Lagrådsremiss

En anpassad försvarsunderrättelseverksamhet

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 18 januari 2007

Mikael Odenberg

Helena Lindberg
(Försvarsdepartementet)

Lagrådsremissens huvudsakliga innehåll

I lagrådsremissen föreslås ändringar i lagen om försvarsunderrättelseverksamhet. Ändringarna innebär att mandatet för försvarsunderrättelseverksamheten anpassas från ”yttre militära hot” till ”yttre hot” och att det uttryckligen anges att verksamheten endast får avse utländska förhållanden. Vidare förtydligas gränsdragningen mellan polisiär verksamhet och försvarsunderrättelseverksamhet. Det föreslås tydligare regler avseende inriktning, rapportering av underrättelser och inhämtning med särskilda metoder. Det föreslås också att samhällets funktioner för inriktning och kontroll av försvarsunderrättelseverksamheten skall förstärkas.

I lagrådsremissen föreslås också en ny lag om signalspaning i försvarsunderrättelseverksamhet. Lagen omfattar signalspaning för försvarsunderrättelseändamål, oavsett om signalerna befinner sig i etern eller i tråd. Förslaget innehåller flera regler till skydd för den enskildes integritet. Signalspaning sker efter inriktning från regeringen eller berörda myndigheter. Ett särskilt tillståndsförfarande föreslås för myndigheternas inriktningar. Vidare föreslås regler om när uppgifter skall förstöras och hur rapportering skall ske. De sökbegrepp som skall användas, liksom att förstöring och rapportering sker i enlighet med lagens bestämmelser, skall kontrolleras i särskild ordning.

För att möjliggöra inhämtning av signaler i elektronisk form föreslås vissa nya regler i lagen (2003:389) om elektronisk kommunikation.

I lagrådsremissen föreslås också en ny bestämmelse i sekretesslagen (1980:100). Den nya bestämmelsen innebär att sekretess skall gälla hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos Försvarets radioanstalt i försvarsunderrättelse- och säkerhetsverksamheten för uppgift om enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan

att den enskilde eller någon närstående till den enskilde lider skada eller men.

Lagstiftningen föreslås träda i kraft den 1 juli 2007.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om ändring i lagen (2000:130) om försvarsunderrättelseverksamhet,
2. lag om signalspaning i försvarsunderrättelseverksamhet,
3. lag om ändring i lagen (2003:389) om elektronisk kommunikation, och
4. lag om ändring i sekretesslagen (1980:100).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om ändring i lagen (2000:130) om försvarsunderrättelseverksamhet

Härigenom föreskrivs att 1–5 §§ lagen (2000:130) om försvarsunderrättelseverksamhet skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Försvarsunderrättelseverksamhet skall bedrivas *för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik.* I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete *och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred.*	Försvarsunderrättelseverksamhet skall bedrivas *till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet.* I verksamheten ingår *också* att medverka i svenskt deltagande i internationellt säkerhetssamarbete. *Försvarsunderrättelseverksamhet får endast avse utländska förhållanden.*
Regeringen skall bestämma försvarsunderrättelseverksamhetens inriktning.	Regeringen skall bestämma försvarsunderrättelseverksamhetens inriktning. *Inom ramen för denna inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten.*
Försvarsunderrättelseverksamhet skall bedrivas av *Försvarsmakten och de andra* myndigheter som regeringen bestämmer.	Försvarsunderrättelseverksamhet skall bedrivas av *den eller de* myndigheter som regeringen bestämmer.
	2 §
Uppgifterna som anges i 1 § skall fullgöras genom inhämtning, bearbetning och analys av information. *Analyser av hotbilder och bedömningar i underrättelsefrågor* skall rapporteras till *Regeringskansliet och andra* berörda myndigheter.	*Verksamheten enligt* 1 § skall fullgöras genom inhämtning, bearbetning och analys av information. *Underrättelser* skall rapporteras till berörda myndigheter. *I verksamheten får användas teknisk och personbaserad inhämtning med särskilda metoder. Vissa bestämmelser om teknisk*

	inhämtning finns i lagen (2007:000) om signalspaning i försvarsunderrättelseverksamhet.
	3 §
De myndigheter som skall bedriva försvarsunderrättelseverksamhet får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer.	*Den eller* de myndigheter som skall bedriva försvarsunderrättelseverksamhet får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer.
	4 §
Försvarsunderrättelseverksamheten får inte *avse* uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande *arbete.*	*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.* *Om det inte finns hinder enligt andra bestämmelser, får dock de myndigheter som bedriver försvarsunderrättelseverksamhet lämna stöd till andra myndigheters brottsbekämpande och brottsförebyggande verksamhet.*
	5 §
En särskild nämnd under regeringen skall ha insyn i försvarsunderrättelseverksamheten enligt vad regeringen närmare föreskriver.	*Den myndighet som regeringen bestämmer skall kontrollera försvarsunderrättelseverksamheten.*

Denna lag träder i kraft den 1 juli 2007.

2.2 Förslag till lag om signalspaning i försvarsunderrättelseverksamhet

Härigenom föreskrivs följande.

1 § I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer inhämta signaler i elektronisk form vid signalspaning.

Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att

1. följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt
2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

2 § Inhämtning som sker i tråd får endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör.

3 § Inhämtning av signaler i tråd skall ske automatiserat. Sådan inhämtning får endast avse signaler som identifierats genom sökbegrepp. Även vid annan automatiserad inhämtning skall sökbegrepp användas för identifiering av signaler.

Sökbegreppen skall utformas och användas så att de medför ett så begränsat intrång som möjligt i den personliga integriteten. Sökbegreppen får inte vara direkt hänförliga till en viss fysisk person om det inte är av synnerlig vikt för verksamheten.

4 § I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. En inriktning av signalspaningen får inte avse endast en viss fysisk person.

Regeringen bestämmer inriktningen av den verksamhet som bedrivs enligt 1 § andra stycket.

5 § För en myndighets närmare inriktning av signalspaning enligt 1 § första stycket krävs tillstånd, om inte inriktningen avser regeringens eget underrättelsebehov. Tillstånd lämnas av den myndighet som regeringen bestämmer. Ett tillstånd får ges för högst sex månader från dagen för beslutet och kan efter förnyad prövning förlängas med högst sex månader i taget.

Tillstånd får endast ges för inriktning som är förenlig med lagen (2000:130) om försvarsunderrättelseverksamhet. Tillstånd får endast lämnas om syftet med inriktningen väger klart tyngre än det integritetsintrång som inhämtning i enlighet med inriktningen kan innebära och detta syfte inte kan tillgodoses på ett mindre ingripande sätt. Tillstånd får inte lämnas om inriktningen endast avser en viss fysisk person.

I brådskande fall får inriktning ges utan att tillstånd har lämnats. Inriktningen skall då omedelbart anmälas till den myndighet som skall lämna tillstånd. Finner tillståndsmyndigheten att inriktningen inte borde

ha getts skall den myndighet som avses i 1 § underrättas. Verksamheten med anledning av inriktningen skall då omedelbart avbrytas.

6 § Upptagning eller uppteckning av uppgifter som inhämtats enligt denna lag skall omgående förstöras om innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för verksamhet som avses i 1 §,
2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 4 § tryckfrihetsförordningen eller 2 kap. 4 § yttrandefrihetsgrundlagen, eller
3. omfattar uppgifter i meddelanden som avses i 27 kap. 22 § rättegångsbalken.

7 § Underrättelser med uppgifter som inhämtats enligt denna lag skall rapporteras till berörda myndigheter i enlighet med vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet. Om uppgifterna berör en viss fysisk person får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § den lagen.

8 § Den myndighet som avses i 1 § får för den verksamhet som anges i 1 § andra stycket, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.

9 § Den myndighet som regeringen bestämmer skall kontrollera att denna lag följs. Kontrollen skall särskilt avse granskning av sökbegrepp som avses i 3 §, förstöring av uppgifter som avses i 6 § samt rapportering enligt 7 §.

Myndigheten får besluta att viss inhämtning skall upphöra eller att upptagning eller uppteckning av inhämtade uppgifter skall förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med denna lag eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten.

10 § I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om operatörers skyldighet att överföra signaler för att möjliggöra inhämtning enligt denna lag.

11 § Beslut enligt denna lag får inte överklagas.

Denna lag träder i kraft den 1 juli 2007.

2.3 Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2003:389) om elektronisk kommunikation

dels att 6 kap. 21 § skall ha följande lydelse,

dels att det skall införas en ny paragraf, 6 kap. 19 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 kap.
	19 a §
	För att inhämtning av signaler i elektronisk form enligt lagen (2007:000) om signalspaning i försvarsunderrättelseverksamhet skall kunna ske, är operatörer som äger tråd i vilka signaler förs över Sveriges gräns skyldiga att överföra dessa till samverkanspunkter. Varje sådan operatör skall anmäla en eller flera samverkanspunkter till den myndighet som regeringen bestämmer. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om samverkanspunkter.
	Samtliga operatörer som för signaler i tråd över Sveriges gräns skall till den myndighet som regeringen bestämmer lämna sådan information de innehar som gör det enklare att ta hand om signalerna.
	Samtliga operatörer skall utföra uppgiften enligt denna bestämmelse så att verksamheten inte röjs.
21 §	
Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till	
1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,	
2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken, och	
	3. angelägenhet som avser inhämtning av signaler i elektronisk

form enligt lagen (2007:000) om signalspaning i försvarsunderrättelseverksamhet.

---

1. Denna lag träder i kraft den 1 juli 2007.

2. Skyldigheten för operatörer som äger tråd att överföra signaler till samverkanspunkter enligt 6 kap. 19 a § skall tillämpas första gången den 1 juli 2008. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om att bestämmelserna om skyldigheten skall börja tillämpas senare.

2.4 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att det i sekretesslagen (1980:100)[1] skall införas en ny paragraf, 9 kap. 32 §, av följande lydelse.

9 kap.

32 § Sekretess gäller hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos Försvarets radioanstalt i underrättelse- och säkerhetsverksamheten för uppgift om enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till den enskilde lider skada eller men.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 juli 2007.

[1] Lagen omtryckt 1992:1474.

3 Ärendet och dess beredning

Den 20 december 2001 beslutade regeringen om direktiv (dir. 2001:120) till en särskild utredare med uppdrag att bl.a. kartlägga och analysera myndigheternas och de övriga offentliga organens samlade beredskap och förmåga att förhindra, bekämpa och i övrigt hantera omfattande terroristattentat och andra likartade extraordinära händelser i Sverige.

Utredningen, som antog namnet 11 september-utredningen, lämnade sitt betänkande (SOU 2003:32) till Justitiedepartementet i mars 2003. 11 september-utredningen lämnade bl.a. förslag som rör lagen (2000:130) om försvarsunderrättelseverksamhet. Justitiedepartementet har överlämnat den delen av ärendet till Försvarsdepartementet. En sammanfattning av betänkandet i nu aktuell del finns i *bilaga 1*. Betänkandets lagförslag i denna del finns i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning av remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga i Justitiedepartementet (dnr. Ju2003/2990/PO). Remissammanställningen i nu aktuell del finns tillgänglig i Försvarsdepartementet (dnr. Fö2003/2728/RS).

Härefter har promemorian (Ds 2005:30) En anpassad försvarsunderrättelseverksamhet utarbetats inom Regeringskansliet (Försvarsdepartementet) med förslag till ändringar i lagen (2000:130) om försvarsunderrättelseverksamhet och i lagen (2003:389) om elektronisk kommunikation samt förslag till en ny lag om signalspaning. En sammanfattning av promemorian finns i *bilaga 4*. Promemorians lagförslag finns i *bilaga 5.* Promemorian har remissbehandlats. I *bilaga 6* finns en förteckning över remissinstanserna. Remissvaren och en remissammanställning finns tillgängliga i Försvarsdepartementet (dnr. Fö2005/1912/RS).

Underrättelsedatautredningen lämnade sitt betänkande (SOU 2003:34) Försvarets underrättelseverksamhet och säkerhetstjänst Integritet – Effektivitet i mars 2003. Utredningen lämnade bl.a. förslag till ändring i sekretesslagen (1980:100). Förslaget i den delen behandlas i lagrådsremissen. En sammanfattning av betänkandet i nu aktuell del finns i *bilaga 7.* Betänkandets lagförslag avseende sekretesslagen finns i *bilaga 8.* Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 9*. Remissvaren och en remissammanställning finns tillgängliga i Försvarsdepartementet (dnr. Fö2003/991/RS).

4 Den svenska säkerhetspolitiska utvecklingen

4.1 Den svenska säkerhetspolitikens mål och inriktning

Sveriges säkerhetspolitik syftar till att bevara vårt lands fred och självständighet, bidra till stabilitet och säkerhet i vårt närområde, samt stärka internationell fred och säkerhet. Det säkerhetspolitiska målet är att i alla lägen och i former som vi själva väljer trygga handlingsfriheten att, som enskild nation och i samverkan, kunna utveckla vårt samhälle. Regeringens syn på det säkerhetspolitiska läget utvecklas i propositionen 2004/05:5 Vårt framtida försvar.

Sveriges militära alliansfrihet kombineras med ett brett och allsidigt deltagande i det internationella säkerhetssamarbetet. Hot mot freden och vår säkerhet kan bäst avvärjas i gemenskap och samverkan med andra länder. Inom ramen för Europeiska unionens (EU) gemensamma utrikes- och säkerhetspolitik (GUSP) bidrar Sverige till den civila och militära krishanteringen.

Syftet med försvarsunderrättelseverksamheten är att ge stöd för bedömningar och beslut till stöd för svensk utrikes-, säkerhets- och försvarspolitik, att bidra till det svenska deltagandet i internationellt säkerhetssamarbete samt att medverka med underrättelser för att stärka samhället vid svåra påfrestningar i fred.

4.2 Nya säkerhetshot och risker

I försvarsbesluten under 1990-talet har framhållits att omvärldsutvecklingen efter det kalla kriget har präglats av föränderlighet och svårbedömbarhet. Idag handlar säkerhetspolitik om att ha förmåga att möta ett brett spektrum av tänkbara hot, risker och påfrestningar mot samhället. Detta kräver en helhetssyn på såväl säkerhet och beredskap som på samhällets underrättelsefunktioner.

Under det kalla kriget dominerades hotbilden av de traditionella säkerhetspolitiska hoten, främst risken för ett storkrig mellan maktblocken i Europa. Försvaret inriktades på att möta en invasion av landets territorium. Idag bedöms ett enskilt militärt angrepp i alla dess former från en annan stat direkt mot Sverige som osannolikt under överskådlig tid, minst en tioårsperiod. Militära incidenter och kränkningar av vår territoriella integritet kan dock inte uteslutas, varför bedömningar av operativ förmåga och avsikter hos väpnade styrkor i vårt närområde förblir en viktig uppgift för försvarsunderrättelseverksamheten.

Regeringen höjer ambitionen för Sveriges deltagande i internationella insatser, och avser att fortsatt delta i insatser under ledning av Förenta nationerna (FN), Europeiska unionen (EU) och NATO. Svenskt deltagande i EU-ledda insatser kräver ett mera omfattande politiskt och resursmässigt engagemang än vad som tidigare har varit fallet vid FN- eller NATO-ledda insatser. Förutom underlag inför beslut om svenska insatser

och stöd till personalen i insatsområdet måste underrättelsetjänsterna också ha förmåga att förse statsmakterna med den information som kan behövas för att Sverige skall kunna göra självständiga bedömningar i säkerhetspolitiska frågor och att kritiskt granska andra aktörers argumentering och agerande.

Dagens säkerhetspolitiska hot, eller hot som är av sådan karaktär att de kan få säkerhetspolitiska konsekvenser, är av en annan karaktär än under det kalla kriget. Hoten är ofta gränsöverskridande, asymmetriska, icke-militära och utgår inte sällan från icke-statliga aktörer. Att förebygga och bekämpa sådana hot kräver inte bara ett nära samarbete mellan svenska myndigheter utan också ett effektivt internationellt samarbete.

Internationell terrorism och andra typer av grov internationell kriminalitet utgör idag hot mot såväl enskilda individer som mot stater. En väl utvecklad underrättelseinhämtning och en god krishanteringsförmåga är viktiga hjälpmedel för att förhindra denna typ av grov brottslighet och att hantera dess konsekvenser. Detsamma gäller åtgärder för att förhindra spridning av massförstörelsevapen, t.ex. Sveriges engagemang i *Proliferation Security Initiative (PSI)* och våra förpliktelser enligt FN:s säkerhetsråds resolution nr. 1540 om åtgärder för att förhindra spridning av massförstörelsevapen till icke-statliga aktörer. Att förhindra framställning och transport av vapen, komponenter och teknologi, särskilt i vårt närområde, kräver ett kvalificerat underrättelsestöd.

Den tekniska utvecklingen inom framförallt informationsteknologin och den framväxande globala kommunikationsstrukturen har bidragit till produktivitetsökningar i industrin och ett ökat välstånd. IT-beroendet inom den samhällsviktiga tekniska infrastrukturen, t.ex. kommunikationer, elförsörjning eller transporter, har samtidigt gjort det moderna samhället mer sårbart och berör enskilda såväl som organisationer, företag och stater. En avancerad teknisk kompetens i signalspaning är en förutsättning för att Sverige skall kunna skydda sina egna kommunikationssystem.

Det finns också en rad andra fenomen som kan påverka Sveriges säkerhet negativt och i vissa fall få säkerhetspolitiska konsekvenser. Hit hör t.ex. olika typer av försörjningskriser, ekologiska obalanser, miljöhot, etniska eller religiösa konflikter, stora flykting- och migrationsrörelser, ekonomiska utmaningar i form av valuta- och räntespekulationer. Snabba, effektiva och samordnade åtgärder från statsmakternas sida för att möta denna typ av hot eller påfrestningar kan i många fall underlättas av den förvarning och analys som en effektiv underrättelseverksamhet kan bidra med.

