintyg för personer och leverantörer på begäran av en annan stat eller mellanfolklig organisation. Ett sådant system har en fördel i och med att säkerhetsintyg kan främja att personer bosatta i Sverige och leverantörer med säte i Sverige kan komma i fråga för uppdrag där det ställs krav på säkerhetsskydd av ett annat land eller en mellanfolklig organisation.

Det saknas i nuvarande säkerhetsskyddslagstiftning bestämmelser om hur denna typ av intyg ska utfärdas, vad som krävs inför ett utfärdande och vilken myndighet som ska utfärda intygen. Avsaknaden av sådana bestämmelser har inneburit tillämpningsproblem

vilket i några fall kan ha medfört att svenska företag och personer bosatta i Sverige inte har kunnat få nödvändiga intyg.[20]

En av frågorna i våra direktiv är om en övergång till ett kläreringssystem skulle vara ändamålsenlig, bl.a. med hänsyn till att det skulle bli lättare att utfärda säkerhetsintyg för person. Vi har i kapitel 18 besvarat den frågan nekande, bl.a. eftersom vi bedömer att även nuvarande system medger att säkerhetsintyg kan utfärdas om tydliga bestämmelser om detta införs i lagstiftningen.

Enligt internationell praxis och enligt Rådets och Natos säkerhetsbestämmelser är det den nationella säkerhetsmyndigheten som normalt är kontaktyta i frågor som rör säkerhetsintyg. Men denna princip kan frångås om det t.ex. finns en särskilt utsedd industrisäkerhetsmyndighet som då kan utfärda säkerhetsintyg för leverantörer och även för anställda hos sådana leverantörer.

Säkerhetsintyget syftar till att visa att en behörig myndighet i ett land har genomfört en utredning och i denna kommit fram till att en person eller en leverantör kan anses pålitlig att hantera säkerhetsskyddsklassificerade uppgifter upp till en viss nivå. Eftersom det är ett annat lands eller en mellanfolklig organisations säkerhetskänsliga uppgifter som behörigheten avser krävs ett ömsesidigt förtroende mellan de inblandade parterna. I många länder krävs t.ex. att det föreligger en gällande säkerhetsskyddsöverenskommelse mellan länderna för att ett intyg ska kunna godtas.

Verkan av ett säkerhetsintyg för person som har utfärdats av en utländsk myndighet eller mellanfolklig organisation har tidigare behandlats i kapitel 16.3. Verkan av motsvarande intyg för leverantör har tidigare behandlats i kapitel 19.2.

20.4.2 Säkerhetsintyg för person

Förslag: Säkerhetsintyg för *person* får utfärdas om behov av sådant intyg finns vid internationell samverkan avseende säkerhetskänslig verksamhet enligt denna lag, eller om intyget kan underlätta för en person som har hemvist i Sverige att delta i en verksamhet som en annan stat eller en mellanfolklig organisation bedömer vara i behov av säkerhetsskydd.

[20] Se Ds 2006:20.

Ett intyg får utfärdas endast om deltagandet avser verksamhet i eller för en stat eller mellanfolklig organisation som omfattas av ett internationellt säkerhetsskyddsåtagande.

Om det finns särskilda skäl, får regeringen besluta om undantag från kravet på ett internationellt säkerhetsskyddsåtagande.

Intyget ska avse en pålitlighetsbedömning när det gäller att hantera säkerhetsklassificerade uppgifter upp till och med en viss nivå. Intyget ska, utom för personer hos leverantörer med vilka staten har träffat ett säkerhetsskyddsavtal, utfärdas av den nationella säkerhetsmyndigheten. Säkerhetsintyg för personer hos leverantörer med vilka staten har träffat ett säkerhetsskyddsavtal ska i stället utfärdas av den nationella industrisäkerhetsmyndigheten.

Ett säkerhetsintyg för person bör utfärdas av den nationella säkerhetsmyndigheten – dels av tydlighetsskäl gentemot utländska myndigheter, dels för att dokumentationen av utfärdade intyg ska finnas samlad på en plats och följa samma rutiner. Resursskäl talar också för att uppgiften finns vid enbart en myndighet. Från denna regel bör dock undantas personer hos leverantörer som staten har träffat säkerhetsskyddsavtal med. I dessa fall bör i stället den nationella industrisäkerhetsmyndigheten utfärda intygen. Skälen till detta redovisas under avsnitt 20.4.3 nedan.

Utifrån den komparativa studie som vi har gjort har vi funnit att andra länder utfärdar säkerhetsintyg endast efter ansökan från behörig myndighet i det land där intyget behövs. Det finns, som vi har uppfattat det, inte något utrymme i dessa länder för enskilda att själva begära och få ett säkerhetsintyg. I den tidigare nämnda departementspromemorian (Ds 2006:20) redovisas exempel på fall där säkerhetsintyg inte har kunnat utfärdas eftersom en formell begäran inte har funnits. Det framgår dock inte om förfarandena i de redovisade exemplen kan anses vara representativa utifrån respektive lands säkerhetslagstiftning. Av vad vi har funnit är så inte alltid fallet eftersom företrädare för de länder vi har studerat har redovisat att en korrekt ansökan om säkerhetsintyg *alltid* kommer från den behöriga myndigheten i landet. Vi anser med ledning av det att det skulle vara olyckligt om denna ordning skulle frångås i svensk lagstiftning. Vidare är det ett tungt vägande skäl att enbart

en uppgift om krav på säkerhetsintyg i en *svensk* platsannons inte i sig ska kunna vara en grund för säkerhetsprövning och detsamma bör naturligtvis gälla för platsannonser i andra länder. En annan ordning skulle kunna öppna för missbruk av registerkontrollinstitutet och en urholkning av den restriktivitet som bör gälla vid registerkontroll.[21]

Om det uppstår sådana fall som anges i något av exemplen i den ovan angivna departementspromemorian (t.ex. att krav på säkerhetsintyg anges enbart i en platsannons eller i upphandlingsdokumentation) bör situationen kunna lösas genom att den nationella säkerhetsmyndigheten eller den nationella industrisäkerhetsmyndigheten, om det är lämpligt, samverkar med behörig myndighet i det aktuella landet. Vid en sådan samverkan skulle eventuella missförstånd kunna klaras ut.

En förutsättning för att ett intyg ska kunna utfärdas bör vidare vara att det finns ett internationellt säkerhetsskyddsåtagande som reglerar intygsförfarandet. Åtagandet kan framgå i en säkerhetsskyddsöverenskommelse mellan Sverige och ett annat land eller mellanfolklig organisation eller följa av EU-rätten. Reciprocitetsskäl medför nämligen att Sverige måste beakta säkerhetsintyg som är utfärdade av den som gör ansökan. En säkerhetsskyddsöverenskommelse innebär att parterna har ett ömsesidigt förtroende för att respektive parts prövning inför ett intyg är tillräcklig. I övriga fall skulle det innebära ett visst risktagande att lita på ett säkerhetsintyg där varken de rättsliga eller faktiska omständigheterna för utfärdandet är kända. Det skulle även kunna förekomma fall där det aktuella landets internationella relationer och samarbeten kan medföra konsekvenser för svenska säkerhetsintressen.

En bestämmelse om ett strikt krav på att ett internationellt säkerhetsskyddsåtagande ska finnas skulle dock kunna få den effekten att ett intyg inte kan utfärdas i vissa fall, även om detta skulle vara önskvärt. Exempel på detta är situationer där säkerhetsskyddsklassificerade uppgifter behöver utbytas med ett annat land trots att en säkerhetsskyddsöverenskommelse ännu inte har ingåtts.

[21] Liknande bedömning i promemorian Några frågor om säkerhetsskyddslagen (Ds 2004:12), s. 27 ff. Även i betänkandet Registerutdrag i arbetslivet (SOU 2014:48), föreslås att en arbetsgivares möjlighet att begära registerutdrag ska begränsas till fall där det finns starka skäl (se avsnitt 6.5.5, s. 120 f.). Betänkandet har remitterats och förslaget bereds inom Regeringskansliet.

Detta kan vara fallet i exempelvis större försvarsexportaffärer där affärsprocessen kan gå snabbare än ratificeringen av en säkerhetsskyddsöverenskommelse. Regeringen bör därför kunna besluta om undantag från huvudregeln under förutsättning att kravet på en säkerhetsskyddsöverenskommelse skulle försvåra internationell verksamhet av stor eller principiell betydelse för Sverige. I dessa fall bör dock åtgärder för att ingå en säkerhetsskyddsöverenskommelse med det aktuella landet prioriteras.

Säkerhetsintyg för person får utfärdas i två olika situationer. Den första situationen är när personen behöver intyget för säkerhetskänslig verksamhet som utgör en del av internationell samverkan mellan Sverige och ett annat land eller en mellanfolklig organisation. Ett exempel på en sådan situation är internationella säkerhetskänsliga materielprojekt som Sverige deltar i. Den andra situationen är när en person behöver ett intyg för att kunna delta i ett annat lands eller en mellanfolklig organisations verksamhet vilken till sin natur närmast motsvarar säkerhetskänslig verksamhet. I det sistnämnda fallet finns det inte några svenska säkerhetsintressen som berörs, utan intyget bygger på ett ömsesidigt förtroende mellan två parter vilket har reglerats i en internationell säkerhetsskyddsöverenskommelse. Ett exempel på en sådan situation är att en i Sverige bosatt person söker anställning i ett annat land där det för anställningen krävs ett säkerhetsintyg på en grund som motsvarar förutsättningarna i vårt förslag till säkerhetsskyddslag.

Säkerhetsintyg för person kommer i huvudsak att utfärdas för personer som redan är placerade i säkerhetsklass vid en myndighet eller leverantör. I dessa fall torde det vara enkelt för den som har genomfört säkerhetsprövningen (vanligtvis arbetsgivaren) att skicka ett underlag till den nationella säkerhetsmyndigheten eller den nationella industrisäkerhetsmyndigheten som utifrån detta underlag utfärdar ett intyg. Underlagets innehåll och utformning kan närmare specificeras i tillämpningsföreskrifter.

I de undantagsfall då personen inte redan är placerad i säkerhetsklass måste personen säkerhetsprövas innan ett intyg kan utfärdas. Säkerhetsprövningen bör då genomföras av den nationella säkerhetsmyndigheten på liknande sätt som myndigheten gör för egen personal i säkerhetsklass i den utsträckning som är möjlig.

Säkerhetsprövning innebär självfallet ett visst osäkerhetsmoment, oavsett hur väl säkerhetsprövningen eller utredningen

genomförs. Det är med anledning av detta svårt att uttryckligen *garantera* säkerheten för personer och leverantörer. Intyg bör därför utformas på ett sådant sätt att den utfärdande myndigheten meddelar att det inte förekommer något i myndighetens utredning som *talar emot* att pålitligheten upp till en viss nivå kan intygas.

I vårt förordade alternativ till nationell säkerhetsmyndighet ovan föreslår vi att ärenden som rör främst Säkerhetspolisens tillsynsområde ska överlämnas dit. Detta bör dock inte gälla för ärenden som rör säkerhetsintyg för person. Skälet till detta är att Säkerhetspolisen i sådana fall dels skulle ta fram underlag för registerkontroll till Säkerhets- och integritetsskyddsnämnden, dels skulle värdera de uppgifter som nämnden sedan eventuellt lämnar ut. En sådan ordning kan ifrågasättas från ett integritetsperspektiv. Därför bör Försvarsmakten utfärda samtliga säkerhetsintyg för personer.

20.4.3 Säkerhetsintyg för leverantör

Förslag: Säkerhetsintyg för *leverantör* får utfärdas om behov av sådant intyg finns vid internationell samverkan avseende säkerhetskänslig verksamhet enligt denna lag, eller om intyget kan underlätta för en leverantör som har sitt säte i Sverige att delta i en verksamhet som en annan stat eller en mellanfolklig organisation bedömer vara i behov av säkerhetsskydd.

Ett intyg får utfärdas endast om deltagandet avser verksamhet i eller för en stat eller mellanfolklig organisation som omfattas av ett internationellt säkerhetsskyddsåtagande.

Om det finns särskilda skäl, får regeringen besluta om undantag från kravet på ett internationellt säkerhetsskyddsåtagande.

Intyget ska avse en bedömning av att leverantören, eller en del av leverantörens verksamhet, kan hantera säkerhetsskyddsklassificerade uppgifter upp till och med en viss nivå. Intyget ska utfärdas av den nationella industrisäkerhetsmyndigheten. Ett intyg får utfärdas för leverantörer som staten har träffat ett säkerhetsskyddsavtal med. I de fall intyget avser en leverantör som staten inte har ett sådant avtal med, ska den nationella industrisäkerhetsmyndigheten träffa ett sådant med leveran-

tören. Den säkerhetsutredning som behövs för att ett säkerhetsskyddsavtal ska kunna träffas genomförs av den nationella industrisäkerhetsmyndigheten.

Ett säkerhetsintyg för leverantör bör utfärdas enbart av den nationella industrisäkerhetsmyndigheten. Även i detta fall talar tydlighetsskäl och administrativa samordningsvinster för en sådan lösning. Säkerhetsintyg för leverantörer kommer i huvudsak att utfärdas för leverantörer som staten, företrätt av olika myndigheter, har träffat säkerhetsskyddsavtal med. Den nationella industrisäkerhetsmyndigheten bör vid en ansökan om säkerhetsintyg för en viss leverantör inhämta upplysningar om gällande säkerhetsskyddsavtal hos Säkerhetspolisen. Myndigheten bör även samråda med de myndigheter som har träffat säkerhetsavtal med leverantören för att få upplysningar som kan påverka intygets innehåll.

Liksom i fallet med säkerhetsintyg för person kan intyg utfärdas i två situationer. Den första situationen är när leverantören behöver intyget för säkerhetskänslig verksamhet som utgör en del av internationell samverkan mellan Sverige och ett annat land eller en mellanfolklig organisation. Den andra situationen är när en leverantör behöver ett intyg för att kunna delta i ett annat lands eller en mellanfolklig organisations verksamhet, vilken till sin natur närmast motsvarar säkerhetskänslig verksamhet.

I de fall en leverantör inte har träffat ett säkerhetsskyddsavtal med staten ska den nationella industrisäkerhetsmyndigheten träffa ett sådant avtal med leverantören. Detta motsvaras närmast av bestämmelsen i 17 § säkerhetsskyddsförordningen. 17 § är dock i sin nuvarande utformning alltför snäv och medger bara för Försvarets materielverk att träffa avtal om ”det är nödvändigt för att företaget skall kunna delta i internationellt samarbete om utveckling eller produktion av försvarsmateriel.” Bestämmelsen bör därför omformuleras så att den ger stöd för Försvarets materielverk (i egenskap av nationell industrisäkerhetsmyndighet) att träffa säkerhetsskyddsavtal i de fall då det behövs för att kunna utfärda säkerhetsintyg för en leverantör. De åtgärder som vidtas inför ett sådant avtal bör vara i huvudsak desamma som när myndigheten träffar säkerhetsskyddsavtal med leverantörer för den egna verksamheten.

Som ovan nämnts bör den nationella industrisäkerhetsmyndigheten även utfärda säkerhetsintyg för personal vid leverantörer som staten har träffat säkerhetsskyddsavtal med. Skälet till detta är att det från effektivitetssynpunkt är bra att ha dessa intyg samlade med dokumentationen rörande de leverantörer som personerna är knutna till. Uppgifterna om gällande säkerhetsintyg för leverantörers personal behövs t.ex. ofta i internationell besökshantering.

En ansökan ska av samma skäl som för säkerhetsintyg för person komma från en behörig myndighet i ett annat land eller en mellanfolklig organisation, se avsnitt 20.4.2 ovan.

20.4.4 Registerkontroll i andra fall

Förslag: Registerkontroll får göras när en annan stat eller mellanfolklig organisation gjort en ansökan om sådant underlag, om den person som ansökan gäller har eller har haft hemvist i Sverige och personen genom anställning eller på annat sätt ska delta i en verksamhet där det för deltagandet gäller regler om registerkontroll vid säkerhetsprövning som motsvarar svenska förhållanden. Vid sådan registerkontroll får också en särskild personutredning göras.

Det förekommer att länder som avser att utfärda säkerhetsintyg för personer som är bosatta i det landet men är medborgare i något annat land för sin utredning behöver uppgifter ur polisregister i medborgarlandet. Detta förfarande har i nuvarande reglering stöd i 15 § säkerhetsskyddslagen. Underlagens relevans bedöms först av Säkerhets- och integritetsskyddsnämnden och förses inte med några uttalanden om personens pålitlighet att ta del av säkerhetsskyddsklassificerade uppgifter. Dessa underlag lämnas sedan av Säkerhetspolisen till behörig myndighet i det aktuella landet. Av samordningsskäl bör sådana underlag dock i stället lämnas av den nationella säkerhetsmyndigheten. Bestämmelsen bör behållas och förtydligas i en ny säkerhetsskyddslag.

20.4.5 Sekretessbrytande bestämmelse vid internationell samverkan i fråga om säkerhetsprövning

Förslag: Av säkerhetsskyddslagen ska framgå att sekretess inte hindrar att den nationella säkerhetsmyndigheten, om ett utlämnade av uppgifter är förenligt med svenska intressen, lämnar ut en uppgift som har kommit fram vid registerkontroll eller särskild personutredning till en utländsk myndighet eller en mellanfolklig organisation.

Det har i ett tidigare utredningssammanhang uppmärksammats att det befintliga författningsstödet för att möjliggöra att uppgifter från en registerkontroll lämnas till en utländsk myndighet är oklart.[22] Säkerhetsskyddslagen bör därför kompletteras med en sekretessbrytande bestämmelse som tar sikte på det slag av uppgifter och ärenden som det här är fråga om. Det kan dock förekomma att uppgifter som kommit fram vid registerkontroll av olika skäl är olämpliga att delge en utländsk myndighet eller mellanfolklig organisation. Det bör därför ställas upp ett förbehåll om att uppgifterna får lämnas ut om utlämnandet är förenligt med svenska intressen.

20.4.6 Dokumentation och giltighet

Dokumentation

Med utfärdande av intyg följer frågan om hur intygshanteringen ska dokumenteras. Dokumentationsfrågan bör vara tydlig både för de fall där förutsättningarna för ett utfärdande redan är klara (då personen är placerad i säkerhetsklass alternativt att leverantören har ett giltigt säkerhetsskyddsavtal), liksom för de fall då en säkerhetsprövning eller ett säkerhetsskyddsavtal initieras först genom ansökan om ett säkerhetsintyg.

Det förstnämnda fallet innebär att det redan finns ett underlag i form av dokumentation om säkerhetsprövning och anställning i en befattning som är placerad i säkerhetsklass eller ett säkerhets-

[22] Se Ds 2006:20, s. 66.

skyddsavtal mellan en leverantör och en myndighet. Den nationella säkerhetsmyndigheten och den nationella industrisäkerhetsmyndigheten bör i dessa fall inhämta relevant underlag inför utfärdandet av intyg. I samband med detta bör de berörda myndigheterna upplysas om att nya omständigheter som kan påverka intygens giltighet måste rapporteras till den nationella säkerhetsmyndigheten respektive den nationella industrisäkerhetsmyndigheten.

De andra fallen innebär att den nationella säkerhetsmyndigheten respektive den nationella industrisäkerhetsmyndigheten själva genomför nödvändiga åtgärder inför utfärdandet av intyg. Dessa åtgärder bör då dokumenteras i samma utsträckning som när det gäller säkerhetsprövning och träffande av säkerhetsskyddsavtal för den egna myndighetens behov.

Giltighetstid

Bör ett säkerhetsintyg ha en viss giltighetstid och hur lång bör en sådan giltighetstid i så fall vara? Vi har i kapitel 18 beskrivit att en säkerhetsprövning är en pågående process som avslutas först i och med att en anställning eller annat deltagande i säkerhetskänslig verksamhet upphör. På samma sätt är ett säkerhetsskyddsavtal mellan en myndighet och en leverantör giltigt så länge leverantörens uppdrag pågår. Med detta synsätt skulle det således inte behövas några särskilda bestämmelser som begränsar giltighetstiden för säkerhetsintyg. Det finns dock krav i internationella bestämmelser som Sverige ska följa att säkerhetsintyg får gälla endast för en viss tidsperiod. Både EU:s och Natos säkerhetsbestämmelser anger att maxtiden för ett säkerhetsintyg för person är tio år utom på nivån *kvalificerat hemlig* där den maximala giltighetstiden i stället är fem år.[23] Denna ordning bör därför gälla även i Sverige. Det finns inga hinder mot att ett säkerhetsintyg förnyas om det finns behov av det. Nackdelen med en giltighetstid torde då enbart vara att det medför ytterligare administration. Motsvarande krav på giltighetstid saknas när det gäller säkerhetsintyg för leverantör (även om olika blanketter som används i dag innehåller fält för att ange giltighetstid vilket antyder att giltighetstid för dessa intyg kan före-

[23] Rådets säkerhetsbestämmelser (2013/488/EU), Bilaga I, Art. 13 samt Natos säkerhetsbestämmelser, AC/35-D/2000, Annex I, Art. 13.

komma[24]). Det kan av praktiska skäl vara lämpligt att ange en giltighetstid för ett säkerhetsintyg för leverantör om leverantörens uppdrag är tidsbegränsat. Giltighetstiden bör då följa uppdragstiden. Om det inte går att bedöma hur lång uppdragstiden kommer att bli, bör maxtiden för giltighet vara densamma som för säkerhetsintyg för person. Det bör vid den nationella säkerhetsmyndigheten och den nationella industrisäkerhetsmyndigheten finnas administrativa rutiner för att bevaka giltighetstiden för säkerhetsintyg och ge möjlighet att vid behov förlänga giltighetstiden. Bestämmelser om dokumentation och giltighetstider bör kunna meddelas i form av myndighetsföreskrifter.

[24] T.ex. i Natos blankett för säkerhetsintyg för leverantör, appendix VI till annex I till Natos säkerhetskommittés direktiv för industrisäkerhet, AC/35-D/2003.

21 Tillsyn, föreskrifter och rapportering

I kapitel 9 har vi redogjort för hur bl.a. den ökade internationaliseringen, informationsteknikens utveckling, och avreglering och efterföljande konkurrensutsättning av offentlig verksamhet innebär förändrade förutsättningar för säkerhetsskyddet. I direktiven tas upp att bl.a. nämnda faktorer också påverkar tillsynen av säkerhetsskyddet och innebär ökade krav på Säkerhetspolisen och Försvarsmakten och de säkerhetsskyddsstödjande myndigheterna.[1] Det betonas att en förutsättning för att reglerna om säkerhetsskydd ska få det genomslag som är avsett är att tillsynen kan utföras på ett effektivt och ändamålsenligt sätt. Det framhålls att den stödjande och rådgivande verksamheten är särskilt betydelsefull.

Vårt uppdrag innefattar att analysera hur Säkerhetspolisens och Försvarsmaktens tillsyn över säkerhetsskyddet bör vara utformad, bl.a. i förhållande till de säkerhetsskyddsstödjande myndigheternas kontroll. Det innebär också att ta ställning till om ett system med sanktioner bör införas och i sådant fall hur det bör utformas.

I kapitel 10, där vi har redovisat viktiga allmänna utgångspunkter för en reformerad säkerhetsskyddslag, har vi berört också frågor om tillsyn, rådgivning och föreskrifter. Vi påpekar att det framför allt handlar om att göra Säkerhetspolisens och Försvarsmaktens

[1] I direktiven används benämningen sektorsansvariga myndigheter som en samlande benämning för Affärsverket svenska kraftnät, Post- och telestyrelsen, Transportstyrelsen och länsstyrelserna. Som framgår av avsnitt 10.1.5 har vi i stället valt att använda säkerhetsskyddsstödjande myndigheter som en samlande benämning för dessa myndigheter såvitt avser deras funktioner för säkerhetsskyddet. Vi föreslår vidare i avsnitt 18.10 och 21.2.4 att Myndigheten för samhällsskydd och beredskap ska ta över de uppgifter länsstyrelserna i detta avseende har samt även i vissa avseenden vara säkerhetsskyddsstödjande myndighet för kommuner och landsting.

övergripande ansvar och de säkerhetsskyddsstödjande myndigheternas roll tydligare. Det innebär att vi inte ser några större behov av förändringar i fråga om tillsynens inriktning och genomförande. Det finns anledning att utveckla hur vi kommit fram till den slutsatsen innan vi redovisar våra överväganden om ansvariga myndigheter och deras roll (avsnitt 21.2), föreskrifter (avsnitt 22.3) och om rapporteringsskyldighet (avsnitt 21.4). I det nu närmast följande avsnittet behandlar vi därför frågan om tillsynens inriktning och genomförande. I det sammanhanget kommer vi också in på frågan om sanktioner.

21.1 Tillsynens inriktning och genomförande – bör sanktioner införas?

Bedömning: Tillsynen bör bedrivas under i huvudsak samma former som i dag. Tillräckliga skäl föreligger för närvarande inte att föreslå en så genomgripande förändring av tillsynens inriktning och genomförande som sanktioner skulle medföra.

Frågan bör dock följas upp när en reformerad säkerhetsskyddslag har varit i kraft en tid. En sådan uppföljning kan behöva göras tidigt om det s.k. NIS-direktivet ger anledning till det.

Generella utgångspunkter för reglering om tillsyn

Det finns anledning att beakta principiella bedömningar som gjorts i fråga om tillsyn. I riksdagsskrivelsen 2009/10:79 En tydlig, rättsäker och effektiv tillsyn, redovisar regeringen generella bedömningar av hur en tillsynsreglering bör vara utformad.[2] Skrivelsen är avsedd att vara ett stöd och en vägledning vid bl.a. översyn av materiella regelverk av olika slag. I skrivelsen framhålls betydelsen av enhetlighet i fråga om offentlig tillsyn. Det lämnas dock utrymme för att göra avsteg från de bedömningar som görs i skrivelsen.

[2] Skrivelsen utgår från de förslag som lämnades av Tillsynsutredningen i dess slutbetänkande Tillsyn – Förslag om en tydligare och effektivare offentlig tillsyn (SOU 2004:100).

En utgångspunkt i skrivelsen är att begreppet tillsyn främst bör användas för verksamhet som avser självständig granskning för att kontrollera om tillsynsobjektet uppfyller krav som följer av lagar och andra bindande föreskrifter. Ett grundläggande moment i tillsynen är därför enligt skrivelsen att tillsynsorganet har författningsreglerade möjligheter att ingripa. Det anges att sådana möjligheter bör finnas även vid mindre allvarliga överträdelser och kunna trappas upp vid allvarligare överträdelser eller om bristen inte rättas till. De mer ingripande sanktioner som förordas i skrivelsen är varning, åtgärdsföreläggande (som ska kunna förenas med vite), rättelse på den enskildes bekostnad, interimistiska beslut, återkallelse av tillstånd eller att förbjuda en verksamhet som inte kräver tillstånd. Tillsynsorganen bör också ha rätt att av den objektsansvarige få del av de upplysningar eller handlingar som behövs för tillsynen. Likaså bör organet ha tillträdesrätt till utrymmen som används i den tillsynspliktiga verksamheten. Tillsynsorganen bör även ha möjlighet att begära biträde från Polismyndigheten och Kronofogdemyndigheten. Vidare bör tillsynsorganen ha möjlighet att ålägga den som är objektsansvarig ansvar för att utöva egen kontroll av sin verksamhet. Enligt skrivelsen bör samtliga ingripanden kunna överklagas.

Ett viktigt skäl för att precisera tillsynsbegreppet anges vara att en tydlig definition gör det enklare att skilja granskandet från främjande verksamhet. Ett strikt avgränsat tillsynsbegrepp anges dock inte hindra att tillsynsmyndigheter även i fortsättningen kan ha till uppgift att arbeta främjande och förebyggande för att effektivt uppnå lagstiftningens mål. Det framhålls att det i allmänhet inte är lämpligt att tillsynsmyndigheten ger råd om hur tillsynsobjekten ska agera i specifika ärenden. Ett skäl till det anges vara att det kan uppstå svårigheter, om tillsynsmyndigheten tidigare lämnat mycket precisa råd i ärenden som sedan blir föremål för tillsyn. Samtidigt framhålls att inom vissa tillsynsområden skäl kan tala för att, utöver upplysningar om gällande rätt, även rekommendationer och vägledning ska vara en del av tillsynen.

Tillsynen av säkerhetsskyddet

Formerna för tillsynen av säkerhetsskyddet avviker i flera avseenden från de redovisade principiella bedömningarna om hur tillsyn bör utformas. I tillsynsmyndigheternas uppgifter ligger bl.a. att kontrollera att myndigheter och andra verksamheter som säkerhetsskyddslagen gäller för följer reglerna om säkerhetsskydd och att säkerhetsskyddet är tillräckligt för den verksamhet som bedrivs. Tillsynen utövas bl.a. genom besök och uppföljning varvid eventuella brister och behov av åtgärder påpekas. Någon sanktion finns inte. Det finns en skyldighet att anmäla inträffade säkerhetsincidenter till Säkerhetspolisen, men den avser endast fall där en hemlig uppgift har röjts, om röjandet kan antas medföra men för rikets säkerhet som inte är ringa (10 § säkerhetsskyddsförordningen). Tillsynen utgår från att de verksamheter som berörs av lagstiftningen samarbetar med de myndigheter som kontrollerar säkerhetsskyddet och självmant vidtar de åtgärder som rekommenderas. Säkerhetspolisens, Försvarsmaktens och de säkerhetsskyddsstödjandemyndigheternas rådgivande och stödjande funktioner i fråga om säkerhetsskyddet är också tydligt uttalade.

