Informations- och cybersäkerhet i Sverige

Strategi och åtgärder för säker information i staten

Betänkande av NISU 2014

Stockholm 2015

STATENS OFFENTLIGA UTREDNINGAR

SOU 2015:23

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 978-91-38-24256-8
ISSN 0375-250X

Till statsrådet Anders Ygeman

Regeringen beslutade den 28 november 2013 (dir. 2013:110) att tillkalla en särskild utredare med uppdrag att föreslå strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system.

Som särskild utredare förordnades från och med den 2 december 2013 generaldirektören Erik O. Wennerström.

Utredningens uppdrag utökades genom tilläggsdirektiv (dir. 2014:66) beslutat den 8 maj 2014. Den särskilde utredaren fick utöver det ursprungliga uppdraget i uppgift att undersöka de rättsliga förutsättningarna för SOS Alarm Sverige AB att inrätta och driva ett system för viktigt meddelande till allmänheten via mobil och fast telefoni vid allvarliga olyckor och kriser.

Som sakkunniga förordnades från och med den 6 februari 2014 departementssekreteraren Ingolf Berg, Näringsdepartementet, ämnessakkunnige John Billow, Justitiedepartementet, departementssekreteraren Andreas Dahlqvist och kanslirådet Jonas Norling, Utrikesdepartementet. Den 17 februari 2014 förordnades utredningschefen Lars Nicander, Försvarshögskolan, som expert i utredningen. Som sakkunniga i utredningen förordnades från och med den 18 februari 2014 kanslirådet Henrik Moberg, Socialdepartementet respektive den 1 maj samma år departementssekreteraren Linda Ericson, Försvarsdepartementet. John Billow entledigades från och med den 6 oktober 2014. Som sakkunniga förordnades den 10 november 2014 ämnessakkunnige Martin Munkelt, Justitiedepartementet och ämnessakkunnige Kristofer Jones, Försvarsdepartementet. Samma dag förordnades som experter säkerhetschefen Anne-Marie Eklund Löwinder, Stiftelsen för internetinfrastruktur, juristen Victoria Ekstedt, Post- och telestyrelsen och säkerhetsansvarige Tommy Svensson, Svenskt Näringsliv.

Utredningen har till sitt arbete knutit en referensgrupp med företrädare för olika myndigheter.

Som sekreterare i utredningen anställdes från och med den 22 januari 2014 numera rådmannen Ann-Kristin Lidström. Med verkan från och med den 1 maj 2014 entledigades Ann-Kristin Lidström från sitt uppdrag. Som huvudsekreterare anställdes från och med den 26 maj 2014 hovrättsassessorn Pernilla Arrland. Som utredningssekreterare anställdes från och med den 1 juni 2014 hovrättsassessorn Margareta Sandén.

Utredningen har antagit namnet NISU 2014.

Den 2 januari 2015 överlämnade utredningen sitt delbetänkande *Viktigt meddelande till allmänheten via mobil telefoni* (SOU 2014:92).

Utredningen får härmed överlämna sitt betänkande *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* (SOU 2015:23).

Stockholm i mars 2015

Erik O. Wennerström

/Margareta Sandén
Pernilla Arrland

Innehåll

Bilagor

Sammanfattning

Strategi och åtgärder i korthet

Utredningen föreslår en strategi för informations- och cybersäkerhet i staten. Strategin har sex mål:

att stärka styrning och tillsyn inom området,

att staten ska ställa tydliga krav vid upphandling på it-området,

att statliga myndigheter ska kommunicera säkert,

att samtliga statliga myndigheter rapporterar it-incidenter,

att arbetet med att förebygga och bekämpa it-relaterad brottslighet stärks och

att Sverige ska vara en stark internationell partner.

Strategin innehåller förslag till åtgärder inom de områden utredningen bedömt som strategiska för att uppnå en god informationssäkerhet i statsförvaltningen. Åtgärderna ska säkerställa att de statliga myndigheterna har ett gemensamt förhållningssätt till informationssäkerhetsfrågor och behovet av skyddad kommunikation samt säkra it-lösningar. Andra åtgärdsförslag innebär att det skapas förutsättningar för de brottsbekämpande myndigheterna att garantera samma skydd mot cyberbrottslighet som mot brottslighet i allmänhet. Det föreslås också att regeringen stärker och samordnar insatserna för att främja Sveriges ställning i internationella samarbeten om informations- och cybersäkerhet.

Uppdrag

Utredningen har haft regeringens uppdrag att föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system samt att föreslå övergripande mål för samhällets informationssäkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur. Enligt direktiven ska utredningen också klargöra begrepp som används inom informationssäkerhetsområdet och vid behov föreslå förtydligande eller alternativa benämningar och definitioner. I uppdraget har vidare ingått att redovisa statliga myndigheters ansvar och roller utifrån de uppgifter och uppdrag på informationssäkerhetsområdet som de har i dag.

Utredningens inriktning

Uppdraget har omfattat övergripande och strategiska åtgärder. Utredningens förslag ska ses i ljuset av att säkerhetsskyddslagen är under översyn och att åtgärdsförslagen inte avser att träffa säkerhetsskyddslagens tillämpningsområde. Vidare begränsas förslagen till det statliga området och till utformning av författningsreglering på förordnings- och föreskriftsnivå. Våra förslag syftar till att skapa en gemensam syn på en lägsta nivå av informationssäkerhet i staten och samtidigt höja denna.

Informationssäkerhet och cybersäkerhet

De två centrala begreppen i denna utredning är informationssäkerhet och cybersäkerhet. Informationssäkerhet innebär en strävan att skydda information så att den alltid finns när den behövs (tillgänglighet), att det går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet) och att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet). Informationssäkerhet omfattar såväl administrativa som tekniska åtgärder för att skydda information. För inrikes angelägenheter täcker begreppet informationssäkerhet flertalet av de i betänkandet föreslagna åtgärderna, medan cybersäkerhetsbegreppet gör sig mer

gällande när perspektivet avser svenskt förhållande gentemot andra hot. I de internationella policydiskussionerna har cybersecurity i allt större omfattning ersatt användandet av begreppet information security. Sverige bör i sina internationella relationer använda begreppet cybersäkerhet.

Myndigheter

Det finns flera statliga myndigheter med särskilda uppgifter eller uppdrag på informationssäkerhetsområdet, såväl nationellt som internationellt, och frågorna spänner över en mängd olika områden och nivåer. Utredningen har beskrivit myndigheternas ansvar och roller på informationssäkerhetsområdet. Myndigheten för samhällsskydd och beredskap, Post- och telestyrelsen, Försvarets radioanstalt, Säkerhetspolisen, Polismyndigheten, Försvarets materielverk och Försvarsmakten är myndigheter med särskilda uppgifter och särskilt ansvar inom informationssäkerhetsområdet. Myndigheterna ingår i samverkansgruppen för informationssäkerhet (SAMFI). I syfte att ytterligare formalisera, utveckla och fördjupa samordningen av informationssäkerhetsarbetet föreslår utredningen inom ramen för strategin att det inrättas ett Myndighetsråd för informationssäkerhet. Myndighetsrådet ska ha till uppgift att stödja och utveckla informationssäkerhetsarbetet i samhället.

Behovet av en strategi för staten

Hoten mot informations- och cybersäkerheten samt Sverige som nation kan inte hanteras enbart nationellt och kommer därför att kräva både sektorsövergripande och internationellt samarbete. Sveriges främsta och strategiska samarbetspartners uppfattar också problemet på samma sätt och manar i sina strategier till ökat samarbete.

Tidigare utredningar på området har i full enlighet med sina uppdrag sökt föreslå allomfattande strategier för hela samhället. Det finns anledning att från denna utrednings sida betona att behoven på informations- och cybersäkerhetens område är så omfattande i Sverige, att det inte behövs en, utan flera strategier. Vad som föreslås är därför det första steget, en första strategi för

statens informations- och cybersäkerhet som söker åtgärda de mest angelägna bristerna i statsförvaltningen. Först när detta är klart finns anledning och förutsättningar att gå vidare till större och mer specifika områden. Senare strategier bör omfatta bl.a. kompetensförsörjningen i samhället, forskning och utveckling, informationssäkerheten inom verksamheten hos landsting och kommuner, liksom försvaret av riket och dess oberoende mot antagonistiska hot med såväl defensiva som offensiva förmågor.

Den föreslagna strategin träffar statsförvaltningen på bredden och höjer, om den genomförs, den generella informations- och cybersäkerheten i statsförvaltningen, vilket främjar samhällets förutsättningar att förebygga och bekämpa de yttersta hoten mot rikets säkerhet.

Strategin vänder sig först och främst till regeringen, Regeringskansliet och till de statliga myndigheterna, och indirekt till den del av näringslivet och de organisationer som samverkar eller ingår affärsrelationer med staten. Den ska bidra till att reducera sårbarheten och uppnå en effektiv risknivå i statens olika informationssystem. Vidare ska strategin bidra till trygg elektronisk kommunikation i offentlig sektor och pålitliga nättjänster från offentlig sektor. Syftet med strategin är att ange grundläggande målsättningar, färdriktningar och arbetssätt för informationssäkerhet i svenska staten.

Förslag till strategi och åtgärder

Strategin anger sex strategiska mål och områden för informationssäkerhetsarbetet. Inom de strategiska områdena anges olika förslag till åtgärder.

Styrning och tillsyn av informationssäkerheten i staten stärks.

Förslag

En nationell styrmodell för informationssäkerhet etableras för att skapa ett systematiskt informationssäkerhetsarbete i statlig verksamhet. Förslaget avser i första hand de statliga myndigheterna och

ska vara normerande för dessa men styrmodellen kan på sikt utsträckas till att omfatta hela den offentliga sektorn.

Det bör inrättas ett statligt myndighetsråd för informationssäkerhet bestående av företrädare för de relevanta myndigheterna på området.

En ny förordning för statliga myndigheters informationssäkerhet bör införas för att tydliggöra ett ökat ansvar för det praktiska säkerhetsarbetet inom myndigheterna.

Tillsynen över den statliga sektorns informationssäkerhet bör samordnas och förstärkas. Myndigheten för samhällsskydd och beredskap ska utöva tillsyn över myndigheternas informationssäkerhetsarbete i enlighet med föreslagen förordning.

Myndigheternas internrevision behöver utvecklas till att inkludera uppföljning och kontroll av myndigheternas informationssäkerhet. Myndighetsledningens ansvar för att upprätthålla säkerhet i sin informationshantering bör förtydligas genom ett författningsreglerat rapporteringskrav.

Staten ställer tydliga krav som upphandlare av tjänster som innehåller informationshantering eller av it-tjänster.

Förslag

Statlig upphandling på it-området bör innehålla hänvisning till för staten gällande standarder och krav på certifiering i de situationer där säkerhetsnivåer har fastställts för respektive verksamhet.

Myndigheten för samhällsskydd och beredskap bör ges i uppdrag att ta fram minimikrav på säkerhet i vanligt förekommande it-produkter som används av statliga myndigheter.

Det bör införas ett krav på att rapportera vilken leverantör som en statlig myndighet har valt då ramavtal rörande it-lösningar används.

När det gäller tjänster och produkter som ska användas för kommunikation inom staten bör upphandlande myndighet överväga möjligheten att tillämpa lagen om upphandling på försvars- och säkerhetsområdet, om upphandling enligt lagen om offentlig upphandling inte medger att nödvändiga krav ställs.

Regeringen bör fördjupa dialogen mellan privata och offentliga aktörer samt utbildnings- och forskningsinstitutioner på informationssäkerhetsområdet.

Statliga myndigheter kommunicerar säkert.

Förslag

För att skapa en myndighetsgemensam infrastruktur för elektronisk kommunikation bör kommunikationssystemet Swedish Government Secure Intranet (SGSI) utvecklas. I ett första steg ansluts samtliga myndigheter som anges i bilagan till förordningen om krisberedskap och höjd beredskap till SGSI.

Under utbyggnaden av SGSI bör det vidtas åtgärder för att utveckla system för att upptäcka intrång och angrepp.

Synkronisering av tid och frekvens är viktig för att vissa funktioner i samhället ska fungera. Statliga myndigheter ska därför använda samma synkroniserade tidsskala för de tidsangivelser de använder i sina it-system.

Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk och Försvarsmakten bör ges i uppdrag att utveckla processen för säkra kryptografiska funktioner på basis av den av myndigheterna föreslagna nationella strategin med åtgärdsplan.

Samtliga statliga myndigheter rapporterar it-incidenter.

Förslag

Det bör inrättas ett system för obligatorisk it-incidentrapportering för samtliga statliga myndigheter. Detta ska anpassas till de krav som EU-direktivet om nät- och informationssäkerhet (NIS-direktivet) kommer att ställa. Ett system för obligatorisk it-incidentrapportering skulle bidra till förmågan att förebygga och hantera it-incidenter.

I syfte att förbereda införandet av ett system för obligatorisk it-incidentrapportering bör Myndigheten för samhällsskydd och beredskap få i uppdrag att utfärda verkställighetsföreskrifter om dess närmare utformning.

Myndigheten för samhällsskydd och beredskap bör ges i uppdrag att förse de statliga myndigheterna med information om bl.a. trender och utveckling avseende it-incidenter.

Förebyggande och bekämpande av it-relaterad brottslighet stärks.

Förslag

Arbetet med ratificering av Europarådets konvention om it-relaterad brottslighet, som Sverige undertecknade 2001, bör slutföras.

Det bör utredas om en tydligare reglering kan införas i offentlighets- och sekretesslagen rörande sekretess för uppgifter som utbyts vid samverkan mellan brottsbekämpande myndigheter och andra myndigheter inom informationssäkerhetsområdet.

Det bör göras en översyn av bestämmelserna om tvångsmedel i 27 och 28 kap. rättegångsbalken och övriga lagrum för att säkerställa att brottsbekämpande myndigheter kan bedriva sin förebyggande och utredande verksamhet i den digitala miljön.

Sverige ska vara en stark internationell partner.

Förslag

Regeringen bör säkerställa att Sverige agerar kraftfullt och konsistent i samtliga internationella och regionala fora av relevans genom att stärka samordningen av både Regeringskansliets och myndigheternas internationella kontakter.

Konsekvenser av förslagen

Utredningens förslag innebär en höjd ambitionsnivå för samhällets informationssäkerhet och vissa av förslagen medför ökade kostnader. Eftersom informationssäkerhet normalt anses ingå i kostnaderna för respektive verksamhet är utgångspunkten att flera förslag bör bäras av respektive verksamheter. Den största kostnaden gäller framför allt den utökade rollen för Myndigheten för samhällsskydd och beredskap, vilket kräver en anslagshöjning. Detta behov kan täckas genom omdisponeringar inom utgiftsområde 06 Försvar och samhällets krisberedskap eller hänföras till en ny förvaltningspolitisk inriktning av statsförvaltningens arbete och därmed hänförlig till utgiftsområde 02 Samhällsekonomi och förvaltning. Likaså kan övervägas om delar av de kostnadsökningar som beskrivs är att hänföra till de krav på ökad digitalisering som hanteras inom utgiftsområde 22 Kommunikationer. Ett sista förslag är om informations- och cybersäkerhet har kommit att bli en så central del av statsförvaltningen att det förtjänar ett eget och nytt utgiftsområde.

Cyber security in Sweden – strategy and measures for secure information in central government

The Inquiry was instructed to propose a national strategy for the handling and transfer of information in electronic communications networks and IT systems, and to propose overall objectives for society's information security work and how Sweden is to maintain the security and integrity of vital public IT infrastructure.

Need for a strategy

The threats against cyber security, and Sweden as a nation, cannot be dealt with nationally and will therefore require both cross-sectoral and international cooperation. Sweden's foremost and strategic cooperation partners also view the problem in the same way, calling in their strategies for greater cooperation.

In light of this perspective, Sweden must continue to build its national capacity and strengthen the protection not only of vital infrastructure, but also of the entire central government administration so as to be able to tackle and avert all threats against central government information assets.

Only with this approach will Sweden, over time, be able to secure the many advantages offered by the digital society to individuals, central government and businesses in the form of economic growth, innovation and national security.

A strategy for central government

Previous proposed strategies have tried to remedy all problems and challenges in the whole of society in one context, which creates an overwhelming challenge.

The Inquiry's remit includes proposing a strategy for the handling and transfer of information in electronic communications networks and IT systems, a national strategy that the Inquiry considers should be adopted by the Government. There is reason for the Inquiry to stress that the needs in the area of cyber security in Sweden are extensive and it seems rational to accept that Sweden needs not one but several strategies. The proposals below are therefore merely the first step – an initial strategy that seeks to remedy the most urgent shortcomings in central government administration. Only when this is finished will there be reason – and necessary conditions – to move on to larger and more specific areas. One such consecutive area is covered by the national security protection legislation, which is currently under reform. This proposed strategy takes a broad approach to central government administration and would, if implemented, improve general cyber security in central government administration, to the advantage of society's resources for preventing and combating the most significant threats to the security of the realm. Consequently, these resources can then be targeted in a more undivided fashion against these threats.

The Inquiry considers that to be an effective, credible, leading and demanding force in society, central government must devote its energies to creating security within the sphere of central government. Therefore, the strategy proposed here is devoted to achieving this exclusively. Only after this has been achieved will central government be in a position to engage society as a whole. Subsequent strategies should cover: skills supply with regard to cyber security in society as a whole; national research and development on cyber security; cyber security within the activities of county councils and municipalities; and the defence of the realm and its independence vis-à-vis antagonistic threats using both defensive and offensive capabilities.

Implementation of the strategy

In the Inquiry's view, a national cyber security strategy should have a medium-term perspective that can lay the foundation for measures for two to three years ahead. The strategy is primarily intended for the Government, the Government Offices and government agencies, and indirectly for the section of the business sector and the organisations that collaborate with or enter into business relations with central government.

The strategy is targeted so as to lay the foundation for political decisions and priorities in the area of cyber security, and to improve the coordination of society's cyber security work. If implemented, the strategy would help to reduce vulnerability and achieve an effective risk level in the various information systems of central government. It would also contribute to secure electronic communications in the public sector and would secure reliable online public sector services.

Cyber security is a support activity to improve the quality of central government functions while also being a necessary activity to guarantee that legislation from the Government and the Parliament is actually implemented. Essentially, it is about protecting the fundamental values and goals in our society, such as democracy, personal privacy, economic growth and political stability.

The objective is to achieve a high level of cyber security in central government administration that promotes:

- the rights and freedoms of citizens, and personal privacy;
- the functionality, efficiency and effectiveness, and quality of central government administration;
- law enforcement;
- the ability of central government to prevent and deal with serious disruptions and crises; and
- business sector growth, through central government being skilled and clear in formulating requirements.

The strategy involves a series of initiatives to strengthen cyber security in Sweden. The initiatives fall into six areas.

Purpose and content of the strategy

The purpose of the proposed strategy is to set out fundamental objectives, directions and working methods for cyber security in Swedish central government. A multitude of different central government actors need a common understanding of cyber security, what its purpose is and how future security measures can be targeted and designed. Those primarily affected are the Government and the heads of government agencies who have to take the decisions needed to implement the strategy in their activities, but also those who work on cyber security at various levels, decision-makers in public administration and in those sections of the business sector that sell goods and services to it; those who work on IT and general security, but also individual citizens who are reliant on central government handling information about them and for them in a secure way.

The strategy sets out six strategic objectives and strategic areas for cyber security. Various proposed measures are given within each strategic area.

1. *Governance and oversight of cyber security in central government shall be strengthened.*

   A national governance model for cyber security in society will be established.

   The Government will establish a government agency council for cyber security comprising representatives of the relevant government agencies.

   A new ordinance on government agencies' cyber security will be introduced.

   Cyber security oversight of the central government sector will be coordinated and strengthened. The Swedish Civil Contingencies Agency will be given a general oversight mandate for government agencies' cyber security. Sectoral oversight will be reviewed.

   Cyber security auditing will be developed. Management responsibility at government agencies for maintaining security in their information management shall be enhanced through a reporting requirement, regulated by statute.

2. *Central government shall state clear security requirements as a procurer of IT products and services, and services involving the handling of information.*

   Central government procurement shall contain references to standards and certification requirements that apply to central government in situations where security levels have been established for each activity.

   The Swedish Civil Contingencies Agency is mandated to establish minimum requirements for security in commonly used IT products used by government agencies.

   A requirement will be introduced, whereby a government agency must report which contractor it has chosen when framework agreements for IT solutions have been used.

   With regard to services and products for use in communication in central government, the procuring agency should consider the possibility of applying the Defence and Security Procurement Act if procurement under the Public Procurement Act permits insufficient security requirements.

   The Government will deepen the dialogue between private and public actors, as well as education and research institutions in the area.

3. *Government agencies shall communicate in a secure way.*

   All government agencies listed in the annex to the Emergency Management and Heightened Alert Ordinance will be connected to the Swedish Government Secure Intranet (SGSI).

   During the expansion of SGSI, appropriate measures will be taken to develop sensor technology.

   All agencies are to use the same synchronized time scale for the time they use in their IT systems.

   The Government will instruct the Swedish Civil Contingencies Agency, the National Defence Radio Establishment, the Defence Materiel Administration and the Swedish Armed Forces to develop the process for securing cryptographic functions.

4. *All government agencies shall report IT incidents to create a basis for improved knowledge and status reports.*

   Systems will be introduced for obligatory IT incident reporting for all government agencies. These will be adapted to the contents of the EU Directive on Network and Information Security (NIS Directive).

   The Swedish Civil Contingencies Agency will be instructed to issue implementation provisions to prepare for obligatory IT incident reporting.

   Government agencies will be provided with status reports regarding IT incidents.

5. *The prevention of and fight against cybercrime shall be strengthened.*

   The ratification of the Council of Europe Convention on Cybercrime should be concluded.

   It should be considered whether a regulation can be introduced in the Public Access to Information and Secrecy Act whereby secrecy can be maintained regarding information that is exchanged between law enforcement agencies and other agencies involved in law enforcement work within the area of cyber security.

   A review of the provisions on coercive measures in Chapters 27 and 28 of the Swedish Code of Judicial Procedure and other sections of law shall be conducted to ensure that law enforcement agencies are able to carry out their activities in the digital environment.

6. *Sweden shall be a strong international partner.*

   The Government will ensure that Sweden takes resolute and consistent action in all relevant international and regional forums.

1 Författningsförslag

1.1 Förslag till förordning för statliga myndigheters informationssäkerhet

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § Bestämmelserna i denna förordning syftar till att främja säker informationshantering i samhället genom att säkerställa att statliga myndigheters informationshantering uppfyller sådana krav på informationssäkerhet att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

2 § Denna förordning innehåller föreskrifter som dels ställer krav på myndigheternas informationssäkerhetsarbete, dels reglerar det nationella myndighetsrådets uppgifter.

3 § Bestämmelserna i 11, 19 och 20 §§ gäller för statliga myndigheter under regeringen, med undantag av Regeringskansliet, kommittéväsendet och Försvarsmakten. För utlandsmyndigheterna tillämpas bestämmelserna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet.

Definitioner

4 § I denna förordning avses med

informationssäkerhet	förmågan att upprätthålla konfidentialitet, riktighet, tillgänglighet och spårbarhet i sin informationshantering,
samhällsviktig verksamhet	verksamhet som uppfyller det ena eller båda av följande villkor: 1. ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället, 2. verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

Myndighetens informationssäkerhetsarbete

5 § Varje myndighet ansvarar för att, genom ett risk- och sårbarhetsbaserat, systematiskt och processinriktat arbetssätt, upprätthålla en tillräcklig nivå av informationssäkerhet för den information de ansvarar för eller hanterar i tjänster som myndigheten levererar till en annan organisation. Myndigheten ska i sitt informationssäkerhetsarbete särskilt beakta behovet av ledningssystem och etablerade standarder för informationssäkerhet.

6 § Det ska i myndighetens ledning finnas en person med ett utpekat ansvar för informationssäkerhetsfrågor.

Myndigheten ska utse en eller flera personer som leder och samordnar det praktiska arbetet med informationssäkerhet, samt i övrigt

tydliggöra roller och ansvar för informationssäkerhetsarbetet i organisationen.

Myndigheten ska aktivt, genom utbildning och övning, verka för att en god säkerhetskultur etableras i organisationen.

7 § Myndigheten ska kartlägga sina informationsprocesser och klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Inträffade it-incidenter i organisationen ska kunna identifieras och hanteras.

Beroende på klassning samt identifierade hot, risker och sårbarheter ska lämpliga säkerhetsåtgärder vidtas. För offentlig förvaltning utvecklade krav- och skyddsnivåer ska följas i detta arbete.

8 § Myndigheten ska, med stöd av risk- och sårbarhetsanalyser, välja och använda säkra it-produkter vid hantering av information där bristande informationssäkerhet kan medföra en betydande försämring av myndighetens förmåga att bedriva sin verksamhet. I de fall säkra it-produkter finns utpekade i verkställighetsföreskrifter som meddelats med stöd av denna förordning ska dessa användas.

9 § Myndigheten ska följa upp sitt eget informationssäkerhetsarbete och i en årlig plan dokumentera de bedömningar som görs avseende hot, risker och sårbarheter samt redogöra för arbetet som bedrivs i enlighet med kraven i 7–8 §§.

Myndigheten ska med stöd av kontinuitetsplanering upprätthålla en sådan nivå av informationssäkerhet att myndigheten har god förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap. I kontinuitetshanteringsarbetet ska sådana hot, risker och sårbarheter som avses i 7 § 3 st beaktas.

10 § Kraven i 5–9 §§ gäller endast i tillämpliga delar sådana myndigheter vars informationshantering eller vars informationssäkerhetsarbete administreras av en annan myndighet, en så kallad värdmyndighet.

En sådan värdmyndighet som avses i första stycket ska informera den anlitande myndigheten om inträffade it-incidenter som har eller kan ha påverkat säkerheten hos den anlitande myndighetens information.

Särskilda krav på informationssäkerhetsarbete

11 § De myndigheter som har ett särskilt ansvar för krisberedskapen enligt 11 § förordning (2006:942) om krisberedskap och höjd beredskap och de myndigheter som Myndigheten för samhällsskydd och beredskap beslutar i enskilda fall, är skyldiga att uppfylla särskilda krav på informationssäkerhet rörande

– användning av säkra kommunikationsnät,
– användning av sensorsystem för it-incidentidentifiering, och
– kompetens för informationssäkerhetschef eller motsvarande.

Säkra kryptografiska funktioner

12 § Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut, Fortifikationsverket, Totalförsvarets rekryteringsmyndighet, Myndigheten för samhällsskydd och beredskap och Regeringskansliet ska ha säkra kryptografiska funktioner.

Myndigheten för samhällsskydd och beredskap beslutar vilka övriga myndigheter som ska ha säkra kryptografiska funktioner.

Myndigheten för samhällsskydd och beredskap beslutar även vilka företag som efter överenskommelse ska få tillgång till säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap får därutöver ingå avtal om tilldelning med kommuner och organisationer som har behov av säkra kryptografiska funktioner.

13 § Försvarsmakten svarar för att Försvarsmakten, Försvarets materielverk, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet och Fortifikationsverket tilldelas säkra kryptografiska funktioner. Försvarets radioanstalt svarar för att övriga som enligt 12 § ska ha säkra kryptografiska funktioner tilldelas sådana.

14 § Myndigheter som tilldelats säkra kryptografiska funktioner ska under normal kontorstid kunna ta emot och sända krypterade meddelanden.

När en situation av den omfattning som avses i 9 § andra stycket förordning (2006:942) om krisberedskap och höjd beredskap upp-

står och vid höjd beredskap ska myndigheterna kunna ta emot och sända krypterade meddelanden även under icke kontorstid.

Myndigheten för samhällsskydd och beredskap, eller annars, efter samråd med Myndigheten för samhällsskydd och beredskap, annan myndighet som har behov av information, ska ingå överenskommelse med sådant företag, sådan kommun eller organisation som tilldelats system med stöd av 12 § tredje stycket om när krypterade meddelanden ska kunna tas emot och sändas.

Upphandling och utveckling av it-system och it-produkter

15 § I samband med upphandling och utveckling av it-system eller it-produkter ska myndigheten i förhållande till leverantören klarlägga ansvar och roller för informationssäkerhetsarbetet. Myndigheten ska även fastställa processer för hur säkerhetskrav ska hanteras och hur uppföljning ska ske.

Upphandlingen eller utvecklingen ska föregås av informationsklassning och riskanalys av berörd information. Resultatet av klassningen och riskanalysen ska vara styrande för utformningen av säkerhetskrav som ställs vid upphandling eller utveckling.

Kraven i första och andra stycket gäller även vid anslutning till myndighetsgemensamma tjänster för e-förvaltning eller liknande syfte.

En myndighet ska endast uppdra åt någon annan att hantera myndighetens information om hanteringen kan ske med tillräcklig säkerhet och enligt denna författning. I detta ingår att försäkra sig om att it-incidenter som har eller kan ha påverkat säkerheten rapporteras till myndigheten.

16 § I samband med upphandling av it-produkter som är avsedda att användas i samhällsviktig verksamhet som myndigheten bedriver eller ansvarar för ska, då sådana finns tillgängliga, endast säkra och certifierade it-produkter användas. I de fall säkra it-produkter finns utpekade i verkställighetsföreskrifter ska dessa användas.

It-incidentrapportering

17 § En myndighet ska till Myndigheten för samhällsskydd och beredskap skyndsamt rapportera it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten levererar till en annan organisation.

För incidenter som ska anmälas till en tillsynsmyndighet enligt bestämmelserna i 10 a § säkerhetsskyddsförordningen (1996:633) gäller rapporteringsplikten enligt första stycket inte förrän tillsynsmyndigheten har meddelat den rapporteringspliktiga myndigheten att incidenten inte längre är föremål för behandling hos tillsynsmyndigheten.

Tillsyn, föreskrifter och myndighetsrådets uppgifter

18 § I Myndighetsrådet för informationssäkerhet ska representanter för myndigheter med särskilda uppgifter på informationssäkerhetsområdet ingå. Myndighetsrådet har till uppgift att stödja och utveckla informationssäkerhetsarbetet i samhället. I detta ingår bland annat att

- utgöra en gemensam beredning- och remissinstans på informationssäkerhetsområdet,
- bidra med stöd rörande informationssäkerhetsfrågor vid utfärdandet av föreskrifter på informationssäkerhetsområdet,
- förvalta och utveckla tillämpliga krav och kontrollordningar i bl.a. standarder för produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet,
- bistå med expertkompetens i samband med upphandling av tjänster och produkter på informationssäkerhetsområdet, och
- utveckla krav- och skyddsnivåer.

Myndigheten för samhällsskydd och beredskap ska tillhandahålla en kanslifunktion för rådet.

Myndighetsrådet ska vid behov inrätta arbetsgrupper.

19 § Myndigheten för samhällsskydd och beredskap ska utöva tillsyn över statliga myndigheters informationssäkerhetsarbete i enlighet med denna förordning, med undantag för sådant arbete som redan är föremål för tillsyn i enlighet med 39 § säkerhetsskyddsförordningen (1996:633).

20 § Myndigheten för samhällsskydd och beredskap får

1. meddela de föreskrifter som behövs för verkställigheten av de allmänna och särskilda krav på statliga myndigheters informationssäkerhetsarbete som avses i 5–11 och 15 §§, med beaktande av nationell och internationell standard,
2. meddela de ytterligare föreskrifter som behövs för verkställigheten av 14 §, utom i fråga om Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut och Fortifikationsverket,
3. meddela de föreskrifter som behövs för verkställigheten av 16 § utom i fråga om myndigheter för vilka Försvarsmakten eller Säkerhetspolisen meddelar motsvarande föreskrifter enligt 44 § säkerhetsskyddsförordningen,
4. meddela de ytterligare föreskrifter som behövs för verkställigheten av sådan it-incidentrapportering som avses i 17 §.

Denna förordning träder i kraft den 1 januari 2016.

1.2 Förslag till förordning om ändring i säkerhetsskyddsförordningen (1996:633)

Härigenom föreslås att det i säkerhetsskyddsförordningen (1996:633) ska införas en ny bestämmelse, 10 a §, av följande lydelse.

10 a §

Om det inträffar en it-incident som allvarligt kan påverka säkerheten i ett informationssystem där hemliga uppgifter behandlas i en omfattning som inte är ringa ska den myndighet som berörs av incidenten skyndsamt anmäla incidenten till den myndighet som enligt 39 § utövar tillsyn över säkerhetsskyddet.

Denna förordning träder i kraft den 1 januari 2016.

2 Uppdragets genomförande och begrepp

2.1 Uppdraget

Enligt regeringens direktiv (dir. 2013:110) ska utredningen

- föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system,
- föreslå övergripande mål för samhällets informationssäkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur,
- klargöra begrepp som används inom informationssäkerhetsområdet och vid behov föreslå förtydligande eller alternativa benämningar och definitioner, särskilt av sådana som används i förslaget till nationell strategi, och
- med utgångspunkt i uppdraget redovisa statliga myndigheters ansvar och roller utifrån de uppgifter och uppdrag på informationssäkerhetsområdet som de har i dag.

Direktiven finns i sin helhet i bilaga 1.

2.2 Uppdragets genomförande

Arbetet inleddes i januari 2014. Totalt har utredningen haft fem utredningssammanträden med experter och sakkunniga varav ett internat. Utredningen har varit angelägen om att ha en öppen dialog och samverka med myndigheter och organisationer som på olika sätt kan beröras och ha intresse av vårt arbete samt bidra med kunskap. Vi har därför fortlöpande haft möten och kontakter med olika företrädare. Syftet har varit att både informera om utred-

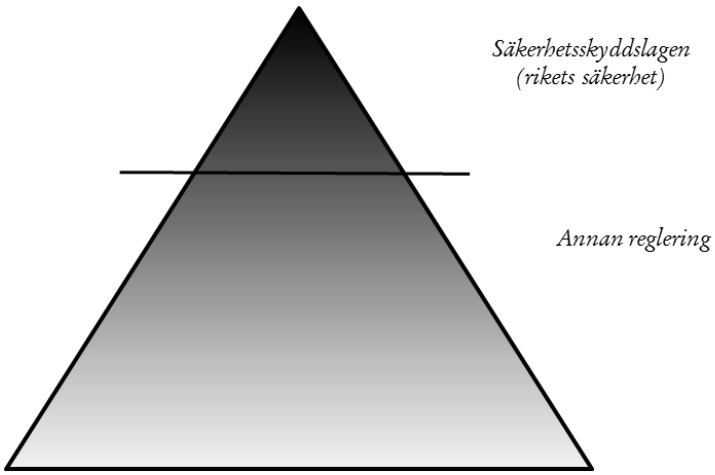
ningens arbete och att inhämta synpunkter. Utredningen har därför som stöd i arbetet också tillsatt en särskild referensgrupp med företrädare för närmast berörda myndigheter, Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen och Säkerhetspolisen. Möten med referensgruppen har hållits vid fyra tillfällen. Referensgruppens ledamöter har dessutom beretts tillfällen att lämna kommentarer på texter till betänkandet, fram till tidpunkten då betänkandetexten förbereddes för slutjustering, varefter referensgruppen informerats. Utöver detta har utredningen vid flera tillfällen träffat berörda myndigheter för möten och studiebesök. Därtill har vi gjort besök vid Bodens kommun och Luleå tekniska universitet och haft möten och seminarier med Centrum för asymmetriska hot- och terrorismstudier (CATS) vid Försvarshögskolan, Totalförsvarets forskningsinstitut (FOI), Riksrevisionen, L M Ericsson, Säkerhets- och försvarsföretagen (SOFF) och Sveriges Kommuner och Landsting. Utredningen har också deltagit i den årliga konferensen om informationssäkerhet för offentlig sektor som anordnas av Myndigheten för samhällsskydd och beredskap i samarbete med övriga SAMFI-myndigheter (se avsnitt 7.5.6). Utredningen har också deltagit i ett arrangemang av AFCEA (Armed Forces Communications and Electronics Association). Vidare har vi haft ett möte med av Post- och telestyrelsen inbjudna teleoperatörer. Utredningen har också genom studiebesök och möten studerat hur arbetet med informations- och cybersäkerhetsfrågor bedrivs i Finland, Danmark, Estland, Italien, Österrike och USA. Vi har även samrått med Utredningen om säkerhetsskyddslagen (Ju 2011:14)och haft kontakt med Utredningen om effektivare användning av statens bredbandsinfrastruktur (N 2014:05).

2.3 Utredningens inriktning

Ett sätt att beskriva lagstiftarens reglering av samhället, såsom det på olika sätt berörs av och har ansvar för informationssäkerhet, är att likna det vid en pyramid, vars bas är alla individer och företag som bor och verkar i landet. Här är regleringen sparsam. Mellansegmentet utgörs av det allmänna, dvs. stat, landsting och

kommuner. Här är regleringen betydligt tätare. I toppen av pyramiden återfinns de delar av statsapparaten som har ansvar för att i fred såväl som i ofred skydda rikets säkerhet. I denna del är regleringen omfattande. Figuren nedan söker beskriva detta.

Figur 1 Principskiss över regleringen av samhällets informationssäkerhet



Toppen av pyramiden är redan högst reglerad och därför mycket säkerhetsmedveten och har sedan länge vidtagit nödvändiga åtgärder för att skydda sin information och sina kommunikationer. De utmaningar som kvarstår i pyramidens topp söker denna utredning inte föreslå lösningar på, utan hänvisar i de delarna till betänkandet från Utredningen om säkerhetsskyddslagen (Ju 2011:14). Inte heller söker betänkandets åtgärder fånga in behoven hos alla och envar, hos företag, kommunala förvaltningar, skolor, sjukhus och hos andra som återfinns i pyramidens fot eller den del av mellansegmentet som inte är statligt. Betänkandets förslag tar endast sikte på den statliga delen – som återfinns i pyramidens mellansegment.

Det är även med dessa begränsningar en tillräckligt stor uppgift – görlig, men på intet sätt lätt. Det är en nödvändig uppgift – staten kan inte bli ett ledande exempel eller ett stöd eller en trovärdig kravställare gentemot resten av samhället förrän den åtgärdat det som inte fungerar optimalt men som staten samtidigt skulle kunna

åtgärda. När staten väl genomfört de föreslagna åtgärderna och nått målen i strategin, då uppstår också positiva effekter i pyramidens övriga delar; när exempelvis staten blivit en bättre kravställare i upphandlingshänseende kommer detta att kunna förenkla också t.ex. kommunal upphandling på motsvarande område och om staten under flera år konsekvent upphandlat med hänvisning till vissa standarder kommer detta sannolikt att med marknadskrafternas hjälp ha pressat priserna på området också till gagn för landsting och kommuner när de hänvisar till samma standarder. Positiva effekter uppstår också i pyramidens topp; till skillnad från dagsläget kommer i en framtid där strategins mål är uppfyllda kraft och resurser avdelade för rikets säkerhet odelat fokuseras i vetskapen om att lägsta säkerhetsnivån i staten i stort har höjts till en betryggande nivå.

Även med mål som avgränsats på sätt som framgår ovan så kommer de genomförda förslagen att få långtgående konsekvenser utanför den statliga sektorn. Så är fallet med allt som avser upphandling men även vad avser kritisk infrastruktur som är föremål för statens ansträngningar som de beskrivs i betänkandet. Framförallt gäller det infrastruktur för elektronisk kommunikation som i huvudsak är privat. Utredningen utvecklar dessa frågor och hur vi ser på statens ansvar inom informationssäkerhetsområdet i avsnitt 3.5.2.

Utredningen ska enligt direktiven hålla sig informerad om och beakta Utredningen om säkerhetsskyddslagen (Ju 2011:14). Det uppdraget redovisas inom kort. I den utredningens direktiv *En modern säkerhetsskyddslag* (dir. 2011:94) anger regeringen att det inte längre framstår som ändamålsenligt att säkerhetsskyddslagens bestämmelser om informationssäkerhet avgränsas till åtgärder som behövs för att skydda uppgifter som omfattas av sekretess och som rör rikets säkerhet. Utredarens uppdrag har därför varit att 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.

Informationssäkerhet enligt säkerhetsskyddslagen avser åtgärder för att förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet (hemliga uppgifter) inte obehörigen röjs, ändras eller förstörs (7 § första stycket 1 säkerhetsskydds-

lagen). Därutöver finns i 9 § säkerhetsskyddslagen en bestämmelse som uttryckligen anger att behovet av skydd vid automatisk informationsbehandling ska beaktas särskilt vid utformningen av informationssäkerheten.

Ändamålen med säkerhetsskyddslagen är 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 (toppen av pyramiden). Lagen ger därför små möjligheter att vidta åtgärder för att skydda statens it-systemen generellt. 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.

Denna utrednings uppdrag (NISU 2014) har omfattat övergripande och strategiska åtgärder för hantering och överföring av information i elektroniska kommunikationsnät och it-system. Utredningens förslag ska ses i ljuset av att säkerhetsskyddslagen är under översyn och att åtgärdsförslagen inte avser att träffa säkerhetsskyddslagens tillämpningsområde. Vidare begränsas förslagen till det statliga området och till utformning av författningsreglering på förordnings- och föreskriftsnivå. Våra förslag syftar vidare till att skapa en gemensam syn på en lägsta nivå av informationssäkerhet i staten och samtidigt höja denna.

I diskussioner rörande informationssäkerhet aktualiseras inte sällan integritetsfrågan. På motsvarande sätt berörs informationssäkerhet ofta i integritetsdiskussioner. Flera verksamheter behandlar idag stora mängder av personuppgifter och annan information som är av känslig karaktär. Förutsättningen för att dessa organisationer ska kunna upprätthålla en hög grad av tillit bland medborgarna är att de kan skydda den känsliga informationen från otillbörlig åtkomst.

Vårt uppdrag har varit att föreslå de övergripande målen som ska utformas så att de ger mål, riktlinjer för och prioriteringar som kan ligga till grund för myndigheternas eget informationssäkerhetsarbete. Utredningen föreslår därför inga åtgärder som reglerar det individuella förhållandet till staten. Förslagen handlar om det kollektiva skyddet för information som staten ska kunna erbjuda. I

de delar utredningens förslag skulle kunna påverka den enskildes personliga integritet föreslår utredningen ytterligare utredningsåtgärder för att väga in sådana aspekter.

2.4 Klargörande av begrepp

I utredningens direktiv anges att det finns ett behov av att definiera begrepp och reda ut hur de förhåller sig till varandra samt vid behov ensa dessa begrepp för att undvika missförstånd. Vårt uppdrag har därför varit att klargöra begrepp. Under utredningens arbete har vi funnit att behovet framförallt gör sig gällande beträffande begreppen informationssäkerhet, cybersäkerhet och informations- och cybersäkerhet. I detta avsnitt förtydligas dessa begrepp.

2.4.1 Begrepp på området

En grundläggande definitionsfråga för hela den svenska informationssäkerhetsnomenklaturen handlar just om innebörden av det svenska begreppet ”informationssäkerhet”. På engelska är detta begrepp uppdelat i två betydelser dels ”Information Security” som utgår från ett tekniskt perspektiv och återspeglas i ISO 27001-standarden, dels i ”Information Assurance” som utgår från ett nationellt säkerhetsperspektiv och där även organisation och policy ingår. I tidigare utredningsarbeten gjordes försök att särskilja det senare begreppet från det förra genom att introducera termen ”informationssäkring”, vilket också infördes i SIS-nomenklatur. Begreppet – liksom den förenklade varianten ”övergripande informationssäkerhet” – vann aldrig någon uppslutning i det offentliga Sverige då det ansågs för komplicerat att beskriva. Följden har dock blivit olyckliga sammanblandningar i begreppens innebörd – inte minst i internationella sammanhang.

Cybersäkerhetsbegreppet är mer strategiskt och fokuserar mer på nationella och internationella nätverk. Därmed har cybersäkerhet en större internationell räckvidd med t.ex. folkrättsliga frågeställningar och normer på cyberområdet än det mer tekniska informationssäkerhetsbegreppet. Det senare har en större tyngdpunkt mot hård- och mjukvara samt standardisering.

Motivet för fokus mot cybersäkerhet är att det är på detta område som statsmaktsperspektivet behöver utvecklas då frågeställningarna ligger ovanför myndigheternas ansvarsområden, samt att avdömningar mellan olika sektorsstrategier kan behöva göras inom ramen för ett svenskt koherent nationellt förhållningssätt gentemot EU och andra internationella organ.

2.4.2 Terminologiutveckling gällande cyberbegreppet

I takt med att internationella systemet i allt större utsträckning påverkas av informations- och kommunikationsteknologifrågor har också nya begrepp och delvis förändrade synsätt utvecklats. I det internationella engelskspråkiga samtalet används sedan längre tid en terminologi med förledet cyber, t.ex. cyber space affairs, cyber governance, cybersecurity och cyber defense. I de internationella policydiskussionerna har cybersecurity i allt större omfattning ersatt användandet av begreppet information security, även om de grundläggande tekniska utgångspunkterna i princip är desamma. En mycket viktig skillnad utgörs dock av uppfattningen att vissa av de stater och internationella organisationer som vidhåller bruket av begreppet information security i internationella policysammanhang har en annan syn på frågan om ett fritt och öppet informationsflöde på internet. I vissa fall gäller det även formerna för internets styrning och förvaltning. Vissa av dessa aktörer tenderar till att förbehålla sig rätten att betrakta information per se som en säkerhetsrisk mot vilken säkerhetsåtgärder kan behöva vidtas.

Sverige och en rad andra länder delar inte denna syn. Ett viktigt sätt att manifestera denna hållning är att inte använda begreppet information security, som i dessa sammanhang alltså närmast har kommit att bli ett diplomatiskt kodord för en mer repressiv inställning till informationsfrihet. Det ska dock noteras att i andra sammanhang kan begreppet information security vara relevant så som när man talar om uppgifter som är av sådan känslig karaktär att de skyddas genom reglering i toppen av pyramiden (figur 1), dvs. motsvarande säkerhetsskyddslagens tillämpningsområde. Exempel på sådana sammanhang är internationellt säkerhetssamarbete som bygger på rådets säkerhetsbestämmelser eller på internationella säkerhetsskyddsåtaganden.

Även i frånvaro av formella konsensusdefinitioner tycks det finnas en bred – om inte helt samstämmig – anpassning till begrepp med förledet cyber, vilket också färgar av sig inom andra språkområden än det engelska.

I säkerhets- och utrikespolitiska sammanhang används därför i praktiken begrepp som cybersäkerhet, cyberrymden, cyberpolitik och liknande, även om dessa för närvarande saknar formella definitioner.

2.4.3 Informationssäkerhet och cybersäkerhet

De två centrala begreppen i denna utredning och den del av verkligheten den söker beskriva är informationssäkerhet och cybersäkerhet. Informationssäkerhet innebär en strävan att skydda information så:

- att den alltid finns när den behövs (tillgänglighet)
- att det går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den (konfidentialitet) och
- att det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet)

Informationssäkerhet omfattar såväl administrativa åtgärder för att skydda information (såsom föreskrifter, behörighetsrutiner, etc.) som tekniska åtgärder (såsom it-säkerhet och fysisk inpasseringskontroll).

Standarder är centrala i ett systematiskt informationssäkerhetsarbete. De anger krav och riktlinjer som är användbara för alla typer av organisationer. Verksamheter får möjligheter att arbeta utifrån beprövade erfarenheter och då enklare skapa förutsättningar för bättre säkerhet.

Cybersäkerhet omfattar, enligt den definition EU använt i sin Cybersäkerhetsstrategi från 2013 de mekanismer och åtgärder som används för att skydda cyberdomänen, både civilt och militärt, mot de hot som är förknippade med eller som kan skada dess ömsesidigt beroende nätverk och informationsinfrastruktur. Cyber-

säkerhet strävar efter att bevara nätverkens och infrastrukturens tillgänglighet och integritet samt konfidentialiteten hos informationen däri.

> Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. [1]

Cybersäkerhet definieras vid International Telecommunications Union (ITU) enligt följande.

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: • Availability • Integrity, which may include authenticity and non-repudiation • Confidentiality.[2]

Begreppen används ofta utan särskillnad och i daglig hantering leder detta sällan till missförstånd. För svensk myndighetsintern verksamhet och med den sammanhängande normgivning går det utan tvekan bra att även framdeles använda begreppet informationssäkerhet, medan större kontextuell precision är tillrådlig så fort en internationell dimension gör sig gällande; när ett större perspektiv ska anläggas som räknar in samarbete med andra länder och skyddsåtgärder mot kända eller okända antagonistiska aktörer är cyberförstavelsen inte bara politiskt utan också tekniskt att föredra. Utredningen är därför av uppfattningen att Sverige i sina internationella relationer bör använda begreppet cybersäkerhet,

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, dokument JOIN(2013) 1 final, Brussels, 7.2.2013, sid. 3, fotnot 4.
[2] Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity.

såvitt det inte i viss diskussion krävs t.ex. en till viss standard relaterad teknisk precision.

För inrikes angelägenheter – dvs. där det är informationen snarare än landet, staten eller rättsordningen som är skyddsobjekt – täcker begreppet informationssäkerhet flertalet av de i betänkandet föreslagna åtgärderna, medan cybersäkerhetsbegreppet gör sig mer gällande när perspektivet avser svenskt förhållande gentemot andra hot. Begreppet ”informations- och cybersäkerhet” bör användas när båda delarna åsyftas, såsom skett t.ex. vid Myndigheten för samhällsskydd och beredskap där ett verksamhetsområde för informations- och cybersäkerhet bildats.

Utredningen behandlar samtliga de ovan beskrivna situationerna och följaktligen används också båda begreppen i betänkandet. Utredningens bedömning är dock att behovet av exakthet i begreppsanvändningen gör sig mer eller mindre tydligt gällande i olika sammanhang. Detta innebär att i de fall utredningen lämnar förslag till åtgärder som innebär olika former av krav behöver begreppen användas med noggrannhet. I de fall det inte föreligger risk för missförstånd ställs lägre krav på begreppsanvändningen. Det betyder att i de delar av betänkandet där vi redogör för andra aktörers erfarenheter har vi endast återgett begreppen så som det beskrivits för oss.

3 Allmänna utgångspunkter

3.1 Inledning

I dagens samhälle hanteras information i elektroniska kommunikationsnät och it-system i större omfattning än någonsin. Det är av största vikt att alla aktörer i samhället kan känna tillit till denna information och hanteringen av den på alla nivåer i samhället. Digitaliseringen innebär utöver fantastiska möjligheter för utveckling och tillväxt i samhället, även en ökad sårbarhet. Arbetet med informationssäkerhet är en angelägenhet för alla. I detta arbete behövs en bättre helhetssyn i vårt samhälle på vad som ska skyddas, vilka hoten är och vilka medel vi ska ha för att förstärka vårt skydd. En gemensam lägesuppfattning behövs som ger tillräcklig överblick och förutsättningar att prioritera insatser, särskilt vid allvarligare händelser som berör flera sektorer.

Utredningen har som uppdrag att föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system samt föreslå övergripande mål för samhällets informationssäkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur. Enligt direktiven krävs för att stärka samhällets säkerhet att skyddsvärden, hot och skyddsmedel ses i ett sammanhang.

Informationssäkerhet kan sägas fokusera på den information som data representerar och dess skyddsbehov. I följande avsnitt resoneras kring vilken information som är värdefull för samhället, vilken information samhället har möjlighet att skydda och gränssnitt där staten har möjlighet att påverka. Den nationella strategin ska enligt direktiven avse hantering och överföring av information i elektroniska kommunikationsnät och it-system. Vidare ska den

nationella strategin hantera risker på alla nivåer i samhället och bör även inkludera alla relevanta aspekter och aktörer.

Vad som behöver skyddas kan naturligtvis i förlängningen sägas vara andra värden än den information som data representerar. Informationssäkerhet anses i de flesta sammanhang omfatta informationens konfidentialitet, tillgänglighet, riktighet och spårbarhet. Det rör sig således inte endast om den information som data representerar utan även om hur information används. Med ett vidare perspektiv är andra värden som ska skyddas samhällets funktionalitet och effektivitet, rättssäkerhet, befolkningens liv och hälsa, men också ytterst rikets säkerhet, demokrati och mänskliga fri- och rättigheter.

3.2 Vilken information är värdefull för samhället

Information från den offentliga sektorn spelar en viktig roll för hur marknaden fungerar och hur individer kan tillvara och utöva sina fri- och rättigheter. Utan användarvänlig och lättillgänglig administrativ, rättslig, ekonomisk eller annan offentlig information kan de samhälleliga aktörerna och ekonomiska aktörerna inte fatta välunderbyggda beslut. Det finns även stora mängder information som är av avgörande betydelse för samhällets funktionalitet. Här kan exempelvis nämnas informationshanteringen i betalningssystemen, styrsystem för samhällsviktig eller kritisk it-infrastruktur.

Genom lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen har Europaparlamentets och rådets direktiv 2003/98/EG om vidareutnyttjande av information från den offentliga sektorn (PSI-direktivet) genomförts. Lagen gäller inte för handlingar eller uppgifter i handlingar som inte får tillhandahållas eller för begränsningar i vidareutnyttjandet av dessa som en myndighet är skyldig att besluta om eller som annars följer av någon författning. Som huvudregel omfattas inte heller myndigheters informationsutbyte av lagen. Ur förarbetena till lagen är följande hämtat (prop. 2009/10:175 s. 32, 67 och 131).

> En del av den information som finns hos kommunala och statliga myndigheter utgör en samhällsgemensam resurs av stort värde för medborgare, företagen och det civila samhället. Det ska vara så enkelt som möjligt för så många som möjligt att tillgodogöra sig värdet av denna informationssamling.

> Genom att till stor del betrakta offentlig information och e-tjänster som gemensamma resurser som kan användas av andra aktörer kan förvaltningen bidra till samhällets utvecklingsförmåga och innovationskraft.
>
> Möjligheterna att få tillgång till, att bearbeta och att sprida förvaltningens information är centralt för förvaltningens legitimitet och dess demokratiska förankring. Utöver insyn och kontroll över offentlig verksamhet, kan medborgare och organisationer använda informationen för sin egen kunskapsuppbyggnad, som underlag för deltagande i det offentliga samtalet och i formella politiska processer. Information från myndigheter kan också användas som underlag för att fatta välavvägda beslut när det gäller individuella val som rör det allmännas tjänster, t.ex. välfärdsval. Sådan information kan därför bidra till att stärka människors självstyre och förbättra förutsättningarna för utövandet av medborgerliga rättigheter.

I detta sammanhang behandlas således värdet för samhället av den information i förvaltningen som är offentlig och vikten av att den görs tillgänglig. En förutsättning för att detta värde ska föreligga är att informationens riktighet kan säkerställas.

I säkerhetsskyddslagen (1996:627) tar informationssäkerhet sikte på uppgifter som omfattas av sekretess och som rör rikets säkerhet (7 § 1).

Offentlighetsprincipen, reglerna om allmänna handlingars offentlighet, innebär bl.a. en rätt att ta del av allmänna handlingar. Rätten till insyn i allmänna handlingar förutsätter att det är fråga om en offentlig handling, dvs. en allmän handling som inte är hemlig till följd av en bestämmelse om sekretess. Rätten att ta del av handlingar får begränsas endast när det är påkallat med hänsyn till rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation, rikets centrala finanspolitik, penningpolitik eller valutapolitik, myndighets verksamhet för inspektion, kontroll eller annan tillsyn, intresset att förebygga eller beivra brott, det allmännas ekonomiska intresse, skyddet för enskilds personliga eller ekonomiska förhållanden och intresset att bevara djur- eller växtart (2 kap. 2 § TF). Begränsningar ska anges i offentlighets- och sekretesslagen eller i andra lagar, till vilka hänvisningar görs i offentlighets- och sekretesslagen. Sekretessens styrka och räckvidd varierar och är ett uttryck för den avvägning som gjorts mellan insynsintresset och skyddet av det allmänna eller enskilda intresset.

Personuppgifter är en typ av information som ges ett sådant särskilt skydd. Enligt personuppgiftslagen gäller särskilda begränsningar i behandlingen av vissa kategorier av personuppgifter. I lagen betecknas dessa som ”känsliga” personuppgifter. Känsliga uppgifter är personuppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och personuppgifter som rör hälsa eller sexualliv.

Skyddsbehovet styrs inte bara av den information som data representerar, utan också av i vilken verksamhet informationen används.

I 6 kap. 3 § lagen (2003:389) om elektronisk kommunikation finns bestämmelser om att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållande av tjänsten skyddas. Den som tillhandahåller ett allmänt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet.

I en nationell strategi för att förebygga uppkomsten av terrorism, förhindra terroristattentat och förbereda för det fall ett terroristattentat ändå inträffar (skr. 2011/12:73) inkluderar viktiga åtgärder att stärka it-säkerhet. I skrivelsen berörs arbetet med att förebygga allvarliga elektroniska angrepp riktade mot samhällsviktiga it-system. Försvarets radioanstalt har utvecklat ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur.

Uttrycket samhällsviktig verksamhet används även i förordningen (2006:942) om krisberedskap och höjd beredskap. I den risk- och sårbarhetsanalys som varje myndighet ska göra årligen ska myndigheten särskilt beakta att de mest nödvändiga funktionerna kan upprätthållas i samhällsviktig verksamhet (9 § andra stycket 3). Enligt föreskrifter utfärdade av Myndigheten för samhällsskydd och beredskap, MSB, (MSBFS 2010:7) om statliga myndigheters risk- och sårbarhetsanalyser ska med samhällsviktig verksamhet i föreskrifterna avses en verksamhet som uppfyller minst ett av följande villkor. Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället. Verksamheten är nödvändig eller mycket väsentlig för

att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

I *Handlingsplan för skydd av samhällsviktig verksamhet* (MSB, december 2013) anges samhällssektorer inom vilka merparten av viktiga samhällsfunktioner och samhällsviktiga verksamheter finns. Bland de samhällssektorer som nämns finns energiförsörjning, finansiella tjänster, handel och industri, hälso- och sjukvård samt omsorg, information och kommunikation, kommunalteknisk försörjning, livsmedel, offentlig förvaltning, lednings- och stödfunktioner, skydd och säkerhet, socialförsäkringar och transporter. Uttrycket samhällsviktig används även beträffande infrastruktur och uttrycket samhällsviktig it-infrastruktur används i beskrivningen av utredningens uppdrag, se bilaga 1.

3.3 Vilken information har samhället möjlighet att skydda

Frågan om vilken information samhället har möjlighet att skydda är kopplad till frågorna om vilka informationsrelaterade hot respektive vilka skyddsmedel som finns. I avsnitt 4.4 redogörs övergripande för den aktuella informationsrelaterade hotbilden. De följande kapitlen om myndigheter med särskilt ansvar för informationssäkerhet (kap. 6), samhällets informationssäkerhet (kap. 7) i Sverige och den internationella utvecklingen på informationssäkerhetsområdet (kap. 8) ger ett underlag om hur information kan skyddas.

Om man ser på frågan mera övergripande kan den också avse vilka styrmedel som finns och i vilka sammanhang samhället har möjlighet att skydda information. Redogörelsen för informationssäkerhetsarbetet i Sverige kan visa på de möjligheter, men också de begränsningar som finns att skydda information i den offentliga sektorn, dvs. i både den statliga och den kommunala förvaltningen. Det finns stora skillnader mellan den statliga och den kommunala sektorn när det gäller regeringens möjligheter att styra. Principen om kommunal självstyrelse (1 kap. 1 § RF) gäller för all kommunal verksamhet, dvs. såväl verksamhet inom den fria sektorn som den specialreglerade sektorn. När det gäller de statliga verksamheterna är regeringens styrning mer direkt.

Näringslivets betydelsefulla roll som den största ägaren och förvaltaren av samhällsviktig informationsinfrastruktur framhålls i direktiven. Genomgången i nämnda kapitel ger också en bild av vilka möjligheter och begränsningar som finns för det offentliga att kunna bidra till skyddet av information i den privata sektorn.

Inom såväl den offentliga som privata sektorn kan utkontraktering s.k. outsourcing och användandet av molntjänster innebära särskilda utmaningar i arbetet med att skydda information.

3.4 Gränssnitt där staten kan påverka

I kapitel 5 ges exempel på hur det i regleringen ställs särskilda krav på hanteringen av en viss typ av information, krav på driftsäkerhet och säkerhet när uppgifter behandlas för de som tillhandahåller allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Det finns i regleringen också krav på åtgärder av betydelse för informationssäkerhetsarbetet som t.ex. att genomföra risk- och sårbarhetsanalyser. Det är krav som följs upp av den myndighet som har tillsynsansvar för det aktuella området.

Ett grundläggande sätt som staten har att påverka är genom att höja medvetenheten och kunskapen i hela samhället om informationssäkerhet. Det kan ske genom utbildning samt forskning och utvecklingsarbete. Andra viktiga områden är brottsbekämpning och brottsförebyggande verksamhet. Att it-relaterade brott blir beivrade ökar allmänpreventionen och förtroendet för it-tjänsterna.

Det finns även gränssnitt där statens påverkan av informationssäkerheten i samhället är mer indirekt. Det kan handla om statlig finansiering, upphandling, rådgivning och uppdrag till samverkan mellan offentliga och privata aktörer. Ett särskilt exempel på situationer där staten har möjlighet att påverka informationssäkerheten för stora delar av samhället är i samband med upphandlingar, exempelvis vid utveckling av stora myndighetsgemensamma system för e-förvaltning av olika slag. En annan del är att höja beställarkompetensen inom såväl privat som offentlig sektor. Även kunskapsökning i form av forskningsstöd, inriktning av utbildningssektorn i form av läroplaner, samt övrigt stöd till skapandet av en säkerhetskultur utgör medel som står till statens förfogande. Andra centrala delar i detta arbete är att skapa förmåga till läges-

beskrivningar över it-incidenter och genom riktade insatser kunna minska påverkan på samhället. Därtill kan staten verka för att underlätta internationellt kunskapsutbyte på området. En ökad kunskap om frågorna i samhället innebär i förlängningen även ökade kundkrav på privata aktörer.

Teleoperatörer och andra företag bygger in säkerhet i sina system utifrån kommersiella grunder. Det kan betyda att bristande säkerhet kan accepteras så länge förlusterna inte överstiger kostnaderna för förebyggande åtgärder, krishantering, återställning och kundförlust. I de fall där det inte finns ekonomiska incitament för teleoperatörerna att erbjuda god robusthet har Post- och telestyrelsen (PTS) exempelvis bidragit med medel som utgörs av s.k. beredskapsavgifter från större teleoperatörer. PTS är också drivande i arbetet med att skapa och delta i samarbeten mellan privata aktörer i el- och telekomsektorn och offentliga aktörer.

MSB lämnar råd och stöd i fråga om det förebyggande arbetet på informationssäkerhetsområdet till statliga myndigheter, kommuner och landsting samt företag och organisationer. Detta beskrivs i kapitlet om MSB. Här kan även nämnas myndighetens stöd i form av medel för att förbättra krisberedskapen och i förlängningen samhällets motståndskraft mot allvarliga händelser, genom det s.k. krisberedskapsanslaget som kan ansökas hos MSB. Alla de myndigheter som nämns i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap kan söka projektmedel från detta anslag, utifrån de förutsättningar som regeringen satt upp. Detta gäller även förbättringar av krisberedskapen på informationssäkerhetsområdet. Anslaget ska användas för särskilda satsningar som ligger utanför det ansvar som varje myndighet, i enlighet med ansvarsprincipen, har för att säkerställa att samhällsviktig verksamhet kan bedrivas även när den utsätts för allvarliga störningar.

3.5 Statens ansvar

Som påpekats av InfoSäkutredningen i betänkandet *Säker information Förslag till informationssäkerhetspolitik* (SOU 2005:42) värnar vi i Sverige om en rad principer som ska garantera att beslut fattas så nära den verksamhet som kommer att påverkas av beslutets inne-

håll som möjligt. Det gäller ända ner på individnivå, där enskilda aktörer så långt möjligt ges ett avgörande inflytande över beslut som rör deras egen välfärd. Med decentraliserat ansvar och beslutsutrymme följer också ansvar för den egna verksamheten. Det finns dock verksamheter, funktioner och situationer då enskilda företag och individer inte förmår, eller rimligen kan avkrävas, att axla detta ansvar helt på egen hand. I vissa fall är det nödvändigt att fatta kollektiva beslut och att flytta över delar av ansvaret till offentliga organ.

En diskrepans föreligger ibland mellan vad som är rationellt handlande för en enskild och vad som är rationellt för samhället. Det finns ett flertal motiv utöver politiska överväganden till offentliga satsningar inom olika områden. Dessa har i stor utsträckning hämtat inspiration ur ekonomiska teorier om statens roll i samhällsekonomin. Sett ur ekonomisk synvinkel kan marknaden hävdas innehålla en del brister, eller marknadsimperfektioner, till exempel över- eller underkonsumtion, bristande beställarkompetens, otillräcklig information vid beslutstillfället och behov som marknaden inte kan eller vill tillgodose på egen hand. Här kan det vara nödvändigt för samhället, genom staten, att intervenera för att skapa balans och ökad samhällsnytta.

Försvar, rättsväsende, räddningstjänst och vissa delar av infrastrukturen är klassiska exempel på kollektiva nyttigheter. Dessa funktioner kommer alla till godo. Krishantering på samhällsnivå har i grunden samma karaktär som dessa verksamheter. Om det offentliga inte engagerar sig inom dessa områden kan man befara att satsningar som görs blir otillräckliga eller till och med uteblir. Det beror på att medborgarna har svårt att överblicka och värdera de risker som finns för allvarliga kriser eller brister i säkerheten i till exempel den infrastruktur som är avgörande för samhällets funktionsförmåga. Allmänheten har svårt att förbereda sig för egen del om offentliga organ inte gör riskbedömningar och förmedlar resultatet. Allvarliga kriser, som följer av till exempel brist på säkerhet i infrastruktur, kännetecknas också av att ett stort antal människor och företag samtidigt drabbas av konsekvenserna.

Statens roll är flerfaldig. Det åvilar staten att lösa uppgifterna att förebygga, förhindra och stödja i hanteringen av it-relaterade incidenter som är av sådan omfattning att det inte är rimligt att begära att drabbade själva ska vidta fullständiga åtgärder. För att det ska

vara möjligt måste staten vara den som har det övergripande perspektivet och ansvar för att korrekt omvärldsbevakning kontinuerligt tas fram. Staten har också rollen av att skapa ett organisatoriskt system för informationssäkerhetsarbetet som garanterar kontinuitet och kvalitet avseende tillgänglighet, riktighet, konfidentialitet och spårbarhet.

3.5.1 Uppgifter för statliga myndigheter

En uppgift för offentliga organ bör vara att upptäcka och identifiera säkerhetsbrister i samhällsviktig verksamhet. Det kan ske genom risk- och sårbarhetsanalyser för att upptäcka och identifiera förhållanden som kan utlösa allvarliga störningar. Informations-, utbildnings- och övningsinsatser som bygger på resultatet av sådana analyser är angelägna. Där så kan ske utan att riskera säkerheten bör stor öppenhet tillämpas beträffande resultatet av risk- och sårbarhetsanalyser för att öka medvetenheten om eventuella allvarliga brister och göra det möjligt att vidta säkerhetsförbättrande åtgärder. Underlag för risk- och sårbarhetsanalyser måste även kunna omfattas av sekretess hos de myndigheter som de avser och som de lämnas ut till. Offentliga organ behöver också kunna bedriva en regelbunden säkerhetsinriktad revision i sin egen verksamhet. En framgångsrik säkerhetsrevision, inom myndigheter, förutsätter att ledningsnivån, som är ytterst ansvarig aktivt engagerar sig i arbetet.

Att ha en god informationssäkerhet innebär att kunna lösa såväl vardagliga problem som att ha en beredskap för att hantera allvarliga, omfattande incidenter och kriser som möjligen även drabbar andra verksamheter än den egna. Ett företags egen, grundläggande vardagssäkerhet är ingen statlig eller offentlig angelägenhet. Att skydda de interna informationssystemen, såväl tekniskt som administrativt, och att ha en beredskap för att hantera incidenter är ett ansvar som åligger var och en som förvaltar ett system. Staten kan dock ha en roll i att stimulera till säkerhetsåtgärder, upprätthålla en lägesbild över it-incidenter och att öka medvetenheten om sårbarheten i informationstekniken. Ett företag har sålunda ansvar för sina egna system och privatpersoner har ansvar för sina datorer. Det kan dock vara en svårighet för den enskilde att överblicka aktuella sårbarheter och tillgängliga säkerhetsåtgärder. För att

skapa adekvata risk- och sårbarhetsanalyser krävs en noggrann omvärldsanalys och en överblick över hotbilden som sträcker sig längre än enskilda system och användare. Detta är inget statiskt dokument som användare kan ta del av, utan en process som måste bedrivas med kontinuitet. Ansvaret för helhetsbilden över samhällets samlade it-relaterade hotbild är en uppgift som bör åvila offentliga organ. Staten står för resurser och en kontinuitet, som inte kan vare sig krävas eller garanteras av någon annan aktör. Det är, som argumenteras ovan, rimligt att ansvaret för den dagliga säkerheten åvilar varje användare, förvaltare eller ägare av informationsteknik. För att hantera allvarligare incidenter, som kan komma att påverka den nationella säkerheten eller nationella intressen, måste givetvis staten ha det övergripande ansvaret. Det handlar om att kunna skydda medborgarna mot brott i form av övergrepp och oegentligheter samt att säkerställa att samhällsviktig verksamhet bedrivs med höga krav på funktionalitet och säkerhet. Det gäller även när nationella intressen bevakas inom EU och i internationella organ. Staten måste också ha ansvar för spelreglerna inom informationssäkerhetsområdet. Mot bakgrund av sin överblick över samhällets säkerhetssituation och den hotbild som kan kopplas till informationssäkerheten föreslogs i SOU 2005:42 att staten skapar en struktur för att hantera extraordinära händelser. Staten har också ett eget intresse för informationssäkerheten inom sitt verksamhets- och ansvarsområde, i sin roll som ansvarig för myndighetsutövning och som ägare av statliga företag.

3.5.2 Ett långtgående statligt ansvar

I modern tid har det ofta hävdats att alla har ett ansvar för informationssäkerheten i samhället, vilket inte sällan leder till att ansvaret för konkreta åtgärder höljs i ett dunkel – allas ansvar blir lätt ingens. Utredningen vill därför understryka det som skiljer statens ansvar från övriga samhällsaktörers, och som gör det betydligt tyngre. Det är endast staten – inte individer, näringsliv, kommuner eller landsting – som har iklätt sig folkrättsliga förpliktelser gentemot resten av världssamfundet. Häri ingår t. ex. åtaganden under Europakonventionen för mänskliga rättigheter (EKMR). Det är den svenska staten som har tagit ansvar för att skydda dess med-

borgares liv, hälsa, säkerhet, integritet och trygghet. Det är samma stat som i första tilläggsprotokollet till EKMR har iklätt sig ansvaret för alla svenska fysiska och juridiska personers rätt att okränkt få njuta skydd för sin äganderätt. När staten omsätter dessa åtaganden i lagstiftning – såsom offentlighets- och sekretesslagstiftningen, säkerhetsskyddslagstiftningen och den straffrättsliga lagstiftningen – har staten inte fullgjort sin skyldighet om den inte gör allt i dess makt för att se till att skyddet den via lagstiftningen utsträcker blir verkningsfullt. Häri ingår att både förebygga, upptäcka och beivra allt som kan kränka de rättigheter som skapats genom åtagandena. Det är för att på ett tydligt sätt visa hur staten axlar detta ansvar som betänkandet föreslår att regeringen och dess myndigheter vidtar åtgärder för att skapa större säkerhet kring den information och de system för dess överföring som staten har ett omedelbart inflytande över, och det är också därför utredningen föreslår att regeringen antar en strategi för informations- och cybersäkerhet.

4 Ökad digitalisering

4.1 Ett ändrat synsätt på informationssäkerhet

Under 1990-talet skedde en dramatisk förändring av internets utveckling. Ett tidigare mer isolerat system öppnades upp och antalet sammankopplingar, såväl nationellt som globalt, ökade. Den dramatiska förändringen påverkade också synsättet kring hanteringen av informationssäkerheten då antalet aktörer och användare ökade. Fokus hamnade på säkerheten i nätverk och system där varje aktör skulle vara medveten om och ta ansvar för sina risker och sårbarheter liksom förebyggande åtgärder. Åtgärder som skapar säkerhet för helheten, i allas intresse, främjades. Tanken var att försöka bygga in säkerhet i en öppen och sammankopplad digital värld i stället för att utveckla riskhantering och sårbarhetsanalyser, s.k. risk management. Detta senare synsätt utvecklades därefter och råder i dag.

Den tekniska utvecklingen har medfört större bandbredd och snabbare överföring av information (kapacitet) i fasta och trådlös uppkoppling under de senaste 15–20 åren. Tillsammans med större nätverk samt ökad lagrings- och processkapacitet har nya produkter och tjänster kunnat utvecklas, bl.a. smarta telefoner, surf- och läsplattor, molntjänster m.m. Innovationer inom mjukvaruområdet har lett till nya affärsmöjligheter och modeller, t.ex. inom appar och genom insamling och bearbetning av stora datamängder, s.k. ”big data”. Sociala medier, den ökade digitala mobiliteten, möjligheten till geografisk lokalisering och annan digital utveckling har också lett till ekonomiska och sociala förändringar till nytta för alla sektorer inom ekonomin och samhället. Samhället har blivit allt mer beroende av den digitala utvecklingen. Kraven ökar på möjligheten att känna tillit till informationssystem och nätverk liksom på de aktörer och mellanhänder som hanterar dessa. Men, kraven ökar

också på digitala tjänsters förmåga att motstå risker och sårbarheter och medarbetares förmåga att förstå och hantera dessa. Det handlar numera om säkerheten för ett större komplex, ett ekosystem. Synsättet har vidgats, från säkerhet i nät och system till att bli betydligt bredare. Vi har också gått från ett statiskt synsätt där det gäller att undvika risk (riskaversion) till dynamisk riskhantering.

De övergripande målen i nya nationella informationssäkerhetsstrategier utgår ifrån att stödja ekonomisk och social utveckling samt att skydda samhällets funktionalitet. Fokus på säkerhet kring informationssystem och nätverk är således en del men inte tillräckligt. Hoten och sårbarheterna i den digitala världen har ökat. Säkerheten i det digitala samhället är inte enbart en teknisk angelägenhet utan omfattar många fler aspekter. Vi har alla ett gemensamt ansvar, utifrån roller, verksamhet och sammanhang, för att skydda den digitala miljön mot hot och angrepp som leder till skada och minskad tillit. Ett dynamiskt riskbaserat synsätt utgår från alla de risker som möter aktörerna i ett föränderligt digitalt samhälle vid realiseringen av ekonomiska och sociala ambitioner. Som utredningen påpekat i kapitel 3 bör staten förbättra arbetet med sin del av ansvaret för dessa frågor.

4.2 En kontinuerlig teknisk utveckling

När samhället blir allt mer beroende av tekniska system måste dessa vara tillräckligt säkra. I det moderna samhället blir konsekvenserna av driftavbrott i informationssystem större och mer oöverskådliga. När en aktör med många kunder drabbas av driftstörningar kan konsekvenserna bli kännbara och oväntade på många olika håll samtidigt.

Utveckling av programvara och tjänster ställer höga krav på både beställarkompetens och säkerhetsmedvetande hos beställaren för att uppnå tillräcklig säkerhetsnivå. It-tjänster i moderna verksamheter är ofta komplexa och utspridda både fysiskt och organisatoriskt (outsourcing). Det får konsekvenser för säkerheten. Riskerna blir mer svårbedömda och svåröverskådliga.

Mer och mer information om oss själva och om våra tekniska lösningar blir allmänt tillgänglig. Frågorna om privatlivet aktualiseras alltmer när större mängd och fler typer av data blir tillgängliga

i det moderna samhället. Den ökade delningen av information ger ökad osäkerhet om vem som äger data t.ex. vid lagring i molntjänster. Teknikutvecklingen gör teknikberoende författningar och regler kring elektroniskt informationsutbyte mellan myndigheter föråldrade, vilket försvårar både önskvärda systemintegrationer och skyddet för privatlivet.

Det pågår en ständig kapplöpning mellan angripare och försvarare. Förekomsten av programvara som identifierar sårbarheter samt enkla och billiga tekniska hjälpmedel för angrepp har sänkt tröskeln och satt verktyg i händerna på fler angripare. Utöver de tekniska sårbarheterna är människan i systemen en svag länk, som med enkla medel kan luras att ladda ner skadlig kod eller uppge känsliga uppgifter. Det är inte fråga om en verksamhet ska bli hackad, utan när.

En väsentlig faktor är att säkerställa att utbildning kan matcha den snabba utveckling som kännetecknar området.

4.3 Politiska mål för en digital tidsålder

It-politiken handlar om att använda och främja de möjligheter som digitaliseringen för med sig. Området omfattar bland annat reglering av it och elektronisk kommunikation, liksom nät- och informationssäkerhet, frekvenspolitik och frågor om internets styrning och förvaltning. I området ingår också frågor om tillgång till bredband och infrastruktur för it.