5 Underrättelseverksamhet

Med underrättelseverksamhet avses vanligtvis en verksamhet eller process för att med särskilda metoder inhämta, bearbeta, analysera och delge svåråtkomlig information som kan tjäna som kompletterande underlag för bedömningar och beslut av regering eller myndigheter. På policynivå tjänar underrättelseverksamhet främst till löpande kunskapsuppbyggnad, kompetenshöjning och förmåga att bekräfta eller vederlägga öppen in-

formation eller andra aktörers utspel och påståenden. I en trängre militärt inriktad säkerhetspolitisk mening brukar underrättelseverksamhet beteckna den verksamhet som syftar till att kartlägga främmande makters militära och politiska förhållanden samt handlingsmöjligheter.

5.1 Nuvarande reglering

Lagen (2003:130) om försvarsunderrättelseverksamhet innehåller bestämmelser om uppgifter och arbetsformer för försvarsunderrättelseverksamheten. En lagreglering av verksamheten är som regeringen framhöll i förarbetena inte obligatorisk, men fyller en viktig funktion genom att markera vikten av en väl fungerande underrättelseverksamhet som bedrivs utifrån i ett demokratiskt samhälle godtagbara grundprinciper. Regeringen anförde också att en lagreglering bidrar till ett högt förtroende för verksamheten från allmänhetens sida (prop. 1999/2000:25 s. 12). Riksdagen delade denna uppfattning och antog regeringens lagförslag i dess helhet (bet. 1999/2000:FöU3, rskr. 1999/2000:158).

Regeringen anförde vidare i förarbetena till lagen att det krävs ett begrepp för verksamheten som inte bara täcker underrättelseverksamhet till stöd för det militära försvaret utan även stöd för svensk medverkan i internationellt säkerhetssamarbete samt för att stärka samhället vid svåra påfrestningar i fred. Regeringen ansåg att en lämplig benämning för den beskrivna underrättelseverksamheten var försvarsunderrättelseverksamhet (prop. 1999/2000:25 s. 7).

Försvarsunderrättelseverksamhet – 1 §

Ett av försvarsunderrättelseverksamhetens syften är att kartlägga yttre militära hot mot landet. Underrättelseverksamheten skall enligt lagens förarbeten ses som ett led i Försvarsmaktens uppgifter i fred, under beredskap och i krig. Verksamheten skall ge underlag för Försvarsmaktens beredskap, operativa verksamhet och förbandsproduktion samt för krigsorganisationens utveckling och materiella förnyelse (se prop. 1999/2000:25 s. 14).

Försvarsunderrättelseverksamheten skall vidare bedrivas till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Försvarsunderrättelseverksamheten skall tidigt identifiera och redovisa eller ge förvarning om sådana förändringar i omvärldsläget som föranleder politiska beslut om totalförsvarets anpassning. Underrättelseverksamheten skall i ett kortare perspektiv fortlöpande bidra med information till ett sådant beslutsunderlag att en anpassning av försvarsorganisationens krigsduglighet hinner genomföras inom en viss tid före ett eventuellt angrepp. Underrättelseverksamheten skall vidare kunna identifiera sådana förändringar i omvärldsläget som kan föranleda beslut om anpassningsåtgärder i ett längre tidsperspektiv (se prop. 1999/2000:25 s. 14).

I verksamheten ingår också att medverka i svenskt deltagande i internationellt säkerhetssamarbete samt att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred. Enligt vad regeringen angav i förarbetena kan det i sistnämnda fall röra sig om att medverka med informa-

tion om och analys av t.ex. internationell terrorism och gränsöverskridande miljöhot. De normala ansvarsförhållandena på sådana områden påverkas inte av försvarsunderrättelseverksamhetens medverkan. Regeringen tillade att det självfallet är viktigt att försvarsunderrättelseverksamhetens medverkan vad gäller svåra påfrestningar är inriktad på sådana hot som den är lämpad för. Regeringen bör därför närmare bestämma över denna del av försvarsunderrättelseverksamheten (prop. 1999/2000:25 s. 14 f.).

Av bestämmelsen framgår att det är regeringen som skall bestämma försvarsunderrättelseverksamhetens inriktning.

Arbetsmetoder– 2 §

Underrättelseverksamhetens arbetsmetoder består av inhämtning, bearbetning och analys av information. Inhämtade underrättelser skall sedan i form av analyser och bedömningar redovisas för Regeringskansliet och andra berörda myndigheter (jfr prop. 1999/2000:25 s. 15).

Utlandssamarbete – 3 §

De myndigheter som skall bedriva försvarsunderrättelseverksamhet får, i enlighet med vad regeringen närmare bestämmer, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer.

Verksamheten skall styras av Sveriges säkerhetspolitiska intressen. Inom regeringen är underrättelsesamarbetet i första hand en uppgift för försvarsministern. Utrikesministern skall emellertid, enligt 10 kap. 8 § regeringsformen, hållas underrättad när fråga som är av betydelse för förhållandet till annan stat eller till mellanfolklig organisation uppkommer hos annan statlig myndighet. Genom den bestämmelsen åläggs de statliga myndigheterna en generell underrättelseplikt gentemot utrikesministern (se prop. 1999/2000:25 s. 16).

Förhållandet till polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete – 4 §

Försvarsunderrättelseverksamheten får inte avse uppgifter som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete.

I författningskommentaren angav regeringen att det i försvarsunderrättelseverksamheten inte får utövas verksamhet som inrymmer polisiära befogenheter, såsom förundersökningsåtgärder enligt rättegångsbalken och tvångsmedelsanvändning enligt bl.a. polislagen (prop. 1999/2000:25 s. 20).

Regeringen framhöll emellertid också att regleringen inte syftar till att utgöra något hinder mot att myndigheter som sysslar med försvarsunderrättelseverksamhet, enligt regeringens bestämmande, lämnar andra myndigheter biträde. Regeringen anförde i det sammanhanget att den tekniska utrustning som kan finnas hos en myndighet som är verksam med till exempel signalspaning inom försvarsunderrättelseverksamheten med

stöd av regeringens uppdrag skulle kunna användas även till stöd för verksamhet som bedrivs av annan myndighet inom ramen för en sådan myndighetsutövning som den senare myndigheten har att svara för. För en sådan ordning talade enligt regeringen också att teknisk utrustning som det allmänna anskaffat bör användas på ett rationellt sätt. Regeringen uttalade vidare att det även skulle finnas utrymme för att ge sådant stöd i andra avseenden och tillade slutligen att myndigheter som ägnar sig åt försvarsunderrättelseverksamhet, i enlighet med regeringens bestämmande, skulle kunna syssla med uppdragsverksamhet för annan myndighets räkning (a.a. s. 18).

Insyn – 5 §

I lagen finns slutligen en bestämmelse om att en särskild nämnd under regeringen skall ha insyn i försvarsunderrättelseverksamheten i enlighet med vad regeringen närmare föreskriver.

Enligt förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd ges nämnden uppgiften att följa underrättelsetjänsten inom Försvarsmakten och de övriga myndigheter som enligt förordningen (2000:131) om försvarsunderrättelseverksamhet bedriver försvarsunderrättelseverksamhet.

5.2 Vissa särskilda underrättelsemetoder

Den nationella underrättelseförmågan avgörs bl.a. av hur effektiv inhämtningen med särskilda metoder är. Utan en effektiv sådan inhämtning försvagas förmågan till efterföljande bearbetning och analys. De huvudsakliga metoderna för inhämtning med särskilda metoder är personbaserad inhämtning och signalspaning. Svenska och utländska underrättelsetjänster nyttjar i huvudsak dessa metoder för att inhämta information som inte är öppet tillgänglig. Inhämtning med särskilda metoder innebär att underrättelseinhämtningen sker genom förfaringssätt som det inte ankommer på andra underrättelseorgan att använda, jfr prop. 2005/06:149 s. 28.

5.2.1 Personbaserad inhämtning

Personbaserad inhämtning med särskilda metoder om utländska förhållanden utförs av Kontoret för särskild inhämtning (KSI). KSI är ett organ inom Militära underrättelse- och säkerhetstjänsten (MUST), som i sin tur är en del av Försvarsmakten. Rapporter baserade på det inhämtade materialet överlämnas normalt till MUST, som bearbetar dem tillsammans med annat underrättelsematerial. Personbaserad inhämtning utförs även åt andra myndigheter, t.ex. de övriga myndigheter som bedriver försvarsunderrättelseverksamhet. Vid personbaserad inhämtning är det av största vikt att underrättelseverksamhetens källor inte röjs, eftersom det kan innebära fara för källornas säkerhet och försvåra eller omöjliggöra fortsatt underrättelseinhämtning.

5.2.2 Teknisk inhämtning

Teknisk inhämtning med särskilda metoder sker till övervägande del genom den signalspaning som utförs av Försvarets radioanstalt. Försvarets radioanstalt är en civil myndighet som, tillsammans med Försvarsmakten, främst svarar för den svenska försvarsunderrättelseverksamheten enligt lagen (2000:130) och förordningen (2000:131) om försvarsunderrättelseverksamhet. Föreskrifter om Försvarets radioanstalts verksamhet finns också i förordningen (1994:714) med instruktion för Försvarets radioanstalt och i det årliga regleringsbrevet för myndigheten.

I instruktionen för Försvarets radioanstalt anges att myndigheten är en central förvaltningsmyndighet med uppgift att bedriva signalspaning enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare (Säkerhetspolisen med flera) anger. Som reglerna i lagen om försvarsunderrättelseverksamhet är formulerade faller viss del av Försvarets radioanstalts verksamhet alltså utanför försvarsunderrättelseverksamheten.

2 § i Försvarets radioanstalts instruktion anger att myndigheten särskilt skall

– följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet,
– fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, samt
– utföra matematiska bedömningar av kryptosystem för totalförsvaret.

Vidare skall Försvarets radioanstalt enligt 3 a § ha hög teknisk kompetens inom informationssäkerhetsområdet. Myndigheten får på begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller ur ett säkerhets- eller försvarspolitiskt avseende. Försvarets radioanstalt skall därvid särskilt kunna

– stödja insatser vid nationella kriser med IT-inslag,
– medverka till identifiering av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system,
– genomföra IT-säkerhetsanalyser, och
– ge tekniskt stöd.

Försvarets radioanstalt skall också samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

Försvarets radioanstalt har dessutom som uppgift att biträda andra myndigheter vid värdering, utveckling, anskaffning och drift av signalspaningssystem (3 §).

En övergripande uppgift för myndigheten är att bedriva signalspaning till stöd för svensk utrikes-, säkerhets- och försvarspolitik. Försvarets radioanstalt skall genom rapportering förse regeringen, Försvarsmakten och andra uppdragsgivare med de underrättelser som behövs för att ge underlag för planering, beslut och verkställighet. Verksamheten skall bedrivas så att den snabbt kan anpassas till den säkerhetspolitiska omvärldsutvecklingen och inriktas mot att bevaka den nationella säkerheten.

Signalspaning

Försvarets radioanstalts signalspaning syftar bl.a. till att ge förvarning om förhållanden i omvärlden som kan påverka landet i säkerhetspolitiska och militära hänseenden, t.ex. i form av väpnat angrepp eller kränkningar av Sveriges territoriella integritet. Signalspaningen bedrivs som kommunikationssignalspaning (KOS) mot utländsk radiokommunikation och som teknisk signalspaning (TES) mot t.ex. radarsignaler. Den utförs från stationer, som med hänsyn till radiovågornas utbredning är placerade på lämpliga platser i Sverige. Spaning bedrivs även från flygplan och fartyg.

KOS riktas mot såväl civila som militära eterburna signaler över kommunikationssatelliter och jordbundna system, t.ex. radiolänkar. Den sändande källans läge bestäms med hjälp av pejlanläggningar. Avsikten är att kartlägga såväl intentioner hos olika internationella aktörer som en potentiell motståndares organisation, stridsindelning, taktik och beredskap m.m. I allt större utsträckning har signalspaningen utvecklat en förmåga att följa de nya hoten som terrorism och gränsöverskridande organiserad brottslighet.

TES riktas mot signaler med andra syften än kommunikation, främst mot radar- och navigeringssystem. TES används i huvudsak för att utvinna teknisk information. Syftet är t.ex. att identifiera och lägesbestämma främmande flygplan och fartyg, att ge information om främmande vapensystems prestanda samt att varna för potentiella hot mot egna vapensystem. TES är också en grund för den egna offensiva förmågan till telekrigföring. Telekrigföring, dvs. verksamhet som innebär utnyttjande av elektroniska stridsmedel för att påverka motståndaren eller som syftar till att minska effekterna av motståndarens utnyttjande av elektronisk utrustning, utgör ett växande hot eftersom den kan förstöra vitala civila informations- och kommunikationssystem samt slå ut påkostade militära ledningss- och vapensystem. Utvecklingen ställer ökande krav på signalkunskap hos Försvarets radioanstalt. Myndigheten måste bl.a. kunna förse Försvarsmakten med aktuella signalreferensbibliotek, som kan utnyttjas i varnar- och motmedelssystem t.ex. på örlogsfartyg och i militära flygplan.

Inhämtade signaler i både KOS- och TES-funktionen bearbetas, analyseras och ställs samman till underrättelserapporter som sänds till Försvarets radioanstalts uppdragsgivare. Den sändande parten söker ofta skydda innehållet i kommunikationen genom olika former av signalskydd, t.ex. kryptering. Bearbetningen inom ramen för KOS-verksamheten syftar till att forcera signalskyddet och frilägga eller bestämma sändningarnas innehåll. Teknisk analys, trafikbearbetning och kryptoforcering är verktyg för detta.

Försvarets radioanstalt har till uppgift att, på uppdrag av Försvarsmakten, stödja svenska förband i internationell tjänst med signalspaningsutrustning och metodik som behövs bl.a. för att förvarna om hot mot förbanden, samt med underrättelser under pågående insats. Stödet till Försvarsmakten innebär bl.a. att stödja förbandsproduktion, utveckla och anskaffa signalspaningssystem samt att utveckla metodik och fackutbilda personal.

Försvarets radioanstalt har vidare att på uppdrag av olika myndigheter medverka med underrättelser i syfte att stärka samhället vid svåra på-

frestningar i fred. Myndigheten skall också stödja sådana statliga myndigheter och statligt ägda bolag som hanterar sådan information som är känslig från sårbarhetssynpunkt eller i säkerhetspolitiskt hänseende. Försvarets radioanstalt har enligt sin instruktion i övrigt att bedriva signalspaning i enlighet med vad de inriktande myndigheterna anger.

Den tekniska utvecklingens konsekvenser för signalspaningen

Inhämtning av information genom signalspaning har i Sverige i princip ansetts tillåten, då den har skett i ett trådlöst skede av transmissioner av kommunikationssignaler. Den tekniska utvecklingen när det gäller överföring av alla typer av signaler, t.ex. telefoni eller dataöverföring, har inneburit att överföringen numera till övervägande del sker genom tråd (kabel). Det saknas idag lagstöd för Försvarets radioanstalt att inhämta den information som förs i tråd. Detta utgör en allvarlig begränsning för att myndigheten nu och i framtiden skall kunna bedriva en ändamålsenlig inhämtningsverksamhet, upprätthålla ett trovärdigt signalskydd och skydda landet mot kvalificerade IT-relaterade hot.

I de flesta med Sverige jämförbara länder ger lagstiftningen, med olika typer av begränsningar till skydd för personlig integritet, möjlighet till inhämtning av såväl trådlös som trådbunden trafik för underrättelseändamål.

Dessa frågor berörs vidare i avsnitt 7.

5.3 Underrättelseverksamhet internationellt

5.3.1 Internationellt samarbete inom underrättelseverksamheten

Det internationella samarbetet på underrättelseområdet är av stor betydelse för enskilda länder. I dagens säkerhetspolitiska situation kan inget land helt på egen hand inhämta ett fullständigt underrättelseunderlag till stöd för den bedrivna utrikes-, säkerhets- och försvarspolitiken, särskilt inte ett litet land som Sverige. Till sammanhanget hör också att allt fler hot är transnationella, bl.a. internationell terrorism och gränsöverskridande brottslighet.

I den senaste budgetpropositionen har regeringen beskrivit försvarsunderrättelseverksamhetens allt viktigare funktion som stöd till EU:s framväxande förmåga inom ramen för den gemensamma utrikes- och säkerhetspolitiken (GUSP) och den europeiska säkerhets- och försvarspolitiken (ESFP). Regeringen anser att hög prioritet bör ges till stöd för svenskt deltagande i internationella uppgifter, inklusive förberedelserna och för Sveriges deltagande i och ledning av den nordiska stridsgruppen. (jfr prop. 2006/07:1 utgiftsområde 6 s. 38 och 56).

Före den nu gällande lagen (2000:130) om försvarsunderrättelseverksamhet saknade Sverige uttrycklig lagreglering av den underrättelseverksamhet som bedrevs till stöd för landets utrikes-, säkerhets- och försvarspolitik. Det huvudsakliga skälet till lagregleringen var, enligt Underrättelsekommittén (dir. 1996:111) att det skulle kunna bidra till att ge den viktiga och ofta uppmärksammade verksamheten ett högt förtroende hos

medborgarna (SOU 1999:37 s. 321). Lagen om försvarsunderrättelseverksamhet anger således ramarna för verksamheten och ger en viss anvisning om underrättelseverksamhetens uppbyggnad och funktion. Även om det med hänsyn till syftet med verksamheten varken är lämpligt eller möjligt att ge en uttömmande bild av landets underrättelseverksamhet, kan dagens lagstiftning ändå anses bidra till att öka allmänhetens insyn i och förståelse för verksamheten.