Behovet av att väga in de förutsättningar som gäller för det specifika tillsynsområdet

Att tillsynen av säkerhetsskyddet i viktiga avseenden avviker från principiella riktlinjer för hur tillsyn bör utformas skulle kunna tala för att en genomgripande förändring behövs. Det är dock viktigt, som också skrivelsen ger uttryck för, att utgå från de förutsättningar som gäller för det specifika tillsynsområdet. I skrivelsen anförs att det inte går att bortse från att många tillsynsområden har väsentligt olika förutsättningar som påverkar hur tillsynsregelverket bör utformas för att effektivt bidra till att de materiella reglerna efterlevs och intentionerna i regelverken förverkligas. Faktorer som kan behöva vägas in är bl.a. vem som bedriver den verksamhet som tillsynen avser, vilket slag av verksamhet som tillsynen riktas mot, vilka risker regelöverträdelser kan orsaka och hur det materiella regelverk som tillsynen avser är utformat. Vidare framhålls att det måste beaktas att tillsyn är kostnadskrävande och orsakar störningar och påfrestningar för den som kontrolleras. Mot

den bakgrunden betonas att det vid tillskapande eller översyn av regelverk för tillsyn även är väsentligt att överväga andra styrformer, t.ex. ekonomiska incitament, information eller utvärdering, för att uppnå regelverkets mål.

Säkerhetsskyddslagens genomslag och uppmärksammade brister

För att kunna bedöma behovet av förändrade styrformer, t.ex. i form av ingripandemöjligheter för berörda myndigheter, är en viktig utgångspunkt det genomslag regelverket om säkerhetsskydd har och antagliga orsaker till de brister som finns.

Brister i säkerhetsskyddet finns i varierande omfattning och tar sig olika uttryck. Allvarligast kan vara att det i dag antagligen finns verksamheter av stor betydelse för Sveriges säkerhet som över huvud taget inte tillämpar säkerhetsskyddslagen. Allvarligt är också att bristerna vad gäller det grundläggande analysarbetet tycks vara omfattande, såväl vid myndigheter som hos enskilda aktörer. Det kan innebära att verksamheten saknar kunskap om vad som behöver ett skydd och hur skyddet behöver vara dimensionerat. Det har bl.a. från Säkerhetspolisen framförts att det inte sällan medför att säkerhetsskyddet får en slagsida mot säkerhetsprövning, framför allt momentet registerkontroll, samtidigt som de åtgärder som vidtas inom ramen för informationssäkerhet och fysisk säkerhet inte är tillräckliga. Som redogjorts för tidigare (se avsnitt 13.2) har Affärsverket svenska kraftnät uppmärksammat väsentliga brister i fråga om krav på säkerhetsskyddsanalyser när det gäller verksamheter inom elförsörjningen.

I fråga om den civila statsförvaltningen bör nämnas att Riksrevisionen nyligen till riksdagen överlämnat en granskningsrapport[3] som behandlar informationssäkerhet och som således i vissa avseenden berör säkerhetsskyddslagens tillämpningsområde. Också av den rapporten är det tydligt att det finns brister hänförliga till det grundläggande analysarbetet. I rapporten redovisas att Säkerhetspolisen i sin tillsyn har funnit systematiska brister i fråga om informationssäkerhet hos de mest skyddsvärda myndig-

[3] RIR 2014:23 Informationssäkerheten i den civila statsförvaltningen, dnr: 31-2013-1288, överlämnad till riksdagen 2014-11-10.

heterna.[4] Det anges handla om att skadekonsekvensbeskrivningar antingen saknas eller utgår från ekonomiska eller andra konsekvenser för den egna verksamheten i stället för konsekvenser som är relevanta utifrån ett säkerhetsskyddsperspektiv. Vidare anges att det också kan handla om att det saknas förmågebedömningar av tänkta angripare vilket medför att det blir oklart hur informationssäkerheten ska dimensioneras.

I rapporten från Riksrevisonen anges att det vid samtal med Säkerhetspolisen också kommit fram att det ibland förekommer att påpekade brister inte rättas till. Vi har bett Säkerhetspolisen att utveckla detta och fått förklaringen att det kan vara vanskligt att vid uppföljning av tillsyn dra slutsatser om hur myndigheterna agerat i fråga om säkerhetsskydd. Säkerhetspolisen framhåller att den inte har möjlighet att väga in samtliga för tillsynsobjektet relevanta omständigheter i sin bedömning av säkerhetsskyddet utan att en fullständig säkerhetsskyddsanalys kan göras endast av den aktuella verksamheten. De situationer som det refereras till i rapporten kan t.ex. därför enligt Säkerhetspolisen ha varit sådana där den påpekade objektiva bristen handlat om en känd sårbarhet som myndigheten i fråga bedömt måste accepteras eftersom alternativet skulle innebära att myndigheten inte kan fullgöra uppgifter som ålagts den. Enligt Säkerhetspolisen handlar det vidare snarare om en bristande förmåga att i en tillräcklig grad analysera och planera för de åtgärder som behöver vidtas än en medveten strategi att inte åtgärda påpekade brister.

I säkerhetsskyddsförordningen (48 §) finns en bestämmelse som innebär att, om brister inte rättas efter påpekande, tillsynsmyndigheten under vissa förutsättningar ska anmäla detta till regeringen. Vad vi känner till har den bestämmelsen inte någonsin behövts tillämpas. Den bild som har framträtt under utredningens arbete är att brister i säkerhetsskyddet oftast tycks ha sin grund i att säkerhetsskyddslagen i olika avseenden uppfattas som otydlig och innebär en osäkerhet i fråga om kraven på säkerhetsskydd. Det gäller bl.a. sådana grundläggande frågor som vilka verksamheter

[4] Uppgifterna i rapporten utgår i den delen från en analys från Säkerhetspolisen utifrån erfarenheter från tillsynsärenden under ett antal år (Säkerhetspolisen: Underlag rörande Säkerhetspolisens bedömning av myndigheters säkerhetsanalyser ur ett informationssäkerhetsperspektiv, 2014-07-11, dnr: 2014-11898-4.

som behöver ett säkerhetsskydd och lagens tillämplighet i enskilda verksamheter.

Det bör emellertid inte förringas att det förekommer brister i säkerhetsskyddet som antagligen inte beror på otydlig lagstiftning eller bristande kunskaper utan snarare på ett medvetet val att inte i tillräcklig grad prioritera säkerhetsskyddet. Det kan gälla såväl myndigheter som enskild verksamhet. Antagligen beror det på att säkerhetsskydd innebär kostnader och kan påverka effektiviteten. Frågan är dock komplex, och det finns också i olika avseenden annan grundläggande problematik som måste beaktas. Inte sällan handlar det om att utvecklingen på andra områden medfört att en prioritering av intressen görs som inte alltid gagnar säkerhetsskyddet. Vi har berört detta i kapitel 9 där vi redogjort för de ändrade förutsättningarna för säkerhetsskyddet.

En särskild svår problematik som vi har att förhålla oss till är försvagande möjligheter att styra och kontrollera vissa för nationen viktiga kärnverksamheter t.ex. i fråga om elförsörjning och telekommunikation. Avreglering och efterföljande konkurrensutsättning, i takt med ökad internationalisering och digitalisering, har medfört att ansvaret för att skydda viktiga svenska intressen i dag kan ligga hos bolag och bolagskoncerner som bedriver sin verksamhet eller delar av den utanför Sverige och där ägarförhållandena är sådana att en prioritering av svenska säkerhetsintressen inte kan tas för given.

Sammanfattningsvis finns det brister som i vissa fall är allvarliga vad gäller uppfyllandet av säkerhetsskyddslagens bestämmelser och intentioner. I några avseenden kan orsakerna till det dock snarast tillräknas förhållanden som inte går att påverka genom en reformerad säkerhetsskyddslagstiftning. Vad i övrigt gäller bristerna i säkerhetsskyddet är det vår bedömning att de i en relativt stor utsträckning kan relateras till otydlig lagstiftning och bristfällig kunskap om hur lagstiftningens krav påverkar och kan tillgodoses i den egna verksamheten. Tillsyn kan endast i begränsad omfattning påverka här redovisade brister.

Särskilda förutsättningar som behöver vägas in i fråga om tillsyn av säkerhetsskyddet

Som nämndes tidigare anges i regeringens skrivelse om tillsyn några faktorer som bör beaktas för att åstadkomma en ändamålsenlig och effektiv styrning av hur ett regelverk efterlevs. I det följande går vi igenom vad som i de nämnda avseendena gäller för säkerhetsskyddslagstiftningen.

En väsentlig faktor är *vilka organ* som bedriver den verksamhet som tillsynen avser. De verksamheter som berörs av tillsynen av säkerhetsskyddet utgörs främst av myndigheter och andra former av allmän verksamhet, bl.a. vissa företag med statligt ägande. Exempel på sådana företag som bedriver säkerhetskänslig verksamhet är Vattenfall, TeliaSonera och SOS Alarm. Andra enskilda företag berörs av tillsynen främst i egenskap av anbudsgivare och leverantörer. Det kan handla om t.ex. företag inom säkerhets- och försvarsmaterielområdet eller om företag som tillhandahåller it- och telekommunikationslösningar. Därutöver berörs också enskilda företag som bedriver verksamhet som är att anse som säkerhetskänslig, t.ex. företag vars verksamhet har väsentlig betydelse för landets elförsörjning.

I fråga om enskilda verksamheter bör beaktas att för det fall att det rör sig om säkerhetsskyddad upphandling, så innebär avtalsförhållandet i sig att det finns ett incitament för en leverantör att leva upp till krav på säkerhetsskydd för att behålla sin position som leverantör på området. I förarbetena till säkerhetsskyddslagen tas också upp att det finns möjlighet att i säkerhetsskyddsavtalen ta in klausuler om skadestånd, vite och hävningsrätt.[5]

Samhällsutvecklingen medför att säkerhetskänslig verksamhet i högre grad än tidigare bedrivs av enskilda. Våra förslag om krav på säkerhetsskydd har också utformats för att tydligare träffa även enskild verksamhet. I viss mån innebär det att den verksamhet som tillsynen avser i större utsträckning än tidigare kan komma att avse enskild verksamhet. Som vi återkommer till i konsekvensbeskrivningen i kapitel 23 är det dock svårt att bedöma omfattningen av en

[5] Säkerhetsskyddsutredningens betänkande Säkerhetsskydd (SOU 1994:149), s. 248. Vad gäller enskilda som själva bedriver säkerhetskänslig verksamhet utgick utredningen från sitt förslag om avtalslösning (som inte kom att genomföras) och menade att det fanns möjlighet att också i sådana avtal föra in skadestånds- eller vitesklausuler.

sådan förändring. En rimlig slutsats bör kunna vara att omfattningen av enskilda verksamhetsformer troligen kommer att öka inom tillsynsområdet men att det även i fortsättningen i avsevärd utsträckning handlar om tillsyn av myndigheter och andra offentliga organ. I fråga om enskilda verksamheter måste vidare beaktas att en anledning till att de i högre grad berörs av säkerhetsskyddslagstiftningen är utvecklingen i fråga om användandet av externa leverantörer. I sådana situationer finns som nämnts andra incitament än sanktioner vid tillsyn för att uppfylla krav på säkerhetsskydd.

I de fall den enskilda verksamheten bedrivs utanför Sveriges gränser, finns givna begränsningar vad gäller möjligheten att ingripa.

En annan faktor som tas upp i regeringens skrivelse och som kan påverka bl.a. vilka befogenheter tillsynsorganen behöver är *vilket slag* av verksamhet som tillsynen riktas mot. Det exemplifieras med de skilda förutsättningar som gäller vid tillsyn mot fysiska objekt, t.ex. livsmedelslokaler och mer svårgreppbar verksamhet, t.ex. försäkringsverksamhet. I fråga om säkerhetsskydd handlar det inte om ett homogent slag av verksamheter utan om verksamheter av vitt skilda slag. Det underlättar inte ett utformande av lämpliga ingripandebefogenheter.

Ytterligare en annan faktor som tas upp i fråga om styrning av ett regelverks efterlevnad är *vilka risker* regelöverträdelser kan orsaka. Regelöverträdelser som innebär risker för exempelvis människors liv och hälsa anges påverka såväl utformning av sanktioner som behovet av en enhetlig tillsyn över hela landet. Det anges även kunna innebära att tillsynen i viss utsträckning ges en förebyggande inriktning. Säkerhetsskydd tar sikte på att förebygga allvarliga konsekvenser till följd av hot mot Sveriges säkerhet. En förebyggande inriktning är därför given.

Av betydelse är också hur det *materiella regelverk* som lagstiftningen ska utövas från är utformat. Inom många tillsynsområden finns ett omfattande och detaljerat materiellt regelverk som utgör grund för tillsynen. Vanligen råder heller ingen tvekan om vilka tillsynsobjekten är, dvs. vilka verksamheter som omfattas av det materiella regelverket. För säkerhetsskyddet gäller det motsatta. Säkerhetsskyddslagen är utformad på ett sätt som ger den verksamhetsansvarige ett stort ansvar och bedömningsutrymme i fråga

om att såväl avgöra lagens tillämplighet som att bestämma hur ett för verksamheten väl anpassat säkerhetsskydd ska åstadkommas. Det innebär svårigheter i fråga om ingripandemöjligheter som förutsätter tydlighet och precision rörande de brister som behöver åtgärdas.

Behovet av råd och stöd

Ett annat förhållande som är viktigt att beakta är att lagstiftningens karaktär medför att det finns ett stort behov av vägledning och stöd till de verksamheter som har att tillämpa säkerhetsskyddslagen. Särskilt i förhållande till enskilda är behovet av råd och stöd framträdande. Det behovet kommer antagligen inte att minska med en reformerad säkerhetsskyddslag. Mot den bakgrunden förefaller det rimligt att anta att lagens genomslag i relativt hög grad även i fortsättningen kan komma att vara beroende av att de myndigheter som har ett särskilt ansvar för säkerhetsskyddet på olika sätt kan vägleda och stödja de säkerhetskänsliga verksamheterna i en tillräcklig omfattning.

Flera av utredningens experter har framhållit att det är viktigt att tillsynen i fråga om säkerhetsskydd utgår från samverkan och ger utrymme för en dialog mellan myndighet och den verksamhet som berörs av tillsynen. Det är också vår uppfattning att det överlag inom säkerhetsskyddsområdet är viktigt att det finns goda förutsättningar för samverkan mellan myndigheter och enskilda verksamheter. Om brister i säkerhetsskyddet skulle kunna medföra åtgärder som t.ex. varningar och vitessanktionerade åtgärdsföreläggande, kan det också få till följd att benägenheten att på eget initiativ ta upp brister med den myndighet som kontrollerar säkerhetsskyddet kan påverkas negativt. Vi ser en betydande risk att sådana inslag skulle kunna medföra att värdefullt erfarenhetsutbyte, t.ex. i fråga om säkerhetshotande incidenter, mellan de verksamheter som kontrolleras och de myndigheter som utövar tillsynen motverkas.

Några av utredningens experter har, utifrån erfarenheter av den nuvarande ordningen, också framfört att det finns en svårighet med att förena en rådgivande och kontrollerande roll. Sådana dubbla roller är svåra att undvika utan att göra stora förändringar av myn-

digheternas ansvar och uppgifter. Antagligen skulle motsättningen upplevas som större om säkerhetsskyddet förändrades mot sådana tillsynsformer där ingripandebefogenheter är i fokus. Det vore olyckligt med en utveckling mot att myndigheter som utövar tillsyn är så restriktiva i sin rådgivning att det innebär ett försämrat säkerhetsskydd.

Sammanfattande bedömning

Formerna för tillsynen av säkerhetsskyddet avviker i väsentliga avseenden från de generella riktlinjerna för hur offentlig tillsyn bör ordnas. Ingripandebefogenheter vid tillsyn är av betydelse. I dag finns inte sådana befogenheter i fråga om säkerhetsskyddet. Det finns skäl att anta att sanktioner, t.ex. i form av förelägganden som förenas med vite, skulle avseende vissa enskilda verksamheter kunna vara ett viktigt verktyg för att inskärpa kraven på säkerhetsskydd. Det argumentet för en förändring får en särskild relevans när utvecklingen går mot att säkerhetskänslig verksamhet i en allt högre grad bedrivs av enskilda. Mycket talar för att den utvecklingen på sikt kommer att medföra ett behov av att kunna tillgripa sanktioner. Samtidigt är det i dag svårt att förutsäga i vilken omfattning enskilda verksamheter kommer att omfattas av en reformerad säkerhetsskyddslag och också vad en sådan utveckling innebär för tillsynen. En omfattande förändring av tillsynen skulle också innebära kostnader och andra konsekvenser. Vi anser att det i dag inte finns ett så tydligt behov av sanktioner som kan motivera sådana konsekvenser. Vår uppfattning är att förändringsbehoven snarare handlar om att förstärka de rådgivande inslagen i tillsynen. Det måste också vägas in att det, mot bakgrund av de förutsättningar som finns på detta tillsynsområde, finns vissa tveksamheter i fråga om ändamålsenligheten av sanktioner.

Sammantaget gör vi bedömningen att det för närvarande inte finns tillräckliga skäl för att förändra tillsynens inriktning och genomförande. Vi föreslår därför inte att sanktioner ska införas. Det är dock angeläget att noga följa utvecklingen och inom en inte alltför avlägsen framtid följa upp frågan. Av den anledningen är den bestämmelse om rapportering till regeringen som vi behandlar i avsnitt 21.4 ett viktigt inslag i regleringen. Det bör i sammanhanget

nämnas att frågor om tillsyn utreds också från ett bredare informationssäkerhetsperspektiv av utredningen NISU 2014.[6] Frågan kan också bli aktuell utifrån en bredare utgångspunkt inom ramen för ett genomförande av det s.k. NIS-direktivet[7](ett förslag till direktiv om informationssäkerhet som nu slutförhandlas inom EU).

21.2 Ansvariga myndigheter och deras roll

21.2.1 Sammanfattning

- Organisationen av tillsynen där flera myndigheter har ett delat ansvar och där det huvudsakliga och övergripande ansvaret är fördelat mellan Säkerhetspolisen och Försvarsmakten bör behållas.
- Samrådsförfarandet mellan berörda myndigheter förenklas för att Säkerhetspolisen och Försvarsmakten ska kunna arbeta mer effektivt med tillsynen av enskilda verksamheter.
- Säkerhetspolisen ska utföra tillsynen av leverantörer som har säkerhetsskyddsavtal med myndigheter etc. inom flera samhällssektorer och i en sådan omfattning att det samlade uppdraget är av stor betydelse för Sveriges säkerhet.
- Säkerhetspolisen har till uppgift att på begäran lämna råd om säkerhetsskydd till Regeringskansliet, riksdagen och dess myndigheter samt till Justitiekanslern. Också Försvarsmakten bör ha sådana uppgifter. Säkerhetspolisen bör samordna sådan rådgivning.

[6] Fö 2013:04 Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system, Dir. 2013:110 och 2014:66.
[7] Förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen [KOM (2013) 48], se Faktapromemoria 2012/13:FPM68.

- Myndigheten för samhällsskydd och beredskap bör från Säkerhetspolisen ta över tillsynsansvaret för kommuner och landsting samt även det ansvar som länsstyrelserna har i dag för enskilda verksamheter som inte hör till övriga säkerhetsskyddsstödjande myndigheters (Affärsverket svenska kraftnät, Post- och telestyrelsen och Transportstyrelsen) ansvarsområden.
- De säkerhetsskyddsstödjande myndigheternas uppgift att lämna råd om säkerhetsskydd till enskilda verksamheter bör framgå av en bestämmelse i säkerhetsskyddsförordningen. Myndigheten för samhällsskydd och beredskap ska även ha ett sådant rådgivningsansvar i förhållande till kommuner och landsting.
- Tillsynsorganisationen bör följas upp när en ny säkerhetsskyddslagstiftning har varit i kraft en tid.

21.2.2 Grunddragen i nuvarande tillsynsorganisation behålls

Säkerhetspolisen och Försvarsmakten har huvudansvaret för tillsynen. När det gäller bolag, föreningar, stiftelser och enskilda näringsidkare utövas kontrollen av de säkerhetsskyddsstödjande myndigheterna (Affärsverket svenska kraftnät för elförsörjningsverksamhet, Post- och telestyrelsen för verksamhet som avser elektronisk kommunikation, Transportstyrelsen för flygtransportverksamhet och i övrigt länsstyrelserna). Även på dessa områden kan dock säkerhetsskyddet kontrolleras av Säkerhetspolisen och Försvarsmakten. Kontrollen ska i så fall utföras i samråd med den primärt ansvariga myndigheten.

Ett flertal myndigheter har således ett särskilt ansvar för säkerhetsskyddet. Det förhållandet i sig kan givetvis göra ansvar och roller otydliga. Våra direktiv pekar inte på skäl för någon genomgripande förändring av den ordningen. Tvärtom framhålls att det är viktigt att den samlade kompetens som finns hos de myndigheter som har till uppgift att kontrollera säkerhetsskyddet kan användas på ett effektivt sätt.

Vi anser att grunddragen i organisationen för tillsynen bör behållas. Vissa förändringar behövs dock för att Säkerhetspolisen och Försvarsmakten ska kunna arbeta mer effektivt med tillsynen

av enskilda verksamheter. Vidare ser vi behov av vissa förändringar i fråga om de säkerhetsskyddsstödjande myndigheterna. Dessa frågor behandlas i de följande avsnitten. Det går inte att utesluta en viss överlappning mellan de olika myndigheternas ansvarsområden, bl.a. i fråga om kommunala bolag. Om sådana situationer uppstår, bör de i samförstånd kunna lösas av myndigheterna. Som utvecklas i det följande är det viktigt att huvudansvaret för de i säkerhetshänseende mest skyddsvärda verksamheterna också i fortsättningen ligger på Säkerhetspolisen och Försvarsmakten. Det är därför möjligt att en utveckling som går mot att enskilda verksamheter i större utsträckning bedriver säkerhetskänslig verksamhet på sikt medför ett behov av att ompröva tillsynsorganisationen. På samma sätt som i fråga om behovet av sanktioner är det viktigt att frågan följs upp när en ny lag har varit i kraft en tid. Om sanktioner övervägs, är det inte självklart att tillsynen bör organiseras på samma sätt som i dag.

21.2.3 Säkerhetspolisen och Försvarsmakten

Uppgifter och ansvar

Som nämnts tidigare har Säkerhetspolisen och Försvarsmakten den huvudsakliga tillsynen av säkerhetsskyddet. Fördelningen myndigheterna emellan innebär att Säkerhetspolisen utövar tillsyn över myndigheter på det civila området och Försvarsmakten över myndigheter som hör till Försvarsdepartementet samt Försvarshögskolan och Fortifikationsverket.[8] Säkerhetspolisens tillsyn omfattar också kommuner och landsting.[9]

Det bör i sammanhaget förtydligas att förslaget att Försvarsmakten ska vara nationell säkerhetsmyndighet[10] i förhållande till andra stater och mellanfolkliga organisationer inte påverkar tillsynsområdena. Formellt sett påverkas dock tillsynens omfatt-

[8] 39 § säkerhetsskyddsförordningen återspeglar inte de justeringar i ansvarsområdena för departementen som gäller sedan den 1 januari 2015 enligt ändring i förordningen (1996:1515) med instruktion för Regeringskansliet, SFS 2014:1466.
[9] Med myndighet avses i säkerhetsskyddsförordningen, om inte annat sägs, också kommuner och landsting (se 3 § säkerhetsskyddsförordningen). Av 39 § säkerhetsskyddsförordningen kan därför utläsas att Säkerhetspolisens tillsynsansvar omfattar kommuner och landsting.
[10] Se kapitel 20.

ning av att lagen utsträcks till att gälla säkerhetsskydd till följd av internationella säkerhetsskyddsåtaganden.

Säkerhetspolisens och Försvarsmaktens tillsyn kan avse även bl.a. kommunala bolag[11] eller en leverantör till t.ex. en myndighet i fråga om en upphandlad verksamhet som omfattas av ett säkerhetsskyddsavtal.[12] Vidare får Säkerhetspolisen och Försvarsmakten utföra tillsyn av sådana bolag, föreningar och stiftelser som en säkerhetsskyddsstödjande myndigheten har i uppgift att kontrollera säkerhetsskyddet vid.[13] Sammantaget innebär regleringen i säkerhetsskyddsförordningen att Säkerhetspolisen och Försvarsmakten har rätt att utöva tillsyn i alla slag av verksamheter som säkerhetsskyddslagen gäller för.[14]

Säkerhetspolisens och Försvarsmaktens övergripande ansvar för säkerhetsskyddet bör rimligen innefatta att ha kunskap om de för nationen mest säkerhetskänsliga verksamheterna och skyddet av dessa samt att följa utvecklingen på säkerhetsskyddsområdet i dess helhet och genom bl.a. föreskrifter verka för att säkerhetsskyddet har den omfattning som behövs. Det innebär också ett ansvar för att förmedla information om aktuella hot till de verksamheter som omfattas av säkerhetsskyddslagen. Vidare bör det också medföra en ledande roll vad gäller metodutveckling inom säkerhetsskyddet, t.ex. i fråga om hur säkerhetsskyddsanalys och säkerhetsprövning ska genomföras samt att åtminstone på en övergripande nivå lämna råd och stöd till alla slags verksamheter som berörs av säkerhetsskyddslagen. Ansvaret medför också enligt 48 § säkerhetsskyddsförordningen en rapporteringsskyldighet i förhållande till regeringen för det fall att det vid utövandet av tillsynen över säkerhetsskyddet konstateras brister som trots påpekanden inte rättas till. Säkerhetspolisens och Försvarsmaktens ansvar förutsätter att erfarenheter om säkerhetsskyddet effektivt kan hämtas in från olika slag av verksamheter.

Det kan i sammanhanget noteras att när säkerhetsskyddslagen infördes tyngdpunkten i säkerhetsskyddet låg vid myndigheters

[11] Dvs. bolag, föreningar och stiftelser som avses i 1 § 2 säkerhetsskyddslagen.
[12] Dvs. enskilda som avses i 8 § säkerhetsskyddslagen.
[13] Dvs. enskilda enligt 1 § 3 säkerhetsskyddslagen.
[14] Dock med undantag för Regeringskansliet, riksdagen och dess myndigheter. Till dessa verksamheter ska i stället Säkerhetspolisen på begäran lämna råd (47 § säkerhetsskyddsförordningen).

verksamhet och avsåg i hög grad behovet av att skydda hemliga uppgifter från att röjas. Säkerhetsskydd är i större utsträckning än tidigare en angelägenhet för enskilda verksamheter inte minst på grund av beroendet av it för grundläggande samhällsfunktioner. Den utvecklingen ställer krav på att särskilt Säkerhetspolisens tillsyn över enskilda verksamheter kan utföras på ett effektivt sätt vilket, som vi nu kommer in på, föranleder vissa ändringar av den nuvarande ordningen.

Ett förtydligande i fråga om tillsynens omfattning

Tillsyn av en myndighets säkerhetsskydd bör kunna innefatta också säkerhetsskyddet hos leverantörer som myndigheten har anlitat i fråga om säkerhetskänslig verksamhet, dvs. verksamhet där säkerhetsskyddet bestämts genom ett säkerhetsskyddsavtal. Det förekommer också att säkerhetskänslig verksamhet bedrivs hos bolag, föreningar och stiftelser som är knutna till myndigheten. Tillsynen av en myndighet bör i förekommande fall kunna avse även sådan verksamhet. Motsvarande gäller vid tillsyn av kommuner och landsting. Ett förtydligande om tillsynens omfattning bör tas in i säkerhetsskyddsförordningen.

Det bör tilläggas att tillsynen av kommuner och landsting i dag utförs av Säkerhetspolisen. Vi föreslår dock i det följande avsnittet att den uppgiften flyttas över till Myndigheten för samhällsskydd och beredskap. Det föreslagna förtydligandet i fråga om bl.a. upphandlad verksamhet bör utformas så att det gäller för samtliga myndigheter som utför tillsyn.

Kravet på samråd behöver lättas upp

För annan tillsyn än den som avser myndigheter, kommuner och landsting ska tillsynen utföras i samråd med de myndigheter som ska kontrollera säkerhetsskyddet vid sådana verksamheter (42 § säkerhetsskyddsförordningen). Det har framförts att samrådsskyldigheten i vissa fall kan försena och försvåra tillsynen. Som framgått är det också av principiell betydelse att Säkerhetspolisens och Försvarsmaktens tillsyn på ett ändamålsenligt sätt kan avse såväl säkerhetskänslig verksamhet vid myndigheter och annan

allmän verksamhet som hos bolag och andra verksamhetsformer i enskild regi.

Samrådsskyldigheten vid tillsyn, som den är utformad i dag, kan konkret innebära att, om t.ex. Säkerhetspolisen vill utföra tillsyn av ett bolag vars verksamhet avser elektronisk kommunikation, så måste sådan tillsyn utföras i samråd med Post- och telestyrelsen. Samrådsskyldigheten är i regel inget problem utan tillsynen utförs av de båda myndigheterna tillsammans och den samlade kompentensen kan på så sätt användas på ett ändamålsenligt sätt. Det kan dock finnas situationer där behovet av tillsyn är av sådan karaktär att Säkerhetspolisen eller Försvarsmakten bör kunna agera utan att först samråda med den säkerhetsskyddsstödjande myndigheten. Det kan gälla såväl i en rådgivningssituation som när behov finns av att relativt omgående kunna utföra en kontroll av t.ex. ett bolag som bedriver en verksamhet som är av stor betydelse för Sveriges säkerhet. En annan situation är när tillsynen avser områden där det är olämpligt att den säkerhetsskyddsstödjande myndigheten utför tillsynen. En säkerhetsskyddsstödjande myndighet har också för enskilda verksamheter inom sitt ansvarsområde i uppgift att besluta om placering av anställningar i säkerhetsklass och, enligt vårt förslag i kapitel 19, att teckna säkerhetsskyddsavtal för sådana verksamheter. I de avseendena bör Säkerhetspolisen kunna utöva tillsyn utan krav på samråd. Av de skäl som anförts bör samråd med annan som ska utföra tillsyn av bolag, föreningar, stiftelser och enskilda näringsidkare inte vara ett absolut krav. Det kan i förordningsbestämmelsen uttryckas på så sätt att tillsynen, om inte särskilda skäl talar emot det, ska utföras i samråd.