Regeringen (och dess myndigheter) har tagit fram ett antal strategier, agendor och handlingsplaner som avser den digitala utvecklingen och berör informationssäkerhetsområdet. Närmast redogörs för några av dessa som bedöms mest relevanta.

4.3.1 Digital agenda

Den 29 september 2011 beslutade den dåvarande regeringen om en ny strategi för it-politiken, *It i människans tjänst – en digital agenda för Sverige* (dnr N2011/342/ITP), kallad den digitala agendan för Sverige. Den digitala agendan för Sverige är en bred och sammanhållen strategi för it-politiken där regeringen presenterar ambitioner och insatser som tar till vara de möjligheter som digitaliseringen ger. Målet för it-

politiken är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. I december 2011 beslutade riksdagen att tidigare it-politiska mål och delmål om tillväxt och kvalitet skulle upphävas och ersättas med det nya it-politiska målet (prop. 2011/12:1, utg.omr. 22, bet. 2011/12:TU1, rskr. 2011/12:87). När det gäller målen för tillgänglighet ska dessa fortsatt gälla (prop. 2009/10:193, bet. 2009/10:TU18, rskr. 2009/10:297).

Den digitala agendan för Sverige pekar ut behov av insatser inom följande fyra strategiska områden, där användarens perspektiv är utgångspunkten:

- Lätt och säkert att använda.
- Tjänster som skapar nytta.
- Det behövs infrastruktur.
- Informationsteknologins roll för samhällsutvecklingen.

Digitaliseringskommissionen

Digitaliseringskommissionens uppdrag är att verka för att det it-politiska målet i den digitala agendan uppnås och att regeringens ambitioner inom området fullföljs. Detta ska ske med hänsyn till det huvudsakliga ansvar som respektive myndighet och departement inom Regeringskansliet har för att vidta och följa upp åtgärder kopplade till målet för it-politiken. Hela uppdraget är formulerat i kommittédirektiven. Kommissionen har i huvuduppdrag att:

- utforma ett förslag till handlingsplan för genomförande av uppdraget att verka för det it-politiska målet,
- analysera utvecklingen i förhållande till det it-politiska målet,
- visa på digitaliseringens möjligheter,
- kommunicera den digitala agendan och dess innehåll,
- vara administrativt ansvarig för de s.k. signatärerna till den digitala agendan, och
- samverka med olika aktörer i samhället för en ökad digitalisering.

Uppdraget ska slutredovisas senast den 31 december 2015.

4.3.2 E-förvaltnings-strategi

I december 2012 presenterade regeringen sin e-förvaltningsstrategi *Med medborgaren i centrum* (dnr N2012/6402/ITP). Strategin förtydligar och preciserar de mål och strategiska ställningstaganden som uttrycks i den förvaltningspolitiska propositionen (prop. 2009/10:175) och i den digitala agendan för Sverige. I e-förvaltningsstrategin beskrivs regeringens målsättningar för arbetet med att förstärka myndigheternas förmåga att samverka digitalt i förvaltningsgemensamma it-frågor. Ett delmål i e-förvaltningsstrategin är att statsförvaltningens informationssäkerhet ska förbättras.

E-delegationen

E-delegationen har med anledning av sitt uppdrag från regeringen tagit fram en strategi för informationssäkerhet i e-förvaltning. De strategiska mål som anges är följande.

- Den enskilde känner tillit till att informationshantering i myndigheters, landstings och kommuners e-tjänster sker på ett sådant sätt att personlig integritet förenas med hög tillgänglighet, spårbarhet och riktighet.
- All informationshantering i e-förvaltning sker med de säkerhetsåtgärder som definieras utifrån risk- och sårbarhetsanalys samt informationsklassning.
- En god säkerhetskultur och gemensamt regelverk finns så att information behandlas med samma krav på säkerhet oavsett vilken myndighet, vilket landsting eller vilken kommun som tillhandahåller eller använder en e-tjänst.
- Tydlig ansvarsmodell för styrning och uppföljning av informationssäkerhet inom e-förvaltning är etablerad på nationell nivå.
- Samhällsviktiga funktioner som stöds av e-tjänster upprätthålls även i krisläge. Detta förutsätter väl utvecklade metoder för kontinuitetsplanering.
- Processer finns inom e-förvaltningsarbetet för att skapa en nationell informationssäkerhetsrelaterad lägesbild.

- Informationssäkerhet i enlighet med informationens krav på skyddsnivå upprätthålls även då information kommuniceras till och från enskilda.

Delegationen består av 16 generaldirektörer från de mest it-intensiva myndigheterna och en representant för Sveriges Kommuner och Landsting, SKL. Ärenden förbereds i en arbetsgrupp med främst it- och verksamhetschefer från myndigheterna och diskuteras sedan i två olika delegationsutskott innan beslut fattas. I varje delegationsutskott ingår flera generaldirektörer.

E-legitimationsnämnden

E-legitimationsnämndens uppgift är att stödja och samordna offentliga sektorns behov av säkra metoder för elektronisk identifiering och signering. Inom detta område finns en rad uppgifter som faller inom nämndens ansvar. E-legitimationsnämnden har den samordnande funktionen på området för e-legitimationer. E-legitimationsnämnden har också fattat ett inriktningsbeslut att jobba för att stödja även privat sektors användning av e-legitimationer, bl.a. genom att möjliggöra för registerhållning och upprättande av regler och avtal för privata aktörer. Nämnden har som uppgift att fungera som en svensk kontaktpunkt för internationell samverkan kring e-legitimationer och digital identifiering och signering, t.ex. vad gäller nationell teknisk standardisering. Det innebär också att delta i samverkan med EU:s organ på området.

4.3.3 Bredbandsutbyggnad i Sverige

Det riksdagsbundna målet för tillgänglighet på it-området är att Sverige ska ha bredband i världsklass. Alla hushåll och företag bör ha goda möjligheter att använda sig av elektroniska samhällstjänster och service via bredband (prop. 2009/10:193).

Enligt målen i *Bredbandsstrategi för Sverige* (dnr N2009/8317/ITP) bör 90 procent av alla hushåll och företag ha tillgång till bredband om minst 100 Mbit/s 2020. Det är marknaden som står för utbyggnaden, men i områden där marknaden inte ser det vara lönsamt att bygga ut finns det behov av riktade insatser som sker med hjälp av stöd.

Enligt Post- och telestyrelsens (PTS) bredbandskartläggning för 2013 hade 57 procent av alla hushåll och företag tillgång till 100 Mbit/s. Fördelningen skiljer sig dock inom och utanför tätort och småort. Enligt samma kartläggning har 99 procent av alla fasta hushåll och företag tillgång till mobilt bredband via LTE (4G).

Bredbandsforum

Bredbandsforum är en viktig del av nämnd strategi. Forumet främjar samverkan kring bredbandsutbyggnad. Företag, myndigheter och organisationer möts i Bredbandsforum för att tillsammans hitta lösningar som ökar tillgången till bredband i hela landet.

Bredbandsforum leds av en styrgrupp med ansvarig minister som ordförande. Bredbandsforums löpande verksamhet drivs av ett kansli som är placerat vid PTS och mandatet gäller t.o.m. 2015.

4.3.4 Nationell eHälsa – strategin för tillgänglig och säker information inom vård och omsorg

E-hälsa är det sammantagna begreppet för digitala tjänster som stödjer utvecklingen inom vården och omsorgen. När informationen är enhetlig och strukturerad på ett bra sätt går det lättare att dela den och att jämföra och följa upp vårdinsatser.

Sedan 2010 finns en nationell strategi för e-hälsa som leds av regeringen i samarbete med Socialstyrelsen, Sveriges Kommuner och Landsting, Vårdföretagarna, Famna (Riksorganisationen för vård och omsorg) och E-hälsomyndigheten. För att e-hälsotjänster ska bli effektiva verktyg i syfte att utveckla och effektivisera vården och omsorgen måste det finnas en samsyn och samordning mellan olika aktörer, och den nationella e-hälsostrategin är ett uttryck för denna samsyn mellan de centrala aktörerna på nationell nivå.

För att hålla samman genomförandet av strategin finns en högnivågrupp där stat, huvudmän och utförare av vård och omsorg finns representerade. Högnivågruppen fokuserar på strategiska frågeställningar och vägval med koppling till den nationella e-hälsostrategin och fungerar som ett organ för gemensamt ställningstagande för inriktningen av det fortsatta arbetet.

I detta sammanhang kan nämnas E-hälsokommitténs utredningsuppdrag (dir. 2013:125) att se över ändamålsenlighet och ansvarsfördelning när det gäller tillhandahållande och utformning av it-stöd för personal, vård- och omsorgsgivare och andra aktörer inom hälso- och sjukvård och socialtjänsten. Uppdraget ska slutredovisas i ett betänkande senast den 27 mars 2015.

4.4 Hot och risker i en digitaliserad värld

Utvecklingen inom informations- och kommunikationsteknik området har skapat nya möjligheter för både medborgare, näringsliv och offentlig sektor. Tillgång till information, oavsett var man befinner sig och oavsett tid på dygnet, har ökat markant under senare år och har bidragit till ökad effektivitet och nytta inom många områden. Myntets baksida är dock att den förändrade kommunikationsinfrastrukturen och sammankopplingen av informationssystem medfört nya och förändrade typer av hot och risker.

Genom informationssystemens ömsesidiga beroenden och deras ökade funktionalitet har det även introducerats sårbarheter och öppnats för hot som delvis inte funnits tidigare. Informationssystemens komplexitet innehåller sårbarheter bl.a. genom att de kan vara svåra att underhålla i den takt som krävs och som tillsammans med brister eller sårbarheter i kommunikationsinfrastrukturen kan skapa möjlighet för obehöriga att få åtkomst till informationssystemen. Olika verksamheters beroende av it-system innebär även att de blir sårbara för handhavandefel, tekniska fel och olyckor.

Många av samhällets tjänster bygger på och är beroende av informations- och kommunikationsteknik vilket bl.a. innebär att det inte längre är frivilligt för medborgarna om man vill använda tekniken eller inte. Det är snarare ett krav. För myndigheter och näringsliv är beroendet av tekniken ofta så stort att verksamheten riskerar att allvarligt störas eller stoppas om tillgång till vissa stödsystem saknas.

I princip alla, både privatpersoner, näringsliv och offentlig verksamhet, som är anslutna mot internet tar en risk och är i dagsläget utsatta för risker eftersom det ständigt pågår angreppsförsök mot internetanslutna system. Denna typ av massangrepp är ofta mer

eller mindre slumpartade. Exempel på detta är den stora ökningen av bedrägerier och identitetsstölder som sker via internet mot i första hand privatpersoner. Andra typer av elektroniska angrepp är riktade mot viss verksamhet eller kategori av användare och kan vara av olika allvarlighetsgrad. En förändring är att system för industriella informations- och styrsystem, så kallade SCADA system (supervisory control and data acquisition), tidigare var leverantörsunika system som var isolerade från omvärlden. Dessa system blir alltmer indirekt eller direkt anslutna mot globala nätverk vilket innebär att de kan bli utsatta för angrepp, se avsnitt 4.4.3. Här har sektorsansvariga myndigheter en viktig roll att fylla när det gäller statens möjlighet att påverka informationssäkerhetsarbetet inom respektive sektor.

Organisatoriska frågor påverkar också utvecklingen inom informationssäkerhetsområdet. Tidigare tog varje verksamhet själv hand om sina system för exempelvis löner, lagerhållning och fakturering. Numera lägger allt fler ut sådana funktioner på externa leverantörer. Samtidigt innebär utvecklingen med outsourcing också en koncentration av it-hanteringen som medför att konsekvenserna av såväl attacker som icke-antagonistiska driftavbrott blir svåröverskådliga.

Att skydda sig mot it-incidenter är svårt. Den som ansvarar för ett it-system måste, trots att en stor mängd attacker kan avvärjas, utgå från att angrepp faktiskt lyckas. För att en angripare ska få ett fotfäste i ett nätverk som inte är ordentligt konfigurerat, krävs inte mer än att en användare öppnar en olämplig e-postbilaga eller webblänk. Därefter kan angriparen ta sig vidare i nätverket och etablera sig långvarigt.

Försvarsberedningen gör i promemorian *Vägval i en globaliserad värld* (Ds 2013:33 s. 36–37) bedömningen att sårbarheterna som uppstår i dagens globala it-system utgör en av våra mest komplexa frågor. I promemorian utvecklas hoten och riskerna enligt följande.

> Internet används för både civila och militära ändamål. Handel, tekniköverföring, nätsäkerhet, samhällsviktig verksamhet och olika former av it-brottslighet har kopplingar till säkerhets- och försvarspolitiska överväganden. Samtidigt riskerar vissa staters ökade krav på säkerhetsåtgärder i den digitala världen att leda till inskränkningar av mänskliga rättigheter och minskade informationsflöden, med stora politiska, sociala och ekonomiska konsekvenser som följd. Hot- och riskskalan inom dagens informationsteknologi spänner från mindre omfattande

> risker för den enskilde medborgaren, till väl planerade och med precision riktade s.k. cyberattacker mot vitala delar i samhällets funktionalitet. En it-incident är inte nödvändigtvis en antagonistisk viljeyttring. Mer vanligt är olika former av driftrelaterade problem. En it-incident skulle dock kunna påverka funktionaliteten i ett samhälle utan att en stats suveränitet utmanas. Mer allvarliga intrång i samhällsviktig verksamhet och kritisk infrastruktur är de som syftar till att störa funktionaliteten, förändra, stjäla, eller manipulera information eller helt ta över ett informationssystem. En växande sårbarhet är sammankopplingen via internet mellan olika typer av industriella styr- och kontrollsystem. Olika typer av störningar eller antagonistiska hot där styr- och kontrollsystem tas över av tredje part kan potentiellt hota både ett lands samhällsviktiga funktioner och ytterst dess suveränitet.

Utredningens bild av situationen inom informations- och cybersäkerhetsområdet överensstämmer med Försvarsberedningens beskrivning och vi anser att det är viktigt att ha en sådan helhetssyn när frågor om informationssäkerhet behandlas. Rapporten *Informationssäkerhet – trender 2015* utgör tillsammans med den bild som förmedlats av utredningens referensgrupp det huvudsakliga underlaget för vår redogörelse. I nämnd rapport lämnar Myndigheten för samhällsskydd och beredskap (MSB) tillsammans med Försvarets radioanstalt, Polismyndigheten och Försvarsmakten en samlad bild av situationen på informations- och cybersäkerhetsområdet. De deltagande myndigheterna har identifierat sju trender dvs. stabila, långsiktiga förändringar på informationssäkerhetsområdet som bedöms påverka samhället i någon form. Inom vart och ett av områdena har tre huvudpunkter tagits upp vilka tillsammans ger en övergripande bild av situationen. Följande trendområden anges:

1. Strategiska beslut om informationssäkerhet tas alltid i en kontext där säkerhet vägs mot andra värden.
2. It-tjänster i moderna verksamheter är ofta komplexa och utspridda både fysiskt och organisatoriskt.
3. Allt mer information om oss själva och om våra tekniska lösningar blir allmänt tillgänglig.
4. Informationssäkerhet har på senare år fått en växande säkerhetspolitisk dimension.
5. I det moderna samhället har så gott som all brottslighet en it-koppling.

6. Det sker en ständig kapplöpning mellan angripare och försvarare.
7. När samhället blir allt mer beroende av tekniska system måste dessa vara robusta.

Närmast utvecklas beskrivningen av den informationsrelaterade hotbilden. Beskrivningen tar upp hotens karaktär och ursprung samt dess möjliga konsekvenser för informationssäkerheten.

4.4.1 Icke-antagonistiska hot

Många it-incidenter och störningar i informationssystem har icke-antagonistiska orsaker. En inte ovanlig anledning till sådana it-incidenter är fel i programvara eller hårdvara. Störningar i stödsystem som t.ex. elförsörjning och kommunikation genom väderförhållanden och avgrävda kablar är också välkända orsaker till it-incidenter.

PTS tar årligen fram en risk- och sårbarhetsanalys (RSA) för sektorn elektronisk kommunikation. Analysen innehåller bedömningar av hot som kan påverka elektroniska kommunikationer och de samhälleliga konsekvenserna av sådana hot. I RSA:n behandlas fem kategorier av hot:

För *det första* handlar det om tekniska fel och brister och bland dessa omnämns sex olika situationer: bortfall av tillgångar orsakade av hårdvarufel, kortvarig störning i elförsörjning med efterföljande fel i befintlig reservkraftsförsörjning, fel i programvara som styr tillgångar, oavsiktliga överbelastningar av tillgångar och förbindelser, överbelastning av mobila kommunikationsnät och förlust av förmåga att övervaka och styra informationstillgångar och nätfunktioner.

För *det andra* nämns naturligt förekommande hot, såsom klimatologiska fenomen, seismiska fenomen, vulkaniska fenomen, stormar, isstormar, snöstormar, värmeböljor och översvämning.

Den tredje hotkategorin utgörs av fysiska skador, med vilket menas vattenskador, damm, korrosion, förfrysning, avgrävning av förbindelser, föroreningar och andra händelser som förhindrar åtkomst till tillgångar.

Den fjärde formen av icke-antagonistiska hot handlar om olika former av fel eller brister i kritiska resurser och funktioner. Följande exempel tas upp: avbrott i elförsörjningen längre än befintliga reservkraftsystem, otillgänglighet av personal, manuell frånkoppling i elbristsituationer, förlust av luftkonditionering eller kylning, fel i användning av tillgångar, brister eller fel i funktioner för felavhjälpning, brister i förebyggande arbete, bristfälliga rutiner vid uppgradering av mjukvara och förekomst av brister i ledningsfunktioner.

Den femte kategorin utgörs av elektromagnetiska och termiska hot i form av åska, rymdväder och termisk strålning.

PTS har konstaterat att de hot som 2012 gav upphov till flest antal allvarliga störningar var av icke-antagonistisk art, nämligen fel vid uppgradering av programvara, elavbrott, avgrävning av kabel, hårdvarufel och överbelastning.

Av de riskbedömningar som PTS redovisar i risk- och sårbarhetsanalysen för 2012 följer att fel vid uppgradering av programvara kan anses vara en betydande risk då sådana fel kan leda till avbrott på nationell nivå. Ytterligare exempel på hot som PTS ser som allvarliga är elavbrott, stormar och andra väderfenomen som leder till omfattande elavbrott samt tillhörande problem i återställningsarbete. Hårdvarufel och överbelastningar av tekniska system är andra exempel på hot som bedöms kunna få negativ samhällelig påverkan.

Vårt ökade beroende av fungerande teknik medför att konsekvenserna av driftavbrott blir allt större och mer oöverskådliga. Tieto-haveriet i slutet av 2011 förblir ett exempel på hur centraliserad drift under olyckliga omständigheter plötsligt leder till oväntade och svårförutsägbara problem för stora och till synes orelaterade delar av samhället. Ovan refererad trendrapport från MSB m.fl. myndigheter påpekar att det är lätt att underskatta icke-antagonistiska hot som beror på våra egna tillkortakommanden såsom kortsiktighet eller slarv. Det anges att buggar i program- och hårdvara, kvalitetsbrister i programvaruutveckling och avsaknad av eller slarv i rutiner vid mjukvaruuppdateringar kan skapa stora problem. Vidare påtalas att ett problem med att ägna för lite uppmärksamhet åt vanliga driftavbrott är att det dessutom kan öppna för antagonistiska angrepp. I rapporten ges som exempel att en kvalificerad motståndare som vill angripa ett ledningssystem kan tänkas maskera sina angrepp som oregelbundet återkommande driftavbrott.

4.4.2 Antagonistiska hot

När det gäller antagonistiska hot och förutsättningarna att verkställa dessa så har det skett stora förändringar. Tidigare, då många verksamheter byggde på manuell hantering och mer eller mindre isolerade it-system, var en antagonist tvungen att exponera sig i något läge av ett angrepp mot en verksamhet och dess information. Angrepp på distans var omöjligt eller mycket ovanligt. I dag är de flesta verksamheter direkt eller indirekt anslutna till internet eller andra globala nätverk vilket kan möjliggöra för en antagonist att angripa en verksamhet utan någon fysisk närvaro eller exponering. En försvårande faktor är att angreppen i princip kan utföras från vilken plats som helst i världen vilket tillsammans med anonymiseringstjänster och jurisdiktionsfrågor gör det svårt att spåra och lagföra en angripare. Denna ”anonymitet”, verklig eller upplevd, gör sannolikt att vissa aktörer som aldrig skulle utföra ett rent fysiskt angrepp mot en verksamhet inte drar sig för att genomföra ett elektroniskt angrepp. Statsunderstödd olovlig underrättelseinhämtning har också i och med detta fått en ny arena att operera från.

När det handlar om de mest kvalificerade hoten rör det sig huvudsakligen om angrepp från stater och statsunderstödda aktörer. Dessa är målinriktade och uthålliga och har stora resurser och hög kompetens. Syften för de statsunderstödda aktörerna är politiska, militära och industrispionage. Andra allvarliga syften kan dock inte uteslutas. Det kan röra sig om förberedelser för att kunna skada svensk kritisk infrastruktur i ett framtida scenario. Det kan handla om politisk utpressning eller ske i samband med militär konflikt.

Det politiska spionaget påverkar vår förmåga att bedriva en självständig försvars-, säkerhets- och utrikespolitik. Industrispionaget leder till att svensk kunskap och innovation stjäls samt att svenska företag inte kan konkurrera på lika villkor vid exempelvis upphandlingar.

Hotutövare finns på alla nivåer. Det kan vara allt från personer som utan egentligt brottsligt uppsåt testar sina kunskaper genom att olovligen försöka ta sig in i informationssystem, till statsunderstödd olovlig underrättelseinhämtning. Det kan även förekomma kombinationer av dessa. Ytterligare en dimension av

antagonistiska hot är då angrepp mot informationssystem sker som ett led i en militär operation för att störa ut och påverka ledningssystem eller andra system för att vinna militärtaktiska fördelar.

Spektrumet av aktörer är således brett och omfattar inte enbart stater och säkerhetstjänster med stora resurser utan även enskilda, fristående hackargrupperingar, religiöst-nationellt-etniskt-ideologiskt drivna aktivister till kriminella organisationer. Till detta tillkommer cyberspionage och grupperingar som tar betalt för att utföra skadlig verksamhet på nätet.

Programvara särskilt utvecklad för it-angrepp av olika slag blir allt lättare att få tag på. Att genomföra ett angrepp kräver i och med detta inte längre någon stor kompetens och tröskeln för angrepp sänks. Det finns en relativt osofistikerad kategori aktörer, vars ageranden ofta är enkla att spåra på internet. Det är personer som har laddat ned information och programvara från nätet om hur man kan gå till väga för att kompromettera konton och filer eller att initiera attacker mot datorsystem. Deras metoder går ut på att skanna av nätet och försöka finna sårbarheter varhelst de uppstår och därefter utnyttja dessa.

Andra angrepp utgår från ett ideologiskt eller politiskt betingat motiv och tar sig uttryck i överbelastningsattacker (DDos), lösenordsstöld, intrång i system och manipulering av hemsidor (Web Defacement). Detta kan vara ett störande inslag mot informationssystem men kan i dagsläget inte sägas utgöra ett samhällsfarligt hot såtillvida de inte lierar sig med andra aktörer med andra syften.

Det förekommer också att en tredje part används som ombud. Det kan vara enskilda hackare eller grupper av sådana med mycket god kompetens. Bakom sådana aktörer kan främmande säkerhetstjänster stå. Poängen med att använda en tredje part är att såväl anstiftare som motiv och intention bakom en operation kan hållas dolda. Förfarandet är intressant även för enskilda individer och företag som via ombud exempelvis kan stjäla känslig och samhällsviktig information. Det är också möjligt att misskreditera specifika organisationer och personer genom att plantera illvilliga uppgifter riktat mot dessa.

Ett antagonistiskt hot som ofta förbises är det s.k. ”insiderhotet” som innebär att någon som deltar i verksamhetens bedrivande eller av annan anledning har behörighet till verksamhetens

lokaler eller informationstillgångar missbrukar detta. Insiders är således inte bara de som är anställda i verksamheten.

I dag har ofta brottslighet en it-koppling. Mest uppenbart är det naturligtvis för brott som till sin natur kräver modern teknik, som datorbedrägeri och dataintrång. Men det moderna samhällets kommunikationsvägar är sådana att även brott som häleri, bidragsfusk, kreditkortsbedrägerier och bluffakturor nästan per definition har stora elektroniska inslag. Ofta handlar det alltså om gamla brott i ny skepnad. Kriminellas aktiviteter riktas mot individer, organisationer och finansiella institutioner. Internet har skapat en brottsarena vars gränser inte sätts av vare sig geografi, nationell härkomst eller nationella lagar. Det förekommer bl.a. en kriminell internetbaserad tjänstesektor, ”crime-as-a-service”. Ett exempel är webbhotell som ger kriminella personer säkerhet, driftsäkerhet och anonymitet. Ett annat exempel på it-brottslighet är användande av skadlig kod som installeras på offrets dator som sedan gör det möjligt för gärningsmannen att kryptera datorn alternativt delar av materialet i datorn. Gärningsmannen kräver sen målsäganden på pengar för att denne ska återfå kontrollen över datorn alternativt det material som har krypterats. Ett annat brott som har vuxit på senare år är identitetstölder. När en identitet har kapats kan förövaren snabbt ta lån och handla varor på internet.

Utredningen utgår från att i stort sett alla terroriströrelser – oavsett situation, geografisk plats och motiv – använder internet för att söka information, koordinera resurser och genomföra operationer av diverse slag. Denna typ av antagonister drar fördel av samhällets stora beroende av it-system. Olika slag av inbyggda sårbarheter i systemen utgör lockande mål för attacker. Internet utgör dock inte ett mål i sig självt, däremot kan kontroll och ledningsfunktioner i viktig infrastruktur, de så kallade systemen för industriella informations- och styrsystem, vara målobjekt om de har direkt eller indirekt koppling mot internet. I tider av kris och konflikt mellan länder utgör angrepp mot kritiska informationsinfrastrukturer det kanske allvarligaste hotet då effekter för samhället av kvalificerade angrepp blir avsevärda. Risken finns att stora delar av samhället skulle kunna lamslås.

För att skydda eller angripa såväl samhällsviktiga system som militära och säkerhetsmässiga strukturer inrättar många högteknologiska nationer särskilda informationskrigsförband. Sådana en-

heter hanterar hela spektrumet av operationer på internet och i de globala nätverken för verkan och skydd. Verksamheten omfattar aktiva skyddsåtgärder såsom hantering av incidenter i egna system, avlyssning av information respektive störning och förstöring av motståndares informations- och kommunikationssystem liksom vilseledning och psykologisk påverkan.

4.4.3 Särskilt om hot mot industriella informations- och styrsystem m.m.

Samhällsviktig verksamhet som t.ex. att producera och distribuera elektricitet, att leverera rent dricksvatten till kranen, att framställa fordonsbränsle och att styra kollektivtrafiken är några exempel på verksamheter som blivit beroende av att datorer fungerar. Tidigare nämnda industriella informations- och styrsystem används inom dessa verksamheter. Regeringen angav i propositionen *Samhällets säkerhet och beredskap* (prop. 2001/02:158 s. 104) att det är angeläget att samhällsviktiga system har en hög säkerhetsnivå och att insatserna för informationssäkerheten ökas. I den digitala agendan *It i människans tjänst – en digital agenda för Sverige* (s. 40) nämnder regeringen också behovet av att arbeta vidare med säkerheten i informations- och styrsystem i samhällsviktig verksamhet.

När det gäller industriella informations- och styrsystem så kan information bestå av styrsignaler som reglerar spänningsnivåer i stora transformatorstationer, eller datorer som skickar instruktioner till dammluckor. Felaktiga eller uteblivna signaler kan i värsta fall leda till dödsfall eller fysisk förstörelse. Till skillnad från information som hanteras på kontor och som bearbetas av människor så arbetar de industriella informations- och styrsystemen ofta autonomt. En operatör talar om för systemet vad det ska uppnå, men systemet får sedan, med hjälp av avancerad matematik, räkna ut exakt hur detta ska realiseras. Styrsystemen förväntas ofta vara i drift dygnet runt under årets alla dagar utan avbrott.

Myndigheten för samhällsskydd och beredskap tog 2013 fram dokumentet *Handlingsplan för samhällsviktig verksamhet.* I handlingsplanen pekas elva sektorer ut som särskilt viktiga. Fyra av dessa elva sektorer är mycket beroende av industriella informations- och styrsystem. Dessa sektorer är energiförsörjning (exempelvis produktion och distribution av elektricitet, fjärrvärme och

bränslen samt hantering av avfall), handel och industri (exempelvis produktion av farliga ämnen), kommunalteknisk försörjning (exempelvis vatten- och avloppsproduktion) samt transporter (exempelvis spårbunden trafik, vägtrafik, sjöfart och hamnar, flygtrafik och flygledning, kollektivtrafik). Även handlingsplanen för samhällets informationssäkerhet lyfter fram industriella informations- och styrsystem som ett centralt område att höja informationssäkerheten inom (se avsnitt 7.3.2)

Störningar i någon av nämnda verksamheter kan leda till stora påfrestningar i samhället. I och med att dessa verksamheter har ett starkt inbyggt beroende av industriella informations- och styrsystem som ofta saknar tillräckligt it-skydd är detta allvarligt. Det är också viktigt att tänka på att störningar i en samhällssektor ofta påverkar andra delar av samhället. Om en region till exempel blir utan elektricitet leder det i förlängningen till att dricksvattenförsörjning och transporter påverkas.

Industriella informations- och styrsystem återfinns också i system utanför nämnda fyra samhällssektorer. Fastighetsautomation är ett exempel på tillämpningar som på senare år har utsatts för angrepp. Exempelvis har angripare kunnat stänga av värmen i fastigheter som haft sina system åtkomliga från internet. Även om den typen av attacker kan tyckas harmlösa är det allvarligt att styrsystem är så lättåtkomliga. Dessutom kan störningar i fastighetsautomation få sekundära effekter – genom att till exempel stänga av kylan i en serverhall kan tillgången till viktig information försvåras eftersom en server behöver kyla för att fungera. På samma sätt är det möjligt att komma åt larm- och övervakningssystem om dessa inte är ordentligt skyddade.

5 Regleringen

5.1 Inledning

Det finns en mängd författningar som berör informationssäkerhetsfrågorna och som syftar till att bereda skydd för viss typ av information eller att ge anvisningar om hur arbetet med informationssäkerhet ska bedrivas. Vissa av dessa författningar har bäring på myndigheters hantering av information, såsom offentlighets- och sekretesslagen, personuppgiftslagen, registerlagstiftningen och säkerhetsskyddslagen. Andra regelverk ställer krav på åtgärder av betydelse för informationssäkerhetsarbetet. Det finns även reglering kring informationssäkerhet som förbjuder viss typ av handling, exempelvis bestämmelser om dataintrång i brottsbalken. Värt att nämna i sammanhanget är även de standarder som är centrala för informationssäkerhetsarbetet. De anger krav och riktlinjer som är användbara för alla typer av organisationer.

Vi har identifierat ett antal rättsregler som direkt eller indirekt uppställer krav som berör informationssäkerhet och informationssäkerhetsarbete. Närmast presenteras ett urval av sådana författningar och föreskrifter som bedöms vara av särskilt intresse för utredningen.

5.2 Övergripande reglering

5.2.1 Tryckfrihetsförordningen

De grundläggande bestämmelserna om offentlighet och tryckfrihet finns i tryckfrihetsförordningen (TF).

I 2 kap. § 1 TF anges att till främjande av ett fritt meningsutbyte och en allsidig upplysning ska varje svensk medborgare ha rätt att ta del av allmänna handlingar. Där denna rätt kolliderar med mot-

stående intressen finns möjlighet enligt kapitlets andra paragraf att göra vissa inskränkningar i rätten. Paragrafen anger som motstående intressen som kan motivera en begränsning av allmänhetens rätt att ta del av allmänna handlingar: rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation, rikets centrala finanspolitik, penningpolitik eller valutapolitik, myndighets verksamhet för inspektion, kontroll eller annan tillsyn, intresset att förebygga eller beivra brott, det allmännas ekonomiska intresse, skyddet för enskilds personliga eller ekonomiska förhållanden, intresset att bevara djur- eller växtart. Begränsning av handlingsoffentligheten ska anges i särskild lag och måste finna stöd i någon av nämnda punkter. Regelverket ger med andra ord en uttrycklig ram för både krav på tillgänglighet och konfidentialitet rörande allmänna handlingar. Därtill innebär TF:s regler i förlängningen även krav på riktighet och spårbarhet hos informationen. Bristande informationssäkerhet som leder till att myndigheternas information förvanskas hindrar allmänhetens faktiska möjlighet att ta del av allmänna handlingar.

5.2.2 Offentlighets- och sekretesslagen

Offentlighets- och sekretesslagen (2009:400) (OSL) innehåller bestämmelser om hantering av allmänna handlingar samt vilka uppgifter som får sekretessbeläggas. Det är inte bara de uttryckliga kraven på sekretess, det vill säga konfidentialitetskrav, som är av intresse. Även reglerna om god offentlighetsstruktur – det vill säga möjligheten att hålla offentliga handlingar tillgängliga är av betydelse ur ett informationssäkerhetsperspektiv.

Kapitel 15 reglerar sekretess med hänsyn till skydd för rikets säkerhet eller dess förhållande till andra stater eller mellanfolkliga organisationer. I 1 § regleras utrikessekretessen. Vidare finns två nyligen införda bestämmelser om sekretess i det internationella samarbetet, 1 a § och utrikessekretess vid direktåtkomst, 1 b §. I 2 § regleras försvarssekretessen. Föremålet för försvarssekretessen är uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret. Det omfattar därmed mer än enbart uppgifter som rör det militära försvaret. För att undvika ett

onödigt hemlighållande av uppgifter som rör de många verksamhetsområden och företeelser som försvarssekretessen omfattar har bestämmelsen utformats med ett rakt skaderekvisit. Samhällets åtgärder för landets försvar ska således inte undandras offentlighet annat än då det verkligen är påkallat. Sekretessen gäller därför bara om det kan antas att ett röjande av uppgifter skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet.

Kapitel 18 reglerar sekretess till skydd främst för intresset av att förebygga eller beivra brott. I 1 § finns regler till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. Sekretess gäller enligt andra paragrafen för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. 7 § 1 eller 5 kap. 1 § 1 polisdatalagen (2010:361). Enligt det förstnämnda lagrummet får personuppgifter behandlas när det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet. Det polisarbete som åsyftas är i första hand underrättelseverksamhet. Bestämmelser som syftar till informationssäkerhet finns i 8 och 9 §§. 8 § innehåller bestämmelser 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. I bestämmelsen är föremålet för sekretessen uppgifter som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd i vissa angivna avseenden. I 9 § regleras sekretessen för uppgifter som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod. Sekretessen enligt paragrafens första punkt är begränsad till uppgifter om chiffer m.m. som avser att slå vakt om sekretessen i allmän verksamhet. Chiffret ska alltså ha till syfte att underlätta befordran eller användning av uppgifter som omfattas av sekretess. För detta ändamål används bl.a. kryptering. Det kan naturligtvis förekomma att chifferspråk används för meddelanden som inte innehåller uppgifter som omfattas av sekretess eller för vilka sekretess efter en tid inte längre gäller. Också sådana meddelanden i klartext kan hållas hemliga så att chiffret inte kan forceras.

5.2.3 Personuppgiftslagen

Skyddet för personuppgifter är av stor betydelse för myndigheternas informationshantering. Personuppgiftslagen (PUL) innehåller både bestämmelser om hur behandlingen av personuppgifter och känsliga personuppgifter får ske (med direkt betydelse för kraven på tillgänglighet, riktighet, konfidentialitet och spårbarhet) samt hur säkerhetsarbetet ska utformas. Av 1 § framgår att lagens syfte är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

Säkerhet är en viktig del av skyddet för den personliga integriteten. Den som behandlar personuppgifter med hjälp av informationsteknik måste därför skydda uppgifterna. Genom att i lagen begränsa och styra de sätt på vilka man får hantera personuppgifter ges informationen ett särskilt skydd. Lagen innehåller även regler om vilka tekniska och organisatoriska säkerhetsåtgärder den som hanterar personuppgifter ska vidta.

Enligt 31 § PUL ska den som är personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Vilka åtgärder som bör väljas är enligt lagrummet beroende av de tekniska möjligheter som finns, kostnaden för åtgärderna, vilka risker som finns och hur pass känsliga de behandlade personuppgifterna är. Till tekniska åtgärder räknas exempelvis brandväggar, krypteringsfunktioner och antivirus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation, rutiner, instruktioner och policyer. Generellt gäller att ju känsligare personuppgifterna är eller ju fler personuppgifter som hanteras, desto mer omfattande bör säkerhetsåtgärderna vara.

Ansvarig för säkerheten är enligt lagen den personuppgiftsansvarige, det vill säga den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige kan överlåta den faktiska behandlingen av personuppgifter till någon annan som då blir att betrakta som personuppgiftsbiträde. Ett sådant biträde får behandla uppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige. Den personuppgiftsansvarige undgår inte ansvar för eventuella fel som personuppgiftsbiträdet gör.

I 9 § PUL redovisas grundläggande krav på behandlingen av personuppgifter. I paragrafen anges bl.a. att den personuppgifts-

ansvarige ska se till att personuppgifter behandlas bara om det är lagligt, att personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed, att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål och att uppgifterna därefter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Vidare anges det att den personuppgiftsansvarige ska se till att de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen. Av stadgandet framgår vidare att inte heller fler uppgifter än vad som är nödvändigt med hänsyn till ändamålet får behandlas och att alla rimliga åtgärder ska vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen.

Datainspektionen har som tillsynsmyndighet över tillämpningen av PUL utfärdat allmänna råd, lämnat vägledande uttalanden, meddelat beslut m.m. med bäring på informationssäkerhet.

5.2.4 Registerförfattningar

Registerlagstiftningen rör specifika verksamheter och kan innehålla förhållandevis detaljerade krav på informationshanteringen. I detta sammanhang kan nämnas polisdatalagen (2010:361), kustbevakningsdatalagen (2012:145), lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Registerförfattningarnas huvudsakliga syfte är att reglera inrättandet och användningen av viktigare register eller andra personuppgiftssamlingar inom den offentliga sektorn. Den bakomliggande tanken är att myndighetsregister med ett stort antal registrerade och med ett känsligt innehåll ska regleras särskilt genom lag (prop. 1990/91:60 s. 50, KU 1990/91:11 s. 11, se även prop. 1997/98:44 s. 41). Som exempel kan nämnas lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration vilken bland annat uttryckligen reglerar vilka som har behörighet att få tillgång till socialförsäkringsdatabasen.

Registerförfattningarna reglerar myndigheternas behandling av personuppgifter och är tänkta att ge ett anpassat integritetsskydd vid myndighetens hantering av personuppgifter då behov finns att avvika från eller komplettera det integritetsskydd som personuppgiftslagen annars ger. Arbetet med att uppnå ett sådant integritetsskydd som avses i författningarna innebär i praktiken att myndigheterna behöver arbeta systematiskt med informationssäkerhet.

Vissa författningar har enbart bestämmelser om myndigheters informationsbehandling. Andra författningar har en del bestämmelser om informationsbehandling, men också om annat. Ytterligare en grupp författningar handlar i huvudsak om något annat, men har någon enstaka inskjuten regel om hantering av information.

5.2.5 Arkivlagstiftningen

Allmänna handlingar är handlingar (oavsett medium) som har inkommit till eller upprättats hos en myndighet och som förvaras hos myndigheten. De allmänna handlingarna bildar enligt 3 § arkivlagen (1990:782) myndigheternas arkiv. Utgångspunkten är att allmänna handlingar ska bevaras och att gallring endast får ske under vissa förutsättningar, ett krav som ställer uttryckliga krav på tillgängligheten hos informationen.

I arkivlagen (1990:782) och arkivförordningen (1991:446) ges bestämmelser om myndigheternas och vissa andra organs arkiv samt om arkivmyndigheterna. Krav på skydd av allmänna handlingar ställs på myndigheter genom arkivlagen och Riksarkivets föreskrifter.

Av 4 § arkivlagen (1990:782) framgår att varje myndighet ska svara för vården av sitt arkiv. I arkivvården ingår enligt 6 § bl.a. att skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst.

Riksarkivet har genom arkivförordningen fått mandat att meddela föreskrifter för statliga myndigheter om bl.a. skydd av arkivet. Av Riksarkivets medieoberoende föreskrifter RA-FS 1991:1 framgår att handlingar ska under hela bevarandetiden hanteras, förvaras och skyddas så att den fysiska och logiska kvaliteten bibehålls. RA-FS 2013:4 innehåller tekniska krav för arkivlokaler. Av föreskrifterna framgår att handlingar som tillhör myndighetens arkiv ska förvaras i arkivlokal som ger skydd mot vatten och skadlig fukt,

brand, brandgas och skadlig upphettning, skadlig klimat- och miljöpåverkan, samt skadegörelse, tillgrepp och obehörig åtkomst. Vid val av lokalens placering ska myndigheten undersöka om den omgivande miljön är lämplig med hänsyn till dessa skyddskrav. Riskbedömningar måste därför göras av miljön både inom och utanför byggnaden.

Vidare har Riksarkivet utfärdat föreskrifter för elektroniska handlingar som innehåller bestämmelser som handlar bl.a. om skydd av information. Föreskrifterna ställer krav på myndigheter att upprätta en strategi för bevarande av elektroniska handlingar (RA-FS 2009:1, 3 kap). Strategin ska innehålla de åtgärder myndigheten avser att vidta för att säkerställa bevarande av elektroniska handlingar, dvs. hur handlingar ska framställas, överföras, hanteras, förvaras och vårdas under den tid som de ska bevaras. Detta tydliggör att det inte bara är mänskliga misstag, tekniska fel eller antagonistiska hot som kan hindra tillgänglighet. Även en sådan företeelse som att tekniken för informationshantering utvecklas över tid ställer krav på informationssäkerhetsarbetet.

Föreskrifterna om elektroniska handlingar innehåller även krav på att upprätta en plan för informationssäkerhet (RA-FS 2009:1, 6 kap). Planen går ut på att myndigheter ska skapa rutiner för att skydda handlingarna från skada, manipulation, obehörig åtkomst och stöld med utgångspunkt i standarden SS-ISO/IEC 27001:2006 (LIS). Detta kan ske genom bl.a. behörighetskontollsystem, loggsystem, skydd mot skadlig kod, säkerhetskopiering etc.

5.2.6 Lagen om elektronisk kommunikation

I lagen (2003:389) om elektronisk kommunikation (LEK) finns bestämmelser om driftsäkerhet som gäller för alla som tillhandahåller elektroniska kommunikationsnät eller -tjänster. I 5 kap. 6 b § LEK framgår följande:

> 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. De åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott. Regeringen eller den myndighet som

regeringen bestämmer får meddela föreskrifter om på vilket sätt skyldigheten ska fullgöras och om undantag från skyldigheten.

Syftet med bestämmelserna är att bidra till effektiva och säkra elektroniska kommunikationer samt att skapa en grundläggande säkerhetsnivå för dessa. Med driftsäkerhet avses främst upprätthållande av funktion och tillgänglighet, men även uthållighet vid extraordinära händelser i fredstid.

Post- och telestyrelsen (PTS) är tillsynsmyndighet över lagen om elektronisk kommunikation och har tagit fram allmänna råd som förtydligar bestämmelserna och utgör PTS rekommendationer om hur säkerhetsarbete kan bedrivas för att uppfylla kraven i LEK. Säkerhetsarbete innebär i detta fall att förebygga avbrott och störningar genom att genomföra riskanalyser och riskhantering, planera för hantering av avbrott och störningar samt följa upp dessa när de inträffar. PTS har även tagit fram förskrifter som ställer krav på hur operatörerna ska skydda sina kunders uppgifter och kommunikation

Av 6 kap. 3, 3 a och 4 §§ LEK framgår bl.a. att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandlade uppgifter skyddas. Den som tillhandahåller ett allmänt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå, som med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter. Med integritetsincident avses enligt 6 kap. 1 § LEK en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring, eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster. Den som är skyldig att lagra uppgifter enligt LEK ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. Om det vid tillhandhållandet av en allmänt tillgänglig elektronisk kommunikationstjänst finns särskild risk för bristande skydd av behandlade uppgifter, ska den som tillhandahåller tjänsten informera abonnenten om risken.

I 6 kap. 5–10 a §§ LEK regleras behandling av trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter. Med trafik-

uppgift förstås uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller som behövs för att fakturera detta meddelande. Huvudregeln är att det åligger anmälningspliktig tillhandahållare av allmänt kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster att utplåna eller avidentifiera dessa uppgifter när de inte längre behövs för att överföra ett elektroniskt meddelande. 6 kap. 8 § LEK reglerar undantag från operatörernas skyldighet att utplåna och avidentifiera trafikuppgifter när de inte längre behövs för att överföra ett elektroniskt meddelande.

Lokaliseringsuppgift definieras enligt 1 kap. 7 § LEK som uppgift som behandlas i ett elektroniskt kommunikationsnät eller av en elektronisk kommunikationstjänst och som visar den geografiska positionen för terminalutrusningen för en användare. Lokaliseringsuppgifter som inte är trafikuppgifter, till exempel uppgifter om position från satellit, som rör användare som är fysiska personer eller abonnenter får behandlas endast sedan de avidentifierats eller användaren eller abonnenten gett sitt samtycke till behandlingen. Även i detta fall ska information lämnas om vilka uppgifter som kommer att behandlas och syfte med mera.

I 6 kap. 15–16 §§ LEK finns bestämmelser om abonnentförteckning och hur dessa får behandlas och 16 a § reglerar lagring av trafikuppgifter för brottsbekämpande ändamål.

I 5 kap. 1–6 §§ LEK regleras samhällsomfattande tjänster, med vilka avses det minimiutbud av tjänster av viss angiven kvalitet, vilka ska vara tillgängliga för alla användare till ett överkomligt pris. Bestämmelser om vilka de samhällsomfattande tjänsterna är finns i 5 kap. 1 § första stycket LEK. Till dessa tjänster hör enligt första och andra punkterna att uppfylla rimliga krav på anslutning till ett allmänt kommunikationsnät i en fast nätanslutningspunkt och på tillgång till allmänt tillgängliga telefonitjänster i en fast nätanslutningspunkt.

I 5 kap. 6 a–11 §§ LEK regleras de allmänna skyldigheter som gäller bl.a. för den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig telefonitjänst (prop. 2010/11:115 s. 169). Av 5 kap. 6 b § LEK framgår 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. De åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för störningar och avbrott.

Enligt 6 kap. 18 § LEK får uppgifter lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till information om ändamålet med behandlingen och samtycker till den. Syftet med bestämmelsen är att förhindra att internetanvändare spåras utan sitt samtycke. Detta genom att förbjuda att data sparas på, eller hämtas från, användarens terminalutrustning, till exempel dator, mobiltelefon eller surfplatta. Bestämmelsen benämns ibland cookie-lagen.

5.3 Reglering av säkerhetsskydd, krishantering och informationssäkerhetsarbete

5.3.1 Säkerhetsskyddslagstiftningen

I säkerhetsskyddslagen (1996:627) finns bestämmelser om säkerhetsskydd, med vilket enligt 6 § avses 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 (2009:400) (OSL) och som rör rikets säkerhet, och skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorlagen), även om brotten inte hotar rikets säkerhet. Säkerhetsskyddsbestämmelserna reglerar hanteringen av sekretessbelagda uppgifter som rör rikets säkerhet (hemliga uppgifter) så att dess inte röjs, ändras eller förstörs.

Av 7 § säkerhetsskyddslagen framgår att 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) och att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som är av betydelse för rikets säkerhet (säkerhetsprövning). Säkerhetsskyddet ska även i övrigt förebygga terrorism.

Lagen gäller enligt 1 § för staten, kommunerna och landstingen, liksom för bolag, föreningar och stiftelser som dessa har ett rätts-

ligt bestämmande inflytande över, samt för enskilda, om verksamheten är av betydelse för rikets säkerhet eller särskilt behöver skyddas mot terrorism.

När staten, kommuner eller landsting ska begära in anbud eller träffa avtal om upphandling, där det förekommer uppgifter som omfattas av sekretess, ska enligt 8 § ett säkerhetsskyddsavtal träffas med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet.

Enligt 9 § ska vid utformningen av informationssäkerheten behovet av skydd för automatisk informationsbehandling beaktas särskilt.

Av 11 § framgår att säkerhetsprövning ska göras innan en person genom anställning eller på annat sätt deltar i verksamhet som är av betydelse för rikets säkerhet eller för skyddet mot terrorism. Prövningen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas i lagen och i övrigt pålitlig från säkerhetssynpunkt. Säkerhetsprövningen ska omfatta registerkontroll och särskild personutredning. Anställning eller annat deltagande i verksamhet som innebär att en anställd får tillgång till sekretessbelagda uppgifter som har betydelse för rikets säkerhet placeras i så kallade säkerhetsklasser. Det finns tre olika säkerhetsklasser och vilken av dessa en anställning eller annat deltagande i verksamheten placeras i beror på i vilken utsträckning den anställde får del av sekretessbelagda uppgifter som rör rikets säkerhet. När det gäller anställningar som har placerats i säkerhetsklass ska säkerhetsprövningen även omfatta registerkontroll, dvs. att uppgifter hämtas från olika polisregister, och i klass 1 och 2 även särskild personutredning. Registerkontroll kan också göras till skydd mot terrorism.

I säkerhetsskyddsförordningen (1996:633) finns närmare bestämmelser om säkerhetsskydd. Enligt 5 § ska myndigheter och andra som förordningen 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 denna undersökning (säkerhetsanalys) ska dokumenteras. Vidare ska en säkerhetsskyddschef utses enligt 6 §. Säkerhetsskyddschefen ska utöva kontroll över säkerhetsskyddet och vara direkt underställd myndighetens chef.

I 9–13 §§ finns också bestämmelser om informationssäkerhet som bl.a. rör inventering samt försändelse av handlingar som omfattas av sekretess som rör rikets säkerhet (hemliga handlingar). Av 12 § framgår att innan en myndighet inrättar ett register, som ska föras med hjälp av automatisk databehandling och som kan förutses komma att innehålla sådana uppgifter att utlämnandet av dem var för sig eller sammanställda kan skada totalförsvaret, ska myndigheten samråda med Försvarsmakten och, om uppgifternas natur ger anledning till det, Säkerhetspolisen. I fråga om uppgifter av betydelse för rikets säkerhet i övrigt ska i motsvarande fall samråd ske med Säkerhetspolisen. Ett system, som av flera personer ska användas för automatisk informationsbehandling av hemliga uppgifter, ska vara försett med funktioner för behörighetskontroll och registrering av händelser i systemet som är av betydelse för säkerheten. Systemet får inte tas i drift förrän det från säkerhetssynpunkt har godkänts av den för vars verksamhet systemet inrättas.

Enligt 13 § ska myndigheter och andra som förordningen gäller för, innan de sänder hemliga uppgifter i ett datanät utanför sin kontroll, förvissa sig om att det för uppgifterna där finns en fullgod informationssäkerhet. Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten.

Säkerhetspolisen och Försvarsmakten har enligt 39 § säkerhetsskyddsförordningen ansvaret för att kontrollera säkerhetsskyddet hos myndigheterna. Säkerhetspolisen och Försvarsmakten har vidare, med stöd av 43–44 §§ förordningen meddelat verkställighetsföreskrifter för respektive tillsynsområde. I föreskrifterna finns bestämmelser bl.a. om informationssäkerhet.

5.3.2 Lagen (1992:1403) om totalförsvar och höjd beredskap

Lagen (1992:1403) om totalförsvar och höjd beredskap reglerar hur beredskapen i Sverige kan höjas. Enligt 1 § är totalförsvar verksamhet som behövs för att förbereda Sverige för krig. I 2 § förskrivs dock att totalförsvarsresurserna ska utformas så att de även kan stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället. Enligt lagmotiven ska dessa resurser kunna ställas till förfogande även för samhällsverksamhet i fred.

Totalförsvaret ska inte ses som en organisation utan som en verksamhet som, utöver det militära försvaret, innefattar det civila försvaret som till alla delar betecknar och består av olika samhällsorgans verksamhet i syfte att kunna stärka samhällets förmåga att förebygga och hantera svåra nationella påfrestningar i fred. När dessa resurser tas i anspråk i sådan verksamhet är det alltså inte fråga om totalförsvarsverksamhet utan det handlar om att totalförsvarsresurser ställs till förfogande för det samhällsorgan som normalt har att hantera en viss situation. Syftet är således att på ett effektivare sätt utnyttja samhällets samlade resurser och inte att utvidga vad som avses med totalförsvar(prop. 1996/97:4 s. 60).

5.3.3 Förordningen (2006:942) om krisberedskap och höjd beredskap och MSB:s föreskrifter om statliga myndigheters informationssäkerhet

Förordningen (2006:942) om krisberedskap och höjd beredskap innehåller föreskrifter som dels reglerar krisberedskapen, dels ansluter till vad som föreskrivs i lagen (1992:1403) om totalförsvar och höjd beredskap. Bestämmelserna i förordningen 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 (1 §). I förordningen regleras myndigheternas krisberedskap, dvs. förmågan att genom utbildning, övning och andra åtgärder samt genom den organisation och de strukturer som skapas före, under och efter en kris förebygga, motstå och hantera krissituationer, och säkra kryptografiska funktioner (4 §).

Enligt 9 § ska samtliga myndigheter genomföra en riskanalys en gång per år. Syftet är enligt 9 § i förordningen att stärka sin egen och samhällets krisberedskap. Myndigheter med särskilt ansvar för krisberedskapen enligt förordningen ska lämna en redovisning baserad på riskanalysen till Regeringskansliet och Myndigheten för samhällsskydd och beredskap (MSB).

Enligt 18 § förordningen om krisberedskap och höjd beredskap ska de myndigheter som har ett ansvar att vidta de förberedelser som krävs inom respektive ansvarsområde vid höjd beredskap (bevakningsansvariga myndigheter) bl.a. planera för att kunna anpassa verksamheten inför en förändrad säkerhetspolitisk situation.

Av 30 a § KBF framgår att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas. Ett ledningssystem anger i sig inte några säkerhetskrav för verksamheten utan det ger stöd för ledningens och organisationens systematiska arbete med ständig förbättring av informationssäkerheten. Även om kravet finns i krisberedskapsförordningen avser det inte endast krisberedskapsarbete, utan gäller generellt för informationssäkerhetsarbete i statsförvaltningen eftersom ett väl fungerande krisberedskapsarbete underlättas av en stabil och säker informationshantering.

I förordningen anges vidare vilka myndigheter som ska ha säkra kryptografiska funktioner.

Med stöd av 34 § nämnda förordning har MSB utfärdat föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10). Enligt föreskrifterna ska en myndighet upprätthålla säkerhet i sin informationshantering och som ett led i detta arbete tillämpa ett ledningssystem för informationssäkerhet. Detta innebär enligt föreskrifterna att myndigheterna ska ha en informationssäkerhetspolicy, ska ha någon eller några som leder och samordnar informationssäkerhetsarbetet, ska klassificera sin information, ska genomföra risk- och sårbarhetsanalyser och utifrån dessa hantera risker samt ska dokumentera granskningar och vidtagna säkerhetsåtgärder av större betydelse. Föreskrifterna ställer även krav på att ledningen löpande informerar sig om arbetet med informationssäkerhet samt att ledningen minst en gång per år följer upp och utvärderar informationssäkerhetsarbetet på myndigheten.

MSB har med stöd av förordningen även utfärdat föreskrifter om civila myndigheters kryptoberedskap (MSBFS 2009:11)och om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2010:7).

5.3.4 Förordningen om statliga myndigheters riskhantering, m.m.

Förordningen (1995:1300) om statliga myndigheters riskhantering ställer också krav på att myndigheterna genomför en riskanalys. Förordningen riktas dock endast till myndigheter under regeringen och har till syfte att identifiera sådana risker som kan innebära

skador eller förluster för staten. Efter att ha värderat riskerna och uppskattat vilka kostnader riskerna medför ska myndigheten vidta lämpliga åtgärder för att begränsa riskerna och förebygga skador eller förluster. Förordningen (2007:603) om intern styrning och kontroll innebär krav på ordning och reda i informationsflödet och därmed informationssäkerhet.

5.3.5 Lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap

Lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap syftar till att kommuner och landsting ska minska sårbarheten i sin verksamhet och ha en god förmåga att hantera krissituationer i fred. Kommuner och landsting ska därigenom också uppnå en grundläggande förmåga till civilt försvar. Enligt 1 kap. 4 § definieras en extraordinär händelse som en sådan händelse som avviker från det normala, innebär en allvarlig störning eller överhängande risk för en allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser av en kommun eller ett landsting. Lagen föreskriver att det i kommuner och landsting ska finnas en nämnd för att fullgöra uppgifter under extraordinära händelser i fredstid (krisledningsnämnd). Kommuner och landsting ska för varje ny mandatperiod anta en plan för hur extraordinära händelser ska hanteras.

Enligt 2 kap. 1 § ska kommunerna och landstingen ta fram en risk- och sårbarhetsanalys till grund för planen för hur de ska hantera extraordinära händelser. Vidare anges i bestämmelsen att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om risk- och sårbarhetsanalyser samt planer för hantering av extraordinära händelser. Med stöd av 12 § förordningen (2006:637) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap har MSB utfärdat föreskrifter om vad som ska ingå i en risk- och sårbarhetsanalys (MSBFS 2015:5 för kommuner och MSBFS 2015:4 för landsting). Bland de olika förhållanden som kommunen ska kunna redogöra för finns krav på rapportering av hur god förmåga kommunen har att skydda informationens konfidentialitet, tillgänglighet och riktighet.

5.4 Specifik reglering av brottsbekämpande och underrättelsemyndigheters arbete på området

Detta avsnitt handlar om en del av de verktyg som de brottsbekämpande myndigheterna och underrättelsemyndigheterna har för att bekämpa it-brottslighet respektive att stödja svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet.

Utredning av it-relaterad brottslighet ger kunskaper om bl.a. tillvägagångssätt och aktörer, vilket är av stort värde vid utformningen av olika skyddsåtgärder. En effektiv lagföring av it-relaterad brottslighet är viktig för att minska benägenheten att begå sådana brott.

5.4.1 27 kap. rättegångsbalken

I 27 kap. rättegångsbalken (RB) tas upp bestämmelser om flera olika straffprocessuella tvångsmedel som kan sättas in under en förundersökning, nämligen beslag, avspärrning av brottsplats m.m. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning. Datorbehandlingsbara uppgifter kan säkras även genom beslag. Enligt 27 kap. 1 § första stycket rättegångsbalken får bl.a. föremål som skäligen kan antas ha betydelse för utredning om brott tas i beslag (s.k. bevisbeslag). Beslag kan endast avse lösa saker. Eftersom elektronisk information har en bärare, exempelvis en dator, en mobiltelefon eller ett fickminne, som är att betrakta som ett föremål och därför kan tas i beslag är beslagsreglerna tillämpliga även på elektroniska uppgifter.

Frågan om behovet av nya hemliga tvångsmedel i den digitala miljön lyftes fram av Beredningen för rättsväsendets utveckling i betänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38). Utredningen tog upp frågan om införandet av tvångsmedlet hemlig dataavläsning. Hemlig dataavläsning förklarades innebära att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel vid förundersökning i brottmål. Utredningen om vissa hemliga tvångsmedel återkom till frågan i betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44).

5.4.2 Lagen om försvarsunderrättelseverksamhet

Lagen (2000:130) om försvarsunderrättelseverksamhet innehåller bestämmelser om försvarsunderrättelseverksamhetens uppgifter och arbetsformer. Där anges att verksamheten ska bedrivas bl.a. för att kartlägga yttre militära hot mot landet samt att verksamheten inte får avse uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete. I lagen anges att verksamheten ska bedrivas av Försvarsmakten och de andra myndigheter som regeringen bestämmer. I lagen finns också bestämmelser om utlandssamarbete i underrättelsefrågor och om insyn i underrättelseverksamheten.

5.4.3 Lagen om signalspaning i försvarsunderrättelseverksamhet

Lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet omfattar signalspaning för försvarsunderrättelseändamål. Lagen innehåller regler till skydd för den enskildes integritet. Signalspaning sker efter inriktning från regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten. I lagen finns regler om när uppgifter ska förstöras, hur rapportering ska ske, och om användning av sökbegrepp. Signalspaning får endast avse kommunikation som är relevant för verksamheten, och signalspaningsmyndigheten ska ansöka om tillstånd för signalspaning hos Försvarsunderrättelsedomstolen.

5.5 Brottsbalken

Rättslig reglering bidrar till informationssäkerhet genom att ställa krav på att vidta åtgärder men även genom att kriminalisera vissa handlingar. Många brott, som bedrägeri, begås i dag ofta med hjälp av it. Ett brott med uttrycklig koppling till it är dataintrång. Enligt 4 kap. 9 c § brottsbalken (BrB) är det förbjudet att olovligen bereda sig tillgång till en uppgift som är avsedd för automatiserad behandling eller att olovligen ändra, utplåna, blockera eller i register föra

in en sådan uppgift. Det är heller inte tillåtet att olovligen allvarligt störa eller hindra användningen av en sådan uppgift. Den som bryter mot detta kan dömas för dataintrång till böter eller fängelse i högst två år eller för grovt dataintrång till fängelse mellan sex månader och sex år. Sedan den 1 juli 2014 är försök eller förberedelse till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa, eller grovt dataintrång straffbart (4 kap. 10 § BrB).

I 4 kap. 8 § BrB finns bestämmelser om brytande av post- och telehemlighet. Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller i ett elektroniskt kommunikationsnät, döms för brytande av post- eller telehemlighet till böter eller fängelse i högst två år.

I 9 kap. 1 § andra stycket BrB finns bestämmelser om s.k. datorbedrägeri. Gärningsmannen ska genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverka resultatet av en automatisk informationsbehandling eller liknande automatisk process, så att det innebär vinning för honom och skada för någon annan.

Allvarliga angrepp som riktas mot egendom som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning, förvaltning eller upprättande av allmän ordning och säkerhet kan vara att bedöma som sabotage eller grovt sabotage enligt 13 kap. 4 och 5 §§ BrB.

6 Myndigheter med särskilt ansvar för informationssäkerhet

Ansvaret för styrning och ledning av statsförvaltningens informations- och cybersäkerhet är fördelat mellan riksdagen, regeringen samt de av regeringen utsedda tillsyns- och stödmyndigheterna. Ett operativt ansvar är också fördelat till den enskilda myndighetsledningen i övriga myndigheter.

Informations- och cybersäkerhet är en viktig del av krisberedskapen. Grunden för samhällets krisberedskap är ansvarsprincipen (prop. 2007/08:92, bet. 2007/08:FöU12, rskr. 2007/08:193). Det innebär att den som har ansvar för en verksamhet under normala förhållanden också har det under allvarliga händelser, kriser eller krig. I ansvarsprincipen ingår även att samverka med andra, ofta sektorsövergripande, i den omfattning som krävs för att effektivt förebygga och hantera en allvarlig händelse. Samverkansdelen i ansvarsprincipen betonas särskilt i den redovisning av krisberedskapen som lämnades av regeringen till riksdagen i mars 2014. Vidare framhålls vikten av att ansvar och roller anges tydligt för att en ändamålsenlig samverkan ska nås (lagen om sprängämnesprekursorer och redovisning av krisberedskapens utveckling, prop. 2013/14:144 s. 51). Detta tydliggörs även genom kravet på att myndigheterna ska samverka och stödja varandra i 5 § förordningen (2006:942) om krisberedskap och höjd beredskap (KBF).

Det finns flera statliga myndigheter med särskilda uppgifter eller uppdrag på informations- och cybersäkerhetsområdet, såväl nationellt som internationellt, och frågorna spänner över en mängd olika områden och nivåer. De statliga myndigheterna bör utveckla sin förmåga att samverka inom informationssäkerhetsområdet. För att underlätta denna förmåga behövs enligt denna utrednings direktiv en enhetlig och samlad beskrivning av respektive myndighets

ansvar och roll utifrån dagens uppgifter och uppdrag på informationssäkerhetsområdet. I kapitlet lämnas en sådan beskrivning.

6.1 Myndigheter i samverkansgruppen för informationssäkerhet (SAMFI)

6.1.1 Myndigheten för samhällsskydd och beredskap (MSB)

Myndigheten för samhällsskydd och beredskap (MSB) har enligt 1 § förordningen (2008:1002) med instruktion för Myndigheten för samhällskydd och beredskap ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris. Myndigheten ska

- utveckla och stödja samhällets beredskap mot olyckor och kriser och vara pådrivande i arbetet med förebyggande och sårbarhetsreducerande åtgärder,
- arbeta med samordning mellan berörda aktörer i samhället för att förebygga och hantera olyckor och kriser,
- bidra till att minska konsekvenser av olyckor och kriser,
- följa upp och utvärdera samhällets krisberedskapsarbete, och
- se till att utbildning och övningar kommer till stånd inom myndighetens ansvarsområde.

När det gäller förebyggande och förberedande arbete ska myndigheten enligt 2 § 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 ska enligt 5 § se till att utbildning inom krisberedskapsområdet tillhandahålls. Myndigheten ska därtill genomföra övningar inom sitt ansvarsområde. Myndigheten ska vid behov

stödja Regeringskansliet i utbildnings- och övningsverksamheten inom krisberedskapsområdet. Vidare ska myndigheten se till att ledningsmetoder, stödsystem och materiel för krishantering utvecklas och tillhandahålls.

När det gäller samordning och stöd vid olyckor och kriser ska myndigheten enligt 7 § ha förmågan att bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av berörda myndigheters åtgärder vid en kris. Myndigheten ska se till att berörda aktörer vid en kris får tillfälle att

- samordna krishanteringsåtgärderna,
- samordna information till allmänhet och media,
- effektivt använda samhällets samlade resurser och internationella förstärkningsresurser, och
- samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder.

Myndigheten ska ha förmågan att bistå Regeringskansliet med underlag och information i samband med allvarliga olyckor och kriser.

För uppföljning, utvärdering och lärande ska myndigheten enligt 10 § såväl områdesvis som på en övergripande samhällsnivå följa upp och utvärdera krisberedskapen och bedöma om vidtagna åtgärder fått önskad effekt. Vidare ska myndigheten kunna göra en samlad bedömning av olycksutvecklingen och det säkerhetsarbete som är kopplat till den.

Myndigheten ska enligt 11 § se till att erfarenheter tas till vara från inträffade olyckor och kriser. Till stöd för detta ska myndigheten tillhandahålla tvärsektoriella och samlade bilder och bedömningar samt utveckla kompetens och metodik inom området som tillgodoser nationella, regionala och lokala behov.

Avseende informationssäkerhet ska myndigheten enligt 11 a § stödja och samordna arbetet med samhället informationssäkerhet samt 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. Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som

kan leda till behov av åtgärder inom olika nivåer och områden i samhället. Myndigheten ska vidare svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Myndigheten ska i detta arbete

- agera skyndsamt vid inträffade it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbetet som krävs för att avhjälpa eller lindra effekter av det inträffade,
- samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och
- vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

Myndigheten ska enligt 17 a § vara Sveriges kontaktpunkt för skydd av europeisk kritisk infrastruktur enligt artikel 10.1 i 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.

Vid avdelningen för risk- och sårbarhetsreducerande arbete bedrivs myndighetens verksamhet för samhällets informations- och cybersäkerhet. Enheten för systematiskt informationssäkerhetsarbete lämnar råd och stöd om det förebyggande arbetet inom området till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Enheten lämnar även råd och stöd till andra statliga myndigheter, kommuner och landsting i arbetet med risk- och sårbarhetsanalyser. Enheten ansvarar för webbplatsen Informationssäkerhet.se. Enheten svarar vidare för att analysera och bedöma omvärldsutvecklingen inom sitt område.

Enheten för cybersäkerhet och skydd av kritisk informationsinfrastruktur lämnar råd och stöd till tekniskt förebyggande arbete inom området, med fokus på kritisk informationsinfrastruktur, till andra statliga myndigheter, kommuner och landsting samt företag och organisationer. Enheten ansvarar för myndighetens arbete med säkra kryptografiska funktioner för det civila samhället och för arbetet med myndighetens uppdrag vad avser eter- och medieberedskap. Enheten leder och samordnar arbetet med informationssäkerhet i myndig-

hetens externa kommunikationstjänster, som WIS, SGSI och RAKEL, för ledning och samverkan så att användarnas behov och krav tillgodoses. Enheten ansvarar vidare för att analysera och bedöma omvärldsutvecklingen inom sitt område.

Enheten för operativ cybersäkerhet och it-incidenthantering upprätthåller Nationell operativ samverkansfunktion för informations- och cybersäkerhet (NOS). Personal från enheterna för systematiskt informationssäkerhetsarbete och för cybersäkerhet och skydd av kritisk informationsinfrastruktur ingår i NOS. Som en del i arbetet med att stödja samhället med att hantera och förebygga it-incidenter ska enheten upprätthålla funktionen CERT-SE, som är Sveriges del av det internationella nätverket av Computer Emergency Response Teams (CERT). Enheten är den operativa kontaktpunkten gentemot motsvarande funktioner i andra länder. Enheten säkerställer att myndighetens verksamhet vad gäller samhällets informations- och cybersäkerhet i sin helhet kan agera skyndsamt vid inträffade it-incidenter genom att sprida information samt vid behov samordna åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade. Enheten har ett ansvar för att operativt stödja arbetet med it-säkerheten i de av myndighetens externa lednings- och stödsystem som kräver det. Enheten ansvarar vidare för webbplatsen cert.se. Enheten ansvarar även för att analysera och bedöma omvärldsutvecklingen inom sitt område. I det ingår bl.a. löpande omvärldsbevakning, att producera och delge anpassad information till relevanta aktörer.

Vid avdelningen för risk- och sårbarhetsreducerande arbete finns också Enheten för skydd av samhällsviktig verksamhet. Enhetens huvudsakliga uppgifter är att stödja och utveckla samhällets förmåga att förebygga och mildra effekterna av naturolyckor och stödja arbetet med säkerhet i samhällsplanering, anpassning till ett förändrat klimat och skydd av kritisk infrastruktur samt att höja förmågan att motstå störningar i samhällsviktig verksamhet. Enheten har ansvar för stöd och utveckling av samhällets systematiska säkerhets- och krishanteringsarbete särskilt i fråga om metodstöd till risk- och sårbarhetsanalyser, kontinuitetshantering och kritiska beroenden enligt förordningen (2006:942) om krisberedskap och höjd beredskap och lagen (2006:544) om kommuners och lands-

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

I arbetet med säkra kryptografiska funktioner för det civila samhället samordnar MSB arbetet med civila myndigheters signalskyddsverksamhet och arbete med säkra kryptografiska funktioner. I denna uppgift ingår att vara kravställare gentemot Förvarsmakten vid utveckling av nya system. MSB är bemyndigad av regeringen i enlighet med 31§ förordningen (2006:942) om krisberedskap och höjd beredskap att besluta om vilka myndigheter som ska kunna kommunicera med kryptografiska funktioner, utöver de som regeringen har pekat ut i krisberedskapsförordningen. Dessutom kan MSB besluta om och ingå avtal med de kommuner, organisationer och företag som ska tilldelas säkra kryptografiska funktioner. MSB fattar årligen ett 30-tal tilldelningsbeslut och har tilldelat cirka 160 olika organisationer säkra kryptografiska funktioner, till dessa räknas myndigheter, landsting, kommuner och privata företag. MSB:s beslut effektueras av Försvarets radioanstalt. Vidare föreskriver MSB genom MSBFS 2009:11 om den signalskyddsberedskap som gäller för de myndigheter och organisationer som tilldelats signalskydd.

MSB deltar i internationella samarbeten som rör informations- och cybersäkerhet, t.ex. informationsdelning och samarbete mellan nordiska nationella CERT-funktioner och samarbete inom nätverket European Governmental CERTs (EGC), samt internationell samverkan kring säkerhet i it-produkter, säkerhet i industriella informations- och styrsystem, cybersäkerhet i finansiella tjänster och standardisering kopplad till informationssäkerhet (ISO). MSB deltar i EU-kommissionens expertgrupp European forum for member states (EFMS) och den privat-offentliga plattformen för nät- och informationssäkerhet (NIS-plattformen) samt representerar Sverige i Natos planeringsgrupp för industriella resurser och kommunikation (IRCSG).

6.1.2 Post- och telestyrelsen (PTS)

Post- och telestyrelsen (PTS) är tillsynsmyndighet för lagen (2003:389) om elektronisk kommunikation, se avsnitt 5.2.6. Av 1 § förordningen (2007:951) med instruktion för Post- och tele-

styrelsen framgår att PTS är en förvaltningsmyndighet med ett samlat ansvar inom postområdet och området för elektronisk kommunikation. Myndigheten ska verka för att målen inom politiken för informationssamhället uppnås. Myndigheten ska även, inom ramen för sina uppgifter enligt lagen (2003:389) om elektronisk kommunikation, verka för att de mål som anges i denna lag uppnås.

Myndigheten ska beskriva och analysera utveckling och resultat inom sitt ansvarsområde och rapportera detta till regeringen. Myndigheten ska särskilt uppmärksamma och analysera eventuella problem inom området och, när det är påkallat, vidta eller lämna förslag till lämpliga åtgärder. Myndigheten ska vidare regelbundet göra strategiska analyser inom området för elektronisk kommunikation och redovisa den långsiktiga inriktningen av myndighetens tillämpning av regleringen på området.

Det anges även i 4 § i förordningen (2007:951) med instruktion för Post- och tele-styrelsen att inom området för elektronisk kommunikation har PTS bl.a. till uppgift att

- främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att tillse att samhällsomfattande tjänster finns tillgängliga,
- följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation,
- pröva frågor om tillstånd och skyldigheter och utöva tillsyn enligt lagen (2003:389) om elektronisk kommunikation,
- meddela föreskrifter enligt förordningen (2003:396) om elektronisk kommunikation,
- utöva tillsyn enligt lagen (2000:832) om kvalificerade elektroniska signaturer samt meddela föreskrifter enligt förordningen (2000:833) om kvalificerade elektroniska signaturer,
- utöva tillsyn enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,
- verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, samt verka för ökad krishanteringsförmåga,

- verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer, och
- lämna råd och stöd till myndigheter, kommuner och landsting samt företag, organisationer och andra enskilda i frågor om nätsäkerhet (4 § 1, 7, 8, 9, 13, 14, 15, 16 och 17).

I 7 § förordningen anges att beträffande EU-arbetet och annat internationellt samarbete ska PTS

- vara det behöriga organ som får begära råd och stöd enligt Europaparlamentets och rådets förordning (EG) nr 526/2013 av den 21 maj 2013 om Europiska unionens byrå för nät- och informationssäkerhet (ENISA) och om upphävande av förordningen (EG) nr 460/2004, och
- delta i arbetet i internationella organ i frågor som rör internets förvaltning genom att vid behov företräda Sverige i dessa organ och genom att bereda ärenden med intressenter på nationell nivå.

Av förordningen framgår även att PTS genom upphandling får stärka samhällets beredskap mot allvarliga störningar av elektronisk kommunikation i fred (8 § 4). Det anges också i 11 § förordningen att PTS ska verka för att företag och andra enskilda har förtroende för samt förmåga och möjlighet att använda it och elektroniska kommunikationstjänster (11 § andra stycket).

I lagen (2003:89) om elektronisk kommunikation (LEK) finns bl.a. bestämmelser om säkerhet som gäller för den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst. Av 5 kap. 6 c § LEK framgår att den som tillhandahåller ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål ska rapportera störningar eller avbrott av betydande omfattning till PTS.

Det är Nätsäkerhetsavdelningen vid PTS som ansvarar för arbetet med robust kommunikation samt frågor kring säkerhet och integritet.

PTS arbetar med informationssäkerhet i enlighet med sin instruktion och lagen om elektronisk kommunikation. PTS har bl.a. tagit fram en vägledning för användare om hur man kan anskaffa robust kommunikation. Råd lämnas bl.a. om hur man ställer adekvata krav vid anskaffningen och hur man identifierar kritiska funktioner genom en risk- och sårbarhetsanalys.

6.1.3 Försvarsmakten

Försvarsmaktens övergripande ansvar är att upprätthålla och utveckla ett militärt försvar (1 § förordningen [2007:1266] med instruktion för Försvarsmakten). Enligt 2 § i instruktionen ska myndigheten kunna försvara Sverige och främja svensk säkerhet genom insatser nationellt och internationellt. Vidare ska Försvarsmakten med myndighetens befintliga förmåga och resurser kunna lämna stöd till civil verksamhet. När det gäller stöd till civil verksamhet m.m. se vidare lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning, förordningen (2006:344) om Försvarsmaktens stöd till polisen vid terrorismbekämpning och förordningen (2002:375) om Försvarsmakens stöd till civil verksamhet.