Sverige skiljer sig emellertid alltjämt från många andra länder, som har valt andra sätt att utåt redovisa eller lagreglera underrättelseverksamheten. För jämförelsens skull redovisas i det följande hur underrättelseverksamheten till stöd för utrikes-, säkerhets- och försvarspolitik bedrivs och regleras i vissa jämförbara länder, samt en kortfattad beskrivning av underrättelsesamarbetet inom EU. Lagregleringen av signalspaningen i de olika länderna redovisas i avsnitt 7.1.2.

5.3.2 Några internationella exempel

Nederländerna

I Nederländerna är såväl den militära, *MIVD (Militäre Inlichtingen- en Veiligheidsdienst),* som den civila underrättelse- och säkerhetstjänstens, *AIVD (Algemene Inlichtingen- en Veiligheidsdienst*), uppgifter och befogenheter fastställda i en gemensam lag från år 2002 (*Intelligence and Security Services Act 2002*). De båda tjänsterna styrs och kontrolleras på ett samordnat sätt och skall enligt lagen samarbeta med varandra.

Lagen är väsentligt utvidgad i förhållande till tidigare lag. Detta har bl.a. att göra med att lagstiftningen numera även innehåller bestämmelser om tjänsternas behandling av personuppgifter. I lagen finns en utförlig beskrivning av underrättelse- och säkerhetstjänsternas uppgifter samt preciseringar av vilka metoder tjänsterna får använda i sina verksamheter.

Kontroll

Den parlamentariska kontrollen över *AIVD* och *MIVD* utövas genom en särskild kommitté för underrättelse- och säkerhetstjänsterna. Vissa frågor som rör *MIVD:s* verksamhet kan också diskuteras i parlamentets försvarsutskott.

Genom 2002 års lagstiftning har ett nytt övervakningsorgan, en s.k. tillsynskommitté, inrättats. Dess uppgift är att övervaka att underrättelse- och säkerhetstjänsternas verksamheter bedrivs på ett lagligt och korrekt sätt. Tillsynskommittén skall även hålla berörda ministrar underrättade samt utreda och bedöma inkommande klagomål.

Metoder för underrättelseinhämtning

I 2002 års lagstiftning finns särskilda bestämmelser om vilka metoder underrättelse- och säkerhetstjänsterna får använda i sina verksamheter när det gäller inhämtning av information. Genom bestämmelserna har *AIVD* och *MIVD* befogenhet att under vissa villkor utnyttja ett antal olika

arbetsmetoder. Dessa metoder innefattar allt från tvångsmedel till signalspaning.

Här finns också särskilda bestämmelser om personbaserad inhämtning av underrättelser, enligt vilka underrättelse- och säkerhetstjänsterna får använda sig av enskilda personer för inhämtning av underrättelser. Dessa tjänstemän får även uppträda under fingerad identitet. Ansvariga myndigheter kan åläggas att samarbeta i nödvändig utsträckning för att förse en tjänsteman med fingerad identitet, varvid andra motstridiga myndighetsföreskrifter inte gäller.

Tjänstemännens uppdrag får avse inhämtning av information om personer eller organisationer som är relevant för syftet med underrättelse- och säkerhetstjänsternas verksamhet, eller åtgärder för att skydda tjänsternas intressen.

Underrättelse- och säkerhetstjänsterna får bedriva verksamhet i privaträttslig form, genom att bilda och driva bolag till operativt stöd för syftet med verksamheten.

Schweiz

Sedan år 1991 är underrättelsetjänsten och den militära säkerhetstjänsten i Schweiz delad. Underrättelsetjänsten är knuten till försvarsmakten och försvarsdepartementet, medan säkerhetstjänsten i dess helhet är knuten till den federala polisen och justitiedepartementet.

Den lagreglering, artikel 99 i *Bundesgesetz über die Armee und die Militärverwaltung (Militärgesetz)* från år 1996, som berör underrättelsetjänsten anger kort att tjänstens uppgift är att hämta in, bedöma och delge sådana uppgifter om främmande stater som är av säkerhetspolitisk betydelse. Vidare finns i artikeln vissa bestämmelser som berör underrättelsetjänstens rätt att hantera personuppgifter. I övrigt ges regeringen fullmakt att särskilt reglera bl.a. frågor om underrättelsetjänstens uppgifter och organisation samt om tjänstens samarbete med utländska underrättelsetjänster.

Den schweiziska regeringen har år 2003, med stöd av artikel 99 i *Militärgesetz*, utfärdat bestämmelser om underrättelsetjänsten, *Verordnung über den Nachrichtendienste im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (Nachrichtendienstverordnung*). Enligt lagens artikel 1 omfattar underrättelsetjänsten den strategiska underrättelsetjänsten (*SND*), den militära underrättelsetjänsten (*MND*) och flygvapenunderrättelsetjänsten *(LWND*).

Den strategiska underrättelsetjänsten svarar för kontakterna med utländska underrättelsetjänster. Informationsutbyte kan ske om det är till gagn för schweiziska säkerhetsintressen eller om det är föreskrivet i lag eller internationell överenskommelse. Allt regelbundet samarbete med utländska underrättelsetjänster kräver dock regeringens godkännande. Chefen för den strategiska underrättelsetjänsten har att en gång om året redovisa samarbetet för försvarsministern, som då även kan ge riktlinjer för den fortsatta verksamheten.

Kontroll

Den parlamentariska kontrollen av *SND* utövas av *Geschaffsprüfungsdelegation*, med uppgift att granska underrättelse- och säkerhetstjänsterna. Kontrollorganet består av sex parlamentariker och innebär en ren eftergranskning. Pågående underrättelseuppdrag berörs inte. Kontrollen tar endast sikte på om felaktigheter har begåtts i verksamheten.

Storbritannien

Det centrala brittiska underrättelseväsendet består dels av den militära underrättelsetjänsten, *Defence Intelligence Staff (DIS)*, dels av de tre civila underrättelse- och säkerhetstjänsterna, *Secret Intelligence Service (SIS* eller *MI6)*, *Government Communications Headquarters (GCHQ)* och *British Security Service (BSS* eller *MI5)*. De tre sistnämnda tjänsterna brukar kort benämnas *the Agencies*.

Teknisk och personbaserad inhämtning

SIS och *GCHQ* är de viktigaste inhämtningsorganen för hemlig underrättelseverksamhet och förser även *DIS* med information. Verksamheten vid *SIS* och *GCHQ* är sedan år 1994 reglerad genom en särskild lagstiftning, *Intelligence Services Act 1994*. Lagen innehåller också regler om bl.a. tillsyn och kontroll över *SIS, GCHQ* och *BSS*.

Inhämtningen inriktas av *Joint Intelligence Committe (JIC)* och avser bl.a. information om andra länder, terrorism, proliferation, internationell brottslighet m.m. *GCHQ* har även till uppgift att ge råd och anvisningar till departement och myndigheter samt försvarsmakten, när det gäller kommunikationssäkerhet och informationsteknologisystem.

SIS inhämtar underrättelser främst genom personbaserad inhämtning (*HUMINT*) men även genom tekniska förfaranden. *GCHQ:s* inhämtning sker genom signalspaning (*SIGINT*), mot bl.a. olika typer av kommunikationssystem och radarsignaler. *GCHQ:s* verksamhet innefattar även dekryptering och annan tolkning av skyddad information. Inhämtningsuppdragen kommer främst från utrikes- och försvarsministerierna, men även från finansministeriet samt *BSS* och andra myndigheter. Både *SIS* och *GCHQ* inhämtar underrättelser och andra uppgifter genom samarbete med ett brett nät av utländska underrättelse- och säkerhetstjänster.

Kontroll

Regeringen utövar kontroll över de civila underrättelse- och säkerhetstjänsterna, *the Agencies*, dels genom att cheferna för dessa är personligen ansvariga inför respektive minister, dels genom en särskild departementskommitté, *Ministerial Committee on the Intelligence Services*. Kommittén leds av premiärministern och i den ingår bl.a. utrikes-, försvars-, inrikes- och finansministrarna. Kommittén bevakar mera övergripande de policyfrågor som berör tjänsterna. Ministrarna biträds i tillsynen och kontrollen av en tjänstemannagrupp, *Permanent Secretaries' Committee on the Intelligence Services.*

År 1994 inrättades en parlamentarisk underrättelsenämnd, *Intelligence and Security Committee*, med uppgift att granska *the Agencies*. Granskningen tar sikte på tjänsternas budget, organisation och verksamhet. Kontrollorganets ledamöter består av nio medlemmar från över- och underhusen. De utses av premiärministern efter samråd med oppositionsledaren. Underrättelsenämnden rapporterar årligen till premiärministern och i vissa delar till parlamentet. Vid behov rapporterar nämnden även löpande till premiärministern.

Underrättelsetjänsten *DIS*, som ingår i försvarsdepartementet, omfattas inte av underrättelsenämndens granskning. *DIS* är underkastad den sedvanliga kontroll och granskning av de olika ministerierna som sker i parlamentet. Kontrollen och granskningen av *DIS* sker genom *Select Committee for Defence*.

De tre underrättelse- och säkerhetstjänsterna är även underkastade tillsyn genom särskilda av premiärministern utsedda tjänstemän, *Security Service Commissioner, Intelligence Service Commissioner* och *Interception Commissioner*. De två förstnämnda funktionerna upprätthålls av höga jurister. Dessa har att granska sådana åtgärder från underrättelse- och säkerhetstjänsternas sida som vidtas mot enskildas egendom med stöd av den lagstiftning som reglerar tjänsternas verksamhet. Tillsynen innefattar även att utreda allmänhetens klagomål mot verksamheten. Årliga rapporter lämnas till premiärministern och till parlamentet. *The Interception Commissioner* har motsvarande funktion vad gäller givna tillstånd för underrättelse- och säkerhetstjänsterna att ta del av post- och telekommunikationer.

Tyskland

Den centrala tyska underrättelsetjänsten *Bundesnachrichtendienst (BND*) arbetar både med civila och militära underrättelser. Därtill kommer säkerhetstjänsterna, den civila *Bundesamt für Verfassungsschutz (BfV),* och den militära säkerhetstjänsten *Militärischer Abschirmdienst (MAD).*

BND är en fristående myndighet som lyder under den tyska statsrådsberedningen, *Bundeskanzleramt*. *BND*:s verksamhet är reglerad i den tyska grundlagen. Därutöver är verksamheten reglerad i särskild lagstiftning, *Gesetz über den Bundesnachrichtendienst.*

I lagen anges att *BND* skall inhämta och analysera information som behövs för underrättelser om utländska förhållanden och som är av betydelse för den tyska utrikes- och säkerhetspolitiken. *BND* skall inte befatta sig med information om inhemska förhållanden annat än om dessa berör *BND:s* egen verksamhet och personal eller kontraspionage. Vidare finns regler som skall garantera att tyska medborgare eller tyska intressen inte träds för när genom *BND:s* verksamhet. Hänvisning görs även till proportionalitetsprincipen.

I lagen ges regler om *BND:s* befogenheter i verksamheten och om behandling av personuppgifter och s.k. överskottsinformation, samt regler om kontroll av information och om skydd för *BND:s* personal, utrustning, källor m.m. Det finns även regler om gränsdragningen mellan underrättelsetjänstens och polisens och säkerhetstjänstens uppgifter. *BND* har inte någon exekutiv befogenhet.

BND:s uppgifter är att bedriva underrättelseverksamhet mot utrikespolitiska och utländska militära och ekonomiska förhållanden. *BND* skall i övrigt utföra underrättelseuppdrag utomlands enligt anvisningar från förbundskanslern och förbundsregeringen samt bevaka utländsk underrättelseverksamhet i Tyskland. *BND* skall även ta emot underrättelseuppdrag från olika departement när det gäller omvärldsbevakning bl.a. om internationella kriser, proliferation och vapenhandel, teknologiöverföring, internationell brottslighet såsom narkotikahandel och penningtvätt, internationell terrorism och extremism. *BND:s* verksamhet skall dock endast bedrivas med utgångspunkt i nationella underrättelsebehov.

Kontroll

Regeringens och chefens för statsrådsberedningen kontroll och styrning av *BND* sker genom en särskild avdelning inom statsrådsberedningen. Därutöver har statssekreteraren i statsrådsberedningen, i sin kapacitet som *Beauftragter für Nachrichtendienste* eller koordinator, att fylla denna uppgift. Koordinatorn har även uppgifter i samband med den parlamentariska kontrollen av de tre underrättelse- och säkerhetstjänsterna och i budgetarbetet för dessa.

Den parlamentariska kontrollen av de tre underrättelse- och säkerhetstjänsterna är omfattande. Kontrollen är lagreglerad och utövas av en parlamentarisk kontrollpanel, *Parlamentarische Kontrollgremium (PKGr),* som idag består av nio parlamentsledamöter. De skall sammanträda en gång per kvartal och har, med undantag av uppgifter om identitetsskyddade källor, oinskränkt rätt att kontrollera verksamheten. Kontrollen innefattar tillgång till arkiv och förhör med personalen. Det sistnämnda medför också möjlighet för personalen att ta upp frågor med kontrollpanelen om hur verksamheten utövas. Kontrollen innefattar även förhör med ansvariga ministrar och med koordinatorn. *PKGr* granskar också förslagen till budget för underrättelse- och säkerhetstjänsterna.

Den parlamentariska kontrollpanelen utser den s.k. G 10-kommissionen, som har till uppgift att granska användningen av metoder riktade mot post och telekommunikationer (signalspaning, hemlig teleavlyssning, hemlig teleövervakning, kameraövervakning, postkontroll etc.) Ordföranden måste ha kompetens som domare och de sju ledamöterna behöver inte vara ledamöter av Förbundsdagen. En av kommissionens uppgifter är att godkänna sökbegrepp inom signalspaningen och att även i övrigt ta ställning till om föreslagna åtgärder har stöd i lag och är nödvändiga.

Underrättelsesamarbetet inom EU

Den gemensamma utrikes- och säkerhetspolitiken (GUSP) och den europeiska säkerhets- och försvarspolitiken (ESFP) har skapat behov av vissa analys- och underrättelsefunktioner på EU-nivå. Det är naturligtvis av största vikt att EU kan göra en korrekt hotbildsanalys för ett område, dit man kan komma att skicka civil eller militär personal.

Underrättelseverksamheten inom EU är fortfarande i ett uppbyggnadsskede, och det finns utrymme för att stärka funktionerna för bearbetning och analys.

Inom EU:s militära stab har upprättats en underrättelsefunktion (*Intelligence Division*). Detta är en formell rådsfunktion som styrs av militärkommittén och skall ägna sig åt militärstrategiska bedömningar.

I samband med Amsterdamfördraget har vid Rådssekretariatet en *Policy Planning and Early Warning Unit* (Policyenheten) inrättats, för att täcka behovet av politisk analys och bakgrundsinformation. I en förklaring till Amsterdamfördraget sägs att medlemsstaterna och kommissionen skall stödja den politiska planeringen genom att i största möjliga utsträckning tillhandahålla relevanta upplysningar, inklusive underrättelser.

Som en del av den särskilda policyenheten har en lägescentral, *Situation Center (SITCEN)*, inrättats. I takt med utvecklingen av den gemensamma säkerhets- och försvarspolitiken för krishanteringsinsatser har lägescentralen utvecklats för att utöka möjligheten till analys och utbyte av relevant information. Under 2005 har inom SITCEN inrättats en enhet för underrättelsebearbetning vad avser terrorism.

Regeringen har i regleringsbrev för budgetåret 2007 för de myndigheter som bedriver försvarsunderrättelseverksamhet uttalat att dessa myndigheter skall bidra till ett förstärkt underrättelsesamarbete inom ramen för EU:s gemensamma utrikes- och säkerhetspolitik och EU:s krishanteringsförmåga.

Sverige har bl.a. ställt en svensk tjänsteman med gedigen erfarenhet från underrättelseverksamhet och säkerhetstjänst till lägescentralens förfogande. Motivet är att lägescentralen bedöms få en central roll för informations- och underrättelseutbyte för GUSP och konfliktförebyggande åtgärder, samt att Sverige vill bidra till att skapa en stark och effektiv gemensam utrikes- och säkerhetspolitik.

6 Anpassning av försvarsunderrättelseverksamheten

6.1 Bakgrund

6.1.1 Underrättelsekommittén

Som har redogjorts för i avsnitt 4 har den säkerhetspolitiska situationen medfört ett bredare spektrum av hot, risker och påfrestningar. Vissa hot och utmaningar av icke-militär natur kan vara av så allvarlig art att de berör hela samhället. Militär förmåga kan komma att behövas för att skydda samhället och nationella intressen.

Underrättelsekommittén konstaterade att det vidgade säkerhetsbegreppet väckte frågor om och i vad mån den militära underrättelsetjänsten skall ta sig an sådana icke-militära hot och påfrestningar. Enligt kommittén borde ansvaret för hanteringen av den förändrade hotbilden såväl i fredstid som i krig enligt gängse princip ligga hos den myndighet som har ansvaret i fredstid, och att det först i den mån en sådan myndighet saknar egen kapacitet för underrättelseinhämtning kan vara aktuellt för

underrättelsetjänsten att bistå denna i olika avseenden (se SOU 1999:37 s. 240 ff.).

Underrättelsekommittén föreslog att de grundläggande uppgifterna inom försvarsunderrättelseverksamheten skulle anges med uttrycket ”kartlägga yttre militära hot och andra yttre hot mot landet”. Verksamheten skulle vidare bidra till att stärka samhället vid svåra påfrestningar i fred. Enligt Underrättelsekommittén skulle den militära underrättelsetjänsten främst belysa hotbildens militära aspekter. Kommittén ifrågasatte behovet av bidrag från den militära underrättelsetjänsten vad gäller ett mer allsidigt, icke-militärt präglat underlag som stöd för ”svensk utrikes- och säkerhetspolitik”. Kommittén framhöll att den militära underrättelsetjänsten synes sakna förutsättningar för en sådan analysuppgift utan en radikalt annorlunda uppgiftsinriktning och organisation (se SOU 1999:37 s. 243).