Leverantörer vars verksamhet är av stor betydelse för Sveriges säkerhet

En situation där samrådsskyldigheten kan vålla betydligt större problem är om tillsynen avser ett bolag som omfattats av säkerhetsskyddsavtal och som är leverantör till ett flertal myndigheter inom olika samhällssektorer. Samrådsskyldigheten som den är utformad i dag innebär då att Säkerhetspolisen behöver samråda med samtliga myndigheter som har ett säkerhetsskyddsavtal med det aktuella bolaget innan tillsyn kan utföras. Det kan i vissa fall röra sig om ett avsevärt antal myndigheter. En leverantörs uppdrag till de olika

myndigheterna kan sammantaget innebära en betydande insyn i och möjlighet att påverka säkerhetskänslig verksamhet av olika slag och inom skilda samhällssektorer. Så kan t.ex. vara fallet i fråga om vissa leverantörer av it- och kommunikationslösningar. Säkerhetspolisen har påtalat att samrådsskyldigheten i praktiken hindrar en effektiv tillsyn av leverantörer som kan vara särskilt angelägna att utföra tillsyn över. En mer ändamålsenlig ordning är att Säkerhetspolisen får till uppgift att utföra tillsyn av sådana leverantörer. Något krav på samråd med myndigheter som har anlitat leverantören bör inte föreskrivas för de fallen.

Rådgivning till bl.a. Regeringskansliet

Säkerhetspolisen ska på begäran lämna råd om säkerhetsskydd till Regeringskansliet, riksdagen och dess myndigheter samt till Justitiekanslern (47 § säkerhetsskyddsförordningen). Det förekommer också att Försvarsmakten på begäran lämnar sådana råd till Regeringskansliet, framför allt till Försvarsdepartementet men också avseende kryptografiska funktioner. Ett genomförande av vårt förslag att Försvarsmakten ska ha rollen som nationell säkerhetsmyndighet kan antas medföra att råd från Försvarsmakten efterfrågas också i t.ex. frågor som rör säkerhetsintyg. Mot den bakgrunden bör också Försvarsmakten nämnas i den aktuella förordningsbestämmelsen (se avsnitt 20.3). Samtidigt bör bestämmelsen kompletteras på så sätt att det framgår att sådan rådgivning samordnas av Säkerhetspolisen.

21.2.4 De säkerhetsskyddsstödjande myndigheterna

Nuvarande ordning

De myndigheter vi valt att benämna säkerhetsskyddsstödjande myndigheter har uppgifter som innebär att de för vissa enskilda verksamheters räkning ska besluta om placering av anställningar och annat deltagande i säkerhetsklass och ansvara för ansökan till Säkerhetspolisen om registerkontroll till följd av sådana beslut. I vissa fall har de även det slutliga avgörandet i fråga om säkerhets-

prövningen.[15] Till dessa uppgifter kommer att myndigheterna enligt den gällande säkerhetsskyddsförordningen har till uppgift att kontrollera säkerhetsskyddet hos bolag, föreningar och stiftelser som avses i 1 § 2 säkerhetsskyddslagen samt hos enskilda som avses i 1 § 3 säkerhetsskyddslagen (40 § säkerhetsskyddsförordningen). De myndigheter det är fråga om har ofta även till följd av annan reglering tillsynsuppgifter inom det angivna ansvarsområdet.[16]

Rådgivning och tillsyn

De säkerhetsskyddsstödjande myndigheterna bör utföra tillsyn i samma omfattning som enligt gällande ordning. På samma sätt som för Säkerhetspolisen och Försvarsmakten påverkas tillsynens omfattning formellt sett av att lagen utsträcks till att gälla säkerhetsskydd till följd av internationella säkerhetsskyddsåtaganden. Därutöver ser vi behov av att de säkerhetsskyddsstödjande myndigheternas roll i fråga om rådgivning uttryckligen framgår av författningstext. I avsnitt 14.1 har vi tagit upp att de säkerhetsskyddsstödjande myndigheterna bör kunna vägleda enskilda verksamheter i fråga om säkerhetsskyddslagens tillämplighet. Sådan vägledning kan innebära framtagande av manualer eller liknande som kan vara ett stöd för att kunna identifiera vad som inom det aktuella området (elförsörjning, elektronisk kommunikation etc.), utgör säkerhetskänslig verksamhet. Det kan också innebära att i samråd med Säkerhetspolisen och Försvarsmakten ta fram underlag i fråga om vilka hot som säkerhetsskyddet inom det berörda området behöver vara dimensionerat för. Råd av det slag som här i fråga är viktigt för att säkerställa ett för nationen tillräckligt säkerhetsskydd.[17] Vad som nu sagts gäller också kommunal och landstingskommunal verksamhet. Rådgivning av sådant slag bör också kunna bidra till att sådana för enskilda ingripande åtgärder som säkerhetsprövning med registerkontroll inte används när det inte är

[15] Se vidare avsnitt 18.11. Enligt vårt förslag i kapitel 19 ska de även teckna säkerhetsskyddsavtal för enskilda verksamheters räkning.
[16] Se vidare redovisningen av närliggande reglering i kapitel 5 och redovisningen av myndigheterna i avsnitt 7.2.
[17] En sådan ordning är i linje med förarbetsuttalanden till nuvarande säkerhetsskyddslag där det framhålls att den beredskapsansvariga myndigheten bör i förekommande fall kunna erinra ett företag om att det omfattas av säkerhetsskyddslagen (Prop. 1995/96:129 Säkerhetsskydd, s. 37).

motiverat och att säkerhetsskyddet utformas på ett kostnadseffektivt sätt.

Myndigheten för samhällsskydd och beredskap bör få uppgifter i fråga om säkerhetsskyddet hos bl.a. kommuner

En fråga som inte tas upp i våra direktiv utan som har aktualiseras på annat sätt är om det finns anledning att göra förändringar i fråga om de utsedda säkerhetsskyddsstödjande myndigheterna och deras respektive ansvarsområden. I det sammanhanget har också frågan om vilken myndighet som ska ansvara för rådgivning och tillsyn över kommunal verksamhet aktualiserats.

I en rapport från Strålsäkerhetsmyndigheten om skydd av kärntekniska anläggningar och transporter av kärnämnen mot antagonistiska hot[18] föreslås att Strålsäkerhetsmyndigheten ska tilldelas bl.a. tillsynsansvar avseende kärntekniska anläggningar som enligt säkerhetsskyddsförordningen ska utövas av Affärsverket svenska kraftnät respektive länsstyrelsen.[19] Vidare har Energimyndigheten i kontakter med utredningen framfört att det finns behov av att myndigheten i fråga om säkerhetsskydd tilldelas föreskriftsrätt och tillsynsansvar avseende olje-, drivmedels-, naturgas- samt fjärrvärme- och fjärrkylaförsörjningen.

En grundläggande fråga är om det är ändamålsenligt att utöka antalet säkerhetsskyddsstödjande myndigheter. Frågan handlar inte enbart om Strålsäkerhetsmyndigheten och Energimyndigheten. Det finns anledning att anta att det kan finnas fler myndigheter som, på samma sätt som Affärsverket svenska kraftnät, Post- och telestyrelsen och Transportstyrelsen skulle kunna komma i fråga för motsvarande föreskriftsrätt och tillsynsansvar. Finansinspektionen är t.ex. en tänkbar myndighet i det här sammanhanget.

Att fördela uppgiften mellan fler myndigheter är dock inte oproblematiskt. Förslaget att Strålsäkerhetsmyndigheten, i syfte att

[18] Översyn av tillståndshavarnas och samhällets förmåga att skydda kärntekniska anläggningar och transporter av kärnämnen mot antagonistiska hot, Strålsäkerhetsskyddsmyndigheten: 2012-01-18, SSM 2010-2632. Rapporten föregicks av att ett uppdrag från Regeringen åt Strålsäkerhetsmyndigheten att i samråd med Rikspolisstyrelsen, Affärsverket svenska kraftnät och Myndigheten för samhällsskydd och beredskap genomföra en översyn av tillståndshavarnas och samhällets förmåga att skydda kärntekniska anläggningar och transporter av kärnämnen mot antagonistiska hot, (M2010/3091/Mk).
[19] Rapporten s. 69.

skapa en sammanhållen tillsynsfunktion för strålskyddet, skulle överta ansvaret för kärnkraftanläggningar från Affärsverket svenska kraftnät skulle samtidigt medföra att tillsynsfunktionen i fråga om elförsörjningen inte längre hålls samman. En ordning där tillsynen över säkerhetsskyddet sprids på fler myndigheter än i dag ser vi inte heller som ändamålsenlig. Samtidigt är det viktigt att säkerhetskänsliga verksamheter inom andra områden än elförsörjning, elektronisk kommunikation och flygtransportverksamhet har en aktiv säkerhetsskyddsstödjande myndighet.

Som regleringen är utformad i dag fördelas ansvaret för enskilda verksamheter inom områden som inte Affärsverket svenska kraftnät, Post- och telestyrelsen eller Transportstyrelsen ansvarar för på de olika länsstyrelserna utifrån geografiskt ansvar. Det tycks ha inneburit att länsstyrelserna i en mycket begränsad utsträckning har en roll i fråga om säkerhetsskyddet hos enskilda. Möjligen skulle en ordning där uppgiften koncentreras till en eller några av länsstyrelserna kunna medföra bättre förutsättningar för att ta hand om uppgiften. En sådan lösning förekommer bl.a. i fråga om tillsyn på andra områden.[20] Vi bedömer dock att det inte är tillräckligt. Det gäller inte minst mot bakgrund av att utvecklingen går mot att säkerhetsskydd i större utsträckning än tidigare är en angelägenhet för enskilda verksamheter. Det medför att de säkerhetsskyddsstödjande myndigheterna som framgått ovan behöver ha en aktiv roll i fråga om att vägleda och stödja enskilda verksamheter.

En i sammanhanget relevant fråga är också vilken myndighet som är bäst lämpad för att stödja kommuner och landsting i fråga om säkerhetsskydd. I dag har Säkerhetspolisen det ansvaret. Det har framförts att det är angeläget att säkerhetsskyddet i den kommunala verksamheten får en omfattning som svarar mot de nationella behoven av säkerhetsskydd, dvs. att kraven på säkerhetsskydd inriktas på sådan verksamhet hos kommuner och landsting som från ett nationellt perspektiv är särskild skyddsvärd.

Myndigheten för samhällsskydd och beredskap har ett övergripande ansvar för bl.a. skyddet av den för samhället kritiska infrastrukturen från ett samhällsskydds- och beredskapsperspektiv. Det innefattar bl.a. uppgiften att utifrån EU-direktivet om skydd för

[20] Se 6 § förordning (2007:825) med länsstyrelseinstruktion.

kritisk infrastruktur[21] utarbeta strategier med fokus på skydd av samhällsviktiga verksamheter och viktiga samhällsfunktioner. Myndigheten har också ett ansvar för att samordna arbetet med samhällets informationssäkerhet (se vidare avsnitt 7.3.1). Myndighetens uppdrag medför upparbetade kontaktytor och strukturer gentemot kommuner och landsting. Detsamma gäller gentemot enskilda som bedriver säkerhetskänslig verksamhet. Myndighetens uppdrag är i stor utsträckning inriktat på att vägleda och stödja verksamheter av olika slag, både allmänna och enskilda, i fråga om beredskap och samhällsskydd. Mot den bakgrunden ser vi goda förutsättningar för Myndigheten för samhällsskydd och beredskap att axla den rollen. I fråga om kommuner och landsting bör, i enlighet med gällande ordning i fråga om beslut om placering i säkerhetsklass, rollen som säkerhetsstödjande myndighet avgränsas till rådgivning och tillsyn.

Transportstyrelsens ansvarsområde bör samtidigt utvidgas från civil flygtransportverksamhet till att avse även verksamhet som i övrigt är av betydelse för luftfartsskydd eller för hamnskydd och sjöfartsskydd. En sådan ordning sammanfaller med Transportstyrelsens föreslagna ansvarsområde i fråga om beslut om placering i säkerhetsklass (se avsnitt 18.10) och även i fråga om Transportstyrelsen tillsynsansvar i andra avseenden vad gäller hamnskydd och sjöfartsskydd.

21.3 Föreskrifter om säkerhetsskydd

Rätten att meddela föreskrifter bör i huvudsak vara densamma som i nuvarande säkerhetsskyddslagstiftning. Det innebär att föreskriftsrätten fördelas främst mellan Säkerhetspolisen och Försvarsmakten. I fråga om föreskriftsrätten behöver nuvarande förordningsbestämmelser kompletteras i vissa avseenden. Det gäller Försvarsmaktens uppgifter i internationellt säkerhetsskyddssamarbete (dvs. uppgifter som följer av rollen som nationell säkerhetsmyndighet, se avsnitt 20.3 och 20.4). Vi har tidigare i avsnitt 16.2.2 föreslagit att den föreskriftsrätt Försvarsmakten har när det gäller

[21] Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av och klassificering som europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EPCIP).

signalskyddstjänsten enligt 33 § förordningen (2007:1266) med instruktion för Försvarsmakten moderniseras och flyttas till en ny säkerhetsskyddsförordning. Föreskriftsrätten ska utformas så att den i stället gäller för kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet.

Även Försvarets materielverk bör ha viss föreskriftsrätt i rollen som nationell industrisäkerhetsmyndighet vilket innefattar de närmare bestämmelser som behövs i fråga om säkerhetsintyg för leverantörer (se avsnitt 20.4).

Säkerhetspolisen och Försvarsmakten bör ha en skyldighet att samråda med varandra innan föreskrifter meddelas. Sådan samrådsskyldighet bör också i relevanta avseenden gälla för Försvarets materielverk.

Det kvarstående utrymmet för de säkerhetsskyddsstödjande myndigheterna att meddela föreskrifter är begränsat. Föreskriftsrätten bör avse sådana kompletteringar av Säkerhetspolisens och Försvarsmaktens föreskrifter som i relation till den aktuella sektorn behövs för att ytterligare konkretisera kraven på säkerhetsskydd, t.ex. närmare förutsättningar inom ansvarsområdet för att placera anställningar i säkerhetsklass. Liksom i dag bör samråd med bl.a. Säkerhetspolisen vara en förutsättning för meddelande av sådana föreskrifter.

21.4 Rapporteringskrav

21.4.1 Allmänt om rapporteringskrav

För att tillsynsmyndigheterna ska kunna utöva sin tillsyn på ett effektivt sätt och för att utfärdade tillämpningsföreskrifter ska bli så ändamålsenliga som möjligt är det av stor vikt att de får kännedom om händelser och företeelser som är av betydelse för säkerhetsskyddet. Nuvarande säkerhetsskyddsförordning innehåller enbart en bestämmelse om en rapporteringsskyldighet till Säkerhetspolisen när en hemlig uppgift kan ha blivit röjd och där röjandet inte enbart medfört ett ringa men. En sådan begränsad rapporteringsskyldighet är inte tillräcklig.

Förslaget till det tidigare redovisade NIS-direktivet innehåller i sin nuvarande utformning bestämmelser om skyldigheter för bl.a. operatörer av kritisk infrastruktur att under vissa förutsättningar

underrätta de behöriga myndigheterna i respektive medlemsstat om sådana incidenter som på ett allvarligt sätt kan påverka kontinuiteten för kritiska tjänster och tillhandahållandet av varor. En sådan rapporteringsskyldighet kan sannolikt antas gälla även annat än vad som omfattas av säkerhetsskyddslagen och därför behöva finnas i annan reglering. Vidare kan de förslag till rapportering som vi föreslår i det följande behöva kompletteras eller förändras beroende på direktivets slutliga utformning och dess genomförande i svensk rätt.

I avsnitt 14.2 har vi föreslagit en bestämmelse i säkerhetsskyddslagen som bl.a. anger en grundläggande skyldighet för den som ansvarar för en säkerhetskänslig verksamhet att utreda behovet av säkerhetsskydd, vidta säkerhetsskyddsåtgärder och kontrollera det egna säkerhetsskyddet. Bestämmelsen anger även en skyldighet att i den omfattning som anges i den till lagen hörande förordningen lämna uppgifter om säkerhetsskyddet. De bestämmelser som vi i de följande avsnitten 21.4.2-21.4.4 föreslår om rapporteringsskyldighet, och som inte enbart berör myndigheter, bör därför kunna meddelas i förordning.

21.4.2 Röjande av en säkerhetsskyddsklassificerad uppgift

I 10 § säkerhetsskyddsförordningen finns som nämnts tidigare en bestämmelse som innebär att, om en hemlig uppgift kan ha röjts, det skyndsamt ska anmälas till Säkerhetspolisen, om röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa. Bestämmelsen bör kvarstå i en ny förordning men anpassas till ny terminologi och i stället ange att, om en säkerhetsskyddsklassificerad uppgift i lägst informationssäkerhetsklassen konfidentiell kan ha röjts, så ska detta skyndsamt anmälas till Säkerhetspolisen. Någon ändring i sak är inte avsedd. Bestämmelsen bör dock kompletteras med ett tillägg som tar sikte på säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande genom att ett röjande av sådana uppgifter även ska rapporteras till Försvarsmakten. Skälet är att Försvarsmakten ska ges förutsättningar att fullfölja sina skyldigheter som nationell säkerhetsmyndighet och kunna rapportera röjandet till

den upprättande myndigheten i en annan stat eller mellanfolklig organisation (se avsnitt 20.3).

21.4.3 Allvarlig säkerhetshotande verksamhet

Att en säkerhetsskyddsklassificerade uppgift har röjts är ett slag av säkerhetshotande verksamhet. Inte sällan handlar det i dag om incidenter av annat slag. Som vi har beskrivit tidigare riktas allvarliga it-angrepp av olika slag allt oftare mot säkerhetskänslig verksamhet. Det förekommer också allvarliga angrepp riktade mot det fysiska skyddet av områden, byggnader eller andra anläggningar eller objekt som avser säkerhetskänslig verksamhet. Kännedom om säkerhetshotande verksamhet är en väsentlig förutsättning för att kunna ta fram en korrekt och aktuell hotbeskrivning och även i övrigt ge råd och stöd till enskilda verksamheter samt utföra tillsyn på ett ändamålsenligt sätt. Det är därför angeläget att de myndigheter som utför tillsyn får information om säkerhetshotande verksamhet inom sitt tillsynsområde. Av skäl som vi redovisat tidigare är det lika angeläget att den samlade informationen om säkerhetshotande verksamhet mot Sverige finns hos Säkerhetspolisen och Försvarsmakten. En rapporteringsskyldighet bör därför utformas så att myndigheter och andra som förordningen gäller för och som får kännedom om säkerhetshotande verksamhet eller misstänker sådan verksamhet ska rapportera förhållandet till berörd tillsynsmyndighet, dvs. Säkerhetspolisen, Försvarsmakten eller den säkerhetsskyddsstödjande myndigheten. Om sådan information lämnas till en säkerhetsskyddsstödjande myndighet ska myndigheten skyndsamt informera Säkerhetspolisen eller, om det är fråga verksamhet inom Försvarsmaktens tillsynsområde, Försvarsmakten.

För att en sådan rapporteringsskyldighet som här är i fråga ska vara ändamålsenlig och inte mer betungande än nödvändigt behöver den innehålla en kvalificeringsregel. Skyldigheten bör begränsas till säkerhetshotande verksamhet av allvarlig karaktär. Exempel på säkerhetshotande verksamhet som är av allvarlig karaktär är sådan där angreppen är av kvalificerad art eller tyder på en systematisk och målinriktad strategi från en aktör. Vidare torde angrepp som samtidigt riktas mot flera verksamheter inom en

samhällssektor ofta anses vara allvarliga. Nya och tidigare okända angreppssätt och metoder medför att allvarlighetskriteriet kan vara uppfyllt. Säkerhetshotande verksamhet av mindre betydelse som t.ex. överträdelser mot tillträdesförbud eller smärre it-incidenter ger i regel inte tillsynsmyndigheterna sådan information som kan motivera en rapporteringsskyldighet.

Bestämmelsen bör också innehålla ett skyndsamhetskrav för att säkerställa att tillsynsmyndigheten ska kunna ge stöd i fråga om säkerhetsskyddsåtgärder i ett tidigt skede i syfte att minska effekter och spridning av den säkerhetshotande verksamheten.

21.4.4 Överlåtelse av säkerhetskänslig verksamhet

I 16 § säkerhetsskyddsförordningen finns en bestämmelse som tar sikte på förhållandet att viss verksamhet kan överlåtas från en myndighet till en enskild. Bestämmelsen anger att när en myndighet ska överlåta verksamhet som är av betydelse för rikets säkerhet eller som särskilt behöver skyddas mot terrorism till en enskild, så ska myndigheten upplysa den enskilde om att säkerhetsskyddslagen gäller för verksamheten.

I kapitel 9 har vi beskrivit att säkerhetskänslig verksamhet i allt större utsträckning bedrivs av enskilda. Särskilt utvecklingen på it-området och avregleringar av el- och telekommunikationsmarknaderna har påskyndat denna utveckling. Bestämmelsen har därför fortsatt giltighet i en ny säkerhetsskyddslagstiftning, men bör enligt vår uppfattning utvecklas i tre avseenden.

För det första bör upplysningen kompletteras med en hänvisning till de skyldigheter som anges i 2 kap. 2 och 4 §§ i förslaget till säkerhetsskyddslag, vilka är centrala för tillämpningen av säkerhetsskyddslagstiftningen. Skyldigheterna redovisas närmare i avsnitt 14.2. För den som övertar verksamheten blir det då tydligt vad som förväntas avseende säkerhetsskydd.

För det andra är det möjligt att även enskilda som bedriver säkerhetskänslig verksamhet kan komma att överlåta sådan verksamhet till andra enskilda. Bestämmelsen bör därför inte vara begränsad till att avse enbart myndigheter utan gälla generellt för de som lagen gäller för.

För det tredje bör bestämmelsen kompletteras med en skyldighet för den som planerar en sådan överlåtelse att anmäla det till den myndighet som ska utföra tillsyn. Skälet till en sådan komplettering är att Säkerhetspolisen och Försvarsmakten, och i förekommande fall de säkerhetsskyddsstödjande myndigheterna, tidigt ska få information om överlåtelsen i syfte att kunna ge råd och stöd för att säkerhetsskyddet för den säkerhetskänsliga verksamheten inte ska försämras i och med överlåtelsen.

21.4.5 Brister i säkerhetsskyddet som konstateras vid tillsyn

I 48 § säkerhetsskyddsförordningen finns en bestämmelse som anger att, om det vid utövandet av tillsynen över säkerhetsskyddet konstateras brister som trots påpekanden inte rättas till, så ska tillsynsmyndigheten anmäla förhållandet till regeringen. Detta gäller dock inte brister hos sådana enskilda där villkoren för säkerhetsskyddet angetts i ett säkerhetsskyddsavtal.

Vi har redovisat att vi anser att tillsynen inte ska kompletteras med sanktioner. Ordningen där regeringen av Säkerhetspolisen och Försvarsmakten ska upplysas om brister i säkerhetsskyddet som inte rättas till efter påpekande fyller därmed alltjämt en funktion. Dels innebär den ett visst incitament för den kontrollerade att rätta sig efter en myndighets påpekanden, dels att regeringen får ett underlag som kan ge anledning till regeringsbeslut eller normgivning. Bestämmelsen bör därför finnas kvar, men även i detta fall bör bestämmelsen kompletteras med ett kvalificeringskrav att rapporteringsskyldigheten enbart ska avse allvarliga brister. Skälet är att enbart de verkligt betydelsefulla bristerna i säkerhetsskyddet kan anses vara relevanta för regeringen att få information om.

Som vi beskrivit ovan kommer även de säkerhetsskyddsstödjande myndigheterna på samma sätt som i dag att utföra tillsyn. Om en sådan myndighet i sin tillsynsverksamhet konstaterar att det föreligger allvarliga brister, bör den säkerhetsskyddsstödjande myndigheten informera Säkerhetspolisen. Skälet till det är att Säkerhetspolisen kan behöva sådan information för att t.ex. följa upp bristerna vid den aktuella verksamheten eller för att vidta andra åtgärder.

Om bristerna gäller verksamhet som omfattas av ett internationellt säkerhetsskyddsåtagande, ska myndigheten också informera Försvarsmakten. Skälet till detta är detsamma som redovisats ovan under rapportering av röjd uppgift, nämligen med avseende på Försvarsmaktens skyldigheter som nationell säkerhetsmyndighet.

22 Övriga frågor

22.1 Tystnadsplikt vid deltagande i säkerhetskänslig verksamhet

Förslag: Den som på grund av anställning eller på annat sätt deltar eller har deltagit i en säkerhetskänslig verksamhet får inte obehörigen röja eller utnyttja vad han eller hon därvid fått veta om förhållanden av betydelse för Sveriges säkerhet eller förhållanden som omfattas av ett för Sverige förpliktande åtagande om säkerhetsskydd (säkerhetsskyddsklassificerade uppgifter). En förutsättning för tystnadsplikten ska vara placering i säkerhetsklass.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400), OSL.

Behovet av en kompletterande bestämmelse om tystnadsplikt

Vi har tidigare behandlat den otydlighet som finns i nuvarande säkerhetsskyddslag i fråga om krav på säkerhetsskydd när uppgifter som är av betydelse för Sveriges säkerhet eller som omfattas av internationella säkerhetsskyddsåtaganden hanteras i enskild verksamhet (se förslag om säkerhetsskyddsklassificerade uppgifter i avsnitt 12.2). Vid behandling av den frågan har vi uppmärksammat att en motsvarande otydlighet finns i fråga om sekretess för sådana uppgifter (dvs. när uppgifterna förekommer i en enskild verksamhet). Frågan har ett sådant samband med säkerhetsskydd att det finns anledning att i detta sammanhang behandla den.

Sekretess innebär ett förbud mot att röja en uppgift som omfattas av sekretess, vare sig det sker muntligen eller genom att lämna ut handlingar som innehåller sekretessbelagda uppgifter.

Sekretess innebär också ett förbud mot att utnyttja sekretessbelagda uppgifter utanför den verksamhet i vilken sekretess gäller för uppgiften. Den personkrets som är bunden av tystnadsplikt och sekretess är i första hand de som är anställda vid organ som ska tillämpa offentlighets- och sekretesslagen (se 2 kap. 1 § OSL). Fysiska personer som agerar som uppdragstagare åt sådana organ anses vara knutna till verksamheten på ett sådant sätt att de också är bundna av offentlighetsprincipen och bestämmelserna om tystnadsplikt och sekretess (RÅ 1996 ref 25). En myndighet kan också ingå avtal eller annan överenskommelse om tystnadsplikt för uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen. Ett sådant förfarande kan tillämpas när en myndighet inom ramen för säkerhetsskyddad upphandling anlitar externa leverantörer.

En brist i fråga om sekretess kan dock föreligga i vissa enskilda verksamheter som, utan att det är fråga om en upphandlingssituation, har kännedom om förhållanden av betydelse för Sveriges säkerhet eller förhållanden som omfattas av internationella säkerhetsskyddsåtaganden. Det handlar om när säkerhetskänslig verksamhet bedrivs i enskild regi. Problemet har således en begränsad räckvidd. Det bör kunna lösas genom en till offentlighets- och sekretesslagen kompletterande bestämmelse om tystnadsplikt.

En till offentlighets- och sekretesslagen kompletterande bestämmelse om tystnadsplikt

Bestämmelser om tystnadsplikt av det slag som det här är fråga om finns i flera andra lagar. En till offentlighets- och sekretesslagen kompletterande bestämmelse om tystnadsplikt finns t.ex. i 16 § elberedskapslagen (1997:288). Den lagen innehåller bestämmelser om elberedskapsåtgärder avseende elproducenter, elhandelsföretag och nätföretag som ska syfta till att förebygga, motstå och hantera sådana störningar i elförsörjningen som kan medföra svåra påfrestningar på samhället. Bestämmelsen om tystnadsplikt innebär ett förbud för den som på grund av bestämmelser i elberedskapslagen eller föreskrifter som meddelats med stöd av den lagen har fått kännedom om bl.a. förhållanden som är av betydelse för totalförsvaret eller för rikets säkerhet i övrigt att obehörigen röja eller ut-

nyttja uppgifterna. En liknande bestämmelse finns i 29 § skyddslagen (2010:305). Där föreskrivs ett förbud för skyddsvakter att bl.a. obehörigen röja eller utnyttja vad han eller hon, på grund av ett uppdrag enligt skyddslagen, fått veta om förhållanden av betydelse för totalförsvaret eller annars för Sveriges säkerhet. En annan bestämmelse om tystnadsplikt som tar sikte på bl.a. förhållanden av betydelse för totalförsvaret eller rikets säkerhet i övrigt finns i 7 kap. 1 § lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Också i 11 kap. 65 § plan- och bygglagen (2010:900) finns en liknande bestämmelse som bl.a. avser förhållanden av betydelse för Sveriges försvar.