Bland Försvarsmaktens verksamhetsuppgifter ingår att bedriva omvärldsbevakning och kunna upptäcka och identifiera yttre hot mot Sverige, svenska intressen och de insatser som Sverige deltar i (3 § första stycket förordningen med instruktion för Försvarsmakten).

Försvarsmakten ska även bedriva försvarsunderrättelseverksamhet, 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 annan signalskyddsverksamhet (3 b § 1–4 förordningen med instruktion för Försvarsmakten).

Försvarsmakten får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret, förutom i fråga om verkställigheten av 33 § förordningen (2006:942) om krisberedskap och höjd beredskap (33 § förordningen med instruktion för Försvarsmakten).

Enligt 1 § lagen (2000:130) om försvarsunderrättelseverksamhet ska försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Verksamheten får endast avse utländska förhållanden. I lagen finns bestämmelser om försvarsunderrättelseverksamhetens inriktning. Inom försvarsunderrättelseverksamheten får det inte vidtas åtgärder som syftar till att lösa uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet (4 §).

Försvarsmakten har ansvar för kontroll av säkerhetsskyddet samt utfärdande av föreskrifter om verkställighet av säkerhetsskyddslagen för sitt tillsynsområde (39 § 1 säkerhetsskyddsförordningen [1996:633]).

Försvarsmakten ansvarar för skydd av sina egna lednings- och informationssystem.

Försvarsmakten ställer för strategiska kommunikationer operativa krav vad avser robusthet, redundans, skydd och drift. Försvarsmakten har genom Försvarets Telenät (FTN) lång erfarenhet av drift av ledningssystem. Utöver Försvarsmakten använder bl.a. av Riksdagen, Regeringskansliet, Polismyndigheten, FMV, FOI och FRA, MSB och PTS Försvarets Telenät.

Försvarsmakten har påbörjat förberedelser för inrättandet av krigsförbandet Försvarsmaktens telekommunikations- och informationssystemförband (FMTIS) i insatsorganisationen. FMTIS ska ha hand om drift och övervakning av infrastruktur, drift av centrala it-system och etablerande av nya system. Förbandet ska bestå av Försvarsmaktens telenät- och markteleförband, Försvarsmaktens logistik och operativ ledningsteknisk bataljon. IT-försvarsförbandet med FM-CERT har hand om försvar av Försvarsmaktens it-infrastruktur och stödjer också systemdrift. Teknikkontor ledningssystem tar fram systemlösningar. Vid Ledningsregementet med telekrigsbataljonen finns rörliga ledningsförband för telekrigföring.

Juridiska staben vid Högkvarteret gjorde 2012 en studie beträffande de rättsliga förutsättningarna för Försvarsmaktens verksamhet i cyberområdet. Syftet med studien var att konkretisera cyberområdet och skapa beslutsunderlag för att bättre inrikta förmågeutvecklingen och öka effekten och rationaliteten inom Försvarsmakten på cyberområdet.

Försvarsmakten deltar i internationella samarbeten som rör cyberförsvar och cybersäkerhet, t.ex. informationsdelning och samarbete mellan nordiska militära CERT:ar, multinationellt forum för harmonisering av planeringsmodeller inom cyberförsvar och förmågeutveckling enligt NATO standarder.

Militära underrättelse- och säkerhetstjänsten (Must) vid Högkvarteret leder och ansvarar för Försvarsmaktens verksamhetsområde underrättelse- och säkerhetstjänst. När det gäller underrättelsetjänst hämtar Must på uppdrag av regeringen och ÖB in information som analyseras och delges som underrättelserapporter. Den militära säkerhetstjänsten bedrivs inom tre huvudområden. Säkerhetsunderrättelsetjänsten upptäcker, klarlägger och motverkar säkerhetshot som riktas mot Försvarsmakten och dess intressen inom och utom landet. Säkerhetsskyddstjänsten förebygger bl.a. att uppgifter som omfattas av sekretess och som rör rikets säkerhet inte röjs, och att endast personer som är pålitliga utifrån säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet. Bland säkerhetsskyddsåtgärder ingår att lämna stöd till andra myndigheter inom området säkra kommunikationer. Signalskyddstjänsten förhindrar att obehöriga får insyn i, eller kan påverka totalförsvarets telekommunikationer. Signalskydd omfattar även användning av krypton i it-system. Vid Musts Säkerhetskontor finns Säkerhetsunderrättelseavdelningen, Säkerhetsskyddsavdelningen och Avdelningen för Krypto och IT-säkerhet. Sistnämnda avdelning producerar och distribuerar kryptonycklar, aktiva kort och certifikat till totalförsvaret samt utövar rollen som CA (Certification Authority). FMV upphandlar efter beställning från Försvarsmakten system (signalskydd och krypto) av industrin. Avdelningen deltar i projekten med kravställning, verifiering, bedömning och godkännande av signalskyddssystem och Krypto för Skyddsvärda Uppgifter (KSU). Avdelningen stödjer Utrikesdepartementet i rollen som National Security Authority avseende NCSA (National Communications Security Authority) och tecknar med bemyndigande från Regeringskansliet COMSEC-avtal med andra länder och deltar i EU CSC(IA), avseende NDA (National Distribution Authority) med ansvar för kryptonyckelproduktion, distribution och materieluppföljning samt TA (Tempest Authority) med bedömningar och deltagande i EU ITTF. Avdelningen har vidare funktionen som AQUA (Appropriately Qualified Authority) dvs.

godkänd andrapartsevaluerare av krypto inom EU. Avdelningen bidrar också med stöd vid export av svenska kryptosystem på uppdrag av Försvarsexportmyndigheten. Det finns i dag fem svenska kryptosystem som godkänts av Europeiska unionens råd.

När det gäller it-säkerhet kravställer, verifierar, bedömer och godkänner avdelningen it-säkerhetsprodukter/mekanismer för Försvarsmakten. Avdelningen har hand om inriktningen av Försvarsmaktens utveckling av it-system med avseende på it-säkerhet och signalskydd. Vidare stödjer avdelningen utvecklingen av it-system. Avdelningen bedömer och godkänner säkerhetsfunktioner för Försvarsmaktens it-system. Avdelningen har tagit fram Krav på Säkra Funktioner (KSF), i vilka specificeras de it-säkerhetsegenskaper som it-system i Försvarsmakten ska ha.

Vid Försvarsmakten finns också Försvarsmaktens underrättelse- och säkerhetscentrum (FMUndSäkC). Centret tillgodoser Försvarsmaktens behov av kompetens, metodik, och teknik inom underrättelse- och säkerhetstjänst, samt inom språk.

6.1.4 Försvarets materielverk (FMV)

Försvarets materielverk (FMV) ska på uppdrag av Försvarsmakten vidmakthålla, destruera och kassera varor samt upphandla byggentreprenader, varor och tjänster. Myndigheten ska vidare på uppdrag av Försvarsmakten tillhandahålla logistik i form av service, förråds-, och verkstadstjänster. Myndigheten ska också biträda Försvarsmakten i materielförsörjnings- och logistikförsörjningsplanering samt med materialsystemkunskap (1 § förordningen [2007:854] med instruktion för Försvarets materielverk).

FMV ska vara patentorgan för de myndigheter som hör till Försvarsdepartementet och handlägger ärenden som rör immaterialrättsliga frågor.

FMV får inom sitt verksamhetsområde även tillhandahålla tjänster åt andra än Försvarsmakten (6 §).

Vid FMV finns ett certifieringsorgan som ska upprätta och driva en certifieringsordning för säkerhet i it-produkter och system (5 §). FMV ska verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat. CSEC (Sveriges Certifieringsorgan för it-säkerhet) ansvarar för certifiering av it-säkerhetspro-

dukter inom ramen för den internationella standarden ISO/IEC IS 15408 (Common Criteria). Arbetet bedrivs inom ramen för CCRA (Common Criteria Recognition Arrangement) som bygger på ömsesidigt erkännande av certifikat utfärdade av i dag 26 medlemsländer. CSEC utfärdar även certifikat enligt EA-MLA (European Cooperation for Accreditation Multilateral Agreement) och enligt SOGIS-avtalet (SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates). SOGIS (Senior Officials Group Information Systems Security) är en rådgivande funktion kopplad till EU-kommissionen. CSEC har vidare i enlighet med mål i handlingsplan för informationssäkerhet 2012 tagit fram en särskild kryptopolicy. CSEC är sedan 2008 ackrediterat av Styrelsen för ackreditering och teknisk kontroll (Swedac).

FMV bedriver verksamhet inom området för säkerhetsskydd vad avser anbudsgivare och leverantörer som har träffat säkerhetsskyddsavtal (41 § säkerhetskyddsförordningen [1996:633]).

FMV bedriver också försvarsunderrättelseverksamhet enligt 2 § förordningen (2000:131) om försvarsunderrättelseverksamhet.

6.1.5 Försvarets radioanstalt (FRA)

Försvarets radioanstalt har enligt förordningen (2007:937) med instruktion för Försvarets radioanstalt till uppgift att bedriva signalspaning (1 §). Myndigheten ska särskilt följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, och utföra matematiska bedömningar av kryptosystem för totalförsvaret (2 §).

Försvarets radioanstalt ska också biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem (3 §).

Enligt 1 § enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.

Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att kartlägga

- yttre militära hot mot landet,
- förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
- strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
- utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
- allvarliga yttre hot mot samhällets infrastrukturer,
- konflikter utomlands med konsekvenser för internationell säkerhet,
- främmande underrättelseverksamhet mot svenska intressen, eller
- främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om internationellt samarbete på försvarsunderrättelseområdet. Signalspaningsmyndigheten får för den verksamhet som anges i 1 § tredje stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer (9 § lagen (2008:717) om signalspaning).

Försvarets radioanstalt ska vidare enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt ha hög teknisk kompetens inom informationssäkerhetsområdet. Myndigheten får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvars-

politiskt avseende. Försvarets radioanstalt ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser, och ge annat tekniskt stöd.

Bland myndighetens tjänster ingår informationssäkerhetsanalyser, stöd vid kvalificerade it-incidenter, forensisk analys, teknisk rådgivning och utbildning i it-säkerhet. Vid informationssäkerhetsanalyser kontrolleras sårbarheter i uppdragsgivarens itsystem och en bild ges av vilka brister som behöver åtgärdas.

Vid myndigheten finns en forsknings- och utvecklingsenhet med uppgift att metodiskt upptäcka och analysera sårbarheter i informationsmiljöer.

Försvarets radioanstalt ska samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet (4 §). Myndigheten deltar både i bilaterala och multilaterala internationella samarbeten för informationsdelning inom informations- och cybersäkerhetsområdet.

Försvarets radioanstalt ska enligt sitt regleringsbrev upprätthålla kompetensen för de nationella behoven avseende kryptologi. Myndigheten utför via kryptologpoolen matematiska bedömningar av kryptosystem för totalförsvaret. Genom de matematiska bedömningarna tillser Försvarets radioanstalt att kunskapen från myndighetens signalspaningsuppdrag kommer totalförsvaret till godo. Myndigheten stödjer även bland annat Utrikesdepartementet, ISP och Rikspolisstyrelsen med kryptologisk kompetens.

Försvarets radioanstalt tillhandahåller av Försvarsmakten nationellt godkända kryptografiska funktioner till civila myndigheter och företag vilket gör det möjligt att utbyta sekretessbelagd information. FRA har en nationellt godkänd kryptoverkstad samt är förvaltare av civil signalskyddsmateriel. Användarstöd kring regelverk, teknik och övrig support lämnas dygnet runt. FRA är kryptonyckel- och certifikatombud, samt ansvarar för att behovet av behörighetsgivande utbildningar inom den civila sektorn uppfylls. Försvarets radioanstalt fick den 14 april 2010 i uppdrag av regeringen att lämna förslag på hur ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur (TDV) kan utformas och införas (Fö2010/703/SSK). Uppdraget redovisades i en rapport i mars 2011. – Myndigheten för

samhällsskydd och beredskap (MSB) fick samtidigt i uppdrag att lämna förslag på vilka aktörer som bör komma i fråga för att delta i ett sådant system. MSB redovisade uppdraget i en rapport i mars 2011. – I rapporten föreslogs att de myndigheter som har ett särskilt ansvar vad gäller krisberedskap och höjd beredskap erbjuds att delta i ett nationellt detekterings- och varningssystem. I en senare fas borde även andra aktörer, såsom landsting och kommuner, erbjudas att få ansluta sig. Även ägare av samhällsviktig verksamhet och kritisk infrastruktur föreslogs delta i ett senare skede.

Försvarets radioanstalt fick den 10 november 2011 (Fö2011/1681/SSK) i uppdrag av regeringen att komma in med ett kompletterande underlag avseende föreslaget system och att utarbeta en pilotversion av systemet. Uppdraget redovisades i april 2012. Försvarets radioanstalt föreslog i rapporten att föreslaget TDV-system med varnande och skyddande sensorer bör placeras hos särskilt skyddsvärd verksamhet med behov av ett förstärkt skydd mot underrättelsehot från kvalificerade aktörer. Pilotverksamheten visade att det tekniska konceptet med varnande sensor fungerade, medan systemet med skyddande sensorer behövde vidareutvecklas genom ytterligare försöksverksamhet. Enligt Försvarets radioanstalt borde framtagande och utplacering av ett TDV-system inledningsvis ske i begränsad skala och rutiner, teknikstöd samt arbets- och samverkansformer utvecklas efter hand. Försvarets radioanstalt föreslog också att det inrättades ett nationellt cyberråd med företrädare för berörda departement och eventuellt myndigheter, industri samt universitet och högskolor.

I dag pågår verksamheten med ett begränsat antal anslutna aktörer. Förslagen i rapporten bereds inom Regeringskansliet.

I FRA:s instruktion anges att myndigheten ska medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system. De kvalificerade aktörer som FRA följer inom underrättelseverksamheten anges i regeringens årliga inriktning.

De kvalificerade aktörerna utgörs i huvudsak av statsunderstödda aktörer och som utgör hot mot de mest skyddsvärda verksamheterna.

Därutöver får FRA kunskap om hotbilden mot svenska verksamheter genom TDV. TDV-system bygger på nära koppling mellan signalunderrättelseverksamhet inriktad mot it-hot och teknisk informationssäkerhet och har goda möjligheter att förstärka

skyddet för de verksamheter som omfattas av ett TDV-system. Kopplat till hotbilden får FRA även kunskap om sårbarheter i it-system hos de statliga myndigheter och bolag där FRA genomför it-säkerhetsanalyser.

6.1.6 Polismyndigheten

Den 1 januari 2015 ombildades Polisen från 21 fristående polismyndigheter, Rikspolisstyrelsen och Statens kriminaltekniska laboratorium till en Polismyndighet. Vid samma tidpunkt ombildas Säkerhetspolisen till en fristående myndighet.

Polismyndigheten är en enrådighetsmyndighet med ett nationellt insynsråd samt ett regionpolisråd i varje polisregion.

Av 1 § polislagen (1984:387) framgår att Polismyndighetens arbete syftar till att upprätthålla allmän ordning och säkerhet samt att i övrigt tillförsäkra allmänheten skydd och annan hjälp.

Av 2 § polislagen (1984:387) framgår att det till Polismyndighetens uppgifter hör att

1. förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten,
2. övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat,
3. utreda och beivra brott som hör under allmänt åtal,
4. lämna allmänheten skydd, upplysningar och annan hjälp, när sådant bistånd lämpligen kan ges av polisen,
5. fullgöra den verksamhet som ankommer på Polismyndigheten enligt särskilda bestämmelser.

Av 2 b § polislagen (1984:387) framgår att det vid Polismyndigheten ska finnas en avdelning som på nationell nivå leder och samordnar viss polisverksamhet (Nationella operativa avdelningen).

Den nationella operativa enheten består av flera enheter varav en utredningsenhet. Vid utredningsenheten finns it-brottssektionen.

Den 4 juli 2014 fattades beslut (Ju 2012:16/2013/4) av Genomförandekommittén för nya Polismyndigheten att dåvarande Riks-

kriminalpolisen skulle säkerställa ett inrättande av ett it-brottscentrum vid den nationella operativa enheten i den nya Polismyndigheten.

6.1.7 Säkerhetspolisen

Av förordningen (2014:1103) med instruktion för Säkerhetspolisen framgår att Säkerhetspolisen i egenskap av säkerhetstjänst bedriver underrättelse- och säkerhetsarbete och att Säkerhetspolisens huvudsakliga uppgifter och ansvar framgår av 3 § polislagen (1984:387). Av denna bestämmelse framgår att det 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),
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.

Enligt 6 § i instruktionen får Säkerhetspolisen, 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 och andra särskilt viktiga samhällsintressen. Av 7 § framgår att Säkerhetspolisen efter medgivande av regeringen i ett särskilt fall får bedriva uppdragsverksamhet när det gäller säkerhetsskydd och annat säkerhetsarbete.

När det gäller informationssäkerhet arbetar Säkerhetspolisen med att förebygga brottsliga handlingar i form av spionage som sker genom s.k. elektroniska angrepp. Arbetet består i första hand av säkerhetsskyddsåtgärder och utredning av särskilt skyddsvärda verksamheter. Vidare arbetar Säkerhetspolisen med att förebygga allvarliga elektroniska angrepp riktade mot samhällsviktiga it-system.

Säkerhetspolisen analyserar och utreder också allvarliga elektroniska angrepp mot samhällsviktiga verksamheter. Vidare utövar Säkerhetspolisen tillsyn enligt säkerhetsskyddslagen (1996:627), varvid tillsynen bl.a. kan avse informationssäkerhet.

6.2 Andra statliga myndigheter och affärsverk

6.2.1 Datainspektionen

Datainspektionen har enligt 1 § förordningen (2007:975) med instruktion för Datainspektionen i uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter. Myndigheten ska särskilt inrikta sin verksamhet på att informera om gällande regler samt ge råd och hjälp åt personuppgiftsombud. Myndigheten ska följa och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik.

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen (1998:204) och lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Myndigheten är också Sveriges nationella tillsynsmyndighet för behandling av personuppgifter enligt Schengenkonventionen, konventionen om EU:s tullinformationssystem samt rådsbeslutet om inrättandet av Europeiska polisbyrån (Europol).

It-säkerhet utgör ett viktigt område för Datainspektionens arbete. Det är myndighetens uppgift att upptäcka och påtala brister och att informera om hur personuppgifter bör skyddas på lämpligt sätt på internet. Myndigheten har bl.a. tagit fram en vägledning om inbyggd integritet i it-system för skydd av den personliga integriteten och en vägledning som tydliggör vilka krav som personuppgiftslagen ställer vid användning av molntjänster. Myndigheten har 2011 inom ramen för ett särskilt projekt granskat användningen av molntjänster och har även i sin tillsynsverksamhet enligt personuppgiftslagen uppmärksammat brister vid användning av sådana tjänster.

6.2.2 Styrelsen för ackreditering och teknisk kontroll (SWEDAC)

Styrelsen för ackreditering och teknisk kontroll (SWEDAC) ansvarar bl.a. för frågor om teknisk kontroll, inklusive ackreditering och frågor i övrigt om bedömning av överensstämmelse (1 § förordningen [2009:895] med instruktion för Styrelsen för ackreditering och teknisk kontroll).

Vid SWEDAC finns en rådgivande teknisk kommitté inom ackrediteringsområdet certifiering, informationssäkerhet och it-säkerhet.

Ackreditering är ett formellt erkännande av att ett företag eller en organisation har kompetens att utföra vissa specificerade uppgifter inom provning, kontroll och certifiering. Ackreditering innebär att SWEDAC regelbundet och oberoende granskar kompetens och arbetsrutiner hos det organ som är ackrediterat. Granskningen görs mot krav som finns i bestämda standarder och olika myndigheters föreskrifter. Ackreditering är obligatorisk inom vissa områden. Inom andra områden är ackreditering frivillig, men kan då fungera som en kvalitetsstämpel. Certifiering innebär att en organisation, produkt eller person bedöms uppfylla särskilda krav som ställs i standarder eller andra normerande dokument. Certifiering utförs beroende på område utan eller under ackreditering. Statistik från den internationella standardiseringsorganisationen ISO för 2012 visar att certifieringar mot standarder för ledningssystem fortsätter att öka. Certifiering enligt standarden för informationssäkerhet, ISO/IEC 27001, ökade med 13 procent till 19 577 certifikat utfärdade i 103 länder. (Japan 7 199, Storbritannien 1 701, Indien 1 600 och Sverige 32). Störst ökning av antal certifikat finns i Rumänien, Japan och Kina.

Certifieringsorgan som är ackrediterade av SWEDAC utför certifiering enligt följande standarder SS-ISO/IEC 27001 vad avser ledningssystem för informationssäkerhet och ISO/IEC 15408:2005 Information technology – Security techniques – Evaluation criteria for IT security, Common criteria 2.3 och Common criteria 3.1 vad avser produkter och processer. SWEDAC ackrediterar också certifieringsorgan för certifiering av Informationssäkerhetsspecialist, Nationell certifieringsordning för personcertifiering inom Inform-

ationssäkerhet 5.0, Information Security Management Professional (ISMP).

SWEDAC har utgett en vägledning för informationssäkerhetsarbete (SWEDAC DOC 10:5, 2010-09-22, utgåva 1). Syftet är att ge ackrediterade verksamheter och verksamheter som söker ackreditering vägledning vid förbättring av informationssäkerhet och om de krav som ställs vid bedömning av informationssäkerhet.

6.2.3 Svenska kraftnät

Det statliga Affärsverket svenska kraftnät (Svenska kraftnät) har enligt 1 § förordningen (2007:1119) med instruktion för Affärsverket svenska kraftnät till uppgift att på ett affärsmässigt sätt förvalta, driva och utveckla ett kostnadseffektivt, driftsäkert och miljöanpassat kraftöverföringssystem, sälja överföringskapacitet samt i övrigt bedriva verksamheter som är anknutna till kraftöverföringssystemet. Enligt 2 § är Svenska kraftnät systemansvarig myndighet enligt 8 kap. 1 § ellagen (1997:857) och 1 § förordningen (1994:1806) om systemansvaret för el samt elberedskapsmyndighet enligt elberedskapslagen (1997:288).

Enligt 3 § har Svenska kraftnät bl.a. i uppgift att svara för tillsyn i frågor om driftsäkerhet hos det nationella elsystemet enligt ellagen (1997:857) och förordningen (1994:1806) om systemansvaret för el, svara för beredskapsplaneringen inom sitt verksamhetsområde under kris- eller krigsförhållanden, främja dammsäkerheten i landet, bygga ut, installera och förvalta ledningar för elektronisk kommunikation, vartannat år genomföra och, efter att ha hört Statens energimyndighet, till Myndigheten för samhällsskydd och beredskap redovisa ett identifieringsarbete av potentiella europeiska kritiska infrastrukturer inom undersektorn el enligt 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.

Av 4 § följer att det i krig eller när regeringen annars bestämmer är Svenska kraftnäts uppgift att i samverkan med övriga totalförsvarsmyndigheter tillgodose samhällets behov av elkraft genom att planera, leda och samordna elförsörjningens resurser.

Vid Svenska kraftnät finns ett råd som har insyn i verksamheten med elberedskap (insynsråd). Rådet har till uppgift att bevaka det övriga totalförsvarets och elföretagens intressen i frågor om elberedskap. Vidare finns ett råd som biträder affärsverket i arbetet med dammsäkerhetsfrågor (Dammsäkerhetsrådet). Rådet är ett informations- och samrådsorgan för frågor relaterade till dammsäkerhet.

6.2.4 Totalförsvarets forskningsinstitut

Totalförsvarets forskningsinstitut (FOI) har enligt 1 § förordningen (2007:861) 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. Myndigheten ska verka för att försvarsforskningen nyttiggörs även utanför totalförsvaret.

Myndigheten ska särskilt verka för samverkan mellan militär och civil forskning samt mellan nationell och internationell forskning (3 §).

FOI bedriver vidare försvarsunderrättelseverksamhet (2 § förordningen [2000:131] om försvarsunderrättelseverksamhet).

Försvarsmakten och Försvarets materielverk är myndighetens huvudkunder, men myndigheten utför även uppdrag för bl.a. civila myndigheter och näringslivet.

Vid FOI bedrivs forskning om bl.a. it-säkerhet, sociala aspekter av informationssäkerhet, riskbedömning och metoder för övning av försvar av it-system och människa-system-interaktion, värdering av informationssäkerhet och utveckling av försvar av it-system. Vid FOI anordnas även kurser i it-säkerhet och säkerhet i industriella styrsystem. Myndigheten koordinerar t.ex. forskningsprogrammet Security Culture and Information Technology (SECURIT), som finansieras av MSB och har som mål att förbättra organisationers informationssäkerhet. FOI och MSB har tillsammans även byggt upp Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3).

6.2.5 Statens inspektion för försvarsunderrättelseverksamheten

Statens inspektion för försvarsunderrättelseverksamheten (Siun) är den myndighet som har till uppgift att kontrollera att den försvarsunderrättelseverksamhet som bedrivs av *Försvarsmakten*, *Försvarets radioanstalt*, *Försvarets materielverk* och *Totalförsvarets forskningsinstitut* sker i enlighet med det av riksdagen och regeringen fastställda regelverket (1 § förordningen [2009:969] med instruktion för Statens inspektion för försvarsunderrättelseverksamheten).

6.2.6 Socialstyrelsen

Socialstyrelsen är förvaltningsmyndighet för verksamhet som rör hälso- och sjukvård och annan medicinsk verksamhet, tandvård, smittskydd, socialtjänst, stöd och service till vissa funktionshindrade samt frågor om alkohol och missbruksmedel (1 § förordningen [2009:1243] med instruktion för Socialstyrelsen). Myndigheten ansvarar för föreskrifter och allmänna råd inom sitt verksamhetsområde (4 §).

Socialstyrelsen får efter samråd med Datainspektionen meddela föreskrifter som behövs för verkställigheten av patientdatalagen (2008:360) i fråga om säkerhetsåtgärder vid helt eller delvis automatiserad behandling av personuppgifter (3 § patientdataförordningen [2008:360]). Föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14) innehåller bl.a. bestämmelser om ansvar för informationssäkerhet och krav på informationssäkerhetspolicy. Myndigheten har utarbetat en handbok – ett stöd för vårdgivare, verksamhetschefer, medicinskt ansvariga sjuksköterskor och hälso- och sjukvårdspersonal som ska tillämpa nämnda föreskrifter.

Socialstyrelsen har också efter särskilt regeringsuppdrag i projektet Nationell Informationsstruktur i april 2010 publicerat delrapporten Informationssäkerhet, Vägledning för hantering av information inom vård och omsorg.

Myndigheten har ett nationellt ansvar för att samordna arbetet för en ändamålsenlig och strukturerad dokumentation i svensk hälso- och sjukvård och socialtjänst. Detta arbete är en del av Nationell eHälsa – strategin för tillgänglig och säker information inom vård och omsorg.

6.2.7 Länsstyrelserna

Länsstyrelsen svarar för den statliga förvaltningen i länet i den utsträckning inte någon annan myndighet har ansvaret för särskilda förvaltningsuppgifter (1 § förordningen [2007:825] med länsstyrelseinstruktion). Länsstyrelsen ska utifrån ett statligt helhetsperspektiv arbeta sektorövergripande och inom myndighetens ansvarsområde samordna olika samhällsintressen och statliga myndigheters insatser (2 §). Länsstyrelsen har bl.a. uppgifter i fråga om skydd mot olyckor, krisberedskap och civilt försvar (3 § 8). Genom sin verksamhet ska länsstyrelsen minska sårbarheten i samhället, bevaka att risk- och beredskapshänsyn tas i samhällsplaneringen samt utveckla en god förmåga att hantera sina uppgifter under fredstida krissituationer och höjd beredskap (52 §). Länsstyrelsen ska ha en tjänsteman i beredskap med uppgift att initiera och samordna det inledande arbetet för att upptäcka, verifiera, larma och informera vid allvarliga kriser som berör länet (53 §). Länsstyrelsen ska ha förmåga att vid en allvarlig kris, som berör länet eller medför behov av samverkan med kommuner eller andra aktörer, omgående kunna upprätta en ledningsfunktion för bl.a. samordning och information. Länsstyrelsen ska avseende krisberedskap vara sammanhållande inom sitt geografiska område och före, under och efter en kris verka för samordning och gemensam inriktning av de åtgärder som behöver vidtas (54 §). Länsstyrelsen ska särskilt

- ansvara för att en samlad regional lägesbild sammanställs vid krissituationer,
- stödja de aktörer som är ansvariga för krisberedskapen i länet avseende planering, risk- och sårbarhetsanalyser samt utbildning och övning,
- ha ett regionalt råd för skydd mot olyckor och krisberedskap, i vilket representanter för länsstyrelsen och berörda aktörer i krishanteringssystemet bör ingå, för att skapa nödvändig samordning,
- upprätta regionala risk- och sårbarhetsanalyser som ska kunna användas som underlag för egna och andra berörda aktörers krisberedskapsåtgärder,

- följa upp kommunernas tillämpning av lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,
- årligen rapportera till MSB vilka beredskapsförberedelser som kommuner och landsting vidtagit och samtidigt redovisa en bedömning av effekten av de vidtagna förberedelserna, och
- verka för att den verksamhet som berörda aktörer bedriver inom länet avseende krisberedskap bidrar till att en grundläggande förmåga till civilt försvar uppnås.

Länsstyrelsen ska enligt 7 § förordningen (2006:942) om krisberedskap och höjd beredskap inom sitt geografiska område i fråga om

- situationer som uppstår hastigt, oväntat och utan förvarning, eller en situation där det finns ett hot eller en risk att ett sådant läge kan uppstå, och
- situationer som kräver brådskande beslut och samverkan med andra aktörer

vara en sammanhållande funktion mellan lokala aktörer, som exempelvis kommuner, landsting och näringsliv, och den nationella nivån, samt verka för att:

- regionala risk-, och sårbarhetsanalyser sammanställs,
- nödvändig samverkan inom länet och med närliggande län kontinuerligt,
- under en kris samordna verksamhet mellan kommuner, landsting och myndigheter,
- information till allmänheten och företrädare för massmedia under sådana förhållanden samordnas, och efter beslut av regeringen prioritera och inrikta statliga och internationella resurser som ställs till förfogande.

Informationssäkerhet och är en av flera indikatorer enligt föreskrifter meddelade av MSB (MSBFS 2010:6) på krishanteringsförmåga. Informationssäkerhet och säkerhet och robusthet i samhällsviktig infrastruktur är två av flera indikatorer på förmåga i samhällsviktig verksamhet att motstå allvarliga störningar.

6.2.8 E-hälsomyndigheten

E-hälsomyndigheten har enligt 1 § förordningen (2013:1031) med instruktion för E-hälsomyndigheten) i uppgift att ansvara för register och it-funktioner som öppenvårdsapotek och vårdgivare behöver ha tillgång till för en patientsäker och kostnadseffektiv läkemedelshantering. Myndigheten ska vidare samordna regeringen satsningar på e-hälsa samt övergripande följa utvecklingen på e-hälsoområdet. E-hälsomyndigheten fortsätter det utvecklingsarbete som påbörjades av det statliga bolaget Apotekens Service. Arbetet vid myndigheten ska garantera en tillgänglig och säker nationell teknisk infrastruktur som kan fungera för hela hälso-, vård- och omsorgssektorn. E-hälsomyndigheten deltar i ett arbete med en federativ infrastrukturlösning för hela den aktuella sektorn, Samverkan för behörighet och identitet inom hälsa, vård och omsorg (Sambi).

6.2.9 Finansinspektionen

Finansinspektionen ansvarar bl.a. för tillsynen, regelgivningen och tillståndsprövningen som rör finansiella marknader och finansiella företag (1 § 1 förordningen [2009:93] med instruktion för Finansinspektionen). Myndigheten har särskilt ansvar för samverkansområdet ekonomisk säkerhet enligt förordningen (2006:942) om krisberedskap och höjd beredskap och ska samverka med Riksbanken och MSB i frågor som rör krisberedskap (6 §). Finansinspektionen har med stöd av 5 kap. 2 § 4 förordningen (2004:329) om bank- och finansieringsrörelse samt 6 kap. 1 § 9–12 och 29 förordningen (2007:572) om värdepappersmarknaden meddelat föreskrifter om informationssäkerhet, it-verksamhet och insättningssystem (FFFS 2014:5).

6.2.10 Kammarkollegiet

Kammarkollegiet har till uppgift att tillhandahålla service inom det statliga området, främst avseende ekonomi, juridik, kapitalförvaltning, riskhantering och administration (1 § förordningen [2007:824] med instruktion för Kammarkollegiet). Efter överens-

kommelse kan myndigheten för statliga myndigheter och stiftelser med statlig anknytning bl.a. tillhandahålla metoder för riskhantering och övrigt biträde i myndigheternas riskhantering (7 § första stycket 4). Myndigheten ska ansvara för att upphandla samordnade ramavtal som är avsedda för andra statliga myndigheter (8 a §). Inom området informationsteknik gäller ansvaret den offentliga förvaltningen. Myndigheten ska verka för att bästa möjliga villkor skapas för myndigheternas anskaffning av varor och tjänster. Inom området informationsteknik ska myndigheten särskilt beakta förvaltningsgemensamma standarder samt intresset av innovationer och teknikneutrala lösningar.

Vid Statens inköpscentral finns enheten för it-upphandling. Det finns ramavtal gällande E-förvaltningsstödjande tjänster, olika it-drifts- och konsulttjänster samt it-utbildning. Bland tjänsterna i ramavtal finns Säkerhetsarbete e-förvaltning. Bland ramavtal gällande programvaror och licenser finns t.ex. kontorsstöd som molntjänst.

Försäkringsavdelningen erbjuder försäkringsskydd för staten och lämnar biträde åt statliga myndigheter i riskhanteringsfrågor. Det erbjuds stöd och utbildning för att underlätta myndigheternas riskhanteringsarbete. Metodstöd utformas utifrån ett verksamhetsperspektiv och anpassas till varje myndighets behov. Avdelningen har tagit fram mallar för olika typer av checklistor. I checklistorna finns frågor om bl.a. informationshantering och informationssäkerhet.

6.2.11 Försvarshögskolan

Vid Försvarshögskolan (FHS) bedrivs utbildning och forskning som rör informationssäkerhet vid flera enheter. I förordningen (2007:1164) för Försvarshögskolan anges vilken högskoleutbildning som bedrivs. Högskolan får även på uppdrag av MSB eller annan uppdragsgivare anordna annan utbildning. Bland uppdragsutbildningar finns utbildningar som rör informationssäkerhet.

Vid Institutionen för säkerhet, strategi och ledarskap (ISSL) finns CATS – Centrum för assymmetriska hot och terrorismstudier. Vid centret bedrivs bl.a. utbildning och forskning/studier kring policys rörande informations- och cybersäkerhet samt inom området informationsoperationer.

Vidare har centret under flera år bedrivit utveckling samt deltagit i tekniska cyberförsvarsövningar, s.k. Cyber Defence Exercises (CDX). Centret har bedrivit studier i övningsmetodik för CDX. Detta har bl.a. resulterat i produktion av den första övningshandboken inom området, vilken även har översatts till engelska för att kunna möta efterfrågan från internationella samarbetspartners.

CATS har sedan 2008 haft ett samarbete med Estland och Natos Cooperative Cyber Defence Centre of Excellence (CCD CoE) i Tallinn. Tidigare avtalssamarbete med två technical agreements (TA) har reglerat verksamhet avseende deltagande i och utveckling av den årligen återkommande övningen Locked Shields (tidigare Baltic Cyber Shield) samt utveckling av Chief Information Assurance Officer-utbilningen (CIAO).

CATS genomför CIAO-utbildning som utvecklats i samverkan med MSB, PTS och FRA. Syftet med kursen är att öka förmågan på informationssäkerhetsområdet inom myndigheter, organisationer och privata aktörer knutna till samhällsviktiga system och funktioner. Syftet med utbildningen är att möta samhällsviktiga företags och myndigheters behov av en funktion som kan hantera de möjligheter och risker som följer av att informationsflödet ökar i omfattning och komplexitet, som exempelvis frågan om hur de operativa kraven kan balanseras mot de alltmer omfattande säkerhetskraven.

Kursen riktar sig till dem som ska leda informationshanteringen inom en central, regional eller lokal myndighet eller inom näringslivet, men även till chefspersoner inom organisationen. Kursen innehåller utbildning avseende internationella aktörer och regelverk, nationella krisledningssystemet, ledning och riskhantering, planering och arkitektur, efterlevnad av regelverk och övning.

I ISSL ingår även IHT – Institutet för högre totalförsvarsutbildning. Utbildning ges här i att hantera många av de svåraste kriserna som kan drabba ett samhälle. Rekryteringen till kurserna på IHT sker bland högre militära chefer och tjänstemän inom offentlig förvaltning, organisationer, media och näringsliv. Utveckling av utbildning avseende cyber- och informationssäkerhet i IHT kursutbud pågår inom FHS.

Vid Militärvetenskapliga institutionen (MVI) finns MTA – Militärtekniska avdelningen. Avdelningen ansvarar för utbildning i militärteknik vid främst de militära programmen, men anordnar

även en grundläggande och orienterande kurs för chefer om informationssäkerhet. Vidare finns vid MTA ett Computer Network Operations-lab (CNO-lab), som drivs i samarbete med CATS för ändamålet att kunna genomföra och leda övningsverksamhet/utbildningar. CDX Baltic Cyber Shield 2010 leddes delvis från CNO-labbet.

Vidare finns vid MVI även Krigsvetenskapliga avdelningen – KVA, som bedriver utbildning och forskning inom områdena Informationsoperationer och informationskrigföring på operativ nivå.

6.2.12 E-legitimationsnämnden

E-legitimationsnämnden har som övergripande uppgift enligt 1 § förordningen (2010:1497) med instruktion för E-legitimationsnämnden i uppgift att stödja och samordna elektronisk identifiering och signering i den offentliga förvaltningens e-tjänster. Den samordnande funktionen på området för e-legitimationer innebär t.ex. att hålla register över utfärdare av e-legitimationer, ställa upp standardiserade krav på e-legitimationers tekniska utformning och säkerhet samt när nya utfärdare önskar delat i infrastrukturen pröva och godkänna dessa.

Myndigheten har också fattat ett inriktningsbeslut att stödja även privat sektors användning av e-legitimationer bl.a. genom att möjliggöra för registerhållning och upprättande av regler och avtal för privata aktörer.

Myndigheten har även i uppgift att delta i internationellt standardiseringsarbete, internationellt samarbete och informationsutbyte inom sitt ansvarsområde (2 §).

6.2.13 E-delegationen

E-delegationen, en kommitté under Näringsdepartementet, inrättades 2009 för att stärka utvecklingen av e-förvaltningen och skapa goda möjligheter för myndighetsövergripande samordning (dir. 2009:19). Genom tilläggsdirektiv (dir. 2010:32) fick delegationen 2010 i uppdrag att främja och samordna myndigheternas arbete med att förbättra förutsättningarna för vidareutnyttjande av hand-

lingar från den offentliga förvaltningen samt ta fram riktlinjer för statliga myndigheter användning av sociala medier. Genom tilläggsdirektiv (dir. 2013:40) fick delegationen 2013 i uppdrag att också undersöka behovet av en nationell standard för it-system inom vård och omsorg.

Delegationen lämnade i *Tredje generationens e-förvaltning* (SOU 2009:86) förslag till en strategi för myndigheternas arbete med e-förvaltning. I *Organisering av framtidens e-förvaltning* (SOU 2013:75) föreslås att samordningen av de gemensamma e-förvaltningsfrågorna tas om hand av en medlemsorganisation med en uppbyggnad liknande Arbetsgivarverkets. För att stärka samverkan med den statliga och kommunala sektorn föreslås vidare att den nya organisationen upprättar ett särskilt samarbetsorgan med den kommunala sektorn. Det föreslås att en särskild utredare utreder de närmare förutsättningarna för en sådan organisation och förvaltning. I *Så enkelt som möjligt för så många som möjligt – IT-standardisering inom socialtjänsten* (SOU 2013:77) beskrivs resultatet av behovsinventeringen inom socialtjänsten i en konsultrapport med förslag om införande av en nationell tjänsteplattform. E-delegationen bedömer att inga specifika förslag om vilka standardiseringar som är lämpliga kan lämnas på området. Vidare görs bedömningen att ett fördjupat analysarbete bör genomföras, dels för att värdera de initiativ som föreslås i rapporten, dels för att tydligare belysa informationssäkerheten på området. Utgångspunkten för arbetet ska vara det arbete som skett inom delegationen vad avser digital samverkan och framför allt den vägledning för digital samverkan som utarbetats. Analysarbetet kräver djupare och specifik kompetens inom socialtjänsten område och bör därför genomföras av de organisationer som finns etablerade inom e-hälsoområdet. För övriga delrapporter, se www.edelegationen.se. Delegationen ska lämna en slutrapport senast den 1 juli 2015.

På webbplatsen anges följande om vad E-delegationen gör vad avser informationssäkerhet.

> Informationssäkerhet behöver förbättras i projekt där flera aktörer samverkar. Bland annat krävs en gemensam säkerhetskultur, metoder och regler. När it-lösningar koncentreras och integreras uppstår också nya risker. E-delegationen arbetar för att utveckla den gemensamma informationssäkerheten. Arbetet ska på sikt leda till en gemensam säkerhetsinfrastruktur och en större effektivitet i samverkansprojekt.

Vidare pågår ett arbete med att ta fram en handlingsplan för att förverkliga de mål som finns i Strategi för informationssäkerhet i e-förvaltning och metodstöd för de projekt som drivs inom delegationen.

6.2.14 Riksarkivet

Riksarkivet har enligt sin instruktion (3 § förordningen (2007:1179) med instruktion för Riksarkivet och landsarkiven) överinseende över den offentliga arkivverksamheten. Myndigheten ska verka för att de statliga myndigheterna fullgör sina skyldigheter enligt arkivlagen att bevara, hålla ordnade och vårda sina arkiv så att arkiven tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipning och förvaltning samt forskningens behov. Riksarkivet ska också verka för en utveckling av arkivverksamheten och en ändamålsenlig gallring av handlingar, ge kommunerna råd i arkivfrågor samt verka för ökad enhetlighet mellan den statliga och den kommunala arkivhanteringen.

Inom ramen för Riksarkivets allmänna regelverk för myndigheterna har föreskrifter om bl.a. informationssäkerhet, upphandling och tekniska krav meddelats beträffande elektroniska handlingar (RA-FS 2009:1 och 2009:2).

Myndigheten har i samverkan med Myndigheten för samhällsskydd och beredskap utarbetat en vägledning för fysisk informationssäkerhet i it-utrymmen. Vidare har förvaltningsgemensamma specifikationer tagits fram inom projektet E-arkiv och e-diarium (eARD) som är knutet till E-delegationen.

7 Samhällets informationssäkerhet

7.1 Politiska mål för Sveriges säkerhet och samhällets krisberedskap

Målen för Sveriges säkerhet är att värna befolkningens liv och hälsa, värna samhällets funktionalitet och värna förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter (prop. 2008/09:140, bet. 2008/09:FöU10, rskr. 2008/09:292). Den svenska säkerhetspolitiken utgår ifrån en bred syn på begreppet säkerhet som inrymmer såväl hot och risker som allvarliga händelser, kriser och militära hot (prop. 2012/13:1 utgiftsområde 6 s. 72).

Med utgångspunkt i dessa övergripande mål för Sveriges säkerhet är målen för samhällets krisberedskap att minska risken för och konsekvenserna av allvarliga störningar, kriser och olyckor. Skulle en sådan händelse inträffa bör alla människors personliga säkerhet och hälsa tryggas samt skador på egendom eller i miljö Vad gäller politikens inriktning uttalas i budgetpropositionen (prop. 2013/14:1 utgiftsområde 6 s. 96) följande om informationssäkerhet.

> I dag är i stort sett all verksamhet beroende av fungerande informationssäkerhet. En större it-incident kan få omfattande samhällskonsekvenser både för den drabbade verksamheten men också för andra verksamheter dels genom ett beroendeförhållande till den verksamhet som påverkats, dels genom spridningsrisk av orsak till incidenten. Flera verksamheter kan därmed påverkas och regeringen vill därför åter betona vikten av informationssäkerhetsarbetet med risk-, sårbarhets- och säkerhetsanalyser. Detta bör dock inte stanna vid att analyser är genomförda utan ansvariga aktörer bör utifrån dessa upprätta handlingsplaner och genomföra åtgärder så att risken för it-incidenter etc. minimeras.

I regeringens skrivelse (skr. 2009/10:124) *Samhällets krisberedskap – stärkt samverkan för ökad säkerhet* har målen för samhällets informationssäkerhet angetts enligt följande:

- Säkra samhällets funktionalitet, effektivitet och kvalitet.
- Bidra till samhällets brottsbekämpning.
- Stärka samhällets förmåga att förebygga och hantera allvarliga störningar och kriser.
- Främja näringslivets tillväxt.
- Värna medborgares fri- och rättigheter och personliga integritet.
- Öka medborgares och verksamheters kunskap om och förtroende för informationshantering och it-system.

Myndigheten för samhällsskydd och beredskap (MSB) har haft i uppdrag att tillsammans med övriga myndigheter som ingår i SAMFI att ta fram en strategi för samhällets informationssäkerhet 2010–2015 utifrån dessa mål, se avsnitt 7.3.2.

I Försvarsberedningens senaste rapport, *Försvaret av Sverige Starkare försvar för en osäker tid (*Ds 2014:20), tar beredningen upp cybersäkerhet i ett eget kapitel. Där konstaterar beredningen, liksom i tidigare rapporter, att människor och stater är alltmer beroende av digitala informations- och kommunikationssystem. Detta har medfört nya former av interaktion, datahantering och datalagring, men även nya sårbarheter. Som utredningen beskrivit i avsnitt 4.4 finns det stora säkerhetsutmaningar i det växande it-användandet och it-beroendet. Utredningen återkommer här till Försvarsberedningens bedömning (sid. 31):

> Hot- och riskskalan inom det informationsteknologiska området spänner från mindre omfattande risker för den enskilde medborgaren, till väl planerade och med precision riktade s.k. cyberattacker mot vitala delar i samhällets funktionalitet. Konsekvenserna innefattar spridningseffekter som drabbar samhällsviktig verksamhet i flera sektorer. Sammankopplingen mellan olika typer av industriella informations-och styrsystem utgör en växande sårbarhet. Störningar eller antagonistiska hot där dessa system tas över av tredje part kan hota samhällsviktiga funktioner och ytterst ett lands suveränitet. Data-och nätverksoperationer har utvecklats till att utgöra ett separat antagonistiskt hot såväl som ett av flera militära maktmedel. Riktade angrepp såväl inom som mot cyberområdet kan utföras av både statliga och icke-statliga aktörer.

Försvarsberedningen konstaterar vidare att Sveriges samlade förmåga att förebygga, motverka och aktivt hantera konsekvenserna av civila och militära hot, händelser och attacker på cyberområdet måste öka. För att möjliggöra ett koordinerat beslutsfattande framhåller Försvarsberedningen betydelsen av att det mellan civila myndigheter och Försvarsmakten finns en delad lägesinformation vid händelser. Försvarsberedningen betonar fortsatt behovet av att se på möjligheten att fortsatt stärka it-robustheten i samhället och analysera behovet av att utveckla cyberförmågor.

7.2 Arbete i Regeringskansliet

Regeringskansliet är den myndighet under regeringen som förbereder regeringens ärenden och i övrigt är regeringen behjälplig. I Regeringskansliet ingår Statsrådsberedningen, Förvaltningsavdelningen och tio departement. Statsministern är chef för Regeringskansliet. Förvaltningsärenden och lagstiftningsärenden fördelas mellan departementen på det sätt som anges i bilagan till förordningen (1996:1515) med instruktion för Regeringskansliet.

Av Riksrevisionens granskningsrapport *Informationssäkerheten i den civila statsförvaltningen* RIR 2014:23 s. 72 f. framgår hur Regeringskansliet är organiserat för att hantera informationssäkerhet:

> I Regeringskansliet har varje fackdepartement på regeringens vägnar ansvar för att följa upp sina respektive myndigheters informationssäkerhetsarbete. I praktiken innebär det att varje myndighetshandläggare hanterar frågor som handlar om myndighetens informationssäkerhet. Detta förutsätter dock att myndighetshandläggaren får signaler om att det finns behov av att uppmärksamma informationssäkerhetsarbetet. Sådana signaler kan vara it-incidenter vid myndigheten, uppmärksamhet i massmedier eller att frågan om informationssäkerhet väcks inom Regeringskansliet.
>
> Hur frågor som berör informationssäkerhet fördelas mellan departementen avgörs tydligast av den ansvarsfördelning som är fastställd i en bilaga till Regeringskanslets instruktion. Beroende på vad informationssäkerhetsfrågan handlar om styrs den till det departement som huvudsakligen berörs. Ett ärende som rör flera departements verksamhetsområden ska handläggas inom det departement till vilket det huvudsakligen tillhör och beredas i samråd med övriga berörda statsråd (gemensam beredning).

7.2.1 Departementens beskrivningar

I arbetet med att få en bild av samhällets informationssäkerhet har utredningen kontaktat Justitiedepartementet, Utrikesdepartementet, Försvarsdepartementet och Näringsdepartementet för att få underlag som beskriver respektive departements arbete med informations- och cybersäkerhetsrelaterade frågor. Underlaget presenteras nedan.

Justitiedepartementet

Justitiedepartementet har en viktig roll i att säkerställa statens ansvar att skydda sina medborgare från att bli utsatta för brott och säkerställa att alla kan åtnjuta sina mänskliga rättigheter fullt ut även i en tid då allt mer av mänsklig interaktion sker genom internet. Justitiedepartementet har ansvar för frågor om allmän ordning, säkerhet och krisberedskap, inklusive ansvaret för Regeringskansliets egen krisberedskap. Departementet har också ansvar för bevakning och hantering av it-relaterad brottslighet, vissa informationssäkerhetsfrågor, inklusive säkerhetsskydd, skydd för personuppgifter samt it-frågor i bredare bemärkelse kopplat till allmän ordning och säkerhet. Beröringspunkterna utgår från horisontella frågor såsom grundläggande fri- och rättigheter, krisberedskap och mer specifika frågor om dataskydd, brottsbekämpning och skydd för rikets säkerhet.

Justitiedepartementet hanterar även frågor kopplade till it, informationssäkerhet och brottslighet genom myndighetstyrning och lagstiftningsarbete. Detta görs för att skapa förutsättningar för myndigheter som lyder under departementet såsom Polismyndigheten, Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap och åklagarväsendet, att utföra sina uppdrag på detta område.

Vid departementet ansvarar polisenheten (PO) för förvaltnings- och utvecklingsfrågor som gäller polisen, inklusive Säkerhetspolisen och därmed för förutsättningar för dessa myndigheter att utreda och beivra it-relaterad brottslighet och förebygga och avslöja brott mot rikets säkerhet. Enheten för samordning av samhällets krisberedskap (SSK) ansvarar för samordning avseende åtgärder m.m. för att utveckla, följa upp och förstärka samhällets krisbered-

skap och civilt försvar, vilket inkluderar samhällets informationssäkerhet. Enheten har beredningsansvar för styrning av bl.a. Myndigheten för samhällsskydd och beredskap. På lagstiftningssidan ansvarar åklagarenheten (Å) för lagstiftningsfrågor som rör allmänt åtal, förundersökning och tvångsmedel i brottmål, vilket innefattar många av de utredningsverktyg som polis och åklagare har till förfogande för utredning av it-relaterad brottslighet. Enheten för brottmålsärenden och internationellt rättsligt samarbete (BIRS) ansvarar för lagstiftningsfrågor som rör bl.a. internationell rättslig hjälp vilket är särskilt viktigt i gränsöverskridande it-relaterade brottsutredningar. Centralmyndigheten, som är en kontaktpunkt för många in- och utgående ärenden i det internationella straffrättsliga samarbetet, är vidare placerad på enheten. Enheten för allmän ordning och säkerhet (L4) har lagstiftningsfrågor som gäller bl.a. polisverksamhet och polisregister, internationellt polissamarbete och säkerhetsskyddslagen. Straffrättsenheten (L5) ansvarar för lagstiftningsfrågor som rör straffrätt, såsom dataintrång och annan it-relaterad brottslighet. Slutligen ansvarar grundlagsenheten (L6) för lagstiftningsfrågor som bl.a. gäller skydd för den personliga integriteten, skydd för personuppgifter och tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

En stor del av de säkerhetsrelaterade aspekterna på it-området handlar om att förebygga och skydda sig mot olika former av it-incidenter. Hot utgörs av allt ifrån tekniska fel till den mänskliga faktorn och olika typer av uppsåtliga it-attacker av antagonistiska statliga eller icke-statliga aktörer. Utöver detta är det inte ovanligt att t.ex. väderfenomen, naturkatastrofer och olyckor orsakar incidenter med it-inslag. Sådana incidenter tar inte sällan formen av olika typer av uppsåtliga it-attacker av antagonistiska statliga eller icke-statliga aktörer och utgör således även brottslig verksamhet. Av den anledningen berörs även Justitiedepartementet av många frågor för vilket huvudansvaret ligger på andra departement vid Regeringskansliet. Justitiedepartementet har ett ansvar för informationssäkerhetsfrågor enligt instruktionen för Regeringskansliet. Det är dock även andra departement som arbetar med informationssäkerhetsfrågor utifrån olika aspekter. Detta reflekteras även i hur samverkan sker mellan en mängd olika myndigheter med ansvar på området som har olika departement som huvudmän. Ett exempel på detta är samarbetet som finns mellan Säkerhetspoli-

sen, Militära underrättelse- och säkerhetstjänsten (MUST) och Försvarets radioanstalt (FRA) för kvalificerade it-brott och mer omfattande angrepp på it-system. Detta samarbete, som kallas Nationell samverkan mot kvalificerade it-brott (NSIT), syftar till att bättre utnyttja de expertresurser som de olika myndigheterna besitter.

Utöver dessa nationella frågor finns det frågor kopplade till it-brottslighet och informationssäkerhet med en tydlig gränsöverskridande dimension. Därför bevakar departementets enheter de internationella frågor som är kopplade till dess ansvarsområden. Här pågår viktigt arbete inom bl.a. EU (bl.a. den lagstiftande verksamheten och samarbetet med it-brottscentret EC3 vid Europol, samt förhandlingar av NIS-direktivet), FN:s organ för narkotika och brottslighet UNODC och Europarådet (i synnerhet kopplat till konventionen om it-relaterad brottslighet – ETS 185). Främjandet av bilateralt samarbete med tredje länder är också en viktig del i detta.

Utrikesdepartementet

Utrikesdepartementet (UD) ansvarar för Sveriges förbindelser med andra länder och de handlingsalternativ som ligger till grund för regeringens ställningstaganden i utrikespolitiska frågor. Globala frågor som rör internationella informations- och kommunikationsteknologier (ICT) har snabbt blivit ett växande och angeläget utrikespolitiskt frågekomplex som spänner över hela bredden av internationella relationer – bl.a. säkerhet, folkrätt, handel, utveckling och inte minst demokrati och mänskliga rättigheter – och behandlas i en mängd multilaterala, regionala och bilaterala fora.

Internationella cyberfrågor utgör i allt högre grad en integrerad del av UD:s verksamhet. Det övergripande ansvaret för cyberområdet inom UD främst ligger hos UD-FMR och UD-SP som har ett mycket nära samarbete. Därutöver berörs en rad andra enheter också av cyber- och internetrelaterade frågor, inklusive UD-IH vad gäller handelsaspekter och allmänt för de olika geografiska enheterna.

UD har nära samarbeten med övriga Regeringskansliet, bl.a. Näringsdepartementet vad gäller internets styrning, Justitiedepar-

tementet vad gäller arbetet med informations- och cybersäkerhet och cyberbrottsfrågor och Försvarsdepartementet vad gäller cyberförsvarsfrågor. UD ansvarar även för Sveriges säkerhetspolitiska doktrinutveckling där cybersäkerhet förväntas spela en tilltagande roll i framtiden

UD ansvarar för en omfattande mängd svenska ställningstaganden och hanterande av internationella cyberfrågor ur en rad olika aspekter, exempelvis internationell normbildning, deltagande i en stor mängd konferenser och möten, internationella förtroendebyggande åtgärder, resolutionsarbete, kapacitetsbyggande åtgärder och samarbeten och övningar liksom EU:s externa samarbeten och politiska dialoger. Cyberfrågor behandlas numera i en rad multilaterala och regionala organisationer för vilka UD har huvud- eller medansvar för, bl.a. FN, EU, Nato, Europarådet och OSSE.

Cyberfrågorna med sådant perspektiv utgör därmed en del av Sveriges samlade utrikes- och säkerhetspolitik. De grundförutsättningar som är allmänt vägledande för Sveriges utrikes- och säkerhetspolitik återspeglas även i arbetet med cyberfrågorna.

Försvarsdepartementet

Försvarsdepartementet ansvarar bl.a. för Sveriges militära försvar och dess stödmyndigheter samt samordning mellan det militära försvaret och det civila försvaret inom ramen för totalförsvar. Departementet planerar på strategisk nivå insatser och säkerhetsfrämjande verksamhet i och utanför vårt närområde och ger uppdrag till myndigheterna att genomföra samt följa upp dessa insatser.

Försvarsdepartementet handlägger bl.a. förvaltningsärenden som gäller det militära försvaret, bi- och multilateralt försvars- och materielsamarbete och försvarsunderrättelseverksamhet. I dessa ingår bl.a. it-försvars-, signalskydds- och vissa informationssäkerhetsrelaterade frågor.

Försvarsdepartementets organisation framgår av Regeringskansliets föreskrifter med arbetsordning för Försvarsdepartementet (RKF 2014:11) och består av ett antal sekretariat och enheter.

Sekretariatet för säkerhetspolitik, internationella relationer och analys (SI) svarar för frågor om säkerhetspolitik och internationell samordning.

Enheten för samordning av försvarsunderrättelsefrågor (SUND) har till uppgift att löpande följa, inrikta och utveckla försvarsunderrättelseverksamheten. Enheten har beredningsansvar för styrning av bl.a. Försvarets radioanstalt (FRA), och Försvarsmakten, såvitt avser myndighetens enhet för underrättelse- och säkerhetstjänst (MUST).

Enheten för materiel, forskning och utveckling (MFU) svarar för materielförsörjning, forskning och utveckling samt annan stödverksamhet avseende departementets myndigheter. Enheten har beredningsansvar för styrning av bl.a. Försvarets materielverk (FMV) och Totalförsvarets forskningsinstitut (FOI).

Enheten för militär förmåga och insatser (MFI) svarar för frågor om det militära försvaret. Enheten har beredningsansvar för styrning av Försvarsmakten med undantag för de delar av myndigheten som SUND ansvarar för.

Vissa av Försvarsdepartementets myndigheter löser uppgifter inom informationssäkerhetsområdet, som en del av sina huvuduppgifter.

Inom Försvarsmakten finns den Militära underrättelse- och säkerhetstjänsten (MUST). MUST:s säkerhetskontor ansvarar för kravställning, granskning, godkännande och vidmakthållande av signalskyddsystem för totalförsvaret samt kravställning och godkännande av säkerhetsfunktioner för IT-system i Försvarsmakten. Signalskyddstjänsten syftar till att förhindra obehörig insyn och påverkan av telekommunikations- och it-system. MUST:s underrättelse- och säkerhetsunderrättelseverksamhet bidrar även till att kartlägga yttre it-hot mot Sverige och svenska intressen.

Inom Försvarsmakten finns även ett antal ledningsförband som har till uppgift att skydda Försvarsmaktens it-system mot angrepp. Inom it-försvarsförbandet (ITF) finns funktionen FM CERT (Computer Emergency Response Team) som hanterar IT-säkerhetsincidenter i Försvarsmakten samt analyserar och föreslår förbättringar i myndighetens verksamhet utifrån ett informationssäkerhetsperspektiv.

FRA har uppgiften att upprätthålla hög kompetens inom teknisk informationssäkerhet och stödjer andra myndigheter och statliga företag med informationssäkerhetsanalyser. FRA biträder även Försvarsmaktens signalskyddsverksamhet med expertkompetens inom kryptografi. Inom myndighetens försvarsunderrättelseverksamhet bedrivs signalspaning för att bl.a. kartlägga allvarliga yttre

hot mot samhällets infrastrukturer. Det omfattar t.ex. att upptäcka it-angrepp från utlandet mot känsliga informationssystem i Sverige.

Hos FMV finns Sveriges certifieringsorgan för it-säkerhet (CSEC). CSEC är en oberoende enhet inom FMV, och verkar som Sveriges nationella evaluerings- och certifieringsorgan för it-säkerhet i produkter och system enligt standarden Common Criteria. CSEC licensierar företag som utför granskningar enligt dessa regler. Produkter som certifierats av CSEC används av bl.a. Försvarsmakten.

FOI bedriver forskning, metod- och teknikutveckling för totalförsvaret, bl.a. inom informationssäkerhetsområdet, t.ex. utveckling av försvar av it-system. Till sin hjälp har man bl.a. avancerade simuleringssystem.

Näringsdepartementet

Inom Näringsdepartementet finns sedan 2015 två enheter som arbetar med digitaliseringen, it-politiska enheten (ITP) och enheten för elektronisk förvaltning (EF). Verksamheten vid enheterna styrs av de mål som beslutats av regering och riksdag samt av de övergripande målen för Näringsdepartementet och it-politiken.

Arbetet vid ITP-enheten handlar om egna sektorsområden (t.ex. myndighetsstyrning av PTS, reglering av elektronisk kommunikation etc.), men också om horisontella frågor och samordning (t.ex. den digitala agendan). Då infrastrukturen och aktörer som utbjuder elektroniska tjänster arbetar på en konkurrensutsatt marknad påverkar det statens möjligheter till påverkan och styrning. Staten och det offentliga (inklusive kommuner och landsting) är å andra sidan en stor it-användare och har i dessa avseenden stora möjligheter att som kund kunna påverka utvecklingen (t.ex. e-förvaltning). Systemet med gemensam beredning innebär att enheterna också blir berörd av it-aspekter inom många politikområden. ITP-enheten ansvarar för övergripande frågor, reglering, främjande och utveckling inom områdena it och elektronisk kommunikation samt post- och betaltjänster. Enheten arbetar bl.a. med bredbandsmarknaden, nätsäkerhet, radiospektrumfrågor och internets förvaltning. Ansvarsområdet omfattar även styrning och uppföljning av Post- och telestyrelsen, samt Digitaliseringskommissionen. De åtgärder som vidtas syftar till att

skapa goda förutsättningar för väl fungerande marknader och effektiv konkurrens. Hushåll och företag ska ha tillgång till effektiv, robust och säker infrastruktur och bästa möjliga utbud av kommunikationstjänster. Därutöver ska alla i samhället ha tillgång till grundläggande betaltjänster till rimliga priser. Politiken omfattar även åtgärder som syftar till att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter och åtgärder som syftar till att Sverige ska ha bredband i världsklass. Hushåll och företag ska ha goda möjligheter att använda sig av elektroniska samhällstjänster och service via bredband.

EF-enheten ansvarar för övergripande it-frågor i statsförvaltningen. Målet är en enklare vardag för medborgare, en öppnare förvaltning som stödjer innovation och delaktighet och en högre kvalitet och effektivitet i verksamheten. Verksamheten omfattar flera delområden. Strategisk styrning och samordning av det myndighetsövergripande arbetet med att digitalisera den offentliga verksamheten inklusive strategiska it-investeringar i statsförvaltningen. Utveckling, införande och förvaltning av förvaltningsgemensamma digitala lösningar. Samordning av myndighetsövergripande digitala lösningar mellan olika verksamhetsområden. Mjuka infrastrukturella förutsättningar för digitalisering: it-arkitektur, standarder och myndighetsövergripande informationssäkerhet. Uppföljning av myndigheternas it-verksamhet. Myndighetgemensamma arbetssätt: vägledningar, ramverk och kompetensutveckling. Juridiska förutsättningar för digital samverkan. Styrning och utveckling av e-legitimationsnämnden, E-delegationen och organisatoriska förutsättningar för det offentliga Sveriges digitalisering. Nämndens uppgift är att stödja och samordna offentliga sektorns behov av säkra metoder för elektronisk identifiering och signering. Delegationen har bl.a. i uppdrag att driva på e-utvecklingen inom offentlig sektor, att arbeta med e-förvaltning, sociala medier och vidareutnyttjande av offentlig information (PSI-direktivet).

ITP-enheten och EF-enheten är involverade i ett stort antal olika internationella samarbeten och EU-samarbeten, till exempel Europeiska Unionens råd (telerådet) och rådsarbetsgrupp H5 telekom/ informationssamhällets tjänster, högnivågrupper för Digital agenda för Europa, Enisa (Europeiska byrån för nät- och informationssäkerhet), Nordiska ministerrådets it-forum, Communications Committee (COCOM) och Radio Spectrum Committee (RSC).

Utöver det så deltar ITP-enheten också i olika internationella samarbeten rörande internets förvaltning till exempel International Corporation for Assigned Names and Numbers (ICANN), International Telecommunications Union (ITU), Universal Postal Union (UPU) och flera olika OECD grupper inom it-området. EF-enheten deltar även i genomförandearbetet avseende EU:s eIDAS-förordning (om EU-gränsöverskridande e-signaturer, e-ID) och i projekten e-Sense/Stork 2.0 om e-ID. Samtliga dessa organ hanterar från tid till annan nät- eller informationssäkerhetsrelaterade frågor.

7.3 Uppdrag från regeringen

7.3.1 Utredningsdirektiv

Regeringen beslutade den 8 december 2011 att tillkalla en särskild utredare med uppdrag att göra en översyn av säkerhetsskyddslagstiftningen *En modern säkerhetsskyddslag* (dir. 2013:110). Utredningens syfte 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.

Utredningens uppdrag har varit 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.

Utredningen beräknas avsluta sitt arbete under mars månad 2015.

7.3.2 Regeringsuppdrag till myndigheter

Under de senaste åren har flera åtgärder initierats för att Sverige ska bli bättre på att utnyttja informationsteknologi i syfte att öka effektiviteten och den konkreta nyttan för medborgare, företag och för regeringens och myndigheternas eget arbete.

Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter

2009 fick Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag lämna förslag på åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera it-incidenter. MSB redovisade uppdraget 2010 och förslaget gick i huvudsak ut på att skapa ett nationellt operativt samverkanscenter lokaliserat på MSB. Ytterligare förslag var exempelvis att utreda obligatorisk it-incidenthantering och tekniskt intrångsdetekterings- och varningssystem, att informationssäkerhet beaktas i risk- och sårbarhetsanalyser samt att ta fram en nationell plan för att hantera allvarliga it-incidenter.

Nationell hanterandeplan för allvarliga it-incidenter

Regeringen beslutade den 14 april 2010 om ett antal uppdrag till MSB på informationssäkerhetsområdet (Fö2010/702/SSK). Uppdragen syftar till att stärka samhällets informationssäkerhet och förmåga att förebygga och hantera it-incidenter. MSB fick då i uppdrag att ta fram en nationell plan som klargör hur allvarliga it-incidenter ska hanteras. MSB redovisade uppdraget 2011 och har tagit fram en nationell plan för att hantera allvarliga it-relaterade kriser *Nationell hanterandeplan för allvarliga IT-incidenter*. Planen

syftar till att underlätta för varje aktör genom att tillsammans med andra aktörer ta fram en gemensam lägesbild.

System för obligatorisk it-incidentrapportering för statliga myndigheter

År 2010 fick MSB även i uppdrag att utreda hur ett system för obligatorisk it-incidentrapportering för statliga myndigheter kan utformas. MSB redovisade 2011 ett förslag där systemet för incidentrapportering föreslogs införas stegvis och föregås av en pilotversion i mindre skala. MSB fick 2012 ett tillkommande uppdrag gällande incidentrapportering vilket redovisades senare samma år *Nationellt system för it-incidentrapportering*. Se vidare i avsnitt 7.5.3.

Utformning av ett sensorsystem benämnt tekniskt detekterings- och varningssystem (TDV)

I april 2010 gav regeringen MSB och Försvarets radioanstalt (FRA) två uppdrag rörande ett tekniskt detekterings- och varningssystem (TDV) för samhällsviktig verksamhet och kritisk infrastruktur. FRA fick i uppdrag att lämna förslag på hur ett sådant system kan utformas. MSB fick i sin tur i uppdrag att lämna förslag på vilka aktörer som ska omfattas av ett sådant system. 2011 redovisade MSB sina förslag, och rekommenderade att alla statliga myndigheter som är särskilt utpekade i bilagan till krisberedskapsförordningen skulle erbjudas att delta i systemet. FRA fick 2011 ett kompletterande uppdrag att komma in med en mer detaljerad redovisning samt att utarbeta en pilotversion av systemet. År 2012 redovisade FRA sitt kompletterande uppdrag och pilotprojektet, vilket innebär att TDV i dagsläget finns i drift hos ett fåtal användare.

Tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor

År 2010 fick MSB i uppdrag av regeringen att lämna förslag på en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting. 2011 lämnade MSB sitt förslag på hur en tillgänglig och skyddad kommunikationsinfrastruktur för offentlig sektor skulle kunna skapas. Förslaget går i huvudsak ut på att skapa en sammanhållande organisatorisk struktur med uppdrag att samordna, inrikta, ansvara för drift och förvalta. Vissa delar av infrastrukturen ska enligt förslaget tillhandahållas genom staten och andra genom näringslivet. Se vidare avsnitt 7.5.4.

Strategi och handlingsplan för samhällets informationssäkerhet

Regeringen gav MSB i uppdrag att tillsammans med övriga myndigheter som ingår i SAMFI att ta fram en strategi för samhällets informationssäkerhet 2010–2015. Strategin omfattar hela samhället, det vill säga alla statliga myndigheter, kommuner och landsting, företag, organisationer och privatpersoner. Den anger strategiska mål och områden samt principer för informationssäkerhetsarbetet. Strategin förvaltas av MSB.

För att förverkliga strategins intentioner har SAMFI-myndigheterna tagit fram en nationell handlingsplan för samhällets informationssäkerhet. Syftet med handlingsplanen är även att skapa en grund för en aktiv dialog om mål och metoder i det nationella informationssäkerhetsarbetet och en möjlighet för den enskilda organisationen att samordna sitt säkerhetsarbete med det nationella säkerhetsarbetet. Planen innehåller ett trettiotal åtgärdsförslag som syftar till att förverkliga den strategi för samhällets informationssäkerhet som SAMFI-myndigheterna gemensamt lade fram i januari 2011.

Arbetet med handlingsplanen har omfattat diskussioner och samverkan med ett stort antal aktörer. Därigenom har arbetet med handlingsplanen fortlöpande förankrats på olika nivåer i samhället.

Arbetet med handlingsplanen utgör även ett verktyg för myndigheterna i SAMFI att ta fram prioriterade åtgärder för att stärka samhällets informationssäkerhet. Åtgärdsförslagen ligger inom

ramen för de uppdrag som myndigheterna i SAMFI har. Planen är dock inte en komplett redovisning av de informationssäkerhetsfrämjande åtgärder som de olika myndigheterna genomför inom sina respektive verksamheter.

Handlingsplanen innehåller ett flertal konkreta åtgärder inom informationssäkerhetsområdet, bl.a. hur allvarliga it-incidenter ska hanteras, samt hur tekniska kompetensnätverk av experter kan skapas för att stödja samhället vid allvarliga it-incidenter och förslag på åtgärder för att skapa en ökad förmåga till respons.

Arbetet med 2012 års handlingsplan kommer att avslutas 2015. Under de senaste två åren har myndigheterna i SAMFI och andra aktörer genomfört ett stort antal aktiviteter för att öka samhällets informations- och cybersäkerhet. Arbetet med aktiviteterna presenteras efter halva tiden i en statusrapport om läget i arbetet.

Hur det civila försvaret kan utvecklas och stärkas

Regeringen uppdrog i juni 2014 åt MSB att redovisa hur det civila försvaret kan utvecklas och stärkas. MSB lämnade den 16 december 2014 en rapport till regeringen *Så kan det civila försvaret utvecklas och stärkas* (dnr MSB 2014-3277). Vad avser informations- och cybersäkerhet lade MSB fram ett flertal förslag och slutsatser. Det konstaterades att informations- och kommunikationssystem är en viktig och avgörande resurs inom i stort sett all samhällsverksamhet. Kris- och krigsviktig verksamhet och kritisk infrastruktur bör kunna skyddas med olika medel och metoder, där kryptografiska funktioner är ett sätt. Vidare konstaterade MSB att obligatorisk it-incidentrapportering är mycket väsentlig för att stärka den nationella förmågan att hantera it-incidenter i system som är kritiska för samhällsviktig verksamhet inför och under höjd beredskap. Även aktörer utanför den statliga sfären kommer att behöva omfattas om förmågan ska bli tillfredsställande. MSB drog vidare följande slutsatser. Arbetet med kommunikationssäkerhet i standardprodukter/program bör utvecklas i syfte att säkerställa att en bred krets av samhällsaktörer kan få tillgång till säker kommunikation inför och under höjd beredskap. Förmågan till informationshantering i dag är av stor vikt för samhällets aktörer. Det systematiska informationssäkerhetsarbetet som redan i dag

bedrivs bör väga in de krav som gäller under höjd beredskap. Utan kännedom om olika informationshanteringsprocessers betydelse och beroendeförhållanden kan varken rätt prioriteringar eller rätt skyddsåtgärder vidtas. All planeringsverksamhet avseende höjd beredskap, liksom för övrigt även viktiga områden inom krisberedskapen, inrymmer betydande delar av information som är av den karaktären att den bör omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400). Informationssäkerhet är därför ett område som i olika avseenden måste åtfölja all den planering för höjd beredskap och krig som genomförs inom olika verksamheter som är av betydelse för det samlade försvaret.

MSB konstaterar i rapporten att möjligheten att i förväg träna sin förmåga i praktisk it-incidenthantering är mycket begränsad. För att praktiskt kunna hantera it-angrepp krävs förmågehöjande träning för samhällsviktig verksamhet. MSB har i samverkan med Totalförsvarets forskningsinstitut utvecklat ett så kallat ”cyberrange” avsedd för förmågehöjande träning i hantering av it-incidenter. MSB kommer att se över möjligheterna till en utökad samverkan för praktisk träning av operatörer i samhällsviktig verksamhet som en del av förberedelserna för höjd beredskap.

MSB anser också att kunskap måste byggas upp hos aktörerna i civila försvaret. Under en följd av år har utbildning avseende försvarssekretess inte genomförts i den omfattning och med den intensitet som kommer att bli nödvändig när planeringen inom området civilt försvar ska påbörjas. MSB bedömer att det är nödvändigt att utbildning snabbt kommer igång inom alla berörda myndigheter, liksom även inom kommuner och landsting, vad avser frågor om informationssäkerhet och försvarssekretess.

MSB avser se över behovet av riktlinjer och metodstöd för kommunikation och lägesrapportering i hela hotskalan. I vardagen och vid kris kan rapportering ske via WIS, eller andra motsvarande system. Rapportering vid höjd beredskap bör kunna ske på motsvarande sätt via SGSI eller andra säkra kryptografiska informations- och kommunikationssystem. MSB kommer verka för ökad anslutning till SGSI och leda utvecklingen av andra tekniska system för kommunikation inför och under höjd beredskap och för samhällsviktig verksamhet.

7.4 Aktuella undersökningar

7.4.1 Riksrevisionens rapport

Riksrevisionen har år 2014 granskat om arbetet med informationssäkerhet i den civila statsförvaltningen är ändamålsenlig utifrån ökande hot och risker, *Informationssäkerhet i den civila statsförvaltningen* (RIR 2014:23). Granskningen har inriktats mot den information som samlats in om vilka hot som realiseras samt de skyddsåtgärder som har vidtagits av övriga myndigheter.

Granskningen omfattar regeringen och dess stöd- och tillsynsmyndigheter: Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt samt i viss mån Post- och telestyrelsen. Granskningen avser att besvara följande två frågor.

- Är regeringens styrning av informationssäkerhet i den civila statsförvaltningen effektiv?
- Har regeringens stöd- och tillsynsmyndigheter vidtagit tillräckliga åtgärder för att informera sig och regeringen om vilka hot som finns mot den civila statsförvaltningen, i vilken omfattning de realiseras och vilka skyddsåtgärder som vidtas?

Granskningen har visat på omfattande brister i statsförvaltningen. Av underlaget till granskningen framgår att 84 procent av myndigheterna som själva administrerar sina it-system uppger att de har en informationssäkerhetspolicy. Samtidigt framgår att 38 procent av myndigheterna bedömer att kompetens, mandat eller resurser är otillräckliga för att utföra informationssäkerhetsarbetet på ett tillfredsställande sätt. Vidare uppger 42 procent av myndigheterna att det saknas regler för vad en riskanalys, som ska göras i ett systematiskt informationssäkerhetsarbete, ska omfatta eller när den ska ske. Slutligen uppger 65 procent av myndigheterna att de saknar en kontinuitetsplan. Riksrevisionens bedömning är därför att en stor andel myndigheter inte har centrala delar av ett systematiskt informationssäkerhetsarbete på plats.