I sitt remissyttrande framförde Säkerhetspolisen vissa betänkligheter när det gällde de nya hoten, särskilt om ansvaret för bekämpning av terrorism och samordningsansvaret för icke-spridningsfrågor. Enligt Säkerhetspolisen framstod det som oklart om kommitténs förslag innebar att underrättelsetjänsten utifrån det vidgade säkerhetsbegreppet skulle bygga upp egna resurser inom området. Säkerhetspolisen erinrade också om att regeringen tidigare hade uttalat (skrivelse till riksdagen om beredskapen mot svåra påfrestningar på samhället i fred, skr. 1998/99:33 s. 18) att ett samarbete mellan Försvarsmakten och ansvarig civil myndighet förutsätter att den civila myndigheten uttryckligen anger att det finns behov av ett sådant stöd.

Regeringen uttalade sig inte i samband med förslaget till lag om försvarsunderrättelseverksamhet om yttre icke-militära hot mot landet. Frågan om försvarsunderrättelseverksamheten skulle omfatta sådana hot berördes dock under utskottsbehandlingen i riksdagen (bet. 1999/2000:FöU3 s. 10 f.).

6.1.2 11 september-utredningen

Den s.k. 11 september-utredningen hade i uppdrag att kartlägga och analysera myndigheternas och de övriga offentliga organens samlade beredskap och förmåga att förhindra, bekämpa och i övrigt hantera omfattande terroristattentat och andra likartade extraordinära händelser.

Utredningen föreslog i betänkandet Vår beredskap efter den 11 september (SOU 2003:32) att uppgiften ”att kartlägga yttre militära hot” i lagen om försvarsunderrättelseverksamhet skulle ersättas med ”kartlägga yttre väpnade hot mot landet”, eftersom den förra uppgiften inte kunde anses innefatta icke-militär terrorism. Utredningen pekade på den oklarhet som det innebär att planering av väpnade terroristangrepp är att betrakta som en kriminell handling som faller inom den polisiära sfären, även om förberedelserna genomförs utomlands. Utredningen föreslog därför ett tillägg till 4 § lagen om försvarsunderrättelseverksamhet med innebörden att den där angivna gränsen mellan polisiär verksamhet och försvarsunderrättelseverksamhet inte skall gälla för försvarsunderrättel-

severksamhet som ”bedrivs utomlands eller med inriktning på utländska förhållanden”.

I remissvaren på utredningens förslag framfördes från Rikspolisstyrelsen att förslaget kan leda till att gränsen luckras upp mellan ”civila och militära myndigheters roll i samhället” och att Försvarsmakten inte skall bearbeta och analysera underrättelseinformation som har betydelse i polisens brottsbekämpande arbete. Sådan information borde enligt Rikspolisstyrelsen omgående överlämnas till behörig polismyndighet. Säkerhetspolisen påpekade det olämpliga i att inom Försvarsmakten bygga upp en med Säkerhetspolisen parallell kompetens för inhämtning, bearbetning och analys.

Även Försvarsmakten avstyrkte utredningens förslag och framhöll att regeringen på annat sätt än genom lagstiftning bör klargöra vilka säkerhetspolitiska aspekter som terrorism har, och hur underrättelsebehovet skall tillgodoses. Försvarsmakten underströk också att den har det odelade ansvaret för inhämtning utomlands med särskilda metoder, samt att man redan idag har möjlighet att inom ramen för försvarsunderrättelseverksamheten inhämta, bearbeta och analysera information som berör terrorism i den utsträckning som krävs för att tillgodose kravet på att stödja svensk säkerhetspolitik.

Många andra remissinstanser redovisade också tvekan eller avstyrkte utredningens förslag om att ge Försvarsmakten underrättelseuppgifter i terroristbekämpningen. Däremot betonade många remissinstanser vikten av nära samarbete och ett effektivt utbyte av information mellan underrättelse- och säkerhetsorganisationerna. Bland remissinstanserna fanns också stor förståelse för behovet av att utvidga försvarsunderrättelseverksamhetens befogenheter att inhämta underrättelser utomlands för att Sverige skall kunna ha beredskap mot terroristangrepp och andra allvarliga hot. Flera remissinstanser framhöll emellertid risken för oklarheter i ansvars- och befogenhetsfrågor mellan de myndigheter som bedriver försvarsunderrättelseverksamhet och Säkerhetspolisen.

6.2 Behovet av en förändrad försvarsunderrättelseverksamhet

Regeringens bedömning: Den allt mer komplexa säkerhetspolitiska hotbilden, den tekniska utvecklingen och det ökande svenska engagemanget i internationella insatser nödvändiggör vissa anpassningar av regelverket för försvarsunderrättelseverksamheten. Det krävs förändringar framförallt i fråga om den rättsliga regleringen av arbetsmetoderna och den samhälleliga kontrollen samt viss anpassning av mandatet för verksamheten.

Promemorians bedömning: Överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser som har yttrat sig har delat bedömningen eller lämnat den utan erinran. *Krisberedskapsmyndigheten* och *Inspektionen för strategiska produkter* har framhållit att de nya hotbilderna skapar ett växande underrättelsebehov även hos andra myndigheter än de brottsförebyggande och brottsbekämpande. *Skatteverket* har betonat att det är väsentligt att resultatet av verksamheten även

kommer civila myndigheter och näringsliv tillgodo. *Svenskt Näringsliv* och *Svenska bankföreningen* har påtalat vikten av att verksamheten styrs av hotbildsanalyser som också omfattar näringslivets skyddsbehov och att resultatet av verksamheten också skall delges näringslivet när vitala samhällsintressen berörs.

Hovrätten för Övre Norrland har framhållit att den föreslagna regleringen innehåller en mängd svårbedömda gränsdragningar och det problematiska i att reglera en verksamhet som egentligen inte låter sig regleras, men har mot bakgrund av behovet av verksamheten ingen principiell invändning mot den föreslagna författningsregleringen som sådan.

Rikspolisstyrelsen och *Säkerhetspolisen* har förordat en förnyad, bredare och djupare analys av vilka effekter, behov och förändringar inom hela den civila och militära underrättelseverksamheten som föranleds av den nya hotbilden rörande den nationella säkerheten i vid mening. *Säkerhetspolisen* och *Svenska polisförbundet* har framhållit att varje sektorsansvarig myndighet måste ges tillräckliga resurser och mandat för att själv kunna lösa sin uppgift, samtidigt som det inte är rimligt att samhället skapar parallella resurser inom områden där speciell kompetens krävs. Om behovet av försvarsunderrättelseverksamhet riktad mot militära yttre hot minskat är det enligt de båda remissinstanserna naturligt att föra över resurser till andra verksamheter som har större behov av dessa. En sådan omprioritering kan på kort sikt ske genom att Säkerhetspolisen ges mandat att beställa och anlita kapacitet hos de myndigheter som bedriver försvarsunderrättelseverksamhet varigenom det goda samarbete som i dag finns kan fortsätta. Verksamheten handlar emellertid då inte om försvarsunderrättelseverksamhet utan om stöd till underrättelseinhämtning inom ramen för polisiär verksamhet. *Kammarkollegiet* har framhållit att tyngdpunkten i underrättelseverksamheten numera finns inom det ickemilitära området och att detta bör återspeglas i en annan struktur och organisation.

Skälen för regeringens bedömning

Lagreglering av försvarsunderrättelseverksamheten

Regeringsformen uppställer inte något formellt krav på lagreglering av underrättelseverksamhet som avser landets yttre säkerhet och dess säkerhetspolitik (SOU 1999:37, s. 204 f.). Detta krävs däremot enligt regeringsformen när det gäller fri- och rättighetsbegränsande åtgärder, regler som gäller åligganden för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden. Staten har också enligt Europakonventionen en skyldighet att garantera att konventionens fri- och rättigheter upprätthålls i lagstiftning, rättstillämpning och annan form av maktutövning. Europakonventionen medger dock i vissa fall inskränkningar som i ett demokratiskt samhälle är nödvändiga med hänsyn till bl.a. statens säkerhet (se t.ex. art. 8) .

I förarbetena till lagen (2000:130) om försvarsunderrättelseverksamhet anförde regeringen att en lagreglering, även om den inte är obligatorisk, ändå borde ske i syfte att understryka att verksamheten måste bedrivas på ett sätt som är förenligt med demokratins och rättssamhällets grundprinciper. Regeringen ansåg att en sådan reglering kan bidra till att skapa

förtroende hos allmänheten och en förståelse för verksamhetens betydelse för landets säkerhet (prop. 1999/2000:25 s. 12). Den bedömningen gör sig alltjämt gällande.

Det ligger i sakens natur att en reglering av försvarsunderrättelseverksamheten inte kan bli heltäckande. Som *Hovrätten för Övre Norrland* har framhållit innehåller den föreslagna regleringen en mängd svåra gränsdragningar som inte i alla avseenden lämpar sig för lagreglering. Detta bör dock inte hindra att de grundläggande förutsättningarna för verksamhetens bedrivande läggs fast i lag.

Även de nödvändiga anpassningar som berörs i det följande bör av samma skäl lagregleras. När det gäller regleringen av signalspaning följer av de bestämmelser till skydd för enskildas fri- och rättigheter i Europakonventionen och regeringsformen som berörts ovan att en lagreglering av verksamheten är nödvändig. Till den frågan återkommer regeringen i avsnitt 7.

Anpassningsbehovet

Den svenska försvarsunderrättelseverksamheten utvecklades efter andra världskriget mot bakgrund av den hotbild som var helt dominerande under det kalla kriget, nämligen ett yttre militärt hot från en annan stat eller grupp av stater. Hotbilden har sedan dess förändrats avsevärt. Trots att något militärt väpnat angrepp i alla dess former från annan stat direkt mot Sverige är osannolikt under överskådlig tid (minst en tioårsperiod), kan emellertid risken för väpnade konflikter, incidenter och kränkningar av Sveriges territoriella integritet inte uteslutas. Att bevaka den militära utvecklingen i vårt närområde förblir därför alltjämt en viktig uppgift för den svenska försvarsunderrättelseverksamheten.

En annan central och allt viktigare uppgift för försvarsunderrättelseverksamheten är att förse regeringen med underlag för beslut i utrikes-, försvars- och säkerhetspolitiska frågor. Den säkerhetspolitiska utvecklingen under det senaste decenniet, som har redovisats i avsnitt 4, har också aktualiserat en rad frågeställningar. Säkerhetsbegreppet har vidgats. En rad andra hot och risker än de traditionella måste nu ges ökad uppmärksamhet i säkerhetspolitiken och därmed också i underrättelseverksamheten. Sådana hot och risker är bl.a.

– terrorism,
– spridning av massförstörelsevapen,
– internationell kriminalitet av stor omfattning och kvalificerad art som t.ex. smuggling av vapen, droger eller människor,
– flykting- och migrationsrörelser, orsakade av t.ex. etniska och kulturella konflikter eller miljöförstöring, samt
– hot mot den tekniska infrastrukturen, inte minst tele- och datasystemen.

Denna typ av risker och hot kännetecknas av att de inte sällan utgår från icke-statliga aktörer samt är transnationella och icke-militära till sin karaktär. Hotbilden är oftast komplex och berör flera samhällssektorer. Den kunskap som krävs för en effektiv nationell politik mot dessa hot och risker finns utspridd på ett större antal myndigheter än tidigare, och kräver bredare kontakt- och samarbetsytor mellan myndigheter än de traditionella.

Såväl Sveriges traditionella engagemang i fredsfrämjande och humanitära internationella insatser som Sveriges medlemskap i EU innebär ökade krav på aktivt svenskt deltagande i civil och militär krishantering utomlands. Detta innebär i sin tur växande krav på försvarsunderrättelseverksamheten att bidra med information av betydelse för beslut om svenskt deltagande samt för skydd av den svenska personalen. Det rör sig ofta om geografiska områden väl bortom vårt närområde och inte sällan om för försvarsunderrättelseverksamheten relativt nya funktionella områden som t.ex. medicinska underrättelser eller organiserad brottslighet av sådan karaktär och omfattning att verksamheten kan få säkerhetspolitiska konsekvenser.

Den säkerhetspolitiska utvecklingen har inneburit att Regeringskansliet blivit en allt större och viktigare konsument av underrättelser för regeringens behov, medan Försvarsmaktens relativa andel har minskat. Därtill kommer växande underrättelsebehov till stöd för verksamheten inom andra samhällssektorer. Polisens kriminalunderrättelseverksamhet, Säkerhetspolisen, Tullverket och Kustbevakningen är exempel på naturliga mottagare av sådan information som på en övergripande nivå har betydelse för den brottsförebyggande och brottsbekämpande verksamheten. På andra områden har t.ex. Inspektionen för strategiska produkter behov av underrättelser av relevans för exportkontroll av produkter kopplade till massförstörelsevapen och Krisberedskapsmyndigheten behov av underrättelser kring hot i vid mening av intresse för samhällets krishanteringsförmåga. Underrättelser är också, som *Skatteverket, Svenskt Näringsliv* och *Svenska bankföreningen* framhållit, av intresse utanför myndighetssfären. Ytterligare en viktig del i försvarsunderrättelseverksamheten är att lämna stöd för EU:s underrättelsesamarbete.

De myndigheter som bedriver försvarsunderrättelseverksamhet måste ha förmåga att inhämta, bearbeta och delge relevanta underrättelser, i rätt tid, i rätt format och till rätt mottagare. En adekvat underrättelseverksamhet mot dagens transnationella säkerhetspolitiska hot förutsätter också ett omfattande internationellt samarbete. Det gäller för alla länder, men i synnerhet för små och medelstora länder som Sverige. För att vara en relevant och intressant samarbetspartner krävs att Sverige har en god förmåga och kunskap på underrättelseområdet.

Säkerhetspolisen, *Rikspolisstyrelsen, Sveriges polisförbund* och *Kammarkollegiet* har påpekat att förflyttningen av fokus från yttre militära hot till en bredare hotbild borde resultera i en omprioritering av de resurser som i dag läggs på försvarsunderrättelseverksamheten till de myndigheter som har ansvar för icke-militära yttre hot, eller att i vart fall resurserna hos de myndigheter som bedriver försvarsunderrättelseverksamhet skall kunna tas i anspråk för underrättelseverksamhet inom ramen för det polisiära arbetet. Det är också regeringens uppfattning att det är angeläget att samhällets underrättelseresurser kan användas mer samordnat för att möta de hot som idag föreligger mot vårt land. De resurser som hittills använts för att möta yttre militära hot bör därför som flera remissinstanser varit inne på få ett breddat användningsområde. Att den breddade hotbild som redovisats i avsnitt 4 berör också andra samhällsintressen framgår av de synpunkter som lämnats av bl.a. *Krisberedskapsmyndigheten, Inspektionen för strategiska produkter, Skatteverket, Svenskt näringsliv* och *Svenska bankföreningen*.

Hos de myndigheter som bedriver försvarsunderrättelseverksamhet finns resurser och kompetens som med de anpassningar som följer av de förslag som nu lämnas möjliggör en effektiv underrättelseverksamhet till gagn för hela samhället. Mot bakgrund av den snabba utvecklingen i omvärlden och den ständiga uppkomsten av nya företeelser av relevans för svensk utrikes-, säkerhets- och försvarspolitik är det angeläget att en anpassning nu sker som möjliggör att förändringarna kan fångas upp och informationen nå ut till berörda intressenter.

Förslagen tar sikte på försvarsunderrättelseverksamhetens uppgifter och arbetsmetoder och hur dessa kan utnyttjas för att tillgodose det växande underrättelsebehovet inom ramen för befintlig organisationsstruktur. Eftersom regeringen ser möjligheten att uppnå den eftersträvade effekten genom de förslag till författningsreglering som nu lämnas, saknas anledning att i detta sammanhang göra någon mer genomgripande omprövning av myndighetsstrukturen eller resursfördelningen på underrättelseområdet. De förslag som lämnas här innebär dock inte några hinder för att en mer övergripande översyn av samhällets resurser för underrättelseverksamhet genomförs.

Skatteverket, Svenskt näringsliv och *Svenska bankföreningen* har betonat vikten av att resultatet av försvarsunderrättelseverksamheten också kommer näringslivet till godo och att näringslivets behov beaktas vid styrningen av verksamheten. Enligt regeringens mening är det naturligt att en försvarsunderrättelseverksamhet till nytta för hela samhället också beaktar näringslivets behov. Det bör dock alltjämt vara förbehållet myndigheterna att inrikta verksamheten och utgöra mottagare av underrättelser. Frågan behandlas närmare i avsnitt 6. 4.

När det gäller försvarsunderrättelseverksamhetens uppgifter i förhållande till de brottsförebyggande och brottsbekämpande myndigheterna och den närmare gränsdragningen mellan verksamheterna behandlas dessa frågor i avsnitt 6.3.

I det följande presenteras de förändringar av den rättsliga regleringen för verksamheten som regeringen bedömer nödvändiga för att anpassa försvarsunderrättelseverksamheten till de växande underrättelsebehoven inom utrikes-, säkerhets- och försvarspolitiken. Ändringarna innebär i korthet följande:

– mandatet för försvarsunderrättelseverksamhet ändras från ”yttre militära hot” till ”yttre hot”,

– gränsdragningen mellan polisiär verksamhet och försvarsunderrättelseverksamhet förtydligas, och

– regleringen av inriktning, rapportering av underrättelser och inhämtningen med särskilda metoder förtydligas.

I därpå följande avsnitt behandlas införandet av ett uttryckligt lagstöd för signalspaningen, i syfte att anpassa verksamheten till den tekniska utvecklingen, regeringens överväganden kring avvägningen mellan verksamhetens intressen och skyddet för enskildas fri- och rättigheter samt en förstärkning av samhällets funktioner för inriktning och kontroll av underrättelseverksamheten.