En tystnadsplikt är straffsanktionerad som brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken. Eventuella negativa konsekvenser av att införa en straffsanktionerad tystnadsplikt måste därför ställas mot de intressen som förbudet avser att skydda. Krav måste också ställas på precision och förutsebarhet avseende det straffbara området.

Hänsynen till skyddet av för nationen viktiga säkerhetsintressen väger tungt. Dessutom är tillämpningsområdet för en bestämmelse av det slag som här är i fråga begränsat. Tystnadsplikten är inte avsedd att träffa annat än uppgifter som avser det för nationen mest skyddsvärda. Uppgifter av det slaget bör ha samma skydd oavsett om uppgiften finns i en verksamhet som omfattas av offentlighets- och sekretesslagen eller i en verksamhet som inte omfattas av den lagen. I fråga om bl.a. anställda vid myndigheter gäller redan enligt offentlighets- och sekretesslagen ett straffsanktionerat förbud att obehörigen röja eller utnyttja motsvarande uppgifter. Den redovisade exemplifiering av tystnadspliktsbestämmelser visar att enskilda verksamheter inom bl.a. elsektorn redan i dag genom annan reglering omfattas av en tystnadsplikt som tar sikte på liknande uppgifter. Tystnadsplikt bör därför gälla för den som deltar eller har deltagit i sådan verksamhet som här är i fråga. Tystnadsplikten bör avse alla slag av säkerhetsskyddsklassificerade uppgifter, dvs. omfatta såväl uppgifter som har betydelse för Sveriges säkerhet som uppgifter som omfattas av internationella säkerhetsskyddsåtaganden.

För att bättre tillgodose straffrättsliga krav på precision och förutsebarhet är det lämpligt att tystnadsplikten begränsas till

sådana anställningar eller andra former av deltaganden i säkerhetskänslig verksamhet där kraven för placering i säkerhetsklass är uppfyllda. På förordningsnivå bör bestämmelser införas som anger en skyldighet för den som ansvarar för säkerhetsprövningen att upplysa den som prövningen avser om tystnadspliktens omfattning och innebörd. En rutinåtgärd i samband med säkerhetsprövning bör också vara att låta den berörde bekräfta att han eller hon har fått information om tystnadspliktens omfattning och innebörd.

22.2 Säkerhetsskyddet i riksdagen och Regeringskansliet

Förslag: Säkerhetsskyddslagens bestämmelser om informationssäkerhetsklass, säkerhetsprövning och säkerhetsintyg ska gälla också för riksdagen och dess myndigheter och för Regeringskansliet.

Säkerhetsskyddslagen gäller endast i viss angiven utsträckning för riksdagen och dess myndigheter[1] och för Regeringskansliet. Det handlar bl.a. om bestämmelserna om placering i säkerhetsklass och om registerkontroll. Säkerhetsskyddsförordningen gäller inte för riksdagen. Den gäller i begränsad utsträckning för Regeringskansliet.[2]

Vad gäller riksdagen finns det bestämmelser om säkerhetsskydd även i lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter. Den lagen, som kompletteras med föreskrifter, har säkerhetsskyddslagen som förebild. För Regeringskansliet gäller på motsvarande sätt även föreskrifter om säkerhetsskyddet i Regeringskansliet (RKF 1998:16). Vid en översiktlig genomgång av de särskilda regleringarna om säkerhetsskyddet för riksdagen och för Regeringskansliet kan konstateras att det där i stor utsträckning finns reglering som svarar mot den som finns i säkerhetsskyddslagen och att de särskilda regleringarna stämmer överens med de grundprinciper som säkerhetsskyddslagen ger uttryck för. Det

[1] I den fortsatta framställningen nämns endast riksdagen.
[2] Beträffande riksdagen och dess myndigheter, se 2 § säkerhetsskyddslagen och beträffande Regeringskansliet se 32 § säkerhetsskyddslagen och 2 § säkerhetsskyddsförordningen.

innebär dock inte att det i alla avseenden finns en konformitet i fråga om kraven på säkerhetsskydd. Några närmare skäl till den gällande ordningen – där säkerhetsskyddslagen endast delvis gäller för riksdagen och Regeringskansliet – redovisas inte i förarbetena till säkerhetsskyddslagen.[3]

Säkerhetsskyddslagens begränsade tillämplighet i fråga riksdagen och Regeringskansliet nämns i våra direktiv endast under redovisningen av gällande ordning. Det hindrar dock inte att vi berör frågan. Vi har haft en inledande dialog med Riksdagsförvaltningen och Regeringskansliet. Vad som därvid förts fram har inte föranlett oss gå närmare in på denna fråga. Vår utgångspunkt har därför varit att, utan någon ändring i sak, föra över gällande bestämmelser om säkerhetsskyddslagens tillämplighet i fråga om riksdagen och Regeringskansliet till förslaget om en ny säkerhetsskyddslag. I vissa avseenden ser vi det dock ändå som nödvändigt att föreslå annat än redaktionella ändringar.

En genomgripande förändring i förslaget till ny säkerhetsskyddslag är att bl.a. uppgifter av betydelse för Sveriges säkerhet ska delas in i en av fyra informationssäkerhetsklasser (kvalificerat hemlig, hemlig, konfidentiell och begränsad) och att nivån på säkerhetsskyddet ska anpassas till den gjorda klassificeringen. I fråga om säkerhetsprövning av anställda och andra som deltar i säkerhetskänslig verksamhet medför förslaget om krav på klassificering av uppgifter att de nuvarande grunderna för placering i säkerhetsklass behöver ändras. Det handlar dels om en anpassning till den fyrgradiga skalan, dels om att nivån på de uppgifter som den berörde får del av i högre grad än i dag ska styra valet av säkerhetsklass (se avsnitt 18.5). För att riksdagen och Regeringskansliet ska kunna tillämpa säkerhetsskyddslagens bestämmelser om placering i säkerhetsklass är det därför enligt vår bedömning nödvändigt att också den föreslagna bestämmelsen om informationssäkerhetsklasser gäller för dessa verksamheter.

[3] Redan enligt den ordning som gällde när förslaget om en säkerhetsskyddslag lades fram fanns särskilda föreskrifter om säkerhetsskydd för riksdagen och för Regeringskansliet, och det förutsattes att den ordningen skulle gälla även efter säkerhetsskyddslagens införande (Prop. 1995/96:129 Säkerhetsskydd, s. 73 och 89). Det ingick inte heller i Säkerhetsskyddsutredningens uppdrag att ta ställning till säkerhetsskyddet hos regering och riksdag (Dir. 1993:123 s. 3).

I avsnitt 20.4.2 har vi behandlat frågan om möjlighet till säkerhetsintyg för internationella behov. Den möjligheten till intyg bör finnas även för anställda och andra som deltar i verksamhet vid riksdagen och i Regeringskansliet. Bestämmelserna i fråga om riksdagen och Regeringskansliet bör därför även hänvisa till säkerhetsskyddslagens bestämmelser om säkerhetsintyg.

Slutligen har vi i fråga om Regeringskansliet uppmärksammat ett behov av en smärre justering. Enligt 32 § säkerhetsskyddslagen får undantagen från lagens tillämpning i fråga om Regeringskansliet avse andra bestämmelser i lagen än sådana som gäller registerkontroll. I fråga om riksdagen avser dock undantagen andra bestämmelser än sådana som gäller säkerhetsprövning. Undantaget för riksdagen fick den omfattningen i enlighet med Lagrådets förslag.[4] I det till Lagrådet remitterade förslaget avsåg undantaget för riksdagen, på samma sätt som undantaget för Regeringskansliet, endast registerkontroll. Det är rimligt att anta att regeringens möjlighet att föreskriva undantag från lagens tillämpning för Regeringskansliet borde ha fått en motsvarande omfattning, dvs. exkludera samtliga bestämmelser om säkerhetsprövning och inte enbart de som handlar om registerkontroll. Den slutsatsen är också i linje med 2 § säkerhetsskyddsförordningen som anger i vilka avseenden säkerhetsskyddslagen gäller för Regeringskansliet. Vi föreslår därför att regeringens rätt att föreskriva om undantag för Regeringskansliet i det avseendet ändras från registerkontroll till säkerhetsprövning.

Det bör tilläggas att det med anledning av de genomgripande förändringar av regleringen som vi föreslår finns behov av att överväga om motsvarande ändringar ska göras i regleringarna för riksdagen och Regeringskansliet.

[4] Se Lagrådets yttrande, bilaga 5 till Prop. 1995/96:21 Säkerhetsskydd, s. 129.

22.3 Frågor som det kan finnas anledning att behandla i annat sammanhang

Sveriges säkerhet och liknande benämningar

I avsnitt 11.2 har vi föreslagit att benämningen *rikets* säkerhet i säkerhetsskyddslagen ska ersättas med *Sveriges* säkerhet. Det är som vi framhåller en språklig ändring i linje med de ändringar som gjorts i 19 kap. brottsbalken till följd av propositionen 2013/14:51 Förstärkt skydd mot främmande makts underrättelseverksamhet.

Vi har noterat att uttrycket rikets säkerhet används i flera andra författningar, bl.a. i andra delar av brottsbalken[5] och i offentlighets- och sekretesslagen (15 kap. 2 §). Redovisningen i avsnitt 22.1 om tystnadspliktbestämmelser i närliggande reglering innehåller fler exempel. Tystnadspliktbestämmelsen i 7 kap. 1 § lagen om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap omfattar förhållanden av betydelse för *totalförsvaret eller rikets säkerhet i övrigt*. Vid de nämnda ändringarna i brottsbalken togs för övrigt hänvisningen till förhållanden av betydelse för totalförsvaret bort eftersom rekvisitet totalförsvaret inte ansågs fylla någon självständig funktion (se vidare avsnitt 4.1.1). I tystnadspliktsbestämmelsen i 29 § skyddslagen finns en annan variant (av betydelse för *totalförsvaret eller annars för Sveriges säkerhet*). Motsvarande bestämmelse i 11 kap. 65 § plan- och bygglagen hänvisar till förhållanden av betydelse för *Sveriges försvar*. Ytterligare ett exempel på begreppsfloran finns i Säkerhetspolisens instruktion (2014:1103) där det hänvisas till *rikets säkerhet eller andra särskilt viktiga samhällsintressen.*

Antagligen är det i stor utsträckning samma förhållanden som avses med de olika uttrycken. För det fall att andra förhållanden än vad som innefattas i Sveriges säkerhet avses kan det finnas anledning att göra det tydligt. Mot den bakgrunden bör behovet av att få till stånd en harmonisering av terminologin på detta område övervägas.

[5] Regeringen konstaterade att visserligen innebär förslaget att det i vissa straffbestämmelser i brottsbalken fortsatt kommer att hänvisas till riket medan det i andra i stället hänvisas till Sverige eller landet. Regeringen påpekade dock att liknande språkliga skillnader finns redan i dag mellan olika paragrafer och det utgör inte ett skäl att avstå från att modernisera språket i de straffbestämmelser som är föremål för en reform (a. prop. s. 36).

En eventuell följdändring i skyddslagen

I kapitel 17 har vi påpekat att skyddslagens och säkerhetsskyddslagens skyddsändamål i stor omfattning är desamma. Det kan därför finnas anledning att eftersträva att terminologin i de båda lagarna överensstämmer i de fall där detta är möjligt. *Hemliga uppgifter som rör totalförsvaret* i skyddslagens bestämmelse om skyddsändamål tycks dock semantiskt referera till en delmängd av de hemliga uppgifter som definieras i säkerhetsskyddsförordningen. En sådan skillnad verkar dock inte vara avsett enligt vad som framgår av förarbetena.[6] Både skyddslagen och säkerhetsskyddslagen tar sikte på såväl civil som militär verksamhet. Den civila verksamheten har fått en ökande betydelse. Vi har föreslagit att i en ny säkerhetsskyddslag ska begreppet säkerhetsskyddsklassificerad uppgift ersätta hemlig uppgift. Det innebär att även uppgifter som ska skyddas enligt internationella säkerhetsskyddsåtaganden omfattas av definitionen (se avsnitt 12.2). Mot bakgrund av vad som anförts kan det finnas anledning att överväga behovet av att en motsvarande ändring i skyddslagen.

[6] Prop. 2009/10:87 Skyddslagen.

23 Konsekvensbeskrivning

Enligt 14–15 a §§ kommittéförordningen (1998:1474) ska vi göra en kostnadsberäkning och andra konsekvensbeskrivningar av de förslag som vi lägger fram. Vidare följer det av 15 a § kommittéförordningen att, om ett betänkande innehåller förslag till nya eller ändrade regler, förslagens kostnadsmässiga och andra konsekvenser ska anges i betänkandet. Konsekvenserna ska anges på ett sätt som motsvarar de krav på innehållet i konsekvensutredningar som finns i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning. Genom att vi föreslår en ny säkerhetsskyddslag och en ny säkerhetsskyddsförordning samt följdändringar i annan reglering är bestämmelsen i 15 a § kommittéförordningen tillämplig.

Innehållet i konsekvensbeskrivningen följer i stort de områden som framgår av de nämnda bestämmelserna. Förslagen har dock enligt vår uppfattning inte någon påverkan på de områden som anges i 15 § kommittéförordningen[1] varför dessa inte tas upp.

I avsnitt 23.1 redovisar vi vad våra förslag syftar till och en sammanfattande bedömning av vilka konsekvenser förslagen medför. Avsnitt 23.2 innehåller den egentliga konsekvensanalysen. Avsnittet är uppdelat på underavsnitt som behandlar generella aspekter, konsekvenser specifikt för företag, organisatoriska frågor och behov av finansiering. Avslutningsvis redovisas övergångsbestämmelser och ikraftträdande i avsnitt 23.3.

[1] Dessa områden rör kommunala självstyrelsen, betydelse för brottsligheten och det brottsförebyggande arbetet, sysselsättning och offentlig service i olika delar av landet, små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, jämställdheten mellan kvinnor och män samt möjligheterna att nå de integrationspolitiska målen.

23.1 Vad syftar våra förslag till

Ett huvudsyfte med vårt arbete har varit att föreslå en modernisering av säkerhetsskyddslagstiftningen. Målet har varit att lämna förslag om ett regelverk som ger bra förutsättningar för ett väl avpassat, effektivt säkerhetsskydd samtidigt som det erbjuder en flexibilitet över tiden, kan möta skiftande förhållanden och även utgöra ett stöd för internationell samverkan på säkerhetsskyddsområdet.

Syftet med att ersätta den nuvarande säkerhetsskyddslagen med en ny lag är att säkerställa säkerhetsskyddet för verksamheter hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet, eller som omfattas av ett för Sverige, i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd. Lagen ska även i övrigt ge stöd för internationell samverkan på säkerhetsskyddsområdet. Skyddet för *Sveriges säkerhet* är därmed fortfarande centralt i lagstiftningen. Lagen definierar *säkerhetskänslig verksamhet* som verksamhet hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet eller omfattas av ett internationellt säkerhetsskyddsåtagande.

Förslaget till en ny säkerhetsskyddslag bygger på ett tydligare sätt än i dag på att varje verksamhet som omfattas av lagen måste utreda behovet av säkerhetsskydd i den egna verksamheten. En sådan säkerhetsskyddsanalys ligger sedan till grund för hur säkerhetsskyddsåtgärderna kan utformas.

Fler icke-statliga och icke-kommunala aktörer är i allt större utsträckning ansvariga för samhällsviktiga verksamheter. En ökad sårbarhet hos många vitala samhällsfunktioner i kombination med framväxten av en breddad hotbild gör det nödvändigt att ge säkerhetsskyddslagstiftningen ett något vidare tillämpningsområde än i dag. Särskilt gäller detta för informationsteknikområdet i den säkerhetskänsliga verksamheten. Lagen innehåller även bestämmelser som syftar till att underlätta internationell samverkan på säkerhetsskyddsområdet, vilket innefattar smärre organisatoriska förändringar och utökade möjligheter att utfärda s.k. säkerhetsintyg för enskilda och leverantörer som har behov av detta för att kunna delta i säkerhetskänslig verksamhet i andra länder och vid mellanfolkliga organisationer.

Utöver de nämnda förändringarna så bygger förslaget till en ny säkerhetsskyddslagstiftning på nuvarande lagstiftning. Stora delar av den nuvarande regleringen överförs till den nya även om vissa delar av systematiken förändras. Detta medför att konsekvenserna av våra förslag inte blir så omfattande i förhållande till nu gällande reglering.

Sammanfattande bedömning

Sammanfattningsvis har vi kommit fram till att våra förslag inte bör innebära annat än marginellt ökade kostnader vare sig för det allmänna eller för enskilda jämfört med nuvarande lagstiftning.

Det kan likväl förefalla troligt att vissa myndigheter får en något ökad arbetsbelastning till följd av den säkerhetsskyddslag som vi föreslår. Särskilt gäller detta för de säkerhetsskyddsstödjande myndigheterna och i synnerhet för Myndigheten för samhällsskydd och beredskap som vi föreslår bl.a. ska ta över de uppgifter som i dag ankommer på länsstyrelserna. Dessa uppgifter är dock enligt nuvarande lag ytterst begränsade till sin omfattning men kan på sikt komma att öka. De myndigheter som vi föreslår ska få uppgifter som rör internationell samverkan på säkerhetsskyddsområdet kan också komma att få en något ökad arbetsbelastning. Att med någon grad av tillförlitlighet förutsäga hur mycket arbetsbelastningen kan komma att förändras är dock omöjligt. Det hänger ihop bl.a. med vilket behov av stöd avseende säkerhetsskyddsavtal för enskilda som kan komma att uppstå hos de säkerhetsskyddsstödjande myndigheterna, vilken ambitionsnivå som den internationella samverkan kräver och vilken utveckling i övrigt den praktiska tillämpningen av säkerhetsskyddslagstiftningen leder till. En annan svårbedömd sak är i vilken omfattning informationssäkerheten kan ge ökade kostnader, särskilt med tanke på att huvuddelen av de verksamheter som i dag omfattas av säkerhetsskyddslagen redan bör ha uppfyllt kraven på tillgänglighet och riktighet, bl.a. på grund av andra regelverk och, för enskilda, även av kommersiella skäl. Dessutom är kostnaderna för it-utveckling i allmänhet höga och ökande varför en viss kostnadsökning med anledning av en ny säkerhetsskyddslag torde ha endast marginella effekter i sammanhanget.

Förslaget till ny säkerhetsskyddslag medför även positiva konsekvenser. Till dessa konsekvenser hör att det ges ett större utrymme att nyansera säkerhetsskyddet än i dag, vilket kan begränsa vissa kostnader, samt att enskilda får en större möjlighet att delta i internationell verksamhet där det ställs krav på säkerhetsintyg.

23.2 Vilka kostnadsmässiga och andra konsekvenser medför våra förslag?

Bedömning: Förslagen medför inte annat än marginella kostnadsökningar för vissa myndigheter som får delvis utökade uppgifter enligt våra förslag. Dessa kostnadsökningar bedöms kunna hanteras inom nuvarande budgetramar.

Förslagen bedöms inte medföra några kostnadsökningar för företag utom i de fall dessa på eget initiativ och för egen nytta begär s.k. säkerhetsintyg för leverantör, då kostnader kan uppkomma för vissa säkerhetsskyddsåtgärder.

Förslagen kan medföra att något fler personer säkerhetsprövas.

23.2.1 Kostnader och andra konsekvenser från ett generellt perspektiv

Internationella säkerhetsskyddsåtaganden

I kapitel 6 har vi beskrivit Sveriges folkrättsliga förpliktelser på säkerhetsskyddsområdet. Dessa kommer till uttryck dels i säkerhetsskyddsöverenskommelser som Sverige har träffat med andra stater och mellanfolkliga organisationer, dels genom förpliktelser som följer av Sveriges medlemskap i EU. Förpliktelserna omfattar främst ett skydd av vissa uppgifter som Sverige får från dessa stater och mellanfolkliga organisationer.

I förslaget till ny säkerhetsskyddslag inför vi en definition av säkerhetsskyddsklassificerad uppgift. Det är en uppgift som rör säkerhetskänslig verksamhet och som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha

omfattats av sekretess, om uppgiften förekommit i en verksamhet där bestämmelser om sekretess i offentlighets- och sekretesslagen gäller. Säkerhetsskyddsklassificerade uppgifter ersätter begreppet hemliga uppgifter i nuvarande lag. Genom kopplingen till säkerhetskänslig verksamhet omfattas uppgifter som antingen är av betydelse för Sveriges säkerhet eller omfattas av ett internationellt säkerhetsskyddsåtagande.

Förtydligandet innebär i realiteten inte någon förändring. En anledning till detta är att en inte oväsentlig delmängd av de uppgifter som omfattas av ett folkrättsligt åtagande om säkerhetsskydd dessutom är av betydelse för Sveriges säkerhet och således utgör hemliga uppgifter. Det innebär att uppgifterna ska ges ett skydd även enligt nuvarande lag. Många myndigheter, bl.a. inom försvarssektorn, där denna typ av uppgifter förekommer har infört interna bestämmelser som innebär att uppgifterna, även om de inte utgör hemliga uppgifter, ska ges ett skydd som motsvarar säkerhetsskydd. Detta sammantaget innebär att de aktuella uppgifterna, möjligen med något undantag, redan i dag har det skydd som föreskrivs i internationella säkerhetsskyddsåtaganden.

Under utredningen har flera av utredningens experter angivit att utvecklingen går mot att uppgifter som omfattas av dessa internationella åtaganden i allt större utsträckning hanteras av myndigheter som tidigare inte har hanterat sådana uppgifter. Det innebär att vårt förslag kan innebära att det på sikt behövs ett säkerhetsskydd i verksamheter där föreskrifter om skydd för denna typ av uppgifter har saknats. Det är dock svårt att göra någon närmare analys av en sådan tänkbar utveckling.

En utökad informationssäkerhet

Nuvarande säkerhetsskyddslag har fokus på skydd mot att hemliga uppgifter röjs, dvs. ett konfidentialitetsperspektiv. Sedan 1996 när säkerhetsskyddslagen trädde i kraft har utvecklingen på informationsområdet varit omfattande. I kapitel 9 beskriver vi hur informationssamhället har medfört ett ökat beroende av att information är tillgänglig och riktig för att vitala samhällsfunktioner ska kunna upprätthållas. Det är därför inte tillräckligt att säkerhetsskyddet ser till att uppgifter inte röjs för obehöriga utan säkerhetsskyddet

måste också tillgodose skyddet för de samhällsfunktioner som är beroende av att korrekt information finns tillgänglig när den behövs. Vi föreslår att informationssäkerheten utvidgas till att avse även riktighets- och tillgänglighetsaspekter på information och informationstillgångar som är nödvändiga för den säkerhetskänsliga verksamheten.

Detta synsätt är emellertid inte i sak något nytt. Stora delar av den samhällsviktiga verksamheten tillämpar, antingen frivilligt eller med stöd av föreskrifter från Myndigheten för samhällsskydd och beredskap, den internationella standarden för ledning av informationssäkerhet (LIS, SS-ISO/IEC 27 000-serien) i vilken dessa aspekter av informationen är omhändertagna. Under ett flertal år har brister i säkerheten i s.k. SCADA-system[2] uppmärksammats vilket har lett till förbättringsåtgärder inom flera sektorer. Samhällsviktiga it-system förekommer även i enskild verksamhet på en konkurrensutsatt marknad. Av kommersiella skäl finns det där starka incitament till en god informationssäkerhet. Vår bedömning är att det finns en stor vilja att i sådan verksamhet följa internationella standarder som t.ex. LIS. Detta sammantaget innebär att den förändring som vi föreslår träffar verksamheter där dessa tillkommande krav på informationssäkerheten redan bör vara omhändertagna.

Det kan dock inte uteslutas att vissa verksamheter påverkas av förslaget och att kostnader kan uppkomma för att uppfylla dessa krav – särskilt när det gäller befintliga system. Kostnader i samband med utveckling av it-system är i allmänhet relativt sett höga och utvecklingen går mot att dessa kostnader snarare ökar än minskar. Informationssäkerheten utgör endast en marginell del av dessa kostnader. Detta medför att vi med viss säkerhet kan bedöma att kostnaderna för en förändrad säkerhetsskyddslag i sammanhanget är betydelselösa.

[2] SCADA står för *Supervisory Control And Data Acquisition* och avser system för styrning och övervakning av bl.a. industriprocesser, energiproduktion och annan processövervakning.

I övrigt säkerhetskänslig verksamhet

Nuvarande säkerhetsskyddslag syftar till att ge ett skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet och skydd mot terroristbrott, även om brotten inte hotar rikets säkerhet.

Skyddet mot terrorism har i praktiken kommit att avse verksamhet vid i huvudsak skyddsobjekt och flygplatser och i synnerhet säkerhetsprövning av personal som tjänstgör på sådana platser.

Vi har i kapitel 11 redogjort för att det nuvarande tillägget om ett skydd mot terrorism inte, utan att någon ändring i sak är avsedd, behöver föras över till en ny säkerhetsskyddslag utan att terrorism som företeelse är ett av de antagonistiska hot som lagen ska skydda mot. Vi beskriver vidare i kapitel 12 att säkerhetsskyddslagen, utöver skydd av säkerhetsskyddsklassificerade uppgifter, ska inriktas mot verksamhet som av annan anledning behöver ett säkerhetsskydd. Det motsvarar delvis vad som i dag skyddas inom ramen för skydd mot terrorism, dvs. i huvudsak verksamhet vid skyddsobjekt, flygplatser och vissa verksamheter som ska skyddas enligt folkrättsliga åtaganden om luftfarts-, hamn- och sjöfartsskydd. Det skyddsvärda området bör dock inte avse enbart skyddsobjekt utan bör innefatta även annan säkerhetskänslig verksamhet, t.ex. verksamheter som innefattar hantering av it-system eller av sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle.

Även om den samhällsviktiga information som behandlats ovan är en betydande delmängd av den säkerhetskänsliga verksamheten, avses även verksamhet inom andra områden som om den störs kan få en stor negativ påverkan för Sverige. Sådana områden är vissa verksamheter som innefattar hantering av farliga ämnen som i fel händer kan orsaka förödande skadeverkningar för nationen. Transporter av kärnavfall och forskningsanläggningar inom kärnindustrin är exempel på verksamheter som kan omfattas. Annan sådan verksamhet är samhällets hantering av sprängämnen och ammunition som vid obehörig hantering kan medföra stor skada på viktiga samhällsfunktioner.

Liksom för informationssäkerheten finns det för de uppräknade verksamheterna redan i dag krav på skyddsåtgärder i annan regle-

ring. Vårt förslag till skyddsåtgärder för säkerhetskänslig verksamhet som inte rör informationssäkerhet blir därmed snarast att anse som ett samlat minimiskydd för de fall där krav i annan reglering inte fullt ut täcker den säkerhetskänsliga verksamheten. Av det skälet är det svårt att mer än gissa om förslaget får några betydande konsekvenser och i så fall i vilken omfattning. Vår bedömning är dock att förslaget inte kommer att medföra några större kostnader.

En något vidgad säkerhetsprövning

Säkerhetsprövningen i vårt förslag till ny lag utgår från nuvarande ordning där skälet till åtgärden är att bedöma en persons pålitlighet från säkerhetssynpunkt. Indelningen i tre säkerhetsklasser behålls där nivån på de säkerhetsskyddsklassificerade uppgifterna är en av grunderna för placering i säkerhetsklass. Den andra grunden för placering i säkerhetsklass, som innebär en nyhet i vårt förslag, baseras på vilken skada som kan åstadkommas i ett deltagande i säkerhetskänslig verksamhet. Den sistnämnda grunden innebär att nuvarande möjlighet till registerkontroll enligt 14 § säkerhetsskyddslagen som stöd för säkerhetsprövning till skydd mot terrorism inordnas i systemet med placering i säkerhetsklass. Enligt våra bedömningar kommer antalet säkerhetsprövningar som i dag görs enligt 14 § i huvudsak att motsvaras av de säkerhetsprövningar enligt den nya grunden, men en viss ökning kan bli aktuell eftersom bestämmelsen inte som i dag är begränsad till skyddsobjekt och flygplatser.

Ett deltagande ska placeras i säkerhetsklass även när ett krav på säkerhetsprövning följer av ett internationellt säkerhetsskyddsåtagande. Vilka krav på säkerhetsskydd som ställs i det internationella åtagandet, t.ex. i internationella åtaganden som rör luftfartsskydd och hamnsskydd, bör avgöra valet av säkerhetsklass, men normalt torde det vara den lägsta säkerhetsklassen (säkerhetsklass 3) som är aktuell.

De säkerhetsklassplaceringar som grundar sig på skyddet av säkerhetsskyddsklassificerade uppgifter förändras något. I vårt förslag avgör i huvudsak nivån på informationen placeringen och inte en kombination av nivå och omfattning som i nuvarande lag.

Detta skulle kunna medföra att något fler än i dag skulle komma att placeras i en högre säkerhetsklass. För att motverka denna effekt inför vi en viss flexibilitet som innebär en möjlighet till en lägre säkerhetsklassplacering, om uppgifterna på den högre nivån förekommer enbart i mindre omfattning. Detta bör leda till att skillnaden mot i dag blir liten.

Även när det gäller uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande föreslår vi en säkerhetsklassplacering som grundar sig på den nivå som informationen har klassificerats i. Det skulle kunna innebära att fler anställningar behöver placeras i en högre säkerhetsklass. Vår bedömning är dock att så inte behöver bli fallet. En konsekvens av den gällande ordningen i fråga om grunder för placering i säkerhetsklass är nämligen att översättningsproblematiken i dag kan leda till placering i en onödigt hög säkerhetsklass. Det utrymme för differentiering som fyra informationssäkerhetsklasser innebär medför goda förutsättningar för en väl avvägd skyddsnivå.