Riksrevisionens slutsats är att granskningen visar att arbetet med informationssäkerheten inte är ändamålsenligt sett till de hot och risker som finns. Regeringen har inte någon samlad lägesbild över hoten mot den civila statsförvaltningen, i vilken omfattning och mot vilka hoten realiseras samt vilka skyddsåtgärder myndig-

heterna vidtar. Detsamma gäller för regeringens stöd- och tillsynsmyndigheter.

För att förbättra statens informationssäkerhet rekommenderar Riksrevisionen därför regeringen följande:

- Utöka tillsynen av informationssäkerheten i den civila statsförvaltningen, så att den omfattar väsentligt mer än endast de allra mest skyddsvärda delarna.
- Låt utreda om regelverket som styr arbetet med informationssäkerheten är ändamålsenligt i sin nuvarande utformning och om ansvar för att utöva tillsyn över informationssäkerheten i den civila statsförvaltningen kan samlas och koordineras på ett bättre sätt än i dag. Dessa brister konstaterade Riksrevisionen redan 2007, och då bristerna fortfarande inte är åtgärdade är det angeläget med en skyndsam hantering.
- Överväg att låta tillsynsmyndigheten få mandat att utfärda sanktioner mot myndigheter som inte vidtar nödvändiga åtgärder efter en tillsyn som visat på brister.
- Inför snarast en obligatorisk incidentrapportering för samtliga myndigheter. Ge en myndighet i uppdrag att hantera denna rapportering.

Riksrevisionen konstaterar att det inte finns någon samlad central funktion i Regeringskansliet med ansvar för att bereda frågor om informationssäkerhet i statsförvaltningen och att ärenden rörande informationssäkerhet hanteras på flera departement beroende på ärendets karaktär (intern styrning och kontroll, förvaltningspolitik, krishantering, infrastruktur, etc.). Riksrevisionen anser att informationssäkerhet är en viktig strategisk fråga för hela statsförvaltningen, att det krävs kraft i styrningen för att skyddet ska kunna höjas till en ändamålsenlig nivå. För att skapa bättre förutsättningar för en effektiv styrning i informationssäkerhet rekommenderar därför Riksrevisionen följande.

- Se till att det finns en funktion och en process i Regeringskansliet med syfte att samlat hantera informationssäkerheten. Denna funktion och process ska kunna bereda alla de ärenden regeringen måste besluta om för att öka informationssäkerheten i statsförvaltningen. Funktionen ska också vara mottagare av

MSB:s information om en samlad lägesbild och annan nödvändig information om läget för informationssäkerheten i statsförvaltningen.

Beträffande regeringens stöd- och tillsynsmyndigheter anges att Riksrevisionen i granskningen kunnat visa att de inom nuvarande mandat skulle kunna göra mera, både genom att öka kunskapen om säkerhetsläget och att lämna stöd till den övriga statsförvaltningen för att öka skyddet. För att förbättra statens informationssäkerhet lämnar Riksrevisionen följande rekommendationer.

- MSB bör fortsätta och även intensifiera sitt arbete med att söka skapa en gemensam lägesbild för informationssäkerhet i statsförvaltningen.
- MSB har enligt 9 § andra stycket förordningen (2006:942) om krisberedskap och höjd beredskap möjlighet att begära att flera myndigheter än i dag lämnar en redovisning av sin risk- och sårbarhetsanalys till Regeringskansliet och MSB. MSB bör utnyttja denna möjlighet för att därigenom öka den samlade kunskapen om informationssäkerhetsläget och därigenom kunna bidra till en förbättring.
- MSB bör lämna de myndigheter som inte uppfyller kraven i föreskrifterna om statliga myndigheters informationssäkerhet (MSBFS 2009:10) det stöd som är nödvändigt, så att de uppnår efterlevnad inom rimlig tid.
- Såväl Säkerhetspolisen som FRA genererar viktig kunskap om säkerhetsläget inom den mest skyddsvärda delen av statsförvaltningen. Säkerhetspolisen och FRA bör därför var för sig systematiskt avge aggregerade rapporter om säkerhetsläget till Regeringskansliet och MSB.

7.4.2 En bild av myndigheternas informationssäkerhetsarbete 2014

Under 2014 har MSB genomfört en kartläggning (enkätundersökning) av hur statliga myndigheter tillämpar MSB:s föreskrifter om statliga myndigheters informationssäkerhet (2009:10) och i övrigt

arbetar med informationssäkerhet, *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter.*

Föreskrifterna ställer krav på att myndigheterna ska bedriva ett systematiskt informationssäkerhetsarbete. Totalt distribuerades enkäten till 351 myndigheter. 334 myndigheter (drygt 95 procent) besvarade enkäten inom undersökningsperioden och övriga (17 stycken) har inte lämnat något svar. Kartläggningen ger en god bild av hur myndigheterna själva uppfattar sitt arbete med informationssäkerhet och hur de arbetar med föreskrifternas olika krav. Frågorna i kartläggningen hade både direkt koppling till föreskrifternas paragrafer, exempelvis om riskanalys, och frågor av mer generell karaktär beträffande informationssäkerhetsarbete.

MSB har inte tagit del av något underlag från myndigheterna, exempelvis policyer eller informationsklassningsmodeller, och någon närmare bedömning av dokumentens och arbetets ändamålsenlighet ingår inte i kartläggningen.

Frågor om hur det praktiska informationssäkerhetsarbetet går till har endast ställts till de 227 myndigheter som själva har hand om sitt informationssäkerhetsarbete. Det är således endast dessa som fått besvara enkäten i sin helhet.

Några av resultaten har sammanfattats på följande sätt (s.7–8).

Policy och styrande dokument

- 84 procent av de myndigheter som besvarat hela enkäten har en informationssäkerhetspolicy.
- 26 procent av de myndigheter som besvarat hela enkäten kontrollerar inte efterlevnaden, det vill säga ifall policyer och riktlinjer följs av medarbetarna.

Leda och samordna informationssäkerhetsarbetet

- 74 procent av de myndigheter som besvarat hela enkäten har utsett en informationssäkerhetschef eller motsvarande roll för att leda och samordna informationssäkerhetsarbetet.

- 81 procent av de som leder och samordnar informationssäkerhetsarbetet hos de myndigheter som besvarat hela enkäten rapporterar direkt till myndighetens ledning.
- 38 procent av de som leder och samordnar informationssäkerhetsarbetet hos de myndigheter som besvarat hela enkäten uppges sakna tillräcklig kompetens, resurser eller mandat för att utgöra uppdraget på ett tillfredsställande sätt.

Informationsklassning

- 67 procent av de myndigheter som besvarat hela enkäten har en informationsklassningsmodell för att identifiera informationstillgångarna och kunna ställa rätt krav på informationssäkerheten.
- 41 procent av de myndigheter som besvarat hela enkäten uppger att det inte är tydligt uttalat vem som ansvarar för att informationsklassning genomförs.
- 59 procent av de myndigheter som besvarat hela enkäten uppger att det inte är fastslaget när informationsklassning ska ske.

Riskanalys och dokumentation

- 78 procent av de myndigheter som besvarat hela enkäten har en metod för riskanalys.
- 42 procent av de myndigheter som besvarat hela enkäten saknar regler för vad riskanalyser ska omfatta eller när det ska ske.
- 35 procent av de myndigheter som besvarat hela enkäten saknar uttalat ansvar för vem som ska initiera riskanalyserna.

Kontinuitetsplanering

- 65 procent av de myndigheter som besvarat hela enkäten saknar kontinuitetsplan.

- 59 procent av de myndigheter som besvarat hela enkäten använder inte riskanalyserna som stöd vid kontinuitetsplanering.

Ledningens engagemang

- 45 procent av de myndigheter som besvarat hela enkäten uppger att myndighetens ledning åtminstone i stor utsträckning löpande håller sig informerade om arbetet med informationssäkerhet.
- 37 procent av de myndigheter som besvarat hela enkäten har ingen eller en mycket begränsad utvärdering av informationssäkerhetsarbetet på myndigheten.

Behov av stöd

- Myndigheterna nämnde ett antal områden inom vilka man önskade mer stöd, bland annat kravställning, uppföljning, informationsklassning och kontinuitetsplanering.
- Myndigheterna önskade sig stöd i flera olika former, bland annat nämndes malldokument, utbildningsdokument, vägledningar och praktiska exempel.

7.5 Tekniska funktioner för skyddad kommunikation

7.5.1 Krypto och signalsskydd

Krypto

Under rubriken krypto ryms en mängd begrepp och metoder som i dag alla bygger på matematisk teoretisk grund. Historiskt sett är ett krypto en metod att förvanska en text eller ett budskap så att avsändaren kan vara säker på att den legitima mottagaren är den ende som kan läsa eller tolka budskapet rätt. Avsikten var också att mottagaren skulle vara övertygad om vem avsändaren var. Nödvändigt, då som nu, var att mottagaren kände till meddelandets hemliga nyckel. En kryptonyckel kan sägas vara den minsta informationsmängd som behövs för att fullständigt återskapa det krypte-

rade meddelandets information. Dessa principer gäller fortfarande, men de historiska metoderna har ersatts efter hand, och kryptologi är i dag ett forskningsområde inom flera akademiska discipliner. Även moderna krypteringsmetoder har i vissa fall visat sig olämpliga eller mindre säkra än vad som först bedömdes. Detta kan bero på nya teoretiska landvinningar, kraftfullare datorer för kryptoanalys eller att krypteringsmetoden fått annan användning.

Kryptoanalys

Kryptoanalys kan vara antingen (a) att på ett metodiskt sätt försäkra sig om att en metod för kryptering uppfyller givna krav på säkerhet och funktion, eller, i princip det omvända, (b) att givet resultatet av en kryptering med alla medel försöka återskapa den dolda informationen eller den okända krypteringsnyckeln. En grov beskrivning är att säga att kryptoanalys (a) bedrivs inom signalskyddsutvecklingen, medan kryptoanalys (b) försiggår inom signalunderrättelseverksamheten. Två traditionellt sett organisatoriskt åtskilda aktiviteter, men där fördelar finns med en närmare relation och ett kunskapsutbyte. Särskilt i riktningen från signalunderrättelseverksamheten till signalskyddsutvecklingen och informations- och cybersäkerhetsarbetet, där vunna erfarenheter kan komma samhället till nytta då det gäller att bygga en säker it -infrastruktur.

Design av krypto

Ett system för informationssäkerhet eller kommunikationssäkerhet – ett kryptosystem eller ett kryptografiskt protokoll – byggs upp av kryptografiska primitiver som var för sig står för grundläggande egenskaper viktiga för ett krypterande system anpassat till en viss användning. Exempel på primitiver är slumptalsgeneratorer (pseudo random number generator, PRNG), envägsfunktioner (one-way function) och naturligtvis krypteringsfunktioner. Säkerheten hos primitiverna styrks genom att applicera kända attacker och angrepp, och på så sätt få ett visst mått på säkerheten i form av en uppskattning av den tid och datorkraft som skulle krävas för en lyckad attack. Nya attacker upptäcks dock ständigt, och revidering av säkerhetsbedömningen kan behöva göras.

Vid design av ett krypto eller kryptosystem är det av största vikt att ta hänsyn till vad kryptot ska användas till. Avvägningar måste göras vad gäller krypteringshastighet, effektförbrukning, minnesutrymme, nyckelhantering, driftsäkerhet, nationella krav, m.m. Alla dessa faktorer påverkar valet av primitiver och kryptosystemets slutliga utformning.

Forcering av krypto

Att forcera, eller knäcka, krypton är en historiskt sett alltid lika aktuell och fascinerade verksamhet. Att forcera ett krypterat meddelande är att med kryptoanalys, beräkningar och databehandling samt eventuellt med hjälp av någon egenskap hos den dolda informationen återvinna hela eller delar av meddelandets innehåll. Det är alltså inte givet att en lyckad forcering också leder till att den hemliga meddelandenyckeln klarläggs.

I de fall krypteringsmetoden är känd och den hemliga nyckeln består av ett lösenord är det enkelt att knäcka kryptot om lösenordet är kort eller illa konstruerat. Då prövar kryptoforceraren helt enkelt att dekryptera med alla korta och alla sannolika längre lösenord tills en läsbar text, bild eller annan meningsfull information erhålls. Vanligt är att krypteringsmetoden är implementerad så att riktigheten hos ett lösenord kan kontrolleras innan dekryptering startar, och detta utnyttjar i så fall forceraren. I detta fall, då man finner ett lösenord genom totalprövning, så talar vi inte om kryptoanalys i egentlig mening eftersom krypteringsmetodens eller kryptots matematiska egenskaper inte utnyttjas.

Metoder för kryptering konstrueras, analyseras och utvärderas av såväl den offentliga forskarvärlden som inom myndigheter och organisationer knutna till nationell säkerhet. Standardiseringsorgan och industrigrupper arbetar fram standarder för hur krypteringsmetoder ska implementeras och användas. Nationella säkerhetsmyndigheter granskar kryptosystem och utarbetar regler för dess användning innan de godkänns för att skydda information som rör nationens säkerhet eller annan skyddsvärd information. Likväl kan kryptoforceraren under vissa omständigheter ha framgång.

Krypteringsmetodens svagheter, ett insteg som utnyttjas vid forceringsarbetet, kan bero på att de förutsättningar och antagan-

den som gällde vid teoretiska analysen inte alltid föreligger då metoden används i praktiken. Avvägningar mellan användarvänlighet, effektivitet, okunskap och kommersiella hänsyn kan bidra till att mer eller mindre kalkylerade risker accepteras när en standard utformas. Det kan t.ex. vara upp till användaren att göra även säkerhetskritiska konfigureringar när ett krypterande protokoll används för informationsöverföring. Och även om informationssystemet i sig är tillförlitligt, så kan felaktigt handhavande eller brister i nyckelhanteringen bidra till att en kryptoforcerare med tillräckligt stora resurser når framgång.

Under förutsättning att forceraren har tillgång inte bara till den krypterade informationen utan även till det program eller den utrustning som utfört krypteringen så öppnar sig andra möjligheter. Det kan vara reverse engineering, som innebär att kryptoutrustningens konstruktion och funktion återskapas in i minsta detalj, och att hemliga parametrar på så sätt eventuellt klarläggs. En annan möjlighet är en s.k. sidokanalsattack, där man studerar strömförbrukning eller annan läckande information, som avslöjar kryptoutrustningens interna tillstånd under krypteringsprocessen.

Signalskydd och krypto för skyddsvärda uppgifter (KSU)

Signalskydd är åtgärder som syftar till att förhindra obehörig insyn i och påverkan av tele- och radiokommunikationer. Signalskydd omfattar bl.a. användning av kryptografiska funktioner i informationssystem. Termen signalskydd har sina rötter i den avlyssning genom signalspaning som ständigt pågår mot telekommunikations- och informationssystem som en väsentlig del av främmande makts underrättelsetjänst

Begreppet signalskydd är starkt reglerat och avser obligatoriskt skydd av elektronisk kommunikation av sekretessbelagda uppgifter som rör rikets säkerhet. Signalskyddssystemens skyddsnivå är dimensionerad att möta hotbilden från andra länders underrättelsetjänster och kräver därför omfattande skyddsåtgärder samt att systemen är företrädesvis är framtagna av en inhemsk kryptoindustri.

Behovet av att skydda elektronisk kommunikation i bredare mening än för rikets säkerhet har kommit att bli allt mer aktuellt.

Därför har det på senare år tagits fram krypto för skyddsvärda uppgifter (KSU). KSU utgörs av kryptosystem som tillsammans med ett regelverk är nationellt godkända av Försvarsmakten och kan användas vid elektronisk kommunikation av sekretessbelagda uppgifter som inte rör rikets säkerhet. KSU är alltså ingen ersättning utan ett komplement till signalskydd. Termen ”säkra kryptografiska” funktioner avser både signalskydd och KSU. Målsättningen med KSU är att kvalitetssäkrade och kommersiellt tillgängliga produkter, tillsammans med ett av Försvarsmakten framtaget regelverk och en för organisationen anpassad hantering, ska kunna höja säkerhetsnivån jämfört med i dag.

För att system som använder säkra kryptografiska funktioner ska kunna ge ett effektivt skydd krävs att hela processen, allt från generering av kryptonycklar till slutanvändarnas hantering av systemet, håller en nivå som är anpassad för den information som systemet avser att skydda. Genom nationellt godkännande säkerställs skyddsnivån och kvaliteten på såväl teknik som regelverk, rutiner och behörighetsutbildning.

I dag har över 160 organisationer godkända signalskyddssystem. För civilt bruk finns 17 godkända signalskyddssystem inom produktområdena datakommunikation, meddelandekrypton och talkrypton. Dessa system är gemensamma för Försvarsmakten och civila sektorn. Det finns endast ett godkänt KSU-krypto (filkryptot KGAI). Detta är dock det nationellt mest utbredda kryptosystemet.

Traditionellt har signalskydd framförallt varit en militär angelägenhet, där det gällt att skydda sin egen kommunikation mot fientlig signalspaning. Historiskt har det militära behovet av signalskydd ensamt motiverat omfattande statliga satsningar på utveckling av signalskyddssystem.

Det civila behovet har uppstått genom samordningsbehov mellan militärt och civilt försvar inom ramen för totalförsvaret. 1959 skapades därför en totalförsvarsgemensam signalskyddsstruktur då Statens signalskyddsnämnd (SN) bildades. Efter det kalla kriget har inriktningen av den civila signalskyddsverksamheten även kopplats till krisberedskap. I 1992 års försvarsbeslut fick den civila delen av totalförsvaret även uppgift att värna civilbefolkningen under kriser. I 1996 års försvarsbeslut kom det vidgade säkerhetsbegreppet. Definitionen av totalförsvaret ändrades

inte utan insikten om samhällets säkerhet och den vidgade hotbilden ledde fram till Sårbarhets- och säkerhetsutredningen 2001. Ansvaret för den civila inriktningen och materielförsörjningen övertogs av Krisberedskapsmyndigheten (KBM) från Överstyrelsen för civil beredskap när KBM inrättades 2002. När KBM lades ned 2008 övergick inriktningsansvaret den civila signalskyddsverksamheten till den nybildade myndigheten MSB och materielförsörjningen till FRA. Den civila signalskyddsverksamheten regleras i Krisberedskapsförordningen.

År 2007 fick Försvarsmakten i myndighetens instruktion uppdraget att, utöver signalskyddstjänsten, även leda och samordna arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information.

Under senare år har behovet av kryptografiska funktioner för internationell verksamhet ökat markant, särskilt inom EU och NATO. Under 2011 blev Sverige en godkänd andraparts-evaluerare av krypto inom EU. Denna funktion, AQUA (Appropriately Qualified Authority), innehas av Försvarsmakten. Det finns i dag fem svenska kryptosystem som godkänts av Europeiska unionens råd.

7.5.2 Sensorsystem

För att skydda information och upptäcka it-säkerhetsincidenter har dagens organisationer ofta ett antal olika säkerhetssystem installerade. Det handlar exempelvis om virusskydd, brandväggar, spamfilter och olika intrångsdetekteringssystem. Effektiviteten hos dessa system när det gäller att detektera och hantera it-säkerhetsincidenter med hjälp av olika sensorer beror i stor utsträckning på de kommersiella aktörernas tillgängliga data om skadlig kod, infekterade IP-adresser och motsvarande.

System som använder sensorer för att upptäcka intrång och angrepp (sensorsystem) kan vara utformade på olika sätt och ha som syfte att inte bara stärka organisationens utan även samhällets säkerhet. Vid angrepp som drabbar kritisk infrastruktur och samhällsviktig verksamhet på bredare front saknas det för närvarande möjlighet att skapa en sammanhållen lägesbild. I dag förfogar nätoperatörerna, säkerhetsföretag och andra aktörer var och en över

sin del av lägesbilden, ingen har direkt tillgång till en helhetsbild. Angrepp eller skadlig kod som drabbar flera verksamheter samtidigt riskerar att uppfattas som mindre allvarliga och som enstaka attacker. Det innebär även en risk att varningar samt kunskap om attackens utformning, konsekvenser och möjliga förebyggande åtgärder inte sprids till andra aktörer som kan drabbas av samma angrepp.

Ett sensorsystem består mycket förenklat av tekniska sensorer, en kommunikationslösning och en central funktion för analys som till sin hjälp för att upptäcka angrepp och skadlig kod har en förteckning över aktuella skadliga koder och IP-adresser. Sensorerna skannar trafik hos anslutna organisationer och om en kod eller IP-adress som finns angiven i förteckningen fångas upp skickas ett larm som kan gå såväl till den verksamhet som är utsatt för it-angreppet som till en central analysfunktion.

7.5.3 It-incidentrapportering

I dagsläget finns två former av rapportering av it-incidenter; operativ it-incidentrapportering som sker med frivillighet som grund, och obligatorisk it-incidentrapportering som genomförs kopplat till tillsynsarbete. Det föreligger en viss skillnad emellan de olika formerna av rapportering. Den operativa rapporteringen sker i samverkanssyfte för att dela information och kunskap om inträffade incidenter. Genom att kontinuerligt samla information om och analysera it-incidenter utvecklas kunskapen inom detta område. It-incidentrapportering som är kopplad till tillsyn utförs för att skapa underlag för en granskning som sker i ett särskilt syfte.

EU:s arbete med reglering av it-incidentrapportering inom medlemsstaterna präglas av att en enhetlig modell för rapporteringen utvecklas inom området. Denna modell återfinns bl.a. i kommissionens förordning 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation, artikel 2. Förordningen ligger till grund för operatörernas skyldighet att rapportera integritetsincidenter enligt lagen (2003:389) om elektronisk kommunikation (LEK). En skyldighet att rapportera

incidenter av samma modell finns även i Europaparlamentet och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, eIDAS, artikel 19. eIDAS börjar tillämpas från den 1 juli 2016.

Operatörerna inom sektorn elektronisk kommunikation omfattas av en skyldighet att rapportera störningar avseende driftsäkerhet, 5 kap. 6 c § LEK, och integritetsincidenter, 6 kap. 4 a § LEK. Rapportering av incidenter sker till sektorsansvarig myndighet, PTS. Syftet med operatörernas rapporteringsskyldighet är att skapa ett informativt underlag om inträffade incidenter. Underlaget granskas och utgör i förekommande fall grund för tillsynsärenden.

EU:s reform av reglerna om skydd för personuppgifter innehåller en skyldighet att rapportera it-incidenter. Sker ett dataintrång ska den nationella tillsynsmyndigheten (i Sverige Datainspektionen) och de som berörs av intrånget informeras inom 24 timmar. Reformförslaget innebär att Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet) ska ersättas av en ny allmän dataskyddsförordning. Dataskyddsdirektivet har i Sverige genomförts genom personuppgiftslagen (1998:204) och ett antal särregleringar i förhållande till denna lag (särskilda registerförfattningar).

Sveriges it-incidentcentrum (Sitic) bildades 2003 på PTS som en nationell funktion med uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter. Sitic fungerade som en nationell CERT-organisation, dvs. en rikscentral för it-incidentrapportering. 2011 omorganiserades Sitic till MSB och bytte namn till CERT-SE. CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter. Det finns även andra CERT:ar hos bl.a. Försvarsmakten som hanterar it-säkerhetsincidenter inom de egna organisationerna och samverkar med andra CERT-funktioner vid it-incidenter och i informationssäkerhetsfrågor.

För att stärka samhällets informationssäkerhet och förmåga att förebygga och hantera it-incidenter beslutade regeringen att ge

MSB i uppdrag att utreda hur ett system för obligatorisk it-incidentrapportering för statliga myndigheter kan utformas (Fö2010/701/SSK). Uppdraget redovisades 2011 och föreslog en dubbelriktad rapporteringsprocess för inrapportering till MSB/CERT-SE och återkoppling till berörda parter. Det bedömdes att en kontinuerlig it-incidentrapportering hos statliga myndigheter skulle kunna bidra till en aktuell lägesbild av tillståndet vid samhällsviktig verksamhet och kritisk infrastruktur.

Regeringen återförde uppgiften till MSB 2012 (Fö2012/717/SSK) med uppdraget att genomföra en fördjupad analys av förslaget om system för obligatorisk it-incidentrapportering för statliga myndigheter som myndigheten redovisade 2011. I uppdragsredovisningen lämnade MSB förslag på ett nationellt system för it-incidentrapportering. Enligt förslaget skulle det bli obligatoriskt för statliga myndigheter under regeringen att ansluta sig till systemet och frivilligt för övriga aktörer. En grundläggande utgångspunkt var att systemet för obligatorisk och frivillig it-incidentrapportering skulle utformas på ett sådant sätt att det skapas mervärde för anslutna aktörer. Systemet skulle bidra till ökad informationssäkerhet och förmåga till krisberedskap både på organisations- och samhällsnivå. I redovisningen påpekas att de rapporterande organisationernas förtroende för it-incidentrapporteringssystemet är centralt för dess funktion och effekt. Vidare konstaterades att det redan i dag finns incidentrapporteringssystem för specifika syften. I uppdraget ingick inte att utforma ett system som ersätter denna typ av rapporteringssystem. Det föreslagna systemet skulle inte ersätta anmälningar om brottslig verksamhet till Polismyndigheten.

7.5.4 Skyddad kommunikationsinfrastruktur

God informationssäkerhet kräver en informationsinfrastruktur som medger säker hantering av information och kommunikation. Informationsinfrastrukturen bör fungera för såväl normala förhållanden som för krisberedskap och för totalförsvarets behov med bibehållande av en hög nivå av informationssäkerhet.

Regeringen gav den 14 april 2010 MSB i uppdrag att senast den 1 mars 2011 lämna förslag beträffande en säker digital informations- och kommunikationsstruktur för myndigheter, kommuner

och landsting (Fö2010/701/SSK). MSB genomförde uppdraget i samråd med andra aktörer, bl.a. SAMFI, FOI, Skatteverket samt Delegationen för e-förvaltning. I uppdraget ingick att beakta såväl befintliga kommunikationsinfrastrukturer, kommersiella system samt alternativa förslag. Samråd skulle även ske med Försvarsmakten samt Försvarets radioanstalt i syfte att analysera hur befintliga eller kommande kryptosystem kan användas för att skydda skyddsvärd eller sekretessbelagd information. Uppdragsredovisningen föranledde inga vidare åtgärder från regeringen.

Det finns flera informationsinfrastrukturer för offentlig sektor. Försvarsmakten är systemägare av Försvarsmaktens Telenät (FTN) och Försvarsmaktens IP-nät (FMIP). Mer om FTN i följande avsnitt. Nätens robusthet och redundans är anpassade efter Försvarsmaktens behov. Trafiken går krypterad över Försvarsmaktens egen radiolänk, samt i förhyrd fiber i privata nät som leds trafikskyddad till Försvarsmaktens egna noder. Trafiken i FMIP är krypterad med Försvarsmaktens egen kryptering och Försvarsmakten elförsörjer sina egna nät. Externa aktörer vars verksamhet är av kritisk betydelse för samhället har tillgång till FTN och FMIP.

Swedish Government Secure Internet, (SGSI) etablerades ursprungligen för att tillgodose behovet av skyddad kommunikation mellan svenska myndigheter och EU-myndigheter. Det är ett virtuellt nät som är logiskt separerat från det allmänna kommunikationsnätet och som medger krypterad kommunikation med de andra aktörer som är anslutna till nätet. SGSI är anslutet till EU:s säkerhetsskyddade kommunikationsnät, sTESTA (secure Trans European Services for Telematics between Administrations) via en gateway. SGSI administreras av MSB. Försvarsmakten ansvarar för drift av knutpunkt samt kryptering.

För att skapa en skyddad kommunikationsinfrastruktur krävs såväl fysiska som logiska skyddsåtgärder. Arbetet med de fysiska skyddsåtgärderna bedrivs på olika sätt beroende av om staten väljer att bygga, äga och förvalta hela kommunikationsstrukturen själv, eller att hyra svartfiber i existerande privata nät, såsom Teracom, Svenska Kraftnät och liknande aktörer. Det logiska skyddet omfattar bl.a. ett krypterat skydd för trafiken och andra åtgärder.

Oavsett vilken lösning som är aktuell är det angeläget att beställaren äger tillräcklig kunskap om vilken säkerhet som krävs för att skydda olika typer av kommunikation. Den statliga förvalt-

ningen omfattar verksamheter vars behov av skydd är av olika karaktär. För att kunna ställa adekvata krav vid upphandling och avtals ingående krävs kunskap om informationssäkerhet och en bred samverkan inom den statliga förvaltningen.

En säker informationsinfrastruktur för den statliga förvaltningen är en förutsättning för dess informationssäkerhet. Det finns i dagsläget alternativ som erbjuder skyddad informationshantering och kommunikation. En avvägning mellan kostnader och behovet av säkerhet behöver ske inför arbetets utveckling. Kostnadsdrivande lösningar måste ställas emot behovet av en säker kommunikationsinfrastruktur som är dimensionerad för den statliga förvaltningens behov. Skyddet måste vara adekvat och anpassat för att fungera för såväl krisberedskap som för totalförsvarets behov. Det kan dock finnas anledning att särskilt beakta konsekvenserna av att involvera privata aktörer då det i dagsläget inte finns någon reglering som kräver att de privata aktörerna inom sektorn elektronisk kommunikation ska bedriva sin verksamhet sammanhållet inom Sverige. Dessutom behöver arbetet med en skyddad kommunikationsinfrastruktur ta hänsyn till att det finns frågor avseende det fortifikatoriska skyddet som kvarstår som olösta.

Försvarets telenät

Hela vårt moderna samhälle är beroende av att telekommunikationerna fungerar bra. Information måste snabbt, säkert och oförvanskad kunna nå fram till rätt mottagare. Detta gäller i särskilt hög grad försvarets olika delar. Såväl i fred som i kris och krig kan störningar i teletrafiken få ödesdigra konsekvenser. I Sverige finns ett separat landsomfattande telenät som skapats för att tillgodose militära behov av ett skadetåligt nät för telekommunikationer. Det kallas Försvarets Telenät (FTN) och är uppbyggt som ett komplement till de publika (allmänt tillgängliga, kommersiella) telenäten. FTN är logiskt avskilt från de publika telenäten, vilket är en grundförutsättning för att kunna säkerställa erforderligt samband när publika nät utsätts för extrema påfrestningar och överbelastningar. Erfarenheter visar att även förhållandevis vardagliga händelser kan generera så mycket trafik att publika nät överbelastas.

Anläggningar i FTN:s stomnät utgörs av fortifikatoriskt skyddade byggnader utformade för obemannad teknisk drift. Anläggningarna är militära skyddsobjekt och tillträdeskontrollerade.

FTN har tillkommit av flera skäl. Det viktigaste är att de militära kraven i vissa avseenden är så höga att de publika telenäten inte uppfyller dem. Ett annat viktigt skäl är att de publika telenäten finns främst i tätbefolkade områden där den kommersiella efterfrågan är störst. Försvaret, å andra sidan, måste kunna verka i hela landet.

Abonnenterna i FTN är främst förband inom mark-, sjö- och luftstridskrafterna samt bemannade och obemannade anläggningar tillhörande dessa stridskrafter. FTN har även abonnenter inom det civila totalförsvaret och antalet civila abonnenter har ökat med tiden. Luftförsvarsutredningen 2040 skriver följande i betänkandet SOU 2014:88 s. 23:

”Robusta lednings- och sambandssystem utgör en viktig grund för den sammanlagda funktionen inom luftstridskrafterna. Att säkerställa ett robust, och inom Försvarsmakten väl balanserat gemensamt ledningssystem, är inte bara en fråga för luftförsvaret utan är en betydelsefull komponent i det civila samhället.”

7.6 Samverkan

7.6.1 Samverkansgruppen för informationssäkerhet (SAMFI)

I gruppen SAMFI samverkar i dag myndigheter med särskilda uppgifter och särskilt ansvar inom området informationssäkerhet. Gruppen träffas cirka sex gånger per år och syftet är att underlätta samarbetet genom informationsutbyte och samverkan. De myndigheter som medverkar är följande.

- Myndigheten för samhällsskydd och beredskap (MSB)
- Post- och telestyrelsen (PTS)
- Försvarets radioanstalt (FRA)
- Säkerhetspolisen (Säpo) och Nationella operativa avdelningen (NOA, tidigare Rikskriminalpolisen) i samverkan

- Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för it-säkerhet (CSEC)
- Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST)

SAMFI bildades 2003 efter att regeringens då nya strategi för samhällets informationssäkerhet föreslagits i propositionen *Samhällets säkerhet och beredskap* (prop. 2001/02:158). Strategin skulle i huvudsak bäras upp av de fyra myndigheterna Krisberedskapsmyndigheten (KBM), PTS, FMV samt FRA. För att underlätta samarbetet mellan dessa myndigheter bildades SAMFI och i samband med detta inbjöds även FM/MUST samt Säpo och Rikskriminalpolisen att medverka. I samband med att MSB bildades år 2009 övertog myndigheten ansvaret för SAMFI.

MSB har i samverkan med övriga myndigheter i SAMFI tagit fram strategin för samhällets informationssäkerhet 2010–2015. År 2012 publicerade MSB tillsammans med de myndigheter som ingår i SAMFI en handlingsplan som ska stärka informationssäkerheten i samhället och förverkliga strategin, se avsnitt 7.3.2.

SAMFI verkar för säkra informationstillgångar i samhället avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet. Genom informationsutbyte och samverkan stödjer SAMFI deltagande myndigheter varandras arbete avseende samhällets informationssäkerhet.

SAMFI berör frågeställningar inom huvudsakligen följande aktivitetsområden:

- Strategi, handlingsplan och regelverk
- Tekniska frågor och standardiseringsfrågor
- Nationell och internationell utveckling inom informationssäkerhetsområdet
- Informationsaktiviteter
- Övningar och utbildning
- Hantering och förebyggande av it-incidenter

MSB avsätter resurser för ett SAMFI-kansli. Övriga SAMFI–myndigheter bidrar med resurser vid behov och efter förmåga.

Representanter för de myndigheter som ingår i SAMFI träffas för att diskutera pågående arbete och aktuella frågor inom samhällets informationssäkerhet. Efter koncensus i SAMFI kan arbetsgrupper tillsättas för att arbeta med aktuella frågor. En SAMFI-myndighet har rätt men inte skyldighet att delta i dessa arbetsgrupper. Som exempel på SAMFI:s arbetsgrupper kan nämnas följande.

- SAMFI Ag Handlingsplan: Arbetsgruppen etablerades för att stödja MSB i arbetet med att ta fram handlingsplanen för samhällets informationssäkerhet 2012.
- SAMFI Ag Skyddsprofiler: Arbetsgruppen arbetar med utvecklingen av skyddsprofiler, enligt standarden Common Criteria, för prioriterade produktkategorier.
- SAMFI Ag Informationssäkerhetskonferens: Arbetsgruppen planerar och genomför den årliga informationssäkerhetskonferensen för offentlig sektor.
- SAMFI Ag Terminologi: Arbetsgruppen har arbetat med att bearbeta underlag för den kommande utgåvan av SIS HB 550 *Terminologi för informationssäkerhet.*

7.6.2 Nationell samverkan till skydd mot allvarliga it-hot (NSIT)

Säkerhetspolisen, Försvarsmakten (Must) och Försvarets radioanstalt (FRA) har inom området it-hot sedan 2012 ett samarbete kallat Nationell samverkan till skydd mot allvarliga it-hot (NSIT). Inom ramen för NSIT-samarbetet analyseras och bedöms hot och sårbarheter när det gäller allvarliga eller kvalificerade it-angrepp mot våra mest skyddsvärda nationella intressen. Syftet är att utveckla samverkan för att försvåra för en kvalificerad angripare att komma åt eller skada svenska skyddsvärda civila och militära resurser.

7.6.3 Nationella telesamverkansgruppen (NTSG)

Inom sektorn elektronisk kommunikation arbetar bl.a. de största operatörerna i den nationella telesamverkansgruppen NTSG. NTSG har initierats av PTS och är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället. I gruppen ingår bl.a. operatörer, Svenska Kraftnät, Teracom, Trafikverket ICT, Försvarsmakten, Myndigheten för samhällsskydd och beredskap samt Post- och telestyrelsen.

Gruppen verkar i syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid extraordinära händelser i samhället. Vid stora kriser eller extraordinära händelser kan det uppstå situationer som underlättas av att operatörerna bistår varandra. Vid en kris sammanställer gruppen skadeläget, återrapporterar läget till berörda parter och ger vid behov förslag till åtgärder. Gruppen kan också om så krävs, koordinera insatser.

I NTSG bedrivs arbetet med Gemensam lägesuppfattning (GLU). Syftet med GLU är att reducera störningar och minska effekten av dem för andra sektorer i samhället vars verksamhet är beroende av elektronisk kommunikation. Syftet är också att öka samhällets förmåga att hantera konsekvenser av störningar och avbrott i näten. Målet är att skapa en gemensam lägesuppfattning hos aktörerna inom sektorn elektronisk kommunikation i händelse av stora störningar. En gemensam lägesuppfattning ökar samverkansmöjligheterna, då operatörerna på ett snabbt sätt kan erhålla och utbyta detaljerad information om status och prognos för pågående störningar i viktiga tjänster i näten. Hos operatörerna utnyttjas informationen i arbetet för att återställa kapaciteten och minska konsekvenserna av störningarna.

Delar av informationen i GLU går att formulera så att den kan göras förståelig och delges andra intressenter. Operatörernas kunder kan exempelvis vara andra teleoperatörer, företag, myndigheter, kommuner och enskilda personer. I GLU får dessa och andra aktörer i samhället inom exempelvis elsektorn, krisansvariga myndigheter, medierna och allmänheten tillgång till information om läget via internet och respektive operatörs webbplats.

Driftinformation mellan operatörer, DIO, är ett system som används mellan operatörer och innebär att driftinformation kan

utbytas på ett standardiserat sätt. DIO syftar till att skapa en mer ekonomisk, säkrare och effektivare överföring av information om driftstörningar orsakade av akuta fel eller planerade avbrott.

7.6.4 Nationellt arbete med fokus på industriella informations- och styrsystem

Inom området industriella informations- och styrsystem är det centralt att upprätthålla en hög nationell kompetens kring säkerhet i industriella informations- och styrsystem (SCADA-system). Se avsnitt 4.4.3 avseende hot och risker inom området. Det är också viktigt att genom internationell samverkan följa och ibland leda arbetet med harmonisering av standarder och branschpraxis och att länder lär av varandra.

För att stötta den speciella situation som råder i verksamheter som hanterar industriella informations- och styrsystem driver Myndigheten för samhällsskydd och beredskap, sedan ett antal år tillbaka dessa frågor i en samlad satsning, ett program för ökad säkerhet i industriella informations- och styrsystem. Arbetet riktar sig såväl mot den offentliga som privata sektorn och fokuserar på medvetandehöjning, kunskapshöjning och förmågehöjning av berörda aktörer. De mer precisa målgrupperna är de aktörer som driver industriella informations- och styrsystem, exempelvis elbolag, vattenproducenter, transportföretag och kemiska processindustrier. Även kommuner och myndigheter med ansvar för en ”sektor” är viktiga målgrupper, liksom leverantörer av teknisk utrustning som ingår i industriella informations- och styrsystem. En central del i detta arbete är det kunskapscentrum som MSB har etablerat i samverkan med Totalförsvarets forskningsinstitut (FOI). Arbetet mellan MSB och FOI har bedrivits de senaste sju åren och för fyra år sedan etablerade myndigheterna tillsammans, Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3). Inom ramen för NCS3 genomförs bland annat teknisk utbildning av aktörer från samhällsviktig verksamhet. Under det senaste året har bland annat ett nytt koncept för praktisk träning i att motstå it-angrepp tagits fram. I ett så kallat *cyberrange* får de olika aktörerna öva och se effekterna av hot- och risker mot samhällsviktig verksamhet.

Inom centrumbildningen (mellan MSB och FOI samt andra berörda aktörer) genomförs också studier som syftar till att analy-

sera säkerhetsproblem kopplade till industriella informations- och styrsystem. Dessa studier kan vara av både teknisk och strategisk karaktär och de färdiga rapporterna används sedan för att öka olika aktörers medvetenhet om hot och risker i denna domän.

De utbildningsinsatser som bedrivs inom NCS3 är av medvetandehöjande, kunskapshöjande och förmågehöjande natur.

En av de centrala delarna i MSB:s program för ökad säkerhet i industriella informations- och styrsystem är medvetandehöjande aktiviteter. Dessa består bl. a. i att hålla föredrag på mässor och branschträffar för att belysa vikten av säkerhet i industriella informations- och styrsystem. I detta sammanhang är det viktigt att nå ut till personer på ledningsnivå. MSB har beskrivit för utredningen att det är slående ofta som ansvariga chefer inte känner till skillnaden mellan kraven på it-säkerhet ”på kontoret” och kraven som råder i industriprocesserna. Industriella informations- och styrsystem ”faller mellan stolarna” och betraktas inte som it-system utan som produktionssystem. Det kan få till följd att det inte finns någon som tar ansvar för säkerheten i dessa system eller ställer krav på att säkerheten ska utvecklas. Genom NCS3 har programmet också utvecklat ett antal så kallade demonstratorer som på ett pedagogiskt sätt kan gestalta effekten av ett angrepp mot ett industriellt informations- och styrsystem. I dagsläget används främst en modell av ett vattenreningsverk, ett portabelt system med trafikljus samt en uppsättning ”fabriker” som kan angripas. Detta ger pedagogiska effekter som gör presentationerna mer levande och verklighetsnära. Behovet av medvetandehöjande aktiviteter är dock stort och åtgärder som dessa skulle behöva öka avsevärt.

En annan central komponent i arbetet är kunskapshöjande aktiviteter. Det är viktigt att även den tekniska personal som arbetar med informations och styrsystem har kunskap och förståelse om vikten av att dessa system är skyddade. Därför har NCS3 tagit fram en tvådagars-utbildning kring säkerhet i industriella informations- och styrsystem. Utbildningen varvar teori med praktik och genomförs fyra till fem gånger per år. Varje kurstillfälle, som är öppet för 16 personer, är anpassat till en specifik målgrupp – exempelvis elproducenter eller vattenproducenter. Den här sektorsanpassningen innebär att både de teoretiska och de praktiska delarna kan anpassas tydligare mot den verklighet som aktörerna befinner sig i

till vardags. Den innebär också att deltagarna får möjlighet att under förtroliga former diskutera sektorsspecifika frågor och att bygga nätverk. De praktiska delarna anpassas utifrån deltagarnas förkunskaper. Generellt går övningarna ut på att experimentera med olika verktyg för säkerhetsanalys. Deltagarna får också försöka sig på att angripa ett industriellt informations- och styrsystem (där riktiga styrsystem finns bakom). Praktiska övningar genomförs också i form av grupparbeten där en säkerhetsanalys av en fiktiv verksamhet ska genomföras. Om förkunskaperna är väldigt olika mellan deltagarna anpassas arbetet utifrån deltagarnas egna förutsättningar. En ny aktivitet är också alumni-träffar där deltagare från de senaste tre årens kurstillfällen bjudits in. Denna typ av sammankomster stärker också förmågan över tiden och säkerställer ett vidmakthållande av nätverken mellan tekniker. En effekt som kursen har haft, utöver den individuella kunskapshöjningen, är att deltagarna tar med sig kunskap till sina respektive organisationer vilket leder till att stärka hela verksamheten. Nätverkandet mellan tekniker inom en bransch men också mellan branscher är centralt; det är dessa personer som åtgärdar problemen när de uppstår. Den kunskap som de besitter och de möjligheter de har att hjälpa varandra är i slutänden vad som avgörför hur effektivt vi kan hantera en allvarlig händelse mot samhällsviktig verksamhet.

Sista steget i utbildningstrappan består av förmågehöjande aktiviteter. Även om kunskapen finns är det viktigt att praktiskt träna sig i att hantera it-incidenter. Hantering skiljer sig ofta mellan industriella informations- och styrsystem och vanliga administrativa system. I ett industriellt informations- och styrsystem är det viktigt att i möjligaste mån upprätthålla produktionen samtidigt som angreppet analyseras och avstyrs. Hanteringen av angreppet bör också ske på ett sätt som underlättar den efterkommande forensiska analysen. I den förmågehöjande utbildningen används den ”cyberrange” som nämnts tidigare. Den består av cirka 300 ihopkopplade datorer som, men hjälp av virtualisering, kan skapa en närmast oändlig mängd olika tekniska nätverkskonfigurationer. Det tekniska nätverk som används för de förmågehöjande insatserna i dag är t.ex. en replikering av ett produktionssystem, exempelvis en läkemedelsprocess, där övningsdeltagarna ska upprätthålla produktionen samtidigt som systemet angrips.

Tekniska och strategiska studier

En annan viktig del är de studier som tas fram inom ramen för MSB och FOIs samarbete NCS3. Varje år genomförs studier som går ut på att djupanalysera något tematiskt område inom it-säkerhet för industriella informations- och styrsystem. Exempel på studier kan vara hur säkert det är med virtuella nätverk i en processmiljö, eller hur säkert det är att använda vitlistning för att hindra att skadlig kod tar sig vidare ner i styrdatorerna. Studierna har ofta koppling till den omvärldsanalys som bedrivs inom MSB:s program.

Inom olika sektorer sker också särskilda studier för att identifiera hot och risker, många av dessa är på grund av sakens natur dock sekretessbelagda. Inom ramen för Säkerhetspolisens arbete sker också mycket kvalificerade analyser mot de mest skyddsvärda objekten i samhället. Det finns dock ett stort behov av ytterligare studier i och med att utvecklingen som beskrivits ovan sker i en oerhört hög takt.

Nationell och internationell samverkan

Inom ramen för MSB:s arbete med industriella informations- och styrsystem drivs sedan 2004 ett samverkansforum för informationsdelning mellan olika aktörer från det offentliga och privata. Forumet heter FIDI-SC och har 10–12 medlemmar från olika verksamheter som hanterar industriella informations- och styrsystem. Forumet träffas fyra gånger per år och diskuterar under förtroliga former faktiska hot, risker och sårbarheter. Varje möte innehåller också en omvärldsanalys och en gästföreläsare inom relevant område. Utöver den information som utbyts inom forumet skapas viktiga förtroliga kontakter mellan aktörerna som borgar för en ökad medvetenhet om säkerheten i industriella informations- och styrsystem.

En central del i det arbetet som bedrivits av MSB är skriften *Vägledning till ökad säkerhet i industriella informations- och styrsystem*. 2014 gavs den tredje utgåvan av vägledningen ut. Vägledningen har under årens lopp blivit ”de-facto” standard i Sverige. De tidigare utgåvorna har varit översatta till så väl engelska som japanska. Den nya utgåvan kommer också att ges ut på engelska

vilket har varit efterfrågat från internationella organ som bland annat IAEA och ENISA.

Inom ramen för MSB:s breda arbete inom krishanteringsområdet så är olika typer av forskning centralt. MSB finansierar här olika typer av forskning där ett område är en generell utlysning av medel för ett akademiskt forskningsprogram kring säkerhet i industriella informations- och styrsystem. Tanken är att, utöver NCS3, också bilda ett forskningscentrum där mer långsiktig forskning kan bedrivas. Forskningscentrumet ska ha ett nära samarbete med NCS3. En annan viktigt komponent där MSB är drivande är forskning tillsammans med Departement of Homeland Security (DHS). Inom ramen för detta arbetar också FOI med sina motsvarigheter i USA.

7.6.5 Övningar

I samhället är allt fler verksamheter och tjänster sammanlänkande med varandra på någon nivå. Detta beroende medför att en händelse kan få organisationsöverskridande, samhälleliga konsekvenser, som inte initialt förutsetts. För att stärka verksamheters förmåga att hantera uppkomna händelser eller kriser vidtas en mängd åtgärder från medvetandehöjande insatser till åtgärder för att stärka redundansen i system. En central komponent i detta är övningar.

Med övningar ges förmåga att hantera kriser både genom att förbereda individer och organisationer i sin helhet men även för hur organisationer ska samverka med andra aktörer i samhället. I Sverige har händelser som influensan A(H1N1) 2009 belyst behovet av åtgärder för att hantera uppkomna kriser.

I Sverige har MSB uppdraget att samordna, genomföra och stödja regionala, nationella och internationella övningar inom området samhällsskydd och beredskap. Arbetet har sin utgångspunkt i ett uppdrag från regeringen. I budgetpropositionen 2014 gör regeringen bedömning att ”utbildningarna vid MSB, samt myndigheternas övningsverksamhet, internationell utbildnings- och övningsverksamhet, samt det övningsstöd som lämnats av MSB har bidragit till en ökad förmåga att hantera olyckor och kriser nationellt och internationellt”(prop. 2013/14:1 utgiftsområde 6 s. 86).

Informations- och cybersäkerhetsövningar

Behovet av att förbereda sig för att hantera incidenter och kriser återfinns även inom informations- och cybersäkerhetsområdet. Den globala marknaden för informations och kommunikations teknologi (IKT) uppskattas till 2 500 miljarder euro och upphandlingar av IKT-produkt- och tjänster inom EU uppskattas till att motsvara 16 procent av all BNP i EU. Under de senaste åren i Sverige har driftproblem hos leverantörer (Tieto- och Evry-händelserna) visat hur incidenter i informationssystem fått stora konsekvenser för organisationer vilket bl.a. kan påverka samhällsviktig verksamhet.

EU-kommissionen betonar betydelsen av cybersäkerhetsövningar och ser det som strategiskt viktigt för att förbättra skyddet av kritisk informationsinfrastruktur. I European Cyber Security Strategy uppmanas medlemsländerna att delta i övningar på nationell och paneuropeisk nivå. Internationellt finns det flera stora aktörer, såväl länder som mellanstatliga organisationer, som identifierat behovet av cybersäkerhetsövningar och numera anordnas det årligen en mängd sådana. Flertalet strävar efter att utveckla samarbetet mellan incidenthanteringsfunktioner från olika länder, företrädelsevis nationella och militära CERT-liknade organisationer.

Sverige var tidigt med att planera och genomföra cybersäkerhetsövningar. Under 2008 genomförde svenska myndigheter tillsammans med Nato CCD CoE i Estland en teknisk cyberövning (CDX). Samma år genomfördes också SAMÖ2008 vilket utgick från en finansiell kris. Ett viktigt moment i denna övning var störningar i betalningssystemet.

För att utveckla samhällets förmåga att hantera incidenter är det viktigt att öva organisationers eller funktioners förmåga som en helhet och inte endast tekniska experters förmåga att lösa tekniska problem. I Sverige betonas därför vikten av simuleringsövningar och då särskilt tvärsektoriella nationella cybersäkerhetsövningar och tekniska cybersäkerhetsövningar med virtuell övningsmiljö. Med simuleringsövning avses en övningsform där deltagarna övas i sina ordinarie roller, där miljön och uppgiften efterliknar verkligheten i så stor utsträckning som möjligt, och där händelseutvecklingen är baserad på ett övergripande scenario.

Nationella tvärsektoriella övningarna, som övningsserien Nationell informationssäkerhetsövning (NISÖ) syftar till att utveckla samordning och samverkan i samhället och är särskilt viktiga för att nå ut till en bredare krets av kritiska aktörer inom privat och offentlig sektor. De möjliggör att öva koordination, beslutsprocesser och policysamverkan mellan berörda aktörer. NISÖ har genomförts 2010 och 2012. Övningen 2010 genomfördes med centrala myndigheter och de stora energibolagen. Övningen 2012 genomfördes också med centrala myndigheter, energibolagen men också transportsektorn samt ett stort telekombolag. Med på övningen fanns också de nordiska nationella CERT-funktionerna. Denna typ av sektorsövergripande övning kommer att genomföras med regelbundenhet.

För att nå alla nivåer vid hantering av händelser kompletteras tvärsektoriella övningar med tekniska cybersäkerhetsövningar i virtuell övningsmiljö. I dessa hanterar de övade funktionerna tekniska problem i en virtuell miljö som återspeglar verkligheten i form av tekniska infrastrukturer och system. På så vis kan funktionerna öva samverkan med andra aktörer, sina processer och tekniska förmåga för att hantera incidenter samtidigt.

Exempel på genomförda övningar nationellt och internationellt de senaste åren där Sverige deltagit i någon form är:

- Cyber Defence Exercise – Locked Shields (2008, 2010): Övningsserie som anordnas av Nato CCD CoE årligen och där Försvarshögskolan (FHS) deltar i planering och genomförande i övningsledningen. Syftet med övningen är att öva hantering av it-incidenter och skydd av civil kritisk infrastruktur.
- Cyber Storm (2010, 2013): Övningsserie som anordnats av U.S. Department of Homeland Security med deltagande av 15-tal länder där syftet bland annat har varit att öva processer för incidenthantering mellan deltagande länder.
- Cyber Europe (2010, 2012, 2014): Paneuropeisk övningsserie som anordnas av ENISA med syfte att utveckla samarbetet och processer för informationsdelningen mellan utpekade nationella funktioner.
- Nationell informationssäkerhetsövning, NISÖ (2010, 2012): Nationell övningsserie med syfte att stärka samhällets förmåga att hantera it-relaterade kriser.

- Nato Crisis Management Exercise, CMX (2012): Övningsserie som övar den politiska beslutsstrukturen i Nato och deltagande länder. Under 2012 var cybersäkerhet ett av två huvudteman.
- Nato Cyber Coalition Exercise (2011–2014): Övningsserie som anordnas av Nato i syfte att utveckla samarbetet och teknisk incidenthantering.
- Nationell teknisk informationssäkerhetsövning (2013): Svensk teknisk övning i syfte att utveckla deltagande organisationers förmåga såväl som de övade individernas färdigheter att hantera it-incidenter samt att utveckla teknisk operativt samarbete vid it-incidenthantering mellan deltagarna.
- Nordisk nationell CERT-övning (2015): Planerad övning under 2015 med syfte att utveckla den gemensamma incidenthanteringen, inklusive lägesbilder och informationsdelning mellan de nordiska CERT-funktionerna.
- Telö-serien är en övning som hålls vartannat år för aktörer inom sektorn för elektronisk kommunikation. Syftet är att vara en lärande övning avseende samverkan inom sektorn och med andra sektorer och myndigheter under en extraordinär händelse.

7.7 Privat-offentligt

7.7.1 Informationssäkerhetsrådet

Myndigheten för samhällsskydd och beredskap (MSB) har, för att utnyttja samhällets samlade kompentens på informationssäkerhetsområdet, knutit till sig ett informationssäkerhetsråd med bred representation från både offentlig förvaltning och näringslivet. Informationssäkerhetsrådet består av representanter från Polismyndigheten, Post- och telestyrelsen, Säkerhetspolisen, Försvarets radioanstalt, Vattenfall AB, .SE (Stiftelsen för Internetinfrastruktur), Karlstads Universitet, Försvarsmakten, L M Ericsson, Sveriges Riksbank, Västra Götalandsregionen, Försvarshögskolan, Riksgälden, Försvarets materielverk och Scania AB.

Informationssäkerhetsrådet har i uppgift att bistå MSB med:

- information om utvecklingstrender inom området informationssäkerhet, det vill säga skydd av information och säkring av informationssystem.
- synpunkter på inriktning, prioritering och genomförande av MSB:s arbete inom området.
- kvalitetssäkring och trovärdighet till MSB:s arbete genom att vara rätt sammansatt och ha koppling till vitala samhällsfunktioner.
- att bidra till spridning av information om MSB:s arbete med informationssäkerhet i omvärlden.

7.7.2 Ytterligare privat-offentliga samverkansforum inom området

Utöver informationssäkerhetrådet ovan finns ett antal privat-offentliga samverkansforum på nationell nivå och till detta kommer även ett stort antal mer eller mindre formella nätverk. När det gäller privat-offentliga samverkansforum av den typ som nämnts ovan om industriella styrsystem, FIDI-SC, så kan även nämnas MSB:s forum FIDI-Finans som engagerar ett 15 tal aktörer i samhällssektorn finansiella tjänster samt FIDI-Vård och omsorg som både engagerar privata och offentliga aktörer inom sektorn. Här bör även nämnas samverkansforumet NTSG (se avsnitt 7.6.3) som omfattar aktörer inom sektorn elektroniska kommunikationer och som leds av PTS. När det gäller arbetet med att förebygga och hantera it-incidenter är även den nyligen startade nationella samverkan mellan olika CSIRT-funktioner av stor vikt. Gruppen benämns informellt Svenskt CERT-forum och samordnas av MSB.

7.7.3 Standardisering av informations- och it-säkerhet

Standarder kan beskrivas som frivilligt och i samförstånd framtagna gemensamma lösningar på ofta återkommande problem. Standarder formaliserar och överför kunskap avseende säkerhet, prestanda, begrepp och processer. På detta sätt ger standarder ofta en värdefull möjlighet att överföra resultat från forskning och utveckling till praktiskt arbete och vidare till specialisering. Inom offentlig upphandling möjliggör lagarna för den upphandlande myndigheten

och enheten att hänvisa till standarder men hänvisningarna ska följas av ordet ”likvärdiga” för att säkerställa konkurrens på lika villkor.

Standardisering är en privaträttslig verksamhet och är i huvudsak en fråga för näringslivet. Det finns emellertid ett antal formella regler som påverkar förhållandet mellan myndigheterna och standardiseringsverksamheten.

För näringslivet är standardisering och kontroll av att produkter tillverkade enligt harmoniserade standarder på marknaden uppfyller föreskrivna krav (marknadskontroll) nog så angeläget som reducering av antalet regler. Standarder är instrument för samarbete mellan näringsliv och förvaltning samt för förenklad lagstiftning. En modern standard måste ta hänsyn till en lång rad av ibland motstridande aspekter och krav som alla ska vägas in i arbetet. Teknikskiftet är tydligast inom it-området då det sammankopplade och uppkopplade samhället berör snart sagt allting.

Området elektroniska kommunikationer kännetecknas av en snabb teknisk utveckling och en pågående sammansmältning av tekniker och tjänster. Tillgången till och användningen av olika typer av standarder är av utomordentligt stor betydelse inom informationstekniken. Samtidigt är området svåröverskådligt genom förekomsten av ett mycket stort antal standarder för liknande funktioner och ett stort antal organisationer som utformar, föreslår eller fastställer nya eller modifierade standarder.

Certifiering och ackreditering

Certifiering är en bedömning av överensstämmelse och en bekräftelse på att en produkt, process eller tjänst uppfyller kraven i t.ex. en standard. Ackreditering är en formell bekräftelse på kompetens hos certifierings- kontroll- och provningsorgan.

7.8 Den privata sektorn

Stora delar av samhället är beroende av att vara uppkopplat mot internet för att fungera. Elektronisk kommunikation är av den anledningen att anse som en kritisk resurs för samhällets funktion och en förutsättning för att samhällets övriga it-infrastruktur ska

fungera. Detta kräver att ett systematiskt informationssäkerhetsarbete genomförs som beaktar alla former av hot och risker som kan inträffa.

1994 upphävdes det statliga monopolet inom telefoni och marknaden öppnades för privata aktörer. I samband med det bildades Post- och telestyrelsen (PTS) då en öppen marknad krävde att en regulatorisk myndighet bildades. PTS arbetar med regulatoriska och främjande åtgärder gentemot operatörer och nätägare i syfte att tillse att samhället har väl fungerande och tillförlitliga elektroniska kommunikationer. Myndigheten verkar även som en statlig kontaktyta för operatörerna.

Lagen (2003:389) om elektronisk kommunikation (LEK) anger vilken grundläggande nivå av informationssäkerhet som operatörerna är skyldiga att ha för att bedriva verksamhet på marknaden för elektronisk kommunikation. Utöver lagens krav kan operatörernas kunder ställa högre krav på säkerhet mot en högre kostnad i enlighet med marknadens villkor. Dessutom har samhället särskilda säkerhetskrav på vissa delar av den elektroniska kommunikationsinfrastrukturen, exempelvis avseende robusthet och redundans. I dessa fall kan PTS bidra med medel. Dessa ekonomiska satsningar inriktas på att stärka infrastrukturen, så att konsekvenser av allvarliga händelser ska kunna minimeras, vilket stärker samhällets informationssäkerhet.

7.8.1 Teleoperatörer

Operatörernas verksamhet bedrivs på kommersiella grunder på en fri marknad. Reglering av operatörernas verksamhet får av den anledningen inte vara mer ingripande än som framstår som rimligt och proportionella med hänsyn till den fria konkurrensen. För att säkerställa att informationssäkerheten i operatörernas verksamhet når en grundläggande nivå, omfattas de dock av olika regulatoriska och främjande åtgärder inom informationssäkerhetsområdet.

Operatörer har en skyldighet enligt LEK att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på säkerhet. De åtgärder som vidtas ska vara ägnade att skapa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra

åtgärderna, är anpassad till risken för störningar och avbrott. I egenskap av tillsynsmyndighet meddelar PTS föreskrifter och allmänna råd som förtydligar kraven på god funktion och säkerhet. Syftet med kraven är att skapa säkra och effektiva elektroniska kommunikationer för enskilda och myndigheter. Dessutom ska operatörerna bedriva ett kontinuerligt och systematiskt säkerhetsarbete för att uppnå säkrare elektroniska kommunikationer.

Operatörerna är skyldiga enligt 5 kap. 6 b § LEK att upprätthålla en viss nivå av driftsäkerhet. Med driftsäkerhet avses upprätthållande av funktion och tillgänglighet, men även uthållighet vid extraordinära händelser. 2007 utarbetade PTS allmänna råd om god funktion och teknisk säkerhet som förtydligar regleringen i LEK. De utgör rekommendationer om hur driftsäkerhetsarbetet kan bedrivas för att uppfylla kraven som ställs i författningen. Kraven på driftsäkerhet kommer att förtydligas ytterligare i de föreskrifter som PTS arbetar med att ta fram under 2015.

Operatörerna har även ett ansvar för informationssäkerheten avseende integritet och skyddet mot obehörig insyn. Uppgifter som behandlas i samband med tillhandahållandet av tjänster ska skyddas. Bestämmelser om operatörernas skydd för abonnenternas trafikuppgifter finns i 6 kap 3 § LEK och kompletteras av Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter, PTSFS 2014:1. Föreskrifterna innehåller bestämmelser om de tekniska och organisatoriska skyddsåtgärder som den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta.

Enligt 6 kap. 3 a § LEK ska operatörerna i samband med trafikdatalagring vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. Operatörerna är även skyldiga att följa PTS föreskrifter och allmänna råd om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål (PTSFS 2012:4). Föreskrifterna innehåller bestämmelser om de särskilda tekniska och organisatoriska skyddsåtgärder som operatörerna är skyldiga att vidta.

Enligt 1 kap. 8 § LEK samt de föreskrifter som PTS utfärdar avseende beredskap och totalförsvar är operatörerna skyldiga att delta i totalförsvarsplanering och i samband med det, vidta åtgärder i syfte att skapa större informationssäkerhet.

7.8.2 Stiftelsen för internetinfrastruktur (.SE)

Stiftelsen för internetinfrastruktur (.SE) bildades 1997 och är en oberoende allmännyttig organisation som verkar för en positiv utveckling av internet i Sverige. .SE ansvarar för internets svenska toppdomän .se, med registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret. Sedan september 2013 sköter .SE också drift och administration för toppdomänen .nu.

I slutet av 2014 fanns det över 1,3 miljoner registrerade .se-domäner .SE är och ska vara det självklara valet för företag, privatpersoner och organisationer som vill ha ett domännamn med anknytning till Sverige.

När någon registrerar en .se- eller .nu-domän går en del av avgiften som .SE tar ut för domännamnsregistrering till projekt som på olika sätt främjar en positiv utveckling av internet i Sverige. 2013 satsade stiftelsen cirka 78 miljoner kronor på internetutvecklande verksamhet. Den överordnade målsättningen är att alla ska kunna ta tillvara internets möjligheter.

.SE:s internetutvecklingsprojekt har sin grund i stiftelsens urkund och stadgar. Mottot för projekten är *Internet för alla*. I detta ligger att alla människor i vårt land ska ha samma rätt och samma möjligheter att utnyttja internets tjänster. Internet ska också vara säkert, så att användarna känner sig trygga och litar på tjänsterna som finns där. Även internets infrastruktur är i fokus för .SE. Den ska vara säker, stabil och skalbar så att internet blir så användbart som möjligt för alla.

Med det övergripande målet att skapa ett internet för alla blir bredden i de olika projekt som .SE driver stor. Här ryms allt från skoltävlingen Webbstjärnan, bokpublicering, statistik, satsningar på ökad digital delaktighet, konferensen Internetdagarna och seminarier till testverktyg, utveckling av program med öppen källkod, stöd vid införandet av internetprotokollet version 6 (IPv6) samt finansiering av fristående projekt genom Internetfonden.

.SE har sedan 2007 genomfört en undersökning av nåbarhet på nätet och hälsoläget i .se. Syftet med den årliga undersökningen är att kartlägga och analysera kvaliteten och nåbarheten i framför allt domännamnssystemet (DNS) i .se-zonen och några andra viktiga funktioner för domäner registrerade i .se. Genom att undersökningen

har genomförts flera år i rad kan .SE också visa på utveckling och trender inom de undersökta områdena. Undersökningen görs på både ett urval av domäner som representerar viktiga funktioner i samhället och ett slumpmässigt urval motsvarande en procent av samtliga domäner i .se

Internet Corporation for Assigned Names and Numbers, ICANN har utsett .SE att administrera den svenska toppdomänen, .se. .SE:s verksamhet regleras av lagen (2006:24) om nationella toppdomäner för Sverige på internet. PTS är tillsynsansvarig myndighet för .SE, vilket ska garantera en stabil drift av det svenska domännamnssystemet.

7.8.3 Stiftelsen för telematikens utveckling (TU-stiftelsen) och Netnod

Stiftelsen för telematikens utveckling (TU-stiftelsen) bildades 1997 med ändamålet enligt stiftelsens urkund och stadgar att främja forskning, utbildning och undervisning inom data- och telekommunikation särskilt såvitt avser internet. Stiftelsen ska bland annat kunna lämna bidrag till inköp av utrustning, anslag till forskarstipendier och bidrag till studieresor. För tillgodoseende av stiftelsens ändamål får stiftelsen äga dotterbolag.

TU-stiftelsen driver dotterbolaget Netnod i syfte att utgöra en oberoende huvudman för etablering och drift av knutpunkter och andra operatörsgemensamma internetfunktioner.

Netnod driver fem internetknutpunkter, så kallade IXP:er, i Sverige och en i Danmark. Till dessa knutpunkter kan internetoperatörer koppla sig och utbyta trafik med andra (så kallad peering).

Netnod erbjuder också mervärdestjänster som distribution av spårbar svensk tid via NTP (network time protocol). Netnod hanterar även ett antal DNS-tjänster på uppdrag från toppdomänadministratörer över hela världen. Slutligen är Netnod operatör av en av internets logiska rotnamnservrar för DNS (i-roten). Den tjänsten erbjuds allmänheten som en tjänst utan kostnad.

7.8.4 Svenskt Näringsliv

Föreningen Svenskt Näringsliv är företagens företrädare i Sverige. Det långsiktiga målet med verksamheten är att Sverige ska återta en tätposition i den internationella välståndsligan, vilket ska uppnås genom en bred intressegemenskap kring värdet av företagande och företagsamhet. Svenskt Näringslivs uppdrag är att öka förståelsen för företagens verklighet och att verka för att alla företag i Sverige ska ha bästa möjliga villkor för att verka och växa.

Svenskt Näringsliv företräder närmare 60 000 små, medelstora och stora företag med totalt över 1,6 miljoner anställda. Två av tre medlemsföretag har färre än tio medarbetare. Medlemsföretagen är organiserade i 49 bransch- och arbetsgivarförbund. Förbunden utgör föreningen Svenskt Näringslivs medlemmar.

Verksamheten täcker ett brett fält och vänder sig till olika målgrupper. Föreningen arbetar med opinionsbildning och kunskapsspridning, utvecklar nya idéer och tar fram konkreta förslag för att skapa ett bättre klimat för företagsamheten. Medlemsorganisationerna ger medlemsföretag konkret och anpassad service, till exempel rådgivning, omvärldsinformation och utbildning. De arbetar även med att påverka politiker och myndigheter i branschspecifika frågor.

Svenskt Näringsliv och dess medlemsorganisationer arbetar brett med säkerhetsfrågor och riskhantering, bland annat inom området informationssäkerhet, där medlemsorganisationen it-företagen intar en framträdande roll. Samverkan sker med ett flertal andra organisationer, bland andra International Chamber of Commerce, ICC, och SIS, Swedish Standards Institute, samt särskilt med Näringslivets Säkerhetsdelegation (NSD) vars kansli finns hos Svenskt Näringsliv.

Näringslivets Säkerhetsdelegation

Svenskt Näringslivs externa arbete med säkerhet och riskhantering bedrivs huvudsakligen via Näringslivets Säkerhetsdelegation, NSD, som är ett informellt nätverk. NSD är registrerat som varumärke men all verksamhet bedrivs formellt under Svenskt Näringslivs organisationsnummer. NSD har cirka 600 medlemmar från privat och offentlig sektor med tillsammans cirka 900 kontaktpersoner. NSD

finns i sex regioner (södra, västra, östra, Stockholm, Bergslagen och norra) med en arbetsgrupp i varje region.

NSD är ett nätverk för lönsam riskhantering, vilket ska uppnås genom att stimulera det medvetna risktagandet. Verksamheten sker i form av konferenser, utbildningar, erfarenhetsutbyte, rådgivning och opinionsbildning samt utvecklingsprojekt. Verksamheten har under många år haft informationssäkerhet som en prioriterad fråga och bland annat producerat ett flertal rapporter.

8 Internationella utvecklingslinjer, organisationer och dialoger

Detta kapitel inleds med att beskriva de globala cyberfrågorna inom utrikes- och säkerhetspolitik samt Sveriges arbete med dessa frågor. Därefter ges en beskrivning av ett antal internationella forum av betydelse inom informations- och cybersäkerhetsområdet. Det ska betonas att detta inte ska betraktas som en i alla sammanhang heltäckande beskrivning.

8.1 Globala cyberfrågor

Globala cyberfrågor utgör en prioriterad utrikespolitisk fråga och är en viktig del av Sveriges politik på det freds- och säkerhetsfrämjande och folkrättsliga området. Denna politik bygger på grundläggande värderingar som mänskliga rättigheter, demokrati och rättsstatsprinciper. En central utgångspunkt är att folkrätten, inklusive de mänskliga rättigheterna, gäller fullt ut även på internet. Ett viktigt mål är att upprätthålla och stärka ett globalt, tillgängligt, öppet och robust internet som bidrar till en rättvis och hållbar global utveckling och där mänskliga rättigheter respekteras.

Den ökande betoningen på cyberfrågor inom utrikes- och säkerhetspolitiken har växt i takt med den tilltagande digitaliseringen och globaliseringen av samhället. Från att tidigare i större utsträckning ha varit en mer avgränsad och teknisk angelägenhet som bl.a. behandlats ur ett nät- och driftsperspektiv har frågan kommit att utgöra en växande beståndsdel i den internationella politiken, inte minst ur geopolitisk hänsyn. Förekomsten av cyberattacker ökar närmast exponentiellt och allt fler länder skaffar sig förmågor och utvecklar doktriner inom cyberområdet.

I kampen för frihet, demokrati och utveckling är individens tillgång till yttrande- och informationsfriheten ett centralt instrument. Fri och öppen tillgång till internet både stärker demokrati och mänskliga rättigheter samtidigt som det utgör en viktig och växande drivkraft för social och politisk utveckling världen över. Internet öppnar nya kanaler för människor att ta emot och sprida information och kunna uttrycka sina åsikter i en globaliserad värld. Dessa möjligheter har gjort att vissa stater söker begränsa yttrandefriheten genom att t.ex. blockera och filtrera information eller stänga ned internet. De nya möjligheterna till övervakning har lett till omfattande internationella diskussioner om rätten till privatliv. Sverige driver en aktiv utrikespolitik som värnar och främjar ett öppet och säkert internet där mänskliga rättigheter till fullo respekteras. Flerpartssamverkan är en viktig del av att främja respekten för folkrätt och mänskliga rättigheter på internet, och inom detta område samarbetar Utrikesdepartementet (UD) internationellt med civilsamhällesorganisationer, privata företag och forskningsvärlden.

Sverige har varit pådrivande vad gäller normbildande kring internetfrågor, särskilt vad gäller rättighetsfrågor. Sverige var t.ex. en av initiativtagarna till den nydanande resolutionen 20/8 (2012) i FN:s råd för mänskliga rättigheter som bekräftar att samma rättigheter som individer har offline gäller även online, liksom uppföljningsresolutionen 26/13 (2014), som också tar upp frågor om internets styrning och rätten till utbildning. Sverige är en aktiv medlem inom den så kallade Freedom Online Coalition (FOC), som driver frågor rörande mänskliga rättigheter och rättstatsprinciper på internet framåt. Sverige är ordförande för en av FOC:s tre arbetsgrupper, som specifikt driver frågan om hur rättstatsprinciper ska kunna implementeras på internet.

När det gäller internets styrning och förvaltning har UD fått en alltmer aktiv roll i samarbete med Näringsdepartementet. Vissa länder som t.ex. Ryssland, Iran och Saudiarabien driver frågan om en övergång mot en mer statsledd förvaltning av internets resurser i flera multilaterala fora. Dessa stater vill föra över kontrollen över internets tekniska förvaltning till FN-systemet, skapa ett nytt mellanstatligt organ och utveckla rättsliga instrument för internetrelaterade policyfrågor. Många befarar att skapandet av nya internationella ramverk kan komma att undergräva etablerade universella politiska och medborgerliga rättigheter. En sådan utveckling

skulle därmed legitimera ökad censur och övervakning på internet och leda till betänklig inskränkning vad gäller personlig frihet och integritet.

Inför hösten 2015 finns en överhängande risk att frågor rörande utökad mellanstatlig kontroll av internets tekniska funktioner, normer, standarder m.m. åter dyker upp i diskussionerna inom FN. Det är möjligt att den alliansfria gruppen G77 kommer att villkora ett fortsatt mandat för flerpartsforumet Internet Governance Forum mot instiftandet av ett rent mellanstatligt organ, alternativt att låta Internationella teleunionen (ITU) få en framskjuten roll i processerna.

Frågorna kring internets globala styrning har på relativt kort tid gått från att vara en huvudsakligen teknisk angelägenhet till en diplomatisk sådan. Såväl externa faktorer, såsom de senaste årens övervakningsavslöjanden, som den allmänna geopolitiska utvecklingen och strategiska hänsyn har drivit på utvecklingen.

Den grundläggande skillnaden i synen på internet och informationsfrihet, liksom de säkerhetspolitiska och folkrättsliga motsättningarna, manifesteras i en rad olika fora, som t.ex. i FN:s generalförsamlings olika utskott, den statliga expertgruppen inom FN:s ram om ICT-frågor och internationell säkerhet (GGE), Internationella teleunionen (ITU), Unesco, The Economic and Social Council (ECOSOC) m.m. Sverige arbetar aktivt tillsammans med andra likasinnande länder för att hålla emot dessa staters många förslag och initiativ. Denna linje innebär bl.a. att motverka att ett enskilt FN-organ skulle ta ett övergripande policyansvar för internetrelaterade frågor. Svensk hållning är att varje specialiserat FN-organ bör hantera frågorna inom sitt ansvarsområde, oavsett om de är internetrelaterade eller inte. För att förbättra samordningen mellan organisationer och med civilsamhälle stödjer UD att den årliga, öppna flerpartskonferensen Internet Governance Forum, ska fungera som länk mellan olika policyområden.

Frågorna om cyberområdets betydelse för global utveckling och därigenom för biståndspolitiken har också ökat, allteftersom ICT-teknologier har kommit även breda befolkningslager till del och brister i institutionell kapacitet och infrastruktur i allt högre grad framstått som utvecklingshinder i låg- och medelinkomstländer. Sverige har arbetat med ICT-relaterade frågor inom det internationella utvecklingssamarbetet sedan slutet på nittiotalet, då Sida bidrog till att bygga upp ICT-infrastruktur i bl.a. Kenya. Under slutet av 2000-talet

– till stor del som respons på händelseutvecklingen i Mellanöstern – fokuserades insatserna i högre grad på att stödja MR- och demokratiseringsaktörer med verktyg för säker kommunikation i repressiva miljöer. Det arbetet fortsätter nu inom ramen för strategin för särskilda insatser för demokratisering och yttrandefrihet. Frågorna om ICT och internets betydelse för utveckling lyfts särskilt fram i senare års strategi-, styr- och policydokument för biståndet. Frågan har under senare år också breddats till att förutom MR- och demokratiaspekter också omfatta ICT och internets bidrag till ekonomiskt hållbar utveckling. Sida bedriver nu ett omfattande arbete på området. UD bidrar också i samarbete med Sida till den snabbt växande diskussionen om kapacitetsbyggnad på området (cyber capacity building) inom EU och andra multilaterala processer.