6.3 Författningsregleringen av försvarsunderrättelseverksamhetens mandat och gränsdragningen mot andra verksamheter

6.3.1 Försvarsunderrättelseverksamhetens uppgifter

Regeringens förslag: Förutom att tjäna som ett stöd för svensk utrikes-, säkerhets- och försvarspolitik skall försvarsunderrättelseverksamheten kartlägga yttre hot mot landet, oavsett om de är militära eller ej. I verksamheten ingår också att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Verksamheten får endast avse utländska förhållanden.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser som har yttrat sig har tillstyrkt förslaget eller lämnat det utan erinran. *Banverket* har framfört att försvarsunderrättelseverksamheten bör avse både inre och yttre hot mot Sverige och att samarbete med näringslivet bör utvecklas. *Krisberedskapsmyndigheten* har ställt sig positiv till ändringen från ”yttre militära hot mot landet” till ”yttre hot mot landet” men anser att en konsekvens av detta borde vara att begreppet ”försvarsunderrättelseverksamhet” byts ut mot ett bredare begrepp. Krisberedskapsmyndigheten har också framhållit att begränsningen till utländska förhållanden kan vara problematisk då det blir allt svårare att skilja på inre och yttre hot, t.ex. på informationssäkerhetsområdet. *Amnesty international* har anfört att begreppet ”yttre hot” framstår som rimligt om det avgränsas till de exempel som tas upp i promemorian men har påtalat risken för att innehållet i detta begrepp sedan utvidgas steg för steg utan att en utförlig kontroll av konsekvenserna görs.

Åklagarmyndigheten, *Kustbevakningen*, *Datainspektionen*, *Kammarrätten i Stockholm* och *Lunds universitet* har påtalat att den föreslagna inriktningen av försvarsunderrättelseverksamheten innebär en överlappning mot den brottbekämpande verksamheten för vilken polis och åklagare har ansvaret och att det finns en risk för oklarheter i ansvars- och befogenhetsfrågor mellan framför allt Säkerhetspolisen och de myndigheter som har att bedriva försvarsunderrättelseverksamhet. Åklagarmyndigheten har särskilt understrukit vikten av att man i den praktiska tillämpningen skapar garantier mot en sammanblandning av polisiära uppgifter och försvarsunderrättelseverksamhet. Kammarrätten har anfört att behovet av förändringen inte synes tillräckligt klarlagt och framhållit att också polisen i ökad omfattning deltar i internationellt samarbete. Kammarrätten har också påpekat att kunskaper och resurser som finns inom försvaret och hos polisen bör kunna samutnyttjas för den verksamhet som berörs i promemorian. Även *Totalförsvarets forskningsinstitut* har anfört att den uppgiftsmässiga skiljelinjen och relationen mellan underrättelsemyndigheterna och polisväsendet inte är helt klar men har framhållit att det finns ett växande gemensamt behov av samma information och att det gäller att förebygga en uppdelning av underrättelseinhämtningen som kan leda till att information tappas bort. Institutet framhåller att överlappningar synes vara oundvikliga, även om den författningsmäs-

siga gränsdragningen har viss betydelse, och förespråkar mot den bakgrunden en funktion för gemensam underrättelseanalys. Institutet framhåller vidare att försvarsunderrättelsefunktionen utgör en nationell resurs och att frågan om hur denna resurs bäst skall utnyttjas snabbt bör få en lösning i den riktning som förslaget anger.

Justitiekanslern, som i huvudsak har ställt sig bakom de överväganden som gjorts kring huvudlinjerna för försvarsunderrättelseverksamheten och gränsdragningen mellan försvarsunderrättelseverksamheten och polisiär verksamhet, har anfört att förslaget att upphäva föreskriften om att i försvarsunderrättelseverksamhet ingår ”att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred” innebär att en befintlig möjlighet för regeringen tas bort utan närmare övervägande. Justitiekanslern har ifrågasatt promemorians bedömning att föreskriften inte behövs eftersom detta område kommer att täckas av det nya uttrycket ”yttre hot mot landet” och har påpekat att det torde finns ”svåra påfrestningar på samhället” som inte utgör ”yttre hot”, t.ex. naturkatastrofer. Justitiekanslern har vidare anfört att också förslaget att försvarsunderrättelseverksamheten endast får avse ”utländska förhållanden” torde innebära en inskränkning jämfört med idag och ifrågasatt om inte t.ex. ett terrorhot riktat mot landet som sådant eller mot dess demokratiska styre borde kunna mötas med försvarsunderrättelseverksamhet även beträffande vissa svenska förhållanden. Justitiekanslern har framhållit att det avgörande för gränsdragningen mot polisiär verksamhet i princip borde vara om det rör sig om ett yttre hot mot landet.

Ekobrottsmyndigheten har anfört att Försvarsmakten endast bör bedriva underrättelseverksamhet som avser yttre militära hot, medan sådan underrättelseverksamhet respektive kriminalunderrättelseverksamhet som avser terrorism och annan gränsöverskridande grov brottslighet skall hanteras av polisen och övriga myndigheter inom rättsväsendet. I den senare verksamheten bör den kapacitet som finns inom försvaret på olika områden kunna tas till vara på ett effektivt sätt och inom ramen för den nyss angivna gränsdragningen. Myndigheten har efterlyst en tydligare gränsdragning.

Säkerhetspolisens och *Sveriges polisförbunds* grundläggande syn på ansvarsfördelningen mellan försvarsunderrättelseverksamhet och polisiär verksamhet har återgetts i föregående avsnitt. När det gäller promemorians författningsförslag har Säkerhetspolisen konstaterat att begreppet utländska förhållanden inte utgör någon begränsning när det gäller var verksamheten kommer att bedrivas och att verksamheten således kommer att kunna bedrivas även i Sverige. Säkerhetspolisen har vidare anfört att underrättelseverksamhet till sin natur är sådan att den bör vara förbehållen sådana företeelser eller hot som det är särskilt angeläget att samhället har information om. Säkerhetspolisen har därför påtalat viss tvekan inför den föreslagna förändringen eftersom beskrivningen av de nya hot som försvarsunderrättelseverksamheten skall riktas mot är så vag att det inte går att förutse vilka företeelser som kan komma att bli föremål för verksamhetens intresse. Säkerhetspolisen har emellertid förklarat att den föreslagna ordalydelsen i och för sig kan godtas, dock under förutsättning att det sker en klar avgränsning till verksamhet som faller under polisens brottsbekämpande och brottsförebyggande verksamhet.

Rikspolisstyrelsen har med hänvisning till de oklara gränser mellan den militära underrättelsetjänsten och den polisiära underrättelseverksamheten som förslaget skapar avstyrkt förslaget och i övrigt ställt sig bakom Säkerhetspolisens ståndpunkter.

Sveriges advokatsamfund har avstyrkt den vidgade inriktningen som försvarsunderrättelseverksamheten föreslås få och den gränsdragning som föreslås beträffande försvarsunderrättelseverksamhet och brottsbekämpande myndigheters verksamhet.

Kammarkollegiet har avstyrkt en utvidgning av Försvarsmaktens mandat inom underrättelseverksamheten och anfört att det inte är en militär uppgift att möta de icke-militära säkerhetshot som i dag gör sig starkt gällande, t.ex. från terrorism och annan grov kriminalitet, utan istället en uppgift för det civila samhället varvid huvudansvaret under regeringen ligger hos polisen. Kollegiet har framhållit att det visserligen är nödvändigt att samhällets samlade resurser används där de behövs, men att detta i det operativa arbetet med att bekämpa terrorism och annan grov brottslighet bör ske genom att polisen får tillgång till resurser som finns hos samhällets övriga organ, t.ex. inom Försvarsmakten. Om det inte görs resursöverföringar från försvarsunderrättelseverksamheten till civila strukturer har kollegiet anfört att det ändå är angeläget att lägga fast tydliga ansvarsområden och att det därvid är viktigt att ansvaret för civila uppgifter behålls inom de civila strukturerna och att polisen skall ha ansvaret för och ledningen av verksamheten medan Försvarsmaktens resurser skall ställas till polisens förfogande när polisen begär det. I vart fall bör polisen få möjlighet att lämna underrättelseuppdrag till de myndigheter som bedriver försvarsunderrättelseverksamhet. Kollegiet har vidare anfört att de oklara begreppen “i övrigt för kartläggning av yttre hot mot landet” och ”utländska förhållanden” skapar en betydande osäkerhet om gränsdragningarna.

Skälen för regeringens förslag

Försvarsunderrättelseverksamhetens uppgifter

Som framhållits i tidigare avsnitt finns det ett växande behov av att kunna förse olika delar av samhället med underrättelser om företeelser som genom utvecklingen i omvärlden kommit att på ett eller annat sätt framstå som hot mot landet. För att tillgodose sådana behov är det angeläget att på ett så effektivt sätt som möjligt utnyttja de samlade resurserna hos olika myndigheter. De förslag som regeringen lämnar syftar till att tillvarata de unika resurser som finns i försvarsunderrättelseverksamheten för att ge ett underrättelseunderlag som beträffande såväl kvantitet som kvalitet överträffar vad som är möjligt inom ramen för nuvarande reglering. Ett sätt att åstadkomma detta är att bredda mandatet för försvarsunderrättelseverksamheten till att omfatta flera typer av hot än i dag. Självklart måste härvid beaktas att försvarsunderrättelseverksamheten därigenom kommer att beröra också områden på vilka andra myndigheter har huvudansvaret, vilket till viss del är fallet redan i dag. Särskilt viktigt är det enligt regeringens uppfattning att undvika överlappningar som får negativa konsekvenser för samhället i stort genom att intressekonflikter och bristande samordning leder till ett sämre resursutnyttjande.

Vissa utgångspunkter framstår i detta sammanhang som närmast självklara. Det finns t.ex. ingen anledning att frångå den sedan länge rådande huvudprincipen att yttre militära hot skall hanteras av Försvarsmakten medan terrorism och annan gränsöverskridande brottslighet är kriminella handlingar som det ankommer på brottsbekämpande myndigheter att förebygga och bekämpa. Denna princip är emellertid alltför schematisk för att kunna tjäna som lösning på de gränsdragningsfrågor som uppkommer när det gäller att tillgodose det ökande behov av underrättelser som föranleds av den säkerhetspolitiska utvecklingen i omvärlden. Omfattningen av försvarsunderrättelseverksamhetens mandat och gränsdragningen gentemot andra verksamheter måste bedömas utifrån ett bredare perspektiv.

Frågan är då hur den eftersträvade utvidgningen av mandatet för försvarsunderrättelseverksamheten skall författningsregleras. 1 § lagen om försvarsunderrättelseverksamhet föreskriver i dag att försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Enligt regeringens mening bör stödet till de i bestämmelsen angivna politikområdena lyftas fram för att tydliggöra verksamhetens huvudsyfte. Anpassningen av försvarsunderrättelseverksamheten bör emellertid också ta sig uttryck i en ny formulering av vilka typer av hot som verksamheten skall inriktas mot. Den nuvarande lydelsen ”yttre militära hot” framstår mot bakgrund av den förändrade hotbild som beskrivits ovan som ett alltför snävt begrepp. 11 september-utredningen föreslog att uttrycket skulle bytas ut mot ”yttre väpnat hot” som en markering av att även terrorism skall omfattas. Den formuleringen täcker emellertid inte de hot av en mer oklar karaktär och ursprung som Sverige också behöver kunna möta, t.ex. kvalificerade IT-relaterade hot, oljeutsläpp samt strålnings-, biologiska och kemiska hot. På vissa av dessa områden besitter de myndigheter som bedriver försvarsunderrättelseverksamhet en betydande kompetens, som det är viktigt att kunna tillvarata. Det är därför angeläget att försvarsunderrättelseverksamheten kan nyttjas mot hela den vidgade säkerhetspolitiska hotbilden, till nytta för en bredare krets av underrättelsemottagare. För att täcka in hela det komplexa hotspektrumet, med betydande inslag av icke-militära och icke-väpnade hot, föreslår regeringen att verksamheten skall avse ”yttre hot”, oavsett deras karaktär och ursprung. Därmed omfattas hela den säkerhetspolitiska hotbilden.

Begreppet yttre hot är vidsträckt och måste också vara det för att ge utrymme för nödvändig flexibilitet och förmåga att anpassa verksamheten efter nya företeelser. Genom att verksamheten är föremål för särskild granskning i enlighet med vad som närmare redogörs för i avsnitt 8, säkerställs dock att innehållet inte utvidgas efterhand på ett sådant sätt som *Amnesty international* påtalat en risk för.

Att försvarsunderrättelseverksamheten skall inriktas på sådana hot eller företeelser av relevans för svensk utrikes, säkerhets- och försvarspolitik som har sitt ursprung utanför landets gränser är en grundläggande princip som det inte finns anledning att frångå. Regeringen finner mot den bakgrunden inte anledning att överväga en sådan ytterligare utvidgning av försvarsunderrättelseverksamhetens mandat till att även omfatta inre hot som *Banverket* föreslagit.

Genom att mandatet utvidgas från ”yttre militära hot” till ”yttre hot” kommer väsentliga delar av vad som åsyftas med den nuvarande uppgiften att ”medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred” att omfattas av den övergripande uppgiften. Som *Justitiekanslern* har påpekat är dock överensstämmelsen inte fullständig och förslaget innebär en viss begränsning i förhållande till vad som gäller i dag. Svåra påfrestningar på samhället som inte samtidigt utgör yttre hot, t.ex. naturkatastrofer i Sverige, kommer inte att omfattas. Extraordinära händelser som är att betrakta som svåra påfrestningar på samhället i fred faller emellertid inom ramen för andra myndigheters kompetensområden och försvarsunderrättelseverksamheten torde på detta område endast kunna bidra i marginell utsträckning. Beredskapen mot och förmågan att hantera sådana företeelser påverkas därför enligt regeringens bedömning inte negativt av en sådan förändring.

Eftersom verksamhetens tyngdpunkt alltjämt ligger på stöd för svensk utrikes- säkerhets- och försvarspolitik finner regeringen inte anledning, att, så som *Krisberedskapsmyndigheten* föreslagit, överväga en förändring av försvarsunderrättelseverksamhetsbegreppet.

Förhållandet till andra myndigheters verksamhet

En utvidgning av mandatet för försvarsunderrättelseverksamheten i enlighet med vad som angetts ovan innebär, som många remissinstanser påpekat, att frågan om gränsdragning mellan försvarsunderrättelseverksamhet och andra myndigheters verksamhet accentueras ytterligare, framförallt när det gäller den verksamhet som bedrivs av polisen och andra brottsbekämpande myndigheter. I praktiken har den tekniska utvecklingen och de gränsöverskridande hoten gjort att skiljelinjen mellan inre/polisiär och yttre/militär säkerhet inte är lika klar som tidigare. Polisiär verksamhet är visserligen av naturliga skäl i första hand inriktad på inhemska förhållanden, eftersom svenska myndigheter har begränsade möjligheter att utöva sina befogenheter på andra länders territorium. Detta hindrar dock inte att en ökande del av den underrättelseinformation som polisen inhämtar och analyserar avser utländska förhållanden. Internationellt samarbete har också i allt högre grad blivit en naturlig del av de brottsbekämpande myndigheternas verksamhet. Säkerhetspolisens verksamhet utgörs i allt högre utsträckning av underrättelseverksamhet.

Utvecklingen har följaktligen redan lett till att gränsen mellan de olika verksamheterna blivit svårare att definiera – i de gränsytor där de möts är konturerna inte alltid så skarpa som de varit tidigare. Det finns därför anledning att vid gränsdragningen i första hand beakta verksamheternas ändamål. Av betydelse är härvid att försvarsunderrättelseverksamheten i första hand är inriktad på att ge sådan strategisk information som regeringen och olika myndigheter behöver för planering, beslut och andra åtgärder, dvs. sådan information som gör att man tidigt kan formulera strategier och politik för att möta olika fenomen som annars kan utvecklas till någon form av kris.

Det är viktigt att betona att i den utsträckning det aktualiseras att inom ramen för försvarsunderrättelseverksamhetens utökade mandat ägna uppmärksamhet åt internationell kriminalitet, det inte är frågan huruvida en verksamhet är kriminell eller inte som står i fokus. Sådana bedöm-

ningar ankommer inte heller fortsättningsvis på de myndigheter som bedriver försvarsunderrättelseverksamhet. Inom ramen för försvarsunderrättelseverksamheten aktualiseras sådan verksamhet istället i den mån den kan bedömas ha potential att utgöra ett hot mot landet, oavsett hur den i rättslig mening skall betraktas. I vilken utsträckning ett sådant hot kan mötas med de instrument som de brottsbekämpande myndigheterna förfogar över är en bedömning som skall göras av dessa myndigheter, när de genom egen verksamhet och eventuella rapporter från försvarsunderrättelseverksamheten fått underrättelser om dessa företeelser. Samma information kan hos en annan myndighet, utanför den brottsbekämpande sektorn, läggas till grund för bedömningar av hur hotet skall hanteras i andra avseenden och med metoder som står den myndigheten till buds.

Det är angeläget att slå fast att försvarsunderrättelseverksamhet med stöd av de förslag som regeringen nu lämnar inte kommer att utgöra brottsbekämpande verksamhet, lika lite som detta är fallet i dag. Det är en annan sak att försvarsunderrättelseverksamhetens resultat kan vara värdefullt även för myndigheter med brottsbekämpande uppgifter, på samma sätt som det kan vara värdefullt för myndigheter med helt andra ansvarsområden.

Det finns ett område där gränsdragningen mellan försvarsunderrättelseverksamheten och den brottsbekämpande verksamheten måste vara helt klar; det gäller användning av tvångsmedel och annat utövande av polisiära befogenheter som riktas mot enskilda och som regleras i lag. Det råder ingen tvekan om att sådana åtgärder skall vara förbehållna polisen och andra brottsbekämpande myndigheter. Detta följer dock redan av de bestämmelser som reglerar användningen av straffprocessuella tvångsmedel och polisiära befogenheter i övrigt; av regleringen framgår att åtgärderna är exklusivt förbehålla brottsbekämpande myndigheter.