Ökningen av antalet säkerhetsklassplaceringar som grundar sig på ett internationellt säkerhetsskyddsåtagande kan därför bedömas bli något enstaka fall per år.

Vi föreslår att medborgarskapskravet i nuvarande säkerhetsskyddslag tas bort för anställningar hos staten som är placerade i säkerhetsklass. En konsekvens av detta förslag är att utländska medborgare kan komma i fråga för flera tjänster i statsförvaltningen. En sådan utveckling ligger väl i linje med Sveriges integrationspolitiska mål.[3]

Sammantaget är det rimligt att bedöma att antalet personer som kommer att placeras i säkerhetsklass och därmed säkerhetsprövas kommer att öka något.

Ett nyanserat säkerhetsskydd

I kapitel 15 har vi beskrivit hur säkerhetsskyddet när det gäller skydd av säkerhetsskyddsklassificerade uppgifter i vid bemärkelse ska indelas i fyra nivåer. Ett klassificeringssystem med fyra nivåer ger bättre förutsättningar att nyansera säkerhetsskyddet än vad

[3] Se bl.a. Regeringens skrivelse 2001/02:129 Integrationspolitik för 2000-talet.

nuvarande två nivåer medger. Det medför även att de myndigheter som i dag tillämpar två nivåer ges bättre möjligheter att undvika ett för högt säkerhetsskydd för framför allt utländska uppgifter på de lägre nivåerna. Ett klassificeringssystem som bygger på fyra nivåer kommer att medföra att en uppgift som i dag ges ett mer kostnadskrävande säkerhetsskydd än nödvändigt i vissa fall kan klassificeras på en lägre nivå och således omfattas av ett mindre kostsamt säkerhetsskydd.

Konsekvenserna av förslaget är dock svåra att bedöma. För myndigheterna inom försvarssektorn gäller detta i huvudsak redan till följd av Försvarsmaktens föreskrifter och interna bestämmelser vid dessa myndigheter. Vid dessa myndigheter torde effekten av förslaget bli försumbar. Besparingsmöjligheterna gäller därmed främst för de myndigheter som omfattas av Säkerhetspolisens föreskrifter om säkerhetsskydd. Det är dock omöjligt att bedöma hur stor denna besparing kan komma att bli.

Regleringen överensstämmer med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

En ny säkerhetsskyddslag påverkar inte Sveriges åtaganden som medlemsstat i EU.

23.2.2 Kostnader och konsekvenser specifikt för företag

Förslaget till ny säkerhetsskyddslag gäller för enskilda på samma sätt som nuvarande lag. När det gäller säkerhetsskyddsåtgärderna och kostnader som är förknippade med dessa har frågan redan behandlats under avsnittet om informationssäkerhet ovan.

För att förbättra möjligheterna för företag att delta i viss konkurrensutsatt verksamhet som anordnas av utländska myndigheter och mellanfolkliga organisationer föreslår vi att företag under vissa förutsättningar kan få s.k. säkerhetsintyg för leverantör (se vidare kapitel 20). Dessa intyg innebär att en myndighet har bedömt att säkerhetsskyddet vid ett företag uppfyller sådana krav att företaget kan hantera säkerhetsskyddsklassificerade uppgifter på en viss nivå. Intygen kan utfärdas efter det att den nationella industrisäkerhets-

myndigheten har träffat ett säkerhetsskyddsavtal med det aktuella företaget.

För de företag som behöver ett sådant intyg innebär förslaget en bättre möjlighet än i dag att delta i verksamhet för andra länder och mellanfolkliga organsationer där krav på sådana intyg har ställts upp.

Samtidigt innebär detta att det ställs krav på att leverantöreren har ett för ändamålet fullgott säkerhetsskydd. Eftersom ett säkerhetsskyddsavtal på denna grund bygger på frivillighet från företagets sida får leverantören i varje enskilt fall avgöra om kostnaderna för sådant säkerhetsskydd motsvarar nyttan av förväntade uppdrag som ett säkerhetsintyg kan medföra.

23.2.3 Organisatoriska frågor

Säkerhetsskyddsstödjande myndigheter

Vi föreslår i kapitel 21 att de uppgifter som i dag fullgörs av länsstyrelserna förs över till Myndigheten för samhällsskydd och beredskap samt även ansvaret för kommuner och landsting. För Myndigheten för samhällsskydd och beredskap innebär det en ökad arbetsbelastning, även om omfattningen av de uppgifter som länsstyrelserna har haft varit mycket begränsad. Vi bedömer att myndigheten har stora möjligheter att samordna arbetet med övriga uppgifter som myndigheten har när det gäller skydd för samhällsviktig verksamhet, varför de utökade uppgifterna bör kunna hanteras inom befintlig budgetram. Transportstyrelsen får ett något större ansvarsområde.

Rutiner kring säkerhetsskyddad upphandling

Säkerhetsskyddad upphandling med säkerhetsskyddsavtal innebär att krav på säkerhetsskydd ställs i kontraktsform på en anbudsgivare eller leverantör i en upphandlingssituation. Bestämmelserna om säkerhetsskyddsavtal behålls förslaget till ny säkerhetsskyddslag. I några avseenden kompletteras nu gällande bestämmelser. Konsekvenserna av detta beskrivs i det följande.

För det första föreslår vi att säkerhetsskyddsstödjande myndigheter ges möjlighet att för enskildas räkning träffa säkerhetsskyddsavtal med leverantörer till dessa. För det andra föreslår vi att Försvarets materielverk i rollen som nationell industrisäkerhetsmyndighet ska få träffa säkerhetsskyddsavtal med enskilda, om det behövs för att utfärda s.k. säkerhetsintyg för leverantör. Försvarets materielverks verksamhet med anledning av förslaget behandlas vidare i avsnittet om internationell samverkan nedan.

De säkerhetsskyddsstödjande myndigheterna föreslås få en ny uppgift, nämligen att träffa säkerhetsskyddsöverenskommelser med leverantörer till de bolag, föreningar och stiftelser som hör till den säkerhetsskyddsstödjande myndighetens verksamhetsområde. I dag är det inte formellt möjligt att träffa sådana avtal, och det finns därför inte någon statistik som stöd för hur omfattande denna uppgift kan komma att bli. Uppgiften kommer att ställa administrativa och personella krav på de säkerhetsskyddsstödjande myndigheterna. Troligtvis kommer dock detta, åtminstone initialt, inte att innebära några större ökningar avseende arbetsbelastning för de aktuella myndigheterna.

Internationell samverkan

De förslag till funktioner som redovisats i kapitel 20 när det gäller nationell säkerhetsmyndighet och nationell industrisäkerhetsmyndighet kräver resurser. Uppgifterna löses i dag av flera myndigheter och i regel av personal som även har andra arbetsuppgifter. Funktionerna är i dag otydligt formulerade och spridda mellan Utrikesdepartementet, Försvarsmakten, Försvarets materielverk och övriga myndigheter som i varierande omfattning stödjer arbetet. Det är därför svårt för att inte säga omöjligt att beräkna kostnaderna för verksamheten vilket även har varit en del av kritiken mot nuvarande ordning. Även om en sådan uppskattning vore möjlig, är det troligtvis så att dagens ambitionsnivå inte uppfyller samtliga krav för dessa uppgifter. Samtidigt kan möjligen en del arbetsuppgifter försvinna, t.ex. kan engagemanget i vissa arbetsgrupper minskas eller till och med upphöra helt, men denna fråga måste analyseras närmare av berörda myndigheter. Genom att lösningarna

i olika länder i vårt närområde skiljer sig åt är det även svårt att dra paralleller till resursåtgången i andra länder.

Vårt förslag innebär att Försvarsmakten ska ges uppgiften att vara nationell säkerhetsmyndighet innefattande nationell informationssäkringsmyndighet och nationell kryptogodkännande myndighet. Vid myndigheten utförs redan i dag åtskilliga sådana uppgifter och det finns redan den kompetens som behövs för uppdraget. Verksamheten kommer dock att behöva omorganiseras något och förstärkas med personal inom ramen för de föreslagna uppgifterna. Verksamheten kräver också utlandsresor och omkostnader för representation och lokaler. Till viss del är detta redan uppfyllt genom Försvarsmaktens nuvarande funktion som nationell säkerhetsmyndighet i bilaterala relationer och genom att i praktiken redan vara nationell kryptogodkännande myndighet. Myndighetens resurser för bl.a. samordning, säkerhetsprövning, itsäkerhetsfrågor och krypografiska funktioner kan behöva förstärkas något. Resursbehovet bör därför analyseras vidare av Försvarsmakten. I en myndighet av Försvarsmaktens storlek bör en formalisering (och viss utvidgning) av uppdraget kunna lösas inom given budgetram utan några resursförstärkningar.

Hur den nationella säkerhetsmyndigheten ska organiseras bör ankomma på Försvarsmakten att besluta efter samråd med Regeringskansliet och andra berörda myndigheter.

Vi föreslår att Säkerhetspolisen i vissa fall liksom hittills ska hantera ärenden som ankommer på den nationella säkerhetsmyndigheten. Det bör röra sig om ett begränsat antal ärenden per år som förvisso kan komma att öka något. Vid Säkerhetspolisen torde resursbehovet vara betydligt mindre än hos Försvarsmakten för att hantera dessa specifika ärenden. Även denna verksamhet bör kunna hanteras inom myndighetens budgetram.

Vid Försvarets materielverk finns i dag den kompetens som behövs för att myndigheten ska kunna ta rollen som nationell industrisäkerhetsmyndighet. Bemanningen är dock dimensionerad för i första hand nationella behov. Även för denna verksamhet krävs resurser för resor, representation och lokaler, men även resurser för att kunna genomföra utredningar om uppskattningsvis 5–7 företag per år samt för att träffa säkerhetsskyddsavtal med dessa inför utfärdande av säkerhetsintyg. Försvarets materielverk har redan i dag delvis denna uppgift och en organisation för att

hantera en viss utvidgning av uppdraget. Försvarets materielverk skiljer sig från Försvarsmakten och Säkerhetspolisen på ett sådant sätt att verksamheten är uppdragsfinansierad. Det talar för att myndighetens anslag höjs motsvarande den kostnadsökning som den föreslagna uppgiften innebär. En uppskattning av ett förväntat resursbehov torde vara 2–3 årsarbetstjänster, men resursbehovet bör analyseras av Försvarets materielverk. Vi återkommer till finansieringen av dessa tjänster nedan.

23.2.4 Behov av finansiering

Vår bedömning är att förslagen sammantagna inte medför en kostnadsökning som kräver särskild finansiering. De i sammanhanget smärre kostnader som kan uppstå vid vissa myndigheter har främst organisatoriska orsaker. I ett perspektiv av dessa myndigheters verksamhet i övrigt och säkerhetsskyddets relativt sett marginella förändring torde dessa kostnader kunna tas inom gällande budgetramar.

Förslaget att Försvarets materielverk ska pekas ut som nationell industrisäkerhetsmyndighet är ett särfall eftersom myndigheten är en så kallad tusenkronorsmyndighet. Den kostnadsökning som hänger samman med den föreslagna uppgiften bör finansieras genom att avgifter ta ut för säkerhetsintyg. Sådana avgifter är inte ovanliga i andra länder och i t.ex. Finland är avgiften för ett säkerhetsintyg för leverantör 10 000 euro. Avgiften uppges svara mot den faktiska kostnad som den behöriga säkerhetsmyndigheten har för att genomföra den utredning som behövs för att kunna utfärda ett intyg. Även säkerhetsintyg för person medför vissa kostnader för den som ska utfärda intyget. Som tidigare nämnts innebär intygen att en person eller ett företag kan få vissa anställningar och uppdrag där sådana intyg krävs vilket också medför att en kostnadstäckning genom en avgift för myndigheternas handläggning är rimlig.

23.3 Ikraftträdande och övergångsbestämmelser

Vi bedömer att en ny säkerhetsskyddslag och en ny säkerhetsskyddsförordning bör kunna träda i kraft den 1 januari 2017 och att nuvarande lag och förordning upphör att gälla vid samma tidpunkt.

För att minska framför allt de administrativa effekterna av en ny reglering föreslår vi övergångsbestämmelser i fråga om bl.a. märkning av hemliga uppgifter, innebörden av pågående deltagande i säkerhetsklass samt att säkerhetsskyddsklassificerade uppgifter under viss tid får lämnas ut till en utländsk myndighet eller mellanfolklig organisation utan hinder av att de inte omfattas av ett internationellt säkerhetsskyddsåtagande hos den mottagande myndigheten eller organisationen. Befintliga säkerhetsskyddsavtal påverkas inte av de nya bestämmelserna om ingående av sådana avtal.

24 Författningskommentar

24.1 Förslaget till säkerhetsskyddslag

1 kap. Lagens syfte och tillämpningsområde samt definitioner

Lagens syfte och tillämpningsområde

1 § Syftet med denna lag är att säkerställa säkerhetsskyddet för verksamheter hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet, eller som omfattas av ett för Sverige i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd.

Lagen ska även i övrigt ge stöd för internationell samverkan på säkerhetsskyddsområdet.

Paragrafen anger lagens syfte och tillämpningsområde. Den motsvarar delvis 1 § 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 11.2–11.3 och 14.1.

Av *första stycket* framgår att lagens huvudsakliga syfte är att säkerställa säkerhetsskyddet för verksamheter hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet, eller omfattas av ett för Sverige, i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd. Vad som avses med säkerhetsskydd framgår av 5 §. På samma sätt som 1996 års säkerhetsskyddslag är lagen direkt tillämplig vid verksamheter hos staten, kommuner, landsting och enskilda oberoende av verksamhetsform. I fråga om beskrivningen av lagens syfte finns två huvudsakliga förändringar i förhållande till 1996 års säkerhetsskyddslag. Dels har ordet ”rikets” ersatts med ”Sveriges”, dels har en kompletterande skrivning om för Sverige, i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtaganden om säkerhetsskydd införts. Förändringarna syftar till en tydligare och mer modern lagstiftning.

Användandet av uttrycket Sveriges säkerhet i stället för rikets säkerhet är i linje med de förändringar i 19 kap. brottsbalken som gjorts genom riksdagens beslut med anledning av prop. 2013/14:51 Förstärkt skydd mot främmande makts underrättelseverksamhet. Uttrycket tar således sikte på förhållanden av grundläggande betydelse för Sverige som möjligheterna att hävda landets oberoende i olika avseenden. Det innebär att lagens krav på säkerhetsskydd på samma sätt som tidigare gäller för såväl militär som civil verksamhet. Vilka verksamheter som är av betydelse för att upprätthålla Sveriges säkerhet måste bedömas i ljuset av samhällsutvecklingen. Vad som behöver skyddas för att förebygga hot mot Sveriges säkerhet kan därför i viss utsträckning variera över tiden.

Vidare anges att lagen ska tillämpas också när krav på säkerhetsskydd följer av för Sverige förpliktigande åtaganden gentemot andra stater och mellanfolkliga organisationer. Det är i första hand fråga om uppgifter som är säkerhetskänsliga för andra stater och mellanfolkliga organisationer och som Sverige genom säkerhetsskyddsöverenskommelser har åtagit sig att skydda. Sådana överenskommelser gäller i dag i förhållande till ett trettiotal stater och vissa mellanfolkliga organisationer, bl.a. Nato. En redogörelse för sådana internationella säkerhetsskyddsåtaganden finns i avsnitt 6.1. Bestämmelsen ger även stöd för säkerhetsskyddsåtgärder som följer av folkrättsliga förpliktelser i övrigt, bl.a. EU-rättsliga bestämmelser inom t.ex. luftfartsskyddsområdet.

Av paragrafens *andra stycke* framgår att lagen även i övrigt ska stödja internationell samverkan på säkerhetsskyddsområdet. Avsikten med tillägget är att tydliggöra att lagen innehåller bestämmelser om säkerhetsintyg för internationella ändamål som har ett något vidare tillämpningsområde än lagen i övrigt.

Definitioner

2 § Med *internationellt säkerhetsskyddsåtagande* avses ett för Sverige, i förhållande till annan stat eller mellanfolklig organisation, förpliktande åtagande om säkerhetsskydd.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Den innehåller en definition av *internationellt säkerhetsskyddsåtagande*.

Vad som avses framgår av kommentaren till 1 §. Övervägandena finns i avsnitt 11.3.

3 § Med *säkerhetskänslig verksamhet* avses sådan verksamhet hos staten, kommuner, landsting och enskilda som är av betydelse för Sveriges säkerhet eller omfattas av ett internationellt säkerhetsskyddsåtagande.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Den innehåller en definition av *säkerhetskänslig verksamhet*. Övervägandena finns i avsnitt 11.4.

Definitionen ger en ram för vilka verksamheter som omfattas av lagen. Den utgår från beskrivningen av lagens syfte i 1 § första stycket och omfattar således såväl verksamheter av betydelse för Sveriges säkerhet som verksamheter som, även om de inte samtidigt är av betydelse för Sveriges säkerhet, ska ha ett säkerhetsskydd till följd av ett internationellt säkerhetsskyddsåtagande. Innebörden är därmed vidare än den definition som finns i 4 § 3 1996 års säkerhetsskyddsförordning och som endast omfattar verksamhet av betydelse för rikets säkerhet.

4 § Med *säkerhetsskyddsklassificerad uppgift* avses en uppgift som rör säkerhetskänslig verksamhet och som av den anledningen omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess, om uppgiften i stället förekommit i en verksamhet där bestämmelser om sekretess i offentlighets- och sekretesslagen gäller.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Den innehåller en definition av *säkerhetsskyddsklassificerad uppgift* som delvis utgår från innehållet i 6 § 2 1996 års säkerhetsskyddslag och 4 § 1 1996 års säkerhetsskyddsförordning. Övervägandena finns i avsnitt 12.2.

Att definitionen utgår från uppgifter som rör säkerhetskänslig verksamhet innebär att den innefattar såväl uppgifter av betydelse för Sveriges säkerhet som uppgifter som ska ha ett säkerhetsskydd enligt internationella säkerhetsskyddsåtaganden, även om de inte samtidigt kan anses vara av betydelse för Sveriges säkerhet. Vidare klargörs att lagen inte uppställer något krav på att verksamheter för vilka lagen gäller också ska omfattas av bestämmelser om sekretess i offentlighets- och sekretesslagen (2009:400). Däremot förutsätts

att en säkerhetsskyddsklassificerad uppgift till sin natur är sådan att uppgiften materiellt sett kan hänföras till en bestämmelse om sekretess, med hänsyn till antingen Sveriges säkerhet eller Sveriges förbindelser med annan stat eller mellanfolklig organisation.

5 § Med *säkerhetsskydd* avses

1. skydd mot spionerі, sabotage, terroristbrott och andra brott som kan hota säkerhetskänslig verksamhet, samt
2. skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.

Paragrafen innehåller en definition av *säkerhetsskydd*. Övervägandena finns i avsnitt 11.5.

Bestämmelsens innehåll motsvarar, med de justeringar av lagens tillämpningsområde som följer av 1 §, i huvudsak 6 § 1996 års säkerhetsskyddslag.

2 kap. Allmänna bestämmelser om säkerhetsskydd

Säkerhetsskyddsåtgärder

1 § Säkerhetsskyddet ska särskilt genom

1. *informationssäkerhet* förebygga dels att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, dels skadlig inverkan på andra informationstillgångar som avser säkerhetskänslig verksamhet,
2. *fysisk säkerhet* förebygga dels att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där verksamhet som av annan anledning är säkerhetskänslig bedrivs, dels skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt, och
3. *personalsäkerhet* förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av annan anledning är säkerhetskänslig (*säkerhetsprövning*) samt säkerställa att de som deltar i säkerhetskänslig verksamhet har en tillräcklig kunskap om säkerhetsskydd (*utbildning i säkerhetsskydd*).

Paragrafen innehåller en beskrivning av säkerhetsskyddets inriktning och anger vad de olika säkerhetsskyddsåtgärderna syftar till. Övervägandena finns i avsnitt 15.1 samt 16.1 (informationssäkerhet), 17.1 (fysisk säkerhet) och 18.2 (personalsäkerhet).

Paragrafen motsvarar delvis 7 § och 30 § 1 1996 års säkerhetsskyddslag. Beskrivningen av det närmare syftet med de olika säkerhetsskyddsåtgärderna har dock vidareutvecklats för att tydligare ge uttryck för att säkerhetsskyddet tar sikte på mer än att enbart skydda uppgifter från ett konfidentialitetsperspektiv. Utgångspunkten för beskrivningen i fråga om de olika åtgärderna är den förändrade systematik för säkerhetsskyddslagen som behandlas i avsnitt 12.1.

Första punkten gäller informationssäkerhet. Åtgärden har ett vidare syfte än bestämmelsen om informationssäkerhet i 7 § 1 1996 års säkerhetsskyddslag. Tillämpningsområdet är utvidgat dels från hemliga uppgifter till säkerhetsskyddsklassificerade uppgifter (se kommentaren till 4 §), dels till att avse även ett skydd av andra informationstillgångar i säkerhetskänslig verksamhet. Med informationstillgång avses i detta sammanhang såväl uppgifter som tekniska system som används för att i olika avseenden elektroniskt kommunicera och i övrigt behandla uppgifter. Det andra ledet i bestämmelsen tar framför allt sikte på skyddsåtgärder för att tillgodose behov av tillgänglighet och riktighet i fråga om sådana itsystem som har en avgörande betydelse för att styra för Sverige viktiga samhällsfunktioner t.ex. inom el- och vattenförsörjning och sådana sammanställningar av uppgifter, t.ex. folkbokföringsregistret som är av grundläggande betydelse för ett fungerande samhälle.

Andra punkten gäller fysisk säkerhet. Åtgärden har ett vidare syfte än bestämmelsen om tillträdesbegränsning i 7 § 2 1996 års säkerhetsskyddslag. I fråga om att förebygga att obehöriga får tillträde har tydliggjorts att åtgärden avser inte bara platser utan också kan avse anläggningar av olika slag och objekt, t.ex. fordon. Även delar av t.ex. en anläggning innefattas. Vidare tydliggörs att åtgärden kan avse också ett skydd mot sådan skadlig inverkan som kan orsakas utan ett obehörigt tillträde. Det skulle exempelvis kunna röra sig om att kabel för samhällsviktig elektronisk kommunikation skyddas genom ett robust hölje eller larm.

Tredje punkten avser personalsäkerhet. Åtgärden har ett vidare syfte än bestämmelsen om säkerhetsprövning i 7 § 3 1996 års säkerhetsskyddslag genom att åtgärden också inkluderar utbildning i säkerhetsskydd. Vidare tydliggörs att säkerhetsprövning kan vara aktuell vid olika slag av verksamheter dels vid deltagande i verksam-

heter där tillgång ges till säkerhetsskyddsklassificerade uppgifter, dels i verksamheter som av annan anledning är säkerhetskänsliga.

Skyldigheter för den som är ansvarig för en säkerhetskänslig verksamhet

2 § Den som är ansvarig för en säkerhetskänslig verksamhet ska se till att

1. behovet av säkerhetsskydd utreds (*säkerhetsskyddsanalys*),

2. säkerhetsskyddsåtgärder enligt 1 § planeras och vidtas för att säkerställa det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter, samt i fråga om säkerhetsskyddsklassificerade uppgifter också är anpassat till uppgifternas informationssäkerhetsklass enligt 3 §,

3. säkerhetsskyddet kontrolleras, och

4. att sådan anmälnings- och upplysningsskyldighet som följer av förordning som har meddelats med stöd av denna lag fullgörs.

Så långt det är möjligt ska säkerhetsskyddsåtgärderna utformas så att de inte medför skada eller annan olägenhet för andra allmänna eller enskilda intressen.

Paragrafen anger huvudsakliga skyldigheter för den som är ansvarig för en säkerhetskänslig verksamhet. Vad som gäller för leverantörer som omfattas av ett säkerhetsskyddsavtal framgår av 4 §. Övervägandena finns i huvudsak i avsnitt 14.2 och 15.2–15.4.

Någon direkt motsvarighet till paragarafen finns inte i 1996 års säkerhetsskyddslag. Innehållet i bestämmelsen är dock i huvudsak hämtat från 1996 års säkerhetsskyddslag med tillhörande förordning (bl.a. 5 och 30 §§ 1996 års säkerhetsskyddslag).

Första punkten tar sikte på säkerhetsskyddsanalysens centrala funktion för verksamhetens säkerhetsskydd. Frågan om säkerhetsskyddsanalys behandlas i avsnitt 13.2.

Andra punkten behandlar behovet av ett väl avvägt och balanserat säkerhetsskydd där olika säkerhetsskyddsåtgärder samverkar med varandra. En liknande bestämmelse finns i 5 § 1996 års säkerhetsskyddslag. En nyhet är dock att det uttryckligen anges att säkerhetsskyddet i fråga om säkerhetsskyddsklassificerade uppgifter också ska anpassas efter uppgifternas informationssäkerhetsklass (se kommentaren till 3 §).

Tredje punkten tar sikte på behovet av intern kontroll. En motsvarande bestämmelse finns i 30 § 2 1996 års säkerhetsskyddslag.

Fjärde punkten avser att ge ett tydligare stöd för att i förordning närmare ange skyldighet för kommuner, landsting och enskilda att bl.a. till den myndighet som utövar tillsyn anmäla säkerhetshotande verksamhet. Överväganden om anmälnings- och upplysningsskyldighet av sådant slag finns i avsnitt 21.4.

Andra stycket innehåller en erinran om vikten av att utforma säkerhetsskyddet med beaktande av sådana till säkerhetsskyddet motstående intressen som skyddet av enskildas personliga integritet och effektivitetshänsyn.

Viktigt att notera är att lagen inte inskränker allmänhetens möjligheter att enligt offentlighetsprincipen ta del av allmänna handlingar. Frågan om sådana uppgifter kan lämnas ut prövas enligt bestämmelserna i offentlighets- och sekretesslagen (2009:400). Säkerhetsskydd kan dock innebära hanteringskrav för att bl.a. förebygga ett obehörigt röjande av uppgifter för vilka sekretess med hänsyn till Sveriges säkerhet gäller enligt offentlighets- och sekretesslagen.

Informationssäkerhetsklasser

3 § Säkerhetsskyddsklassificerade uppgifter ska utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet delas in i en informationssäkerhetsklass enligt följande

1. *Kvalificerat hemlig* vid en synnerligen allvarlig skada,
2. *Hemlig* vid en allvarlig skada,
3. *Konfidentiell* vid en inte obetydlig skada, eller
4. *Begränsad* vid en ringa skada.

Säkerhetsskyddsklassificerade uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande ska, om de inte redan av annan stat eller mellanfolklig organisation har klassificerats, på motsvarande sätt delas in en informationssäkerhetsklass enligt första stycket utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Den innehåller bestämmelser om indelning i nivåer av säkerhetsskyddsklassificerade uppgifter. Övervägandena finns i avsnitt 15.3.

Bestämmelsen är av central betydelse för bl.a. placering i säkerhetsklass vid säkerhetsprövning enligt lagens 3 kap. 4 §.

Första stycket föreskriver krav på indelning i fyra nivåer (kvalificerat hemlig, hemlig, konfidentiell eller begränsad) i fråga om säkerhetsskyddsklassificerade uppgifter som är av betydelse för Sveriges säkerhet. Indelningen ska göras utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Bedömningen ska göras endast som ett led i bestämmande av skyddsnivå för uppgiften och är således på intet sätt avgörande vid en prövning enligt offentlighets- och sekretesslagen om utlämnande av uppgift.

Andra stycket innehåller bestämmelser om en motsvarande nivåindelning av uppgifter som ska skyddas enligt internationella säkerhetsskyddsåtaganden. I regel är dock sådana uppgifter redan klassificerade på motsvarande sätt av den stat eller mellanfolkliga organisation från vilken uppgifterna härrör. En gjord klassificering ska då godtas och läggas till grund för bestämmande av skyddsnivå. I vissa internationella samarbeten förekommer det dock att en svensk myndighet upprättar handlingar som innehåller uppgifter som träffas av ett internationellt säkerhetsskyddsåtagande. Bestämmelsen tar sikte på sådana situationer. I dessa fall kan det bli aktuellt att göra en klassificering utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation. Det regelverk som är tillämpligt i det aktuella samarbetet kan utgöra ett stöd vid bedömningen.

Säkerhetsskyddsavtal

4 § Vid upphandling eller ingående av ett avtal avseende varor, tjänster eller byggentreprenader där det förekommer säkerhetsskyddsklassificerade uppgifter i informationssäkerhetsklassen konfidentiell eller däröver, eller som i övrigt avser säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, ska villkor anges i ett säkerhetsskyddsavtal för hur krav på säkerhetsskydd enligt 2 § ska tillgodoses av leverantören.

Den som ingått ett säkerhetsskyddsavtal med en leverantör ska också kontrollera att de angivna villkoren om säkerhetsskydd följs och se till att sådan anmälningsskyldighet som avses i 2 § första stycket 4 fullgörs.

Paragrafen innehåller bestämmelser om säkerhetsskyddsavtal vid upphandling och anbudsförfaranden. Övervägandena finns i avsnitt 19.1–19.3.

Bestämmelserna har ett vidare tillämpningsområde än motsvarande bestämmelser om säkerhetsskyddad upphandling i 8 § 1996 års säkerhetsskyddslag och ger också ett tydligare stöd för säkerhetsskyddsavtal när den upphandlande verksamheten är ett bolag, en förening eller en stiftelse som omfattas av säkerhetsskyddslagen. Med leverantör avses även anbudssökande och anbudsgivare. Ledning för tolkning av begreppet kan hämtas från upphandlingslagstiftningen.