En viktigt handelspolitisk målsättning med koppling till cyberområdet är att främja en fri, öppen och konkurrensutsatt marknad för ICT-produkter såväl inom EU som globalt. Frågan om dataöverföringar spelar en allt viktigare roll i internationella handelspolitiska relationer. Flera länder kräver striktare regler för dataöverföringar, och vissa har gått så långt som att diskutera krav på att data måste lagras inom landets gränser. För Sverige är det viktigt att driva på för bättre integritetsskydd och informationssäkerhet som samtidigt tar hänsyn till behovet av att dataöverföringar ska vara så okomplicerade som möjligt. För närvarande diskuteras dataöverföringar inom ramen för TiSA-förhandlingarna (Trade in Services Agreement), och i TTIP-förhandlingarna mellan EU och USA. Möjligheterna till dataöverföringar kan påverkas avsevärt av frågan om nätets framtida styrning.

Det ökande samarbetet inom EU på cyberområdet har lett till framtagandet av en EU-cybersäkerhetsstrategi och etablerandet av den horisontella gruppen Friends of the Presidency Group on Cyber Issues för att kunna hantera övergripande, strategiska cyberfrågor inom EU. UD bereder och samordnar svenska positioner i denna grupp.

Det pågår också samarbeten kring cyberfrågor på ad hoc-basis inom ramen för internationella och regionala samarbetsgrupper. Ett viktigt exempel är det nordisk-baltiska säkerhetspolitiska samarbetet som i stor uträckning har kommit att omfatta cyberfrågor, ofta i samarbete med andra likasinnade partner som t.ex. USA, Storbritannien eller Polen. Sverige har också deltagit inom den så

kallade Londonprocessen, som inneburit en rad återkommande internationella konferenser med syfte att bidra till ökad global samsyn inom cyberområdet. Nästa internationella cyberkonferens i detta format, som är på utrikesministernivå, äger rum våren 2015 i Haag och kommer att hantera ett brett spektrum av frågor: internationell säkerhet, mänskliga rättigheter, kapacitetsbyggnad och governance-frågor.

8.2 Europeiska unionen

Inom EU regleras nät- och informationssäkerhet inom sektorn elektronisk kommunikation främst genom regler i de s.k. ramdirektivet och e-dataskyddsdirektivet. I ramdirektivet regleras teleoperatörers driftsäkerhet och incidentrapportering. I e-dataskyddsdirektivet regleras operatörernas skydd av personuppgifter och s.k. integritetsincidenter. Båda dessa regleringar är införda i svensk rätt genom lagen (2003:389) om elektronisk kommunikation.

8.2.1 ENISA

Europeiska unionens byrå för nät- och informationssäkerhet (European Union Agency for Network and Information Security, ENISA) inrättades 2004 med säte i Heraklion på Kreta, Grekland. Medan byråns ledning och administrationen alltjämt är kvar i Heraklion har den operativa avdelningen flyttat till Aten. Byrån är ett expert- och kompetenscentrum för informationssäkerhetsfrågor och ska öka gemenskapens och medlemsstaternas, och därigenom även näringslivets, förmåga att förebygga, åtgärda och lösa problem som rör nät- och informationssäkerhet.

Byråns arbete bygger på insatser som Europeiska unionens medlemsstater har gjort och insatser som har gjorts på EU-nivå. Byrån ska ge råd till Europaparlamentet och Europeiska kommissionen. Sammanfattningsvis är byråns arbetsuppgifter bl.a. att:

- analysera framväxande risker, framför allt på europeisk nivå,
- bidra till större medvetenhet om nät- och informationssäkerhet,

- förbättra samarbetet mellan och inom till exempel näringslivet, forskare, leverantörer och användare av produkter och tjänster inom informationssäkerhetsområdet,
- möjliggöra samarbete om utveckling av metoder för att förebygga och hantera informationssäkerhetsproblem, och
- att bidra till det internationella samarbetet utanför EU.

ENISA:s nät- och informationsverksamhet bestäms mer i detalj genom årliga arbetsprogram som fastställs av byråns styrelse. Styrelsen består av alla medlemsstater och Europeiska kommissionen. EES-länderna får delta men utan rätt att rösta. För närvarande är den svenske styrelseledamoten även styrelseordförande. Myndigheten leds av en verkställande direktör.

ENISA deltar i många av de initiativ på området som initierats eller leds av kommissionen, som exempelvis EFMS (en informell grupp för medlemsstaternas utbyte av information om nät- och informationssäkerhetsfrågor) och NIS-plattformen (en informell grupp under kommissionen för att få input kring nät- och informationssäkerhet från näringslivet).

I enlighet med Europeiska kommissionens önskemål en översyn av den digitala agendan för Europa i december 2012 har det inom EU tagits fram en ”cybersäkerhetsstrategi” (se avsnitt 8.2.4) och föreslagits ett direktiv på området (se avsnitt 8.2.2 om NIS-direktivet). I genomförandet av denna strategi har det inte identifierats några åtgärder som gäller specifikt sektorn för elektronisk kommunikation. NIS-direktivet föreslås avseende driftssäkerhet och incidentrapportering inte träffa dagens teleoperatörer (vilkas driftssäkerhet och incidentrapportering regleras i annan lagstiftning, se ovan) men däremot andra it-företag.

I den digitala agendan för Europa (DAE) understryks stärkt politik för nät- och informationssäkerhet. Det enda med direkt relevans för sektorn elektronisk kommunikation avsåg moderniseringen av ENISA:s mandat som beslutades 2013.

8.2.2 Direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet inom hela unionen

Det pågår för närvarande förhandlingar inom EU avseende ett direktiv (NIS-direktivet) om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen. Syftet är att uppnå och vidmakthålla en hög gemensam nät- och informationssäkerhet inom hela EU för att förbättra den inre marknadens funktion.

Direktivet ska bl.a. innehålla skyldigheter för alla medlemsstater rörande förebyggande åtgärder och åtgärder för att hantera och svara på allvarliga risker och incidenter som påverkar nätverk och informationssystem. Aktörer som omfattas av direktivet kan vara både myndigheter, kommuner, landsting och enskilda (inom sektorerna transport, vattenförsörjning, hälso- och sjukvård, bank och finans samt informationssamhällets tjänster). Direktivet ska innehålla krav på bestämmelser om sanktioner om operatörerna inte uppfyller sina skyldigheter och en överklagandemöjlighet.

Direktivet ska vidare innehålla krav på en nationell strategi för nät- och informationssäkerhet, att det ska finnas en eller flera nationella myndigheter för nät- och informationssäkerhet, en nationell kontaktpunkt för nät- och informationssäkerhet, nationella incidenthanteringsorgan (CSIRT). Det ska också etableras ett nätverk för samarbete mellan medlemsstaterna, EU-kommissionen och the European Network and Information Security Agency, ENISA samt ett nätverk för de nationella incidenthanteringsorganen, CSIRTs, inklusive CERT-EU. Genom nätverk för behöriga nationella myndigheter ska medlemsstaterna utbyta information och samarbeta på grundval av den europeiska planen för samarbete inom detta område för att bekämpa nät- och informationssäkerhetshot och nät- och informationssäkerhetsincidenter.

Direktivet kommer troligen att beslutas under våren 2015. Utredningen konstaterar att de skyldigheter som direktivet förväntas ålägga medlemsstaterna kan komma att behöva regleras för att Sverige ska kunna genomföra direktivet på ett korrekt sätt.

8.2.3 EU:s digitala agenda och allmän uppgiftsskyddsförordning

EU-kommissionens digitala agenda för Europa (KOM[2010] 245) är ett av huvudinitiativen inom ramen för Europa 2020 – *En strategi för smart och hållbar tillväxt för alla*, (KOM[2010] 2020), kallad Europa 2020-strategin. Strategin lanserades i mars 2010 som ett led i att ta Europa ur den finansiella krisen och förbereda EU:s ekonomi för nästa årtionde. Den beskriver bland annat hur viktig användningen av informations- och kommunikationsteknik är för att Europa ska kunna uppnå de i strategin angivna målen.

Förslag till åtgärder omfattar sju olika områden:

- En pulserande digital inre marknad
- Interoperabilitet och standardisering
- Tillit och säkerhet
- Snabb och ultrasnabb internettillgång
- Forskning och innovation
- Främjande av digital kompetens, digitala färdigheter och digital integration
- Vinster för EU-samhället som möjliggörs av it

8.2.4 Europeisk cybersäkerhetsstrategi

Europeiska kommissionen och utrikestjänsten (EEAS) presenterade den 7 februari 2013 en övergripande europeisk cybersäkerhetsstrategi – *En öppen, säker och trygg cyberrymd*. Strategin berör it-frågor i ett brett perspektiv och presenterar unionens vision och principer för hur dess centrala värderingar och intressen ska komma till uttryck i cyberrymden. Strategin berör både EU-interna som externa aspekter av internetrelaterade frågor i ett brett perspektiv och lyfter fram EU:s vision och principer för hur unionens centrala värderingar och intressen ska tydliggöras och tillvaratas inom cyberområdet. It-säkerhet, it-brottslighet, industri- och handelsrelaterade frågor liksom utrikes-, säkerhets- och försvarspolitiska frågor inom cyberområdet är viktiga delar av strategin.

Implementeringen och uppföljning av strategin och rådslutsatserna samt frågor som berör EU:s internationella cyberpolitik hanteras övergripande i den tillfälliga arbetsgruppen inom rådet, Friends of the Presidency Group on Cyber issues (FoP). Gruppen tillsattes av Coreper (de ständiga representanternas kommitté, Comité des représentants permanents) den 7 november 2012. Syftet med FoP är att förbättra det horisontella arbetet, öka medlemsstaternas insyn och stärka samordningen såväl internt som externt avseende cyberfrågor i vid mening. Gruppen ska utgöra ett strategiskt verktyg för unionens övergripande politiska mål på området. Under hösten 2013 fattades beslut om att utsträcka FoP-gruppens mandat med ytterligare tre år.

Inom FoP verkar Sverige för en övergripande och strategisk inriktning och hantering av cyberfrågorna. Sverige har varit drivande såväl vid tillsättande av gruppen som i diskussionerna om dess fortsatta arbete mot bakgrund av vikten av att bidra till utvecklingen av EU:s cyberpolicy. Detta arbete tar utgångspunkt i grundläggande värderingar som mänskliga rättigheter, demokrati och rättsstatsprincipen. Sverige fortsätter att bidra till policyutvecklingen när det gäller globala cyberfrågor inom EU och verkar aktivt för att utveckla uppföljningsarbetet till EU:s cybersäkerhetsstrategi. Övergripande rådslutsatser på basis av strategin antogs 2013 och under 2014 har olika områden inom strategin följts upp, t.ex. med rådslutsatser om internets förvaltning och förhandlingar om rådslutsatser om EU:s cyberdiplomati.

Ett ramverk för cyberförsvarsfrågor inom den gemensamma säkerhets- och försvarspolitiken (GSFP) har antagits som svar på en begäran från Europeiska rådet i december 2013, vilket också återspeglas i rådslutsatserna allmänt om GSFP från november 2014.

Genomförande och uppföljning av strategin, liksom andra frågor som berör EU:s internationella cyberpolitik, hanteras övergripande inom rådet i vängruppen för cyberfrågor som tillsattes i slutet av år 2012 och vars mandat förlängdes med tre år under hösten 2013. Syftet med gruppen är att förbättra det horisontella arbetet, öka medlemsstaternas insyn och stärka samordningen såväl internt som externt när det gäller cyberfrågor i vid mening. Vängruppen ska vara ett strategiskt verktyg för unionens övergripande politiska mål på området.

Sverige verkar för en övergripande och strategisk inriktning och hantering av cyberfrågorna inom vängruppen. Sverige har varit dri-

vande för att såväl strategin och dess uppföljningsarbete som gruppens fortsatta arbete ska bidra till policyutvecklingen av en global cyber- och internetpolitik för EU, i linje med grundläggande värderingar och politiska prioriteringar som fred, säkerhet, mänskliga rättigheter och utveckling.

8.2.5 Europol

Sedan den 1 januari 2013 finns det ett Europeiskt Cybercrime Center (EC3) vid Europol i Haag. EC3 är knutpunkten för EU:s it-brottsbekämpning och ska bl.a. bidra till kortare reaktionstid vid online-brott. EC3 ska stödja medlemsstaternas myndigheter i uppbyggnaden av operativ och analytisk kompetens för utredning och för samarbete med internationella partner. EC3 har fem huvudfunktioner inom den digitala brottsligheten:

6. Information och stöd: Insamling och bearbetning av information samt funktion som ”helpdesk” för medlemsländerna inom it-brottsbekämpning.
7. Operativt stöd: Stöd till medlemsländerna i det operativa arbetet inom teknik, analys, forensik och samordning.
8. Framtagande av strategier: Hotbedömningar, trendutvecklingar och analyser.
9. Forskning, utveckling och utbildning.
10. Uppsökande verksamhet: Utveckla samarbete med den privata sektorn och andra viktiga funktioner inom området.

EC3 fokuserar på följande kärnområden av it-relaterad brottslighet:

- Organiserad brottslighet som genererar stora brottsvinster, t.ex. internetbedrägerier.
- Brott som orsakar stora skador hos brottsoffret som t.ex. it-relaterade sexualbrott mot barn.
- Brott som påverkar kritisk infrastruktur och informationssystem inom den Europeiska Unionen, t.ex. dataintrång.

Den 1 september 2014 inrättade Europol som ett pilotprojekt en Joint Cybercrime Taskforce (J-CAT) som ska stärka bekämpningen av it-brottslighet inom EU och globalt. Aktionsgruppen ska samordna internationella utredningar i syfte att agera mot de viktigaste hoten och aktörerna. I gruppen ingår både medlemsstaters brottsbekämpande myndigheter, myndigheter utanför EU och EC3. Förutom samordning av operativa insatser kommer aktionsgruppen att samla information från myndigheter och privata partner, analysera och bearbeta den för att kunna rikta in arbetet mot olika mål och nätverk.

8.3 OECD

8.3.1 OECD:s arbete inom områdena informationssäkerhet och integritet

OECD, som grundades 1961, är ett samarbetsorgan för 34 länder och har sitt säte i Paris. Syftet med samarbetet är att bidra till tillväxt, sysselsättning och ökad levnadsstandard i medlemsländerna, att bidra till sund ekonomisk utveckling, både i medlemsländerna och i omvärlden, samt att bidra till expansion av världshandeln. Samarbetet sker på marknadsekonomisk grund.

OECD utgör ett forum för utbyte av idéer och erfarenheter samt analyser av frågor inom ett stort antal politikområden. Ett viktigt syfte är att medlemsländerna ska lära av varandra, diskutera gemensamma problem och aktuella internationella ekonomiska frågor. Insamling av statistik är omfattande, liksom publikationsverksamheten.

OECD har cirka 200 kommittéer och arbetsgrupper. I dessa arbetar medlemsländerna, partnerländer och inbjudna organisationer tillsammans med OECD:s sekretariat med studier, rekommendationer och riktlinjer som stöd till medlemsländernas policyutveckling. Dessa är inte juridiskt bindande, men förutsätts ändå ha en påverkan och efterföljas. Sekretariatet har drygt 2 500 anställda och den årliga budgeten ligger på cirka 350 miljoner euro. Beslut fattas med consensus, dvs. enhälligt.

Verksamheten inom OECD är indelad i olika direktorat, där direktoratet för vetenskap, teknologi och industri (Directorate for Science Technology and Industry) har fyra underkommittéer. Den

ena av dessa arbetar med den digitala ekonomin (Committe on Digital Ecomony Policy, CDEP) som i sin tur har tre arbetsgrupper. Arbetsgruppen för informationssäkerhet och integritet (Working Party on Information Security and Privacy in the Digital Economy – WPSPDE) bildades redan 1992 och är den som närmast hanterar områden av betydels för utredningen.

Arbetsgruppen förvaltar och reviderar löpande ett flertal rekommendationer och riktlinjer som redovisas nedan. Därutöver sker för närvarande arbete med att ta fram indikatorer för att mäta informationssäkerhet, bl.a. via data från CSIRTs, fortsatt arbete med ID-management samt utveckling av ”Privacy Risk Management”. En rapport har färdigställts tillsammans med hälsokommittéen avseende säkerhet och integritet vid återanvändning av hälsodata. Tidigare arbete har bl.a. handlat om analys av medlemsstaters nationella strategier för informationssäkerhet, informationssäkerhetsfrågor avseende ”Internet of Things” och ”Big Data”, framtagande av en rekommendation avseende skydd av barn som är uppkopplade på internet (Protection of Children Online), analyser av nationella strategier avseende informationssäkerhet för kritisk infrastruktur m.m. Artbetsgruppen bedriver också ett omfattande arbete med olika analyser inom dataskyddsområdet (personlig integritet).

8.3.2 OECD:s rekommendationer och riktlinjer – Security Guidelines

1992 utvecklade OECD sina första riktlinjer för att understödja medlemsstaternas arbete inom informationssäkerhetsområdet. Dessa reviderades år 2002 och genomgår för närvarande en ny revision som beräknas bli klar under våren 2015. Den pågående revisionen tar fasta på informationssäkerheten i nätverk och system utifrån ekonomiska och sociala välfärdsaspekter i en öppen, internationell och uppkopplad teknisk miljö.

Internet har blivit en allt viktigare plattform för samhällets funktionalitet. De digitala hoten ökar med mer sofistikerade aktörer. Nya former av ekonomiska och sociala störningar har uppkommit. Ökad digital mobilitet, molntjänster, sociala nätverk, sakernas internet (internet of things) m.m. är nya parametrar för informationssystemen. Ambitionen är att de nya riktlinjerna ska ta dessa

och andra förändringar i beaktande utifrån ett holistiskt synsätt. Utgångspunkt är också ett riskbaserat synsätt då system och nätverk i dag bli med internationella, större och komplexa. Både förebyggande åtgärder och krishanteringsförmåga förutsätts.

Den nya rekommendationen är indelad i tre sektioner: generella principer, operationella principer och om nationella strategier. Till rekommendationen finns också ett förklarande annex.

De generella principerna handlar om att medvetandegöra alla berörda om vilka digitala säkerhetsrisker som de kan utsättas för genom utbildning och därigenom också ge nödvändiga färdigheter för att kunna bedöma och hantera dessa. Alla har ett gemensamt ansvar, utifrån den egna rollen eller verksamheten, beaktat att en viss risknivå är oundviklig utifrån ekonomiska eller sociala målsättningar i en öppen och sammanvävd internationell miljö. Ledningssystem för riskhantering (risk management) bör införas för att få en styrning av säkerhetsarbetet på ett transparent sätt och i enlighet med mänskliga rättigheter och andra fundamentala värden. Global uppkoppling innebär också att alla aktörer behöver samarbeta internationellt och över landsgränser.

De operationella principerna handlar om systematiska risk- och sårbarhetanalyser samt hantering av risker. Riskhanteringen kan resultera i att risken accepteras, reduceras, överförs, undviks eller kombinationer i de olika alternativen. Vidare handlar den andra sektionen om säkerhetsåtgärder, innovation och kontinuitetsplanering.

OECD rekommenderar medlemsstaterna att anta nationella strategier, vilket behandlas i den tredje sektionen. Avsikten är att minska de digitala säkerhetsriskerna på alla nivåer, inom landet och över landsgränser, utan onödiga restriktioner som påverkar det fria dataflöden eller teknikutvecklingen. Andra aspekter är att skydda individer från digitala säkerhetshot (t.ex. dataintrång, identitetsstölder eller bedrägerier), att beakta behovet av nationell säkerhet och suveränitet samt att bevara mänskliga rättigheter och fundamentala värden. Det sägs att strategierna ska riktas mot alla aktörer och vara anpassade för såväl små och medelstora företag som individer. Allas ansvar och agerande utifrån den egna verksamheten och roller ska påtalas. Viktigt är också att stödja utbildning och träning av personal.

Det anges att nationella strategier ska inkludera åtgärder som bör utföras av regeringarna. Exempel på sådana åtgärder anges också. Det handlar bl.a. om framtagande av en holistisk handlingsplan för den offentliga förvaltningen baserade på risk- och sårbarhetsanalyser, bättre koordinering mellan relevanta myndigheter, inrättande av CSIRT, ökade informationssäkerhetskrav i offentliga upphandlingar och anställning av fler säkerhetsexperter, att stimulera FoU, innovation samt utvecklig av öppna standarder.

Behovet av internationellt samarbete och assistans understryks. Deltagande i internationell fora, etablering av bilaterala och multilaterala nätverk för utbyte av erfarenheter och bästa tillämpade teknik är vägar att gå. Internationellt samarbete för att bemöta gränsöverskridande hot och risker kan t.ex. ske via samarbete mellan CSIRT och genom internationell övningsverksamhet.

Skapande av förtroendefullt samarbete mellan aktörer sker inte över en natt då informationen i många fall kan vara känslig eller t.o.m. hemlig och leda till skada om den kommer i orätta händer. Partnerskap och olika samarbeten mellan offentliga och privata aktörer, formella och informella, kan stimuleras med syfte att få till stånd förtroendefulla kunskaps- och erfarenhetsutbyten.

Andra åtgärder som regeringarna kan vidta för att stimulera den digitala säkerheten är stöd till frivilliga märkningsordningar, uppmuntra till certifieringar och rapportering av incidenter. Statistiken på området behöver också utvecklas genom framtagande av nya och internationellt jämförbara indikatorer.

8.3.3 Privacy Guidelines

Skydd av personuppgifter vid dataöverföring och datalagring är ett område som OECD arbetat med över 35 år. De första riktlinjerna beslutades år 1980 med bl.a. Australien och Sverige som pådrivande länder. Vid denna tid inrättades också Datainspektionen.

Olaglig lagring av persondata, bevarande av inaktuella data och utlämnande av känsliga persondata är områden som berörs i riktlinjerna. Persondata behöver emellertid också kunna hanteras på ett rationellt sätt inom viktiga sektorer av ekonomin, inom sjukvården och av myndigheter samt för forskningsändamål. Återanvändning av data är ett annat område. För att undvika skillnader i lagstift-

ningen mellan länder och därigenom bl.a. underlätta för fria dataflöden över landsgränser utvecklades riktlinjerna.

Åtta olika principer togs fram med begränsningar och krav på mängden insamlade persondata, datakvalitet, syftet, användningen, säkerhet, öppenhet kring användningen, individens rättigheter samt om ansvar för datahanteringen. Dessa kvarstår än i dag och har utvecklats ytterligare vid en revidering som slutförts år 2013. Två nya aspekter tillfördes då, dels behovet av att införa ett riskbaserat ledningssystem för skydd av personuppgifter, dels att skapa ökad global interoperabilitet för området genom internationella regelverk. Nya koncept har också introducerats, bl.a. behovet av att utarbeta nationella strategier för hantering av persondata, behovet av ledningsprogram för organisationer och om incidentrapportering vid dataläckage. Organisationers ansvar vid hantering av persondata lyfts särskilt fram.

8.3.4 Recommendation on the Protection of Critical Information Infrastructure (CIIP)

Rekommendationen bygger på studier och analyser utförda 2006–2007 i sju OECD-länder. Området var då under utveckling och visade på skillnader i utveckling av policyer, praktisk riskhantering, uppföljning och hantering av sårbarheter, roller och ansvar m.m. Rekommendationen beskriver olika koncept för skydd av kritiska infrastrukturer och hur dessa definieras i olika länder. Behovet av att även införa nationella handlingsplaner, i enlighet med ovan nämnda ”security guidelines”, rekommenderas. Fokus ligger på hur regeringarna kan demonstrera ett ledarskap och engagemang när det gäller riskhantering i samarbete med den privata sektorn. Informationsspridning på såväl regional som global nivå är exempel på åtgärder som kan initieras.

Under 2014 presenterades förslag till ändringar i CIIP-rekommendationen utifrån vunna erfarenheter från revisionen av “security guideline”. Översynen kommer enligt planeringen att slutföras under 2016.

8.3.5 Guidelines for Cryptography Policy

Kryptografi möjliggör överföring av information på ett skyddat sätt, där möjligheterna att förvanska innehållet försvåras eller omöjliggörs. De flesta OECD-länder har utvecklat och infört policyer och lagstiftningar kring användningen av kryptografi. Olikheter i dessa regelverk kan emellertid skapa hinder vid utveckling av t.ex. nationella och globala nätverk för elektronisk kommunikation och därmed vara handelshindrande. 1996 initierade OECD därför ett projekt kring kryptografi då medlemsstaterna såg behovet av att skapa en bättre harmonisering kring utvecklingen av en effektivare och säker it-infrastruktur. Avsikten var att nå enighet kring viss policy- och regleringsfrågor vid användning av krypton i elektroniska nätverk. Hänvisning finns också till digitala signaturer. Riktlinjerna, med åtta grundläggande principer, har en stor bredd och ger uttryck för medlemsstaternas olika uppfattningar. Dessa finns också i ett bakgrundsdokument. Något behov av att i dagsläget revidera rekommendationen har inte framställts.

8.4 FN:s arbete och internationella initiativ inom cyberområdet

8.4.1 FN:s generalförsamlings första utskott

I FN:s generalförsamlings första utskott som tillägnas nedrustning och internationell säkerhet har cybersäkerhet behandlats utifrån ett internationellt säkerhetspolitiskt perspektiv. Tongivande har bl.a. en rysk utskottresolution varit som sedan 1998 har uppmärksammat utvecklingen av informations- och telekommunikationsteknologier i en internationell säkerhetskontext. Resolutionen tar bl.a. upp frågan med risker och hot i samband med användande av dessa teknologier, liksom möjliga samarbetsåtgärder som skulle kunna vidtas för att hantera denna utveckling, inklusive utvecklandet av normer och förtroendebyggande åtgärder. Resolutionen, som oftast antagits utan omröstning och under tidigare år inte getts så stor uppmärksamhet, har gett mandat till statsexpertgrupper inom området, Group of Governmental Experts (GGE). Sådana grupper har utsetts vid fyra tillfällen, och två gånger har konsensus nåtts kring en rapport om gruppens överläggningar. Särskilt den GGE-

rapport som antogs 2013 har setts som ett viktigt framsteg då den bl.a. konstaterade att internationell rätt, och särskilt FN-stadgan, var applicerbar inom cyberområdet. Den fjärde GGE-gruppen (med utökat deltagarantal till 20 experter) tillsattes förra året och har nyligen påbörjat sitt arbete med syfte att rapportera till UNGA 2015.

Sedan några år tillbaka har hanteringen av dessa frågor i UNGA:s första utskott föranlett ett särskilt svenskt engagemang; Sverige har sedan 2011 tagit initiativ till ett särskilt gemensamt anförande för att förklara vår och andra likasinnades hållning till den ryska resolutionen. En huvudorsak till detta initiativ med ett gemensamt anförande var de utkast till uppförandekod och konvention kring informationssäkerhet som Ryssland tillsammans med Kina, Tadzjikistan och Uzbekistan cirkulerade för några år sedan. Utformningen och innehållet i dessa dokument ansågs inte acceptabelt av flera skäl, inte minst i ett människorätts- och yttrandefrihetsperspektiv.

Samtidigt som de framsteg som den statliga FN-expertgruppen har gjort välkomnas, har det gemensamma anförandet betonat behovet av ett brett säkerhetsperspektiv som lyfter fram mänskliga rättigheter men även flerpartsmodellen för internets styrning. Sverige – för första gången i nationell kapacitet – rapporterade 2014 till FN:s generalsekreterare om vår syn på ICT-relaterade frågor i ett internationellt säkerhetsperspektiv, i enlighet med inbjudan att göra så som framförs i den ryska resolutionen.

8.4.2 FN:s generalförsamlings andra utskott

FN:s generalförsamlings andra utskott behandlar allmänt ekonomiska och sociala frågor, inklusive utvecklingsfrågor. En viktig resolution som lyfter fram vikten av den potential som ICT (Information and Communications Technology) kan innebära för ekonomisk och social utveckling är den så kallade ICT4D-resolutionen i FN:s generalförsamlings andra utskott. Ett högnivåmöte kommer att äga rum inom ramen för de så kallade World Summit on the Information Society (WSIS) som avses hållas under hösten 2015. De omfattande förberedande förhandlingarna inför översynen i ITU och Unesco är avslutade. Den så kallade Commission for Science and Technology for

Development (CSTD) förbereder en syntesrapport som ska delges UNGA inför hösten. Textförhandlingar inför WSIS-toppmötet 2015 påbörjas under våren 2015.

8.4.3 FN:s generalförsamlings tredje utskott

FN:s generalförsamlings tredje utskott ägnas åt människorättsfrågor, inklusive vad gäller fullt åtnjutande av mänskliga rättigheter på internet. En aktuell fråga i detta utskott har berört det brasiliansk-tyska initiativet att introducera en resolution om rätten till privatliv i den digitala eran. Detta genererade en omfattande förhandlingsprocess som även Sverige deltog mycket aktivt i. Resolutionen ombad FN:s högkommissarie för mänskliga rättigheter att ta fram en rapport på området, som nu publicerats och diskuterats i FN:s råd för mänskliga rättigheter.

8.4.4 FN:s råd för mänskliga rättigheter

I FN:s råd för mänskliga rättigheter i Geneve antogs 2012 resolution 20/8 med Sverige som en av initiativtagarna. Resolutionen togs med konsensus och bekräftar – för första gången i sådant sammanhang – att samma rättigheter som finns offline också gäller online. En uppföljningsresolution antogs under 2014, där även frågor rörande rätten till utbildning och styrningsfrågor togs upp.

Högkommissariens rapport om Right to Privacy in the Digital Age diskuterades i en panel i FN:s råd för mänskliga rättigheter i september och presenteras i UNGA:s tredje utskott i oktober. Det är också möjligt att frågan om en ny specialrapportör för rätten till privatliv kommer att avhandlas under vårens sessioner i FN:s råd för mänskliga rättigheter. Debatten kan förväntas beröra ställningstaganden kring bl.a. extraterritoriell tillämpning av mänskliga rättigheter och rapportens kritik mot användandet av hemliga domslut i underrättelsedomstolar.

8.4.5 World Summit on the Information Society

I FN-kontexten har en viktig konfliktyta funnits kring den så kallade WSIS-processen (World Summit on the Information Society) – en i grunden utvecklingsfokuserad process som påbörjades genom två toppmöten i Geneve 2003 och Tunis 2005, där Sverige deltog med en 40-mannadelegation. Den ursprungliga bärande idén, att förbättra FN:s arbete för att bättre tillgång till ICT i låg- och medelinkomstländer, hamnade snart i skymundan till förmån för skarpa motsättningar kring huruvida kontrollen över internets centrala tekniska resurser, standarder m.m. skulle styras i en flerpartsmodell eller genom instiftandet av nya FN-organ.

En kompromisslösning, som inbegrep skapandet av en öppen, global mötesplats i FN:s regi – Internet Governance Forum – samt ett löfte om att de närmaste tio åren etablera ”enhanced cooperation”, en formulering utan tydlig definition, gjorde att den så kallade Tunisagendan kunde antas.

Tio år efter toppmötet i Tunis har en utvärderingsprocess – där Internationella teleunionen och Unesco spelat framträdande roller – precis avslutats. Sverige har varit mycket aktiv i båda processerna. Ett högnivåmöte inom ramen för WSIS-processen kommer att hållas hösten 2015. Textförhandlingar kring ett slutsatsdokument kommer inledas under senvåren 2015.

8.4.6 Working Group on Enhanced Cooperation, Commission on Science and Technology for Development (CSTD) inom ECOSOC

Sverige var ett av ett fåtal EU-länder som under 2013–2014 deltog i förhandlingarna i den arbetsgrupp inom Commission on Science and Technology for Development (CSTD), en kommitté under ECOSOC, som uppdrogs av FN:s generalförsamling att hitta en väg ur de låsningar i synen på mellanstatligt samarbete på internetområdet som var resultatet av WSIS-toppmötet i Tunis. Motsättningarna i arbetsgruppen var dock alltför stora och förhandlingarna resulterade inte i några gemensamma rekommendationer av substansvärde. Konflikten som gruppen sattes att lösa kvarstår därmed och kommer sannolikt att åter komma i fokus under WSIS-högnivåmötet hösten 2015.

8.4.7 Internationella teleunionen (ITU)

FN-organet den Internationella teleunionen (ITU) hanterar vissa frågor relaterade till cybersäkerhet. Den verkställande delen av ITU är IMPACT (International Multilateral Partnership Against Cyber Threats), vilket även är den första internationella alliansen mot digitala hot. IMPACT ger ITU:s 193 medlemsstater tillgång till expertis, utrustning och resurser för att effektivisera hanteringen av cyberhot samt att bistå för att skydda infrastrukturen hos samtliga FN organ.

ITU:s senaste fullmaktskonferens hölls mellan den 20 oktober och den 7 november 2014 i Busan, Sydkorea.

8.4.8 NETmundialkonferensen i Brasilien

Under april 2014 tog Brasilien ett fristående initiativ genom att bjuda in till det s.k. NETmundial-mötet i Sao Paulo. Mötet arrangerades som en direkt konsekvens av de avslöjandena om massövervakning som framkomit under året, men kom till slut att i mycket begränsad utsträckning hantera övervakningsfrågorna. Deltagandet var brett och förhandlingarna öppna och inkluderande. Sverige betonar gärna utfallet från detta initiativ, snarare än den nu alltför politiserade WSIS-processen, som normgivande för det bredare internet governance-området.

8.4.9 Londonprocessen

Den så kallade Londonprocessen har informellt fått beteckna de internationella cyberkonferenser som tog sin början genom ett brittiskt initiativ. I London anordnades 2011 en konferens med Storbritanniens dåvarande utrikesminister William Hague för att diskutera normer inom ramen för cybersäkerhetsfrågor, med förhoppningen om att öka samstämmigheten inom dessa frågor i den internationella debatten. Diskussionerna fortsatte i Budapest 2012 och i Seoul 2013, där 87 länder deltog. Denna konferenskedja går närmast vidare med ”Global Conference on Cyberspace” i Haag i april 2015. Samtliga konferenser har berört aspekter angående ekonomiska möjligheter på internet, kapacitet främjande, cyberbrott

och internationell säkerhet. Haagkonferensen kommer därtill behandla frågor rörande internets globala styrning.

8.4.10 Freedom Online Coalition (FOC)

Freedom Online Coalition (FOC) är en koalition av 23 länder som grundades 2011. Initiativet till koalitionen togs av Nederländerna och Sverige ingick i den första kretsen av 14 medlemmar. Koalitionens ursprungliga mål var att samarbeta mot övergrepp av de mänskliga rättigheterna på internet och i internationella fora samt att stötta bloggare och andra i repressiva miljöer och att stärka dialogen med it-branschen om företagens ansvar för att respektera yttrandefrihet på internet. Vid grundandet antogs en handlingsplan och en gemensam fond för skyndsamma insatser till stöd för utsatta MR-aktivister och bloggare etablerades. Fonden (Digital Defenders Partnership) har sedan detta blivit operativ och mottar stöd från bl.a. Sida.

Samarbetet inom FOC har under bara ett fåtal år fördjupats avsevärt. Koalitionen har ett gemensamt sekretariat som för närvarande finansieras av Nederländerna och USA och som effektivt driver arbetet framåt. De i alliansen ingående länderna samordnar positioner inför möten i multilaterala forum, bereder gemensamma inlagor till internationella organisationer och gör gemensamma uttalanden. Tre arbetsgrupper har etablerats inom FOC. Dessa ska i samarbete med näringslivet, akademi och civilsamhälle, upprätthålla och föra diskussionerna framåt mellan ministerkonferenserna. Sverige har nyligen påbörjat arbetet kring en arbetsgrupp om rule of law- och utvecklingsfrågor. Sverige deltar också i en arbetsgrupp om ”Privacy and transparency online” som leds av Storbritannien. Arbetsgrupperna förväntas öka i betydelse allteftersom förväntningarna och intresset från näringsliv och civilsamhället tilltar.

Ett stort antal informella samordningsmöten har hållits inom FOC:s ram, inom bland annat OSSE, Unesco, UNGA, ITU m.m. Likaså arrangeras varje år, under den årliga flerpartskonferensen Internet Governance Forum, en öppen diskussionspanel samt särskilda möten med företrädare för civilsamhället och MR-försvarare. Ordförandeskapet i koalitionen roterar och tas över av det land som arrangerar påföljande konferens. Således är Estland för när-

varande ordförande fram till det att Mongoliet tar över under våren 2015.

Förutom den grundande konferensen i Haag 2011 har tre FOC-konferenser genomförts på ministernivå – i Nairobi 2012, Tunis 2013 samt i Tallinn 2014. Nästa ministerkonferens kommer att hållas i Ulan Bator, Mongoliet under 2015.

8.5 OSSE

Den 3 december 2013 beslutade medlemsstaterna i Organisationen för säkerhet och samarbete i Europa (OSSE) att anta en första uppsättning av förtroendeskapande åtgärder (”Confidence-building measures” – CBMs) inom cybersäkerhetsområdet. Åtgärderna syftar till att främja samarbete, transparens, förutsägbarhet och stabilitet och således minska risken för missförstånd, eskalering eller konflikter i cyberrymden. I beslutet betonas att implementeringen av åtgärderna ska vara i linje med internationell rätt (särskilt FN-stadgan, den Internationella konventionen om medborgerliga och politiska rättigheter och Helsingforsslutakten).

Enligt de överenskomna förtroendeskapande åtgärderna åtar sig de deltagande staterna att frivilligt deklarera aspekter av nationella och transnationella hot angående information- och kommunikationsteknologi. Staterna kan även, på en frivillig basis, bistå med konsultationer för att minska riskerna för missförstånd och politisk spänning. För att ytterligare reducera missförstånd i brist på en gemensam syn på terminologifrågor har stater möjlighet att tillkännage nationellt definierade termer relaterade till cybersäkerhet.

EU har tillsammans med USA varit drivande i arbetet som syftar till att skapa förtroendebyggande åtgärder för cybersäkerhet inom OSSE. Sverige har särskilt värnat en tvärdimensionell ansats för att säkerställa att såväl människorätts- som säkerhetsaspekter bejakas. För svenskt vidkommande har det således varit angeläget att åtaganden inom den så kallade mänskliga dimensionen (som en av tre huvudinriktningar av OSSE:s arbete) har en framskjuten plats i arbetet. Vidare avses att redan beslutade förtroendebyggande åtgärder ska implementeras och utvecklas, samt att nya åtgärder bör främjas. Ett normativt ramverk för statsagerande anses kunna främja global utveckling inom området.

8.6 Europarådet

Europarådet arbetar med sina 47 medlemsländer, den privata sektorn, civilsamhället och andra aktörer för att forma ett internet som baseras på mänskliga rättigheter, en pluralistisk demokrati och rättsstatsprincipen. Den övergripande målsättningen är att bidra till en säker och öppen internetmiljö där yttrandefrihet, mötesfrihet, mångfald, kultur, utbildning och kunskap kan blomstra.

Europarådets verksamhet omfattat konventioner inom områden som it-brottslighet, dataskydd och skydd för barn, via utveckling av rekommendationer till medlemsländerna och av riktlinjer för internetaktörer inom den privata sektorn.

Organisationen är aktiv i olika internationella internetrelaterade forum, inklusive det FN-ledda forumet Internet Governance Forum (IGF), den europeiska dialogen om Internetstyrningsfrågor (EuroDIG) och är observatör till den mellanstatliga rådgivande kommittén (GAC) till ICANN (Internet Corporation för Assigned Names och Numbers).

Den 23 november 2001 antogs Europarådets konvention om it-relaterad brottslighet, också känd under namnet Budapestkonventionen. Detta är första internationella konvention som berör brott som begås över internet och utgör fortfarande det enda bindande rättsinstrumentet vars övergripande mål är att skydda och främja frihet, säkerhet och mänskliga rättigheter på internet. Konventionens syfte är primärt att skapa en gemensam straffrättslig policy för skyddet av samhället mot cyberbrottslighet. Konventionen trädde i kraft den 1 juli 2004. Majoriteten av EU:s medlemsländer har ratificerat konventionen. Även stater som inte är medlemmar i Europarådet kan ansluta sig till konventionen, bland annat har den undertecknats av USA, Kanada, Japan och Sydafrika. Sverige undertecknade konventionen samma dag den öppnades för signering. Frågor om kriminalisering av gärningar av rasistisk och främlingsfientlig natur som begåtts med hjälp av datorsystem behandlas i ett tilläggsprotokoll till konventionen – vilket tillkom den 28 januari 2003. Sverige undertecknade protokollet samma dag. Det trädde i kraft den 1 mars 2006. Beredning för att förbereda en svensk ratificering av konventionen och dess tilläggsprotokoll pågår.

I mars 2012 antog Europarådet en ny strategi för internetstyrning; (Council of Europe Strategy 2012–2015 on Internet Gover-

nance). Strategin avser att identifiera prioriteringar och målsättningar för perioden 2012–2015, med syftet att utveckla och skydda respekten för mänskliga rättigheter, rättsstaten samt demokrati på nätet.

I april 2014 lanserade Europarådet en guide för nätfrihet – ”Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users” – avsedd att informera internetanvändare om deras rättigheter på internet samt vad de kan göra om rättigheterna inskränks. Guiden anger att medlemsstaterna i Europarådet har skyldighet att säkra mänskliga rättigheter i enlighet med Europakonventionen även på internet. Dokumentet anger även att andra instrument som reglerar frågor angående yttrandefrihet på nätet, rättighet till information, skydd av privatliv samt skydd från cyberbrott är tillämpliga online.

8.7 Nato

Natos strategiska koncept som antogs vid toppmötet i Lissabon 2010 betonar vikten av att Nato utvecklar sin förmåga på cyberförsvarsområdet. Cyberförsvar ingår som del av Natos kärnuppgift kollektivt försvar, vilket bekräftades av deklarationen från toppmötet i Wales 2014. Nato beslutar i varje enskilt fall om ett cyberangrepp mot en medlemsstat ska utlösa de ömsesidiga försvarsförpliktelserna i Artikel 5 i Natofördraget.

Ett av initiativen under senare tid för att öka förståelsen och kunskapen om hotbilder inom cybersäkerhetområdet är det Natoackrediterade cyberförsvarscentret NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE), vilket har upprättats i Tallinn, Estland. År 2013 presenterade en expertgrupp knutna till centret olika perspektiv på hur folkrättsliga normer kan appliceras inom cyberområdet. Arbetet har sammanställts i en rapport – ”Manual on the International Law Applicable to Cyber Warfare” – även känt som Tallinnmanualen. Detta dokument är inte bindande utan ger endast uttryck för ett antal experters syn. Manualen uppmärksammar internationell lag som reglerar genomförandet av väpnade konflikter.

Försvarsmakten samverkar med Nato inom ramen för planerings- och utvärderingsprocessen PARP i syfte att utveckla sam-

arbetet på cyberförsvarsområdet vad avser internationell militär krishantering.

I Försvarsdepartementets rapport ”Raminstruktion för det civila krisberedskapsarbetet inom NATO (EAPR/PFF)” framgår att Sverige ska vara ett drivande partnerland samt att cyberförsvar är ett prioriterat område. Sverige ska utnyttja möjligheterna till erfarenhetsutbyte och deltar således också i övningar på området.

8.8 Interpol

Den 30 september 2014 invigdes Interpol Global Complex for Innovation (IGCI) i Singapore som kan beskrivas som ett forsknings- och utvecklingscentrum. Inom IGCI inryms Interpols Digital Crime Centre som har till uppdrag att öka informationssäkerhet och motverka it-relaterade brott. I centret inryms ett kriminaltekniskt laboratorium för att stödja utredningar rörande digitala brott. Det bedrivs forskning- och utvecklingsverksamhet som syftar till att testa protokoll, verktyg och tjänster samt till att utveckla praktiska lösningar i samarbete med polisen, forskningslaboratorier, universitet, offentlig och privat sektor. Centret anlyserar också trender rörande it-attacker.

IGCI:s tre viktigaste initiativ i förhållande till medlemsstaterna fokuserar på harmonisering, kapacitetsuppbyggnad samt operativt och kriminaltekniskt stöd.

- Harmonisering: jämförande granskningar av nationell lagstiftning, strategiutveckling rörande informationssäkerhet och rådgivning till enskilda medlemsstater rörande nationella strategier.
- Kapacitetsuppbyggnad: brett utbud av utbildningar rörande nya trender inom it-brottslighet, utredningsteknik, digital kriminalteknik, m.m. Särskilt fokus på training-the-trainers.
- Operativt och kriminaltekniskt stöd: Stöd till nationella utredningar och samordning av internationella insatser. Regional samordning i arbetsgrupper för Afrika, Amerika, Europa och Asien samt Mellanöstern och Nordafrika. Arbetsgrupper har skapats för att underlätta utvecklingen av regionala strategier, teknik och delning av information om de senaste brottstrenderna.

9 Överväganden och förslag

9.1 En nationell strategi för statens informations- och cybersäkerhet

Förslag: Regeringen antar en strategi som tar sikte på att stärka informations- och cybersäkerheten i staten.

9.1.1 Inledning

Utredningen har i avsnitt 4.4 pekat på att sårbarheterna som uppstår i dagens globala it-system är, och kommer inom överskådlig framtid att vara en av våra mest komplexa frågor att hantera. De hot som finns mot informations- och cybersäkerheten och Sverige som nation kräver både sektorsövergripande och internationellt samarbete. Sveriges strategiska samarbetspartners uppfattar problemet på liknande sätt och satsar på att öka sitt internationella samarbete.

Sverige måste i ljuset av detta perspektiv fortsätta att bygga sin nationella kapacitet och stärka skyddet av såväl kritisk infrastruktur som hela den statliga förvaltningen för att därmed kunna hantera och avvärja hot mot statliga informationstillgångar.

Endast med detta tillvägagångssätt kommer Sverige över tid att kunna säkra de många fördelar det digitala samhället erbjuder individen, staten och näringslivet i form av ekonomisk tillväxt, innovation och nationell säkerhet

9.1.2 Bakgrund

I propositionen. 2001/02:158 s. 103 gjorde regeringen följande bedömning i fråga om en strategi för informationssäkerhet i samhället och skydd av samhällsviktiga it-beroende system.

> Målet bör vara att upprätthålla en hög informationssäkerhet i hela samhället som innebär att man skall kunna förhindra eller hantera störningar i samhällsviktig verksamhet. Strategin för att uppnå detta mål bör liksom övrig krishantering i samhället utgå från ansvarsprincipen, likhetsprincipen och närhetsprincipen. Principiellt gäller att den som ansvarar för informationsbehandlingssystem även ansvarar för att systemet har den säkerhet som krävs för att systemet skall fungera tillfredsställande. En viktig roll för staten är därför att se till hela samhällets behov av informationssäkerhet och vidta de åtgärder som rimligen inte kan åvila den enskilda systemägaren. För att förhindra allvarliga informationsattacker mot Sverige bör underrättelse- och säkerhetstjänsternas arbete förstärkas.

I betänkandet *Säker information Förslag till informationssäkerhetspolitik* (SOU 2005:42 s. 56 f.) sammanfattade InfoSäkutredningen de överordnade målen för informationssäkerheten, utifrån ett verksamhetsorienterat perspektiv:

- Infrastruktur: Samhällets infrastruktur för informationstjänster ska vara robust och säker i förhållande till de funktioner den utför. Kritiska informationssystem ska vara så säkra att en skada inte får större verkningar än som kan anses acceptabla.
- Verksamhet: Det ska byggas en säkerhetskultur runt användandet och utvecklingen av IT i Sverige. Informationssäkerhet ska vara en central faktor vid användandet av IT i Sverige.
- Medborgare: Sverige ska ha en allmänt tillgänglig samhällsinfrastruktur för elektroniska signaturer, autentisering av avsändare av elektronisk information samt säker överföring av känslig information.
- Styrning: Regelverk som berör informationssäkerhet ska tillhandahållas och vidareutvecklas på ett samordnat och för användarna enkelt och översiktligt sätt.
- Utbildning: Det ska finnas möjligheter till utbildning inom informationssäkerhetsområdet för alla målgrupper.

– Agerande: Den informationssäkerhet som byggs upp ska stödjas av möjligheter till ingripande vid hot, incidenter, angrepp eller IT-relaterad brottslighet.

InfoSäkutredningen föreslog en strategi som innefattade att:

11. utveckla Sveriges position inom EU och i internationella sammanhang
12. skapa förtroende, trygghet, säkerhet, och öka integritetsskyddet
13. främja ökad användning av IT
14. förebygga och kunna hantera störningar i informations- och kommunikationssystem
15. förstärka underrättelse- och säkerhetstjänstens arbete samt utveckla delgivningen
16. förstärka förmågan inom området nationell säkerhet
17. utnyttja samhällets samlade kapacitet
18. fokusera på samhällsviktig verksamhet
19. öka medvetenheten om säkerhetsrisker och möjligheter till skydd
20. säkerställa kompetensförsörjningen

I dåvarande Krisberedskapsmyndighetens regleringsbrev för budgetåret 2007 gav regeringen myndigheten i uppdrag att ta fram en nationell handlingsplan för samhällets informationssäkerhet (Fö2009/2566/SSK). Handlingsplanen redovisades till regeringen i april 2008. Enligt handlingsplanens tredje åtgärdsförslag skulle den nationella strategin som hade redovisats av InfoSäkutredningens delbetänkande uppdateras.

I regeringens skrivelse *Samhällets krisberedskap – stärkt samverkan för ökad säkerhet* (skr. 2009/10:124 s. 65 ff.) behandlades informationssäkerhet särskilt och sex olika områden togs upp nämligen en nationell strategi för samhällets informationssäkerhet, samhällets samlade förmåga att förebygga och hantera it-incidenter, it-incidentrapportering och it-säkerhetsanalyser, rapportering avseende hot, sårbarheter och risker samt internationell samverkan kring informationssäkerhet. När det gällde den första punkten om

en nationell strategi angavs att det behövdes en tydlig strategi med bred förankring i samhället för att kunna bedriva ett strategiskt och sammanhållet informationssäkerhetsarbete på nationell nivå i Sverige. Regeringen tillade följande.

> Strategin bör ange långsiktiga målsättningar och arbetssätt för informationssäkerhet i Sverige och omfatta informationssäkerhet i verksamheter, kompetensförsörjning, informationsdelning, samverkan och respons, kommunikationssäkerhet, samt säkerhet i produkter och system där nyckelorden är helhetssyn, ansvar och samverkan. Strategin bör omfatta hela samhället, dvs. alla statliga myndigheter, kommuner, landsting, företag, organisationer och privatpersoner. Målen för samhällets informationssäkerhet, som förväntas uppnås genom strategin, är följande:
> - Säkra samhällets funktionalitet, effektivitet och kvalitet.
> - Bidra till samhällets brottsbekämpning.
> - Stärka samhällets förmåga att förebygga och hantera allvarliga störningar och kriser.
> - Främja näringslivets tillväxt.
> - Värna medborgares fri- och rättigheter och personliga integritet.
> - Öka medborgares och verksamheters kunskap om och förtroende för informationshantering och IT-system.

Utredningen menar att den av regeringen tidigare redovisade strategin (prop. 2001/02:158) liksom den i betänkandet SOU 2005:42 föreslagna i grunden var riktiga. Utredningen anser dock att de båda har sökt åtgärda samtliga problem och utmaningar i hela samhället i ett sammanhang, något som ställer genomföranden inför överväldigande utmaningar.

9.1.3 Behovet av en strategi

I utredningens uppdrag ingår att föreslå en strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system, en nationell strategi som utredningen bedömer bör antas av regeringen. Det finns anledning att från utredningens sida betona att behoven på informations- och cybersäkerhetsområdet är så omfattande i Sverige, att det ter sig mest förnuftigt att redan från början acceptera att Sverige inte behöver en, utan flera strategier. Tidigare utredningar på området har i full enlighet med sina uppdrag sökt föreslå allomfattande strategier för hela samhället, vilket har fördelen att inte utelämna någon del av samhället; nack-

delen är att de inte beaktar de svårigheter och utmaningar som kan föreligga med att inom ett begränsat område av samhället åstadkomma normering och styrning utan kännedom om ekonomiska och andra förutsättningar som kan föreligga. Vad som föreslås nedan är endast det första steget, en första strategi som endast söker åtgärda de mest angelägna bristerna i statsförvaltningen. Den här föreslagna strategin träffar statsförvaltningen på bredden och höjer, om den genomförs, den generella informations- och cybersäkerheten i statsförvaltningen, till gagn för samhällets resurser för att förebygga och bekämpa de yttersta hoten mot rikets säkerhet, vilka följaktligen mer odelat kan inriktas mot dessa hot.

Utredningen anser i stället att staten, för att kunna bli en effektiv och trovärdig ledande och kravställande kraft i samhället, måste ägna sin kraft åt att skapa säkerhet inom den statliga sfären. Den strategi som här föreslås ägnas därför uteslutande åt att åstadkomma det. Först därefter är staten i en position där den kan engagera hela samhället.

En höjd informations- och cybersäkerhet måste bygga på att regeringen i en första strategi lyckas skapa en grundstruktur för att sedan kunna fånga in frågeställningar som kan omfattas av flertalet aktörer och intressenter.

Mot bakgrund av detta resonemang föreslår utredningen en strategi som uppställer sex mål för staten under regeringens ledning:

1. Staten förstärker styrning och tillsyn av informationssäkerheten i staten.
2. Staten blir en tydlig kravställare.
3. Staten kommunicerar säkert.
4. De statliga myndigheterna ska rapportera it-incidenter.
5. Statens förebyggande och bekämpande av it-relaterad brottslighet stärks.
6. Sverige ska vara och uppfattas som en stark internationell partner.

9.1.4 Strategins innehåll

Enligt utredningen bör en strategi för statens informations- och cybersäkerhet ha ett medellångt perspektiv som kan ligga till grund för åtgärder på två till tre års sikt. Strategin vänder sig först och främst till regeringen, Regeringskansliet och till de statliga myndigheterna. Indirekt kan strategin även påverka den del av näringslivet och de organisationer som samverkar eller ingår affärsrelationer med staten. I det följande redovisar utredningen några utgångspunkter som bör kunna ligga till grund för det fortsatta arbetet.

Strategin inriktas för att kunna ligga till grund för politiska beslut och prioriteringar inom informationssäkerhetsområdet, och förbättra samordningen av samhällets informationssäkerhetsarbete. Om den genomförs bidrar strategin till att reducera sårbarheten och uppnå en effektiv risknivå i statens olika informationssystem och till trygg elektronisk kommunikation i offentlig sektor, samt säkrar pålitliga nättjänster från offentlig sektor.

Strategin innehåller sex målsättningar, till vilka de olika förslagen i kapitlets senare delar bidrar.

Det första målet är förstärkt styrning och tillsyn av informationssäkerheten i staten. Bland åtgärderna finns krav för alla myndigheter att driva ett ledningssystem för informationssäkerhet, vilket måste uppfylla internationellt erkända säkerhetsstandarder. Arbetet med informationssäkerhet professionaliseras och tillsynen över de statliga myndigheterna stärks.

Det andra målet är att staten blir en tydlig kravställare som upphandlare av tjänster som innehåller informationshantering eller av it-tjänster. Statliga myndigheter ska arbeta mer systematiskt med att ställa konkreta it-säkerhetsmässiga krav i anslutning till upphandling och avtal på it-området. Dessutom ska det ske löpande uppföljning på den säkerhetsmässiga leverantörstyrningen i staten. Dialogen mellan privata och offentliga aktörer samt relevanta utbildnings- och forskningsinstitutioner på området fördjupas.

Det tredje målet är tillgång till säker kommunikation i staten. Information som kommuniceras i staten är skyddsvärd och vital för att statsförvaltningen ska kunna fungera. I orostider ökar detta skyddsbehov, varför lägstanivån måste säkerställas dessförinnan.

Informationen omfattas bl.a. av tryckfrihetsförordningen, offentlighets- och sekretesslagen (2009:400) och arkivlagen (1990:782) varför medborgarna har rätt att förvänta sig att staten har full kontroll över informationens säkerhet och inte sparat någon möda för att omsätta statens skyldigheter i praktisk handling.

Det fjärde målet är att alla statliga myndigheter ska rapportera it-incidenter för att skapa kunskap och lägesbeskrivningar. I målet ingår också att konkretisera samordningsansvaret för att hantera allvarliga it-incidenter. Detta kan ses som ett delmål till det tredje målet, men är dessutom ett av kraven som EU kommer att ställa på samtliga medlemsstater.

Det femte målet är att stärka förebyggande och bekämpande av it-relaterad brottslighet. Denna verksamhet ställer särskilda krav på ansvariga myndigheter för att upprätthålla samma nivå av skydd för individer som i samhället i stort. De verktyg som ställs till ansvariga myndigheters förfogande måste hålla jämna steg med den tekniska utvecklingen och balanseras mot skyddet av den enskildes integritet.

Det sjätte målet är att Sverige ska vara och uppfattas som en stark internationell partner. I detta mål ingår att regeringen stärker och samordnar insatserna för att främja Sveriges ställning i internationellt samarbete om cybersäkerhet.

Senare strategier bör omfatta bl.a. kompetensförsörjningen avseende informationssäkerhet i samhället i stort, nationell forskning och utveckling om informations- och cybersäkerhet, informationssäkerhet inom verksamheter hos landsting och kommuner, liksom försvaret av riket och dess oberoende mot antagonistiska hot med såväl defensiva som offensiva förmågor.

De åtgärder som utredningsdirektivens andra delar har lett utredningen att föreslå kan, på sätt som visas i bilaga 5, hänföras till de olika strategiska målen.

9.1.5 Strategigenomförande och handlingsplan

Förslag:
1. Inrättandet av en genomförandekommitté övervägs.
2. MSB ges i uppdrag att i samverkan med ett nybildat myndighetsråd ta fram en ny handlingsplan.

Flera tidigare utredningars resultat (se exempelvis SOU 2005:42) har endast i begränsad omfattning kommit att genomföras. Då ingen studie har gjorts över skälen till att förslagen inte kommit att realiseras ligger det nära till hands att anta att det hänger samman med dels kostnaderna för vissa av de föreslagna åtgärderna, dels den omfattande krets av myndigheter med olika intressen och roller som är involverade, tillsammans med de departement som ansvarar för styrningen och dess myndigheter. Med förstärkningen av säkerhetsfrågornas hantering inom regeringen som statsministerns inrättande av ett säkerhetspolitiskt råd innebär och den kraftsamling som mandatet för inrikesministern möjliggör, föreligger i dag bättre förutsättningar än tidigare att förmå den centrala statsförvaltningen att agera samfällt.

Vissa av strategins åtgärder kommer att behöva tas omhand av lagstiftningsansvariga inom Regeringskansliet, medan andra åtgärder främst kommer att beröra ansvariga för myndighetsstyrning. Regeringen kan här överväga om man vill hantera de olika strategiska åtgärderna enligt gängse beredning av regeringsärenden, vilket med ansvarsfördelningen efter regeringsbildningen 2014 torde innebära att inrikesministern ”äger” strategin, eller om man vill låta en för ändamålet inrättad genomförandekommitté (se exempelvis den s.k. polissamordningen, dir. 2012:129) genomföra de i strategin ingående åtgärderna.

Koncentrationen av ansvar och myndighetsresurser under inrikesministern skapar goda förutsättningar för att effektivt styra verksamheten under regeringens politik för informations- och cybersäkerhet. Att det i avsaknad av ett definierat politik- och utgiftsområde finns relaterade och i viss mån tangerande ansvarsområden ställer stora krav på samordning inom Regeringskansliet. I ljuset av Riksrevisionens påpekanden och av erfarenheterna från tidigare försök att genomföra strategiska kursändringar från regeringens sida, finns det anledning att noggrant övervaka att de en-

skilda åtgärdernas beredning sker i full enlighet med den politiska viljan som ligger i inrikesministerns mandat och att denna beredning vid behov också stöttas proaktivt från politisk nivå.

Även om flera åtgärder som föreslås nedan är regeringsfrågor kommer de att behöva genomföras av myndigheter. Det är därför lämpligt att de ansvariga myndigheterna inom det föreslagna myndighetsrådet under MSB:s ledning utarbetar en handlingsplan för de åtgärder som krävs som följd av förslagen i betänkandet, på liknande sätt som skett under SAMFI-strategin. Då behovet av politisk vägledning även framgent kan förväntas vara stort bör regeringen överväga att med jämna mellanrum följa upp arbetet i myndighetsrådet och vid behov kalla rådet till sig för uppföljning; med hänsyn till rådets uppgifter föreligger inga hinder enligt 12 kap. 2 § regeringsformen för ett nära samarbete mellan regering och råd.

9.2 Ansvar, styrning, samordning och tillsyn

9.2.1 En nationell styrmodell

Bedömning: En nationell styrmodell för informationssäkerhet i samhället bör etableras.

Förändrade förutsättningar för informationssäkerhetsarbete

Förändringarna i informationshantering innebär att informationssäkerhetsarbete måste utföras på ett förändrat sätt jämfört med tidigare. Information hanteras inte enbart inom en enskild myndighet eller organisation utan även mellan sådana, exempelvis genom direktåtkomst till olika databaser. Konsekvensen av detta är att informationssäkerhetsarbete för att fungera måste bedrivas i former som är myndighetsöverskridande. För att detta ska kunna genomföras krävs en långsiktig och uthållig nationell styrning, stödd av en kontinuerligt utvecklad kompetens. I detta sammanhang är det viktigt att notera att styrning kan ske i olika former och bör avpassas efter de aktuella förutsättningarna.

Övergripande kan sägas att den offentliga informationshanteringen tidigare skett i en renodla offentlig styrning, dvs. en situation där offentligt finansierad verksamhet utförts av i huvudsak

offentliga aktörer. Nu utförs en allt större andel av den offentligt finansierade verksamheten av privata aktörer. Därmed är det nödvändigt att lagstiftning och föreskrifter kompletteras med olika former av avtal för att styrningen ska kunna nå samtliga aktörer som deltar i den gemensamma informationshanteringen. Det innebär att det offentliga på ett helt annat sätt än tidigare måste lägga mycket mer tid på att vara en kvalificerad beställare.

En alltmer nationellt integrerad informationshantering ställer krav på en sammanhållen nationell styrning och kontroll av informationssäkerheten i all den informationshantering som det offentliga ansvarar för. För att detta ska fungera bör det systematiska informationssäkerhetsarbete som bedrivs i statliga myndigheter sammanfogas i en nationell struktur.

Det är inte längre möjligt att göra enskilda bilaterala överenskommelser inom en och samma sektor kring säkerhetsåtgärder när hundratals aktörer, eller i vissa fall tusentals som inom hälso- och sjukvård, är involverade i samma system för informationshantering. Den fragmentiserade kravställningen utgör en stor utmaning för de privata organisationer som ska leverera de olika tjänsterna till det offentliga. Att ta fram ett stort antal unika men snarlikna lösningar är inte rationellt vare sig för kund eller för leverantör.

Inom e-förvaltning och e-hälsa samverkar ett stort antal aktörer, offentliga såväl som privata, med mycket olika förutsättningar. Ett exempel är när en liten kommun som har begränsade ekonomiska resurser och små möjligheter att tillförsäkra sig informationssäkerhetskompetens delar information med bland annat landets största landsting. Det innebär att den lilla kommunen kan äventyra säkerheten i hela den gemensamma infrastrukturen om inte gemensamma regler finns och kommunen inte har resurser att genomföra de säkerhetsåtgärder som regelverket kräver. På detta sätt kan även de investeringar som andra aktörer gör i sin och den gemensamma säkerheten blir underminerade. Detta förhållande gäller inom ett stort antal samhällsområden. Det är därför viktigt att börja skapa en utveckling där säkerheten stärks både hos den enskilda organisationen och i den gemensamma infrastrukturen.

Under de senaste åren har staten gjort ett antal satsningar på nationell informationshantering både i form av tjänster som Mina meddelanden, en svensk e-legitimation och i organisatoriska former som i Statens servicecenter (SSC) och E-hälsomyndigheten.

Det har även bedrivits ett aktivt arbete från E-delegationen och inom vårdområdet för att främja utvecklingen mot ett e-samhälle. I dessa satsningar finns en stor potentiell möjlighet att höja den nationella informationssäkerhetsnivån inom viktiga områden. Myndigheter har också i olika utsträckning ålagts att överföra sin informationshantering till Statens servicecenter och att använda de nationella tjänsterna.

En nationell styrmodell för systematiskt informationssäkerhetsarbete

Förändringarna i myndigheternas informationshantering har skett under förhållandevis kort tid. Till det kommer att tiden för själva genomförandet av respektive åtgärd har varit kort. Koncentration av informationshantering på nationell nivå sammantaget med otydligheter i ansvarsförhållanden och i vilka krav och förväntningar på informationssäkerheten som ska gälla, gör att ett samlat grepp behöver tas för att se till att ansvar för informationssäkerheten klargörs och säkerställs på ett betryggande sätt.

Det behövs således enligt utredningens bedömning en nationell satsning på systematiskt informationssäkerhetsarbete i statlig verksamhet. Utredningen föreslår därför att ett gemensamt ramverk, en nationell styrmodell, för statens informationssäkerhetsarbete etableras. Genom denna ska ett för de statliga myndigheterna gemensamt förhållningssätt till informationssäkerhetsfrågor säkerställas. Styrmodellen blir en gemensam bas för statligt informationssäkerhetsarbete. Utredningens förslag avser i första hand de statliga myndigheterna och ska vara normerande för dessa men styrmodellen kan på sikt utsträckas till att omfatta hela den offentliga sektorn.

En gemensam styrmodell syftar till att myndigheters informationssäkerhetsarbete ska utföras på ett ensat sätt. Därigenom tas ett samlat grepp om informationssäkerheten i det offentliga. Syftet är att skapa en gemensam syn på en lägsta nivå av informationssäkerhet i staten och samtidigt höja denna från dagens situation.

Det ska alltså skapas en samlad modell innefattande bl.a. gemensamma metoder för riskanalys, riskhantering, informationsklassning och kontinuitetshantering, definierade skyddsnivåer med tillhörande skyddsåtgärder och gemensamma kravbilder, stöd för

informationsklassning och säkerhetsnivåer, terminologi för informationssäkerhetsarbete och regelverk. Styrmodellen ska baseras på existerande krav i författningar och verksamheternas behov.

Genom etablering av en sådan styrmodell möjliggörs att information kan överföras mellan myndigheter med samma skydd, eftersom en ensad modell för informationsklassning inklusive skyddsnivåer skapas.

Av särskild betydelse att generellt besluta om är ansvarsförhållanden i informationshanteringen och därmed för olika delar av informationssäkerhetsarbetet.

Ytterst handlar kraven om hur lösningar för drift och kommunikation ska utformas och detta kommer att i hög grad påverka privata leverantörer av denna typ av tjänster. För att leverantörerna ska kunna få en tillräckligt god förutsägbarhet och därmed kunna utveckla standardiserade och prisvärda lösningar är gemensamma regelverk också ett mycket gott stöd. Den statliga sektorn skulle på så sätt också utveckla sin beställarkompetens och som följd skulle utvecklingen av den nationella säkerhetsarkitekturen styras av verksamhetskrav i stället för att, som ofta nu är fallet, vara händelsestyrd och teknikdriven.

En nationell satsning på systematisk informationssäkerhet skulle innebära att de beskrivna förhållandena kan hanteras på ett över tiden sammanhållet och proaktivt sätt. En viktig del i detta är att skapa sektorsspecifika strukturer för informationssäkerhet utifrån en generisk nationell styrmodell.

Genom en nationell styrmodell för systematiskt informationssäkerhetsarbete skulle ett effektivt stöd för de aktörer som ingår i den integrerade informationsinfrastrukturen skapas. Styrmodellen skulle också verka sammanbindande eftersom såväl andra offentliga som privata organisationer på sikt skulle kunna ansluta sig till den.

Att ett sådant gemensamt ramverk tas fram på nationell nivå måste också vara det mest ekonomiskt försvarbara sättet att bedriva systematiskt informationssäkerhetsarbete i staten med hänsyn till att metodarbetet då inte behöver utföras hos varje enskild myndighet även om varje myndighet måste göra sin egen riskbedömning, kartlägga sina egna skyddsvärda tillgångar och bestämma över sitt eget behov av skyddsnivå.

Samverkan, långsiktighet och uthållighet är nödvändiga förutsättningar för att en nationell styrmodell för systematisk inform-

ationssäkerhet ska fylla den funktion som är önskvärd. Genom en styrmodell skapas en långsiktighet och tydlighet i samhällets arbete med informationssäkerhet.

En styrmodell skapar också en indirekt styrning mot det privata näringslivet då staten, jämte landstingen och kommunerna, är de största beställarna av privata tjänster. Det blir på detta sätt tydligt vilka regler och ramar som gäller vid leverans av olika tekniska lösningar vilket med hänsyn till förutsägbarheten kommer att innebära ekonomiska fördelar för privata aktörer.

MSB ges i uppdrag att utveckla styrmodellen

Enligt utredningen är MSB den myndighet som bör får i uppdrag att utveckla, förvalta och vidareutveckla styrmodellen. MSB bör utveckla denna med stöd från övriga myndigheter i det av utredningen föreslagna Myndighetsrådet för informationssäkerhet, se följande avsnitt. Med sitt regeringsuppdrag att stödja samhällets arbete med informationssäkerhet ska MSB alltså även få ett utvidgat uppdrag att efter samverkan i myndighetsrådet och i samverkan med andra myndigheter utveckla, förvalta och vidareutveckla en styrmodell för statens informationssäkerhet. Myndigheter som ingår i myndighetsrådet bör ges i uppdrag att stödja förvaltningen och utvecklingen av styrmodellen.

9.2.2 Inrättande av ett myndighetsråd

Förslag: Regeringen inrättar ett statligt myndighetsråd för informationssäkerhet bestående av företrädare för de relevanta myndigheterna på området.

Samordning på informationssäkerhetsområdet i dag

I gruppen SAMFI samverkar i dag myndigheter med särskilda uppgifter och särskilt ansvar inom området informationssäkerhet (se avsnitt 7.6.1). MSB har en uttalad samordningsroll när det gäller samhällets informationssäkerhet och myndigheten har ett samordnande ansvar i SAMFI. Utöver detta har MSB för att utnyttja sam-

hällets samlade kompetens i övrigt knutit till sig ett informationssäkerhetsråd med bred representation från både offentlig förvaltning och näringslivet (se avsnitt 7.7.1).

SAMFI träffas sex gånger per år och syftet är att underlätta samarbetet genom informationsutbyte och samverkan. De myndigheter som medverkar är följande.

- Myndigheten för samhällsskydd och beredskap (MSB)
- Post- och telestyrelsen (PTS)
- Försvarets radioanstalt (FRA)
- Säkerhetspolisen (Säpo) och Nationella operativa avdelningen (NOA, tidigare Rikskriminalpolisen) i samverkan
- Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för IT-säkerhet (CSEC)
- Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST)

Samordningens betydelse

Det finns ett stort behov av ledning på informationssäkerhetsområdet och det gäller såväl samordning av myndigheter som styrning av informationssäkerhetsarbetet.

De allvarliga brister i informationssäkerheten i den civila statsförvaltningen som påtalats såväl i Riksrevisionens granskning RiR 2014:23 *Informationssäkerheten i den civila statsförvaltningen* som i MSB:s kartläggning *En bild av myndigheternas informationssäkerhetsarbete 2014* av hur statliga myndigheter tillämpar MSB:s föreskrifter och i övrigt arbetar med informationssäkerhet gör att det är angeläget att åtgärder vidtas för att stärka säkerheten. För att stärka informationssäkerheten är samordning av statliga myndigheters arbete av central betydelse.

Regeringen har i sin skrivelse *Samhällets krisberedskap – stärkt samverkan för ökad säkerhet* (Skr. 2009/10:124) betonat betydelsen av SAMFI:s arbete: ”SAMFI (…) har en särskilt viktig roll då den syftar till att åstadkomma samverkan mellan de statliga myndigheter som har särskilda uppgifter på informationssäkerhetsområdet.”

Grunden för samhällets krisberedskap är ansvarsprincipen (propositionen *Stärkt krisberedskap – för säkerhets skull*, prop. 2007/08:92, bet. 2007/08:FöU12, rskr. 2007/08:193-194). Det innebär att den som har ansvar för en verksamhet under normala förhållanden också har det under allvarliga händelser, kriser eller krig. I ansvarsprincipen ingår även att initiera och bedriva sektorsövergripande samverkan. Det finns flera statliga myndigheter med särskilda uppgifter eller uppdrag på informationssäkerhetsområdet, såväl nationellt som internationellt, och frågorna spänner över en mängd olika områden och nivåer. I ansvarsprincipen ingår att samverka och samordna sig med andra aktörer i den omfattning som krävs för att effektivt förebygga och hantera en allvarlig händelse. I utredningens direktiv anges särskilt att de statliga myndigheterna bör utveckla sin förmåga att samverka inom informationssäkerhetsområdet.

Fördjupad samordning

Samordning av ansvariga myndigheter är alltså en central fråga för arbetet med statens informationssäkerhet. Den samverkan mellan myndigheter som i dag sker inom ramen för SAMFI är enligt utredningens mening mycket betydelsefull. Dagens komplexa och snabba utveckling av informationsteknik och it-tjänster och samhällets sårbarhet gör att det är nödvändigt att ytterligare fördjupa samordningen mellan myndigheterna. Med hänsyn till denna utveckling och påtalade brister är behovet av att stärka informationssäkerheten stort. Det är därför av vikt att insatser görs för att stärka säkerheten inom området för att Sverige ska kunna upprätthålla säkerhet, robusthet och integritet i samhällsviktig it-infrastruktur. Detta kan bl.a. ske genom en utveckling och fördjupning av det arbete som i dag sker inom ramen för SAMFI.

Ett myndighetsråd inrättas

I syfte att ytterligare formalisera, utveckla och fördjupa samordningen av arbetet även i de delar av statens informationssäkerhet som inte främst gäller krisberedskap bör regeringen inrätta ett myndighetsråd för informationssäkerhet. Rådet ska främst bestå av

företrädare för relevanta statliga myndigheter på området. Genom inrättandet av rådet ges förutsättningar för en bättre systematisk analys av hot och risker och uppfattning om genomförda säkerhetsåtgärder. Genom att etablera rådet skapas också bättre förutsättning för det bredare informationssäkerhetsarbetet. Förslaget ger MSB och deltagande myndigheter förbättrade möjligheter att uppfylla arbetet med en gemensam lägesbild och därigenom ett bättre stöd till samhället.

Ett annat samordningsorgan, Samverkansrådet mot terrorism, kan nämnas. Detta samverkansråd består av fjorton myndigheter. Nätverket har visserligen inget formellt uppdrag men ett uttalat stöd från regeringen.

Med hänsyn till MSB:s samordnande roll inom området för informationssäkerhet bör myndigheten leda myndighetsrådet samt sköta administrationen. Myndighetsrådet bör också kunna sammankallas under Regeringskansliets ledning för diskussioner av policykaraktär (jfr konstruktionen i Rådet för rättsväsendets informationsförsörjning). Även de övriga myndigheter med särskilda uppgifter och särskilt ansvar inom området informationssäkerhet som i nuläget samverkar i SAMFI bör ingå i rådet. Utöver nämnda myndigheter kan även andra myndigheter och aktörer som inte direkt omfattas av regeringens uppdrag ges en viktig roll. Exempelvis kan sektorsmyndigheter bjudas in för samverkan i rådet. Rådet skulle också efter utvärdering kunna överta flera av de funktioner som i dag handhas av SAMFI-gruppen. Vidare föreslås att det i en förordning för statliga myndigheters informationssäkerhet (se avsnitt 9.2.3) föreskrivs att arbetsgrupper kan inrättas. På detta sätt skapas en flexibilitet som över tiden kan adressera den dynamiska it-utvecklingen och de utmaningar som e-samhället efterhand ställs inför.

Att inrätta ett råd för informationssäkerhet ligger i linje med de synpunkter och rekommendationer som Riksrevisonen lämnat i sin rapport (RIR 2014:23).

Myndighetsrådets uppgifter

Myndighetsrådet för informationssäkerhet ska ha som uppgift att förebygga, följa och åtgärda brister i statens informationssäkerhet. Ett särskilt inrättat myndighetsråd medför en kontinuitet och tydlighet i det samordnade arbetet jämfört med SAMFI som baseras på frivillighet. Inrättandet av ett myndighetsråd innebär således en förstärkning av insatserna för säkerheten på området. För att närmare tydliggöra myndighetsrådets uppgifter bör dessa slås fast på förordningsnivå.

Myndighetsrådet ska agera inom SAMFI:s nuvarande aktivitetsområden (se avsnitt 7.6.1) samt inom de områden som kan följa av den nya förordningen för statliga myndigheters informationssäkerhet (se avsnitt 9.2.3). Arbetet ska ske genom samråd och samverkan och grundas på informations- och erfarenhetsutbyte mellan myndigheterna och samordning av insatser. Myndighetsrådet föreslås inte ha egen beslutanderätt utan myndigheterna fattar beslut inom respektive ansvarsområden efter samråd i rådet. Myndighetsrådet kan fungera som en gemensam remiss- och beredningsinstans i informationssäkerhetsfrågor. Vid framtagande av styrmodellen kan MSB inhämta kommentarer i rådet. Sektorsansvariga myndigheter som inte ingår i rådet bör kunna ges stöd i rådet inför utfärdande av föreskrifter på informationssäkerhetsområdet.