Frågan om förhållandet mellan försvarsunderrättelseverksamhet och polisiär verksamhet handlar dock inte bara om denna mer begränsade distinktion, hänförlig till verksamheternas *metoder*, utan också om i vilken utsträckning verksamheternas *uppgifter* kan komplettera varandra. Att myndigheterna i viss utsträckning ägnar sig åt att kartlägga samma företeelser är som ovan konstaterats ofrånkomligt och förekommer redan med dagens reglering; i det avseendet innebär inte regeringens förslag någon förändring.

Som framhålls i propositionen Lag om försvarsunderrättelseverksamhet (prop. 1999/2000:25) är underrättelseverksamheten av sådan art att det av naturliga skäl inte är möjligt att i lagform reglera den i detalj (a. prop. s. 12). Detta konstaterande har naturligtvis också giltighet när det gäller att dra upp gränserna för försvarsunderrättelseverksamhetens förhållande till andra myndigheters ansvarsområden. Det är följaktligen inte möjligt att, som vissa remissinstanser efterlyst, i lag uttömmande reglera respektive verksamhets gränser. Lagen om försvarsunderrättelseverksamhet drar upp den yttre ramen för verksamheten. Förhållandet att lagen inte i detalj reglerar alla de gränsdragningsfrågor som kan uppstå innebär dock på intet sätt att frågorna är olösta. Liksom tidigare skall regeringen inom ramen för lagstiftningen bestämma försvarsunderrättelseverksamhetens inriktning. De myndigheter som bedriver försvarsunderrättelseverksamhet har följaktligen inte frihet att efter eget skön avgöra i vilken

omfattning deras verksamhet får utsträckas till att även beröra andra myndigheters ansvarsområden.

I den styrning av verksamheten som regeringen utövar genom att inrikta verksamheten ligger naturligtvis också att överväga gränsdragningen i förhållande till andra myndigheter, på motsvarande sätt som regeringen i andra sammanhang reglerar frågor om relationen mellan olika myndigheter i t.ex. instruktioner och delegeringsföreskrifter. Gränsdragningsfrågorna på detta område bör följaktligen hanteras som andra myndighetsstyrningsfrågor. Utanför det område där en lagreglering är nödvändig, och som berörs i nästa avsnitt, bör det följaktligen ligga i regeringens hand att genom sin inriktning göra de avvägningar mellan myndigheternas ansvarsområden som *Åklagarmyndigheten, Kustbevakningen, Datainspektionen, Kammarrätten i Stockholm, Lunds universitet, Rikspolisstyrelsen, Säkerhetspolisen, Sveriges polisförbund* och *Kammarkollegiet* efterlyser. Regeringens inriktning kommer därigenom att få ökad betydelse som styrinstrument för försvarsunderrättelseverksamheten.

Som 11 september-utredningen har påpekat behöver en viss teoretisk överlappning av mandaten på terrorismområdet inte innebära något problem, åtminstone så länge de polisiära myndigheterna och de myndigheter som bedriver försvarsunderrättelseverksamhet håller varandra informerade om sin verksamhet. Flera remissinstanser, däribland *Åklagarmyndigheten* och *Totalförsvarets forskningsinstitut*, har också påpekat att det – mot bakgrund av att det i viss mån är oundvikligt att verksamheterna berör samma områden – är väsentligt att i den praktiska tillämpningen lösa verksamhetshämmande gränsdragningsproblem. Samverkansrådet mot terrorism, under ledning av Säkerhetspolisen, torde i detta sammanhang kunna spela en viktig roll för att främja samarbete och informationsutbyte och förhindra dubbelarbete på terrorismområdet. Ytterligare ett förhållande som bör kunna minska risken för oklarheter mellan försvarsunderrättelseverksamheten och polisiär verksamhet är att försvarsunderrättelseverksamheten enligt regeringens förslag skall fokusera på att i första hand rapportera underrättelser och inte i samma utsträckning som tidigare utföra övergripande analyser (se avsnitt 6.4).

Gränsdragningsfaktorer

Även om det varken är möjligt eller lämpligt att i lag detaljreglera försvarsunderrättelseverksamhetens gränser i förhållande till andra myndigheters ansvarsområden, skall lagen naturligtvis i så stor utsträckning som möjligt ange de väsentligaste gränsdragningsfaktorerna och begränsningarna av verksamheten.

Den föreslagna regleringen innehåller också flera restriktioner som innebär att verksamheternas ansvarsområden inte kommer att beröra varandra i sådan omfattning som några av remissinstanserna anfört. I begreppet ”yttre hot mot landet” ligger att hotet måste vara av så kvalificerad art att det kan anses riktat mot rikets säkerhet eller samhällsviktiga strukturer. Därigenom faller mycket av den internationella brottsligheten utanför ramen för försvarsunderrättelseverksamhetens uppgifter. Gränsdragningsproblematiken i förhållande till den öppna polisens verksamhet kommer följaktligen inte att vara av sådan omfattning som några remissinstanser uttryckt farhågor för.

Regeringen delar dessutom promemorians bedömning att utvidgningen av försvarsunderrättelseverksamhetens mandat till att omfatta yttre hot mot landet bör förenas med ytterligare en uttrycklig begränsning, nämligen att verksamheten endast får avse utländska förhållanden. Denna begränsning har inte kommit till tydligt uttryck i hittillsvarande lagstiftning, men har i viss mån varit underförstådd genom det sätt på vilket verksamhetens uppgifter angetts. Mot bakgrund av det vidgade mandatet bör denna restriktion nu tydliggöras.

Begränsningen till utländska förhållanden innebär att försvarsunderrättelseverksamheten typiskt sett skall inhämta, bearbeta och delge sådan information om företeelser och förhållanden i andra länder som bl.a. ger svenska beslutsfattare ett förbättrat underlag för beslut och bedömningar i utrikes-, säkerhets- och försvarspolitiska frågor eller att skydda svensk personal som deltar i internationella insatser.

Att försvarsunderrättelseverksamheten bör förbli inriktad uteslutande på utländska förhållanden, dvs. verksamheter eller företeelser som har sin utgångspunkt i utlandet, hindrar dock inte att verksamheten kan avse även vissa företeelser inom landet. Avgörande är följaktligen inte, så som *Säkerhetspolisen* helt riktigt påpekat, var den relevanta verksamheten bedrivs. Exempel på när utländska förhållanden måste anses sträcka sig innanför landets gränser är när en organisation med verksamhet som utgör ett hot mot landet har sitt ursprung i ett annat land men verkar genom representanter i Sverige eller genom att på annat sätt utnyttja resurser i Sverige. Det handlar då om att följa upp utländska förhållandens koppling till Sverige för att kunna bedöma hotbilden mot landet. I sådana situationer är det viktigt att framhålla att mandatet för de myndigheter som bedriver försvarsunderrättelseverksamhet är begränsat till just underrättelseverksamhet; alla åtgärder som syftar till att hantera de hot av kriminell karaktär som kan identifieras inom landet är förbehållna de brottsbekämpande myndigheterna, vilket också är förhållningssättet i många andra jämförbara länder.

Även om begränsningen av verksamheten till utländska förhållanden således inte innebär en sådan långtgående restriktion som *Justitiekanslern* och *Krisberedskapsmyndigheten* uttryckt farhågor för, kan det aldrig bli fråga om att de myndigheter som bedriver försvarsunderrättelseverksamhet ägnar sin uppmärksamhet åt förhållanden av rent inhemsk karaktär, oavsett om dessa ligger under de brottsbekämpande myndigheternas ansvarsområde eller är av helt annan art. Sådana förhållanden ligger i sin helhet under andra myndigheters ansvar.

6.3.2 Gränsdragning gentemot brottsbekämpande och brottsförebyggande åtgärder

Regeringens förslag: 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.

Om det inte finns hinder enligt andra bestämmelser, får dock de myndigheter som bedriver försvarsunderrättelseverksamhet lämna

stöd till andra myndigheters brottsbekämpande och brottsförebyggande verksamhet.

Promemorians förslag överensstämmer inte med regeringens förslag. I promemorian har föreslagits att försvarsunderrättelseverksamhet inte får innefatta åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete enligt lagar och förordningar. Utan hinder härav får försvarsunderrättelseverksamheten, utan att riktas mot fysisk person, bedrivas för kartläggning av utländska förhållanden som innebär yttre hot mot landet.

Remissinstanserna: De flesta remissinstanser som har yttrat sig har tillstyrkt förslaget eller lämnat det utan erinran. *Justitiekanslern* har instämt i att det med hänsyn till behovet av att anpassa försvarsunderrättelseverksamheten till de hot som numera kan uppstå mot landet är nödvändigt att verksamheten får avse också vissa åtgärder som även ligger inom ramen för polisiär verksamhet, men anfört att det klart borde sägas ifrån att försvarsunderrättelsetjänsten inte skall ägna sig åt sådana polisiära uppgifter som exempelvis går ut på att avslöja grov brottslighet som visserligen är mycket allvarlig men som inte utgör något ”hot mot landet” i egentlig mening. Annars torde det finnas en risk enligt Justitiekanslern, både att kravet på ett ”yttre hot mot landet” urholkas och att överlappningen mellan försvarsunderrättelseverksamhet och den polisiära verksamheten blir alltför omfattande.

Amnesty international har betonat att det är viktigt ur rättssäkerhetssynpunkt att en så tydlig lagstiftning som möjligt antas och att det är väsentligt att det inom ramen för försvarsunderrättelseverksamheten inte bedrivs verksamhet som inrymmer straffprocessuella tvångsmedel eller polisiära befogenheter i övrigt och att det inte heller sker inhämtning i brottsförebyggande syfte av information om inhemska förhållanden. *Stockholms tingsrätt, Ekobrottsmyndigheten* och *Totalförsvarets forskningsinstitut* har anfört att begränsningen att försvarsunderrättelseverksamhet inte får ske om verksamheten avser fysisk person bör utgå eller ges en annan utformning, eftersom det bakom all kommunikation och information ligger fysiska personer och inskränkningen därmed blir svårhanterlig i praktiken. Tingsrätten har vidare anfört att en alltför långtgående inskränkning kan undvikas om det i författningstexten anges att inskränkningen inte gäller när det är fråga om uppdrag från en brottsbekämpande myndighet. De gränsdragningsproblem mellan olika verksamheter som kan uppstå bör enligt tingsrätten i första hand lösas genom samverkan.

Säkerhetspolisen har påpekat att begreppet ”uppgifter” i den aktuella bestämmelsen ersatts med det snävare begreppet ”åtgärder” utan att innebörden av detta närmare berörts i promemorian. Likaså har ”andra föreskrifter” utan motivering ersatts med ”förordningar”. Säkerhetspolisen har ifrågasatt bestämmelsen att försvarsunderrättelseverksamhet, utan att riktas mot en fysisk person, ändå får bedrivas för att kartlägga utländska förhållanden som innebär yttre hot mot landet och anfört att det alltid finns en fysisk person bakom de uppgifter som inhämtas och att det därför är svårt att se hur de myndigheter som bedriver försvarsunderrättelseverksamhet överhuvudtaget skall kunna utföra någon verksamhet inom området, vilket skulle förhindra att försvarsunderrättelseverksamheten

ger polisen och andra brottsbekämpande myndigheter stöd i deras underrättelseverksamhet.

Även i övrigt har Säkerhetspolisen funnit innebörden av bestämmelsens andra stycke så oklar att förslaget i denna del inte utan vidare beredning kan ligga till grund för det fortsatta lagstiftningsarbetet. Säkerhetspolisen har vidare anfört att försvarsunderrättelseverksamhet – liksom idag – inte skall få innefatta åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete, medan de brottsbekämpande myndigheterna alltjämt måste ha möjlighet att få stöd av resurserna hos de myndigheter som bedriver försvarsunderrättelseverksamhet vid inhämtning av underrättelser. Säkerhetspolisen har mot denna bakgrund avstyrkt den föreslagna förändringen av 4 § lagen om försvarsunderrättelseverksamhet och istället förordat att det skall föreskrivas en rätt för polisen och andra brottsbekämpande myndigheter att få stöd av de myndigheter som bedriver försvarsunderrättelseverksamhet vid underrättelseinhämtning i det brottsbekämpande och brottsförebyggande arbetet. Enligt Säkerhetspolisen skall det då inte vara fråga om att bedriva försvarsunderrättelseverksamhet inom området utan istället underrättelseinhämtning på uppdragsbasis utifrån de rättsliga förutsättningar polisen och de andra myndigheterna har för sin verksamhet, med de rättssäkerhetsgarantier som följer av detta.

Kustbevakningen har påpekat att de överväganden som föranlett ändringarna i 4 § första stycket inte närmare redovisas, liksom när det gäller undantaget i andra stycket att försvarsunderrättelseverksamhet inte får riktas mot fysisk person. Kustbevakningen har vidare efterlyst en bestämmelse av innebörden att förvarsunderrättelsemyndigheterna skall vara skyldiga att omedelbart i första hand till Säkerhetspolisen överlämna underrättelser som faller under polisens eller andra brottsbekämpande myndigheters verksamhet, vilket torde innefatta behandling av uppgifter om fysiska personers samband med brottslig verksamhet och därför kräver särskild reglering.

Datainspektionen och *Malmö tingsrätt* har anfört att den föreslagna ändringen i 4 § lagen om försvarsunderrättelseverksamhet kan leda till gränsdragningsproblem när det gäller förhållandet mellan försvarsunderrättelseverksamhet och polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet vilket i sin tur kan leda till problem när det gäller att tillämpa de begränsningar som föreslås ifråga om signalspaning.

Sveriges advokatsamfund har, bl.a. med hänvisning till tidigare ställningstaganden, avstyrkt förslaget i denna del och anfört att det inte innebär en tillräckligt tydlig gränsdragning. En sammanblandning av försvarsunderrättelseverksamhet och polisiär verksamhet är enligt samfundets mening olycklig och kan leda till att de bestämmelser som finns rörande t.ex. förundersökning, som syftar till att tillvarata misstänktas rättigheter, åsidosätts. Detta är oroande i synnerhet mot bakgrund av förarbetsuttalanden i anslutning till nuvarande lag om att gränsdragningsbestämmelsen inte hindrar att myndigheter som sysslar med försvarsunderrättelseverksamhet, enligt regeringens bestämmande, kan lämna andra myndigheter biträde t.ex. avseende signalspaning.

Svenska polisförbundet har avstyrkt förslaget med hänvisning till att brottsbekämpning i första hand är en polisiär uppgift och att förslaget

leder till en självständig verksamhet där underrättelseinhämtning sker utifrån andra rättsliga grunder än de polisiära. Förbundet har anfört att försvarsunderrättelseverksamheten inte skall få innefatta åtgärder som ligger inom ramen för polisens brottsbekämpande och brottsförebyggande arbete.

Kammarkollegiet har anfört att den föreslagna ändringen i 4 § förstärker intrycket att försvarsunderrättelseverksamheten avses sättas in som primär resurs i det brottsbekämpande arbetet utan att polisen har ledning av och kontroll över vad som utförs och att författningstexten inte ens utesluter att försvarsunderrättelseorganen, polisen ovetandes, i Sverige bedriver underrättelseverksamhet mot vissa utländska brottsaktiva som utför brott här i landet, t.ex. smugglingsligor, spioner eller bedragare. Kollegiet har vidare påpekat att formuleringen ”enligt lagar och förordningar” i 4 § första stycket skapar en betydande osäkerhet eftersom en stor del av polisens befogenheter, arbetsmetoder eller arbetsområden inte är författningsreglerade. Enligt kollegiet öppnar förslaget för att försvarsunderrättelseverksamheten självständigt skall kunna bedrivas mot enskilda fysiska personer på alla områden inom brottsbekämpningen där det saknas uttryckliga författningsbestämmelser om att befogenheten eller uppgiften är förbehållen polisen och att verksamheten kan bedrivas utan polisens ledning eller kontroll mot grov kriminalitet i form av t.ex. organiserad smuggling, människohandel och IT-bedrägerier.

Skälen för regeringens förslag

Som flera remissinstanser har varit inne på bör försvarsunderrättelseverksamheten inte heller i fortsättningen avse uppgifter som det ankommer på de brottsbekämpande myndigheterna att lösa. Självklart är exempelvis att det, som *Amnesty International* påpekat, i försvarsunderrättelseverksamheten inte skall bedrivas verksamhet som inrymmer straffprocessuella tvångsmedel eller polisiära befogenheter i övrigt. Som framhållits i föregående avsnitt följer detta emellertid direkt av den lagstiftning som reglerar sådan verksamhet och behöver därför inte upprepas. Ett angivande av detta i lagen om försvarsunderrättelseverksamhet skulle endast innebära en erinran om vad som ändå följer av annan lag.

Inte heller inhämtning i brottsförebyggande syfte av information om inhemska förhållanden får ingå i försvarsunderrättelseverksamheten. Den begränsningen följer redan av att det enligt regeringens förslag uttryckligen anges i 1 § lagen om försvarsunderrättelseverksamhet att verksamheten endast får avse utländska förhållanden, se föregående avsnitt.

Det är vidare klart att någon brottsutredande verksamhet inte skall bedrivas av de myndigheter som ägnar sig åt försvarsunderrättelseverksamhet.