Paragrafen reglerar i vilka fall av upphandling som villkor för säkerhetsskydd ska anges i ett säkerhetsskyddsavtal. Hänvisningen till 2 § innebär att säkerhetsskyddet inte får göras mindre långtgående än vad som följer av den bestämmelsen. Kravet på säkerhetsskyddsavtal omfattar inte upphandlingar som avser säkerhetsskyddsklassificerade uppgifter i den lägsta informationssäkerhetsklassen. En begränsning till verksamhet av motsvarande betydelse för Sveriges säkerhet finns också i fråga om upphandling i verksamhet som, utan att den innebär tillgång till säkerhetsskyddsklassificerade uppgifter, är att anse som säkerhetskänslig. Det kan t.ex. vara fråga om upphandling av it-system eller andra elektroniska kommunikationslösningar som avser för samhället vitala funktioner och som medför höga krav på tillgänglighet och riktighet. Ledning för vad som avses med *motsvarande betydelse* kan hämtas från 3 kap. 4 § första stycket 3 om placering av anställningar och annat deltagande i säkerhetsklass 3. Att krav inte ställs upp på säkerhetsskyddsavtal för alla upphandlingar vid säkerhetskänslig verksamhet innebär inget hinder mot att sådana avtal ändå ingås när det t.ex. gäller en upphandling där det förekommer säkerhetsskyddsklassificerade uppgifter i den lägsta informationssäkerhetsklassen.

I andra stycket erinras också om att den som ingått ett säkerhetsskyddsavtal med en anbudsgivare ska kontrollera det överenskomna säkerhetsskyddet och att viss anmälningsskyldighet fullgörs.

5 § Ett säkerhetsskyddsavtal enligt 4 § får, om det inte finns särskilda skäl, ingås endast av staten, kommuner eller landsting.

Om en upphandlande verksamhet i enlighet med första stycket inte själv får ingå ett säkerhetsskyddsavtal, ska en ansökan om ingående av säkerhetsskyddsavtal göras till den myndighet som regeringen bestämmer.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 19.1–19.3. I paragrafen regleras vem som får ingå ett säkerhetsskyddsavtal och anges hur en upphandlande verksamhet som inte på egen hand får ingå sådant avtal ska gå till väga för att få till stånd ett avtal.

Första stycket innebär att enskilda verksamheter som regel inte på egen hand får ingå ett säkerhetsskyddsavtal. Ordningen motsvaras och motiveras av den ordning som gäller för beslut om placering i säkerhetsklass enligt 3 kap. 5 § andra stycket. Säkerhetsskyddsavtal innebär i regel villkor om att personal hos leverantören ska vara placerade i säkerhetsklass. Beslut om sådan placering får fattas av enskilda endast om det föreligger särskilda skäl. Särskilda skäl för eget beslutsfattande har ansetts kunna föreligga i fråga om bolag där starka krav på oberoende gör sig gällande t.ex. i fråga om Sveriges Radio Aktiebolag. Sådana bolag bör på egen hand kunna ingå säkerhetsskyddsavtal.

Andra stycket innehåller en anvisning till upphandlande verksamheter som inte på egen hand får ingå ett säkerhetsskyddsavtal att ansöka hos den myndighet som regeringen bestämmer att ett sådant avtal ska träffas. Den ordningen avser att säkerställa att avtalet formellt ingås av den myndighet som beslutar om placering i säkerhetsklass för verksamheten i fråga.

Undantag från bestämmelser om säkerhetsskydd

6 § För riksdagen och dess myndigheter gäller endast bestämmelserna om informationssäkerhetsklasser, säkerhetsprövning och säkerhetsintyg. I övrigt gäller lagen (2006:128) om säkerhetsskydd för riksdagen och dess myndigheter.

Paragrafen anger i vilken utsträckning som lagen gäller för riksdagen och dess myndigheter och motsvarar i huvudsak 2 § 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 22.2.

För att riksdagen ska kunna tillämpa bestämmelserna om placering i säkerhetsklass behöver även bestämmelsen i 2 kap. 3 § om informationssäkerhetsklass gälla för riksdagen och dess myndigheter. I förhållande till vad som gäller i dag kommer således lagens tillämplighet i fråga om riksdagen och dess myndigheter att utvid-

gas något. Även den reglering som ger möjlighet till säkerhetsintyg för internationella behov bör gälla för riksdagen och dess myndigheter.

För att ange vad som i övrigt gäller i fråga om säkerhetsskydd för riksdagen och dess myndigheter har en upplysning om lagen (2006:128) om säkerhetsskydd för riksdagen och dess myndigheter lagts till.

7 § Regeringen får i fråga om Regeringskansliet förordna om undantag från andra bestämmelser i lagen än sådana som gäller informationssäkerhetsklasser, säkerhetsprövning och säkerhetsintyg.

Paragrafen innehåller ett bemyndigande för regeringen att i fråga om Regeringskansliet i viss utsträckning förordna om undantag från lagen och motsvarar i huvudsak 32 § 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 22.2. Undantagets räckvidd motsvarar vad som gäller för riksdagen och dess myndigheter enligt 6 §. Det innebär bl.a. att undantaget från registerkontroll justerats till säkerhetsprövning.

Särskilda bestämmelser om statsministerns tjänstebostäder

8 § I lagen (2014:514) om ansvar för vissa säkerhetsfrågor vid statsministerns tjänstebostäder finns särskilda bestämmelser om ansvar för fysisk säkerhet och om samrådsskyldighet inför att säkerhetsskyddsavtal ska träffas och inför beslut om placering i säkerhetsklass.

Paragrafen, som i sak motsvaras av 32 a § 1996 års säkerhetsskyddslag upplyser om att det finns särskilda bestämmelser om ansvar för fysisk säkerhet och om samrådsskyldighet inför att säkerhetsskyddsavtal ska träffas och inför beslut om placering i säkerhetsklass i lagen (2014:514) om ansvar för vissa säkerhetsfrågor vid statsministerns tjänstebostäder. I övrigt gäller säkerhetsskyddslagens bestämmelser även i verksamhet som bedrivs vid de aktuella fastigheterna.

En justering har gjorts så till vida att benämningen tillträdesbegränsning ändrats till fysisk säkerhet. Det är en följd av motsvarande ändring i 1 § 2.

9 § Bestämmelser om förbud mot tillträde till vissa byggnader, andra anläggningar, områden och andra objekt finns i skyddslagen (2010:305).

Paragrafen har efter viss språklig justering förts över från 10 § andra stycket 1996 års säkerhetsskyddslag. Den innehåller en hänvisning till de i förhållande till säkerhetsskyddslagen mer kvalificerade åtgärder i fråga om fysisk säkerhet som bestämmelser i skyddslagen (2010:305) gör möjliga. Övervägandena finns i avsnitt 17.2.

3 kap. Säkerhetsprövning

Vem som ska säkerhetsprövas

1 § Den som genom anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas. Säkerhetsprövning ska dock inte göras när det gäller

1. ledamöter av regeringen, av Europaparlamentet, av riksdagen eller av kommun- och landstingsfullmäktige, eller
2. andra uppdrag som offentliga försvarare eller ombud inför domstol än sådana som avser offentligt ombud enligt 27 kap. 27 § rättegångsbalken eller integritetsskyddsombud enligt 6 § lagen (2009:966) om Försvarsunderrättelsedomstol.

Paragrafen anger krav på säkerhetsprövning när en person genom anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet. Från kravet på sådan prövning undantas bl.a. riksdagsledamöter. I huvudsak motsvarande bestämmelser finns i 11 och 13 §§ 1996 års säkerhetsskyddslag. Undantagen har dock tidigare avsett endast registerkontroll. De särskilda skäl som i förarbetena till 1996 års lag har redovisats för undantagen motiverar att undantagen utsträcks till att avse säkerhetsprövning. Vidare har i första punkten förtydligats vilka grupper som omfattas av undantaget. Undantaget från kravet på säkerhetsprövning enligt denna paragraf hindrar inte att ett säkerhetsintyg enligt 4 kap. 2 § utfärdas för att underlätta internationell samverkan. Vidare gäller undantaget endast när sådana funktioner som anges i paragrafen utövas. Om t.ex. en person som är ledamot av riksdagen i någon annan egen-

skap deltar i säkerhetskänslig verksamhet, ska personen säkerhetsprövas.

Säkerhetsprövningens syfte och dess innehåll

2 § Säkerhetsprövningen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas i denna lag och i övrigt pålitlig från säkerhetssynpunkt. Vid säkerhetsprövningen ska beaktas sådana omständigheter som kan antas innebära sårbarheter i säkerhetshänseende.

I paragrafen anges vad säkerhetsprövningen syftar till att klarlägga. I huvudsak har bestämmelsen överförts från 11 § första stycket 2 1996 års säkerhetsskyddslag. Bestämmelsen har dock gjorts tydligare på så sätt att det anges att omständigheter som kan innebära sårbarheter i säkerhetshänseende hos den person som prövningen avser ska beaktas. Övervägandena finns i avsnitt 18.4.

3 § En inledande säkerhetsprövning ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas. Prövningen ska innefatta en grundutredning samt registerkontroll och särskild personutredning i den omfattning som anges i 6, 7 och 10 §§. Om det finns särskilda skäl, får den inledande säkerhetsprövningen göras mindre omfattande.

Säkerhetsprövningen ska därefter följas upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.

I paragrafen finns bestämmelser om när säkerhetsprövning ska göras och vilka huvudsakliga moment prövningen består av. Övervägandena finns i avsnitt 18.4. Bestämmelserna, som i sak delvis motsvarar 11 § 1996 års säkerhetsskyddslag, har utformats i syfte att tydliggöra dels att kravet på säkerhetsprövning kan aktualiseras inte bara vid ett anställningstillfälle eller liknande, utan också när t.ex. ändrade arbetsuppgifter innebär deltagande i säkerhetskänslig verksamhet, dels att säkerhetsprövning är en åtgärd som innebär ett uppföljningsansvar under hela den tid deltagandet i den säkerhetskänsliga verksamheten pågår. Bestämmelsen kompletteras av 14 § om bedömning vid säkerhetsprövning.

I *första stycket* har uttrycket *grundutredning* lagts till för att understryka att säkerhetsprövningen förutsätter en mer allsidig personkännedom än den som en registerkontroll kan ge. Med

grundutredning avses uppgifter om personliga förhållanden av betydelse för säkerhetsprövningen. Utredningen kan innebära kontroll av betyg, intyg och referenser samt att uppgifter från den som kontrollen avser hämtas in, t.ex. genom en intervju eller genom ett frågeformulär. Omfattningen av grundutredningen och utförandet av den bör anpassas till vilket slag av deltagande i säkerhetskänslig verksamhet det är fråga om. En grundutredning bör alltid ha gjorts innan en registerkontroll kan komma i fråga, men utredningen kan också behöva kompletteras om uppgifter lämnas ut efter registerkontroll. Om det mot bakgrund av vad som kommit fram vid grundutredningen står klart att det är olämpligt att den som prövningen avser deltar i den säkerhetskänsliga verksamheten, ska inte någon ansökan om registerkontroll göras.

I första stycket anges också att, om det finns särskilda skäl, den inledande säkerhetsprövningen får göras mindre omfattande. Bestämmelsen motsvaras närmast av det undantag från registerkontroll som finns i 16 § 1996 års säkerhetsskyddslag. Särskilda skäl bör kunna föreligga om den som prövningen avser redan tidigare har prövats på motsvarande sätt och ytterligare utredning därför inte bedöms kunna tillföra något nytt i sak. Ett undantag bör dock inte kunna avse registerkontrollmomentet i dess helhet eftersom den kontrollen innebär att också uppgifter som tillförs registren efter den inledande säkerhetsprövningen kan komma att lämnas ut för säkerhetsprövning (se 7 § andra stycket).

Andra stycket saknar direkt motsvarighet i 1996 års säkerhetsskyddslag och innehåller bestämmelser om uppföljande säkerhetsprövning. Bestämmelsen innebär krav på att den inledande säkerhetsprövningen, som föranleder en bedömning enligt 14 §, följs upp. Det innebär ett förtydligande om att säkerhetsprövning är en åtgärd som ska fortgå så länge deltagandet i den säkerhetskänsliga verksamheten pågår. Ett avslutningssamtal kan vara en viktig del av säkerhetsprövningen. Krav på uppföljning innebär bl.a. att uppgifterna i grundutredningen ska hållas uppdaterade. Att registerkontrollen pågår genom en bevakning förtydligas också särskilt i 7 § andra stycket.

Säkerhetsklasser

4 § En anställning eller ett annat deltagande i säkerhetskänslig verksamhet ska placeras i säkerhetsklass enligt följande.

1. *Säkerhetsklass 1,* om den anställde eller den som på annat sätt deltar i verksamheten i en omfattning som inte är ringa får del av uppgifter i informationssäkerhetsklassen kvalificerat hemlig, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka synnerligen allvarlig skada för Sveriges säkerhet.

2. *Säkerhetsklass 2,* om den anställde eller den som på annat sätt deltar i verksamheten i en omfattning som inte är ringa får del av uppgifter i informationssäkerhetsklassen hemlig eller i ringa omfattning får del av uppgifter i informationssäkerhetsklassen kvalificerat hemlig, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka allvarlig skada för Sveriges säkerhet.

3. *Säkerhetsklass 3,* om den anställde eller den som på annat sätt deltar i verksamheten får del av uppgifter i informationssäkerhetsklassen konfidentiell eller i ringa omfattning får del av uppgifter i informationssäkerhetsklassen hemlig, eller på annat sätt till följd av sitt deltagande i verksamheten har möjlighet att orsaka en inte obetydlig skada för Sveriges säkerhet.

En anställning eller ett annat deltagande i säkerhetskänslig verksamhet ska också i andra fall än sådana som följer av första stycket placeras i en säkerhetsklass som motsvarar de krav på säkerhetsprövning som följer av ett internationellt säkerhetsskyddsåtagande.

En anställning eller ett annat deltagande får placeras i säkerhetsklass endast om behovet av säkerhetsskydd inte kan tillgodoses på annat sätt.

I paragrafen finns bestämmelser om placering av anställningar eller annat deltagande i säkerhetskänslig verksamhet i säkerhetsklass. Övervägandena finns i avsnitt 18.5, 18.6 och 18.8.

I *första stycket* anges grunderna för indelning i säkerhetsklass som i flera avseenden avviker från motsvarande bestämmelser om säkerhetsklasser i 17 § 1996 års säkerhetsskyddslag. Tillämpningsområdet är vidare dels genom övergången från hemliga uppgifter till säkerhetsskyddsklassificerade uppgifter, dels genom att en alternativ grund införs för placering i säkerhetsklass som delvis motsvarar säkerhetsprövning med registerkontroll enligt 14 § 1996 års säkerhetsskyddslag (skydd mot terrorism). I fråga om säkerhetsskyddsklassificerade uppgifter utgår bestämmelserna från den fyrgradiga indelning i informationssäkerhetsklasser som ska göras

enligt 2 kap. 3 §. Den lägsta informationssäkerhetsklassen föranleder dock inte placering i säkerhetsklass.

I *andra stycket* finns en bestämmelse som anger att en anställning eller ett annat deltagande i säkerhetskänslig verksamhet också i andra fall än sådana som följer av första stycket ska placeras i en säkerhetsklass som motsvarar de krav på säkerhetsprövning som följer av ett internationellt säkerhetsskyddsåtagande. Bestämmelsen bedöms ha ett begränsat tillämpningsområde. Avsikten med bestämmelsen, är att fullt ut kunna tillgodose bl.a. krav på säkerhetsskydd som följer av internationella konventioner och EU-rätten inom områdena luftfartsskydd, hamnskydd och sjöfartsskydd. I fråga om verksamhet som innebär hantering av säkerhetsskyddsklassificerade uppgifter är regleringen i första stycket uttömmande. Den alternativa grunden för placering i säkerhetsklass enligt första stycket förutsätter en bedömning att deltagandet i verksamheten är av sådan art att det finns en möjlighet att orsaka en varierande grad av skada för Sveriges säkerhet. Om deltagandet inte bedöms kunna orsaka skada för Sveriges säkerhet av det slag som förutsätts i första stycket, innebär bestämmelsen i andra stycket att deltagandet ändå ska placeras i säkerhetsklass om krav på säkerhetsprövning följer av ett internationellt säkerhetsskyddsåtagande.

Tredje stycket innehåller en erinran om att en anställning eller ett annat deltagande i säkerhetskänslig verksamhet får placeras i säkerhetsklass endast om behovet av säkerhetsskydd inte kan tillgodoses på annat sätt.

Vem som beslutar om placering i säkerhetsklass

5 § Riksdagen och dess myndigheter beslutar om placering i säkerhetsklass såvitt avser riksdagens förvaltningsområde.

I övrigt beslutar regeringen om placering i säkerhetsklass. Regeringen får föreskriva att myndigheter och andra för vilka bestämmelserna om säkerhetsprövning gäller beslutar om placering i säkerhetsklass. Denna beslutanderätt får tilldelas enskilda endast om det finns särskilda skäl.

I paragrafen finns den grundläggande regleringen om vem som beslutar om placering i säkerhetsklass. Övervägandena finns i avsnitt 18.10. Bestämmelsen motsvarar i sak 20 § 1996 års säkerhetsskyddslag. Viss reglering som avsåg för riksdagen och dess myndig-

heter interna angelägenheter har dock utgått. En skillnad är vidare att bestämmelsen endast avser beslut om placering i säkerhetsklass. I princip all registerkontroll enligt lagen ska föregås av ett beslut om placering i säkerhetsklass. Att en registerkontroll ska göras vid sådan placering följer av 7 § varför ett särskilt beslut om registerkontroll inte behövs. I den till lagen hörande förordningen regleras på ansökan av vem som Säkerhetspolisen ska utföra registerkontroll. Av den regleringen framgår att huvudregeln är att sådan ansökan till Säkerhetspolisen endast görs av myndigheter och andra till vilka regeringen delegerat rätten att besluta om placering i säkerhetsklass.

Registerkontroll

6 § Med registerkontroll avses i denna lag att uppgifter i den omfattning som följer av 12 § hämtas från register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller lagen (2010:362) om polisens allmänna spaningsregister. Med registerkontroll avses också att uppgifter som behandlas med stöd av polisdatalagen (2010:361) hämtas in.

Paragrafen motsvarar 12 § 1996 års säkerhetsskyddslag. Mindre redaktionella ändringar har gjorts. Någon ändring i sak är inte avsedd.

7 § Registerkontroll ska göras om anställningen eller deltagandet i verksamheten har placerats i säkerhetsklass.

Vid registerkontroll enligt första stycket ska också uppgifter enligt 6 § löpande hämtas in under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.

Paragrafen som anger när registerkontroll ska göras motsvarar delvis 13 § 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 18.4.

Första stycket motsvarar 13 § första stycket 1996 års säkerhetsskyddslag. Vissa redaktionella ändringar har gjorts i syfte att förenkla bestämmelsen. Någon ändring i sak är inte avsedd.

Av *andra stycket* framgår det förhållandet att registerkontollen i praktiken innebär en kontinuerlig bevakning av tillkommande upp-

gifter (s.k. spontanutfall). Någon motsvarande bestämmelse finns inte i 1996 års säkerhetsskyddslag utan stödet för förfarandet finns i förordningen till 1996 års säkerhetsskyddslag (29 § andra stycket 1996 års säkerhetsskyddsförordning).

8 § Om det finns särskilda skäl, får registerkontroll av någon som ska delta i en säkerhetskänslig verksamhet göras utan föregående placering i säkerhetsklass. Föreskrifter om detta meddelas av regeringen, utom såvitt gäller riksdagen och dess myndigheter.

Paragrafen innehåller ett bemyndigande för regeringen i fråga om registerkontroll i annat fall än vid placering i säkerhetsklass. Övervägandena finns i avsnitt 18.6. Bestämmelsen saknar direkt motsvarighet i 1996 års säkerhetsskyddslag. I sak motsvaras dock bestämmelsen delvis av 14 § 1996 års säkerhetsskyddslag (skydd mot terrorism) som innebär registerkontroll utan placering i säkerhetsklass. Bestämmelserna i 4 § om placering i säkerhetsklass medför dock att i princip all registerkontroll enligt den tidigare bestämmelsen om skydd mot terrorism inordnas i det systemet. I fråga om verksamhet av tillfällig karaktär i samband med statsbesök, vissa internationella konferenser och liknande bör dock på samma sätt som enligt 14 § 1996 års säkerhetsskyddslag finnas ett utrymme för regeringen att föreskriva om registerkontroll (jfr. 26 a § 1996 års säkerhetsskyddsförordning).

9 § Bestämmelser om registerkontroll finns också i 4 kap. om internationell säkerhetsskyddssamverkan och säkerhetsintyg.

Paragrafen som endast är av upplysande slag saknar motsvarighet i 1996 års säkerhetsskyddslag. Den innehåller en hänvisning till de möjligheter att besluta om registerkontroll som följer av bestämmelserna om bl.a. säkerhetsintyg för internationella behov i 4 kap.

Särskild personutredning

10 § En särskild personutredning ska göras vid registerkontroll som avser anställning eller annat deltagande i verksamhet, om anställningen eller deltagandet i verksamheten har placerats i säkerhetsklass 1 eller 2. Utred-

ningen ska omfatta en undersökning av den kontrollerades ekonomiska förhållanden. I övrigt ska utredningen ha den omfattning som behövs.

Paragrafen motsvarar i stort 18 § 1996 års säkerhetsskyddslag. Den del av bestämmelsen som handlar om kontroll efter ansökan från annan stat eller mellanfolklig organisation har dock flyttats till 4 kap. 5 §. I övrigt har vissa mindre redaktionella ändringar gjorts. Någon ändring i sak är inte avsedd.

Krav på samtycke

11 § Registerkontroll och särskild personutredning får göras endast om den som säkerhetsprövningen gäller har lämnat sitt samtycke. Samtycket ska anses gälla också kontroller och utredningar under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår.

Paragrafen motsvarar i huvudsak 19 § 1996 års säkerhetsskyddslag. Vissa redaktionella ändringar har gjorts. Någon ändring i sak är inte avsedd.

Bestämmelsen innebär att ett lämnat samtycke gäller också kontroller och utredningar som görs efter den inledande säkerhetsprövningen. Den som hämtar in samtycket bör klargöra detta förhållande för den som säkerhetsprövningen gäller.

Utlämnande av uppgifter

12 § Säkerhets- och integritetsskyddsnämnden beslutar om uppgifter som kommit fram vid registerkontroll och särskild personutredning ska lämnas ut för säkerhetsprövning. Utlämnande av uppgifter får omfatta

1. för säkerhetsklass 1 eller 2: uppgifter om den kontrollerade som finns i något av de register som anges i 6 § eller som behandlas med stöd av polisdatalagen (2010:361). Om det är oundgängligen nödvändigt, får också motsvarande uppgifter om den kontrollerades make eller sambo lämnas ut, eller
2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret och misstankeregistret samt uppgifter som behandlas hos Säkerhetspolisen med stöd av polisdatalagen.

Om det finns synnerliga skäl, får utlämnandet omfatta även andra uppgifter än sådana som avses i första stycket.

En uppgift som har kommit fram vid registerkontroll eller särskild personutredning får lämnas ut för säkerhetsprövning endast om den i det enskilda fallet kan antas ha betydelse för prövningen av den kontrollerades pålitlighet från säkerhetssynpunkt.

Innehållet i paragrafen har förts över från 21 och 23 §§ 1996 års säkerhetsskyddslag samt 31 § 1996 års säkerhetsskyddsförordning. Redaktionella ändringar har gjorts. Vidare betonas särskilt att bedömningen ska gälla den aktuella anställningen eller motsvarande. Övervägandena finns i avsnitt 18.9.

13 § Innan en uppgift lämnas ut för säkerhetsprövning ska den som uppgiften avser ges tillfälle att yttra sig över uppgiften. Detta gäller dock inte om uppgiften omfattas av sekretess i förhållande till den enskilde enligt någon annan bestämmelse i offentlighets- och sekretesslagen (2009:400) än 35 kap. 3 §.

Även om uppgiften omfattas av sådan sekretess, ska den som uppgiften avser ges tillfälle att yttra sig innan uppgiften lämnas ut, om hans eller hennes intresse av att få yttra sig skäligen bör ha företräde framför det intresse som sekretessen ska skydda.

Paragrafen har förts över från 25 § 1996 års säkerhetsskyddslag. Vissa redaktionella ändringar har gjorts. Någon ändring i sak är inte avsedd.

Bedömning vid säkerhetsprövning

14 § Säkerhetsprövningen innebär en bedömning enligt 2 § av en persons lämplighet för att delta i en säkerhetskänslig verksamhet. Bedömningen ska utgå från uppgifter som kommit fram vid genomförandet av grundutredningen och den kännedom som i övrigt finns om den som ska prövas, uppgifter som har lämnats ut efter registerkontroll och särskild personutredning, arten av den verksamhet för vilken prövningen görs samt omständigheterna i övrigt.

Bedömningen görs av den som beslutar om anställning eller annat deltagande i den säkerhetskänsliga verksamheten. Har någon annan ett avgörande bestämmande över den prövades lämplighet att delta i den säkerhetskänsliga verksamheten, gör dock denne den slutliga bedömningen.

Om det finns anledning till det, ska en tidigare gjord bedömning avseende en persons lämplighet för att delta i den säkerhetskänsliga verksamheten omprövas.

Innehållet i paragrafen är delvis nytt. Delar av innehållet har dock hämtats från 27 § 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 18.4 och 18.11.

I *första stycket* klargörs inledningsvis att säkerhetsprövningen innebär en bedömning enligt 2 § av en persons lämplighet för att delta i en säkerhetskänslig verksamhet. Därefter anges vad bedömningen ska grundas på. Innehållet i den delen överensstämmer i stort med motsvarande bestämmelse i 27 § 1996 års säkerhetsskyddslag. Innehållet har dock utvecklats något.

Innehållet i *andra stycket* är nytt men motsvarar delvis 27 § 1996 års säkerhetsskyddslag. Bestämmelsen tydliggör att bedömningen görs av den som beslutar om anställning eller annat deltagande i den säkerhetskänsliga verksamheten. I det avseendet kan bestämmelsen för vissa verksamheter innebära en ändring i sak för det fall att arbetsgivaren inte själv beslutar om säkerhetsklass och därigenom bestämmer om registerkontroll (jfr 27 § 1996 års säkerhetsskyddslag).

Av det sista ledet i stycket följer dock att det sistnämnda inte gäller om någon annan har ett avgörande bestämmande över den prövades lämplighet att delta i den säkerhetskänsliga verksamheten. I vissa fall förutsätts nämligen att den slutliga bedömningen i fråga om deltagandet i säkerhetskänslig verksamhet görs av en myndighet eller annat offentligt organ. Det gäller bl.a. i fråga om verksamheter vid flygplatser där det följer av internationella konventioner om luftfartsskydd att t.ex. ett tillträde till vissa säkerhetsområden som ska finnas på en flygplats förutsätter en godkänd registerkontroll. I dessa fall genomförs säkerhetsprövningen i regel på så sätt att den som beslutar om anställningen ansvarar för grundutredningen och utifrån den gör en första bedömning. Om den prövade bedöms vara pålitlig, begärs sedan att den ansvariga myndigheten (Transportstyrelsen) går vidare i ärendet med en registerkontroll. För det fall att uppgifter efter sådan kontroll lämnas ut till myndigheten, bestämmer myndigheten om den som kontrollen avser ska få delta i verksamheten. På grundval av myndighetens beslut kan sedan ett behörighetsbevis i enlighet med internationella

regelverk utfärdas. Motsvarande ordning kan gälla på andra områden t.ex. hamnskydd, sjöfartsskydd och strålskydd. Också när det gäller säkerhetsskyddad upphandling innebär avtalet i regel en liknande uppdelning av ansvar för säkerhetsprövningen. På samma sätt som i övrigt gäller för säkerhetsprövningen bör i regel eventuella uppgifter som kommer fram vid en registerkontroll bedömas utifrån vad som i övrigt kommit fram under säkerhetsprövningen och utifrån vad arbetsuppgifterna innebär. Samrådsskyldigheten, som liksom i dag bör framgå av förordning, bör därför innebära ett krav samråd om inte särskilda skäl talar emot sådant samråd.

I *tredje stycket* förtydligas att en tidigare gjord bedömning avseende en persons lämplighet för att delta i den säkerhetskänsliga verksamheten ska omprövas om det finns anledning till det.

4 kap. Internationell säkerhetsskyddssamverkan och säkerhetsintyg

Nationell säkerhetsmyndighet

1 § Den som regeringen bestämmer ska fullgöra uppgiften som nationell säkerhetsmyndighet och nationell industrisäkerhetsmyndighet i enlighet med internationella säkerhetsskyddsåtaganden.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 20.3.

Bestämmelsen utgår från att det enligt olika internationella säkerhetsskyddsåtaganden förutsätts att Sverige anger funktioner för fullgörandet av uppgifter som enligt åtagandena ankommer på en nationell säkerhetsmyndighet och en nationell industrisäkerhetsmyndighet. Bestämmelsen upplyser om att regeringen bestämmer vilka myndigheter som ska fullgöra dessa funktioner. Bestämmelsen är således endast av upplysande karaktär. En upplysning om sådana nationella funktioner i fråga om säkerhetsskydd bör finnas i lagen för att göra kapitlets bestämmelser om bl.a. säkerhetsintyg begripliga. I 7 § anges behörighet att besluta om registerkontroll och utfärda intyg i ärenden enligt 2 och 5 §§ för den nationella säkerhetsskyddsmyndigheten och den nationella industrisäkerhetsmyndigheten.