Myndighetsrådet ska, vid sidan av den föreslagna genomförandekommittén (se avsnitt 9.1.5) säkerställa verkställandet av den nationella informations- och cybersäkerhetsstrategin. Vidare ska myndighetsrådet, baserat på ett system för incidentrapportering, förses med lägesbeskrivningar av hot- och risknivåer i den statliga verksamheten (se vidare avsnitt 9.5).

En uppgift för myndighetsrådet ska vara att förvalta och utveckla tillämpliga krav på standarder och certifiering för produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet. All anskaffning av produkter som av myndighetsrådet bedöms vara kritiska för säkerställandet av säker kommunikation i staten skulle kunna göras till föremål för en certifieringsprocess där rådet skulle kunna spela en viktig roll (se vidare avsnitt 9.3.1 om säkra it-produkter i staten). För det fall ett behov uppstår av nationella evalueringslaboratorier kan myndighetsrådet få i uppgift

att vara remissinstans för de regler och krav som utfärdas av det nationella certifieringsorganet CSEC inordnat vid FMV.

Myndighetsrådet bör med bland annat stöd av den nationella styrmodellen och tillsammans med den nya upphandlingsmyndigheten ge stöd till myndigheter som har behov av expertkompetens vad gäller it- och informationssäkerhet. Stödet bör ges till myndigheter som står inför upphandling av informations- och it-lösningar och bör bestå av allmänna rekommendationer om bl.a. it-standarder och krav på certifiering.

I uppgifterna för det av regeringen inrättade myndighetsrådet bör ingå att identifiera andra frågor än de ovan nämnda som kan göras till föremål för rådets behandling.

En utvärdering av rådets verksamhet bör genomföras efter två år.

Kansli

Som stöd för myndighetsrådet ska ett kansli inrättas med uppgift bl.a. att säkerställa informationsutbytet och samordning av de samverkande myndigheterna samt förse rådet med beslutsunderlag. MSB driver i nuläget på frivillig väg SAMFI:s kansli. Myndighetsrådets kansli bör med hänsyn till MSB:s roll vara placerat hos denna myndighet.

9.2.3 En ny förordning för statliga myndigheters informationssäkerhet

Förslag: En ny förordning för statliga myndigheters informationssäkerhet införs.

Utredningen föreslår att en förordning för statliga myndigheters informationssäkerhet införs. I en sådan förordning kan existerande regler på området samlas. Vidare kan också nya regler, bl.a. sådana som föreslås i detta betänkande, införas. På detta sätt regleras tydligare den civila statsförvaltningens arbete med informationssäkerhet och en gemensam lägstanivå kan skapas. Existerande regelkrav, främst hämtade från förordningen (2006:942) om krisberedskap

och höjd beredskap (KBF), förs till förordningen. Placeringen i en ny förordning med generellt tillämpliga regler gör att bestämmelserna tydliggörs när de placeras i annan kontext än krisberedskap. Härigenom kan också tillämpningen förenklas.

Skyldigheten i 30 a § KBF för myndigheter att ansvara för att de egna informationshanteringssystemen uppfyller säkerhetskraven bör flyttas till den nya förordningen.

Utredningen föreslår att följande bestämmelser ska införas.

Inledande bestämmelser (1–3 §§)

Nya bestämmelser som klargör förordningens bl.a. syfte och innehåll ska införas. 1 § motsvarar i huvudsak 30 a § i KBF. Vidare krävs en reglering som stadgar att bestämmelserna om MSB:s tillsyn och föreskriftmandat samt bestämmelsen om särskilda krav på informationssäkerhetsarbete gäller för statliga myndigheter med undantag av Regeringskansliet, kommittéväsendet och Försvarsmakten samt att bestämmelserna tillämpas för utlandsmyndigheterna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet. Avseende föreskriftsmandatet motsvarar skrivningen 3 § KBF.

Definitioner (4 §)

Definitioner av informationssäkerhet och samhällsviktig verksamhet ska införas i en inledande bestämmelse. Det ska anges att med informationssäkerhet avses förmågan att upprätthålla konfidentialitet, riktighet, tillgänglighet och spårbarhet i sin informationshantering. När det gäller samhällsviktig verksamhet bör den definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv som används av Myndigheten för samhällsskydd och beredskap användas (se Myndigheten för samhällsskydd och beredskap, Faktablad augusti 2009 Samhällsviktig verksamhet Definition av samhällsviktig verksamhet ur ett krisberedskapsperspektiv).

Regler rörande det interna säkerhetsarbetet (5–10 §§)

Paragraferna bygger på och förtydligar 30 a § KBF. Det förslås att en inledande bestämmelse slår fast att statliga myndigheter ska säkerställa att den information de ansvarar för eller hanterar i tjänster som myndigheten levererar till en annan organisation, upprätthåller en tillräcklig nivå av informationssäkerhet, varvid ska anges att detta ska ske genom ett risk- och sårbarhetsbaserat, systematiskt och processinriktat arbetsätt. Vidare ska stadgas att myndigheterna särskilt ska beakta behovet av ledningssystem och etablerade standarder för informationssäkerhet.

Ledningens ansvar och roller i verksamheten ska slås fast. Det ska stadgas att det i ledningen ska finnas en person med utpekat ansvar för informationssäkerhetsfrågor samt att myndigheten ska peka ut vem som leder och samordnar det praktiska arbetet med informationssäkerhet. Myndigheten ska också enligt denna bestämmelse tydliggöra roller och ansvar för informationssäkerhetsarbetet i myndighetens organisation. Vidare ska anges att myndigheten aktivt ska verka för att en god säkerhetskultur etableras i organisationen och att detta ska ge genom utbildning och övning.

En ny bestämmelse föreslås som slår fast hur informationsklassning ska genomföras, att inträffade it-incidenter ska kunna identifieras och hanteras och att lämpliga säkerhetsåtgärder ska vidtas. Det ska anges att myndigheter ska kartlägga sina informationsprocesser och klassificera sin information med utgångspunkt i krav på informationssäkerhet i enlighet med den i 4 § fastslagna definitionen. Vidare ska stadgas att säkerhetsåtgärder ska vidtas beroende på klassning samt identifierade hot, risker och sårbarheter. I detta arbete ska utvecklade krav och skyddsnivåer följas.

Ett krav ska införas på myndigheter att välja och använda säkra it-produkter vid hantering av information där bristande informationssäkerhet kan medföra en betydande försämring av myndighetens förmåga att bedriva sin verksamhet. Det förslås att it-produkter som finns utpekade i verkställighetsföreskrifter som meddelats med stöd av förordningen ska användas.

En ny bestämmelse ska införas om uppföljning och dokumentation av informationssäkerhetsarbete samt om kontinuitetsplanering. Det ska införas krav på att upprätta en årlig informations-

säkerhetsplan som tydliggör hur arbetet med informationssäkerhet för att uppnå ställda krav ska bedrivas och krav på att med stöd av kontinuitetsplanering upprätthålla en sådan nivå av informationssäkerhet att myndigheten har god förmåga att hantera sina uppgifter i kris och under höjd beredskap. Det ska slås fast att myndigheter ska följa upp sitt informationssäkerhetsarbete, dokumentera bedömningar avseende hot, risker och sårbarheter samt redogöra för arbetet som bedrivs med kartläggning av informationsprocesser, klassificering av information, identifiering och hantering av inträffade it-incidenter, säkerhetsåtgärder samt användning av säkra it-produkter.

Kravet på kontinuitetsplanering förtydligar behovet av att även beakta krisberedskaps- och kontinuitetshanteringsperspektivet i informationssäkerhetsarbetet. Detta följer implicit av det faktum att nuvarande krav på att statliga myndigheter arbetar med informationssäkerhet är placerad i krisberedskapsförordningen. I detta avseende förtydligas alltså 30 a § KBF.

Vidare ska det införas en bestämmelse som anger att kraven i 5–9 §§ endast gäller i tillämpliga delar för sådana myndigheter vars informationshantering eller informationssäkerhetsarbete administreras av en annan myndighet. Syftet är att omhänderta de särskilda förutsättningar som informationssäkerhetsarbete hos exempelvis nämndmyndigheter vars hela informationshantering administreras av en annan myndighet skapar. Målsättningen är inte att undanta arbetet den här typen av myndigheter utför åt annan myndighet från kraven, utan i stället nyansera kravbilden så att förordningen blir praktiskt möjlig att tillämpa. I bestämmelsen benämns en myndighet som sköter arbetet åt en annan myndighet ”värdmyndighet”. Det föreslås att ett krav ställs på en värdmyndighet att informera den anlitande myndigheten om it-incidenter som har eller kan ha påverkat säkerheten för information hos den anlitande myndigheten.

Särskilda krav på informationssäkerhetsarbete (11 §)

En bestämmelse föreslås som ger möjlighet att ställa särskilda krav på de myndigheter som anges i KBF att vidta säkerhetsåtgärder, nya bestämmelser om krav på utpekade resurser för informationssäkerhet och kompetenskrav (såsom certifiering eller motsvarande erfarenhet)

för informationssäkerhetschef eller motsvarande i statliga myndigheter som omnämns i KBF. Även denna bestämmelse förtydligar innebörden av de särskilda krav på informationssäkerhet som ställs i 30 a § KBF.

Säkra kryptografiska funktioner (12–14 §§)

Bestämmelserna i 31–33 §§ KBF om säkra kryptografiska funktioner föreslås flyttas över till den nya förordningen. Dessa regler kan behöva utvecklas senare för att täcka in nya behov, exempelvis avseende civilt försvar.

Upphandling av it-system och it-produkter (15–16 §§)

I avsnitt 9.3.1 behandlar utredningen frågor om kravställning vid upphandling. I förordningen föreslås nya bestämmelser om säkerhet vid upphandling och hantering av säkerhetsfrågor i samband med anslutning till myndighetsgemensamma tjänster. Syftet är att omhänderta det växande behovet av att säkerställa att säkra it-produkter används så långt möjligt i samhällsviktig verksamhet. Det ska införas en bestämmelse enligt vilken myndigheter i samband med upphandling och utveckling av it-system eller it-produkter i förhållande till leverantören ska klarlägga ansvar och roller för informationssäkerhetsarbetet. Vidare ska stadgas att upphandlingen eller utvecklingen ska föregås av informationsklassning och riskanalys av berörd information. Resultatet av detta ska därefter vara styrande för utformningen av säkerhetskrav som ställs vid upphandling eller utveckling. Det ska förtydligas att de angivna kraven även gäller vid anslutning till myndighetsgemensamma tjänster för e-förvaltning eller liknande. Vidare föreslås krav på att en myndighet endast ska uppdra åt en annan myndighet att hantera myndighetens information om hanteringen kan ske med tillräcklig säkerhet, varvid it-incidenter som påverkat eller kan ha påverkat säkerheten ska rapporteras till myndigheten.

En ny bestämmelse ska införas enligt vilken – i samband med upphandling av it-produkter som ska användas i samhällsviktig verksamhet som bedrivs av staten – krav ställs på att endast säkra it-produkter ska användas. I de fall säkra it-produkter finns

utpekade i verkställighetsföreskrifter (se vidare nedan) ska dessa användas. Paragrafen kompletterar bestämmelsen i 8 § förordningen där krav ställs på säkra it-produkter i den egna verksamheten.

It-incidentrapportering (17 §)

Utredningen föreslår i avsnitt 9.5 att det inrättas system för obligatorisk incidentrapportering för samtliga statliga myndigheter. I förordningen ska nya bestämmelser om krav på it-incidentrapportering införas. För statliga myndigheter föreslås en rapporteringsskyldighet av it-incidenter till MSB. Detta ska gälla för it-incidenter som allvarligt kan påverka säkerheten i myndighetens informationshantering eller tjänster som en myndighet levererar. Det ska anges att rapporteringen ska ske skyndsamt.

För att klargöra avgränsningen mot den tillsyn som sker enligt säkerhetsskyddförordningen ska stadgas att rapporteringplikten inte gäller för it-incidenter som ska anmälas till en tillsynsmyndighet enligt bestämmelserna i 10 a § säkerhetsskyddsförordningen förrän tillsynsmyndigheten har meddelat den rapporteringspliktiga myndigheten att incidenten inte längre är föremål för behandling hos tillsynsmyndigheten.

Tillsyn, föreskrifter, Myndighetsrådets uppgifter (18–20 §§)

I avsnitt 9.2.2 har utredningen föreslagit att ett statligt myndighetsråd för informationssäkerhet ska inrättas. En ny bestämmelse om rådets uppgifter ska införas i förordningen. Det ska anges att myndighetsrådet har till uppgift att stödja och utveckla informationssäkerhetsarbetet i samhället, varvid det som exempel bör räknas upp att det i detta ingår att utgöra en gemensam beredning- och remissinstans på informationssäkerhetsområdet, bidra med stöd rörande informationssäkerhetsfrågor vid utfärdandet av föreskrifter på informationssäkerhetsområdet, förvalta och utveckla tillämpliga krav i standarder samt certifiering och ackreditering (kontrollordningar) för produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet, bistå med expertkompetens i samband

med upphandling av tjänster och produkter på informationssäkerhetsområdet, och utveckla krav- och skyddsnivåer.

I samma bestämmelse ska slås fast att MSB ska tillhandahålla en kanslifunktion för Myndighetsrådet och att rådet vid behov ska inrätta arbetsgrupper.

I avsnitt 9.2.4 nedan beskrivs utredningens förslag avseende tillsyn. Förslaget om MSB:s tillsynsmandat över statliga myndigheters informationssäkerhetsarbete ska slås fast i en ny bestämmelse.

För att avgränsa MSB:s tillsynsuppgift mot den tillsyn som sker enligt säkerhetsskyddsförordningen föreslås att det föreskrivs att undantag ska gälla för sådant arbete som redan är föremål för tillsyn i enlighet med 39 § säkerhetsskyddsförordningen. Enligt den bestämmelsen ska säkerhetsskyddet kontrolleras av Försvarsmakten och Säkerhetspolisen.

MSB bör på motsvarande sätt som anges i 34 § KBF ges rätt att meddela föreskrifter rörande internt informationssäkerhetsarbete, kryptografiska funktioner. Föreskriftsmandatet bör också gälla för upphandling och incidentrapportering. Föreskriftsuppgiften för MSB ska således gälla de föreskrifter som behövs för verkställigheten av de allmänna och särskilda krav på statliga myndigheters interna informationssäkerhetsarbete som avses i 5–11 och 15 §§, med beaktande av nationell och internationell standard, de föreskrifter som behövs för verkställigheten av 14 §, utom i fråga om Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut och Fortifikationsverket, de föreskrifter som behövs för verkställigheten av 16 § utom i fråga om myndigheter för vilka Försvarsmakten eller Säkerhetspolisen meddelar motsvarande föreskrifter enligt 44 § säkerhetsskyddsförordningen samt de föreskrifter som behövs för verkställigheten av sådan it-incidentrapportering som avses i 17 §.

Förordningen föreslås träda i kraft den 1 januari 2016. I en bilaga till förordningen kan anges vilka myndigheter som ingår i myndighetsrådet.

Införs föreslagen förordning ska motsvarande bestämmelser i KBF upphävas.

9.2.4 Tillsyn

Förslag: Tillsynen över den statliga sektorns informationssäkerhet samordnas och förstärks. MSB får i uppgift att bedriva tillsyn över statliga myndigheters arbete med informationssäkerhet. Den sektorsvisa tillsynen i staten ses över.

Tillsyn i dag

Säkerhetspolisen är den enda myndighet som har mandat att granska informationssäkerhet i den civila statsförvaltningen. Säkerhetspolisens granskning utgår från säkerhetsskyddsregleringen, vilket begränsar vad som kan omfattas av och göras i en granskning. De verksamheter som granskas av Säkerhetspolisen utgör också i praktiken en ytterst liten del av den totala statsförvaltningen.

Försvarsmakten (MUST) bedriver tillsyn av informationssäkerheten enligt säkerhetsskyddsförordningen över de myndigheter som hör till Försvarsdepartementet, Försvarshögskolan och Fortifikationsverket.

Datainspektionen genomför tillsyn som omfattar informationssäkerhet men dess tillsyn berör en delmängd av informationssäkerheten, nämligen integritetsskyddsaspekterna.

PTS tillsynsroll över sektorn elektroniska kommunikationer ger PTS indirekt en viktig roll för statsförvaltningens informationssäkerhet eftersom den är beroende av tillgång till säkra elektroniska kommunikationer. PTS har bland annat i uppgift att bedriva tillsyn över att operatörer upprätthåller en grundläggande driftsäkerhet avseende allmänna elektroniska kommunikationer.

Riksarkivet har ett tillsynsansvar avseende informationssäkerhet men tillsynen är begränsad till att omfatta det som finns i myndigheternas arkiv, det vill säga i huvudsak allmänna handlingar.

Behov av förstärkning och samordning av tillsyn

Riksrevisionen (RiR) har poängterat behovet av tillsyn. I sin rapport anger RiR följande slutsatser och rekommendationer avseende stöd och tillsyn (samt rekommendationer för att förbättra statens

informationssäkerhet) (s. 80). ”Rikspolisstyrelsen genom Säkerhetspolisen utövar tillsyn, men har av resursskäl inte möjlighet att göra det i hela förvaltningen, utan har inriktat sin tillsyn på de myndigheter som har den allra mest skyddsvärda verksamheten.”/…/” RiR bedömer att resurser för tillsyn generellt inte har prioriterats i tillräcklig utsträckning.” Vidare anges (s. 81) att den tillsyn som sker täcker i stort sett endast den mest skyddsvärda verksamheten – merparten av den civila statsförvaltningen lämnas utan tillsyn. Åtgärder vidtas inte alltid efter genomförda inspektioner. ”/…/

För att förbättra statens informationssäkerhet rekommenderar RiR därför regeringen bl.a. att utöka tillsynen av informationssäkerheten i den civila statsförvaltningen, så att den omfattar väsentligt mer än de allra mest skyddsvärda delarna. Vidare föreslås att regeringen låter utreda om ansvaret för att utöva tillsyn över informationssäkerheten i den civila statsförvaltningen kan samlas och koordineras på ett bättre sätt än i dag. Som bakgrund till rekommendationen om att stärka MSB:s roll för att samla kunskapen om informationssäkerhetsläget konstaterade RiR därtill följande(s. 43). ”MSB har ett omfattande uppdrag att stödja samhällets informationssäkerhet, men har inget uppdrag att utöva tillsyn. MSB är därför till stor del beroende av att aktörer lämnar uppgifter frivilligt. Den nätverksstruktur som MSB delvis grundar sin informationsinhämtning på ger enligt RiR en insyn i vilka problem och hot som finns mot samhället i stort. Sättet att inhämta informationen kan dock innebära svårigheter för MSB att agera mot myndigheter och företag som deltar i informationsutbytet, eftersom agerandet kan riskera förtroendet och därmed grunden för informationsinsamlingen.”

För flera av de uppgifter som nu helt eller delvis ligger inom MSB:s ansvarsområde, samhällets informationssäkerhet inklusive incidentberedskap samt även krisberedskap i stort saknas möjligheter att genom tillsyn öka kunskapen om hot, risker och vidtagna säkerhetsåtgärder. Riksrevisionen pekar på att en bra och systematiskt underbyggd lägesbild är en förutsättning för att kunna säkerställa att man vidtar rätt åtgärder (s. 77). Även om uttalandet görs med koppling till informationssäkerheten i förvaltningen torde det ha bäring på både arbete med samhällets informationssäkerhet i stort liksom krisberedskap.

Enligt MSB:s föreskrifter om statliga myndigheters informationssäkerhet, MSBFS 2009:10, ska en myndighet i sitt arbete med att upprätthålla säkerhet i sin informationshantering tillämpa ett ledningssystem för informationssäkerhet (LIS) (se avsnitt 5.3.3) Den senare uppföljningen av efterlevnaden av LIS-föreskrifterna gjordes under 2014. MSB har kartlagt hur statliga myndigheter tillämpar föreskrifterna om ledningssystem för informationssäkerhet (LIS). Av rapporten ”En bild av myndigheternas informationssäkerhetsarbete 2014” framgår att en stor del av myndigheterna inte har ett fungerande systematiskt informationssäkerhetsarbete. Med hänsyn till att föreskrifterna varit i kraft sedan december 2009 och rör grundläggande informationssäkerhetsarbete är det enligt utredningens mening tydligt att det krävs tillsyn av informationssäkerheten hos den civila statsförvaltningen. Vidare instämmer utredningen i RiR:s rekommendationer och slutsatser i frågan.

MSB ges tillsynsuppgift

Mot bakgrund av MSB:s nuvarande ansvar på området samt utredningens förslag avseende MSB:s roll i det föreslagna myndighetsrådet och förordningen för statliga myndigheters informationssäkerhet lämpar sig MSB bäst för att utföra tillsynen över myndigheternas arbete med informationssäkerhet. MSB bör därför utöver det föreslagna föreskriftsmandatet i den nya förordningen även ges tillsynsuppgift över statliga myndigheters arbete med informationssäkerhet. Tillsynen kopplas till föreskriftsmandatet och bör röra efterlevnaden av förordningen.

Genomförandet av MSB:s tillsynsuppgift kommer säkerligen att kräva samverkan med myndigheterna i myndighetsrådet. Det är dessutom nödvändigt att samordning sker i förhållande till den tillsyn som utövas under säkerhetsskyddslagen för att undvika överlappande tillsynsansvar. Vidare krävs samordning med den tillsyn inom staten avseende informationssäkerhet som sker genom sektorsansvariga myndigheters försorg.

Tillsyn sektorsvis

Ett antal myndigheter vid sidan om Försvarsmakten, Säpo och sektorsmyndigheterna har tillsynsansvar inom informationssäkerhetsområdet, t.ex. Datainspektionen, Finansinspektionen och Strålsäkerhetsmyndigheten. Det är en krävande uppgift som ställer höga krav på expertkompetens. Uppdraget omfattar alla aspekter av informationssäkerhet, allt från administrativ säkerhet till it-säkerhet och krypto. Det är inte rimligt att kräva eller förutsätta att den bredd och djup i kompetens som krävs ska finnas inom varje tillsynsmyndighet. Betydligt effektivare och mer rationellt vore om tillsynen genomförs i samverkan med en utpekad myndighet som har den djupa kompetens som krävs. Då skulle tillsynsmyndigheten ha ansvaret och kunskapen om föremålet för tillsyn, och samtidigt dra fördel av expertmyndighetens djupa fackkunskaper. Detta bidrar till kvalitet och stabilitet i tillsynen och en jämn tillämpning av informationssäkerhetskraven på tillsynsobjekten. En samordning av stöd till tillsynsverksamheten vore också effektivt sett till både ekonomi och säkerhet.

Enligt utredningens mening kan konstateras att en generell översyn behövs för att säkerställa att tillräcklig tillsyn över informationssäkerheten föreligger i olika aktuella sektorer. Utredningen anser att en sådan översyn även bör omfatta frågan om hur den sektorsvisa tillsynen ska organiseras. Det är av vikt att se till att den sektorsvisa tillsynen harmonierar med den allmänna tillsyn som MSB ska bedriva.

9.2.5 Informationssäkerhet som en del av myndighetens revision

Bedömning: Revision av informationssäkerhet bör utvecklas. Myndighetsledningens ansvar för att upprätthålla säkerhet i myndighetens informationshantering förtydligas genom rapporteringskrav i förordning (2000:605) om årsredovisning och budgetunderlag.

Ledningens roll för informationssäkerhetsarbetet

Ett systematiskt arbete med informationssäkerhet i en organisation behöver bedrivas som en process innehållande en rad steg. Att identifiera skyddsvärda tillgångar, klassificera sin information för att veta vilken nivå av skydd som krävs och sedan hantera risker och sårbarheter kopplade till hanteringen av informationen är centrala delar i denna process. Det är dock betydelsefullt att peka på att informationssäkerhetsarbetet inte är avslutat i och med detta. En organisations informationshantering utvecklas och förändras kontinuerligt. På samma sätt sker en konstant utveckling av nya typer av risker och sårbarheter som organisationen behöver identifiera och hantera. En grundläggande förutsättning för att arbetet med att skydda en av organisationens mest centrala tillgångar – informationen – är att ledningen engagerar sig i arbetet och driver frågorna.

Ledningens roll för informationssäkerhetsarbetets framgång kan svårligen överskattas eftersom det är ledningen som i den praktiska kontexten beslutar om både mål och medel för arbetet. Ledningens agerande spelar dessutom en stor roll för säkerhetskulturen inom organisationen, det vill säga om informationssäkerheten upplevs som prioriterad eller inte. Redan InfoSäkutredningen 2002–2005 pekade på att informationssäkerhet är en ledningsfråga.

För att ledningen av organisationen ska få verktyg för att kunna säkerställa att informationssäkerhetsarbetet bedrivs på ett sådant sätt som avsetts och mot de mål som satts upp i organisationen krävs en kontinuerlig uppföljning och granskning av det bedrivna arbetet. Detta ger inte bara ledningen möjlighet att säkerställa att tid och resurser har använts på avsett sätt utan även viktiga beslutsunderlag för inriktning och resurssättning av framtida arbete. Uppföljningens och därmed granskningens yttersta syfte är att förbättra verksamheten genom att följa upp, granska och analysera hur den fungerar. Ofta följer man upp i vilken utsträckning organisationen med sitt arbete lyckas nå de uppsatta målen.

Uppföljning och granskning kan ske på många olika sätt. Revision, både extern och intern sådan, är ett särskilt kraftfullt verktyg i och med att det utförs enligt i förväg givna regler och av oberoende parter. För organisationer som är certifierade i enlighet med de internationella informationssäkerhetsstandarderna i

ISO/IEC 27000-familjen ställs uttryckliga krav på revision. I kravstandarden ISO 27001 framgår att själva ledningssystemets funktion ska granskas regelbundet, liksom riskbedömningarna, alla kvarvarande risker och den risknivå man har fastställt som godtagbar. Organisationen ska också göra interna revisioner av ledningssystemet.

Brister i arbete med uppföljning och revision

Även för organisationer som inte till alla delar följer nämnda informationssäkerhetsstandarder är uppföljning och revision en viktig del i ett systematiskt arbete. Bristande uppföljning och revision kan mycket snabbt få påtagliga konsekvenser för organisationens arbete. Det rör sig inte bara om risker att organisationen på grund av okunskap och bristande underlag prioriterar och genomför säkerhetsåtgärder i en mindre lämplig tidsordning. Det kan även innebära att allvarliga säkerhetsbrister inte hanteras och förblir oupptäckta under en längre tid.

Säkerhetsbrister kan skapa risker för att antagonister tillskansar sig känslig information eller förvanskar densamma. Vidare kan processer och tekniska system fallera vilket kan leda till allvarliga tillgänglighetsbrister. Säkerhetsbrister kan även resultera i att organisationen genom sitt förfarande de facto bryter mot lagar och förordningar. En stor del av de nationella och internationella regelverk som organisationer har att följa ställer uttryckliga krav på hur information ska hanteras. Detsamma gäller för exempelvis olika typer av branschregleringar och interna föreskrifter.

De som reviderar och genomlyser informationssäkerhetsarbetet har en mycket viktig roll att spela när det gäller kontrollen av att detta arbete bedrivs på ett korrekt sätt och mot etablerade mål. För att kunna bedriva ett systematiskt informationssäkerhetsarbete torde det mot denna bakgrund kunna slås fast att revision och uppföljning är av avgörande betydelse.

I dag finns dock brister på området. Beroende på vilken aktör som uppvisar brister kan konsekvenserna av bristande säkerhet i informationshanteringen (bristande informationssäkerhetsarbete) även få följdverkningar för andra aktörer. Det handlar om ett brett

spektra av aktörer, såsom kunder, underleverantörer, bidragsmottagare och resenärer i alla delar av samhället.

När det gäller myndigheter och deras uppföljning har Riksrevisionen konstaterat i sin årsrapport från 2007 att den interna kontrollen behöver stärkas eftersom granskning visat på flera olika typer av svagheter i myndigheternas interna styrning och kontroll. Bland annat slås fast att de ”myndigheter som med hjälp av it hanterar samhällsviktig och känslig information måste ha en god informationssäkerhet”.

En konsekvens av svagheterna i myndigheternas interna styrning och kontroll konstaterade Riksrevisionen är att ”incidenter, till exempel virusattacker, medfört att medborgare och företag inte fått den service de förväntar sig. Brister i skyddet av webbplatser har också lett till att obehöriga fått tillgång till integritetskänsliga uppgifter.” Därefter konstaterar Riksrevisionen att dess granskningar visar på ”allvarliga brister i hur många ledningar styr och kontrollerar informationssäkerheten vid myndigheten”.

Ett av åtgärdsförslagen som Revisionen lägger fram till regeringen för att hantera detta är att ”klargöra myndigheternas ansvar för såväl intern kontroll som informationsskyldigheten gentemot regeringen”.

MSB:s kartläggning av myndigheternas informationssäkerhetsarbete

I MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10) ställs krav på statliga myndigheter under regeringen (med undantag för Regeringskansliet, Försvarsmakten, Kommittéväsendet och utlandsmyndigheterna) att arbeta systematiskt med informationssäkerhet. Föreskrifterna ställer uttryckliga krav på att myndigheterna ska införa ett ledningssystem för informationssäkerhet och uttryckliga krav på att ledningen löpande ska informera sig om arbetet samt minst en gång per år följa upp och utvärdera arbetet.

MSB genomförde under våren 2014 en kartläggning av hur de statliga myndigheterna tillämpade föreskrifterna i sitt informationssäkerhetsarbete. Resultatet har publicerats i en rapport, En bild av myndigheternas informationssäkerhetsarbete 2014, som visar att det fortfarande finns påtagliga brister när det gäller arbete

med att kontrollera efterlevnad. Endast 65 procent uppger att de kontrollerar hur myndighetens styrande dokument efterlevs, 26 procent anger att de inte gör en sådan kontroll och 9 procent uppger att de inte har några styrande dokument.

I rapporten konstateras också att ”mindre än hälften av myndigheterna uppger att de alltid, eller i stor utsträckning, dokumenterar granskningar och säkerhetsåtgärder av större betydelse som har vidtagits”. När det gäller ledningens roll visar resultatet att knappt hälften av myndigheternas ledning i stor utsträckning håller sig löpande informerade om arbetet respektive följer upp informationssäkerhetsarbetet åtminstone en gång per år. Den höga svarsfrekvensen i undersökningen gör de redovisade resultaten signifikanta och extra intressanta.

Behov av ett tydligare regelverk

Sammantaget kan dels konstateras att uppföljning och revision är en nödvändig förutsättning för ett systematiskt informationssäkerhetsarbete, dels konstateras att det fortfarande finns brister. När det gäller statliga myndigheter kan noteras att de brister som Riksrevisionen pekat på, trots att det sedan ett antal år tillbaka ställs tydligare krav på informationssäkerhetsarbetet hos statliga myndigheter, fortfarande till del finns. Detta gäller även med all sannolikhet såväl den kommunala nivån som landstingen. I detta ska också beaktas att leverantörerna av it-tjänster till det offentliga i huvudsak består av privata företag, vilket gör att även dessa på olika sätt måste omfattas av informationssäkerhetsarbetet.

Samhällsutvecklingen och det ökande beroendet av fungerande informationshantering samt den nu allt mer utbredda avsaknaden av alternativ till informationshantering med hjälp av it-system gör att vikten av ett informationssäkerhetsarbete som får faktisk effekt för skyddet av information har ökat betydligt. Detta innebär samtidigt att de brister som påvisats i uppföljning och revision av säkerhetsarbetet kan potentiellt sett få allt större konsekvenser för allt fler.

Regelverket som i dag reglerar revision, både inom privat och inom offentlig sektor, kan förtydligas. Givet de brister som påvisats och ovan redovisats finns det skäl att se närmare på dessa möjligheter. Här

behöver dock skiljas på reglerna för extern revision, som exempelvis görs av Riksrevisionen, och intern revision. Det är särskilt reglerna för intern revision som upplevs uppvisa brister i dag.

Förvaltningsmyndigheter under regeringen

När det gäller förvaltningsmyndigheter under regeringen styrs internrevisionen av internrevisionsförordningen (2006:1228). Enligt 4 § nämnda förordning ska internrevisionen ”utifrån en analys av verksamhetens risker självständigt granska om ledningens interna styrning och kontroll är utformad så att myndigheten med en rimlig säkerhet fullgör de krav som framgår av 3 § myndighetsförordningen (2007:515)”.

Som framgått har behovet av att skydda information blivit en allt viktigare angelägenhet för myndigheterna. Att i en sådan situation säkerställa att internrevisionen beaktar även informationssäkerhetsfrågorna har potential att öka fokus på frågorna och skapa än förbättrade förutsättningar för att ett systematiskt informationssäkerhetsarbete som får faktisk effekt kan bedrivas. Utredningen föreslår därför att det i förordningen (2000:605) om årsredovisning och budgetunderlag införs en bestämmelse om att till årsredovisningen en tilläggsupplysning ska lämnas om genomförd internrevision och status för informationssäkerhetsarbete på myndigheten.

Ett alternativ vore att i myndighetsförordningen (2007:515) införa en bestämmelse om att myndighetens ledning ansvarar för att upprätthålla säkerhet i sin informationshantering.

9.3 Staten som tydlig kravställare

Informationssäkerhetsproblematiken når samhällets alla delar och nivåer. Privat och offentlig sektor är en del av och drabbade av samma informationssäkerhetsproblematik. Båda sektorerna kan också bidra till att förbättra situationen på olika sätt.

De överväganden och förslag som utredningen redovisar i betänkandet rör statens eget agerande. Detta innebär inte att utredningen anser att tyngdpunkten i informationssäkerhetsarbetet ska ligga där. Som nämnts i det inledande avsnittet ska förslagen

snarare ses som ett första steg som avser att åtgärda de mest angelägna bristerna i den centrala statsförvaltningen.

I detta avsnitt redovisas hur utredningen anser att staten bör utveckla beställarkompetensen avseende hantering och överföring av information i elektroniska kommunikationsnät och it-system. Syftet är att få tillfredsställande it-lösningar och samtidigt förenkla och sänka kostnader för tjänster och produkter.

Utifrån sammanfallande intressen inom informationssäkerhetsområdet tas hänsyn till näringslivets behov samtidigt som staten bygger sin informationssäkerhet. Detta kan ske genom att samtalet mellan näringslivet och regeringen med dess myndigheter fördjupas.

9.3.1 Kravställning vid upphandling

Förslag:
1) Statlig upphandling ska innehålla hänvisning till för staten gällande standarder och krav på certifiering i de situationer där säkerhetsnivåer har fastställts för respektive verksamhet.
2) Myndigheten för samhällsskydd och beredskap (MSB) ges i uppdrag att ta fram skyddsprofiler som anger minimikrav på säkerhet i vanligt förekommande it-produkter som används av statliga myndigheter.
3) Det bör införas ett krav på att rapportera vilken leverantör som en statlig myndighet valt då ramavtal rörande it-lösningar används.
4) Avseende tjänster och produkter att användas för kommunikation inom staten, bör upphandlande myndighet överväga möjligheten att tillämpa lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet, om upphandling enligt lagen (2007:1091) om offentlig upphandling inte medger nödvändigt kravställande.

It-standarder och krav på certifiering

En grundförutsättning för dagens informationssamhälle är säkerheten i informationssystemen. All användning av informationsteknik är starkt beroende av att it-produkter och it-tjänster har säkerhetsegenskaper som ger det skydd som krävs och utlovas. Eftersom nationellt godkända system inte kan omhänderta hela samhällets behov i stort bygger de allra flesta säkerhetslösningar på allmänt tillgängliga kommersiella produkter, så kallade COTS (Commercial of the shelf). Fördelarna med COTS är att det finns ett stort utbud och anskaffningen är enkel. Nackdelarna i jämförelse med nationellt godkända produkter, är att myndigheter måste förlita sig på att produkter håller de säkerhetsegenskaper som leverantören utlovat.

I dag pågår ett flertal internationella initiativ för att ta fram standarder och rekommendationer för hur man skapar it-säkerhet i produkter. Ett sätt att skapa en kommersiellt driven process för att tillgodose samhället med kryptolösningar med tillräcklig kvalitet är att låta kommersiella aktörer bekosta evalueringar av sina produkter genom internationellt erkända certifieringssystem som Common Criteria (CC) inom ramen för CCRA- överenskommelsen. Angående Common Criteria.

Upphandling

När en organisation väljer att upphandla nya it-lösningar som till exempel system, molntjänster eller outsourcing av it-drift ska det föregås av en riskanalys eftersom det påverkar informationssäkerheten. En väl genomförd upphandling kan ha positiva säkerhetseffekter inte bara på det system eller den tjänst som upphandlas utan även i ett vidare perspektiv. Ett exempel på detta är att det generella säkerhetsmedvetandet kan höjas när de informationshanteringsprocesser som ska stödjas analyseras och behovet av säkerhet fastställs. Å andra sidan kan upphandlingar som sker utifrån ett otillräckligt underlag leda till att organisationens säkerhet avsevärt försämras för lång tid framåt. Med tanke på att upphandling av it-relaterade tjänster blir allt vanligare får upphandling också en alltmer framskjuten plats i informationssäkerhetsarbetet.

För att möta detta behov har MSB tillsammans med Kammarkollegiet tagit fram ett stöd riktat till myndigheter, kommuner och landsting i form av en vägledning *Vägledning – informationssäkerhet i upphandling* (Publ.nr MSB555). Även PTS har tagit fram en vägledning för att ge stöd vid anskaffning av extern elektronisk kommunikation, exempelvis internetanslutning och telefoni *Robust elektronisk kommunikation – vägledning för användare vid anskaffning* (PTS-ER-2011:16). Som en fördjupning har också ett par avgränsade studier *Outsourcing av it-tjänster i kommuner* (publ.nr MSB728) och *Informationssäkerhet i Kammarkollegiets ramavtal* (dnr 2013-3300) genomförts som båda visar att den offentliga upphandlingen av system och it-relaterade tjänster har stora brister. Studierna har dels rört hur ett antal myndigheter, ett landsting och en offentlig intresseorganisation formulerat krav på säkerhet när de använt Kammarkollegiets ramavtal för it-drift, dels hur kommuner uppfattar möjligheterna att genomföra upphandlingar där säkerhet är inkluderad. Sammanfattningsvis kan sägas att studierna indikerar att det finns omfattande svårigheter både för statliga myndigheter och kommuner att formulera initiala krav vid upphandlingen men också att upprätthålla en beställarkompetens under hela den tid som avtal gäller. Det är sannolikt inte heller helt tydligt för de myndigheter som nyttjar Kammarkollegiets ramavtal att hela ansvaret för att formulera säkerhetskrav ligger på varje enskild myndighet. Sannolikt finns det outtalade förväntningar både på ramavtalet och på leverantörerna om att säkerhetsaspekterna ska beaktas på ett generellt plan vid upphandlingarna utan att kunderna behöver genomdriva egna villkor. Osäkerheten kring säkerhetsaspekter vid upphandling bör ses i ljuset av att var och en av myndigheterna, landstingen och kommunerna är sällan-köpare av it-lösningar där flertalet knappast kan förväntas kunna ha hela den kompetens som krävs för att upphandla säkerhet i den egna organisationen. Intrycket av att uppgiften att säkerställa god informationssäkerhet vid upphandlingar uppfattas som svårlöst stärks i tidigare refererad rapport från MSB *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter* (avsnitt 7.4.2).

Utöver den bristande säkerhet som blir följden av ovanstående förhållanden leder oklarheterna också till att den utvecklingspotential som finns hos leverantörerna inte utvecklas. Till skillnad

mot flertalet av de offentliga kunderna finns hos leverantörerna en hög kompetens att utveckla it-lösningar. Denna kompetens skulle kunna tas i anspråk även för att inkludera standardiserade säkerhetslösningar vilket skulle vara ekonomiskt fördelaktigt för både kund och leverantör. Förutsättningen för detta är en mer standardiserad kravställning från de offentliga aktörerna. Här finns det anledning att peka på den gemensamma nationella styrmodell som föreslås i avsnitt 9.2.1 och som bl.a. ska innehålla ett ramverk med gemensamma skyddsnivåer kopplade till informationsklassning. Leverantörerna får genom skyddsnivåerna möjlighet att utveckla standardiserade paketlösningar som kunderna kan välja utifrån sin informationsklassning. Vid sidan om den möjliga ekonomiska rationalisering som ligger i en sådan lösning blir även kraven på heltäckande kompetens hos kunderna mindre eftersom de inte behöver detaljera sina kravställningar utan snarare välja en fastställd skyddsnivå. Ytterligare en vinst är att kontroll av efterlevnad avseende leverantörerna skulle kunna samordnas eftersom kraven skulle vara i huvudsak de samma.

Samma ramverk bör även användas då myndigheter och kommuner samverkar i gemensamma it-lösningar. Av utredningens kontakter med MSB har framgått att den nuvarande situationen bedöms oroande då kravställningen och ansvarsfördelningen i dessa relationer förefaller vara ännu mer eftersatta än i de kommersiella relationerna. Det saknas för närvarande också former för att reglera parternas ansvar på ett effektivt sätt. Dessutom saknas incitament för att följa upp ingångna överenskommelser vilket gör motivationen att utarbeta avtalsliknande förbindelser låg.

Koncentration av leverantörer

På nationell nivå blir hot- och riskbilden aggregerad då allt större informationsmängder samlas hos ett fåtal leverantörer. Att det är ett fåtal leverantörer beror både på att den svenska marknaden är begränsad och är en konsekvens av de krav som finns i lagen om offentlig upphandling vilka leder till formell begränsning i mångfald leverantörer. Statliga myndigheter är hänvisade till att sköta sina upphandlingar via Kammarkollegiets ramavtal som i praktiken leder till att det i huvudsak är tre stora leverantörer som levererar

exempelvis drifttjänster. MSB har i den rapport som togs fram i samband med den så kallade Tieto-incidenten *Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter* (Publ.nr. MSB367) lyft fram risken med den starka koncentrationen eftersom en it-incident hos en av dessa kan få mycket vittomfattande konsekvenser på samhällsnivå. I en nyligt publicerad rapport från MSB förstärks denna bild. I rapporten *It- och informationssäkerhet i Sverige. Erfarenheter och reflektioner från några större it-incidenter under 2012–2014* (publ.nr: MSB721 – januari 2015) beskrivs fem fall av it- och informationssäkerhetsincidenter, som inträffat i Sverige de senaste tre åren och där samhällets informationshantering påverkades kraftigt. Trenden mot koncentration stärks ytterligare av att de nationella tjänster och myndigheter, som exempelvis Statens servicecenter har sina tjänster placerade hos i huvudsak samma leverantörer. Ett första steg för att reducera riskerna för ökad koncentration på leverantörssidan är att införa ett krav på myndigheterna att återrapportera vilken leverantör som valts då ramavtal rörande it-lösningar används. Utredningen föreslår därför att MSB bemyndigas att meddela föreskrifter om ett rapporteringskrav. Ett sådant bemyndigande föreslås i 20 § förordningen för statliga myndigheters informationssäkerhet, se avsnitt 9.2.3. Det bör därvid utredas om det finns ett behov av samordning avseende till vilken myndighet som återrapportering ska ske när det gäller it-produkter som omfattas av säkerhetsskyddslagens krav.

Utvecklad beställarkompetens

Som vi konstaterat ovan är beställarkompetensen för informationssäkerhet alltför svag, vilket är ett grundläggande problem. Ägarna och användarna av samhällskritisk infrastruktur måste först och främst inse att den infrastruktur de äger respektive nyttjar i många delar är kritisk, att den behöver skyddas, att skyddet inte enbart ska vara fysiskt utan även av informationssäkerhetsskydd. Om beställaren är medveten om vad som krävs av ett bra informationssäkerhetsskydd så är det också möjligt att definiera skyddet, anpassa det och upphandla. En metod att utveckla beställarkompetensen kan vara att använda en gemensam standard för informationssäkerhet.

Tillgång till certifierade produkter enligt evalueringskriterier för it-säkerhet, Common Criteria (CC), eller för tjänster enligt Ledningssystem för informationssäkerhet (LIS) underlättar upphandling av informationssäkerhet. CC tillämpas redan inom flera olika sektorer, exempelvis försvar, finans, sjukvård, transport och kommunikation.

Staten har ett ansvar för att utveckla beställarkompetensen. Det kan bland annat ske genom att successivt infoga kravet på certifiering vid upphandling men också genom tillämpning av kvalitetskraven i LIS.

Utveckling av informationssäkerhet med stöd av internationellt accepterade standarder är en konstruktiv metod för att skapa tillit och förtroende såväl inom en organisation som mellan olika parter. Den möjliggör också en meningsfull revision av säkerheten, eftersom revisionen kan ske gentemot definierade mål och kvalitetsrutiner, se avsnitt 9.2.5.

Utredningen anser att statliga upphandlingar ska innehålla hänvisningar till it-standarder och krav på certifiering i de situationer där säkerhetsnivåer har fastställts för respektive verksamhet. Därmed kan samma krav som ställs på myndigheterna genom den föreslagna förordningen för statliga myndigheters informationssäkerhet även omfatta leverantörer av it-produkter (CC-certifierade) i samband med upphandling, se avsnitt 9.2.3. Detta medför också att det ställs krav på sådana produkter som ska upphandlas och användas i samhällsviktig verksamhet som bedrivs av staten.

Krav på it-säkerhet i it-produkter kan ställas i form av skyddsprofiler som följer CC-standarden. Sådana skyddsprofiler beskriver kraven på olika typer av it-produkters säkerhetsegenskaper. MSB skulle tillsammans med berörda myndigheter och leverantörer kunna utveckla de skyddsprofiler som anger olika it-produkters minsta tillåtna säkerhetsnivå. I den föreslagna styrmodellen (se avsnitt 9.2.1) kan hänvisning ske till sådana skyddsprofiler. Härigenom skulle minimikrav för olika typer av it-produkters säkerhetsegenskaper kunna anges. Upphandlande myndighet som ska tillämpa styrmodellen kan kräva att leverantörerna certifierar sina produkter mot kraven som formulerats i dessa skyddsprofiler. Upphandlande myndigheter och Statens inköpscentral kan referera till skyddsprofilerna i ramavtal. Leverantörer av produkterna kan få sina

produkter certifierade mot dessa krav och därmed få åtkomst till den stora myndighetssektorns marknad. På detta sätt undviks att oseriösa leverantörer med produkter med dålig säkerhet och lägre pris konkurrerar ut leverantörer med en mer medveten säkerhetsinriktning med potentiellt högre utvecklingskostnad.

Utredningen föreslår därför att MSB ges i uppdrag att ta fram skyddsprofiler som anger minimikrav i vanligt förekommande it-produkter som används av statliga myndigheter. Vid utvecklingen av skyddsprofilerna kan samverkan ske med berörda myndigheter och representanter för näringslivet. Detta förslag innebär en betydande förstärkning av beställarnas förmåga att ställa tydliga och relevanta krav på it-produkters säkerhet.

En satsning på tydligare hänvisning till standarder och krav på certifiering kan medföra större behov av i förväg utpekade evalueringslaboratorier.

Möjligheten att tillämpa lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS)

Lagen (2007:1091) om offentlig upphandling (LOU) utgör den generella regleringen avseendet det allmännas upphandling. Det finns möjligheter inom LOU-systemet att ställa krav avseende t.ex. informationssäkerhet i de tjänster eller produkter som ska upphandlas, (se MSB:s rekommendationer.) I en framtid där statliga myndigheter enligt föreskrifter är skyldiga att rapportera inträffade it-incidenter är det troligt att ett stående krav vid upphandling av it-tjänster kommer att vara att leverantören ska rapportera alla incidenter av visst slag.

Då LOU-systemet tenderar att gynna det lägsta priset när andra faktorer är lika, är det av största vikt att myndigheter som avser upphandla tjänster eller produkter som ska garantera informationssäkerhet och skydd för den information som myndigheten enligt offentlighets- och sekretesslagen (2009:400) är skyldig att hantera på särskilt sätt, alltid utnyttjar möjligheter till kravställande i enlighet med de standarder som framförallt MSB:s föreskrifter kräver att myndigheten följer.

Om upphandlande myndighet efter att ha uttömt de möjligheter till kravställande som LOU medger likafullt inte anser att upphandling kan ske med erforderliga garantier för säkerhet i staten

kan myndigheten i stället överväga att använda upphandlingsförfarandet enligt lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS). Lagen är avsedd för upphandlingar av materiel och tjänster som är av så känslig natur att upphandling enligt LOU eller lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster inte lämpar sig. LUFS är i stort sett parallell till dessa två lagar men till skillnad från dem innehåller LUFS bestämmelser om informationssäkerhet, försörjningstrygghet och underentreprenad. Lagen genomför huvudsakligen Europaparlamentets och rådets direktiv2009/81/EG.

9.3.2 Fördjupad dialog mellan privat och offentlig sektor

Förslag: Regeringen fördjupar dialogen mellan privata och offentliga aktörer.

Näringslivets roll

Den tekniska utvecklingen på it-området är i allt väsentligt styrd av olika privata aktörer på marknaden. Tekniska framsteg omsätts mycket snabbt i olika produkter och tjänster. På motsvarande sätt expanderar marknaden för informationssäkerhet inom offentlig och privat verksamhet och omfattar också ett stort antal sektorer. Datorisering av de system som förser samhället med bränsle, el, värme, vatten och transporter sker i snabb takt och är i huvudsak privatägd. Tillverkarnas produkter och system styrs av programvaror och blir i allt högre grad uppkopplingsbara över elektroniska kommunikationsnät för styrning, övervakning, service m.m. Därmed ställs höga krav på den gemensamma infrastrukturen när det gäller leveranssäkerhet och kvalitet. En utveckling av informationsförsörjningen i alla dessa avseenden förutsätter att ett antal säkerhetsproblem löses. Dessutom har såväl privata som statliga aktörer likartade problem och behov i den dagliga verksamheten, vilket också kan ligga till grund för utbyte av praktiska erfarenheter.

Näringslivet har även en betydelsefull roll som den största ägaren och förvaltaren av samhällsviktig informationsinfrastruktur.

Upphandling av it-relaterade tjänster blir allt vanligare och får därmed också en framskjuten plats i informationssäkerhetsarbetet.

Tillgången till och användningen av olika typer av standarder är av utomordentligt stor betydelse inom informationstekniken och det är it-leverantörer som i hög grad har svarat för krav och standarder i de system som används i offentlig förvaltning. Vidare finns det standarder så som exempelvis SS-ISO/IEC 27001 Ledningssystem för informationssäkerhet som ligger till grund för systematiskt informationssäkerhetsarbete hos såväl den privata som den offentliga sektorn. Utredningen konstaterar att standardisering vid sidan av reglering är ett kraftfullt styrmedel när det gäller informationssäkerhetsarbetet som flera aktörer har ett delat intresse av.

Samverkan mellan privat och offentlig sektor genom dialog

Det är viktigt att ta till vara det engagemang för informations- och cybersäkerhetsfrågor som redan finns inom näringslivet, i synnerhet den del av näringslivet som bedriver samhällskritisk verksamhet, och att öka medvetenheten kring konsekvenserna av it-incidenter. Hoten mot elektroniska kommunikationsnät och it-system är mångfacetterade, komplexa, svårdefinierade och föränderliga (jfr avsnittet om hot och risker 4.4). Det är också så att informationssäkerheten inte är ett problem som kan lösas en gång för alla, utan arbetet med att värna om informationssäkerheten i samhället måste ske i en kontinuerlig process. Eftersom den tekniska utvecklingen i huvudsak finns på marknaden så är det också där ifrån man kan förvänta sig säkerhetslösningar. Staten får här en viktig roll som tydlig kravställare på informationssäkerhet i olika offentligt finansierade verksamheter. Detta ställer samtidigt krav på offentliga sektorn att kunna nivåanpassa tillgänglighet och skydd. Det borde därför inom flera olika sektorer utvecklas samverkan genom kontinuerlig dialog mellan privata och offentliga aktörer.

Utredningen anser att regeringen med stöd av det föreslagna myndighetsrådet bör inleda en dialog med centrala näringslivsorganisationer och andra intresseorganisationer. Den överordnade målsättningen med en dialog är att stärka informationssäkerheten i samhället, särskilt avseende de delar som berör den kritiska infrastrukturen. Alla ägare eller leverantörer av komponenter till kritisk

infrastruktur i offentlig och privat sektor bör bjudas in till dialog, liksom aktörer som, utan att vara ägare, är kravställare på nationell, regional och lokal nivå. Ett övergripande syfte med dialogen är att skapa förståelse och beredskap för de krav staten kan komma att ställa i anslutning till upphandlingar, och att det från statens sida skapas en motsvarande förståelse för exempelvis standardiserings- och certifieringsarbetet i näringslivet. Utredningen vill betona att förslaget inte syftar till att ersätta existerande samverkansforum utan att fördjupa den dialog som redan finns.

Förslag på dialogområden

Ett dialogområde skulle kunna handla om hur det skapas it-lösningar som uppfyller olika behov av tillgänglighet och skydd, och som även är kostnadseffektiva.

Att tydliggöra hur säkra och kostnadseffektiva it-lösningar kan tas fram för olika centrala it-komponenter i samhällsviktig verksamhet är av största vikt för att samhällsviktig verksamhet ska kunna motstå olika former av störningar. Detta är en central del av en långsiktig satsning på informationssäkerhet. Delar av arbetet behöver ske i internationella samverkansforum men även i dialog med näringslivet.

Utredningen återkommer i senare avsnitt till behovet av att regeringen även inleder dialog med näringslivet i frågor om svensk kryptoindustri och kryptologisk kompetens (se avsnitt 9.4.2) och även kompetensförsörjningen inom området (se avsnitt 9.8.2).

9.4 Säkrare kommunikation i staten

9.4.1 Statliga nätverk

Förslag:
1) Samtliga myndigheter som anges i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap ansluts till kommunikationssystemet Swedish Government Secure Intranet (SGSI).
2) Under utbyggnaden av SGSI bör lämpliga åtgärder vidtas för att utveckla sensorteknik.
3) Statliga myndigheter ska använda samma synkroniserade tidsskala för de tidsangivelser de använder i sina it-system.

Statens behov av skyddade och tillgängliga kommunikationer

I takt med att samhället blir alltmer beroende av modern teknik, minskar toleransen för avbrott och andra störningar. Informations- och kommunikationssystem är en viktig och avgörande resurs inom i stort sett all samhällsverksamhet. Efter hand som e-förvaltningen etableras får många offentliga aktörer dessutom allt större behov av att elektroniskt förmedla stora mängder information sinsemellan. Detta ökar bl.a. kraven på tillgängliga och skyddade kommunikationsinfrastrukturer.

Hoten mot den globala, digitala informations- och kommunikationsinfrastrukturen representerar stora ekonomiska och säkerhetsmässiga utmaningar för samhället. Samhällets beroende av denna infrastruktur innebär att det ytterst också finns en säkerhetspolitisk dimension.

Kris- och krigsviktig verksamhet och kritisk infrastruktur måste kunna skyddas för att kunna utveckla planeringen för att lösa uppgifter inför och under höjd beredskap. Civila aktörer behöver ha en förmåga att dela skyddsvärd information t.ex. då de deltar i arbetet med gemensamma planeringsfrågor, deltar i övningsverksamhet eller deltar i beslutsfattande. Information som är väsentlig inför och under höjd beredskap ska identifieras, klassas och därefter skyddas utifrån informationssäkerhetens aspekter konfidentialitet, riktighet, tillgänglighet och spårbarhet. En viktig fråga är att tillgo-

dose tillgängliga och skyddade kommunikationslösningar som möter kraven för att kunna dela skyddsvärd information eller information som omfattas av sekretess.

Flera länder har skapat övergripande strukturer för koordinering och samverkan i syfte att säkerställa kommunikationen inom den offentliga sektorn, med samhällsövergripande samverkansfunktioner och nya gemensamma lösningar. Flera länder redovisar också bedömningar om att de totala kostnaderna för den offentliga sektorns it-behov kan minskas tack vare de vidtagna åtgärderna. Det är rimligt att anta att motsvarande effekt skulle kunna uppnås även i Sverige. Att inte agera gemensamt inom offentlig sektor leder till att nuvarande fragmenterade arbetssätt cementeras. Riskerna blir svåra att överblicka. Småskaliga lösningar blir divergerande och kostnadsdrivande vilket inte ligger i linje med den digitala agendan som syftar till en effektiv användning av offentliga it-resurser.

I Sverige finns i dag ett stort behov av myndighetsgemensamma infrastrukturer för säker kommunikation som ett verktyg för svenska myndigheters informationshantering. Merparten av myndigheternas informationshantering sker i dag via publika system. Stora delar av den information som hanteras, såväl i form av datatrafik som tal, är skyddsvärd. Den publika infrastrukturen som används omfattas inte av något kontrollerat eller dimensionerat säkerhetsskydd.

Dessa bristande möjligheter till att på ett säkert sätt dela och bereda skyddsvärd information leder till såväl effektivitets- som säkerhetsbrister för svenska myndigheter. Problemet är i dag inte avgränsat till kommunikation mellan myndigheter utan omfattar, delvis som en följd av ökad mobilitet, även myndigheters interna verksamhet.

Ett väl utbyggt och säkert myndighetssamband skulle medföra stora vinster med avseende på myndigheters informations- och cybersäkerhet genom att information kan sändas via skyddad infrastruktur under myndigheternas kontroll. Verksamhetsnytta skulle levereras genom att ge möjligheter till realtidsberedning och delgivning, mellan och inom myndigheter, av skyddsvärd information som i dag enbart kan hanteras via fysisk förmedling eller med stora hot mot informationens integritet.

Utvecklade kommunikationssystem för säkrare kommunikation i staten

Staten äger i dag fysisk kommunikationsinfrastruktur såsom i exempelvis Teracom AB, Trafikverket, Affärsverket svenska kraftnät och MSB genom Rakel-systemet. Detta är resurser som är möjliga att kontrollera och strategiskt viktiga för vissa myndigheters verksamhet. Försvarsmaktens myndigheters behov av att kunna kommunicera säkert tillgodoses exempelvis av Försvarets Telenät (FTN). Ett praktiskt möjligt och kostnadseffektivt sätt att skapa en myndighetsgemensam infrastruktur för andra myndigheters behov är att bygga på redan etablerade strukturer. Swedish Government Secure Intranet (SGSI) är ett samarbete mellan anslutna myndigheter där MSB är systemägare och utgörs av ett kommunikationssystem som ger säker kommunikation mellan myndigheter i Sverige och i Europa. SGSI är logiskt skilt från det publikt tillgängliga internet och trafiken är krypterad (med nationellt godkända kryptosystem) samt utformat för att klara höga krav på tillgänglighet och driftsäkerhet. Inom Sverige använder myndigheter SGSI som ett tillräckligt säkert system för utbyte av känslig information och minskar därmed risker kopplat till att skicka information över internet. SGSI används bland annat för att få åtkomst till olika databaser hos de olika anslutna myndigheterna och förutom vanlig datatrafik ingår även tjänster som skyddad videokonferens och skyddad e-post. SGSI är också anslutet till EU:s säkerhetsskyddade kommunikationsnät sTesta (secure Trans European Services for Telematics between Administrations) vilket medger kommunikation med andra EU-stater och myndigheter. sTESTA uppfyller EU-rådets och EU-kommissionens föreskrifter för hantering av information klassificerad som EU RESTRICTED. Myndigheter som vill kommunicera med EU-administrationen eller med en annan medlemsstat genom sTESTA måste vara anslutna till SGSI. SGSI är Sveriges enda system med koppling till sTESTA och uppfyller EU-rådets och EU-kommissionens föreskrifter för hantering av information.

För att skapa en myndighetsgemensam infrastruktur för elektroniska kommunikationer behöver SGSI utvecklas. I dag är det frivilligt för offentliga aktörer att ansluta sig till SGSI och kommunikationssystemet är inte baserat på statligt ägd fysisk

infrastruktur. Till detta kommer att anslutna myndigheter inte heller alltid använder alla de tjänster som tillhandahålls via SGSI. Exempelvis skickas inte e-post per automatik över SGSI även om möjligheten finns (s.k. mail relay).

I ett första steg bör samtliga myndigheter som pekas ut i bilagan till förordning (2006:942) om krisberedskap och höjd beredskap (KBF) anslutas till SGSI. De myndigheter som särskilt pekas ut i KBF har en särskild roll i krishanteringssystemet och behöver kunna samverka även under ansträngda förhållanden. Dessa myndigheter har ett utvecklat säkerhetsmedvetande och arbetar systematiskt med informationssäkerhet.

Vid utbyggnaden av SGSI bör det också övervägas att utveckla ett fysiskt nät som i huvudsak är baserat på statligt ägd infrastruktur. Detta utesluter dock inte andra alternativ när staten ska lösa behovet av säker kommunikation. Val av infrastrukturlösning bör enligt utredningen föregås av en behovsanalys, följd av en analys av hot och risker. Utifrån denna kan designkrav och krav på tekniska lösningar, robusthet och skyddsåtgärder utarbetas. Sannolikt kan mer än ett nät behövas för att uppfylla behoven och samtidigt upprätthålla tillräcklig säkerhetsnivå. Analysen kan också leda till insikt om nya hot som det finns skäl att beakta särskilt.

Som tidigare nämnts äger staten i dag fysisk kommunikationsinfrastruktur såsom i exempelvis Teracom AB, Trafikverket, Affärsverket svenska kraftnät och MSB genom Rakel. Detta är resurser som är möjliga att kontrollera och strategiskt viktiga för vissa myndigheters verksamhet. Utredningen om effektivare användning av statens bredbandsinfrastruktur (N 2014:05) ser för närvarande över möjligheterna att effektivisera användningen av de statligt ägda bredbandsnäten genom förbättrad samordning mellan de statliga aktörerna. Bland annat ingår det i uppdraget att analysera om, och i så fall på vilket sätt, en förbättrad samordning mellan de statliga aktörernas bredbandsverksamheter kan bidra till ökad säkerhet och robusthet i de statliga aktörernas kommunikationsnät. Ett utvecklat SGSI som i huvudsak baseras på en statligt ägd infrastruktur skulle med fördel kunna användas som fundament till ett statligt mobilt bredbandsnät för samhällsviktig verksamhet.

Vidare kan det tillföras ett antal mer tekniska lösningar för att öka skyddet i en myndighetsgemensam kommunikationsinfrastruktur. Här kan bl. a. nämnas robusta domännamnsservrar DNS,

DNSSEC och skyddad e-post, vilket ger högre tillgänglighet och även möjliggör insynsskyddad kommunikation mellan deltagande organisationer. Det försvårar exempelvis kartläggning av enskilda myndigheter och ger möjligheten att prioritera trafik. Sedan bör det även tillses att myndighetsnätet har gemensamma utgångar mot internet med tekniska skyddsmekanismer. Motsvarande lösning är redan införd i Tyskland och obligatorisk för alla anslutna myndigheter. Till detta kommer även en gemensam tidssynkronisering för spårbar tid i loggar, e-post etc. Dessa tekniska förutsättningar ger stöd för bibehållen nationell trafik även vid fragmentering och störningar i omgivande internet.

Ytterligare viktiga förutsättningar för att stödja arbetet med en statlig kommunikationsinfrastruktur är sensorer till stöd för it-incidenthantering, obligatorisk it-incidentrapportering och lägesbeskrivningar, se vidare nedan. I en skyddad kommunikationsinfrastruktur är det också centralt att använda nationellt godkända kryptosystem.

Sensorsystem

It-relaterade hot mot svenska intressen och organisationer har utvecklats och blivit mer sofistikerade. Detta skapar ökande behov av en förmåga att identifiera och hantera it-säkerhetsincidenter samt skapa en rättvisande nationell lägesbild. Av denna anledning ökar nu behovet av att främja sådana sensornätverk som har till syfte att stödja samhällets och organisationernas informationssäkerhet. Sensorsystem beskrivs i avsnitt 7.5.2. Sensornätverk kan ge underlag för att skapa en lägesbild, generera statistik och rapporter samt bidra till att höja medvetandet angående it-säkerhet hos anslutna organisationer.

Sverige, till skillnad från sina grannländer Norge, Finland och Danmark saknar i dag nationella sensorsystem kopplade till ansvariga myndigheter. Denna brist på nationella sensorsystem i Sverige innebär med stor sannolikhet att ett stort antal allvarliga it-incidenter aldrig upptäcks, eller upptäcks för sent. De legala frågorna med koppling till sensorsystem och dess utformning samt användning kräver i vissa delar närmare analys. Exempelvis, ett sensorsystem kan vara av avgörande betydelse i arbetet med att upptäcka intrång där angriparen kommer åt känslig information genom att få användare i en

organisation att ladda ned skadlig kod som automatiskt läser av och skickar ut informationen till en mottagare utanför organisationen. Sensorsystemet upptäcker denna attack genom att identifiera den mottagande IP-adressen som en sådan IP-adress som tidigare använts just i detta syfte. Insamling och hantering av IP-adresser inom ramen för sensorsystemet är därför centralt för att upptäcka denna typ av angrepp. Genom att IP-adresser kan vara personuppgifter så behöver personuppgiftslagens regler om ändamål, informationsplikt med mera i förhållande till denna typ av uppgifter beaktas. En annan rättslig aspekt som det är oklarheter kring är möjligheten för en myndighet att säkerställa att insamlad information omgärdas av sekretesskydd eller inte. Det finns därför skäl att analysera följande rättsliga frågor:

– När är det ur ett personuppgiftsskyddsperspektiv acceptabelt att med hjälp av ett sensorsystem samla in och behandla personuppgifter för ett informationssäkerhetsändamål?
– Hur bör informationsplikten i 23 § personuppgiftslagen hanteras vid insamling av nya skadliga IP-adresser?
– Vilka möjligheter finns det att med stöd av sekretessregler skydda information som samlats in med stöd av ett sensornätverk?

Spårbar tid

En okomplicerad och allmänt tillgänglig spårbar nationell tidsskala är en viktig del i arbetet med att skapa tillit till it-samhället – framför allt när vi talar om samhällsviktiga funktioner och e-förvaltning. Korrekt och spårbar tid är också en förutsättning för ett högteknologiskt samhälles förmåga att fungera såväl till vardags som vid svåra påfrestningar. Detta leder till behovet av ett nationellt uthålligt och robust system för tid- och frekvenssynkronisering för att minska Sveriges beroende av satellitsystem som GNSS, eller andra för störningar känsliga radiobaserade system för sådan synkronisering eftersom dessa system i huvudsak kontrolleras av en annan nation.

Spårbar tid kan i dag hämtas via internet från atomur placerade vid de större nationella knutpunkterna för internet. Genom att utnyttja den befintliga infrastrukturen för internet för överföring

av tid och frekvens parallellt med ordinarie trafik på nätet ökar robustheten och beroendet av radiobaserade metoder minskar.

Ur ett administrativt perspektiv bör krav på noggrannhet för tid byggas in redan från början när regler formuleras för olika typer av system. Det skulle spara mycket resurser och dessutom stödja rättssäkerheten. Inom många administrativa tillämpningsområden är det inte självklart uppenbart att korrekta tidsstämplar är väsentliga för en effektiv hantering av ärenden. Det är ofta först vid haverier, vid överklaganden eller liknande händelser som behovet av känd tidsnoggrannhet kan bli uppenbar och detta skapar stora kostnader som skulle kunna undvikas.

Behovet av spårbar tid och frekvens kan uttryckas på följande sätt:

- Spårbar tid för juridisk nytta
- Spårbar tid i samband med fel och funktionsstörningar
- Spårbar frekvens (takt) i kommunikation med andra systemkomponenter
- Spårbar tid för att säkerställa ansvar i affärsrelationer eller rättsprocesser som vid felaktig tid kan äventyra rättssäkerheten i samhället

En hög grad av automatisering är också starkt kopplat till tid och frekvens. Det medför att en del av säkerhetsarbetet i organisationer och företag alltmer inriktas på metoder för att förhindra störningar och manipulering av tid och frekvens vilket utgör ytterligare en aspekt.

Viktiga samhällsfunktioner har med åren kommit att bli mycket beroende av tillgång till spårbar tid- och frekvenssynkronisering. Flera av dessa funktioner skulle få omfattande problem om tillgången till sådan tid begränsades, vissa skulle sannolikt avstanna helt. Listan över sådana system går att göra lång. Utredningen lyfter här bara fram några få exempel för att ge en bild av behoven och vilken bredd de spänner över:

- Riksbankens transaktionshanteringssystem för tidsstämpling av transaktioner
- Banverkets signalsystem för trafikplanering och säkerhetsarbete

- Luftfartsverket flygledningssystem för trafikplanering och säkerhetsarbete, även internationell luftfart
- Gemensamt radiokommunikationssystem för skydd och säkerhet, Rakel, för dess tekniska funktion
- Svenska kraftnäts och andra nätbolags driftövervakningssystem för att övervaka och styra Sveriges eldistribution
- SWEPOS – Lantmäteriets referenssystem för positionering och som används för mark- och anläggningsarbeten
- Storstockholms lokaltrafik och vägtullar för trafikplanering, säkerhetsarbete men också betalningssystem med tidsgränser för olika taxor
- Basstationer för mobiltelefoni för teknisk funktion
- Gatubelysningsautomatik för styrning, trafiksäkerhet men också energihushållning

Denna problematik har även belysts i en rapport från MSB publicerad 2014, *Vikten av var och när – Samhällets beroende av korrekt tids- och positionsangivelse*.

Frekvensnoggrannheten för taktgivning i sådana nät är specificerad i olika standarder. När det gäller noggrannheten i tid för olika tillämpningar finns inte motsvarande standarder och som regel avstannar inte en kommunikation eller transaktion omedelbart även om en tidstämpel är felaktig. Den stora olägenheten och de stora kostnaderna uppstår i stället förmodligen främst vid incidenter eller driftstörningar då olika tidsstämplar måste justeras för att kunna relateras till varandra. Om det i en framtid handlar om mycket stora datamängder, om miljontals datafiler per sekund är den enda rimliga lösningen att ha tillräckligt korrekt tid från början.

Mot bakgrund av att tid och frekvens eller frekvenssynkronisering är extremt viktig i dagens samhälle föreslår utredningen att statliga myndigheter ska för sina tidsangivelser använda samma tidsskala samt ett uthålligt och robust system för tid- och frekvenssynkronisering.

9.4.2 Säkra kryptografiska funktioner

Bedömning och förslag: Frågan om säkra kryptografiska funktioner är mycket angelägen. På basis av den av Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk och Försvarsmakten föreslagna nationella strategin med åtgärdsplan för säkra kryptografiska funktioner bör regeringen ge de fyra myndigheterna i uppdrag utveckla processen för säkra kryptografiska funktioner.

Normalt överförs information över näten i klartext. Det är en flexibel lösning, som samtidigt gör det möjligt att till exempel avlyssna kommunikation, sända information i andras namn samt förvanska information. En metod för att skydda information är att använda kryptering. En säker nätkommunikation kräver flera olika sorters kryptografiska funktioner på flera olika nivåer. Kryptografiska funktioner kan användas för att uppnå konfidentialitet genom att endast den som har tillgång till ett visst kryptosystem och använd kryptonyckel har möjlighet att tyda eller förändra den information som skyddas av systemet. I många fall används kryptografiska funktioner enbart för att skapa elektroniska signaturer och för att identifiera komponenter och användare på ett säkert sätt. Genom elektroniska signaturer kan en avsändare av elektronisk information med olika grad av visshet identifieras och förvanskning av information, utan att detta upptäcks, försvåras.

I en skyddad kommunikationsinfrastruktur är det viktigt att det finns möjlighet att använda nationellt godkända kryptosystem om kraven på skydd motiverar detta. Arbetet med att skapa en skyddad kommunikationsinfrastruktur bör därför innefatta utveckling av nationellt godkända kryptosystem för ändamålet. I följande avsnitt kommer utredningen in på frågan om hur det kan utvecklas en process för säkra kryptografiska funktioner.

Åtgärdsplan för säkra kryptografiska funktioner

Informations- och kommunikationssystem är viktiga och strategiska resurser för alla organisationer, både internt och i samverkan med andra aktörer. För att skydda informationen i dessa system

kan kryptering användas. För staten är det särskilt viktigt att skydda hemlig information som rör rikets säkerhet eller utrikessekretess. Men samhället i stort har på senare år blivit alltmer it-beroende, ett beroende som i dag omfattar alla samhällssektorer. Andelen it-relaterade hot och risker mot kritisk infrastruktur och samhällsviktiga verksamheter ökar i omfattning. Samhället har i dag därför ett starkt och ökande behov av att skydda sin information i olika nivåer oavsett om informationen omfattas av sekretess eller inte. Att arbeta med denna typ av grundskydd innebär dock att det skapas en helt annan basplatta vad avser skydd för rikets säkerhet.

Samhällets förmåga till hantering och överföring av information i elektroniska kommunikationsnät och it-system, och Sveriges förmåga att upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur är beroende av vår kryptoförmåga.

Genom ett myndighetsgemensamt projekt mellan MSB, Försvarets radioanstalt (FRA), Försvarsmakten (FM) och Försvarets materielverk (FMV) har en rapport med förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner tagits fram och överlämnats till utredningen. Rapporten finns som bilaga 4 till betänkandet och innehåller förslag till en nationell strategi för kryptering. Rapporten innehåller även ett förslag till åtgärdsplan för hantering och överföring av information i elektroniska kommunikationsnät och it-system med hjälp av kryptering. Vidare föreslås övergripande mål för samhällets informationssäkerhetsarbete med avseende på användning av kryptografi. Det beskrivs även hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur med hjälp av kryptografiska funktioner.

Det är utredningens bedömning att den modell och de förslag som beskrivs i rapporten skulle kunna möta behovet av säkra kryptografiska funktioner på ett nytt sätt. Utredningen noterar att den samlade kompetensen på området står bakom förslagen och att rapporten utgör ett mycket gott underlag för regeringen att fatta beslut om ett gemensamt uppdrag till aktuella myndigheter att utveckla processen säkra kryptografiska funktioner. Frågan är mycket angelägen bl.a. eftersom säkra kryptolösningar är en nödvändig och fundamental faktor för att kunna etablera säker kommunikation och säkra it-lösningar i staten.

Svensk kryptoindustri och kryptologisk kompetens som dialogområde

Behovet av nationellt godkända kryptolösningar är stort, såväl för att skydda konfidentiell eller sekretessbelagd information. Förmågan att ta fram sådana system finns i dag i Sverige genom den samlade kunskap som finns hos de svenska kryptotillverkarna och de svenska myndigheter som bidrar med kryptologiska kunskaper vid utveckling och granskning av systemen, främst FRA och FM.

För att nå höga assuransnivåer för de nationella system som skyddar rikets säkerhet eller utrikessekretess måste kunskapen om systemlösningarna omges av sträng sekretess, något som endast kan upprätthållas med nationellt framtagna lösningar. Svenska kryptoprodukter håller vid internationell jämförelse en mycket hög nivå, som det tar decennier att nå. Det är enligt utredningen ytterst viktigt att värna om denna förmåga och förstärka förutsättningarna för en nationell marknad för krypto.

Av nämnda skäl menar utredningen även svensk kryptoindustri och kryptologisk kompetens bör kunna bli föremål för en dialog av det slag som föreslås i avsnitt 9.3.2 mellan det allmänna och näringslivet. Dialogen bör vara inriktad mot att finna möjligheter att slå vakt om svenska kryptoprodukter och kompetensen på området.

9.5 Incidentrapportering

Förslag:
1) Det inrättas system för obligatorisk it-incidentrapportering för samtliga statliga myndigheter. Detta anpassas till innehållet i EU-direktivet om nät- och informationssäkerhet (NIS-direktivet).
2) I syfte att förbereda införandet av detta system för obligatorisk it-incidentrapportering får MSB i uppdrag att utfärda verkställighetsföreskrifter om dess närmare utformning.
3) MSB bör ges i uppdrag att förse de statliga myndigheterna med information om bl.a. trender och utveckling avseende it-incidenter.

9.5.1 Informationssäkerhetsrelaterade lägesbeskrivningar

För att arbetet med informationssäkerhet inom statlig förvaltning ska vara effektivt krävs kunskap om såväl hot och risker som vilka hot som förverkligas och vilka skyddsåtgärder myndigheterna vidtar. Behovet av samlade lägesbeskrivningar sträcker sig över sektorsgränser och ansvarsnivåer, nationellt och i vissa fall även inom EU och internationellt (jfr prop. 2007/08:92).