Förhållandet mellan försvarsunderrättelseverksamhet och polisiär verksamhet

I 4 § lagen om försvarsunderrättelseverksamhet regleras närmare försvarsunderrättelseverksamhetens förhållande till de brottsbekämpande och brottsförebyggande myndigheterna. Den nuvarande bestämmelsen

hindrar de myndigheter som bedriver försvarsunderrättelseverksamhet att utföra uppgifter som enligt lagar och andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsförebyggande och brottsbekämpande arbete. Denna avgränsning av försvarsunderrättelseverksamheten har hitintills inte orsakat några större svårigheter. Vid ett utvidgat mandat för försvarsunderrättelseverksamheten kan dock avgränsningen vålla problem. Det framstår exempelvis som osäkert om och i vilken utsträckning regleringen ger utrymme för att bedriva försvarsunderrättelseverksamhet avseende yttre hot i form av allvarlig brottslighet.

Terrorism är ett exempel på kriminalitet som kan utgöra yttre hot. Det ligger inom ramen för Säkerhetspolisens författningsreglerade uppgifter att leda och bedriva polisarbete beträffande denna typ av kriminalitet även om den har sin bakgrund i utländska förhållanden. Samtidigt är det som betonats tidigare väsentligt att försvarsunderrättelseverksamhetens unika kapacitet kan utnyttjas för att tillgodose flera olika intressenters behov av underrättelser om bl.a. terrorism. Det nu framlagda förslaget rörande gränsdragningen mellan polisiär verksamhet och försvarsunderrättelseverksamhet, liksom tidigare förslag på området, bygger på det grundläggande synsättet att samhällets samlade underrättelseresurser utgör en kvalificerad nationell resurs. Denna resurs bör på ett flexibelt sätt, och under adekvat kontroll, kunna användas mot alla de former av yttre hot mot landet som omfattas av den vidgade säkerhetspolitiska hotbilden. Utifrån detta synsätt bör försvarsunderrättelseverksamheten ses som en samverkande service för att tillgodose behov hos såväl regeringen som andra myndigheter.

I och med att försvarsunderrättelseverksamhetens mandat utvidgas till att omfatta en bredare hotbild kommer verksamheten så som angetts i föregående avsnitt att i högre grad än hittills beröra de brottsbekämpande myndigheternas verksamhet. Detta är emellertid i viss mån nödvändigt om försvarsunderrättelseverksamheten skall kunna fylla den angivna funktionen att utgöra en resurs för hela samhällets behov av underrättelser. Mot den bakgrunden måste bestämmelsen i 4 § anpassas så att kartläggning av terrorism och annan internationell brottslighet av sådan kvalificerad art att den kan anses utgöra yttre hot mot landet inte utesluts från tillämpningsområdet för försvarsunderrättelseverksamheten. Det är dock samtidigt viktigt att framhålla att det även i fortsättningen är polisen som har ansvaret för att leda och bedriva bekämpningen av sådan kriminalitet. Vad de myndigheter som ägnar sig åt försvarsunderrättelseverksamhet i fortsättningen kan göra är att bidra med underrättelser. Inhämtningen av sådana underrättelser får förstås inte ske på ett sådant sätt att polisens eller andra brottsbekämpande myndigheters arbete i landet störs eller motverkas. Det fordrar en samverkan som det får ankomma på regeringen att ge närmare föreskrifter om.

Författningsreglering av gränsdragningen

I förarbetena till nuvarande 4 § konstateras i huvudsak två saker – dels att i försvarsunderrättelseverksamheten inte får utövas verksamhet som inrymmer polisiära befogenheter såsom förundersökningsåtgärder enligt rättegångsbalken och tvångsmedelanvändning enligt bl.a. polislagen, dels att bestämmelsen inte syftar till att utgöra något hinder mot att myndig-

heter som sysslar med försvarsunderrättelseverksamhet skall, enligt regeringens bestämmande, kunna lämna andra myndigheter biträde inom ramen för sådan myndighetsutövning som den senare myndigheten har att svara för. Vidare konstateras att myndigheter som ägnar sig åt försvarsunderrättelseverksamhet skall, i enlighet med regeringens bestämmande, kunna syssla med uppdragsverksamhet för annan myndighets räkning (prop. 1999:2000:25 s. 17 f).

För såväl de myndigheter som bedriver försvarsunderrättelseverksamhet som de myndigheter som har brottsbekämpande uppgifter är det väsentligt att den begränsning som behövs mellan verksamheterna i första hand tar sikte på sådana specifika *metoder eller åtgärder* som ligger inom ramen för de senares verksamhet i landet. En helt annan sak är i vilken utsträckning samma företeelser får omfattas av verksamheten. Som vi framhållit är det snarast en fördel att flera myndigheter – med de skilda metoder som står dem till buds – riktar sin uppmärksamhet mot samma företeelser och därigenom bidrar till ett fullständigare och mer mångfacetterat underrättelseunderlag. Det måste dock säkerställas att en sådan ordning inte leder till ett ineffektivt resursutnyttjande genom uppbyggnad av parallellkompetens eller att verksamheterna kan störa varandra. Det är för att undvika sådana effekter som en reglering av gränsdragningen föreslås. Av det anförda följer att det i första hand är den del av försvarsunderrättelseverksamheten som består i inhämtning som berörs av gränsdragningsbehovet.

Enligt regeringens uppfattning bör en begränsningsregel, för att uppnå det ovan angivna syftet, omfatta vidtagande av *åtgärder* som syftar till att lösa sådana uppgifter som enligt lagar och andra föreskrifter ligger inom ramen för de brottsbekämpande myndigheternas verksamhet. Med sådana åtgärder avses handlande som tar sig mer konkreta uttryck än inhämtning från redan tillgängliga källor. Försvarsunderrättelseverksamhet som består i att genom tekniska metoder inhämta kommunikation kan inte anses utgöra en sådan konkret åtgärd. Sådan verksamhet bedrivs inte på sådant sätt att den kan störa andra myndigheters verksamhet, och den syftar inte heller till att lösa en föreskriven uppgift för brottsbekämpande och brottsförebyggande verksamhet. Bestämmelsen är följaktligen inte avsedd att utgöra några hinder för t.ex. signalspaning även avseende sådana förhållanden som är av relevans för det brottsbekämpande arbetet. Inte heller omfattas sådana åtgärder inom försvarsunderrättelseverksamheten som i och för sig tar sig mer konkreta uttryck men som har andra syften – t.ex. stöd för svensk utrikes-, säkerhets- och försvarspolitik – än att lösa uppgifter av brottsbekämpande eller brottsförebyggande karaktär. Exempel på uppgifter som ligger inom ramen för den senare verksamheten är bedrivande av brottsutredningar och säkerhetstjänstverksamhet såsom författningsskydd och kontraspionage. På de områden där särskilda uppgifter föreskrivs för den brottsbekämpande och brottsförebyggande verksamheten omgärdas försvarsunderrättelseverksamheten följaktligen av ytterligare begränsningar utöver vad som följer av utformningen av det generella mandatet. Regeringen menar att en på detta sätt formulerad gränsdragning på ett ändamålsenligt sätt tillgodoser behovet av att tydliggöra den gränsdragning som *Datainspektionen* och *Malmö tingsrätt* efterlyst.

Som framgår av föregående avsnitt ankommer det på regeringen att genom sin inriktning av försvarsunderrättelseverksamheten ange de närmare gränsdragningar som är nödvändiga utöver lagregleringen. I den praktiska tillämpningen kommer det naturligtvis också att vara nödvändigt med en omfattande samverkan mellan myndigheterna inom respektive verksamhet.

Skall de myndigheter som bedriver försvarsunderrättelseverksamhet därutöver också stödja de brottsbekämpande myndigheternas verksamhet?

Bl.a. *Säkerhetspolisen* och *Kammarkollegiet* har förespråkat att de myndigheter som bedriver försvarsunderrättelseverksamhet också skall kunna inhämta underrättelser för de brottsbekämpande myndigheternas behov. Regeringen anser det vara angeläget att de resurser för underrättelseinhämtning som Sverige förfogar över kan användas för hela samhällets behov. Principiellt bör därför de inhämtningsresurser som finns inom försvarsunderrättelseverksamheten också kunna användas för att stödja polisens och andra brottsbekämpande myndigheters verksamhet, om det inte finns hinder för det enligt andra föreskrifter. Sådana hinder kan t.ex. vara lagbestämmelser om tvångsmedelsanvändning, så som rättegångsbalkens regler om hemliga tvångsmedel inom ramen för en förundersökning, och om att vissa arbetsmetoder är förbehållna polisman. Det skall således inte finnas någon möjlighet att kringgå de lagbestämmelser som ställts upp till skydd för den personliga integriteten vid brottsbekämpande arbete genom att begära stöd av myndigheter inom försvarsunderrättelseverksamheten. Frågan är då hur en sådan lagreglering till stöd till de brottsbekämpande myndigheterna närmare bör utformas.

I den utsträckning det är möjligt bör behoven hos de brottsbekämpande myndigheterna tillgodoses inom ramen för försvarsunderrättelseverksamheten. Regeringen menar att den förändring av mandatet för verksamheten som behandlats ovan innebär att de brottsförebyggande och brottsbekämpande myndigheterna i allt väsentligt kommer att kunna få tillgång till de underrättelser om yttre hot mot landet som behövs i deras verksamhet.

För att tillgodose det av *Stockholms tingsrätt* betonade behov som andra myndigheter har av att kunna påverka verksamhetens inriktning föreslås att berörda myndigheter skall få möjlighet att inrikta försvarsunderrättelseverksamheten inom den ram som anges i lag och i regeringens inriktning, se vidare avsnitt 6.4. De brottsbekämpande myndigheterna kommer följaktligen också att få möjlighet att i viss mån styra verksamheten mot de egna behoven.

Även om andra myndigheters behov i hög grad tillgodoses inom ramen för den breddade försvarsunderrättelseverksamheten bör det dock även fortsättningsvis finnas visst utrymme för att utnyttja resurserna hos de myndigheter som bedriver försvarsunderrättelseverksamhet, framförallt den tekniska utrustningen och kompetensen, för stöd till andra myndigheter vid sidan av försvarsunderrättelseverksamheten. Regeringen har i förarbetena till lagen om försvarsunderrättelseverksamhet uttalat att sådant stöd skall kunna lämnas enligt regeringens bestämmande till stöd för verksamhet som bedrivs av annan myndighet, inom ramen för sådan

myndighetsutövning som den senare myndigheten har att svara för (prop. 1999/2000:25 s. 17).

Regeringen har i förordningen (1994:714) med instruktion för Försvarets radioanstalt meddelat bestämmelser om visst sådant stöd. Därutöver har de myndigheter som bedriver försvarsunderrättelseverksamhet samma generella skyldighet att inom ramen för den egna verksamheten hjälpa andra myndigheter som enligt 6 § förvaltningslagen (1986:223) åvilar alla myndigheter. De förslag som regeringen nu lämnar innebär ingen förändring i dessa avseenden. När det gäller de brottsbekämpande och brottsförebyggande myndigheterna kan dock den ovan behandlade gränsdragningsbestämmelsen komma att uppfattas som att möjligheten till sådant stöd skulle vara begränsad, jämfört med vad som gäller i förhållande till andra myndigheter. Det finns därför skäl att klargöra att de myndigheter som bedriver försvarsunderrättelseverksamhet även gentemot de brottsbekämpande och brottsförebyggande myndigheterna får lämna sådant stöd.

Förutsättningarna för stöd till annan myndighet avgörs av vad som gäller för verksamheten hos den myndighet som mottar stödet. Det handlar följaktligen om att inom ramen för en sådan myndighets verksamhet biträda med åtgärder som den mottagande myndigheten i och för sig kunnat vidta på egen hand, men har otillräckliga resurser för. I syfte att klarlägga detta bör i lagen anges att en förutsättning för stöd är att det inte finns hinder enligt andra bestämmelser. Därigenom tydliggörs också att i den utsträckning det finns bestämmelser som närmare reglerar förutsättningarna för t.ex. Försvarsmakten att lämna stöd i vissa avseenden gäller dessa bestämmelser. Som regeringen framhöll i det ovan refererade förarbetsuttalandet till nuvarande lagstiftning skall stödet kunna lämnas i den utsträckning regeringen bestämmer.

Exempel på sådan verksamhet som kan komma i fråga är biträde med kryptoforcering, tekniskt stöd på informationssäkerhetsområdet och stöd i andra situationer då det är särskilt angeläget att resurserna hos de myndigheter som bedriver försvarsunderrättelseverksamhet kan användas för samhällsviktiga ändamål.

Behovet av ytterligare reglering av gränsdragningen

När det gäller det i promemorian föreslagna andra stycket i 4 § lagen om försvarsunderrättelseverksamhet har flera remissinstanser haft invändningar mot dess utformning. I och med att regeringen föreslår en annan utformning av den del av bestämmelsen som motsvarar förslagets första stycke ändras också förutsättningarna för behovet av ett sådant undantag som föreslagits i promemorian. Regeringens förslag innebär att det av 4 § tydligare framgår vilket område som är förbehållet de brottsbekämpande myndigheterna, medan gränsdragningsfrågor i övrigt får behandlas inom ramen för regeringens inriktning av försvarsunderrättelseverksamheten. Att uttryckligen ange att verksamheten får bedrivas för kartläggning av utländska förhållanden som innebär yttre hot mot landet framstår därvid som överflödigt, eftersom inriktningen mot yttre hot och begränsningen till utländska förhållanden redan framgår av förslaget till 1 §, se föregående avsnitt.

Beträffande försvarsunderrättelseverksamhetens befattning med underrättelser om enskilda personer är det som *Stockholms tingsrätt*, *Totalförsvarets forskningsinstitut, Ekobrottsmyndigheten* och *Säkerhetspolisen* framhållit ett faktum att sådana kommunikationer som är av intresse i försvarsunderrättelseverksamheten i regel utväxlas mellan enskilda och därmed ofrånkomligt att verksamheten ibland måste omfatta enskildas förehavanden. En särskild reglering i denna del bör därför, för att inte få ett alltför vidsträckt och därigenom verksamhetshämmande tillämpningsområde, förbehållas den lagstiftning som omfattar sådana metoder för underrättelseinhämtning som aktualiserar ett särskilt skydd för enskilda, d.v.s. signalspaning. Försvarsunderrättelseverksamhet är i övrigt en mångfacetterad verksamhet där en mängd olika metoder utnyttjas, varav huvuddelen inte är av sådan karaktär att några särskilda regler i förhållande till enskilda är nödvändiga. Mot denna bakgrund finns inte heller anledning att i anslutning till 4 § föreslå en sådan reglering.

När det gäller de synpunkter som *Justitiekanslern* och *Kammarkollegiet* lämnat angående karaktären av den brottslighet mot vilken försvarsunderrättelseverksamhetens resurser kan användas hänvisas till vad som i föregående avsnitt anges om den begränsning som ligger i att verksamheten skall avse yttre hot mot landet.

6.4 Ytterligare anpassningar av försvarsunderrättelseverksamheten

Regeringens förslag: I lagen om försvarsunderrättelseverksamhet skall det framgå att en närmare inriktning av verksamheten får anges av de myndigheter som regeringen bestämmer.

Verksamheten skall bedrivas av den eller de myndigheter som regeringen bestämmer.

Underrättelser skall rapporteras till berörda myndigheter.

I försvarsunderrättelseverksamheten får användas teknisk och personbaserad inhämtning som sker med särskilda metoder.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: *Stockholms tin*gsrätt har anfört att det inte framgår vad som närmare gäller för bl.a. den personbaserade inhämtning som görs av KSI. Detta kan ses som en brist om syftet med lagregleringen är att understryka att verksamheten måste bedrivas på ett sätt som är förenligt med demokratins och rättssamhällets grundprinciper. Enligt tingsrätten säger det sig dock självt att det är fråga om ett på många sätt känsligt område som inte lämpar sig särskilt väl för detaljerad lagreglering och tingsrätten nöjer sig därför med att konstatera detta och att det i grundlag (se SOU 1999:37 s. 204) inte har uppställts några formella krav på lagreglering av underrättelseverksamhet. *Malmö tingsrätt* har påpekat behovet av en sekretessbrytande bestämmelse som möjliggör rapportering av underrättelser till andra myndigheter och ifrågasatt om förslaget tillgodoser detta behov.

Säkerhetspolisen, Försvarsmakten och *Lunds universitet* har ifrågasatt den definition av begreppet ”underrättelser” som används i promemorian och pekat på att den skiljer sig från vedertagen begreppsbildning, enligt

vilken formuleringen innefattar värderad och analyserad information från samtliga – även öppna – underrättelsekällor, samt att utvecklingen snarare kräver förbättrad förmåga till övergripande analyser. Säkerhetspolisen har framhållit att utvecklingen i flera viktiga länder och inom EU går i riktning mot mer analys och ökad integration av öppen information i produktionen av underrättelseunderlag och att det är just det analytiska djupet i svenska bidrag som är mest uppskattat i underrättelsesamarbetet inom EU.

Säkerhetspolisen har vidare anfört att även om myndigheten besitter egen analyskapacitet sätts stort värde på kvalificerade analytiska bidrag från de myndigheter som bedriver försvarsunderrättelseverksamhet. Säkerhetspolisen har sammanfattningsvis anfört att den föreslagna lydelsen i 2 § lagen om försvarsunderrättelseverksamhet inte utan vidare bearbetning bör ligga till grund för en ändrad inriktning av underrättelsemyndigheternas rapportering. Försvarsmakten har framfört att även om underrättelsespecifik information kan delges underrättelsekonsument då så påkallas, t.ex. om informationen är tidskritisk, är detta förfarande riskfyllt och bör inte utgöra normalfallet. Försvarsmakten har därför förespråkat att utgångspunkten bör vara att regeringen och myndigheterna mottar värderade och analyserade underrättelser, men att de efter särskild inriktning även skall kunna delges underrättelsespecifik, dvs. obearbetad, information.