Säkerhetsintyg

2 § Ett säkerhetsintyg får utfärdas för personer och leverantörer när en annan stat eller mellanfolklig organisation ansökt om sådant underlag, om

1. behov av sådant intyg finns vid internationell samverkan avseende säkerhetskänslig verksamhet enligt denna lag, eller

2. intyget, utöver vad som följer av punkten 1, kan underlätta för en person som har hemvist i Sverige eller för en leverantör med säte i Sverige att delta i en verksamhet som en annan stat eller en mellanfolklig organisation bedömer vara i behov av säkerhetsskydd.

Ett intyg enligt första stycket får utfärdas endast om deltagandet avser verksamhet i eller för en stat eller mellanfolklig organisation som omfattas av ett internationellt säkerhetsskyddsåtagande. Om det finns särskilda skäl, får regeringen besluta om undantag från kravet på ett internationellt säkerhetsskyddsåtagande.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 20.4.1–20.4.3.

Bestämmelsen i *första stycket* omfattar två huvudsakliga situationer. I den första situationen förutsätts en internationell samverkan mellan Sverige och en annan stat eller mellanfolklig organisation som rör säkerhetskänslig verksamhet. I den andra situationen får ett intyg utfärdas för att tillgodose behovet av att underlätta för en person eller leverantör att kunna delta i det som i en annan stat eller mellanfolklig organisation motsvarar säkerhetskänslig verksamhet. I den sistnämnda situationen behöver deltagandet inte vara inom ramen för ett internationellt samarbete som Sverige deltar i.

I *andra stycket* anges att för båda situationerna gäller att den ifrågavarande staten eller organisationen ska omfattas av ett internationellt säkerhetsskyddsåtagande. Skälet till detta krav är att Sverige av reciprocitetsskäl måste godta ett motsvarande intyg från den andra parten. Regeringen får besluta om undantag från detta krav om det finns särskilda skäl. Sådana skäl torde enbart vara aktuella för intyg enligt den första punkten, t.ex. i internationella samarbeten där ett internationellt säkerhetsskyddsåtagande ännu inte har trätt i kraft men där det finns ett behov av att delge säkerhetsskyddsklassificerade uppgifter mellan parterna.

3 § En säkerhetsprövning som innefattar registerkontroll enligt 3 kap. 6 § får göras, om det behövs för att ett säkerhetsintyg ska kunna utfärdas. Vid

sådan registerkontroll får också en särskild personutredning enligt 3 kap. 10 § göras.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 20.4.2 och 20.4.3. Huvuddelen av de personer som kan komma i fråga för intyg enligt 2 § kommer redan att vara placerade i säkerhetsklass. Intyget kan då utfärdas på den grunden utan att någon ytterligare utredning behöver göras. Bestämmelsen i denna paragraf tar sikte på det fåtal fall när en tidigare säkerhetsprövning saknas. I dessa fall görs ingen placering i säkerhetsklass och därför behövs en möjlighet till registerkontroll inom ramen för den säkerhetsprövning som görs för att kunna utfärda ett intyg.

4 § Vid ärenden om säkerhetsintyg gäller bestämmelserna om säkerhetsprövning i 3 kap. 2, 6, 10–13 §§ samt 14 § första stycket.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 20.4.1–20.4.3. Bestämmelsen kompletterar 3 § på ett sådant sätt att det förtydligas att det som normalt gäller för säkerhetsprövning enligt 3 kap. även i tillämpliga delar gäller säkerhetsprövning som görs i syfte att kunna utfärda ett säkerhetsintyg. Säkerhetsprövning enligt 3 § måste dock anpassas till att det endast är fråga om en inledande säkerhetsprövning. Den för vars verksamhet intyget utfärdas övertar det kontinuerliga säkerhetsprövningsansvaret i enlighet med de bestämmelser som gäller där verksamheten bedrivs.

Registerkontroll på ansökan av en annan stat eller mellanfolklig organisation

5 § Registerkontroll enligt 3 kap. 6 § får göras när en annan stat eller mellanfolklig organisation ansökt om sådant underlag, om

1. den person som ansökan gäller har eller har haft hemvist i Sverige, och
2. personen genom anställning eller på annat sätt ska delta i en verksamhet där det för deltagandet gäller regler om registerkontroll vid säkerhetsprövning som motsvarar reglerna i denna lag.

Vid registerkontroll enligt första stycket får också en särskild personutredning enligt 3 kap. 10 § göras.

Paragrafen motsvarar närmast 15 § 1996 års säkerhetsskyddslag. En till bestämmelsen korresponderande sekretessbrytande bestämmelse finns i 5 kap. 3 §. Övervägandena finns i avsnitt 20.4.4.

Första stycket utgår i stort från motsvarande bestämmelse i 15 § första stycket 1996 års säkerhetsskyddslag. Vissa redaktionella ändringar har dock gjorts. Bestämmelsen är ett komplement till regleringen om säkerhetsintyg enligt 2–4 §§. Den tar sikte på det förhållandet att en person med anknytning till Sverige ska genomgå något som motsvarar en säkerhetsprövning i en annan stat eller mellanfolklig organisation. I dessa fall ska det inte utfärdas något säkerhetsintyg, utan det är fråga endast om att lämna ut uppgifter efter registerkontroll.

I *andra stycket* anges att det i dessa fall även får göras en särskild personutredning enligt 3 kap. 10 § enligt förutsättningarna i den bestämmelsen. I 1996 års säkerhetsskyddslag finns en motsvarande bestämmelse i 18 §.

6 § Vid ärenden enligt 5 § gäller bestämmelserna om registerkontroll, särskild personutredning och samtycke i 3 kap. 6 och 10–13 §§.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag men får anses följa av bestämmelsen i den lagens 15 §. Övervägandena finns i avsnitt 20.4.4.

Bestämmelsen förtydligar på samma sätt som 4 § att bestämmelserna i 3 kap. om registerkontroll, särskild personutredning och samtycke i tillämpliga delar gäller vid sådana förfaranden som avses i 5 §.

Vem som beslutar om registerkontroll och utfärdar intyg

7 § Den nationella säkerhetsmyndigheten beslutar om registerkontroll enligt 3 och 5 §§ samt utfärdar intyg enligt 2 § och lämnar underlag enligt 5 §.

Om en registerkontroll föranleds av ett ärende om säkerhetsintyg för leverantör, beslutar i stället den nationella industrisäkerhetsmyndigheten om registerkontrollen och utfärdar intyg enligt 2 §.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 20.3 och 20.4.

Första stycket anger att det är den nationella säkerhetsmyndigheten enligt 1 § som beslutar om och vidtar de åtgärder som anges i 2, 3 och 5 §§.

Andra stycket anger en särskild ordning när en registerkontroll eller ett säkerhetsintyg enligt bestämmelser i kapitlet avser en leverantör. I sådana situationer är det den nationella industrisäkerhetsmyndigheten enligt 1 § som beslutar om registerkontroll och utfärdar intyg.

5 kap. Övriga bestämmelser

Tystnadsplikt

1 § Den som med stöd av denna lag har fått del av uppgifter om någon annans personliga förhållanden får inte obehörigen röja eller utnyttja dessa uppgifter.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 18.12.

Första stycket innebär en tystnadsplikt som tar sikte på att skydda enskildas integritet vid säkerhetsprövning enlig denna lag. I sådana ärenden kan förekomma såväl uppgifter som efter registerkontroll lämnats ut för säkerhetsprövning som uppgifter om den kontrollerade som kommit fram vid en grundutredning t.ex. vid en intervju med den kontrollerade.

Andra stycket upplyser om att motsvarande tystnadsplikt gäller i det allmännas verksamhet enligt bestämmelser i offentlighets- och sekretesslagen (2009:400).

2 § Den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet enligt denna lag får inte obehörigen röja eller utnyttja säkerhetsskyddsklassificerade uppgifter. Tystnadsplikten gäller om anställningen eller deltagandet placerats i säkerhetsklass enligt 3 kap. 4 §.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 22.1.

I *första stycket* anges att tystnadsplikt gäller för den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet enligt denna lag. En förutsättning för tystnadsplikten är dock att anställningen eller deltagandet placerats i säkerhetsklass. Den som under sådana former har deltagit i säkerhetskänslig verksamhet får således inte obehörigen föra vidare eller på annat sätt utnyttja uppgifter som är av betydelse för Sveriges säkerhet eller som Sverige i förhållanden till annan stat eller mellanfolklig organisation har åtagit sig att skydda. Bestämmelserna i 3 kap. 4 § om placering i säkerhetsklass innebär att den som genom anställning eller genom annat deltagande enbart får del av uppgifter i den lägsta informationssäkerhetsklassen inte ska placeras i säkerhetsklass. Det medför att tystnadsplikten inte omfattar den som kommer att hantera säkerhetsskyddsklassificerade uppgifter enbart i den lägsta informationssäkerhetsklassen. Avgränsningen till anställning eller deltagande som medför en placering i säkerhetsklass har valts för att det ska vara tydligt i vilka fall tystnadsplikten gäller. Ett förbud mot att obehörigen röja eller utnyttja säkerhetsskyddsklassificerade uppgifter kan dock åstadkommas även genom att vid ett överlämnade av sådana uppgifter till en verksamhet som inte omfattas av offentlighet- och sekretesslagen (2009:400) ställa upp förbehåll om sekretess för uppgifterna.

I fråga om hur tystnadsplikten förhåller sig till meddelarfriheten bör vissa bestämmelser i tryckfrihetsförordningen (TF) och yttrandefrihetsgrundlagen (YGL) noteras. Av 7 kap. 3 § 1 TF och 5 kap. 3 § YGL följer att meddelarfriheten är inskränkt om ett uppgiftslämnande är straffbart som bl.a. spionerі, grovt spionerі eller grov obehörig befattning med hemlig uppgift eller försök, förberedelse eller stämpling till sådant brott.

I *andra stycket* finns en upplysning om att i det allmännas verksamhet gäller i stället bestämmelser i offentlighets- och sekretesslagen.

Sekretessbrytande bestämmelse

3 § Sekretess hindrar inte att den nationella säkerhetsmyndigheten enligt 4 kap. 1 § i ett ärende om underlag för säkerhetsprövning enligt 4 kap. 5 § till en utländsk myndighet eller en mellanfolklig organisation lämnar ut en uppgift som har kommit fram vid registerkontroll eller särskild personutredning, om det står klart att ett sådant utlämnande är förenligt med svenska intressen.

Paragrafen saknar motsvarighet i 1996 års säkerhetsskyddslag. Övervägandena finns i avsnitt 20.4.5.

Bestämmelsen ger stöd för att lämna ut uppgifter som omfattas av bestämmelser om sekretess i offentlighets- och sekretesslagen (2009:400) till en annan stat eller mellanfolklig organisation i ett ärende enligt 4 kap. 5 § om underlag för säkerhetsprövning. Bestämmelsen utgör en sådan föreskrift som anges i 8 kap. 3 § 1 offentlighets- och sekretesslagen. Kravet på att det står klart att utlämnandet är förenligt med svenska intressen har sin grund i att det kan förekomma uppgifter som kommit fram vid en registerkontroll som av olika skäl är olämpliga att delge en utländsk myndighet eller mellanfolklig organisation.

Tillsyn

4 § Den som regeringen bestämmer ska utföra tillsyn över säkerhetsskyddet hos myndigheter och andra som lagen gäller för samt hos leverantörer som har träffat ett säkerhetsskyddsavtal.

Paragrafen motsvarar 31 § första stycket 1996 års säkerhetsskyddslag. Vissa redaktionella ändringar har gjorts. Någon ändring i sak är inte avsedd.

Föreskrifter om verkställighet

5 § Regeringen eller den myndighet som regeringen bestämmer meddelar de närmare föreskrifter som behövs för lagens tillämpning.

Paragrafen motsvarar 33 § 1996 års säkerhetsskyddslag. Vissa redaktionella ändringar har gjorts. Någon ändring i sak är inte avsedd.

Ikraftträdande och övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 2017.
2. Genom lagen upphävs säkerhetsskyddslagen (1996:627).
3. En anställning eller annat deltagande som enligt säkerhetsskyddslagen (1996:627) placerats i säkerhetsklass 1–3 ska motsvara en placering enligt 3 kap. 4 § i säkerhetsklass 1–3. En registerkontroll med stöd av 14 § säkerhetsskyddslagen ska i den utsträckning regeringen föreskriver motsvara ett beslut om placering i säkerhetsklass 3.

Första och andra punkten i de avslutande bestämmelserna i lagen anger datum för lagens ikraftträdande och att 1996 års säkerhetsskyddslag därigenom upphävs.

Till följd av upphävandet behövs en reglering om vad som ska gälla i fråga om beslut om placering i säkerhetsklass och registerkontroll till skydd mot terrorism enligt 1996 års säkerhetsskyddslag.

Tredje punkten anger att en anställning eller annat deltagande som enligt 1996 års säkerhetsskyddslag placerats i säkerhetsklass 1–3 ska anses motsvara en placering enligt 3 kap. 4 § i säkerhetsklass 1–3. I fråga om registerkontroll till skydd mot terrorism enligt 14 § 1996 års säkerhetsskyddslag anges att sådan registerkontroll i den utsträckning regeringen föreskriver ska motsvara ett beslut om placering i säkerhetsklass 3. Avsikten är att regeringen för merparten av de kontroller som utförts med stöd av den nämnda bestämmelsen ska kunna föreskriva att det tidigare beslutet gäller som ett beslut om placering i säkerhetsklass 3.

24.2 Förslaget till lag om ändring i polislagen (1984:387)

Den ändring som föreslås i polislagen (3 §) är en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Hänvisningen i 3 § till säkerhetsskyddslagen måste därför justeras. Någon ändring i sak är inte avsedd.

24.3 Förslaget till lag om ändring i elberedskapslagen (1997:288)

Den ändring som föreslås i elberedskapslagen (2 §) är en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Hänvisningen i 2 § till säkerhetsskyddslagen måste därför justeras. Till följd av benämningen tillträdesbegränsning i säkerhetsskyddslagen ändrats till fysisk säkerhet behöver dessutom i hänvisningen den nya benämningen läggas till.

24.4 Förslaget till lag om ändring i lagen (1998:938) om behandling av personuppgifter om totalförsvarspliktiga

Den ändring som föreslås i lagen om behandling av personuppgifter om totalförsvarspliktiga polislagen (9 §) är en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Hänvisningen i 9 § till säkerhetsskyddslagen måste därför justeras. Någon ändring i sak är inte avsedd.

24.5 Förslaget till lag om ändring i lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter

De ändringar som föreslås i lagen om (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter är en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Hänvisningarna i 7, 8 och 10 §§ till säkerhets-

skyddslagen och till paragrafer i den lagen måste därför justeras. Vidare görs i 7 § en mindre ändring i sak till följd av den justering som har gjorts i 2 kap. 6 § säkerhetsskyddslagen i fråga om i vilken omfattning lagen ska gälla för riksdagen och dess myndigheter.

24.6 Förslaget till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

Den ändring som föreslås i lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (1 kap. 10 §) är en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Hänvisningen i 1 kap. 10 § till säkerhetsskyddslagen måste därför justeras. Någon ändring i sak är inte avsedd.

En övergångsbestämmelse behövs för att även personuppgifter enligt den gamla lagen ska kunna behandlas även efter ikraftträdandet av denna ändring.

24.7 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

De ändringar som föreslås i offentlighets- och sekretesslagen (35 kap. 1, 3 och 10 §§) är i huvudsak en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Övervägandena finns i avsnitt 18.12. Hänvisningarna i de nämnda paragraferna till säkerhetsskyddslagen måste justeras. Därutöver görs en ändring i sak i 35 kap. 1 § 3 som handlar om sekretess för uppgift om en enskilds personliga och ekonomiska förhållanden för uppgifter i angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen. Bestämmelsen utvidgas till att avse säkerhetsprövning. Syftet med ändringen är att ge ett motsvarande skydd för uppgifter som på annat sätt än genom registerkontroll och särskild personutredning kommer fram vid genomförande av säkerhetsprövningen. Det kan bl.a. vara fråga om uppgifter om personliga

och ekonomiska förhållanden som den som kontrollen avser lämnar vid en intervju.

En övergångsbestämmelse behövs för att sekretess för uppgifter som avser registerkontroll och särskild personutredning enligt den gamla säkerhetsskyddslagen ska gälla även efter ikraftträdandet av denna ändring.

24.8 Förslaget till lag om ändring i polisdatalagen (2010:361)

Den ändring som föreslås i polisdatalagen (5 kap. 1 §) är en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Hänvisningen i 5 kap. 1 § till säkerhetsskyddslagen måste därför justeras. Någon ändring i sak är inte avsedd.

24.9 Förslaget till lag om ändring av lagen (2010:1767) om geografisk miljöinformation

Den ändring som föreslås i av lagen om geografisk miljöinformation (15 §) är en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Hänvisningen i 15 § till säkerhetsskyddslagen måste därför justeras. Någon ändring i sak är inte avsedd.

24.10 Förslaget till lag om ändring i lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet

Vid tillkomsten av lagen om upphandling på försvars- och säkerhetsområdet saknades definitioner i annan lagstiftning av begreppet säkerhetsskyddsklassificerade uppgifter. I förslaget till 1 kap. 4 § säkerhetsskyddslagen (2017:xx) finns en sådan nationell definition. Det är därför nödvändigt att i 2 kap. 22 § lagen om upphandling på försvars- och säkerhetsområdet klargöra att definitionen av säkerhetsskyddsklassificerade uppgifter i den paragrafen avser tillämpningen av den lagen.

I *första stycket* är därför tillagt ”i denna lag”. Genom den nya säkerhetsskyddslagen ersätts begreppet ”rikets säkerhet” med ”Sveriges säkerhet”. En motsvarande ändring föreslås även i denna bestämmelse.

I andra stycket hänvisas till säkerhetsskyddslagen som innehåller regler om de åtgärder som kan tillämpas för att skydda säkerhetsskyddsklassificerade uppgifter.

24.11 Förslaget till lag om ändring i lagen (2014:514) om ansvar för vissa säkerhetsfrågor vid statsministerns tjänstebostäder

De ändringar som föreslås i lagen om ansvar för vissa säkerhetsfrågor vid statsministerns tjänstebostäder (1, 2, 4 och 5 §§) är en följd av att 1996 års säkerhetsskyddslag upphör att gälla och ersätts av säkerhetsskyddslagen (2017:xx). Hänvisningen i de nämnda paragraferna till säkerhetsskyddslagen måste därför justeras. I fråga om 2, 4 och 5 §§ behöver också paragrafhänvisningarna justeras.

Vidare görs en mindre ändring i sak i *2 §* genom att uttrycken tillträdesbegränsning och tillträdesbegränsande åtgärder ersätts av fysisk säkerhet och åtgärder avseende fysisk säkerhet. Ändringarna är en följd av att bestämmelser om tillträdesbegränsning i 1996 års säkerhetsskyddslag genom 2 kap. 2 § säkerhetsskyddslagen (2017:xx) ersätts av bestämmelser om fysisk säkerhet. Som redovisats i kommentaren till den bestämmelsen har åtgärden ett vidare syfte än tillträdesbegränsning.

Kommittédirektiv 2011:94

En modern säkerhetsskyddslag

Beslut vid regeringssammanträde den 8 december 2011

Sammanfattning

En särskild utredare ska göra en översyn av säkerhetsskyddslagstiftningen. Syftet är främst att bättre anpassa lagstiftningen till det som krävs för att skydda verksamhet som har betydelse för rikets säkerhet och till de krav det internationella samarbetet ställer.

Utredaren ska bl.a.

- analysera vilka verksamheter som är av betydelse för rikets säkerhet eller som behöver skyddas mot terrorism och därför är i behov av säkerhetsskydd,
- föreslå hur reglerna om informationssäkerhet, som en del av säkerhetsskyddet, bör vara utformade,
- analysera vilka förändringar som kan behövas för att bättre anpassa lagstiftningen till de krav på säkerhetsskydd som ställs i det internationella samarbetet,
- analysera hur ett system med säkerhetsklarering kan utformas för svenska förhållanden,
- bedöma inom vilka verksamheter registerkontroll till skydd mot terrorism bör få ske,
- analysera behovet av förändringar av bestämmelserna om säkerhetsskyddad upphandling,

- ta ställning till om kravet på svenskt medborgarskap i säkerhetsskyddslagen bör förändras och
- utarbeta nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 30 april 2014.

Nuvarande reglering

Säkerhetsskyddslagen (1996:627) trädde i kraft den 1 juli 1996. I lagen finns bestämmelser om säkerhetsskydd. Med säkerhetsskydd menas dels skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, dels skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet och dels skydd mot terroristbrott, även om brotten inte hotar rikets säkerhet. Säkerhetsskydd ska, i behövlig omfattning, finnas vid verksamhet hos staten, kommunerna och landstingen, hos juridiska personer som staten, kommunerna eller landstingen utövar ett rättsligt bestämmande inflytande över samt hos enskilda om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Säkerhetsskyddet ska förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet), att obehöriga får tillträde till platser där de kan få tillgång till sådana uppgifter eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning) samt att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning). Säkerhetsskyddet ska även i övrigt förebygga terrorism. Lagen innehåller också bestämmelser om skyldighet att teckna säkerhetsskyddsavtal i vissa fall samt om utbildning, kontroll och tillsyn.

För riksdagen och dess myndigheter finns kompletterande bestämmelser om säkerhetsskydd i lagen (2006:128) om säkerhetsskydd i riksdagen och dess myndigheter.

Uppdraget att föreslå en modern lagstiftning för säkerhetsskydd

Säkerhetsskyddslagstiftningen har varit i kraft i mer än femton år. Under den tiden har förutsättningarna för säkerhetsskyddet förändrats på många sätt. Inte minst har utvecklingen inom informationstekniken och det internationella samarbetet medfört ett ökat fokus på säkerhetsskyddsfrågor. Även avregleringar av offentlig verksamhet har påverkat förutsättningarna för säkerhetsskyddet. Till detta kommer de förändringar som hotbilden genomgått sedan det kalla krigets slut och som bl.a. inneburit ett ökat fokus på civila områden samt på internationell terrorism och andra typer av grov internationell brottslighet.

Säkerhetspolisen och andra berörda myndigheter har i olika sammanhang pekat på frågor som behöver ses över inom ramen för en översyn av säkerhetsskyddslagen. Behovet av en allmän översyn av säkerhetsskyddslagen togs också upp av den dåvarande regeringen i samband med vissa ändringar av säkerhetsskyddslagen år 2006, se propositionen Ändringar i säkerhetsskyddslagen m.m. (prop. 2005/06:137 s. 14). Säkerhetspolisen har även i en skrift till regeringen år 2005 tagit upp behovet av relativt omfattande förändringar och anpassningar av säkerhetsskyddsförordningen (1996:633) (Ju2005/5877/L4).

Mot denna bakgrund gjorde regeringen i juni 2009 bedömningen att det var lämpligt att inleda en allmän översyn av säkerhetsskyddslagstiftningen och det behov av säkerhetsskydd som kan finnas för olika slags verksamheter. För att få en bättre bild av de frågeställningar som bör behandlas i en sådan översyn gavs Säkerhetspolisen i uppdrag att genomföra en förstudie över de frågeställningar som myndigheten anser bör behandlas i översynen (Ju2009/5174/PO).

Säkerhetspolisen redovisade uppdraget i oktober 2009 (Ju2009/8933/L4). I rapporten anger myndigheten ett antal större och mindre frågor som bör behandlas i en översyn av säkerhetsskyddslagstiftningen. Behovet av en översyn har därefter tagits upp av regeringen i propositionen Upphandling på försvars- och säkerhetsområdet (prop. 2010/11:150 del 1 s. 258).

Arbetet går nu vidare och en särskild utredare ges i uppdrag att göra en översyn av säkerhetsskyddslagstiftningen. Lagstiftningen

ska utformas på ett sådant sätt att den är enkel och tydlig att följa och tillämpa.

I följande avsnitt anges ett antal områden som utredaren ska ägna särskild uppmärksamhet.

Säkerhetsskyddets syfte

Säkerhetsskyddslagen är i första hand inriktad på att skydda rikets säkerhet. I förarbetena till lagen anges att det visserligen inte finns någon legaldefinition av begreppet rikets säkerhet, men att begreppet kan sägas avse såväl den yttre säkerheten för det nationella oberoendet som den inre säkerheten för det demokratiska statsskicket (prop. 1995/96:129 s. 22 och 74).

Skyddet för den yttre säkerheten tar framför allt sikte på totalförsvaret, dvs. den verksamhet som behövs för att förbereda Sverige för krig. Ett hot mot rikets yttre säkerhet anses dock kunna förekomma även om det inte hotar totalförsvaret. Skyddet av rikets yttre säkerhet anses omfatta uppgifter och förhållanden av rent militär betydelse eller av betydelse för totalförsvaret i övrigt och andra uppgifter som har betydelse för rikets nationella oberoende (prop. s. 23).

Också rikets inre säkerhet kan vara hotad utan att totalförsvaret berörs. Angrepp på det demokratiska statsskicket kan förekomma från grupperingar utan förbindelse med främmande makt. Det kan vara fråga om försök att ta över den politiska makten genom våld eller att använda våld, hot eller tvång mot statsledningen i syfte att påverka politikens utformning. Försök att systematiskt hindra medborgarna från att utnyttja sina demokratiska fri- och rättigheter räknas också till hoten mot rikets inre säkerhet (prop. s. 23).

Även om begreppet rikets säkerhet inte är reserverat för förhållanden som har betydelse för totalförsvaret har det i hög grad kommit att förknippas med framför allt militära förhållanden. Samtidigt har utvecklingen gått mot att andra samhälleliga verksamheter fått en allt större betydelse från säkerhetsskyddssynpunkt, något som bl.a. lyfts fram i Säkerhetspolisens förstudie. Ett uttryck för detta är den förändring som hotbilden genomgått under de senaste tio åren.

I förarbetena till säkerhetsskyddslagen konstaterades att hotbilden mot Sverige förändrats efter det kalla krigets slut. Trots det gjordes bedömningen att det nya säkerhetspolitiska läget inte hade inneburit några radikala förändringar av förutsättningarna för en ny säkerhetsskyddsreglering, se Säkerhetsskyddsutredningens betänkande Säkerhetsskydd (SOU 1994:149 s. 14 f.). Det nya regelverket utarbetades mot den bakgrunden.

Sedan säkerhetsskyddslagen trädde i kraft har hoten mot rikets säkerhet ytterligare förändrats. Ett enskilt militärt angrepp direkt mot Sverige bedöms som osannolikt under överskådlig tid. Kriser eller incidenter, som även inbegriper militära maktmedel kan dock uppstå i vår region, och på längre sikt kan militära angreppshot aldrig uteslutas, se propositionen Ett användbart försvar (prop. 2008/09:140 s. 28). Dagens säkerhetspolitiska hot, eller hot som är av sådan karaktär att de kan få säkerhetspolitiska konsekvenser, är ofta gränsöverskridande, icke-militära och utgår inte sällan från icke-statliga aktörer. Som exempel kan nämnas internationell terrorism och andra typer av grov internationell brottslighet, spridning av massförstörelsevapen samt framställning och transport av vapen, komponenter och teknologi, jfr propositionen En anpassad försvarsunderrättelseverksamhet (prop. 2006/07:63 s. 17). Säkerhetspolisen har också noterat att främmande staters underrättelseverksamhet de senaste decennierna har breddats mot forskning och utveckling inom civila områden samt mot politiska frågor och information som rör samhällsviktiga system, jfr regeringens direktiv till Utredningen om förstärkt skydd mot främmande makts underrättelseverksamhet (dir. 2010:35). Vidare betraktar Säkerhetspolisen elektroniska angrepp i olika former som ett av de allvarligaste hoten. Även den ökade internationaliseringen innebär nya förutsättningar för säkerhetsskyddet. En särskild fråga är de svårigheter som kan uppstå från säkerhetsskyddssynpunkt vid utflyttning av verksamheter till utlandet, bl.a. inom energiförsörjningen.

Det är alltså angeläget att lagstiftningen är utformad på ett sådant sätt att den ger utrymme för att vidta de åtgärder som krävs för att möta de förändringar som skett när det gäller hoten mot rikets säkerhet. Lagstiftningen måste också vara utformad så att den har förutsättningar att stå sig över tid. Det är därför viktigt att reglerna inte får ett allt för snävt tillämpningsområde.

Säkerhetsskyddslagen bör även i fortsättningen kunna omfatta vissa andra nationella skyddsändamål än rikets säkerhet, bl.a. skydd mot terroristbrott som saknar koppling till rikets säkerhet.

Säkerhetsskyddsåtgärder bör också kunna vidtas för att skydda samhällsviktig verksamhet vars funktionalitet är av betydelse för rikets säkerhet mot andra brottsliga angrepp, även om angreppet i det konkreta fallet inte anses kunna hota rikets säkerhet. Exempel som Säkerhetspolisen nämner i förstudien är kritisk infrastruktur såsom verksamhet för produktion eller distribution av dricksvatten och elektricitet.

Säkerhetsskyddslagens koppling till rikets säkerhet innebär att säkerhetsskyddsåtgärder endast i begränsad omfattning kan vidtas för att tillgodose skyddsintressen med anknytning till andra länder eller mellanfolkliga organisationer i fall där det saknas en koppling till svenska säkerhetsintressen.