Vilka hot eller risker som realiseras mot de myndigheter som inte omfattas av säkerhetsskyddslagstiftningen eller vilka skyddsåtgärder dessa myndigheter vidtar finns det ingen myndighet som kontrollerar. Riksrevisionen har i rapporten *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23) konstaterat att kunskapsläget för informationssäkerheten i statsförvaltningen är oklart. Varken regeringen eller någon av stöd- och tillsynsmyndigheterna har en kontinuerlig och systematiskt underbyggd lägesbild över den statliga förvaltningens informationssäkerhet, vilket är en förutsättning för att kunna säkerställa att man vidtar rätt åtgärder. I syfte att få en förbättrad och samlad nationell lägesuppfattning över it-incidenter finns det enligt utredningen skäl att vidta åtgärder som kan ge sådan information.

Lägesbeskrivningar sammanställs av olika uppgifter för att skapa en bild över vad som har hänt, händer eller kommer att kunna hända. Uppgifter kan exempelvis inhämtas från öppna källor och från sektorsmyndigheter samt näringslivet. Under utredningens

arbete har det framkommit att det finns ett behov av att utveckla system och metoder som ger underlag för lägesbeskrivningar. Ett system för obligatorisk it-incidentrapportering respektive användning av sensorteknik skulle bidra till att stärka förmågan att förebygga och hantera it-incidenter. Utredningen berör i följande avsnitt förutsättningarna för att införa obligatorisk it-incidentrapportering.

Upprättandet av en lägesbeskrivning på central nivå förutsätter även att myndigheterna lämnar en redovisning om informationssäkerhet i risk- och sårbarhetsanalyserna. Riksrevisionen har i nämnd rapport pekat på att bristerna är så omfattande att det inte går att ställa samman en gemensam bild av samlad förmåga att kunna motstå och hantera kriser inom informationssäkerhetsområdet. Som Riksrevisionen konstaterat leder detta i sin tur till att det blir svårt att analysera vilka brister som finns och därmed kunna göra en grundlig riskbedömning. Problemet har uppmärksammats av regeringen och MSB har fått i uppdrag att analysera och vidareutveckla sitt arbete med risk- och sårbarhetsanalyser och förmågebedömningar. Utredningen menar att vid sidan av MSB:s insatser skulle förslaget om att samla regleringen kring informationssäkerhet i en förordning kunna tydliggöra kravet på risk- och sårbarhetsanalyser (se avsnitt 9.2.3). Detta skulle i förlängningen bidra till att ge en bra och systematiskt underbyggd lägesbild.

Behovet av lägesbeskrivningar skiftar för olika myndigheter och för regeringen. De lägesbeskrivningar som behövs som underlag för operativa insatser kan behöva vara detaljerade. På den nationella nivån behövs i stället en mer övergripande beskrivning för att strategiskt inrikta och samordna övergripande resurser.

9.5.2 Obligatorisk it-incidentrapportering

Regeringen har vid ett flertal tillfällen i propositioner och skrivelser uttalat behovet av en funktion för it-incidentrapportering. Så skedde i 2002 års proposition om samhällets säkerhet och beredskap (prop. 2001/02:158) då ett nationellt ”rikscentra” för it-incidentrapportering inrättades vid PTS under namnet Sitic. Denna funktion är numera benämnd CERT-SE och överförd till MSB, se tidigare avsnitt 6.1.1.

I prop. 2003/03:93 s. 78 om it-säkerhet och sekretess fastslogs vikten av att myndigheter och organisationer rapporterade in it-incidenter för att Sitic skulle kunna fullgöra sitt uppdrag. I propositionen *Från IT-politik för samhället till politik för IT-samhället* (prop. 2004/05:175) konstaterade regeringen att Sitics viktigaste uppgift kommit att bli omvärldsbevakning och informationsspridning, medan endast ett fåtal sårbarheter blivit upptäckta genom incidentrapportering. Genom att sekretesslagen hade ändrats så att möjligheten att sekretessbelägga incidentrapporter blivit större och det fanns en förhoppning om att frekvensen för inrapporteringen skulle öka.

I proposition 2007/08:92 *Stärkt krisberedskap – för säkerhets skull* skriver regeringen följande: ”En samlad lägesbild utgör grunden för att aktörerna i krisberedskapssystemet ska kunna genomföra lämpliga åtgärder och samverka. Förmågan att skapa samlade lägesbilder bör stärkas. Vid kriser behöver samhällets resurser samordnas och samverka för att utnyttjas på ett effektivt sätt. Det räcker därför inte att inom det egna ansvarsområdet ha en uppfattning om vad som har hänt, vilka konsekvenserna blir och vad det ställer för krav på agerande. Det krävs dessutom en uppfattning om hur andra aktörer har uppfattat krisen och vilka åtgärder de vidtar. Det egna agerandet måste sättas in i ett bredare perspektiv. Därför finns det ett behov av samlade lägesbilder och samlad lägesuppfattning som sträcker sig över sektorsgränser och ansvarsnivåer, nationellt och i vissa fall även inom EU och internationellt”.

År 2009 återkom regeringen i budgetpropositionen för 2010 till frågan om bristerna i systemet för inrapportering av it-incidenter och det konstaterades att rapporteringen av it-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur i samhället behöver förbättras.

I budgetpropositionen för 2012 anges för första gången betydelsen av att anpassa skyddsåtgärder till hot och risker. Detta förutsatte dock enligt regeringen kännedom om hur många incidenter som inträffar och omfattningen av dessa. Sådan kunskap skulle förstärka möjligheten till ett samlat agerande vid it-incidenter där konsekvenserna bedöms bli omfattande. En obligatorisk it-incidentrapportering utgjorde enligt regeringen en del av det arbetet. I budgetpropositionen för 2013 upprepade regeringen betydelsen av tillgång till kunskap om hur läget är. Regeringens bedömning

angavs vara att information om det aktuella läget vid en allvarlig händelse är en förutsättning för att de inblandade aktörerna skulle få en ömsesidig förståelse för situationen och därmed kunna vidta samordnade åtgärder. Ett system för obligatorisk it-incidentrapportering skulle enligt regeringen bidra till detta.

Det finns således en tydlig politisk vilja i Sverige att genom en förstärkt it-funktion för incidentrapportering öka samhällets förmåga att förebygga och hantera incidenter som hotar eller skadar samhällsviktig verksamhet. Detta är också den inriktning som är drivande inom EU. Europeiska kommissionen överlämnade i februari 2013 direktivförslag om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen, NIS-direktivet (avsnitt 8.2.2). Där föreslås bl.a. ett system med obligatorisk it-incidentrapportering.

MSB har i tidigare nämnt underlag till regeringen (se avsnitt 7.5.3) uttryckt att en obligatorisk it-incidentrapportering är nödvändig för att bedriva ett effektivt arbete med informationssäkerhet i samhället. MSB har också påtalat att införandet av obligatorisk incidentrapportering skulle ge statsförvaltningen kunskap om såväl hot och risker som vilka hot som förverkligas och vilka skyddsåtgärder som vidtas. Denna information skulle ge en bra och underbyggd lägesbild, vilket är en förutsättning för att kunna säkerställa att rätt åtgärder vidtas.

Riksrevisionen har i nämnd rapport från 2014 konstaterat att varken regeringen eller stöd- och tillsynsmyndigheterna har den fulla bilden av i vilken omfattning hot realiseras eller vilka skyddsåtgärder som myndigheterna vidtar, och att det därför saknas en nödvändig förutsättning för ett effektivt arbete med informationssäkerhet. Riksrevisionens påpekande mynnar ut i en rekommendation till regeringen om att införa obligatorisk incidentrapportering för samtliga myndigheter. Utredningen instämmer i denna slutsats och föreslår att det inrättas ett system för it-incidentrapportering som är anpassat till de krav NIS-direktivet kommer att ställa. Utredningen föreslår att obligatoriet regleras i förordningen för statliga myndigheters informationssäkerhet (jfr. utredningens förslag i avsnitt 9.2.3). Av förordningen bör bl.a. framgå vilka it-incidenter som behöver rapporteras. Därvid ska andra krav på rapportering beaktas. Om en hemlig uppgift kan ha röjts ska det idag enligt 10 § säkerhetsskyddsförordningen skyndsamt anmälas

till Säkerhetspolisen, om röjandet kan antas medföra men för rikets säkerhet som inte endast är ringa. Dessutom framgår av 13 § andra stycket samma förordning att hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten. Vidare anges i 39 § säkerhetsskyddsförordningen att Försvarsmakten och Säkerhetspolisen har i uppgift att kontrollera säkerhetsskyddet inom respektive myndighets utpekade tillsynsområde. En it-incident kan allvarligt påverka säkerheten i ett it-system och därmed innebära att olika typer av åtgärder behöver vidtas, inte bara för den drabbade organisationen utan även för andra organisationer med motsvarande system. Dessutom finns ett uttalat krav på rapportering inom området. Med hänsyn tagen särskilt till Försvarsmaktens och Säkerhetspolisens utpekade uppgifter inom säkerhetsskyddet, bör enligt utredningens mening rapportering av it-incidenter med huvudsaklig koppling till sådana informationssystem i vilka hemliga uppgifter enligt offentlighets- och sekretesslagen (2009:400) behandlas i mer än ringa omfattning i första hand rapporteras till de myndigheter som utövar ett tillsynsansvar över säkerhetsskyddet i berörd verksamhet. Sådana särskilda informationssystem kan ha anordnats för att möta särskilda krav på säkerhet som ställts med stöd av säkerhetsskyddslagen (1996:627) eller för att handha uppgifter om totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

MSB är den myndighet som för närvarande ansvarar för it-incidenthanteringen. Med hänsyn till det uppdrag som MSB enligt sin instruktion har på informationssäkerhetsområdet, se särskilt 11 a § förordningen (2008:1002) med instruktioner för Myndigheten för samhällsskydd och beredskap, så bör MSB också vara den myndighet som fortsättningsvis tar emot de it-incidentrapporter som lämnas från myndigheterna. Systemet bör utformas så att det säkerställer behovet hos de brottsbekämpande myndigheterna av att kunna informera sig om misstänkta brottsliga angrepp. Med dessa utgångspunkter är det också MSB som på olika sätt arbetar vidare med inrapporterad information. Det handlar bl.a. om att bearbeta uppgifterna för att kunna ge respons till den som rapporterat in uppgifterna och att sammanställa aggregerad informationen till relevanta myndigheter, såsom exempelvis hotbildsuppdateringar. Baserat på ett utvecklat system för it-incidentrapportering kan

MSB ge regeringen, Regeringskansliet och det föreslagna myndighetsrådet samt de statliga myndigheterna information om bl.a. trender och utveckling avseende it-incidenter. Lägesinformation om hot- och risknivåer bör utgöra grunden för myndighetsrådets arbete för att förebygga, följa och åtgärda brister i statens informationssäkerhet samt även för att kunna säkerställa att staten vidtar rätt åtgärder.

Rapporteringsförfarandet bör konkretiseras genom verkställighetsföreskrifter. Utredningen föreslår att MSB ges rätt att utfärda verkställighetsföreskrifter om den närmare utformningen av ett system för obligatorisk incidentrapporteringen. Det kan t.ex. handla om vad som ska rapporteras in och på vilket sätt rapportering ska ske.

9.6 Brottsbekämpning

9.6.1 It-brottskonventionen

Förslag: Arbetet med ratificering av Europarådets konvention om it-relaterad brottslighet, som undertecknades av Sverige 2001, bör slutföras.

Befogenheten och även skyldigheten att uppdaga, beivra och utreda brott i den digitala miljön åligger de brottsbekämpande myndigheterna. De polisiära myndigheterna utgör i detta en unik del i samhällets informations- och säkerhet då de i sina roller har ett mandat att aktivt uppspåra och lagföra aktörer som ligger bakom antagonistiska it-angrepp. De polisiära myndigheterna har därför på nationell nivå och i nära samverkan med övriga myndigheter ett särskilt ansvar att sörja för säkerheten kring samhällets kritiska infrastruktur och hantera de brottsliga angrepp som förekommer relaterat till detta.

It-brott och brott relaterade till den digitala miljön utgör en ny typ av gränsöverskridande brottslighet som gör att ett väl fungerande internationellt samarbete är vitalt för att nå framgång i det brottsbekämpande arbetet.

Detta förhållande är väl erkänt i många strategier och policyer och inom EU även avhandlat på konventionsnivå. Europarådets konvention om it-relaterad brottslighet, även benämnd Budapest-

konventionen, upprättades redan 2001. Konventionen kan sägas ha tre huvudsyften. Det första är att åstadkomma en harmonisering av den nationella straffrätten beträffande brott som tas upp i konventionen. Det andra är att få fram nationella processrättsliga bestämmelser som tillgodoser behoven av regler för att på ett effektivt sätt utreda och lagföra it-relaterade brott och andra brott som begår med hjälp av datorer samt för att ta tillvara bevisning i elektronisk form. Det tredje är att lägga grunden för ett effektivt internationellt samarbete. Sverige var en av de första staterna att erkänna dess innehåll och skriva på konventionen. Sedan dess har dock ingen ratificering skett. En offentlig utredning, SOU 2013:39, har utrett vilka åtgärder Sverige behöver göra inom bland annat författningsområdet för att kunna ratificera konventionen. Vissa författningsändringar har med anledning av detta ägt rum, exempelvis införandet av brottet grovt dataintrång. Någon ratificering har dock inte skett och Sverige är nu en av få medlemsstater som inte har ratificerat konventionen. Därmed saknar Sverige flera av de instrument och verktyg som förväntas av oss som samarbetspart och medlemsstat inom EU. En ratificering med de lagändringar som är nödvändiga skulle dessutom öka möjligheten att framgångsrikt bekämpa denna typ av brottslighet.

Utredningen ser det därför som angeläget att arbetet med att ratificera it-brottskonventionen slutförs.

9.6.2 Informationsutbyte

Förslag: Det bör utredas om en tydligare reglering kan införas i offentlighets- och sekretesslagen rörande sekretess för uppgifter som utbyts vid samverkan mellan brottsbekämpande myndigheter och andra myndigheter inom informations- och cybersäkerhetsområdet.

Även nationellt har behovet av samverkan ökat inom området och flera olika myndigheter från olika sektorer behöver därför ha en god förmåga att samverka och utbyta information i syfte att tillförsäkra samhället godtagbar informationssäkerhet. En satsning på ökad samverkan, anpassade lagstöd och en utvecklad kompetens skapar

förutsättningar för de brottsbekämpande myndigheterna att framgångsrikt uppdaga, beivra och utreda brott i den digitala miljön.

Polismyndigheten har uppmärksammat utredningen på att det föreligger svårigheter när en brottsbekämpande myndighet ser ett behov av att delge samverkande myndigheter information. Det finns situationer då Polismyndigheten behöver delge en annan myndighet underrättelseinformation men samtidigt bedömer att sekretess alltjämt bör råda. En reglering i offentlighets- och sekretesslagen (2009:400) avseende överföring av sekretessen skulle då förenkla delgivningen av information. Utredningen bedömer därför att det finns ett behov att denna fråga i syfte att skapa förutsättningar för en mer ändamålsenlig och effektiv samverkan för brottsbekämpning inom informations- och cybersäkerhetsområdet.

9.6.3 Översyn av bestämmelser om tvångsmedels i den digitala miljön

Förslag: En översyn av bestämmelserna om tvångsmedel i 27 och 28 kap. rättegångsbalken och övriga lagrum bör göras för att säkerställa att brottsbekämpande myndigheter kan bedriva sin förebyggande och utredande verksamhet i den digitala miljön.

Översyn av befintliga tvångsmedel

Den digitala miljön har på ett genomgripande sätt förändrat människors, företags och myndigheters sätt att kommunicera och interagera. Denna utveckling är samhällsgenomgripande till sin karaktär och skapar enorma möjligheter. För brottsbekämpningens förmåga att uppfylla sina uppgifter i denna digitala miljö uppstår dock en rad mycket stora utmaningar. Bland annat gäller detta användningen och tillämpningen av hemliga tvångsmedel. Då samma befogenheter och skyldigheter gäller i den digitala världen som i den verkliga så gäller även de hemliga tvångsmedlen på samma sätt i båda miljöer. Dessa verktyg är dock inte i sin utformning skapade för eller anpassade för den digitala miljön. Även stöd i tillämpning kopplat till den nya digitala miljön saknas i stort sätt helt. Samtidigt som samhället i ökande omfattning flyttar ut i det digitala rummet

så har brottsbekämpningen i stora delar redskap, verktyg och lagstöd kopplade till den analoga världen.

Att kunna fullgöra sin skyldighet att uppdaga, beivra och utreda brott i den digitala miljön ställer krav på verktyg som kan verka i denna miljö. De nuvarande verktygen är inte i sin utformning skapade för eller anpassade till den digitala miljön och de styrkor och förmågor som de befintliga hemliga tvångsmedlen har är i stort överspelade i denna miljö.

Ett av de stora problemen i dagsläget är att stöd och tillämpning avseende de redan befintliga tvångsmedlen kopplat till den nya digitala miljön i stort saknas. Det finns således stora kunskapsluckor och svarta fält avseende hur de existerande tvångsmedlen kan, får och ska användas i den digitala miljön.

Bara ett sådant, i den fysiska världen, relativt enkelt hanterat tvångsmedel som husrannsakan och beslag utgör ett stort problem inom den digitala miljön för dagens brottsbekämpande organisationer och antalet tolkningar och tillämpningar är otaliga. Detta gör i förlängningen att rättssäkerheten riskerar att urholkas, dels genom att lagstiftningen tillämpas på olika sätt i liknande förhållanden, dels genom att lagstiftningen inte används trots att den kanske skulle vara tillämpbar.

Ett annat problem är att många av de befintliga tvångsmedlen inte är teknikneutrala och därmed med tiden kommer att bli obsoleta i den moderna digitala miljön. Ett beslut avseende hemlig avlyssning av kommunikation utfärdat av domstol är inte särskilt mycket värt om kommunikationen som beslutet omfattar är krypterad eller saknar teknisk lösning för att vidarebefordras till de brottsbekämpande myndigheterna. Listan med exempel kring denna typ av problem kan göras omfattande.

Om dessa olika typer av tekniska begränsningar, tillämpningssvårigheter och direkta avsaknad av specificerat lagstöd skulle sammanställas befaras att mängden tillämpbara verktyg inom detta område skulle bli relativt begränsat och troligen avsevärt mer begränsat än lagstiftaren både avsett och känt till.

Utifrån detta sagda är det därför av vikt att just med den digitala miljön och dess särskilda förutsättningar som utgångspunkt göra en genomgripande och detaljerad genomgång och analys över de befintliga tvångsmedlen och bestämmelserna inom området, och

sedan utifrån denna analys utröna vilka nya tillämpningar, förändringar eller nyordningar som är påkallat.

Utredningen föreslår därför en förnyad utredning, Tvångsmedel i den digitala miljön, med uppgift att se över bestämmelserna i 27 och 28 kapitlet rättegångsbalken samt övriga befintliga tvångsmedel avseende dess tillämpning i den digitala miljön samt vid behov föreslår förändringar eller nya lagstöd. Utredningen bör särskilt beakta förslag som framförts i SOU 2005:38 och 2012:44 rörande behovet av ett nytt tvångsmedel, hemlig dataavläsning (HDA).

9.7 Internationella och regionala relationer

Förslag: Regeringen säkerställer att Sverige agerar kraftfullt och konsistent i samtliga internationella och regionala fora av relevans.

9.7.1 Sverige som stark internationell spelare

Den internationella dimensionen är mycket påtaglig när det gäller informations- och cybersäkerhet. Dels därför 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, vilket innebär att förebyggande och hantering av sådana störningar måste ske såväl på nationell som på internationell nivå. För att hantera dessa typer av angrepp finns omfattande internationella samarbetsnätverk, vilka i stor utsträckning bygger på förtroende. Det pågår också viktigt arbete inom exempelvis OECD och EU där särskilt förhandlingarna av NIS-direktivet förtjänar att nämnas. I skrivelsen *Samhällets krisberedskap – stärkt samverkan för ökad säkerhet* (skr. 2009/10:124 s. 71 f.) angav regeringen att internationell samverkan är en grundförutsättning för att öka informationssäkerheten i Sverige, både när det gäller förebyggande arbete och när det gäller att hantera inträffade störningar. Vidare slogs det fast att Sveriges medverkan i internationella samarbeten inom informationssäkerhetsområdet är av strategisk betydelse och

bör stödjas och utvecklas. Regeringen konstaterade även att merparten av den internationella samverkan kan genomföras av aktörer på eget initiativ, men viss samverkan kräver en nationell samordning, exempelvis där det är av vikt att Sverige tar en officiell ställning. I det sammanhanget angavs att Sveriges nationella samordning för internationell samverkan inom informationssäkerhetsområdet bör, där så är lämpligt, göras tydligare. Utredningen återkommer till detta nedan.

9.7.2 Olika perspektiv

Det internationella perspektivet inom området inrymmer både de globala cyberfrågorna inom utrikes- och säkerhetspolitiken och de internationella samarbeten som förekommer kring policyfrågor och tekniska angelägenheter med nät- och driftsperspektiv. Det internationella samarbetet sker såväl inom de olika politikområdena som inom olika verksamhetsområden. När det gäller de internationella relationerna inom respektive politikområde är det för frågan ansvarigt departement som företräder Sverige vid förhandlingar. På verksamhetsnivå är det myndigheterna som har mycket viktiga kontakter med motsvarande myndigheter i andra länder, inom och utom EU. Samarbeten finns inom flera områden från de rent tekniska frågorna till mer övergripande policyfrågor. Utredningen har i kapitel 8 redogjort för några av de internationella forum och samarbeten i vilka Sverige deltar. I detta kapitel har utredningen även skildrat svensk global cyberpolitik (avsnitt 8.1) och noterat att det utgör en prioriterad utrikespolitisk fråga och en viktig del av Sveriges politik på det freds- och säkerhetsfrämjande och folkrättsliga området. I avsnittet beskrivs också hur den ökande betoningen på cyberfrågor inom utrikes- och säkerhetspolitiken har växt i takt med den tilltagande digitaliseringen och globaliseringen av samhället. Det kan konstateras att cyberfrågor är till sin karaktär gränslösa och kräver omfattande internationell samverkan och samförstånd, inte minst för att skapa goda förutsättningar för ökad stabilitet och transparens liksom utvecklandet av normer för ett ansvarsfullt beteende i cyberrymden. Utredningens bedömning är att i ett globalt perspektiv är samarbete för normbildande och förtroendebyggande åtgärder inom cyberområdet viktigt för att

stärka internationell fred och säkerhet vid användandet av informations- och kommunikationsteknologi, liksom för att minska sårbarheter och risker för it-angrepp och konflikter inom detta område. Som vi kunnat se tidigare finns det flera kanaler och forum där Sverige deltar i arbetet med dessa frågor. Målet för detta arbete måste vara att få genomslag för svenska intressen och gehör för Sveriges politik på det fredsfrämjande och folkrättsliga området.

9.7.3 Samordning av det internationella agerandet

Den nationella informations- och cybersäkerheten förstärks genom ett aktivt och effektivt deltagande i verksamheten vid internationella organisationer och i samarbetsforum som är viktiga med tanke på informations- och cybersäkerheten. Detta är också något som regeringen har konstaterat i ovan refererad skrivelse. I utredningens direktiv påpekas också att det är viktigt att Sverige har en tydlig inriktning på området för att kunna påverka den säkerhetspolitiska inriktningen. En stor utmaning i arbetet sägs ligga i staters skilda syn på hotbilder, doktriner och definitioner kopplade till cybersäkerhet.

För att svenska aktörer ska få genomslag på den internationella arenan är det viktigt att hänsyn tas till överordnade svenska intressen, och att utgångspunkten för vårt internationella agerande utgörs av en gemensam svensk ståndpunkt. Detta gäller på alla nivåer, regeringen, Regeringskansliet och myndigheter. Utan en sådan samordning kan svenska representanter komma att framföra olika ståndpunkter som får till följd att målen inte uppnås och att Sveriges budskap uppfattas som tvetydigt eller oklart. Det är utredningens uppfattning att det budskap som framförts i internationella sammanhang inte i alla lägen har varit samordnat och därmed inte gynnat svenska intressen i den utsträckning som annars hade varit möjlig. Orsaken till detta kan vara den snabba utvecklingen inom området. På kort tid har cybersäkerhetsfrågorna uppmärksammats inom en rad internationella organisationer och politikområden. Vidare har den strategiska inriktningen på politiken i vissa avseenden inte varit tillräcklig för att ge tillräcklig vägledning.

Frågorna har behandlats inom vitt skilda politikområden, ibland med tydliga målkonflikter, vilket har gjort det svårt att skapa en gemensam värdegrund att utgå ifrån. En annan orsak kan vara uppdelningen av ansvaret inom informations- och cybersäkerhetsområdet, i meningen att det finns risk att samordningen har försvårats eller i vissa fall fallit mellan stolarna. De nationella samordningssvårigheterna grundas också i att Sverige deltar i ett stort antal forum vilket bidrar till samordningsbehov. Cybersäkerhetsfrågor är vidare komplexa och rör sig inom en lång rad olika sakområden. Som regeringen påpekat i tidigare nämnd skrivelse så finns det ett behov av att tydliggöra Sveriges nationella samordning för internationell samverkan.

Regeringskansliet har enligt sin instruktion ansvaret för att utse Sveriges ombud och andra representanter vid förhandlingar med annan stat eller vid förhandlingar med och möten inom internationella organisationer. Med en väl genomarbetad och förankrad nationell strategi och en tydlig arbetsfördelning inom Regeringskansliet och mellan myndigheterna bör de befintliga verktygen, dvs. gemensam beredning, regleringsbrev och myndighetsinstruktioner, vara tillräckliga för att hantera såväl förutsedda som snabbt uppkomna frågor. Det kan däremot finnas skäl att lägga större vikt vid de internationella frågorna när myndigheternas instruktioner och regleringsbrev ses över.

Processer och arbetsorganisation inom Regeringskansliet har stor betydelse för den samlade statliga styrningen. Det gäller inte minst för strategiska ställningstaganden och för utformningen av myndigheternas uppdrag. Hur frågor som berör informationssäkerhet fördelas mellan departementen avgörs tydligast av den ansvarsfördelning som är fastställd i bilagan till förordningen (1996:1515) med instruktion för Regeringskansliet. Beroende på vad frågan huvudsakligen handlar om hanteras den av det departement som huvudsakligen berörs, se avsnitt 7.2.1

Riksrevisionen konstaterade i rapporten *Informationssäkerheten i den civila statsförvaltningen* (RiR 2014:23) att det saknas en samlad central funktion i Regeringskansliet med ansvar för att bereda frågor om informationssäkerhet i statsförvaltningen. Riksrevisionen rekommenderade regeringen att inrätta en funktion och en process i Regeringskansliet med syfte att samlat hantera informationssäkerheten. Utredningen har i avsnitt 9.1.5 berört frågan om

samordning av det nationella arbetet och konstaterat att det genom departementsombildningen skapats bättre förutsättningar än tidigare för att förmå den centrala statsförvaltningen att agera samfällt när det gäller hanteringen av informations- och cybersäkerhetsfrågor. Ett samordnat svenskt agerande i internationella och regional relationer är på samma sätt avhängigt hur frågorna bereds i Regeringskansliet.

Utredningen konstaterar att ansvaret för de internationella relationerna är spritt över en rad olika myndigheter och departement vilket ställer stora krav på väl fungerande samordning i Regeringskansliet. Som vi också kunnat konstatera finns motsvarande behov av stärkt samordning när det gäller det nationella informations- och cybersäkerhetsarbetet mellan Regeringskansliet och ansvariga myndigheter. Utredningen har i avsnitt 9.2 lämnat förslag som vi menar bidrar till att samordna det nationella arbetet. Det är viktigt att förslagen åtföljs av övergripande strategier och åtgärder som bl.a. innebär att regeringen säkerställer att Sverige agerar kraftfullt och konsistent i samtliga internationella och regionala fora av relevans. Nationell samordning för internationell samverkan bedöms här som en av åtgärderna.

För att därtill säkerställa konsistens i det internationella agerandet behöver samordning ske antingen under det mandat som inrikesministern erhöll i samband med regeringsbildningen 2014 eller, om frågorna är av utrikes- och säkerhetspolitisk karaktär, genom Utrikesdepartementets försorg.

På myndighetsnivå gör sig samma behov av stringens i ansvarsfördelningen och konsistens i uppträdandet gällande, vilket regeringen kontinuerligt behöver säkerställa. Flera av de internationella operativa relationerna har vuxit fram och också ändrat karaktär över tid. Så har exempelvis EU-organet ENISA med varje år kommit att inta rollen som EU:s informationssäkerhetsansvariga myndighet och bedriver idag ett brett arbete med informations- och cybersäkerhet, i vilket även ingår en nära samverkan med CERT-EU och framtagandet av stöd till CERT-funktioner i medlemsstaterna. Beträffande NATO-centret för cyberförsvar i Tallinn (NATO Cooperative Cyber Defence Centre of Excellence, CCD CoE), ryms vid sidan av rena försvarsangelägenheter också numera verksamhet som är av relevans för informations- och cybersäkerhet i allmänhet.

9.8 Övriga förslag

I avsnitt 9.1 samt bilaga 5 presenterar utredningen ett förslag till strategi för statens informations- och cybersäkerhet. Som vi där redogjort för syftar strategin till att söka åtgärda de mest angelägna bristerna i statsförvaltningen. Avsikten är dock att i nästa skede gå vidare till mer specifika områden. Kompetenshöjande åtgärder är ett sådant område som kräver särskilda insatser och medverkan från privat och offentlig sektor. Utredningen vill redan nu lyfta fram två åtgärder som rör detta område, nämligen övningsverksamhet och planering för kompetensförsörjning.

9.8.1 Framtida övningsutveckling inom informations- och cybersäkerhetsområdet

Bedömning: Övningsverksamhet inom informations- och cybersäkerhetsområdet bör fortsätta och förstärkas. Det finns även behov av att utveckla övningar av olika slag för flera sektorer och nivåer i olika organisationer.

Regelbundna nationella övningar är en förutsättning för att utveckla och utvärdera strukturer för hantering av allvarliga it-relaterade kriser. Övningar utgör ett kraftfullt instrument för att öka deltagares krishanteringsförmåga och för att identifiera tekniska och administrativa utvecklingsbehov. Regeringen utrycker i Budgetpropositionen 2012 (UO 6) att ”MSB bör fortsatt arbeta utifrån myndighetens strategi för tvärsektoriella övningar på nationell nivå. Inriktningen för övningar bör ta sin grund i erfarenheter från inträffade händelser, genomförda övningar samt myndigheters risk- och sårbarhetsanalyser samt förmågebedömningar.”

Dessa slutsatser torde även omfatta informations- och cybersäkerhetsområdet och är i linje med EU-kommissionen syn att cybersäkerhetsövningar är strategiskt viktigt för att förbättra skyddet av kritisk informationsinfrastruktur.

Sverige bör fortsätta att aktivt delta i internationella övningar då de utgör en god katalysator för att bygga förtroende och utveckla processer för internationellt samarabete. Det är ett samarbete som är allt viktigare med tanke på informations- och cybersäkerhets-

områdets gränsöverskridande natur och det faktum att tekniska experter inom informations- och cybersäkerhet fortfarande är en begränsad resurs. Det kostar även förehållandevis lite i form av personalresurser, tid och pengar att delta i internationella övningar. Det stora antalet aktörer som planerar och genomför övningar medför däremot att det är viktigt att prioritera vilka övningar Sverige ska delta i. Av särskild vikt är det att Sverige här snarast formellt ansluter sig till CCD CoE där den mest aktiva utvecklingen av civila tekniska cybersäkerhetsövningar (t ex Baltic Cyber Shield 2010, Locked Shields-serien) nu äger rum, och där i princip alla västländer nu deltar.

Att genomföra egna nationella övningar är än viktigare och Sveriges förmåga att planera och genomföra informations- och cybersäkerhetsövningar står sig väl internationellt. Det beror bland annat på den kunskap som byggts upp under planeringen av sektorövergripande övningar som CDX (2008, 2010), NISÖ (2010, 2012), och tekniska informations- och cybersäkerhetsövningar med virtuell övningsmiljö (2013). Telö-serien utgör ett annat exempel på en återkommande övning som genomförs inom sektorn för elektronisk kommunikation. Därutöver har Sverige en virtuell övningsmiljö bekostad av Försvarsmakten och MSB i form av en teknisk övningsmiljö vid Totalförsvarets Forskningsinstitut (FOI). Försvarshögskolan har varit drivande i både utvecklingen och genomförandet av övningar. Bland annat har en handbok tagits fram för CDX-övningar på såväl svenska som engelska. Detta medför att Sverige kan återanvända och vidareutveckla tekniska moduler till nya övningar. Denna förmåga förenklar arbetet och reducerar kostnaderna för att planera och genomföra nya övningar. Fördelen med att skapa egna övningar är att Sverige anpassar övningens utformning gentemot egna mål vilket blir allt viktigare ju mer specifika behov som finns för att utveckla verksamheters förmåga att hantera händelser och kriser. Sverige bör därför fortsätta enligt den aktuella inriktningen och regelbundet genomföra tvärsektoriella informations- och cybersäkerhetsövningar och tekniska informations- och cybersäkerhetsövningar.

Tekniska informations- och cybersäkerhetsövningar kan användas för att utveckla kunskapen i samhället och utvidga samarbetet mellan offentlig och privat sektor. Exempelvis kan det etablerade Svenskt CERT-forum, med deltagare från privat och offentlig

sektor, övas i syfte att stärka förtroendet och samverkan mellan dessa organisationer och därmed utveckla samhällets krishanteringsförmåga.

För att nå fler aktörer och nivåer i samhället bör övningar utnyttjas till att bygga upp förmågan hos andra aktörer i samhället som inte har samma resurser för it-incidenthantering. Arbetet inom ramen för MSB och FOI:s gemensamma satsning för att öka förmågan till att hantera it-relaterade risker och hot mot industriella informations- och styrsystem (NCS3) utgör också en grund för skapandet av övningsmiljömoduler och för att genomföra enklare tillämpade övningar. På detta sätt uppnås skalfördelar mellan förebyggande och förberedande arbete och ren övningsverksamhet och på så vis nås fler organisationer. Detta är ett arbete som bör fortsätta och förstärkas. Det är även i linje med slutsatserna från NISÖ 2012 som pekade på att det finns ett stort behov av övningar inom området – på alla nivåer i samhället men att övningar bör utformas så att varje aktör får möjlighet att delta utifrån sina egna förutsättningar, och på ett sätt som ger nytta i den dagliga verksamheten.

9.8.2 Fördjupad dialog om kompetensförsörjning

Förslag: Regeringen fördjupar dialogen mellan privata och offentliga aktörer samt utbildnings- och forskningsinstitutioner i fråga om utbildning och forskning inom informationssäkerhetsområdet.

Utredningen har i avsnitt 9.3.2 föreslagit att regeringen fördjupar dialogen mellan privata och offentliga aktörer. Gemensamt för dessa är även behovet av att rekrytera personer med kvalificerad utbildning inom informationssäkerhetsområdet och det finns därför även ett behov av att det allmänna samverkar med näringslivet kring frågeställningar som rör forskning och utbildning samt kompetensförsörjning.

Utredningen har genom olika kontakter inom offentlig och privat verksamhet uppmärksammats på behovet av att vidta åtgärder för att förbättra utbildning och forskning inom informationssäkerhetsområdet. Bland annat har det framförts att svårigheten att hitta

kompetent personal går ut över expansionen av infrastrukturen på ett sätt som ger allvarliga konsekvenser bl.a. för kvaliteten på den service som tillhandahålls av operatörerna av både nät och tjänster. Brist på spetskompetens drabbar data- och telekommunikationsföretagen särskilt hårt. Dessa företag har ett stort rekryteringsbehov eftersom verksamheten expanderar snabbt. Myndigheter nämner att det finns behov av att rekrytera personer som har såväl sektorsspecifik som informationssäkerhetsinriktad kompetens. Den offentliga sektorn upplever konkurrens om arbetskraften med det privata näringslivet som erbjuder högre löner.

Behovet av kvalificerad utbildning i informationssäkerhet omfattar olika yrkesgrupper såsom jurister, samhällsvetare, tekniker, och ekonomer. En betydande del av utbildningsbehovet måste tillgodoses inom högskolans ram. Försvarshögskolan anordnar som beskrivs i 6.2.11 sedan 2011 en högre informationssäkerhetskurs där eleverna efter kursen diplomeras som "Chief Information Assurance Officers" (CIAO), vilken utvecklats med stöd av MSB, FRA och PTS. Deltagarna kommer både från offentlig sektor och från kritisk infrastruktur inom privat sektor. Genomgången kurs kan utgöra ett sådant krav på kompetens som föreslås i 9.2.3 för informationssäkerhetschefer. Det finns dessutom ett mycket begränsat antal personer i Sverige som besitter de kunskaper som krävs för att kunna genomföra sådan utbildning.

Det kan också finnas behov av att stärka sambandet mellan utbildning och forskning. Vidare behövs det särskild kompetens på Polishögskolan för utredning av brott med anknytning till informationsteknik. I många andra länder har behovet lett till att man inrättar specialiserade funktioner inom polisorganisationerna, där man samlar personer med nödvändiga kunskaper för utredning av it-relaterad brottslighet. I Sverige har vi sett en tillväxt på både efterfrågan och utbud när det gäller utbildning i forensisk analys.

Den som ska kunna ge råd i förebyggande informationssäkerhetsarbete och vid incidenter måste själv ha hög kompetens och god kännedom om flera områden som berör informationssäkerhet som till exempel om hur systemen är uppbyggda (operativsystem, DNS, IP och nätteknik), om säker applikationsutveckling och om skydd mot intrång samt skydd mot avlyssning.

Utredningen föreslår således att även frågan om kompetensförsörjningen inom informations- och cybersäkerhet görs till föremål

för dialog. Representanter från utbildningssystemet bör delta i dialogen. Målsättning med dialogen är att komma fram till hur man bör inrikta och stödja kompetensutvecklingen på informationssäkerhetsområdet både på bredden och på djupet. Det handlar bl.a. om att diskutera tvärvetenskapligt forskningsbehov, resursbehov och kompetensuppbyggnaden inom de högre utbildningarna. Dagens forskning inom informations- och cybersäkerhetsområdet uppvisar luckor och har i många fall ett snävt tekniskt fokus. Här finns ett behov av att vidga kunskapsbasen, inte minst vad gäller frågor med koppling till säkerhetskultur.

10 Konsekvenser av förslagen

10.1 Inledning

Enligt 14–15 a §§ kommittéförordningen (1998:1474) ska utredningen beräkna och redovisa de ekonomiska konsekvenserna av sitt förslag. Det gäller förslag som påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda och förslag som innebär samhällsekonomiska konsekvenser i övrigt. När det gäller kostnadsökningar eller intäktsminskningar för staten, kommuner eller landsting ska utredningen föreslå en finansiering. Vidare följer av 15 § att om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, ska konsekvenserna i det avseendet anges i betänkandet. Detsamma gäller när ett förslag har betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

Utredningens förslag innebär en höjd ambitionsnivå för statens informationssäkerhet. Åtskilliga av åtgärdsförslagen kan rymmas inom myndigheters befintliga budget. Nedanstående beräkningar avser främst de kostnader som uppstår hos Myndigheten för samhällsskydd och beredskap, som är den myndighet som enligt den föreslagna förordningen får ett utökat förvaltningsansvar. Kostnader av mindre omfattning kan också komma att uppstå i andra delar av statsförvaltningen. Dessa är dock svårare att överblicka. De förslag i föregående kapitel som varit möjliga att kostnadsberäkna anges nedan.

I nedanstående beräkningar ligger en schablon på en miljon kronor per person och år. Av beloppet utgör 700 000 kronor ordinarie personalkostader (lön och lönekostnadspåslag) och 300 000

kronor kostnader för kompetensutveckling, förvaltningskostnader (overhead), reseersättningar, m.m.

10.2 Åtgärdsförslagen

10.2.1 En nationell styrmodell för informationssäkerhet

En nationell styrmodell för informationssäkerhet består av ett antal komponenter som måste utvecklas och förvaltas över tid. En del är ett sammanhållande regelverk som innehåller olika nivåer av reglering under föreskriftsnivån, det vill säga en regelhierarki som motsvarar ett ledningssystem inom en organisation. Förutom de resurser som krävs för att utveckla och förvalta styrmodellen krävs en lösning för anslutning och efterlevnadskontroll som löpande samordnas med andra intressenter. I detta ligger också omfattande utbildningsinsatser.

I styrmodellen är informationsklassning den mest omfattande aktiviteten som går från processorienterad informationskartläggning via själva klassningsmomentet till utvecklade gemensamma skyddsnivåer. För att skyddsnivåerna ska kunna fylla sin funktion krävs omfattande insatser av både egen och extern kompetens inom områdena administrativ, fysisk och it-inriktad säkerhet.

Slutligen förutsätter en nationell styrmodell en väl utvecklad kunskapsstyrning. Kunskap kan i detta sammanhang röra sig om kunskap om metoder men i ännu högre grad om att kunna ge ett vederhäftigt underlag för en styrning utifrån risk. Det innebär att kunna förmedla en uppdaterad riskbild och att samtidigt kunna förmedla stöd för riskreducerande åtgärder.

Sammantaget estimat för att lösa ovanstående uppdrag är fem tjänster. Men med en viss samordning med befintlig verksamhet vid MSB så torde tre till fyra tjänster vara tillräckligt, vilket enligt angiven schablon motsvarar tre till fyra miljoner kronor per år. Övriga kostnader bedöms kunna finansieras inom MSB:s befintliga budget för ordinarie verksamhet.

10.2.2 Upprättandet av ett kansli för myndighetsrådets arbete

Utredningen föreslår ett myndighetsråd med ett antal uppgifter. Rådet förslås fungera som en gemensam remiss- och beredningsinstans i informationssäkerhetsfrågor. Rådet ska även säkerställa verkställandet av den nationella informations- och cybersäkerhetsstrategin. Vidare föreslås att rådet ska förvalta och utveckla tillämpliga krav på standarder och certifiering och för produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet. Myndighetsrådet bör även med stöd bl.a. av den nationella styrmodellen och tillsammans med den nya upphandlingsmyndigheten ge stöd till myndigheter som har behov av expertkompetens vad gäller it- och informationssäkerhet. Slutligen ska rådet även identifiera andra frågor än de ovan nämnda som kan göras till föremål för rådets behandling.

Till ovan tillkommer att rådet ska förses med lägesbeskrivningar av hot- och risknivåer i den statliga verksamheten baserat på ett system för incidentrapportering.

För att kunna driva arbetet med att förebygga, följa och åtgärda brister i statens informationssäkerhet behöver myndighetsrådet ett kansli. Förutom att tillgodose kansliet med underlag enligt ovan, så är kansliets uppgift även att säkerställa ett informationsutbyte och en samordning av de samverkande myndigheterna. Enligt utredningen bör myndighetsrådets kansli vara placerat hos MSB.

Huvuddelen av uppgifterna kopplade till myndighetsrådet kan finansieras inom befintlig budget för respektive deltagande myndighet. För att bereda ärenden, följa upp nationella strategin, effektuera förvaltning och utveckling av tillämpliga krav på standarder och certifiering av produkter och tjänster, säkerställa ett informationsutbyte, ge stöd till myndigheter som har behov av expertkompetens samt samordna lägesbeskrivningar av hot- och risknivåer finns det dock behov av tillskott på två tjänster för MSB vilket enligt angiven schablon motsvarar två miljoner kronor per år. Övriga kostnader bedöms kunna finansieras inom befintlig budget för respektive myndighet.

10.2.3 Uppgiften att bedriva tillsyn

Utredningen föreslår att MSB ges en allmän tillsynsuppgift över statliga myndigheters arbete.

Uppgiften att bedriva tillsyn av efterlevnaden av regelverk hos statliga myndigheter, kommer med största sannolikhet innebära uppföljning, utvärdering och samordning av tillsynen samt att ge stöd och råd till myndigheterna. Uppföljning och revision är en nödvändig förutsättning för ett systematiskt informationssäkerhetsarbete. Detta arbete måste av nödvändighet till stor del bedrivas ute hos berörda myndigheter.

Vidare innebär tillsynsuppgiften sannolikt att samordna och koordinera tillsynsmyndigheternas arbete i likhet med det förslag som Riksrevisionen tagit fram. Uppgiften innebär även att samverka med olika, för området relevanta aktörer (t.ex. myndigheterna i myndighetsrådet). Sammantaget är en tillsynsverksamhet av denna karaktär personalintensiv om den ska ha avsedd effekt. Utredningen bedömer resursbehovet till fem till sex tjänster, vilket enligt angiven schablon motsvarar fem till sex miljoner kronor per år. Övriga kostnader bedöms kunna finansieras inom befintlig budget för respektive myndighet.

10.2.4 Incidentrapportering

Huvuddelen av denna uppgift kan finansieras inom befintlig budget. I och med att ett obligatorium för it-incidentrapportering för statliga myndigheter föreslås kan en viss ökning av uppgifter förespås. Utredningen bedömer behovet till cirka två tjänster vid MSB. Den stora förändringsfaktorn är vad för kostnader som NIS-direktivet kommer att innebära. Om NIS-direktivet eller annan kravställning innebär att en dygnet runt verksamhet (s.k. 24/7/365) ska etableras vid MSB/CERT-SE så kommer detta innebära att minst fyra tjänster måste tillföras för att upprätthålla verksamheten över hela dygnet. Resursbehov bedöms därför på sikt vara två till sex tjänster vilket enligt angiven schablon motsvarar två till sex miljoner kronor per år.

Redan nu torde det finnas etablerade rutiner hos alla myndigheter i och med de krav som redan nu finns på ett systemetiskt informationssäkerhetsarbete genom MSB:s föreskrift. I detta sammanhang handlar

det om att anpassa dessa rutiner till den obligatoriska it-incidentrutinen. När det gäller kostnader för övriga myndigheter bedöms dessa kunna finansieras inom befintlig budget.

10.2.5 Säkrare kommunikation i staten

Utredningen föreslår att samtliga myndigheter som anges i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap ansluts till kommunikationsnätverket Swedish Government Secure Intranet (SGSI).

Uppgiften att samordna, förvalta och säkerställa funktionalitet och säkerhet i SGSI omfattar redan i dag ett antal uppgifter i form av ackreditering, uppföljning av efterlevnad och utveckling av nya tjänster. SGSI i sig är avgiftsfinansierad vad avser nya tjänster och funktionalitet. En ökad anslutningstakt och merutnyttjande av SGSI medför dock att det behöver tillföras personella resurser för förvaltning och säkerhetsarbete.

För att genomföra de åtgärder som föreslås i utredningen kopplat till säkrare kommunikation i staten bedöms det att två tjänster måste tillföras MSB, vilket enligt angiven schablon motsvarar två miljoner kronor per år. Övriga kostnader bedöms kunna finansieras inom ordinarie budget för MSB och de anslutande aktörerna.

Utredningen föreslår att lämpliga åtgärder bör vidtas för att utveckla sensorteknik. Härvid uppstår en engångskostnad för tekniken. Kostnaden för sensorer kan till stor del finansieras inom ordinarie budget för berörda myndigheter.

En stor osäkerhet ligger i vad säkra kommunikationstjänster kan komma att kosta för att säkerställa kontakten med de utplacerade sensorerna. De stora löpande kostnaderna ligger i att hyra in särskild kapacitet och är beroende på hur många kopplingar ut mot myndigheterna som ska utföras, samt hur kommunikationslösningen kommer se ut. En möjlighet skulle på sikt kunna vara att nyttja den statliga kommunikationsinfrastrukturen.

10.3 Statens intäkter

Utredningen bedömer att det snarare blir minskade kostnader på sikt än ökade statliga intäkter som följd av utredningens förslag. På informationssäkerhetens område är det sannolikt så att en förbättrad organisation, i enlighet med våra förslag i normalfallet dels leder till lägre kostnader, dels förorsakar genomförandekostnad men på sikt en kostnadsminskning tack vare bättre säkerhet.

En samordning inom statsförvaltningen som bygger på en gemensam styrmodell kan leda till lägre kostnader för statliga myndigheter, om man i stället för att utveckla egna varianter följer gemensamma principer.

Standardiseringsinsatser, liksom de flesta it-investeringar, innehåller i teorin en inledande investeringskostnad och därefter en period av ökande effektivitet, möjligen lägre kostnader förutsatt att organisation, resurser och kompetens anpassas till den nya tekniken. Det är dock svårt att kvantifiera dessa effekter.

10.4 Finansiering

Eftersom informationssäkerhet normalt anses ingå i kostnaderna för respektive verksamhet är utgångspunkten att flera förslag bör bäras av respektive verksamheter; kostnaderna kan antas vara ganska marginella i förhållande till de totala verksamhetskostnaderna.

Den största kostnaden gäller framför allt den utökade rollen för Myndigheten för samhällsskydd och beredskap, vilket kräver en anslagshöjning. Samverkan kommer i stor utsträckning att behöva utvecklas med myndigheter med stor egen informationssäkerhetsverksamhet och kunskap om strategiskt arbete bl.a. de i det föreslagna myndighetsrådet ingående myndigheterna. En sådan samverkan kan leda till att man delar med sig av utvecklingsarbetets resultat.

Behovet av höjt anslag för Myndigheten för samhällsskydd och beredskap, som specificerats ovan i anslutning till de olika förslagen, kan täckas genom omdisponeringar inom utgiftsområde 06 Försvar och samhällets krisberedskap, varifrån myndighetens ramanslag finansieras. Det kan också övervägas om en del av kostnaderna är att hänföra till en ny förvaltningspolitisk inriktning av statsförvaltningens arbete och därmed hänförlig till utgiftsområde 02 Samhällsekonomi och förvaltning, liksom det kan övervägas om

delar av de kostnadsökningar som beskrivs är att hänföra till de krav på ökad digitalisering som statsförvaltningen varit föremål för, framförallt genom åtgärder hänförliga till utgiftsområde 22 Kommunikationer. Ett sista förslag till övervägande är huruvida informations- och cybersäkerhet kommit att bli en så central del av statsförvaltningen i dess helhet att det förtjänar ett eget och nytt utgiftsområde.

10.5 Samhällsekonomiska effekter

En utbredd användning av standarder i statlig verksamhet är till sin karaktär att betrakta som investeringar med förväntan om framtida vinster i form av ökad effektivitet, ökad säkerhet, liksom större konkurrens i näringslivet. Några av de samhällsvinster av en förbättrad statlig användning av standarder och andra förslag som utredningen identifierat är:

En säkrare och därigenom effektivare förvaltning ger större utrymme för andra ändamål än hantering av brister och fel.

En större dynamik och konkurrenskraft uppnås om företag i sina mellanhavanden med den statliga förvaltningen kan använda öppna standarder och inte behöver anpassa sig till specifika myndighetsstandarder, vilket också kan minska den administrativa bördan för företagen.

En ökad nationell konkurrenskraft kan åstadkommas om insatser görs för ett ökat användande av internationella öppna standarder i statlig verksamhet.

10.6 Förslagens brottsförebyggande konsekvenser

Förslagen bör om de genomförs ha en brottsförebyggande verkan. Såväl den nationella styrmodellen som tillsynen av regelefterlevnad och i synnerhet it-incidentrapporteringen torde, förutom åtgärdernas primära effekt, dessutom skapa en större tydlighet kring det icke önskvärda beteendet, som kan tangera det kriminaliserade området, närmare bestämt brottet dataintrång. Sålunda är det också utredningens förväntning att de föreslagna åtgärderna ska verka avskräckande i förhållande till det icke önskvärda beteendet, dvs. att förslagen ska ha en allmänpreventiv effekt på de uppsåtliga

formerna av hot mot informationssäkerheten. Utredningen menar också att de föreslagna åtgärderna kan ha en höjande effekt på anmälningsbenägenheten avseende misstänkta fall av dataintrång. För att få varaktig verkan för det brottsförebyggande arbetet måste flera av förslagen fullföljas och förenas med ytterligare åtgärder, se t.ex. härom avsnitt 9.6.

Kommittédirektiv 2013:110

Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system

Beslut vid regeringssammanträde den 28 november 2013

Sammanfattning

En särskild utredare ges i uppdrag att föreslå strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system.

Utredaren ska då

- föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och itsystem,
- föreslå övergripande mål för samhällets informationssäkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur,
- klargöra begrepp som används inom informationssäkerhetsområdet och vid behov föreslå förtydligande eller alternativa benämningar och definitioner, särskilt av sådana som används i förslaget till nationell strategi, och
- med utgångspunkt i uppdraget redovisa statliga myndigheters ansvar och roller utifrån de uppgifter och uppdrag på informationssäkerhetsområdet som de har i dag.

Nuvarande ansvarsförhållanden och åtaganden ska beaktas men inte begränsa utredningen, som ska utgå från ansvarsprincipen och

gällande ekonomiska ramar. De begrepp eller benämningar som används i dessa direktiv ska inte föregripa eller begränsa utredarens arbete.

Uppdraget ska redovisas senast den 1 december 2014.

Bakgrund

Samhällets informationssäkerhet

Målen för Sveriges säkerhet är att värna befolkningens liv och hälsa, samhällets funktionalitet samt vår förmåga att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter (propositionen Ett användbart försvar, prop. 2008/09:140, bet. 2008/09:FöU10, rskr. 2008/09:292). Det finns ingen motsättning mellan frihet och säkerhet utan dessa är ömsesidigt förstärkande. Med utgångspunkt i dessa övergripande mål för vår säkerhet är målen för arbetet med samhällets krisberedskap att minska risker för, och konsekvenser av, allvarliga störningar, kriser och olyckor. Skulle en sådan händelse inträffa bör människors liv, personliga säkerhet och hälsa tryggas samt skador på egendom och miljö begränsas (budgetpropositionen för 2013, prop. 2012/13:1 utg.omr. 6, bet. 2012/13:FöU1, rskr. 2012/13:93-95).

All verksamhet är i dag beroende av fungerande informationssystem. Våra nätverk och system behöver vara säkra och stabila över tid. Näringslivet, offentlig förvaltning och medborgarna måste känna tillit till att de digitala tjänsterna i samhället fungerar. Näringslivet har en betydelsefull roll som den största ägaren och förvaltaren av samhällsviktig informationsinfrastruktur. Konsekvenserna av en allvarlig it-incident skulle med stor sannolikhet genom bl.a. spridningseffekter kunna drabba samhällsviktig verksamhet i flera sektorer. Informationssäkerhet berör således många olika verksamhetsområden bl.a. säkerhets- och utrikespolitiken, försvarspolitiken, näringsfrågor, socialfrågor och brottsbekämpning. För att nå målen för Sveriges säkerhet är det mot denna bakgrund viktigt att ett systematiskt informationssäkerhetsarbete genomförs på bred front i samhället.

Informationssäkerhet bör vara väl integrerat i arbetet med risk-, sårbarhets- och säkerhetsanalyser. Analyserna behandlar bl.a. samhällets förmåga att motstå och hantera allvarliga händelser och verksamheters ömsesidiga beroendeförhållanden.

Förmåga att hantera it-angrepp är nödvändig främst för att minska risken för, och konsekvenser av, allvarliga it-incidenter som drabbar samhällsviktig verksamhet och kritiska infrastruktursystem. Allvarliga it-incidenter som drabbar dessa system och även förluster av mindre mängder information över tid, kan medföra allvarliga konsekvenser och stora kostnader för samhället oavsett om det sker genom medvetna angrepp, misstag eller av olycka.

Ökad digitalisering

Informationsteknikens utveckling har medfört nya former av kommunikation, datahantering och datalagring vilket också innebär nya former för interaktion mellan individer, organisationer och stater. I allt väsentligt är detta en positiv utveckling. Samtidigt medför it-utvecklingen ett större beroende mellan olika sektorer och verksamheter och därmed också ökade sårbarheter. Detta har utvecklats till en av vår tids mest komplexa frågor.

En ökande hantering av personinformation i informationssystem medför också behov av funktioner för att tillgodose den personliga integriteten.

Den 29 september 2011 beslutade regeringen om *It i människans tjänst – en digital agenda för Sverige*, (N II 2, N2011/342/ITP, m.fl.). Av detta beslut framgår regeringens mål att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Detta mål har också antagits av riksdagen (budgetpropositionen för 2012, prop. 2011/12:1, bet. 2011/12:TU1, rskr. 2011/12:87).

Den 13 december 2012 beslutade regeringen om *Med medborgaren i centrum. Regeringens strategi för en digitalt samverkande statsförvaltning*, (N II 10, N2012/6402/ITP m.fl.). Genom att samverka digitalt kan myndigheternas kontakter med medborgarna förenklas, innovation och delaktighet stödjas, samtidigt som statsförvaltningens effektivitet och kvalitet ytterligare kan höjas. En viktig utgångspunkt i all utveckling av statsförvaltningens tjänster är att effektivitet och service alltid måste vägas mot skyddet för den enskildes integritet och behov av sekretesskydd och att medborgarna har tillit till att systemen är säkra.

I dag utgör säkerhet, öppenhet och integritet kopplat till informationssäkerhet en stor utmaning såväl nationellt som internationellt.

En allvarlig it-incident, men även långvariga oupptäckta informationsförluster, bedöms kunna få stora konsekvenser för den svenska ekonomin, för samhällsviktig verksamhet, kritisk infrastruktur och för enskilda individer.

Internet används för både civila och militära ändamål och såväl staters som individers och organisationers säkerhet måste tillgodoses. Handel, immaterialrätt, tekniköverföring, nätsäkerhet, frågor om kritisk infrastruktur, demokrati, mänskliga rättigheter, bistånd och it-brott hänger samman med säkerhetspolitiska och försvarspolitiska överväganden och utgör delar av samma problemkomplex. Det medför att en ansats att hantera problem inom området bör koppla samman dessa frågeställningar.

Hot mot elektroniska kommunikationsnät och it-system

Hoten mot elektroniska kommunikationsnät och it-system är mångfacetterade, komplexa, svårdefinierade och föränderliga. Hot utgörs av allt ifrån tekniska fel till den mänskliga faktorn och medvetna handlingar. Utöver detta är det inte ovanligt att t.ex. väderfenomen, naturkatastrofer och olyckor orsakar incidenter med it-inslag.

It-angrepp kan utgöras av intrång som syftar till att störa funktionaliteten, förändra, stjäla eller manipulera information eller helt ta över ett informationssystem. It-angrepp mot samhällsviktig verksamhet och kritisk infrastruktur, såväl statlig som privat, kan också syfta till att begränsa tillgången till information eller funktioner. Ett exempel på sådana angrepp är överbelastningsattacker. En aktör kan också via it-angrepp störa, slå ut eller skaffa sig tillgång till styr- och kontrollsystem samt ledningscentraler för samhällsviktig verksamhet och kritiska infrastrukturer, exempelvis telenät, elnät, transportsystem, finanssystem, va-verk, processindustrier eller militära ledningssystem. Sådana it-angrepp kan förekomma såväl i fredstid som under kris eller krig och kan användas för att komplettera konventionella militära förmågor. Utvecklingen av militära it-förmågor internationellt innebär att även Sverige måste förhålla sig till nya krav på hur man försvarar sig mot en motståndare som har tillgång till sådana förmågor.

Det sker en ansenlig mängd brottsliga angrepp inriktade på att kompromettera informationssystem för att otillbörligen komma åt information. Spionage sker i ökad omfattning och utförs såväl av stater som av organisationer och enskilda.

Det är tydligt att verksamhetskritisk och känslig information inom både det offentliga och det privata är potentiella mål för olika typer av angrepp. Ett annat hot är att ökande krav på säkerhetsåtgärder i elektroniska kommunikationsnät, it-system och på internet riskerar att leda till inskränkningar av mänskliga rättigheter med stora politiska, sociala och ekonomiska konsekvenser som följd. Särskilt på det internationella planet är detta en oroväckande trend som ofta grundar sig i olika definitioner av begreppet säkerhet och där vissa regimer använder säkerhet som skäl för att kontrollera den egna befolkningen.

Ansvar och samverkan mellan samhällsaktörer

Att öka förmågan att förebygga och hantera allvarliga it-incidenter som drabbar samhällsviktig verksamhet är inte en uppgift för en enskild aktör eller myndighet utan något som privata och offentliga aktörer tillsammans bör bidra till. Nationell och internationell samverkan mellan militära och civila statliga myndigheter, inklusive försvarsunderrättelseverksamheten, och med kommuner och landsting är en förutsättning för att kunna förebygga, förhindra och hantera dessa risker. Övningar är ett viktigt instrument för att förbättra förutsättningarna för samverkan samt att identifiera, åtgärda och förebygga brister.

Grunden för samhällets krisberedskap är ansvarsprincipen (propositionen Stärkt krisberedskap – för säkerhets skull, prop. 2007/08:92, bet. 2007/08:FöU12, rskr. 2007/08:193-194). Det innebär att den som har ansvar för en verksamhet under normala förhållanden också har det under allvarliga händelser, kriser eller krig. I ansvarsprincipen ingår även att samverka och samordna sig med andra aktörer i den omfattning som krävs för att effektivt förebygga och hantera en allvarlig händelse.

Internationellt

It-utvecklingen utmanar många traditionella föreställningar om säkerhetspolitikens omfattning, aktörer och logik. Ökat beroende av elektroniska kommunikationsnät och it-system förutsätter internationell samverkan. Internationellt är det viktigt att Sverige har en tydlig inriktning på området för att kunna påverka den säkerhetspolitiska utvecklingen. En stor utmaning i arbetet är staters skilda syn på hotbilder, doktriner och definitioner kopplade till informationssäkerhet. En tydlig skiljelinje är staters olika syn på hur grundläggande mänskliga rättigheter som yttrandefrihet förhåller sig till nationellt definierade säkerhets- och suveränitetsaspekter. För att alla på bästa sätt ska kunna nyttja de möjligheter som informationstekniken ger behöver frihet, öppenhet och säkerhet för användarna baserat på rättsstatsprincipen utgöra en självklar grund för informationssäkerhetsarbetet.

Att kunna upprätthålla en öppen, säker, motståndskraftig och tillförlitlig elektronisk kommunikationsmiljö är betydelsefullt för alla länder, och säkerheten för Sverige är beroende av den globala utvecklingen.

I strategin för Europeiska unionens inre säkerhet (ISS) konstateras att it-brottslighet är ett hot särskilt mot medlemsstaternas informationssystem. EU-kommissionen och utrikestjänsten (EEAS) har presenterat en övergripande europeisk cybersäkerhetsstrategi som berör både EU-interna som EU-externa aspekter av it-frågor (JOIN(2013) 1 final). Den digitala agendan för Europa ägnar ett avsnitt åt it-brottslighet och it-attacker mot informationssystem samt ett avsnitt om tillit och säkerhet. OECD-länderna har antagit flera rekommendationer som berör informationssäkerhet och internetpolicy. Organisationen genomför också analyser av området, bl.a. av nationella informationssäkerhetsstrategier som under senare år antagits i ett flertal länder.

Uppdraget

Föreslå en strategi och mål för samhällets informationssäkerhet

Myndigheternas arbete med informationssäkerhet ska bedrivas utifrån en nationell strategi som tar sin utgångspunkt i att värna befolkningens liv och hälsa, samhällets funktionalitet samt förmågan att upprätthålla grundläggande värden som demokrati, rättsäkerhet och mänskliga fri- och rättigheter. Att stärka samhällets säkerhet kräver att skyddsvärden, hot och skyddsmedel ses i ett sammanhang. Denna helhetssyn bör genomsyra verksamhet över hela kedjan från orsaksförebyggande och sårbarhetsreducerade till hanterande och återuppbyggande verksamhet.

Informationssäkerhet är en betydelsefull del i arbetet med att nå målen för Sveriges säkerhet och samhällets krisberedskap. Därför bör arbetet med att stärka informationssäkerheten vara en del av det allmänna säkerhets- och krisberedskapsarbetet. För att hålla samman såväl det nationella som det internationella arbetet inom informationssäkerhetsområdet och för att nå Sveriges politiska mål är det viktigt med en nationell strategi som bl.a. tar sin utgångspunkt i en bred säkerhetspolitisk kontext. Strategin ska ta sin utgångspunkt i målen för Sveriges säkerhet och målen för samhällets krisberedskap.

Strategin ska utgå från, och även kunna bidra till, fortsatt utveckling av politiska prioriteringar på området. Strategin ska innehålla övergripande mål samt utgångspunkter för hur aktörer i samhället ska samverka i arbetet med att förebygga, upptäcka, ingripa mot och agera i samband med allvarliga it-incidenter som drabbar samhällsviktig verksamhet.

De övergripande målen ska utformas så att de ger mål, riktlinjer för och prioriteringar som kan ligga till grund för myndigheternas eget informationssäkerhetsarbete. Utredaren ska ta hänsyn till den internationella samverkan som existerar på området, åtaganden som ålagts Sverige till följd av internationella konventioner samt Sveriges förpliktelser som EU-medlem. Den nationella strategin för hantering och överföring av information i elektroniska kommunikationsnät och it-system ska ses som ett övergripande sammanhållet ramverk för hur arbetet med informationssäkerhet ska bedrivas i Sverige. Det förutsätts att mer nedbrutna detaljerade riktlinjer och handlingsplaner skapas för delområden och sektorer i

samhället inklusive det militära försvaret och försvarsunderrättelseverksamheten.

Den nationella strategin för hantering och överföring av information i elektroniska kommunikationsnät och it-system ska hantera risker på alla nivåer i samhället. Informationssäkerhetsområdet är tvärsektoriellt och omfattar många aktörer i samhället på lokal, regional och central nivå. Även näringslivet har en stor roll i detta arbete. Till detta kommer också den internationella dimensionen där olika aspekter måste beaktas. Den nationella strategin bör inkludera alla relevanta aspekter och aktörer.

Syftet med strategin ska vara att uppnå ett effektivare och mer samordnat arbete med informationssäkerhet i samhället. Strategin ska vara ett stöd för myndigheternas arbete och kopplas till styrmedel och åtgärder för att åstadkomma ett operativt och verksamt arbete med informationssäkerhet i hela samhället. Nuvarande ansvarsförhållanden och åtaganden ska beaktas men inte begränsa utredningen, som ska utgå från ansvarsprincipen och gällande ekonomiska ramar.

Utredaren ska

- föreslå en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system och
- föreslå övergripande mål för samhällets informationssäkerhetsarbete, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur.

Inför arbetet med strategin ska utredaren ta del av de nationella strategier som redan tagits fram av ett flertal länder. Utredaren ska också beakta det arbete som sker på informationssäkerhetsområdet inom bl.a. EU, Nato och OECD.

Definiera begrepp inom området

Uttrycket informationssäkerhet används bl.a. i regeringens propositioner, skrivelser och i vissa författningar, t.ex. myndighetsinstruktioner. Internationellt förekommer ”information security” och ”cyber security”. Dessa uttryck används delvis med över-

lappande betydelse, delvis med olika betydelse utifrån skilda utgångspunkter.

Informationssäkerhet är enligt terminologi för informationssäkerhet (SIS handbok 550 utgåva 3) säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet (även ansvarighet och oavvislighet).

Informationssäkerhet är även ett legaldefinierat begrepp i säkerhetsskyddslagen (1996:627) där det finns bestämmelser om informationssäkerhet till skydd för rikets säkerhet. Säkerhetsskyddslagstiftningen är för närvarande under översyn och utredningen ska redovisa sitt uppdrag i april 2014 (dir. 2011:94).

Mot bakgrund av en ökad internationalisering och behov av interoperabilitet är även en jämförelse med andra nationer och organisationers syn på definitioner viktig. En särskild utmaning är staters skilda syn på hotbilder, regleringsbehov m.m. inom området som lett till skillnader i definitioner och begreppsanvändning. Begreppet informationssäkerhet kopplas av vissa länder till censur och statlig kontroll av medborgarna.

På senare tid har även andra begrepp börjat användas i det svenska språket, framför allt cybersäkerhet och cyberförsvar men även benämningar som digital säkerhet och it-säkerhet förekommer utan att den närmare innebörden av dessa förklarats.

Det finns således ett behov av att definiera begrepp och reda ut hur de förhåller sig till varandra samt vid behov ensa dessa begrepp för att undvika missförstånd. De begrepp eller benämningar som används i dessa kommittédirektiv ska inte föregripa eller begränsa utredarens arbete i detta avseende.

Utredaren ska

- klargöra begrepp som används inom informationssäkerhetsområdet och vid behov föreslå förtydligande eller alternativa benämningar och definitioner, särskilt sådana som används i förslaget till nationell strategi.

Utredningsuppdraget omfattar inte att föreslå förtydligande definitioner av begrepp som används inom ramen för säkerhetsskyddslagstiftningen.

Redovisa roller och ansvar på området

Grunden för samhällets krisberedskap är ansvarsprincipen. Det finns flera statliga myndigheter med särskilda uppgifter eller uppdrag på informationssäkerhetsområdet, såväl nationellt som internationellt, och frågorna spänner över en mängd olika områden och nivåer. De statliga myndigheterna bör utveckla sin förmåga att samverka inom informationssäkerhetsområdet. För att underlätta denna förmåga behövs en enhetlig och samlad beskrivning av respektive myndighets ansvar och roll utifrån dagens uppgifter och uppdrag på informationssäkerhetsområdet.

Utredaren ska

- med utgångspunkt i uppdraget redovisa statliga myndigheters ansvar och roller utifrån de uppgifter och uppdrag på informationssäkerhetsområdet som de har i dag.

Konsekvensbeskrivningar

Utredaren ska beskriva eventuella konsekvenser av sina förslag för statliga myndigheter, landsting, kommuner och andra relevanta aktörer som kan beröras.

Om förslagen påverkar kostnaderna eller intäkterna för staten, landstingen, kommunerna eller enskilda ska en beräkning av dessa konsekvenser redovisas och utredaren föreslå finansiering för detta. Om förslagen får samhällsekonomiska konsekvenser i övrigt ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, landstingen eller kommunerna ska utredaren föreslå en finansiering. Sådan finansiering ska föreslås ske inom området och gällande ekonomiska ramar.

Om något av förslagen påverkar det kommunala självstyret ska utredaren särskilt redovisa dessa konsekvenser och de särskilda avvägningar som lett till förslagen, i enlighet med bestämmelserna i 14 kap. 2 och 3 §§ regeringsformen.

Samråd och redovisning av uppdraget

Utredaren ska löpande hålla Regeringskansliet (Försvarsdepartementet) informerat.

Vidare ska utredaren hålla sig informerad om och beakta relevant arbete om informationssäkerhetsfrågor som pågår inom Regeringskansliet och i utredningar, som t.ex. Försvarsberedningens arbete. Utredaren ska även hålla sig informerad om och beakta Utredningen om säkerhetsskyddslagen (Ju 2011:14), Utredningen om förbättrad tillgång till personuppgifter inom och mellan hälso- och sjukvården och socialtjänsten (S 2011:13), Sveriges Kommuner och Landstings insatser inom området eSamhället, den Digitala agendan för Sverige, e-förvaltningsstrategin, den europeiska cybersäkerhetsstrategin, kommissionens förslag till direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen (COM (2013) 48 final), det arbete som pågår inom ramen för regeringens arbete med EU:s digitala agenda, e-förvaltning och allmän uppgiftsskyddsförordning (COM(2012) 11 final) samt andra relevanta internationella dokument. I det fall EU beslutar om direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen ska det beaktas i arbetet med strategin. Utredaren ska också beakta andra länders samt nationella och internationella organisationers strategier för informationssäkerhet. Utredaren bör även beakta nuvarande politik som bedrivs på området.

Uppdraget ska redovisas senast den 1 december 2014.

(Försvarsdepartementet)

Kommittédirektiv 2014:66

Tilläggsdirektiv till NISU 2014 (Fö 2013:04)

Beslut vid regeringssammanträde den 8 maj 2014

Utvidgning av uppdraget

Regeringen beslutade den 28 november 2013 kommittédirektiv om strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system (dir. 2013:110). Utredningen har tagit namnet NISU 2014.

Utöver det ursprungliga uppdraget ska utredaren undersöka de rättsliga förutsättningarna för SOS Alarm Sverige AB (SOS Alarm) att inrätta och driva ett system för viktigt meddelande till allmänheten (VMA) via mobil och fast telefoni vid allvarliga olyckor och kriser. Utredaren ska i det sammanhanget undersöka om det finns behov av ny eller ändrad lagstiftning och i så fall lämna fullständiga författningsförslag.

Detta tilläggsuppdrag ska redovisas senast den 31 december 2014. Det ursprungliga uppdraget ska fortfarande redovisas senast den 1 december 2014.

Viktigt meddelande till allmänheten

Programföretag som sänder radio och tv har under lång tid omfattats av krav att sända viktiga meddelanden till allmänheten. Av 4 kap. 9 § 15 radio- och tv-lagen (2010:696) framgår att ett tillstånd att sända tv eller sökbar text-tv får förenas med villkor om skyldig-

het att kostnadsfritt sända meddelanden som är av vikt för allmänheten, om en myndighet begär det. Det finns möjlighet att ställa sådana villkor även för ljudradio, se 11 kap. 3 § 15 samma lag. Enligt sändningstillstånden för Sveriges Radio AB och Sveriges Television AB, vilka beslutades av regeringen den 19 december 2013, ska bolagen kostnadsfritt sända meddelanden som är av vikt för allmänheten om en myndighet begär det (Ku2013/2524/MFI och Ku2013/2525/MFI).

Att ett system för varning och information genom mobiltelefoner bör införas stegvis anges i propositionen Samverkan vid kris – för ett säkrare samhälle (prop. 2005/06:133, bet. 2005/06:FöU9, rskr. 2005/06:295-296).

Regeringen bemyndigade den 20 november 2008 (Fö2008/3431/SSK) chefen för Försvarsdepartementet att underteckna alarmeringsavtalet (Fö2008/3587/SSK) mellan Svenska staten och SOS Alarm. I regeringsbeslut den 28 februari 2013 (Fö2013/468/SSK) anges att parterna efter förhandling enats om tillägg till alarmeringsavtalet som innebär att SOS Alarm under 2013 ska inrätta ett nytt tekniskt system för VMA via mobil och fast telefoni vid allvarliga olyckor och kriser. SOS Alarm ska därefter svara för driften och underhållet av systemet. Det nya tekniska systemet ska komplettera de befintliga systemen för varning. SOS Alarm ska enligt tilläggsavtalet även i samverkan med berörda aktörer undersöka förutsättningarna för att med det nya tekniska systemet nå svenska mobilabonnenter som befinner sig i annat land i händelse av en allvarlig olycka eller kris. SOS Alarm ska vidare under 2013 säkerställa att ansvariga aktörer bereds möjlighet att leverera samordnad och kvalitetssäkrad VMA vid allvarliga olyckor och kriser. Tjänsten ska vara en del av det totala VMA-systemet. I regeringsbeslut den 13 februari 2014 (Fö2014/280/SSK) anges att parterna enats om att ovan nämnda uppdrag ska fortsätta under 2014.

Under arbetet med att inrätta ett system för VMA via mobil och fast telefoni vid allvarliga olyckor och kriser har SOS Alarm uppmärksammat regeringen på att det kan finnas behov av ändringar i befintlig lagstiftning för att SOS Alarm ska kunna inrätta och driva systemet. SOS Alarm gör bedömningen att föreslagen behandling av abonnentuppgifter kan ske med stöd av personuppgiftslagen (1998:204). Enligt SOS Alarm krävs det emellertid reglering i lagen

(2003:389) om elektronisk kommunikation för att teleoperatörer ska kunna skicka VMA per sms till de mobilabonnenter som befinner sig inom ett visst drabbat område, (N2013/5082/ITP).

Tilläggsuppdraget om ett system för viktigt meddelande till allmänheten

Att varna eller informera allmänheten vid olyckor eller vid överhängande fara för olyckor, andra allvarliga händelser eller för spridning av allvarlig smittsam sjukdom är viktigt för att hindra och begränsa skador på liv, hälsa, egendom eller miljö. Utnyttjande av informationsteknik och elektroniska kommunikationsnät kan vara ett värdefullt komplement till det befintliga VMA-systemet. Det är angeläget att varnings- och informationsarbetet präglas av snabbhet och tydlighet. Detta ställer stora krav på de tekniska systemens tillgänglighet och säkerhet. Det är också viktigt att det finns rättsliga förutsättningar för att systemet ska kunna användas på ett lämpligt och effektivt sätt.

Utöver det ursprungliga uppdraget ska utredaren

- undersöka de rättsliga förutsättningarna för SOS Alarm att inrätta och driva ett system för VMA via mobil och fast telefoni vid allvarliga olyckor och kriser,
- i sitt arbete särskilt uppmärksamma behovet av skydd för den personliga integriteten, och
- undersöka om det finns behov av ny eller ändrad lagstiftning och i så fall lämna fullständiga författningsförslag.

I uppdraget ingår inte att bedöma eller ta ställning till olika tekniska lösningar som kan användas för att inrätta eller driva VMA.

Konsekvensbeskrivningar

Utredaren ska beskriva eventuella konsekvenser av sina förslag för statliga myndigheter, landsting, kommuner, operatörer och andra relevanta aktörer som kan beröras.

Om förslagen påverkar kostnaderna eller intäkterna för staten, landstingen, kommunerna eller enskilda ska en beräkning av dessa

konsekvenser redovisas och utredaren ska föreslå finansiering för detta. Om förslagen får konkurrensmässiga eller samhällsekonomiska konsekvenser i övrigt ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, landstingen eller kommunerna ska utredaren föreslå en finansiering. Sådan finansiering ska föreslås ske inom området och gällande ekonomiska ramar.

Om något av förslagen påverkar det kommunala självstyret ska utredaren särskilt redovisa dessa konsekvenser och de särskilda avvägningar som lett till förslagen, i enlighet med bestämmelserna i 14 kap. 2 och 3 §§ regeringsformen.

Samråd och redovisning av tilläggsuppdraget

Utredaren ska löpande hålla Regeringskansliet (Försvarsdepartementet) informerat om arbetet. Vid genomförande av tilläggsuppdraget ska utredaren inhämta synpunkter från SOS Alarm, Datainspektionen, Myndigheten för samhällsskydd och beredskap och Post- och telestyrelsen.

Detta tilläggsuppdrag ska redovisas senast den 31 december 2014. Det ursprungliga uppdraget ska fortfarande redovisas senast den 1 december 2014.

(Försvarsdepartementet)

Kommittédirektiv 2014:152

Tilläggsdirektiv till NISU 2014 (Fö 2013:04)

Beslut vid regeringssammanträde den 27 november 2014

Förlängd tid för uppdraget

Regeringen beslutade den 28 november 2013 kommittédirektiv om bl.a. en nationell strategi för hantering och överföring av information i elektroniska kommunikationsnät och it-system (dir. 2013:110).

Regeringen beslutade den 8 maj 2014 tilläggsdirektiv till utredaren. Enligt tilläggsdirektivet ska utredaren även undersöka de rättsliga förutsättningarna för SOS Alarm att inrätta och driva ett system för viktigt meddelande till allmänheten (VMA) via mobil och fast telefoni vid allvarliga olyckor samt undersöka om det finns behov av ny eller ändrad lagstiftning och i så fall lämna fullständiga författningsförslag (dir. 2014:66).

Det ursprungliga uppdraget (dir. 2013:110) skulle redovisas senast den 1 december 2014. Utredningstiden förlängs nu. Uppdraget ska istället redovisas senast den 1 mars 2015.

Tilläggsuppdraget enligt dir. 2014:66 ska fortfarande redovisas senast den 31 december 2014.

(Försvarsdepartementet)

MSB Dnr: 2014-105

Förslag till nationell strategi och åtgärdsplan för säkra kryptografiska funktioner

Rapporten är ett resultat från ett myndighetsgemensamt projekt mellan Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt (FRA), Försvarsmakten (FM) och Försvarets materielverk (FMV)

Syfte

Syftet med denna rapport är att föreslå

- en nationell strategi och åtgärdsplan för hantering och överföring av information i elektroniska kommunikationsnät och it-system med hjälp av kryptering även för den information som inte faller in under signalskyddstjänstens mandat
- övergripande mål för samhällets informationssäkerhetsarbete relaterat till kryptografi, och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur med hjälp av kryptografiska funktioner.

Rapporten är avsedd att utgöra underlag till NISU 2014-utredningen, som ska föreslå en strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och it-system.

Rapporten är ett resultat från ett myndighetsgemensamt projekt mellan Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt (FRA), Försvarsmakten (FM) och Försvarets materielverk (FMV). MSB är initiativtagare till projektet. Rapporten har tagits fram genom dokumentstudier och intervjuer av ett antal nationella experter inom området, både från den offentliga sektorn och från kryptoindustrin.

Bakgrund och problembeskrivning

Kryptologi är grunden för säker informations- och kommunikationsteknologi

Innan moderna, så kallade asymmetriska, algoritmer uppfanns på 1970-talet (Diffie-Hellman för nyckelutbyte och RSA-algoritmen för kryptering, autentisering och signering) var myndigheter och försvarssektorn de centrala användarna av krypto. Men introduktionen av Diffie-Hellman och RSA ledde till att krypto började användas även i kommersiella produkter och konsumtionsprodukter. Exempelvis för att skydda data både medan den skickas över ett nätverk (data i transit) och när den lagras, till exempel på en hårddisk, smarta telefoner eller ett flashminne (data i vila).

Produkter som modem, digitalboxar, smarta kort och SIM-kort använder alla kryptering. Moderna kommunikationsprotokoll som SSH, S/MIME och SSL/TLS som används för att skydda data som överförs på internet baseras på kryptering. Kryptering används för att skydda data i transit som skickas från alla typer av enheter i alla sorters nätverk, inte bara på internet. Varje gång någon använder en bankomat eller köper något på nätet med en smart telefon, gör ett mobilsamtal eller trycker på en nyckelbricka för att låsa upp en bil, är det kryptering som används för att autentisera användaren och skydda den information som förmedlas. Skydd som förhindrar obehörig användning eller reproduktion av upphovsrättsskyddat material är ännu ett exempel på kryptering för att skydda data.

Engångslösenordsgeneratorer, säkra betalningar, inpasseringssystem, säker inloggning till datatjänster lokalt eller via nätverk är några av väldigt många applikationer där säkerheten baseras på kryptering.

Samhällets förmåga till hantering och överföring av information i elektroniska kommunikationsnät och it-system och Sveriges förmåga att upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur står och faller med vår förmåga att försäkra oss om att kryptolösningen är väl vald för ändamålet, att den är korrekt implementerad och att den används på rätt sätt.

Säker kryptering är ett fundamentalt behov i it-samhället

Samhället har på senare år blivit allt mer it-beroende – ett beroende som idag omfattar alla samhällssektorer. It-incidenter kan idag hota kritisk infrastruktur, samhällsviktiga verksamheter och ytterst Sveriges säkerhet. Samhället behöver därför lägga resurser på att förebygga och hantera it-relaterade risker på ett helt annat sätt än tidigare. Den snabba it-utvecklingen medför även en ökad hotbild och de angrepp som svenska myndigheter dagligen utsätts för gör behovet av skydd än mer angeläget.

Samhället har idag därför ett mycket stort och ökande behov av att skydda sin information i olika nivåer. Många organisationer har behov av att skydda information som omfattas av sekretess med hänsyn till rikets säkerhet och behöver signalskydd, men den allra största andelen uppgifter som behöver skyddas ligger på en lägre nivå. Sådana uppgifter kan vara hälso- och sjukvårdsuppgifter, risk- och sårbarhetsanalyser, förundersökningar eller asylärenden.

Informationssäkerhet handlar om att information ska skyddas utifrån krav på dess konfidentialitet, riktighet och tillgänglighet där en vanligt förekommande skyddsåtgärd är användningen av krypto och kryptering av information.

Kryptolösningar används idag inte bara vid kommunikation i traditionell mening för att skydda information som är skyddsvärd eller hemlig (konfidentialitet). Krypton används även till skydd för t.ex. signering av information (riktighet), automatiserade processer i samhällsviktiga funktioner som t.ex. kritiska infrastrukturer (tillgänglighet) och för att kunna följa hur och när information har hanterats och kommunicerats.

Den pågående reformen av det nationella försvaret kan komma att innebära omfattande behov av kryptografiska funktioner i och med återuppbyggnaden av det civila försvaret. Det finns en stark politisk inriktning att planering inför höjd beredskap ska genomföras för civila aktörer, inte minst för de ansvariga myndigheterna. Behovet av såväl signalskydd som andra tillförlitliga krypton kommer att öka för de aktörer i samhället som berörs av planläggningsarbetet för det civila försvaret.

Det finns även ett ökat behov av kryptolösningar genom ökad samverkan med andra stater och internationella organisationer, inte minst inom EU och NATO.

Hur kan säker kryptering uppnås?

Kryptologi används för att implementera säkerhetsfunktioner som skyddar informations konfidentialitet, riktighet och tillgänglighet. Dock krävs det en komplicerad kedja av teknik, processer och kunskap hos användarna för att sådana säkerhetsfunktioner verkligen ska ge det skydd som avsetts.

Nedan listas de viktigaste faktorerna för att kryptolösningar ska vara tillräckligt säkra:

- **Säkra kryptografiska algoritmer**, dvs. att de matematiska algoritmer som ligger till grund för skyddet inte innehåller svagheter som kan utnyttjas av en angripare.
- **Säkra standarder**, dvs. att de matematiska algoritmerna översatts till säkra standarder för datalagring och kommunikation.
- **Säkra it-produkter**, dvs. att produktutvecklarna implementerat valda standarder korrekt och att produkterna i övrigt är fria från sårbarheter som skulle kunna utnyttjas av en angripare.
- **Säkra systemarkitekturer**, dvs. att it-produkterna kombinerats på ett sådant sätt att det önskade skyddet uppnås.
- **Säkra systemimplementationer,** dvs. att systemintegratörer skapar system där krypteringsfunktionerna används korrekt, upplevs tillräckligt användaranpassade och inte innehåller konfigurationsmisstag eller andra sårbarheter som kan användas av en angripare.
- **Säker nyckelhantering**, dvs. att de krypteringsnycklar som används i förekommande fall har genererats, distribueras, används och destrueras på ett säkert sätt, dvs. så att nycklarna inte i något led i kedjan kan användas av någon obehörig.
- **Utbildade användare**, som förstår hur de använder systemen korrekt, som är medvetna om riskerna med felaktig användning samt omedelbart anmäler förlorade nycklar och andra relevanta incidenter.

Vart och ett av ovan områden är en nödvändig och fundamental faktor för att kunna etablera säker kommunikation och säkra it-lösningar.

Kryptoincidenter kan vara utomordentligt samhällsfarliga

Om någon av faktorerna som redovisats i föregående avsnitt inte är korrekt omhändertagna kan det få oerhörda effekter på individer, grupper, företag eller t.o.m. hela samhället. Några exempel:

Brister i kryptografiska algoritmer: Om en krypteringsalgoritms styrka innehåller svagheter kan (i värsta fall) samtliga säkerhetsfunktioner som baseras på denna algoritm slås ut i det ögonblick detta blir allmänt känt. Det skulle inte gå att skilja en korrekt transaktion från en förfalskad. Det skulle t.ex. innebära att (för de tjänster som baseras på algoritmen) samtliga e-legitimationer skulle gå att förfalska och all datatrafik gå att avlyssna eller förfalska. Inloggningar är inte längre säkra. All information som någonsin krypterats med en komprometterad algoritm måste betraktas som röjd. Detta kan leda till ohyggligt omfattande informationsförluster. En sådant incident vore direkt samhällsfarlig. Tidigare har flera väl etablerade kryptoalgoritmer fasats ut då brister i dessa har blivit kända.

Brister i kryptografiska standarder: Om en standard skulle innehålla brister kan det få liknande konsekvenser som ovan, till dess att standarden åtgärdats och samtliga system uppdaterats. Även denna typ av incident kan bli direkt samhällsfarlig, eftersom den kan komma att omfatta många produkter och system samtidigt och det kan ta lång tid innan nödvändiga uppdateringar genomförts. Historiskt har flera sådana brister upptäckts.

Brister i it-produkter: Om kryptostandarden är felaktigt implementerad i en produkt på ett sådant sätt att det finns brister, kan samtliga system där en sådan produkt finns installerad drabbas hårt. Beroende på den enskilda produktens spridning och användningsområde kan sådana incidenter drabba berörda användare hårt och även bli samhällsfarliga.

Bristfälliga systemarkitekturer: Att etablera säkra system utgående från komponenter (it-produkter) är en komplicerad uppgift som kräver särskild kompetens. Om ett system inte har rätt arkitektur kan det leda till brister vilka kan leda till mer eller mindre allvarliga incidenter för det berörda systemet. På nationell nivå är det rimligt att anta att det finns många system med bristfällig arkitektur (eller implementation, se nästa exempel). Om det finns många sådana system leder det till en aggregering av risk och att viktiga samhällsfunktioner inte har it-system som är robusta nog.

Fel i systemimplementationer: Om en systemintegratör gör misstag då ett visst system etableras kan den berörda verksamheten drabbas av mer eller mindre allvarliga incidenter. En sådan incident kan vara allvarlig för det berörda systemet.

Osäker nyckelhantering: Om nyckelhanteringen inte är säker, kan samtlig information som skyddats med den/de berörda nycklarna vara komprometterad. Om en nyckel röjts är all information som krypterats med denna nyckel att betrakta som komprometterad. Eftersom nycklar i många tillämpningar inte byts ut regelbundet kan detta innebära mycket stora informationsförluster. Beroende på den information som skyddats kan nyckelincidenter vara mycket allvarliga.

Outbildade användare: Om användarna inte är utbildade kan det leda till nyckelincidenter och/eller att obehöriga får tillgång till systemen, vilket kan få följdverkningar.

Som framgår av ovan finns det olika former av brister som kan omfatta olika stora delar av kritisk infrastruktur och få olika långtgående konsekvenser för samhället. I samtliga fall där ovan faktorer kan leda till allvarliga it-incidenter eller vara samhällsfarliga finns det därmed anledning för staten att ha en strategi för hur dessa frågor omhändertas.

Bristen på styrning ger falsk trygghet

Som beskrivits i föregående avsnitt är det flera faktorer som måste vara korrekt hanterade för att önskat skydd ska erhållas. Det är en komplicerad kedja av aspekter som var och en är vital, och som var och en måste hanteras och därmed styras.

Bristen på styrning har visat sig ge en falsk trygghet, för även om moderna kryptokomponenter har en oerhört stor potential att ge det skydd vi behöver så är tekniken i sin grund avancerad och därför är fallgroparna många för den som inte har tillräcklig kompetens inom området.

Varje länk som innehåller svagheter i denna kedja är en attackvektor för att kringgå den skyddsnivå man vill upprätthålla. Beroende på hur lätt det är att utnyttja svagheten och var i kedjan svagheten finns blir konsekvenserna olika allvarliga. Lite kort kan man säga att ju tidigare i kedjan som bristerna finns, ju större omfattning får konsekvenserna.

Att tro att en verksamhet är säker för att man använder kryptering leder i många fall till en falsk trygghet, där riskerna kan vara mycket större än man tror. Enbart när samtliga faktorer som angivits i föregående avsnitt är väl hanterade kan man anse att skyddet är adekvat.

Signalskyddstjänsten och Krypto för Skyddsvärda Uppgifter (KSU)

Samhällets mest skyddsvärda uppgifter skyddas i dag av signalskyddstjänsten. Signalskyddstjänsten omhändertar kryptobehovet, med beaktande av ovan nämnda risker, för information som kan leda till men för rikets säkerhet och skyddet mot terrorism.

Signalskyddstjänsten vidtar åtgärder som syftar till att förhindra obehörig insyn i och påverkan av tele- och radiokommunikationer med hjälp av signalskydd. Termen signalskydd har sina rötter i den signalspaning som ständigt pågår mot telekommunikations- och informationssystem som en väsentlig del av främmande makts underrättelsetjänst. Utveckling av signalskyddssystem ställer stora krav på leverantörens kunskap och processer. För att uppnå den tillförlitlighet (assurans) som krävs är det också nödvändigt att ha nationella kryptoleverantörer.

Begreppet signalskydd är starkt reglerat och avser obligatoriskt skydd av elektronisk kommunikation av sekretessbelagda uppgifter som rör rikets säkerhet. Signalskyddssystemens skyddsnivå är dimensionerad att möta hotbilden från andra länders underrättelsetjänster.

För att svara upp mot det ökade behovet av kryptografiskt skydd har det på senare år tagits fram en ny klass för nationellt godkända krypton – *krypto för skyddsvärda uppgifter* (KSU) – vilket ska skydda annan skyddsvärd information än den som är hemlig med hänsyn till rikets säkerhet. Sådana krypton ska vara kommersiella produkter som genomgått en djupare granskning och som omgärdas av ett regelverk för att uppnå avsett skydd. Det är dock inte rimligt att alla kryptobehov i samhället kan täckas av nationellt godkända krypton såsom signalskydd eller KSU. För det första är behovet alldeles för stort för att kunna täckas in av de ansvariga myndigheternas förmåga att upprätthålla en sådan stor mängd tillgängliga lösningar. För det andra finns det ingen anledning för någon att lägga den ekonomiska eller administrativa bördan det innebär att upprätthålla den skyddsnivå ett nationellt godkänt krypto innebär för den stora mängden trafik. Här måste kostnaderna ställas i relation till skyddsvärdet på den information som ska skyddas.

Tillämpningen av KSU kan inte skalas upp till att täcka hela det allmänna behovet av att skydda känslig eller sekretessbelagd information som inte rör rikets säkerhet inom kritisk infrastruktur eller samhällsviktig verksamhet, även om kraven är lägre för KSU jämfört med signalskydd.

Denna rapport ger förslag på hur framförallt området utanför signalskyddets domän ska hanteras. Ett sådant regelverk måste utgå från kommersiella grunder.

Sverige saknar förmåga att utvärdera it-produkter som ska motstå fysiska angrepp

En av de stora utmaningarna inom informationssäkerhetsområdet idag är de oerhört stora mängder information som kan lagras i olika former av bärbar datautrustning, till exempel USB-minnen, mobiltelefoner och bärbara datorer. En av de vanligaste orsakerna till stora sekretessförluster är stöld eller förlust av sådan utrustning. Genom kryptering av information som lagras på bärbar datautrustning kan sekretessförlust i flertalet fall förebyggas. Ett sådant krypteringsskydd förutsätter dock att det kan motstå angripare som får fysisk tillgång till upphittad utrustning. En sådan angripare kan genom olika former av fysiska attacker röja kryptonyckeln och därigenom få åtkomst till den krypterade informationen.

Risken för sådana fysiska attacker har ökat markant eftersom tillgången till kunskap om hur dessa fysiska attacker kan genomföras får ökad spridning, samtidigt som den utrustning som behövs för att genomföra attackerna i många fall blivit mycket billigare. Om det fysiska skyddet av kryptonycklarna inte är korrekt utformat finns det en tilltagande risk att en motiverad angripare framgångsrikt kan forcera skyddet hos en upphittad eller stulen bärbar datorutrustning, trots att informationen är krypterad. Det finns en lång rad exempel där olika former av skydd av information i bärbara enheter haft allvarliga brister vilket fått till följd att informationen kunnat läsas utan större insatser.

Till skillnad från andra ledande länder inom it-säkerhetsområdet (t.ex. Storbritannien, Tyskland, Nederländerna och Spanien) saknar Sverige idag ett nationellt kompetenscentrum för att analysera hur sådana attacker genomförs och hur de kan förhindras genom lämpliga tekniska lösningar, även i det fall angriparen har tillgång till datorutrustningen. Konsekvensen av detta är att svenska myndigheter och leverantörer i många fall måste vända sig till andra länder för att få produkter prövade. Bristen på nationell kompetens inom området innebär även en väsentlig risk att information i bärbar utrustning inte har det skydd som utlovats.

Sverige bör etablera en egen förmåga att analysera hur fysiska attacker mot information i bärbar datorutrustning kan genomföras och förebyggas, se förslag på uppdrag till FMV/CSEC i avsnitt 5.2 punkt f.

Nationellt godkända krypton vs CC-certifierade produkter

Eftersom nationellt godkända krypton inte kan omhänderta samhällets behov i stort så bygger de flesta säkerhetslösningar på allmänt tillgängliga kommersiella produkter, så kallade COTS[1]. Fördelarna med dessa är att det finns ett stort utbud och att det är enkelt att köpa dem. Nackdelarna med kommersiellt tillgängliga produkter, i jämförelse med nationellt godkända krypton, är att myndigheterna måste förlita sig på att leverantören av produkterna levererar den säkerhetsfunktionalitet de utlovar.

Ett sätt att skapa en kommersiellt driven process för att tillgodose samhället med kryptolösningar med tillräcklig kvalitet är att låta kommersiella leverantörer bekosta evalueringar av sina produkter genom ett internationellt erkänt certifieringssystem som Common Criteria (CC) inom ramen för CCRA-överenskommelsen[2].

Men att låta sin produkt genomgå en CC-granskning kan vara kostsamt och leverantörerna har idag i många fall inga incitament att genomgå denna typ av process eftersom de inte vet om de skulle få tillbaka sin investering. Därför finns idag ett stort gap mellan de nationellt godkända och kvalitetssäkrade kryptosystemen och alla andra tillgängliga lösningar.

Denna rapport föreslår en strategi som kombinerar kommersiell kryptogranskning baserad på internationell eller nationell standard, med nationell granskning och godkännande av kryptosystem. I kombination med lämpliga lösningar på arkitekturnivå kan gapet då överbryggas.

[1] Commercial off-the-shelf.
[2] Common Criteria Recognition Arrangement.

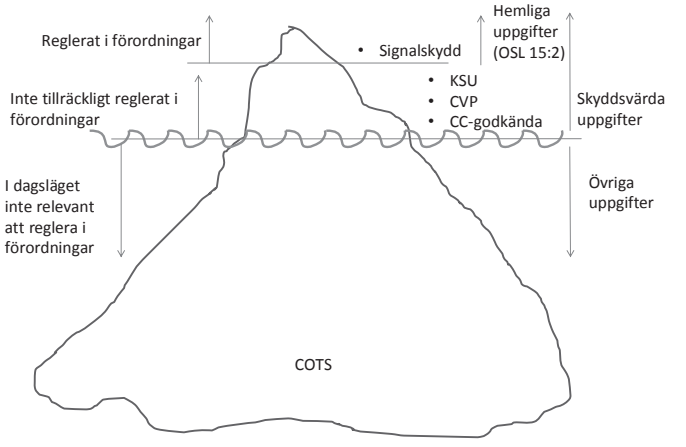


Bild 1 Om statens samlade informationstillgångar och infrastrukturer liknas med ett isberg där skyddsvärdet stiger med höjden ovanför isbergets lägsta punkt, så är kryptoanvändningen idag reglerad på en ytterst liten del av toppen på isberget. Enligt detta förslag lämnas större delen utan reglering (den del som finns ”under ytan”), medan en mindre del skyddas med CC-godkända krypton (internationell standard), CVP (nationella tillägg till internationell standard), nationellt godkända kommersiella krypton (KSU) samt (högst upp) signalskydd. Indelningen är ett förslag till att öka informationssäkerheten till en lämplig nivå kopplat till skyddsvärdet på det som ska skyddas.

Länders strävan att skydda sig leder till tekniska handelshinder

OECD konstaterar i en rapport om det globala cybersamhället att:

> ”… IT and the Internet have become so essential that our economy and society depend on them not only for their development but also for their basic functioning. Today, the stakes are higher and the challenges greater. Cyberspace is inherently international and characterised by interdependencies.”

Nationer står inför ett dilemma: Å ena sidan inför nationer informations- och kommunikationsteknologi (IKT) i mycket stor omfattning för att utveckla tjänster och öka sin konkurrenskraft. Å andra sidan leder denna teknikutveckling till nya och mycket svårkontrollerade risker. Det moderna it-samhället blir effektivt, men samtidigt kolossalt sårbart för cyberattacker. Varje komponent (dvs. it-produkt) i samhällets IKT-infrastruktur kan vara föremål för angrepp i syfte att bedriva spionage och sabotage. IKT-infrastrukturen är en oemotståndlig attackväg för både statsaktörer och it-brottslighet. Angriparen har en låg kostnad, liten risk för upptäckt, svårt att bli avkrävd på ansvar, och via internet har angriparen enorm åtkomst till kritiska system i hela världen.

Allt fler länder inför därför regleringar för att skydda sina kritiska informations- och kommunikationssystem. Exempel på åtgärder:

- krav på användning av nationella kryptografiska standarder
- utveckling av nationella standarder för att ställa krav på produkters design
- krav på certifiering mot dessa standarder i det egna landet
- utveckling av olika former av regelverk som avser att dels reglera den tekniska kontrollen, dels motverka att ”icke tillförlitliga” produkter upphandlas och används.

Denna utveckling har lett till en allvarligt tilltagande protektionism och tekniska handelshinder. Sverige är en exportnation och det är viktigt för Sveriges industri att inte vår export onödigtvis hindras av andra länders regleringar. Därmed blir det viktigt för Sverige att föregå med gott exempel.

En strategi för hur information i elektroniska kommunikationsnät och it-system ska skyddas och hur Sverige ska upprätthålla säkerhet och integritet i samhällsviktig it-infrastruktur, bör därmed beakta handelsaspekten.

Omfattningen av tekniska regleringar med hänvisning till Sveriges säkerhetsintressen måste balanseras mot behovet av frihandel med it-säkerhetsprodukter. Utom för den mest skyddsvärda informationen (vilket inkluderar hemlig information) bör Sverige kunna tillåta användning av utländska kryptoprodukter, samtidigt som rimliga åtgärder vidtas för att tillvarata våra essentiella säkerhetsintressen.

Förutsättningar för strategi och åtgärder

En strategi som utnyttjar myndigheternas samlade kompetens

I Sverige finns idag ett antal myndigheter som av regeringen har tilldelats ett utpekat ansvar att stödja arbetet med samhällets informationssäkerhet, de så kallade SAMFI-myndigheterna[3]. Myndigheterna har olika ansvar, mandat och kompetens inom området. För att staten på ett effektivt sätt ska kunna stödja informationssäkerhetsarbetet i samhället avseende lösningar som baseras på krypton och kryptering, krävs det att myndigheterna får tydliga direktiv för att kunna se till att en nationell strategi för kryptering ska fungera samt att andra relevanta aktörer utöver SAMFI-myndigheterna identifieras.

Att välja rätt kryptering kräver kunskap om teknik och säkerhetspolitik

Samtidigt som kryptering är den främsta skyddsmekanismen i it-samhället (och just därför!) arbetar underrättelseorganisationer och andra aktörer i hela världen med att finna och utnyttja brister i krypteringssystemen för att kunna samla underrättelser och förbereda för cybersabotage. Det avsätts oerhörda resurser för att finna och utnyttja brister i krypteringsalgoritmer, standarder och implementationer till sin egen fördel.

Att skydda de egna kryptosystemen förutsätter därför inte bara en hög kompetens om krypteringens matematik och hur den säkert kan implementeras och användas i det egna landet. Det förutsätter också en förståelse av vilken förmåga andra länders underrättelseorgan kan ha inom området. Detta kräver därmed en helt unik kompetens som för svensk del finns samlad hos Försvarsmakten och Försvarets radioanstalt.

[3] Samverkansgruppen för informationssäkerhet. I SAMFI ingår MSB, FMV, Försvarsmakten, FRA, PTS och Polisen.

En riskbaserad modell

I det här avsnittet visas hur verksamheter kan lösa upphandling och användning av kommersiellt framtagna kryptoprodukter så att de uppnår tillräcklig säkerhet på ett kostnadseffektivt sätt.

Vi har redan noterat att detta innebär stora utmaningar, och att staten för att skydda den mest känsliga informationen utvecklar signalskyddssystem. Hotbilden gör att det ställs mycket höga krav på funktionalitet och assurans. Utvecklingen kännetecknas därför av långa utvecklingstider och höga kostnader. Det ställs också högre krav på genomtänkt livscykelhantering samt välutbildade och säkerhetsmedvetna användare. Av ekonomiska skäl innebär detta att signalskydd endast kan användas för det mest skyddsvärda, dvs. hemlig information.

En rimlig produktstrategi måste därmed baseras på användning av kommersiella produkter. Kommersiella produkter kan vara framtagna utifrån ”statliga” krav, så kallad GOTS[4], eller riktade mot en mer allmän kundmarknad, så kallad COTS. GOTS och COTS kan i varierande nivå uppfylla myndigheters funktionella krav, men i frånvaro av nationell granskning ge mindre assurans.

Denna brist på tillit kan medföra att stater försöker gynna sin egen industri, samtidigt som man bygger murar mot omvärlden för att skydda sig. Ett större land är mer lyckosamt med att driva en sådan strategi. Men för alla kommer det leda till en fragmenterad marknad, långsammare teknologiutveckling, mindre innovation och högre kostnadsnivå.

För mindre länder som Sverige där vi är beroende av att köpa it-säkerhetsprodukter på en internationell marknad leder ett sådant tänkande till dyrare och sämre produkter ur säkerhetssynpunkt. Vi bör i stället uppmuntra och medverka till en gemensam kravställning på global nivå med repeterbara tester av säkerhetsfunktionalitet. Detta ger en adekvat kravställning och en viss grad av förvissning om att krävd funktionalitet är korrekt implementerad. Utan egen granskning på detaljnivå kan vi emellertid aldrig få tillräcklig assurans till alla delar i en produkt, oaktat att vi ändå inte har råd att bekosta detta. Öppenhet och transparens i kravställningen med delaktighet av både myndigheter och industri har potential att resultera i effektiv konkurrens på en global marknad, och där små länder inte behöver betala för assuransåtgärder de inte sätter tillit till.

Ovanstående omsätts nu i praktiken inom CCRA[5] enligt den nya överenskommelsen. För ett importberoende land som vårt leder detta till kostnadseffektiva produkter med känd och adekvat säkerhetsfunktionalitet.

Genom att användningen av certifierade produkter regleras så kommer marknaden i Sverige att växa, fler leverantörer vill konkurrera om marknaden, myndigheter får fler produkter att välja mellan och därmed borde även produkterna bli billigare men samtidigt behålla nivån av säkerhetskrav de uppfyller.

Första delen av vår riskbaserade modell innebär följaktligen att vi förordar att behovet av kryptoprodukter tillgodoses av CC-certifierade produkter baserade på nationellt godkända internationella skyddsprofiler, s.k. cPP:er[6]. Vi undviker då att framtagningen av produkter blir en trång sektor. Produkterna är baserade på funktionella krav som Sverige medverkat till och godkänt.

[4] Government off-the-shelf.
[5] Common Criteria Recognition Arrangement, se https://www.commoncriteriaportal.org.
[6] Collaborative Protection Profile.

Problemet som kvarstår är att assuransen till produkterna i många fall kommer att bli för låg. Det kan finnas missar i implementationen som resulterar i sårbarheter. För att vår riskhanteringsmodell ska bli fullständig måste vi därför komplettera med åtgärder som reducerar risken för sådana sårbarheter till en acceptabel nivå. Ett sådant exempel beskrivs i nästa avsnitt.

Säkrare kommersiella kryptolösningar med kombinationsprincipen

Att granska att en kryptoprodukt är korrekt implementerad och saknar allvarliga sårbarheter som kan leda till incidenter är en mycket komplex och kostnadskrävande uppgift. Det kräver även personal med hög kompetens om kryptologi och it-säkerhet.

Statens begränsade resurser i kombination med den stora mängden produkter som används gör det i praktiken omöjligt att genomföra nationell granskning på samtliga produkter som används i kritiska system.

Samtidigt är det för flera kritiska tillämpningar inte tillräckligt att enbart förlita sig på den nivå av kryptogranskning som kan uppnås inom ramen för CCRA. CCRA har dock fördelen av att vara baserad på internationell standard och ett system för ömsesidigt erkännande av certifikat. Därmed kan långt fler produkter granskas inom ramen för CCRA än vad som är möjligt med nationell granskning.

Vi beskriver här en metod kallad kombinationsprincipen som kan användas för att kompensera för otillräcklig assurans i enskilda produkter. Den kan tillämpas i de fall en kritisk tillämpning behöver skyddas, där CC-certifiering inte bedöms vara tillräckligt och KSU-godkända krypton inte finns.

Kombinationsprincipen innebär att två eller flera produkter kombineras för att skapa flera lager av kryptering. Genom att kombinera CC-certifierade produkter på detta sätt kan riskerna ändå minskas. Säkerheten kan alltså behållas gentemot en angripare som kan utnyttja sårbarheter i en av produkterna.

Standarder används för upphandling och reglering – nationell granskning görs på produkter i drift

Det förslag på strategi som ges i kapitel 4 bygger på en modell som ska användas för att minska riskerna för det generella användandet av it-produkter, skapa kommersiella villkor för industrin samt inte skapa onödiga tekniska handelshinder.

Målet med strategin är att möta behoven av kryptering som skydd för till exempel information som är skyddsvärd, samhällsviktiga system eller kritisk infrastruktur och där det idag saknas reglering för vilka åtgärder en myndighet eller verksamhet behöver vidta för att skydda sina informations-tillgångar. Se markerat område på bild 2 nedan.

MSB ska med stöd av övriga SAMFI-myndigheter kravställa på it-produkter genom deltagandet i internationella tekniska arbetsgrupper inom ramen för CCRA.

MSB ska ge ut föreskrifter om användandet av CC-evaluerade produkter samt upprätta en lista på evaluerade produkter. Statliga myndigheter ska sedan välja evaluerade produkter enligt MSB:s lista.

När MSB identifierat eller ser en stor spridning på användandet av en specifik CC-evaluerad produkt så kan produkten bedömas behöva ytterligare granskning, baserat på omfattningen som produkten används i eller för att produkten till exempel används för att skydda samhällsviktig verksamhet eller

kritisk infrastruktur. MSB beställer då en extra kryptogranskning baserat på CVP[7] vid FMV/CSEC. Detta ger en återkoppling i rapportform över produktens kryptoegenskaper som kan användas vidare för en uppdatering av riskbedömningen. Detta höjer assuransen ytterligare ett steg. Granskningen resulterar också i underlag för återkoppling till den internationella arbetsgruppen där leverantören deltar samt till de myndigheter eller verksamheter som använder den granskade produkten. När CVP-godkännandet är klart kan MSB även hemställa att Försvarsmakten genomför en granskning av produkten och, om den motsvarar kraven, utfärdar ett KSU-godkännande av produkten.

Normalt ska processen för KSU-godkännande föregås av en godkänd CVP-granskning hos FMV/CSEC. Om det finns särskilda skäl kan dock en produkt bli aktuell för KSU-granskning utan föregående CVP-godkännande.

En KSU-granskning av Försvarsmakten ger en återkoppling i rapportform över produktens kryptoegenskaper och om den klarar kraven för nationellt godkännande. Med ett nationellt godkännande följer även ett regelverk kring användningen för att säkerställa avsett skydd. Granskningen används även för en uppdatering av riskbedömningen. Även KSU-granskningen kan resultera i underlag för återkoppling till den internationella arbetsgruppen där leverantören deltar samt till de myndigheter eller verksamheter som använder den granskade produkten.

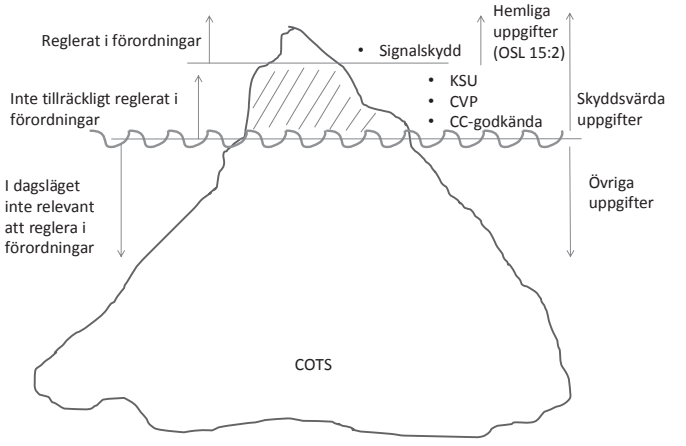


Bild 2 Det streckade området i bilden utgör den delen av skyddsvärd information och skyddsvärda system och infrastrukturer som förslaget på ny kryptostrategi främst försöker täcka in.

[7] Cryptographic validation program.

Förslag till strategi

En nationell strategi för it- och kommunikationssäkerhet bör innehålla mål och åtgärder som borgar för att skyddet för samhällets information och infrastruktur läggs på rätt nivå i förhållande till skyddsvärdet genom att

- statlig förvaltning använder säkra kryptoalgoritmer, kryptoformat och kryptoprotokoll
- statlig förvaltning använder säkra kryptostandarder
- statlig förvaltning använder produkter som genomgått grundläggande kryptoverifiering
- statlig förvaltnings kritiska it-system är säkert konstruerade när det gäller kryptering
- statlig förvaltning utnyttjar internationell standard för att definiera grundläggande krav på design, funktion, implementation och granskning av säkerhetsfunktioner baserade på kryptografi i it-produkter, utökade med kompletterande nationella krav där internationell standard inte motsvarar svenska behov
- statlig förvaltning tillämpar en riskbaserad modell för att öka säkerheten i kryptolösningar under nivån signalskydd
- statlig förvaltning har nödvändig kompetens, processer och teknik för säker nyckelhantering
- statlig förvaltnings personal har relevant utbildning om riskerna med kryptering, samt utbildning om säker användning av kryptosystem
- ansvar för utveckling av signalskyddssystem kvarstår enligt nuvarande ordning
- signalskydd pekas ut som nationellt säkerhetsintresse
- statlig förvaltning har nödvändigt stöd vid riskbedömning, kravställning, upphandling, driftsättning, förvaltning, avveckling och utbildning av kryptosystem.

En svensk nationell strategi för kryptering förutsätter att flera olika myndigheter ges ansvar, resurser och instruktioner som åstadkommer ovan strategi.

Förslag till åtgärder

Utöver den reglering som finns för signalskydd borde övriga kryptosystem regleras ytterligare.

Nedan beskrivs ett förslag på uppgifter som borde ges myndigheterna, i syfte att implementera den föreslagna strategin. Dessa åtgärder ska minska de informationssäkerhetsrelaterade riskerna genom att främja kostnadseffektiva och snabba evalueringar av krypton, som leder till ökad tillgång till säkerhetsrelaterade funktioner.

Regeringens uppdrag till MSB

Föreskrift inom kryptoområdet

MSB bör ges regeringens uppdrag att ta fram föreskrift enligt följande:

Föreskriften bör avse alla krypton som används av eller på uppdrag av statliga myndigheter under regeringen, förutom Försvarsmakten och Regeringskansliet, i syfte att skydda civila kritiska informationsinfrastrukturer och samhällsviktiga system.

Sådana krypton ska uppfylla kraven och vara certifierade i enlighet med MSB:s föreskrivna cPP:er genom FMV/CSEC:s kryptografiska valideringsprogram (CVP) eller i förekommande fall vara KSU-godkända (Krypto för skyddsvärda uppgifter) genom granskning av Förvarsmakten.

Statliga myndigheter under regeringen förutom Försvarsmakten och Regeringskansliet ska

a. välja evaluerade krypton enligt MSB:s upprättade lista över sådana produkter
b. samarbeta med MSB för att identifiera och prioritera nya behov av evaluerade krypton
c. om möjligt delta i utveckling av CC-skyddsprofiler
d. anlita behöriga systemintegratörer upphandlade inom Kammarkollegiets ramavtal
e. utbilda egen personal med stöd av behöriga lärare upphandlade inom Kammarkollegiets ramavtal.

MSB:s ansvar i sin egen verksamhet

MSB ska i sin egen verksamhet ansvara för att

a. utveckla cPP (Collaborative Protection Profiles) samt bidra till tekniska kravställningar för krypton som ska användas i informationsinfrastrukturer och samhällsviktiga system. Utvecklingen ska om möjligt ske i öppna processer i samverkan med berörda myndigheter, leverantörer samt övriga berörda aktörer.
b. utveckla nationella skyddsprofiler där inte internationellt stöd för svenska behov för en cPP finns
c. ge ut föreskrifter och rekommendationer för användning av cPP
d. föra en förteckning över certifierade krypton för användning i kritiska informationsinfrastrukturer och samhällsviktiga system
e. publicera vägledningar för implementering av kommersiella kryptosystem enligt föreskrifter
f. ge uppdrag till Kammarkollegiet i syfte att ta fram ramavtal för upphandling av kommersiella kryptosystem
g. göra risk-/sårbarhetsanalys över vilka kryptoprodukter som används i Sverige och beställa tilläggsgranskning enligt CVP av de mest kritiska produkterna
h. rekommendera till Försvarsmakten vilka produkter som bör bli föremål för KSU-granskning
i. ge ut vägledning och stöd vid val och avseende systemkonstruktion av lämpliga krypton som används i kritiska informationsinfrastrukturer och samhällsviktiga system
j. ge ut årliga analyser kring allvarliga it-incidenter i krypton samt vanligt förekommande handhavandefel av krypton, som ingångsvärden för en eventuell nationell kravställning.

Regeringens uppdrag till FMV/CSEC

FMV/CSEC ska ansvara för att

a. ta fram och utveckla regler för granskning av krypton i kritiska informationsinfrastrukturer och samhällsviktiga produkter och system enligt Common Criteria (CC)
b. granska och godkänna evalueringsföretagens rapporter samt utfärda certifikat vid godkända evalueringar av krypton
c. samverka internationellt för att utveckla en standard för granskning av it-säkerhet och kryptering som motsvarar svenska behov
d. ge stöd till MSB vid utveckling av internationella och nationella PP:ar[8]
e. utveckla CVP, vilket ska bestå av tilläggsregler för kryptogranskning inom ramen för Common Criteria, i de fall där internationell standard inte motsvarar svenska behov
f. i samverkan med MSB, Försvarsmakten och FRA utarbeta ett förslag (med kostnader) för hur Sverige kan erhålla förmågan att utvärdera skyddsåtgärder i it-produkter som ska motstå fysiska angrepp
g. på MSB:s uppdrag göra tilläggsgranskning av kommersiella kryptoprodukter baserat på CVP.

[8] Protection profile.

Regeringens uppdrag till Försvarets radioanstalt (FRA)

Försvarets radioanstalt (FRA) ska ansvara för att

a. analysera kryptotillämpningar på arkitekturnivå i syfte att ge stöd kring att fastställa en rimlig och komplett säkerhetslösning för givna applikationer och miljöer vid kravställning
b. ge stöd till Försvarsmakten vid val av kryptografiska algoritmer, protokoll och standarder.

Regeringens uppdrag till Försvarsmakten

Försvarsmakten ska ansvara för att

a. föreskriva vilka kryptografiska algoritmer, protokoll och standarder som får användas av statliga myndigheter
b. genomföra kryptogranskning och KSU-godkännande
c. ge stöd till FMV/CSEC i deras arbete med utveckling av tilläggsregler för kryptogranskning inom ramen för Common Criteria
d. ge stöd till MSB vid utveckling av internationella och nationella PP:ar.

Regeringens uppdrag till Kammarkollegiet

Kammarkollegiet ska på uppdrag av MSB genomföra ramavtalsupphandlingar av

a. certifierade produkter
b. systemintegratörer som kan krypto
c. utbildningsorganisationer.

Regeringen bör utnämna utvecklingen av signalskydd till ett nationellt säkerhetsintresse

Regeringen bör utpeka och anmäla till EU-kommissionen att utveckling och anskaffning av signalskydd utgör ett nationellt säkerhetsintresse inom försvars- och säkerhetsområdet.

Resurser

För att genomföra ovanstående åtgärder bedöms inledningsvis ett minimum av elva nya årsarbetskrafter tillföras myndigheterna, varav tre till MSB, tre till FM, två till FMV/CSEC, två till FRA samt en till Kammarkollegiet.

Bilaga 1: Nulägesbeskrivning

Vad är signalskydd och KSU?

Signalskydd är åtgärder som syftar till att förhindra obehörig insyn i och påverkan av tele- och radiokommunikationer. Signalskydd omfattar bl.a. användning av kryptografiska funktioner i informationssystem. Termen signalskydd har sina rötter i den avlyssning genom signalspaning som ständigt pågår mot telekommunikations- och informationssystem som en väsentlig del av främmande makts underrättelsetjänst.

Begreppet signalskydd är starkt reglerat och avser obligatoriskt skydd av elektronisk kommunikation av sekretessbelagda uppgifter som rör rikets säkerhet. Signalskyddssystemens skyddsnivå är dimensionerad att möta hotbilden från andra länders underrättelsetjänster och kräver därför omfattande skyddsåtgärder samt att systemen företrädesvis är framtagna av en inhemsk kryptoindustri.

Behovet av att skydda elektronisk kommunikation i bredare mening än för rikets säkerhet har kommit att bli allt mer aktuellt. Därför har det på senare år tagits fram krypto för skyddsvärda uppgifter (KSU). KSU utgörs av kryptosystem som tillsammans med ett regelverk är nationellt godkända av Försvarsmakten och kan användas vid elektronisk kommunikation av sekretessbelagda uppgifter som inte rör rikets säkerhet. KSU är alltså ingen ersättning utan ett komplement till signalskydd. Termen ”säkra kryptografiska funktioner”[9] avser både signalskydd och KSU. Målsättningen med KSU är att kvalitetssäkrade och kommersiellt tillgängliga produkter, tillsammans med ett av Försvarsmakten framtaget regelverk och en för organisationen anpassad hantering, ska kunna höja säkerhetsnivån jämfört med i dag.

För att system som använder säkra kryptografiska funktioner ska kunna ge ett effektivt skydd krävs att hela processen, allt från generering av kryptonycklar till slutanvändarnas hantering av systemet, håller en nivå som är anpassad för den information som systemet avser att skydda. Genom nationellt godkännande säkerställs skyddsnivån och kvaliteten på såväl teknik som regelverk, rutiner och behörighetsutbildning.

Idag har över 160 organisationer godkända signalskyddssystem. För civilt bruk finns 17 godkända signalskyddssystem inom produktområdena datakommunikation, meddelandekrypton och talkrypton. Dessa system är gemensamma för Försvarsmakten och civila sektorn. Det finns endast ett godkänt KSU-krypto (filkryptot KGAI). Detta är dock det nationellt mest utbredda kryptosystemet.

Traditionellt har signalskydd framförallt varit en militär angelägenhet, där det gällt att skydda sin egen kommunikation mot fientlig signalspaning. Historiskt har det militära behovet av signalskydd ensamt motiverat omfattande statliga satsningar på utveckling av signalskyddssystem.

Det civila behovet har uppstått genom samordningsbehov mellan militärt och civilt försvar inom ramen för totalförsvaret. År 1959 skapades därför en totalförsvarsgemensam signalskyddsstruktur när Statens signalskyddsnämnd (SN) bildades. Efter det kalla kriget har inriktningen av den civila signalskyddsverksamheten även kopplats till krisberedskap. I 1992 års försvarsbeslut fick den civila delen av totalförsvaret även till uppgift att värna civilbefolkningen under kriser. I 1996 års

[9] Termen ”Säkra kryptografiska funktioner” definieras i krisberedskapsförordningen SFS (2006:942) 4§ som ”kryptografiska funktioner godkända av Försvarsmakten”.

försvarsbeslut kom det vidgade säkerhetsbegreppet. Definitionen av totalförsvaret ändrades inte utan insikten om samhällets säkerhet och den vidgade hotbilden ledde fram till Sårbarhets- och säkerhetsutredningen 2001. Ansvaret för den civila inriktningen och materielförsörjningen övertogs av Krisberedskapsmyndigheten (KBM) från Överstyrelsen för civil beredskap när KBM inrättades 2002. När KBM lades ned 2008 övergick inriktningsansvaret för den civila signalskyddsverksamheten till den nybildade myndigheten MSB och materielförsörjningen till FRA. Den civila signalskyddsverksamheten regleras i krisberedskapsförordningen.

År 2007 fick Försvarsmakten i myndighetens instruktion uppdraget att, utöver signalskyddstjänsten, även leda och samordna arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information. Detta uppdrag föranledde dock ingen ökad tilldelning av medel.

Under senare år har behovet av kryptografiska funktioner för internationell verksamhet ökat markant, särskilt inom EU och NATO. Under 2011 blev Sverige en godkänd andraparts-evaluerare av krypto inom EU. Denna funktion, AQUA (Appropriately Qualified Authority), innehas av Försvarsmakten. Det finns idag fem svenska kryptosystem som godkänts av Europeiska unionens råd.

Myndigheternas ansvar

Försvarsmakten (FM)

Försvarsmakten ska leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information (KSU)[10]. Försvarsmakten ska också biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet[11]. Detta är en olycklig skrivning eftersom säkra kryptografiska funktioner här definieras som en delmängd av signalskyddet medan säkra kryptografiska funktioner i krisberedskapsförordningen definieras som signalskydd och KSU. Försvarsmakten arbetar därför för att få till ett förtydligande i instruktionen till FM.

Försvarsmakten får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret, förutom i fråga om verkställigheten av 33 § förordningen (2006:942) om krisberedskap och höjd beredskap[12].

Försvarsmakten beställer all utveckling och vidmakthållande av signalskyddsmateriel samt leder och samordnar kravställning, utveckling, granskning, godkännande, drift och avveckling av signalskyddssystem. I detta arbete har myndigheten ett tydligt ansvar att ta fram en relevant hotbild och korrekta säkerhetskrav som ska möta denna hotbild. Försvarsmakten anskaffar också löpande färdigutvecklad signalskyddsmateriel för eget och till viss del för andra myndigheters[13] behov[14]. Alla Försvarsmaktens beställningar inom detta område går till FMV.

Försvarsmakten producerar och distribuerar totalförsvarets behov av kryptonycklar, aktiva kort och certifikat. FRA stödjer genom att ombesörja beställningar och distribution till de civila myndigheter som själva inte har tillgång till Försvarsmaktens system.

[10] Förordning (2007:1266) med instruktion till Försvarsmakten, 3 b § punkt 3.
[11] Förordning (2007:1266) med instruktion till Försvarsmakten, 3 b § punkt 4.
[12] Förordning (2007:1266) med instruktion till Försvarsmakten, 33 §.
[13] Försvarets materielverk, Försvarshögskolan, Totalförsvarets forskningsinstitut, Fortifikationsverket och Totalförsvarets rekryteringsmyndighet.
[14] Förordning (2006:942) om krisberedskap och höjd beredskap, 32 §.

I rollen att leda och samordna ingår förutom att utarbeta föreskrifter[15] att fastställa krav på utbildningsnivåer och annat erforderligt regelverk. Försvarsmakten utbildar personal vid Regeringskansliet, statliga myndigheter och Försvarsmaktens organisationsenheter i syfte att uppnå de behörigheter som behövs för att få verka inom signalskyddstjänsten. Man följer också upp signalskyddstjänstens verksamhet genom återkommande kontroller.

Försvarsmakten[16] stödjer UD/NSA (National Security Authority), NCSA/CAA (National Communications Security Authority/Crypto Approval Authority), NDA (National Distribution Authority) samt TA (Tempest Authority) och tecknar med bemyndigande från Regeringskansliet COMSEC-avtal (Communications Security) med andra länder. Av Europeiska Unionens råds beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter framgår bland annat att kryptoprodukter för skydd av sådana uppgifter ska vara godkända av en medlemsstats nationella kryptogodkännande organisation (CAA) samt ha genomgått en andra granskning, en s.k. andrapartsevaluering, av en AQUA (Appropriately Qualified Authority) innan produkten godkänns av rådet. En AQUA utnämns av rådet på grundval av kriterier som rådet fastställt och innebär att organisationen har teknisk kompetens och goda processer inom kryptoområdet som gör den lämplig att genomföra kryptoevalueringar. I Sverige är Försvarsmakten CAA och även utnämnd till AQUA såsom ett av sex länder. Nationellt får dock medlemsstaterna godkänna signalskyddssystem för skydd av EU-sekretess upp till och med nivån EU Confidential.

Försvarsmakten har även godkänts av NATO för att godkänna system för skydd av NATO-sekretess upp till och med nivån NATO Confidential.

Försvarsmakten har också uppgiften att på uppdrag av Försvarsexportmyndigheten stödja den svenska kryptoindustrin med export av svenska kryptosystem.

Myndigheten för samhällsskydd och beredskap (MSB)

MSB har uppgiften att inrikta civila myndigheters signalskyddsverksamhet och arbete med de säkra kryptografiska funktioner som är nationellt godkända. Genom att nyttja nationellt godkända kryptografiska funktioner ges Regeringskansliet, myndigheter och andra samhällsviktiga verksamheter förmåga till säkert tvärsektoriellt informationsutbyte.

MSB är bemyndigat av regeringen[17] att besluta om vilka myndigheter som ska kunna kommunicera med kryptografiska funktioner, utöver de som regeringen pekat ut i krisberedskapsförordningen. Dessutom kan MSB besluta om och ingå avtal med de kommuner, organisationer och företag som ska tilldelas säkra kryptografiska funktioner. I krisberedskapsförordningen har regeringen pekat ut följande myndigheter: Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut, Fortifikationsverket, Totalförsvarets pliktverk, Myndigheten för samhällsskydd och beredskap samt Regeringskansliet.

[15] FFS 2005:2 Förvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret.
[16] Egentligen Avdelningen för Krypto och IT-säkerhet vid MUST.
[17] I enlighet med 31§ förordningen 2006:942 om krisberedskap och höjd beredskap med ändringen SFS 2008:1003.

MSB:s beslut effektueras av Försvarets radioanstalt. MSB föreskriver[18] om den signalskyddsberedskap som gäller för de myndigheter och organisationer som tilldelats signalskydd.

MSB har det övergripande ansvaret att leda och samordna arbetet med säkra kryptografiska funktioner för civila aktörer. I detta ingår att vara kravställare gentemot Förvarsmakten vid utveckling av nya system samt anskaffa och besluta om tilldelning.

Försvarets radioanstalt (FRA)

FRA stödjer statliga myndigheter, statligt ägda bolag samt samhällsviktiga företag som hanterar information vilken bedöms vara känslig ur krishanteringssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. FRA ger tekniskt stöd avseende signalskyddsverksamheten och säkra kryptografiska funktioner.

FRA har uppgiften[19] att tilldela Försvarets radioanstalt, Kustbevakningen, MSB och Regeringskansliet säkra kryptografiska funktioner. FRA tilldelar också säkra kryptografiska funktioner till de myndigheter som MSB beslutar om ska ha det samt företag, kommuner och organisationer som efter överenskommelse ska få tillgång till eller ingå avtal om tilldelning. Tilldelning innefattar materiel och användarstöd, nycklar och certifikat samt samordning och utbildning.

Användare som tilldelats kryptosystem ska ges särskild utbildning i handhavande av materiel och kryptonycklar. FRA ansvarar för att civila användare kan ges den signalskyddsutbildning som föreläggs. FRA har en av tre nationellt godkända kryptoverkstäder samt civilt användarstöd för signalskydd och KSU.

Civila myndigheter och samhällsviktiga verksamheter som inte själva kan beställa kryptonycklar, aktiva kort och servercertifikat av Försvarsmakten beställer dessa via FRA. FRA distribuerar aktiva kort och servercertifikat till civila myndigheter och företag.

FRA upphandlar utbildning för civila myndigheter av Totalförsvarets signalskyddsskola (TSS). FRA har behöriga lärare som genomför utbildning vid akuta eller särskilda behov. FRA deltar även vid inriktning av TSS.

FRA:s kryptologer stödjer Försvarsmakten med matematiska bedömningar av nya kryptoalgoritmer genom den så kallade kryptopoolen som har funnits sedan 80-talet.

Försvarets materielverk (FMV)

FMV:s uppgift är att utveckla och anskaffa signalskyddsmateriel för textskydd, trafikskydd, intrångsskydd, behörighetskontroll m.m. i enlighet med uppdrag från Försvarsmakten. Signalskyddsmaterielen nyttjas inom hela totalförsvaret.

Huvuduppdragsgivare för utveckling samt anskaffning inom området är Försvarsmakten samt MSB/FRA. Dessutom genomförs anskaffning av aktuellt materiel på uppdrag av FMV, FRA, FOI, PTS, UD m.fl. FMV har även uppdraget att samordna signalskyddsverksamheten inom försvarsindustrin.

[18] MSBFS 2009:11 Myndigheten för samhällsskydd och beredskaps föreskrifter om civila myndigheters kryptoberedskap.
[19] I enlighet med 32§ förordningen 2006:942 om krisberedskap och höjd beredskap med ändringen 2008:1003.

Sveriges Certifieringsorgan för IT-säkerhet vid FMV (CSEC)

Sveriges Certifieringsorgan för IT-säkerhet (CSEC) är en självständig enhet vid Försvarets materielverk som verkar som nationellt certifieringsorgan för granskning av it-säkerhet i produkter och system enligt den internationella standarden Common Criteria (ISO/IEC 15408). Syftet är att säkerställa att säkerhetsfunktioner i certifierade it-produkter verkligen ger det skydd som utlovats.

CSEC utfärdar regler för hur kommersiella evalueringsföretag under myndighetens tillsyn granskar säkerhet i it-produkter. Reglerna omfattar bl.a. metoder för sårbarhetsanalyser, penetrationstester, kryptoverifiering, kontroll av produktleverantörens metodik, analys av design- och användardokumentation, funktionstester samt användning av automatiska analysverktyg. Exempel på pågående certifieringsuppdrag: säker kortläsare, dataslussar, brandväggar, säkra skrivare och VPN-system.

FMV/CSEC fick 2009 Försvarsmaktens uppdrag att utveckla kompletterande regler för hur krypto kan granskas inom ramen för CSEC:s certifieringsordning. Ett förslag levererades till Försvarsmakten 2011.

Inom ramen för den nationella handlingsplanen för informationssäkerhet har FMV/CSEC i samverkan med Försvarsmakten och MSB vidareutvecklat förslaget. Det vidareutvecklade kryptogranskningsregelverket kallas Cryptographic Validation Program (CVP) och kan utgöra grunden för hur kommersiella produkter genom certifiering vid CSEC enligt dessa kryptoregler kan ligga till grund för ett KSU-godkännande från Försvarsmakten.

Inom ramen för den nationella handlingsplanen för informationssäkerhet har även FMV/CSEC i samverkan med Försvarsmakten och FRA påbörjat en studie för att analysera förutsättningarna för ett nationellt evalueringslaboratorium med nödvändig kompetens och utrustning för att analysera fysiska attacker mot information i datorutrustning.

Kryptoindustrin

Förmågan att ta fram kryptosystem för att skydda hemlig information som rör rikets säkerhet finns i dag i Sverige inte minst hos de svenska kryptoleverantörerna. Den samlade kryptokunskapen ger Sverige ett informationsövertag. För att nå höga assuransnivåer för de nationella system som skyddar rikets säkerhet eller utrikessekretess måste kunskapen om systemlösningarna omges av sträng sekretess, något som endast kan upprätthållas med nationellt framtagna lösningar. En egen svensk kryptoindustri är fundamental för att kunna ha möjligheten att utveckla signalskyddssystem. Utan en livskraftig svensk kryptoindustri riskerar nationella säkerhetsintressen att i allt högre grad bli beroende av utländska leverantörer. Detta skulle utgöra ett allvarligt hot mot den svenska säkerheten eftersom Sverige inte kan få samma tilltro till en produkt från en utländsk industri som en från en svensk leverantör.

Svenska kryptoprodukter håller vid internationell jämförelse en mycket hög nivå som det tar decennier att utveckla och svenska kryptoprodukter har en växande marknad framför sig, främst inom Europa. Även det faktum att Sverige är en godkänd andraparts-evaluerare av krypto inom EU (AQUA) kräver att vi har en inhemsk kryptoindustri. Det är därför av stor vikt att värna om denna förmåga.

En svensk kryptoindustri är således av nationellt intresse. De svenska kryptoföretagen, nuvarande som framtida, som vill leverera kryptolösningar för nationella behov måste ges förutsättningar att långsiktigt bedriva sin verksamhet så att detta gagnar såväl dem som nationen. Att upprätthålla denna typ av kompetens är dyrt och för att industrin ska känna sig tillräckligt trygg för att fortsätta satsa på att utveckla och vidmakthålla signalskyddssystem på en hög nivå så måste det finnas en uttalad vilja hos nationen Sverige att efterfråga denna kompetens. Detta skulle exempelvis kunna åstadkommas med att göra signalskydd till ett nationellt säkerhetsintresse.

Signalskyddsprocessen

Försvarsmakten svarar för utvecklingen av nationellt godkända kryptosystem genom att fastställa de målsättningar och kravspecifikationer som gäller för de system som ska utvecklas. All utveckling och vidmakthållande av signalskydd för hela totalförsvaret finansieras av Försvarsmaktens materielanslag. De system som utvecklas säkerhetsgranskas av Försvarsmakten som sedan godkänner systemen för skydd av information upp till en viss klassningsnivå, nationellt och internationellt. Systemen följs sedan upp under hela sin livstid för att dessa ska behålla sin skyddsnivå.

Försvarsmakten leder utvecklingsarbetet och MSB deltar i kravställningsarbetet som representant för det civila samhället. Behov av utveckling av nya system ställs av Försvarsmakten, MSB eller FRA till Försvarsmakten. Försvarsmakten beställer nya system av FMV som i sin tur upphandlar av industrin. Under utvecklingsarbetet deltar Försvarsmakten aktivt med löpande avdömningar för att i slutändan kunna granska och godkänna leveransen.

Försvarsmakten följer teknikutvecklingen av framtida metoder och system för kommunikation samt kommande kryptolösningar. MSB deltar i Försvarsmaktens process för utveckling av nya system genom att föra in kraven från civila myndigheter i Försvarsmaktens arbete med målsättningar och kravspecifikationer. MSB har en referensgrupp med representanter från civila myndigheter för att få en tydligare bild av behoven på kort och lång (10 års) sikt.

När systemen är utvecklade, godkända och tillgängliga att beställa uppdaterar MSB sin materielplan för anskaffning av säkra kryptografiska funktioner och detta utgör sedan ett inriktningsbeslut till FRA över vilka system som ska köpas in. FRA lämnar uppdrag till FMV att anskaffa det fastställda behovet av säkra kryptografiska funktioner. Då leverans sker fördelar FRA systemen till de aktörer som MSB har beslutat.

MSB beslutar vilka aktörer inom krisberedskapen som ska ha signalskydd och KSU för tvärsektoriell samverkan. MSB ska också ingå avtal med kommuner och organisationer som har behov av säkra kryptografiska funktioner, vilket innebär att dessa aktörer förbinder sig att följa gällande regelverk för signalskydd.

Krisberedskapsanslaget (2:4-anslaget) täcker kostnader av engångskaraktär såsom genomförande av olika projekt inom området samt anskaffning av kryptomateriel som är beslutade av MSB. Varje myndighet är ansvarig för att finansiera skydd av information och intern kommunikation. Kryptosystem för samverkan mellan myndigheter kan finansieras med anslag 2:4 Krisberedskap. FRA förser myndigheter med nationellt godkända krypton i båda fallen.

KSU-processen

Processen och finansieringen av KSU är idag desamma som för signalskydd. Anledningen till detta är snarare avsaknad av en anpassad process för KSU än en uttalad ambition att följa signalskydds-processen. Arbete med den nya processen för KSU pågår i ett samarbete mellan Försvarsmakten, MSB och FRA.

Signalskyddsmateriel för den civila sidan finansieras idag till cirka 90 procent genom 2:4-anslag, vilket innebär att de är avsedda för krisberedskap och samverkan mellan myndigheter. För KSU är behovet det omvända eftersom det huvudsakliga behovet inte täcks av principerna för 2:4-anslaget. Detta innebär att organisationerna själva måste finansiera KSU-anskaffning.

För närvarande finns ett filkrypto godkänt som KSU. Detta är emellertid ett av de mest utbredda godkända kryptosystemen i det civila samhället. Ett 80-tal myndigheter, organisationer och företag har idag KSU.

Enligt den nationella handlingsplanen[20] för informationssäkerhet bör det utvecklas ytterligare kryptosystem för nivån KSU avsedda för till exempel mobil tal- och datakommunikation, förbindelsekryptering över Virtuella Privata Nät (VPN) samt för kryptering av USB-minnen. Målet är att KSU ska byggas ut och få sådan spridning att skyddsvärd information som hanteras i myndigheter, landsting, kommuner och andra organisationer skyddas med krypto för skyddsvärda uppgifter.

Alternativet till KSU är allmänt tillgängliga kommersiella produkter. Fördelarna med dessa är att det finns ett stort utbud och anskaffningen är enkel. Nackdelarna med kommersiellt tillgängliga produkter i jämförelse med KSU är att de inte är nationellt granskade eller godkända och därför tyvärr alltför ofta inte levererar den säkerhetsfunktionalitet de utlovar. Eftersom anskaffning av dessa produkter inte heller kräver nationell samordning mellan organisationer skapas heller inga gemensamma system för säker kommunikation mellan organisationer.

[20] Samhällets ***informationssäkerhet. Nationell handlingsplan*** 2012. Myndigheten för samhällsskydd och beredskap (MSB).

Bilaga 2: Författningssamling

Nedan sammanfattas de uppdrag som FMV, FRA, FM och MSB har gällande signalskydd och kryptografiska funktioner. Informationen kommer från instruktioner, regleringsbrev och andra författningar.

Försvarets materielverk (FMV)

Förordning (2007:854) med instruktion för Försvarets materielverk

5 § Vid Försvarets materielverk finns ett certifieringsorgan som ska upprätta och driva en certifieringsordning för säkerhet i IT-produkter och system. Försvarets materielverk ska verka för att uppnå och vidmakthålla internationellt erkännande för utfärdade certifikat.

Försvarets radioanstalt (FRA)

Förordning (2007:937) med instruktion för Försvarets radioanstalt

2 § Försvarets radioanstalt ska särskilt
3. utföra matematiska bedömningar av kryptosystem för totalförsvaret.

4 § Försvarets radioanstalt ska ha hög teknisk kompetens inom informationssäkerhetsområdet. Försvarets radioanstalt får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Försvarets radioanstalt ska särskilt kunna

1. stödja insatser vid nationella kriser med IT-inslag,
2. medverka till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system,
3. genomföra IT-säkerhetsanalyser, och
4. ge annat tekniskt stöd.

Försvarets radioanstalt ska samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

Förordning (2006:942) om krisberedskap och höjd beredskap

32 § Försvarsmakten svarar för att Försvarsmakten, Försvarets materielverk, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet och Fortifikationsverket tilldelas säkra kryptografiska funktioner. Försvarets radioanstalt svarar för att övriga som enligt 31 § ska ha säkra kryptografiska funktioner tilldelas sådana.

Regleringsbrev för budgetåret 2014 avseende Försvarets radioanstalt

4 § Försvarets radioanstalt ska upprätthålla kompetensen för de nationella behoven avseende kryptologi.

Försvarsmakten (FM)

Förordning (2007:1266) med instruktion för Försvarsmakten

3 b § Försvarsmakten ska särskilt

1. leda och bedriva militär säkerhetstjänst
2. leda och samordna signalskyddstjänsten, inklusive arbetet med säkra kryptografiska funktioner som är avsedda att skydda skyddsvärd information,
3. biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet.

33 § Försvarsmakten får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret, förutom i fråga om verkställigheten av 33 § förordningen (2006:942) om krisberedskap och höjd beredskap.

Säkerhetsskyddslag (1996:627)

33 § Regeringen eller den myndighet som regeringen utser meddelar de närmare föreskrifter som behövs för lagens tillämpning (1996:627).

Säkerhetsskyddsförordning (1996:633)

13 § Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten.

44 § Rikspolisstyrelsen och Försvarsmakten får meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) för sina respektive tillsynsområden enligt 39 §.

Första stycket gäller inte omfattningen av inventeringen av hemliga handlingar enligt 9 § andra stycket.

45 § Myndigheterna skall meddela ytterligare föreskrifter om verkställigheten av säkerhetsskyddslagen (1996:627) i fråga om säkerhetsskyddet inom sina verksamhetsområden, om det inte är uppenbart obehövligt. Om det behövs skall myndigheterna innan dess samråda med den myndighet som enligt 43 och 44 §§ meddelar föreskrifter för myndighetens område.

Myndigheternas föreskrifter får avvika från föreskrifterna enligt 43 och 44 §§ endast om detta har medgivits av den myndighet som har meddelat dessa föreskrifter.

Förordning (2006:942) om krisberedskap och höjd beredskap

32 § Försvarsmakten svarar för att Försvarsmakten, Försvarets materielverk, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets rekryteringsmyndighet och Fortifikationsverket tilldelas säkra kryptografiska funktioner. Försvarets radioanstalt svarar för att övriga som enligt 31 § ska ha säkra kryptografiska funktioner tilldelas sådana.

Myndigheten för samhällsskydd och beredskap (MSB)

Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

1 § Myndigheten för samhällsskydd och beredskap har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller en kris.

7 § Myndigheten ska ha förmågan att bistå med stödresurser i samband med allvarliga olyckor och kriser samt stödja samordningen av berörda myndigheters åtgärder vid en kris. Myndigheten ska se till att berörda aktörer vid en kris får tillfälle att

1. samordna krishanteringsåtgärderna,
2. samordna information till allmänhet och media,
3. effektivt använda samhällets samlade resurser och internationella förstärkningsresurser, och
4. samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder.

Myndigheten ska ha förmågan att bistå Regeringskansliet med underlag och information i samband med allvarliga olyckor och kriser.

11 a § Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt 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. Myndigheten ska även rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället.

Myndigheten ska vidare svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter. Myndigheten ska i detta arbete:

1. agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade,
2. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och
3. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa (förordning 2010:1901).

Förordning (2006:942) om krisberedskap och höjd beredskap

30a § Varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt. Därvid ska behovet av säkra ledningssystem särskilt beaktas.

31 § Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut, Fortifikationsverket, Totalförsvarets rekryteringsmyndighet, Myndigheten för samhällsskydd och beredskap och Regeringskansliet ska ha säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap beslutar vilka övriga myndigheter som ska ha säkra kryptografiska funktioner.

Myndigheten för samhällsskydd och beredskap beslutar även vilka företag som efter överenskommelse ska få tillgång till säkra kryptografiska funktioner. Myndigheten för samhällsskydd och beredskap får därutöver ingå avtal om tilldelning med kommuner och organisationer som har behov av säkra kryptografiska funktioner.

34 § Myndigheten för samhällsskydd och beredskap får

1. meddela de ytterligare föreskrifter som behövs för verkställigheten av 9 § om risk- och sårbarhetsanalyser,

2. meddela föreskrifter om sådana säkerhetskrav som avses i 30 a § med beaktande av nationell och internationell standard, samt

3. meddela de ytterligare föreskrifter som behövs för verkställigheten av 16-20 samt 33 §§, utom i fråga om Försvarets materielverk, Försvarets radioanstalt, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut och Fortifikationsverket.

I 3 § finns undantag från 34 §.

3 § Bestämmelserna i 5-22 och 33-34 §§ gäller för statliga myndigheter under regeringen, med undantag av Regeringskansliet, kommittéväsendet och Försvarsmakten. För utlandsmyndigheterna tillämpas bestämmelserna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet.

Strategi för statens informations- och cybersäkerhet

Syftet med denna strategi är att ange grundläggande målsättningar, färdriktningar och arbetssätt för informationssäkerhet i svenska staten. En mängd olika aktörer i staten behöver en gemensam förståelse för informationssäkerhet, vad den syftar till och hur framtida säkerhetsinsatser ska inriktas och utformas. Främst berörda är regeringen och myndighetscheferna, som har att fatta besluten som genomför strategin i verksamheten, men också de som arbetar med informationssäkerhet på olika nivåer, beslutsfattare i offentlig förvaltning och i de delar av näringslivet som säljer varor och tjänster till den, de som arbetar med it eller generell säkerhet, men också de enskilda medborgarna, som är beroende av att staten hanterar information om och för dem på ett säkert sätt.

Strategin anger strategiska mål och strategiska områden för informations- och cybersäkerhetsarbete. Inom de strategiska områdena anges de initiativ och åtgärder som föreslagits i betänkandet.

Strategiska mål

Informations- och cybersäkerhet är en stödjande verksamhet för att öka kvaliteten hos statens funktioner samtidigt som det är en nödvändig verksamhet för att garantera att lagstiftning från regering och riksdag (såsom all integritetsskyddande lagstiftning) verkligen genomförs. Ytterst handlar det om att slå vakt grundläggande värden och mål i vårt samhälle, såsom demokrati, personlig integritet, ekonomisk tillväxt samt politisk stabilitet.

Målet är att uppnå en god informations- och cybersäkerhet i statsförvaltningen som främjar:

- medborgares fri- och rättigheter samt personliga integritet
- statsförvaltningens funktionalitet, effektivitet och kvalitet
- brottsbekämpningen
- statens förmåga att förebygga och hantera allvarliga störningar och kriser
- näringslivets tillväxt, genom att staten blir en både skicklig och tydlig kravställare.

Med strategin tas en rad initiativ för att stärka cyber- och informationssäkerheten i Sverige. Initiativen faller inom sex områden.

FÖRSLAG TILL STRATEGI OCH ÅTGÄRDER

1. Styrning och tillsyn av informationssäkerheten i staten stärks.

Arbetet med informationssäkerhet professionaliseras och tillsynen över de statliga myndigheterna stärks.

En nationell styrmodell för informationssäkerhet i samhället etableras.

Regeringen inrättar ett statligt myndighetsråd för informationssäkerhet bestående av företrädare för de relevanta myndigheterna på området.

En ny förordning för statliga myndigheters informationssäkerhet införs.

Tillsynen över den statliga sektorns informationssäkerhet samordnas och förstärks. Myndigheten för samhällsskydd och beredskap får i uppgift att bedriva tillsyn över statliga myndigheters arbete med informationssäkerhet. Den sektorsvisa tillsynen i staten ses över.

Revision av informationssäkerhet utvecklas. Myndighetsledningens ansvar för att upprätthålla säkerhet i myndighetens informationshantering förtydligas genom rapporteringskrav i förordningen om årsredovisning och budgetunderlag.

2. Staten blir en tydlig kravställare.

Statliga myndigheter ska arbeta mer systematiskt med att ställa säkerhetsmässiga krav i anslutning till upphandling och avtalsingående på it-området. Dessutom ska det ske löpande uppföljning på den säkerhetsmässiga leverantörstyrningen i staten. Dialogen mellan privata och offentliga aktörer samt relevanta utbildnings- och forskningsinstitutioner på området fördjupas.

Statlig upphandling ska innehålla hänvisning till för staten gällande standarder och krav på certifiering i de situationer där säkerhetsnivåer har fastställts för respektive verksamhet.

Myndigheten för samhällsskydd och beredskap ges i uppdrag att ta fram skyddsprofiler som anger minimikrav på säkerhet i vanligt förekommande it-produkter som används av statliga myndigheter.

Det införs ett krav på att rapportera vilken leverantör som en statlig myndighet valt då ramavtal rörande it-lösningar används.

Avseende tjänster och produkter att användas för kommunikation inom staten överväger upphandlande myndighet möjligheten att tillämpa lagen om upphandling på försvars- och säkerhetsområdet, om upphandling enligt lagen om offentlig upphandling inte medger nödvändigt kravställande.

Regeringen fördjupar dialogen mellan privata och offentliga aktörer samt utbildnings- och forskningsinstitutioner på informationssäkerhetsområdet.

3. Statliga myndigheter kommunicerar säkert.

Statliga myndigheter ska kommunicera säkert. I ett första steg ansluts myndigheterna som omfattas av krisberedskapsförordningen till SGSI. På sikt utvecklas detta till ett säkert kommunikationssystem för hela staten.

Samtliga myndigheter som anges i bilagan till förordningen om krisberedskap och höjd beredskap ansluts till kommunikationssystemet Swedish Government Secure Intranet (SGSI).

Under utbyggnaden av SGSI vidtas lämpliga åtgärder för att utveckla sensorteknik.

Statliga myndigheter ska använda samma synkroniserade tidsskala för de tidsangivelser de använder i sina it-system.

Regeringen ger Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk och Försvarsmakten i uppdrag att utveckla processen för säkra kryptografiska funktioner.

4. Samtliga statliga myndigheter rapporterar it-incidenter för att skapa underlag för bättre kunskap och lägesbeskrivningar.

Det inrättas system för obligatorisk it-incidentrapportering för samtliga statliga myndigheter. Detta anpassas till innehållet i EU-direktivet om nät- och informationssäkerhet (NIS-direktivet).

I syfte att förbereda införandet av ett system för obligatorisk it-incidentrapportering får Myndigheten för samhällsskydd och beredskap i uppdrag att utfärda verkställighetsföreskrifter om dess närmare utformning.

De statliga myndigheterna förses med information om bl.a. trender och utveckling avseende it-incidenter.

5. Förebyggande och bekämpande av it-relaterad brottslighet stärks.

Sverige skapar nödvändiga förutsättningar för de brottsbekämpande myndigheterna att garantera samma skydd mot cyberbrottslighet som mot brottslighet i allmänhet. Som ett led i detta ratificeras Europarådets konvention om it-relaterad brottslighet och en översyn görs avseende tvångsmedlens tillämpning i den digitala miljön.

Arbetet med ratificering av Europarådets konvention om it-relaterad brottslighet slutförs.

Det utreds om en tydligare reglering kan införas i offentlighets- och sekretesslagen rörande sekretess för uppgifter som utbyts vid samverkan mellan brottsbekämpande myndigheter och andra myndigheter inom informations- och cybersäkerhetsområdet.

En översyn av bestämmelserna om tvångsmedel i 27 och 28 kap. rättegångsbalken och övriga lagrum görs för att säkerställa att brottsbekämpande myndigheter kan bedriva sin förebyggande och utredande verksamhet i den digitala miljön.

6. Sverige ska vara en stark internationell partner.

Regeringen stärker och samordnar insatserna för att främja Sveriges ställning i internationellt samarbete om informations- och cybersäkerhet.

Regeringen säkerställer att Sverige agerar kraftfullt och konsistent i samtliga internationella och regionala fora av relevans.

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.

Statens offentliga utredningar 2015

Systematisk förteckning