Enligt Säkerhetspolisens förstudie och tidigare översyner, bl.a. promemorian Några frågor om säkerhetsprövning inför utlandsverksamhet, m.m. (Ds 2006:20), bör säkerhetsskyddsåtgärder i högre grad än vad som är möjligt med nuvarande regler kunna vidtas här i landet, bl.a. när det gäller svenskar eller svenska företag som ska delta i säkerhetskänslig verksamhet utomlands. Samma sak gäller för att skydda viss säkerhetskänslig information som tagits emot av svenska myndigheter och andra organ inom ramen för internationellt samarbete, t.ex. inom EU-arbetet och samarbetet med Nato. En given utgångspunkt i detta sammanhang är att lagstiftningen ska uppfylla de krav som ställs enligt de folkrättsliga åtaganden som Sverige gjort på säkerhetsskyddsområdet, vilket berörs närmare nedan. En framtida reglering av säkerhetsskyddsfrågorna bör alltså tydligt göra klart att även vissa berättigade säkerhetsskyddsintressen med anknytning till andra länder eller mellanfolkliga organisationer kan vara ett ändamål för lagstiftningen, även i fall där det saknas en koppling till svenska säkerhetsintressen.

Utredaren ska därför

- analysera vilka verksamheter som är av betydelse för rikets säkerhet eller som behöver skyddas mot terrorism och därför är i behov av säkerhetsskydd,

- ta ställning till vilka säkerhetsskyddsintressen med anknytning till andra länder eller mellanfolkliga organisationer som bör kunna bli föremål för säkerhetsskyddsåtgärder här i landet,
- i övrigt föreslå hur tillämpningsområdet för lagstiftningen bör avgränsas och
- utarbeta nödvändiga författningsförslag.

Informationssäkerhet

En viktig del i säkerhetsskyddet är informationssäkerheten. Med det avses åtgärder för att förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (7 § första stycket 1 säkerhetsskyddslagen). Därutöver finns i 9 § säkerhetsskyddslagen en bestämmelse som uttryckligen anger att behovet av skydd vid automatisk informationsbehandling ska beaktas särskilt vid utformningen av informationssäkerheten.

Termen informationssäkerhet infördes i samband med säkerhetsskyddslagen och ersatte den äldre termen sekretessskydd. Skälet till ändringen var att markera att utvecklingen på informationsteknikens område medfört att skyddet av sekretessbelagd information fått en annan dimension än tidigare (prop. 1995/96:129 s. 27).

Sedan säkerhetsskyddslagen trädde i kraft 1996 har informationstekniken och användningen av den genomgått en betydande utveckling. Bland annat internet, som fick sitt egentliga genomslag i mitten på 1990-talet, har i grunden förändrat förutsättningarna för informationssäkerhetsarbetet. Mycket stora informationsmängder, såväl öppen som hemlig, hanteras i it-system. En rad verksamheter, både hos det allmänna och inom näringslivet, är helt beroende av digitala system för bl.a. styrning, reglering och övervakning. Även internationaliseringen har påverkat förutsättningarna för informationssäkerheten. Det gäller exempelvis i samband med utflyttning av verksamhet till utlandet, bl.a. inom energiförsörjningen. Denna utveckling har även inneburit att hotbilden förändrats. Som tidigare nämnts anser Säkerhetspolisen att angrepp i form av elektroniska attacker på samhällsviktiga informationssystem är ett av de allvarligaste hoten mot rikets

säkerhet. Säkerhetsskyddslagstiftningen måste vara utformad på ett sådant sätt att den ger utrymme för att vidta de åtgärder som krävs för att möta utvecklingen på it-området. Lagstiftningen bör vidare vara så utformad att den har förutsättningar att stå sig över tid.

Som beskrivits i det föregående är ett av ändamålen med säkerhetsskyddslagen att skydda uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet. Det gäller bl.a. bestämmelserna om informationssäkerhet, som uteslutande är inriktade på att skydda uppgifter som omfattas av sekretess och som rör rikets säkerhet. Lagen ger därför små möjligheter att vidta åtgärder för att skydda it-systemen som sådana. Samtidigt har utvecklingen på it-området inneburit att vissa informationssystem för bl.a. styrning, reglering och övervakning, t.ex. inom energiförsörjningen, fått en allt större betydelse för rikets säkerhet. Det gäller oavsett om det i systemen hanteras uppgifter som omfattas av sekretess som rör rikets säkerhet. Avgränsningen av säkerhetsskyddslagens bestämmelser om informationssäkerhet till åtgärder som behövs för att skydda uppgifter som omfattas av sekretess och som rör rikets säkerhet framstår alltså inte längre som ändamålsenlig.

Vid sidan av Säkerhetspolisens arbete med informationssäkerhet enligt säkerhetsskyddslagen finns flera myndigheter som är verksamma inom informationssäkerhetsområdet med stöd av andra författningar. Bland annat har Myndigheten för samhällsskydd och beredskap i uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet. Det är angeläget att den samlade kompetens som finns vid de myndigheter som utför uppgifter på informationssäkerhetsområdet kan utnyttjas på ett effektivt och ändamålsenligt sätt.

Utredaren ska därför

- föreslå hur reglerna om informationssäkerhet, som en del av säkerhetsskyddet, bör vara utformade och
- med beaktande av övrig rättslig reglering på informationssäkerhetsområdet, utarbeta nödvändiga författningsförslag.

Ett nytt system för säkerhetsprövning?

Av 17 § säkerhetsskyddslagen följer bl.a. att en anställning ska placeras i säkerhetsklass om den anställde i viss omfattning får del av uppgifter som omfattas av sekretess och är av betydelse för rikets säkerhet. Att en anställning har placerats i säkerhetsklass har betydelse bl.a. för möjligheterna till och omfattningen av registerkontroll av den enskilde. Bestämmelserna om placering i säkerhetsklass och kopplingen till skyddet av sekretessbelagda uppgifter innebär att verksamheter där det hanteras sekretessbelagda uppgifter som har betydelse för rikets säkerhet intar en särställning i säkerhetsskyddshänseende.

I det föregående har det redogjorts för att hoten mot rikets säkerhet har förändrats och dessutom kommit att rikta sig mot fler områden än tidigare. Exempel som Säkerhetspolisen nämner är vissa samhällsviktiga system som endast i mindre omfattning, eller inte alls, hanterar sekretessbelagda uppgifter som har betydelse för rikets säkerhet. Kopplingen till skyddet av sekretessbelagda uppgifter har också medfört vissa oklarheter när det gäller att bedöma hur bestämmelserna om placering i säkerhetsklass ska tillämpas på privaträttsliga subjekt. I takt med de avregleringar av offentlig verksamhet som skett har frågorna fått allt större aktualitet.

Säkerhetsskyddslagens bestämmelser om placering i säkerhetsklass och säkerhetsprövning innebär att omfattningen av de kontroller som görs av en person som ska delta i säkerhetskänslig verksamhet styrs av den mängd säkerhetskänsliga uppgifter som personen får del av. Exempelvis gäller för placering i säkerhetsklass 1 att personen i stor omfattning får del av uppgifter som omfattas av sekretess och är av synnerlig betydelse för rikets säkerhet (17 § 1 säkerhetsskyddslagen). Härigenom skiljer sig den svenska säkerhetsskyddsregleringen från vad som gäller för flertalet länder i vår närhet.

Gemensamt för lagstiftningen i dessa länder är att regelverken är uppbyggda kring ett system med säkerhetsklarering (eng: *personal security clearance*). Med säkerhetsklarering avses i princip att den person som ska kontrolleras godkänns – klareras – i en viss skyddsklass, som ger honom eller henne behörighet att befatta sig med säkerhetskänsliga uppgifter upp till och med en viss skydds-

nivå. Systemen med säkerhetsklarering innebär vidare att varje handling som bedöms skyddsvärd förses med en särskild markering som anger vilken skyddsnivå som gäller för handlingen.

Systemet med säkerhetsklarering har sin grund i Nato-samarbetet och förekommer i flera länder och mellanfolkliga organisationer. Ett sådant system tillämpas även i EU enligt vad som föreskrivs i rådets beslut av den 31 mars 2011 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2011/292/EU). Vidare har nyligen ett multilateralt säkerhetsskyddsavtal undertecknats mellan EU:s medlemsländer, som även det utgår från systemet med säkerhetsklarering (EUT 2011/C 202/05). Avtalet har ännu inte trätt i kraft. På det nordiska området träffades 2010 ett generellt säkerhetsskyddsavtal om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter (traktat nr 06893) som också grundas på systemet med säkerhetsklarering.

Den avgörande skillnaden mellan ett system med säkerhetsklarering och säkerhetsskyddslagens systematik har allmänt ansetts vara att den svenska säkerhetsprövningen är knuten till anställningen medan kontrollen i ett system med säkerhetsklarering hänför sig till den anställde.

Frågor om säkerhetsklarering togs upp 2001 i en skrivelse från Säkerhetspolisen till Justitiedepartementet (Ju2001/8231/L4). Enligt Säkerhetspolisen var olägenheterna med det svenska systemet bl.a. förknippade med möjligheterna att utfärda intyg över en utförd säkerhetsprövning. Säkerhetspolisen ansåg därför att grunderna för säkerhetsprövning och registerkontroll behövde ändras. Frågorna har också behandlats i promemorian Några frågor om säkerhetsprövning inför utlandsverksamhet, m.m. (Ds 2006:20). Promemorians förslag har inte lett till några lagändringar.

Sedan säkerhetsskyddslagen trädde i kraft har det internationella samarbetet intensifierats. Det gäller dels stater emellan, dels inom näringslivet. Samarbetet inom EU har utvecklats och blivit tätare. I näringslivet ställs allt oftare krav på säkerhetsskyddsåtgärder som villkor för att delta i olika internationella affärssamarbeten. Sammantaget innebär det att säkerhetsskyddsfrågorna fått en allt större betydelse. Denna utveckling har gjort det tydligt att skillnaderna mellan systemen i den praktiska tillämpningen blivit allt svårare att överbrygga. Säkerhetsskyddslagen innehåller

exempelvis inte någon reglering om utfärdande av intyg över en utförd säkerhetsprövning – vilket kan göra det svårare för svenskar att delta i säkerhetskänslig verksamhet utomlands. Ett annat problem utgör de svårigheter som finns när det gäller att jämföra de säkerhetsskyddsåtgärder som genomförs enligt de olika systemen. Dessa omständigheter kan innebära en risk för att det svenska systemet uppfattas som inte fullt likvärdigt med systemen med säkerhetsklarering. Dessutom är det förenat med svårigheter i den praktiska tillämpningen. Det är angeläget att framtidens regler om säkerhetsskydd utformas så att de är bättre anpassade till de system för säkerhetsskydd som tillämpas såväl i flertalet länder i vår närhet som i de internationella organisationer som Sverige är medlem i eller samarbetar med. Mycket talar därför för att tiden nu är mogen för Sverige att gå över till ett system med säkerhetsklarering.

En sådan reform förutsätter noggranna överväganden på en rad områden. Till att börja med får regelverket inte innebära att medborgarnas möjligheter att ta del av allmänna handlingar enligt offentlighetsprincipen begränsas. En ytterligare förutsättning är att det är rättssäkert och godtagbart från integritetsskyddssynpunkt. Bland annat krävs noggranna överväganden av omfattningen av de kontroller som bör ligga till grund för ett beslut om säkerhetsklarering. Även de praktiska konsekvenserna av en reform måste analyseras.

En annan fråga som måste analyseras är vilken eller vilka myndigheter som ska kunna besluta om säkerhetsklarering och hur godkännandeprocessen ska gå till. I det internationella arbetet med säkerhetsskydd spelar den Nationella säkerhetsmyndigheten (eng. National Security Authority, NSA) inom respektive stat en central roll. I Sverige är denna funktion fördelad på ett flertal myndigheter, bl.a. Försvarsmakten och Försvarets materielverk, och innebär ansvar för bl.a. tillsyn samt att företräda Sverige i arbetet med säkerhetsskyddsfrågor inom EU, Nato och den europeiska rymdorganisationen (eng: *European Space Agency, ESA*).

Oavsett om Sverige går över till ett system med säkerhetsklarering eller inte måste lagstiftningen uppfylla de krav som ställs enligt de internationella åtaganden som Sverige gjort på säkerhetsskyddsområdet. Det gäller bl.a. att här i landet skydda viss säkerhetskänslig information som tagits emot av svenska

myndigheter och andra organ inom ramen för internationellt samarbete, exempelvis inom EU-arbetet.

Utredaren ska därför

- översiktligt redovisa de regler och förfaranden som gäller i länder som är jämförbara med Sverige och som tillämpar ett system med säkerhetsklarering, särskilt de nordiska länderna och länderna inom EU,
- analysera vilka förändringar som kan behövas för att bättre anpassa säkerhetsskyddslagstiftningen till de krav på säkerhetsskydd som ställs i det internationella samarbetet,
- analysera hur ett system med säkerhetsklarering kan utformas för svenska förhållanden,
- föreslå hur behovet av säkerhetsskydd ska tillgodoses i verksamheter som är av betydelse för rikets säkerhet men som i begränsad omfattning eller inte alls hanterar uppgifter som omfattas av sekretess och som rör rikets säkerhet,
- bedöma vilka organisatoriska förändringar som en övergång till ett system med säkerhetsklarering skulle kräva och vilka praktiska konsekvenser en sådan övergång skulle medföra och
- utarbeta nödvändiga författningsförslag.

Registerkontroll till skydd mot terrorism

Vid anställning eller annat deltagande i verksamhet som har placerats i säkerhetsklass ska en registerkontroll göras. Av 14 § säkerhetsskyddslagen följer att en registerkontroll får ske även i andra fall om det behövs för skyddet mot terrorism och det finns särskilda skäl. Närmare bestämmelser om registerkontroll till skydd mot terrorism finns i säkerhetsskyddsförordningen. Bestämmelserna innebär bl.a. att en registerkontroll får göras beträffande den som ska delta vid vissa närmare angivna verksamheter, t.ex. vid civila flygplatser, anläggningar inom elförsörjningen som är skyddsobjekt samt vissa andra skyddsobjekt (26 och 27 §§ säkerhetsskyddsförordningen).

Vid registerkontroll som görs till skydd mot terrorism får samtliga uppgifter om den kontrollerade som finns i belastnings-

registret, misstankeregistret, SÄPO-registret och som annars behandlas hos Säkerhetspolisen lämnas ut (22 § säkerhetsskyddslagen). En viktig begränsning är dock att endast sådana uppgifter får lämnas ut som kan antas ha betydelse för prövningen av den kontrollerades pålitlighet från säkerhetssynpunkt (24 § säkerhetsskyddslagen). Det är Säkerhets- och integritetsskyddsnämnden som i varje enskilt fall beslutar vilka uppgifter som får lämnas ut. Registernämnden, vars verksamhet den 1 januari 2008 övertogs av Säkerhets- och integritetsskyddsnämnden, har i verksamhetsberättelsen för år 2007 ifrågasatt om bestämmelserna om utlämnande i 24 § fått en alltför restriktiv utformning när det gäller personal som är verksam vid flygplatser eller kärnkraftverk (Ju2008/1653/L4). Även Säkerhetspolisen har framfört invändningar mot regelverket i denna del.

Enligt Säkerhetspolisen kan det i vissa fall finnas anledning att utvidga möjligheterna till registerkontroll till skydd mot terrorism. Exempel som Säkerhetspolisen nämner är transporter av kärnämnen och kärnavfall. Behov av säkerhetsskyddsåtgärder vid transporter av farligt gods har även tagits upp av Riksrevisionen i rapporten Skyddet för farligt gods, RiR 2008:29 (Ju2008/10750/L4, N2008/8857/TE, Fö2008/3701/SSK).

Det finns alltså anledning att överväga hur bestämmelserna om registerkontroll till skydd mot terrorism bör vara utformade. Utredaren ska därför

- bedöma inom vilka verksamheter registerkontroll till skydd mot terrorism bör få ske,
- ta ställning till om reglerna om utlämnande av uppgifter bör ändras när det gäller registerkontroll till skydd mot terrorism och
- utarbeta nödvändiga författningsförslag.

Säkerhetsskyddad upphandling och industrisäkerhetsskydd

Av 1 § säkerhetsskyddslagen följer att lagen gäller även hos enskilda om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism. Exempel på enskilda som omfattas av säkerhetsskyddslagen är företag inom försvarsindustrin

och vissa privata energiproducenter, bl.a. inom kärnkraftsindustrin. Härutöver kan krav på säkerhetsskyddsåtgärder i vissa fall komma att gälla även för enskilda som normalt sett inte omfattas av lagens bestämmelser. Av reglerna om s.k. *säkerhetsskyddad upphandling* följer nämligen att en statlig myndighet, en kommun eller ett landsting som avser träffa avtal om upphandling eller begära in anbud ska träffa ett säkerhetsskyddsavtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det aktuella fallet (8 § säkerhetsskyddslagen). Säkerhetsskyddsavtal förekommer även vid internationellt samarbete om utveckling eller produktion av försvarsmateriel (17 § säkerhetsskyddsförordningen).

Skyldigheten att upprätta säkerhetsskyddsavtal är dock begränsad i flera avseenden. Den gäller t.ex. inte för enskilda eller rättssubjekt över vilka staten, kommunerna eller landstingen utövar ett rättsligt bestämmande inflytande, även om dessa bedriver verksamhet som är av betydelse för rikets säkerhet eller som särskilt behöver skyddas mot terrorism. Inte heller gäller den för myndigheter, kommuner och landsting vid en upphandling som inte innehåller uppgifter om rikets säkerhet men däremot uppgifter som är betydelsefulla för skyddet mot terrorism.

Numera är det, i långt större utsträckning än när säkerhetsskyddslagen trädde i kraft, vanligt att myndigheter och enskilda i stora projekt tar hjälp av externa leverantörer, som i sin tur kan komma att anlita underleverantörer. Det är också vanligt att utländska leverantörer och entreprenörer deltar i säkerhetsskyddade upphandlingar här i landet samt att svenska företag deltar i motsvarande verksamhet utomlands. I andra länder och mellanfolkliga organisationer förekommer dessutom att krav ställs på s.k. säkerhetsgodkännande av verksamhetsställe (eng: *Facility Security Clearance, FSC*) som villkor för att delta i viss verksamhet, vilket kan innebära att företaget ska visa upp ett godtagbart säkerhetsskydd i fler avseenden än vad som gäller enligt säkerhetsskyddslagen eller ett svenskt säkerhetsskyddsavtal. Bestämmelser om säkerhetsgodkännande av verksamhetsställe finns bl.a. i rådets säkerhetsbestämmelser.

Säkerhetspolisen har pekat på att det nuvarande systemet med säkerhetsskyddsavtal är komplicerat samt tids- och kostnadskrävande att tillämpa för företagen, vilket kan innebära en risk för att reglerna inte får det genomslag som lagstiftningen förutsätter.

Säkerhetsskyddslagstiftningen bygger på grundtanken att de intressen lagstiftningen slår vakt om ska ha samma skydd oavsett om verksamheten bedrivs av det allmänna eller av enskilda (jfr prop. 1995/96:129 s. 35). Det är angeläget att reglerna är utformade så att detta kommer till utryck på ett tydligt sätt. Lagstiftningen bör även göra det möjligt för svenska företag att delta på likvärdiga villkor vid upphandlingar och anbudsförfaranden som rör säkerhetskänslig verksamhet utomlands, jfr propositionen Upphandling på försvars- och säkerhetsområdet (prop. 2010/11:150 del 1 s. 258). Den utveckling som har skett ställer nya krav på det säkerhetsskydd som kan behövas för svenska företag som deltar i säkerhetskänslig verksamhet, här såväl som i utlandet, och för utländska företag som får del av säkerhetskänslig information som rör svenska förhållanden.

Utredaren ska därför

- analysera behovet av förändringar av säkerhetsskyddslagens bestämmelser om säkerhetsskyddad upphandling, bl.a. möjligheterna att träffa säkerhetsskyddsavtal,
- bedöma vilka förändringar i övrigt som kan behövas för att bättre anpassa reglerna till de krav som ställs i det internationella samarbetet, bl.a. när det gäller systemen med säkerhetsgodkännande av verksamhetsställe och
- utarbeta nödvändiga författningsförslag.

Medborgarskapskravet

Bestämmelser om krav på svenskt medborgarskap för vissa anställningar finns bl.a. i 11 kap. 11 § och 12 kap. 6 § regeringsformen, 5 och 6 §§ lagen (1994:260) om offentlig anställning och 29 § säkerhetsskyddslagen.

Enligt 29 § första stycket säkerhetsskyddslagen får en säkerhetsklassad anställning vid staten, en kommun eller ett landsting innehas endast av den som är svensk medborgare. Regeringen får i enskilda fall medge undantag från kravet på svenskt medborgarskap (29 § tredje stycket säkerhetsskyddslagen).

Det finns anställningar inom totalförsvaret där medborgarskapet är av väsentlig betydelse. Enligt Säkerhetspolisen kan dock de

nuvarande reglerna försvåra möjligheterna att rekrytera kompetent personal inom verksamheter som har behov av specialistkompetens som inte finns att tillgå här i landet. Reglerna kan även innebära att personer med utländsk bakgrund i onödan utestängs från delar av arbetsmarknaden. Vidare kan de innebära svårigheter att åstadkomma en jämnare personalsammansättning med avseende på etnisk bakgrund, vilket bedömts angeläget för vissa verksamheter. Ett sådant exempel är Kriminalvården som arbetar aktivt för att öka andelen anställda med utländsk bakgrund samtidigt som en stor del av anställningarna är placerade i säkerhetsklass.

Mot denna bakgrund finns det skäl att överväga om kravet på svenskt medborgarskap för innehav av en säkerhetsklassad anställning bör förändras.

Utredaren ska därför

- ta ställning till om, och i så fall hur, kravet på svenskt medborgarskap i säkerhetsskyddslagen bör förändras, i vart fall för de lägre säkerhetsklasserna, och
- utarbeta nödvändiga författningsförslag.

Tillsyn

Tillsynsansvaret enligt säkerhetsskyddslagen omfattar myndigheter och andra organ som säkerhetsskyddslagen gäller för samt anbudsgivare och leverantörer som ingått säkerhetsskyddsavtal. Säkerhetspolisen och Försvarsmakten har huvudansvaret för tillsynen (jfr 39 § säkerhetsskyddsförordningen och 3 § 1 förordningen [2002:1050] med instruktion för Säkerhetspolisen).

När det gäller bolag, föreningar och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande samt i fråga om enskilda som lagen gäller för utövas kontrollen av den sektorsansvariga myndigheten, t.ex. Affärsverket svenska kraftnät för elförsörjningsverksamhet och Post- och telestyrelsen för telekommunikationsverksamhet. Säkerhetsskyddet hos anbudsgivare eller leverantörer som har träffat säkerhetsskyddsavtal kontrolleras av den avtalsslutande myndigheten, kommunen eller landstinget. Även på dessa områden kan dock säkerhetsskyddet kontrolleras av Säkerhetspolisen och

Försvarsmakten. Kontrollen ska i så fall utföras i samråd med den primärt ansvariga myndigheten.

I tillsynsuppgifterna ligger bl.a. att kontrollera att myndigheterna och berörda organ följer reglerna om säkerhetsskydd och att säkerhetsskyddet är tillräckligt för den verksamhet som bedrivs. Särskilt i förhållande till enskilda är behovet av råd och stöd framträdande. Tillsynen utövas bl.a. genom besök, inspektioner och s.k. penetrationstester, varvid eventuella brister påpekas och förslag till förbättringar lämnas. Om brister inte rättas till ska tillsynsmyndigheten under vissa förutsättningar anmäla detta till regeringen (48 § säkerhetsskyddsförordningen). Några sanktionsmöjligheter finns emellertid inte. Inte heller finns någon skyldighet att anmäla inträffade säkerhetsincidenter till tillsynsmyndigheten i andra fall än där en hemlig uppgift har röjts, om röjandet kan antas medföra men för rikets säkerhet som inte är ringa (10 § säkerhetsskyddsförordningen).

Bland annat den ökade internationaliseringen och informationsteknikens utveckling ställer nya krav på säkerhetsskyddet och därmed även på tillsynen. Även avregleringar av offentlig verksamhet, som beskrivits ovan, innebär ökade krav på tillsynsmyndigheterna, framför allt för Säkerhetspolisen, men även för sektorsansvariga myndigheter. En förutsättning för att reglerna om säkerhetsskydd ska få det genomslag som är avsett är att tillsynen kan ske på ett effektivt och ändamålsenligt sätt. Särskilt betydelsefull är tillsynsmyndigheternas stödjande och rådgivande verksamhet. Det är också viktigt att den samlade kompetens som finns hos de myndigheter som har tillsyns- och kontrollansvar på säkerhetsskyddsområdet kan utnyttjas på ett effektivt sätt.

Utredaren ska därför

- analysera hur Säkerhetspolisens och Försvarsmaktens tillsyn över säkerhetsskyddet bör vara utformat, bl.a. i förhållande till de sektorsansvariga myndigheternas kontroll,
- ta ställning till om ett system med sanktionsåtgärder bör införas och i sådant fall hur det bör utformas och
- utarbeta nödvändiga författningsförslag.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och konsekvenserna i övrigt av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska även bedöma vilka konsekvenser förslagen får för företag. Kostnadsberäkningar och andra konsekvensbeskrivningar ska redovisas enligt bestämmelserna i 14–15 a §§ kommittéförordningen (1998:1474).

Arbetsformer och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och utredningsväsendet, bl.a. Utredningen om förstärkt skydd mot främmande makts underrättelseverksamhet (Ju 2010:03) samt inom internationella organisationer, särskilt EU. Utredaren är oförhindrad att ta upp sådana närliggande frågor som har samband med de frågeställningar som ska utredas.

Under genomförandet av uppdraget ska utredaren samråda med och inhämta upplysningar från berörda myndigheter och andra organ, särskilt Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen, Affärsverket svenska kraftnät, Transportstyrelsen och Myndigheten för samhällsskydd och beredskap.

Uppdraget ska redovisas senast den 30 april 2014.

(Justitiedepartementet)

Statens offentliga utredningar 2015

Kronologisk förteckning

1. Deltagande med väpnad styrka i utbildning utomlands. En utökad beslutsbefogenhet för regeringen. Fö.
2. Värdepappersmarknaden MiFID II och MiFIR. + Bilagor. Fi.
3. Med fokus på kärnuppgifterna. En angelägen anpassning av Polismyndighetens uppgifter på djurområdet. Ju.
4. Ett svenskt tonnageskattesystem. Fi.
5. En ny svensk tullagstiftning. Fi.
6. Mer gemensamma tobaksregler. Ett genomförande av tobaksproduktdirektivet. S.
7. Krav på privata aktörer i välfärden. Fi.
8. En översyn av årsredovisningslagarna. Ju.
9. En modern reglering av järnvägstransporter. Ju.
10. Gränser i havet. UD.
11. Kunskapsläget på kärnavfallsområdet 2015. Kontroll, dokumentation och finansiering för ökad säkerhet. M.
12. Överprövning av upphandlingsmål m.m. Fi.
13. Tillämpningsdirektivet till utstationeringsdirektivet – Del I. A.
14. Sedd, hörd och respekterad. Ett ändamålsenligt klagomålssystem i hälso- och sjukvården. S.
15. Attraktiv, innovativ och hållbar – strategi för en konkurrenskraftig jordbruks- och trädgårdsnäring. N L.
16. Ökat värdeskapande ur immateriella tillgångar. N.
17. För kvalitet – Med gemensamt ansvar. S.
18. Lösöreköp och registerpant. Ju.
19. En ny ordning för redovisningstillsyn. Fi.
20. Trygg och effektiv utskrivning från sluten vård. S.
21. Mer trygghet och bättre försäkring. Del 1 + 2. S.
22. Rektorn och styrkedjan. U.
23. Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. Ju Fö.
24. En kommunallag för framtiden. Del A + B . Fi.
25. En ny säkerhetsskyddslag. Ju.

Statens offentliga utredningar 2015

Systematisk förteckning

Arbetsmarknadsdepartementet

Tillämpningsdirektivet till utstationeringsdirektivet – Del I [13]

Finansdepartementet

Värdepappersmarknaden MiFID II och MiFIR. + Bilagor [2]

Ett svenskt tonnageskattesystem. [4]

En ny svensk tullagstiftning. [5]

Krav på privata aktörer i välfärden. [7]

Överprövning av upphandlingsmål m.m. [12]

En ny ordning för redovisningstillsyn. [19]

En kommunallag för framtiden. Del A + B. [24]

Försvarsdepartementet

Deltagande med väpnad styrka i utbildning utomlands. En utökad beslutsbefogenhet för regeringen. [1]

Justitiedepartementet

Med fokus på kärnuppgifterna. En angelägen anpassning av Polismyndighetens uppgifter på djurområdet. [3]

En översyn av årsredovisningslagarna. [8]

En modern reglering av järnvägstransporter. [9]

Lösöreköp och registerpant. [18]

Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. [23]

En ny säkerhetsskyddslag. [25]

Miljö- och energidepartementet

Kunskapsläget på kärnavfallsområdet 2015. Kontroll, dokumentation och finansiering för ökad säkerhet. [11]

Näringsdepartementet

Attraktiv, innovativ och hållbar – strategi för en konkurrenskraftig jordbruks- och trädgårdsnäring. [15]

Ökat värdeskapande ur immateriella tillgångar. [16]

Socialdepartementet

Mer gemensamma tobaksregler. Ett genomförande av tobaksproduktdirektivet. [6]

Sedd, hörd och respekterad. Ett ändamålsenligt klagomålssystem i hälso- och sjukvården. [14]

För kvalitet – Med gemensamt ansvar. [17]

Trygg och effektiv utskrivning från sluten vård. [20]

Mer trygghet och bättre försäkring. Del 1 + 2. [21]

Utbildningsdepartementet

Rektorn och styrkedjan. [22]

Utrikesdepartementet

Gränser i havet. [10]