Kammarkollegiet har beträffande underrättelsernas förädlingsgrad också framhållit att för underrättelseverksamheten viktiga källor kan komma att avslöjas eller spridas till en större krets om förslaget genomförs, vilket kan göra det svårare för underrättelseorganen att få och behålla källor. *Krisberedskapsmyndigheten* har å andra sidan anfört att regleringen inte bör begränsas till rapportering av underrättelser utan att det också – beroende på tidsaspekten och karaktären av andra myndigheters inriktning av försvarsunderrättelseverksamheten – kan finnas behov av rapportering av endast insamlad och bearbetad information, varvid den inriktande myndigheten ansvarar för analys av informationen.

Tullverket och *Sveriges Riksbank* har anfört synpunkter på vilka myndigheter som skall inrikta försvarsunderrättelseverksamheten respektive motta underrättelserapporter. *Vattenfall AB* har betonat vikten av att det på ett tydligt sätt framgår hur och på vilket sätt informationen får spridas vidare till ansvariga aktörer, t.ex. inom näringslivet, för verksamheter och infrastruktur av betydelse för rikets säkerhet. *Svenskt Näringsliv* och *Svenska bankföreningen* har påtalat vikten av att verksamheten styrs av hotbildsanalyser som också omfattar näringslivets skyddsbehov och att resultatet av verksamheten också skall delges näringslivet när vitala samhällsintressen berörs.

Skälen för regeringens förslag

Inriktning av försvarsunderrättelseverksamhet

I 1 § lagen om försvarsunderrättelseverksamhet anges att regeringen skall bestämma försvarsunderrättelseverksamhetens inriktning. Utgångspunkten är således att regeringen skall inrikta och styra försvarsunderrättelseverksamheten. Regeringens inriktning skall avse de samlade behoven av

underrättelser och följaktligen innefatta såväl regeringens egna behov som behoven hos berörda myndigheter. I detta ligger också att det ankommer på regeringen att göra nödvändiga prioriteringar mellan behoven. Även om regeringen bestämmer inriktningen krävs emellertid att de uppdragsgivande myndigheterna ges möjlighet att, inom den ram som regeringen fastställt, närmare inrikta verksamheten mot en företeelse eller ett förhållande som är relevant med avseende på de ändamål för vilka försvarsunderrättelseverksamheten får bedrivas. I lagen bör därför införas en bestämmelse av denna innebörd. Regeringen skall bestämma vilka myndigheter som skall ges denna möjlighet. Det saknas anledning att i lag reglera på vilket sätt – i förordning eller genom beslut – regeringens ställningstagande skall komma till uttryck.

Endast statliga myndigheter kan komma ifråga för att närmare inrikta försvarsunderrättelseverksamheten. Regeringen anser i likhet med *Svenskt Näringsliv* och *Svenska bankföreningen* att det är naturligt att försvarsunderrättelseverksamhetens roll som nationell resurs också innefattar att beakta de intressen som näringslivet har av relevant information om omvärldsförhållanden som påverkar näringslivets förutsättningar. Det är dock i första hand ett ansvar för de myndigheter som har möjlighet att inrikta verksamheten och är mottagare av underrättelser att på lämpligt sätt tillgodose näringslivets intressen. Det är däremot inte aktuellt att införa en möjlighet för andra intressenter än statliga myndigheter att inrikta verksamheten eller ta del av underrättelserapporteringen direkt från de myndigheter som bedriver försvarsunderrättelseverksamhet.

En myndighets inriktning skall utgöra en behovsframställning. Det är den myndighet till vilken inriktningen lämnas som avgör vilka medel och metoder som skall utnyttjas för att tillgodose behovet.

Vilka skall bedriva försvarsunderrättelseverksamhet?

Försvarsunderrättelseverksamhet skall enligt 1 § tredje stycket lagen om försvarsunderrättelseverksamhet bedrivas av Försvarsmakten och de andra myndigheter som regeringen bestämmer. Av förordningen (2000:131) om försvarsunderrättelseverksamhet framgår att sådan verksamhet bedrivs, förutom av Försvarsmakten, även av Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut.

Vanligen namnges den eller de myndigheter som skall bedriva en viss verksamhet i en förordning. En författningsteknisk förändring föreslås därför, vilken innebär att Försvarsmakten inte längre uttryckligen anges i lagen om försvarsunderrättelseverksamhet som en myndighet som bedriver försvarsunderrättelseverksamhet. I lagen bör i stället införas en bestämmelse om att det är regeringen som beslutar om vilka myndigheter som skall bedriva sådan verksamhet. Dessa myndigheter bör vara desamma som nu, nämligen Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut.

Rapportering av underrättelser

I 2 § lagen om försvarsunderrättelseverksamhet anges att försvarsunderrättelseverksamheten skall fullgöras genom inhämtning, bearbetning och

analys av information. Analyser av hotbilder och bedömningar i underrättelsefrågor skall rapporteras till regeringen, via Regeringskansliet, och till andra berörda myndigheter.

Försvarsunderrättelseverksamheten bör i första hand vara inriktad på att inhämta, bearbeta och genomföra grundanalys av information. Det som kommer ut ur denna process är underrättelser. Detta innebär t.ex. att rent råmaterial, såsom en radarsignal, utan att ha genomgått den resterande delen av processen inte är en underrättelse.

Vad som skall rapporteras från försvarsunderrättelseverksamheten har koppling till diskussionen i föregående avsnitt angående gränsdragningen mellan försvarsunderrättelseverksamheten och andra myndigheters verksamhet. Det breddade mandatet för verksamheten innebär att de myndigheter som bedriver försvarsunderrättelseverksamhet kommer att hantera information om en mängd olika företeelser, varav vissa utgör mer eller mindre nya inslag i verksamheten.

Den kompetens som myndigheterna besitter kommer inte i alla sammanhang att vara fullt anpassad för att utföra fullständiga analyser av dessa nya företeelser. Det är inte regeringens avsikt att det inom myndigheterna skall byggas upp en fullständig analyskapacitet för att i alla avseenden kunna värdera den nya information som det breddade mandatet omfattar, också i den utsträckning informationen primärt är av intresse främst för annan verksamhet. En sådan långtgående överlappning av myndigheternas verksamheter är inte önskvärd, bl.a. därför att uppbyggnad av parallella analyskompetenser innebär ett dåligt utnyttjande av de samlade resurserna. I sådana situationer bör därför tyngdpunkten i det fördjupade analysarbetet ligga på den närmast berörda myndighet som är mottagare av underrättelserna.

För att tydliggöra att det följaktligen inte i första hand är den färdiganalyserade bedömningen som skall rapporteras bör föreskriften om att analyser av hotbilder och bedömningar i underrättelsefrågor skall rapporteras till Regeringskansliet och andra berörda myndigheter utgå. I stället bör den information som har framkommit rapporteras i form av underrättelser. Den slutliga och samlade analysen bör följaktligen göras hos ansvariga myndigheter, där den kan anpassas efter myndigheternas specifika behov. Underrättelser som omfattas av den aktuella lagen bör i detta sammanhang ses som ett komplement till annan tillgänglig information. Detta innebär också att samma underrättelser kan ligga till grund för analyser i olika typer av verksamhet.

Försvarsmakten och *Säkerhetspolisen* har påpekat att det i underrättelsesammanhang vedertagna är att definiera begreppet "underrättelser" (*finished intelligence*) som bearbetad, dvs. värderad och analyserad information från samtliga tillgängliga källor, medan begreppet "underrättelsespecifik information" (*raw intelligence*) avser information från enskild källa som efter urval och preliminär värdering utgör underlag för bearbetning. Utöver vad som angetts ovan om att rapporteringen inte i första hand skall avse den färdiganalyserade bilden finner regeringen dock inte anledning att närmare precisera begreppets innebörd i nu aktuellt sammanhang. I vilken utsträckning de rapporterade underrättelserna t.ex. skall innefatta information från olika källor måste överlåtas till de myndigheter som bedriver försvarsunderrättelseverksamhet att bedöma med utgångspunkt från bl.a. källornas karaktär, vad informationen avser,

mottagarens behov och egna analyskapacitet samt med beaktande av regeringens och berörda myndigheters inriktning.

Genom att graden av analys i viss utsträckning kan anpassas efter mottagarens behov finns också utrymme för att i någon mån tillgodose de synpunkter som *Krisberedskapsmyndigheten* anfört om att bl.a. tidsaspekten kan nödvändiggöra rapportering av endast inhämtad och bearbetad information. Enligt regeringens bedömning bör emellertid alltid i vart fall en sådan analys göras att informationen kan sättas in i sitt rätta sammanhang. När det gäller *Kammarkollegiets* synpunkter i denna del kan konstateras att det är självklart att underrättelserapporteringen utformas på ett sådant sätt att inte någon enskild källa röjs.

Det finns naturligtvis inget som hindrar t.ex. Försvarsmakten eller Totalförsvarets forskningsinstitut från att producera mer aggregerade analyser eller hotbildsbedömningar inom ramen för sina egna ansvarsområden. Hur resultaten av denna verksamhet skall rapporteras behöver inte lagregleras.

Underrättelserapporteringen omfattas självfallet av den kontroll av verksamheten som skall genomföras (se vidare avsnitt 8).

I försvarsunderrättelseverksamheten gäller ofta sekretess för de uppgifter som förekommer i verksamheten. Uppgifterna omfattas i många fall av reglerna om så kallad utrikes- och/eller försvarssekretess i 2 kap. 1 och 2 §§ sekretesslagen (1980:100). Enligt 2 kap. 1 § sekretesslagen gäller sekretess för uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Enligt 2 kap. 2 § gäller sekretess för uppgift som angår verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Utrikes- och försvarssekretessen gäller oavsett i vilken verksamhet eller hos vilken myndighet uppgiften förekommer.

Enligt 14 kap. 1 § sekretesslagen hindrar sekretess inte att en uppgift lämnas till annan myndighet om uppgiftsskyldighet följer av lag eller förordning, dvs. om det i sådan författning återfinns en bestämmelse med sekretessbrytande verkan. En sådan bestämmelse kan t.ex. föreskriva en skyldighet för en viss myndighet att lämna andra myndigheter information. Uppgifter kan också lämnas ut med stöd av 14 kap. 3 § samma lag. Av den bestämmelsen framgår att uppgifter får lämnas till annan myndighet om det är uppenbart att intresset av att uppgifterna lämnas har företräde framför det intresse som sekretessen skall skydda. Förslaget till ändring av 2 § lagen om försvarsunderrättelseverksamhet innebär ingen förändring av möjligheten för de myndigheter som bedriver försvarsunderrättelseverksamhet att utlämna uppgifter i förhållande till nuvarande ordning, vilken inte föranlett några tillämpningsproblem. Det finns därför inget behov av en sådan förändring som *Malmö tingsrätt* föreslagit.

Regeringen finner heller ingen anledning att frångå nuvarande ordning genom att, som *Tullverket* föreslagit, författningsreglera vilka myndigheter som skall vara mottagare av underrättelser. Den fråga som *Vattenfall AB* berört i sitt remissvar, hur och på vilket sätt informationen får spridas

vidare till ansvariga aktörer, t.ex. inom näringslivet, kan inte regleras i den föreslagna lagen. Den bedömningen måste göras av respektive sektorsansvarig myndighet inom ramen för bl.a. sekretesslagstiftningen.

Inhämtning med särskilda metoder

En mycket väsentlig del av försvarsunderrättelseverksamheten utgörs av teknisk och personbaserad inhämtning med särskilda metoder. Sådana inhämtningsmetoder används endast av Försvarsmakten och Försvarets radioanstalt. Vid Försvarsmakten finns den militära underrättelse- och säkerhetstjänsten (MUST) med Kontoret för särskild inhämtning (KSI), som har till uppgift att bedriva personbaserad inhämtning. Försvarets radioanstalt bedriver teknisk inhämtning genom signalspaning.

Dessa metoder är inte närmare preciserade annat än att det i 2 § lagen om försvarsunderrättelseverksamhet anges att verksamheten fullgörs bl.a. genom inhämtning. Av samma skäl som i avsnitt 6.2 har angetts för att i lag reglera försvarsunderrättelseverksamheten, nämligen att slå fast de huvudsakliga uppgifterna och arbetsformerna, bör i lag anges vilka särskilda verktyg som får användas för att bedriva verksamheten, de särskilda inhämtningsmetoderna. I lagen bör därför framgå att det i försvarsunderrättelseverksamheten får användas teknisk och personbaserad inhämtning som sker med särskilda metoder. Härigenom ges dock inte de myndigheter som bedriver försvarsunderrättelseverksamhet med sådana metoder några tvångsmedelsliknande befogenheter gentemot enskilda.

Begreppet särskilda metoder är väl etablerat i underrättelsesammanhang och förekommer i förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd och förordningen (2000:131) om försvarsunderrättelseverksamhet. Med avseende på personbaserad inhämtning återfinns begreppet också i 2 § tredje punkten lagen (2006:939) om kvalificerade skyddsidentiteter och behandlas i anslutning till den bestämmelsen i prop. 2005/06:149 s. 28.

Ytterligare förslag beträffande regleringen av teknisk inhämtning genom signalspaning redogörs för i avsnitt 7. Som *Stockholms tingsrätt* har påpekat är det med hänsyn till verksamhetens karaktär inte möjligt att i detalj reglera den personbaserade inhämtningen. Denna berör heller inte – till skillnad från signalspaning – skyddet för enskildas fri- och rättigheter på sådant sätt att en närmare reglering är nödvändig.

7 Signalspaning

7.1 Nuvarande begränsningar och framtida behov

7.1.1 Teknikutvecklingen

Huvuddelen av det inhämtade råmaterialet för underrättelseproduktion kommer från signalspaning. Den nuvarande verksamheten hos Försvarets radioanstalt bygger dock på 1990-talets teknik och regelverk, då överföring av stora mängder kommunikation över längre avstånd oftast skedde

helt eller delvis trådlöst, dvs. i ”etern”. FRA får idag endast spana mot trådlös kommunikation, t.ex. radio- och satellitkommunikation.

I dag sker dock en helt dominerande, och växande, del av den elektroniska kommunikationen via tråd eller kabel. Signalspaningens möjligheter att inhämta relevanta underrättelser har därför radikalt reducerats, vilket har minskat den tillgängliga mängden underrättelser. Detta kan på sikt medföra allvarliga men för underrättelseproduktionen till stöd för Sveriges utrikes-, säkerhets- och försvarspolitik. För att bevara och stärka underrättelseverksamheten är det nödvändigt att ge signalspaningen tillgång till såväl eter- som trådburen kommunikation. Andra jämförbara länders underrättelsetjänster har redan denna möjlighet eller håller på att få den (se vidare avsnitt 7.1.2). Detta kräver dock förstärkningar av det regelverk som syftar till att skydda den personliga integriteten.

Såväl de olika kommunikationssystemens komplexitet som volymen av elektronisk kommunikation ökar mycket snabbt. Även skyddet av systemen blir allt mer avancerat, vilket bl.a. ställer stora tekniska krav på forcering i samband med signalspaning. Försvarets radioanstalt måste därför fortlöpande utveckla ny teknik och metodik.

Det globala nätet

Trådlös överföring sker på marken genom radiolänkar samt över längre avstånd via kortvåg och kommunikationssatelliter. Trådbunden överföring sker via kablar, t.ex. fiberoptiska nät. De olika kommunikationsvägarna är i huvudsak civila och numera sammankopplade och nyttjade gemensamt i det så kallade globala nätet. Det globala nätet kan ses som helheten av all tekniköverförd kommunikation, oavsett om den går via Internet, i radio eller telenät och oberoende av vilket medium som används, t.ex. kablar, länkar eller radiovågor (se SOU 2004:32 s. 28).

Valet av väg och medium (radiolänk, satellit eller tråd/kabel) för kommunikationen styrs av de operatörer – statliga eller privata kommunikationsföretag – som tillhandahåller kommunikationskapacitet inom det globala nätet. Valet av kommunikationsväg är i princip helt automatiskt, och den som använder nätet kan inte bestämma vilken väg eller vilken kombination av medier som skall användas vid ett visst kommunikationstillfälle. Det är inte heller säkert att den geografiskt sett kortaste vägen för överföring används. Valet sker helt utifrån företagsekonomiska bedömningar med hänsyn till pris och kommunikationskapacitet.

Det globala nätet förmedlar all sorts kommunikation och utnyttjas av alla typer av användare, offentliga organ, företag och enskilda. Operatörerna använder hela nätets kapacitet för att förmedla telefonsamtal, telefax, datasändningar m.m. Internetföretag använder nätet för att företagens kunder skall få tillgång till hemsidor, ta fram texter och bilder, göra mjukvaruuppdateringar etc. Internationella företag hyr kapacitet på nätet för att knyta samman huvudkontor och lokalkontor i interna nät. Genom nätet ansluter banker, affärsföretag och bankomater till sina centrala datorer för att göra det möjligt att handla med kreditkort och göra bankuttag. Även myndigheter använder det globala nätet i växande utsträckning.

Volymen av den kommunikation som överförs via det globala nätet ökar ständigt och har redan i dag enorma proportioner. Enbart antalet

telefonisamtal som på en och samma gång förmedlas via nätet kan uppskattas till flera tiotals miljoner. Den absolut största delen av kommunikationen sker naturligtvis för syften som helt saknar intresse ur ett försvarsunderrättelseperspektiv. Nätet används dock även för syften som i allra högsta grad är av intresse för svensk utrikes-, säkerhets- och försvarspolitik, och för sådan verksamhet som kan utgöra yttre hot mot landet.

En effektiv signalspaning som kan hantera den enorma informationsmängden och identifiera kommunikation av intresse ur underrättelsesynpunkt bygger på att stora trafikvolymer kan spanas av för att få en bild av det normala trafikflödet. Dessutom krävs en mycket selektiv sökprocess för att skilja ut den mycket begränsade trafik som är av intresse i underrättelsearbetet.

IT-relaterade hot

Det är angeläget att de unika inhämtningsmetoder och det avancerade tekniska kunnande som finns inom de myndigheter som bedriver försvarsunderrättelseverksamhet också kan utnyttjas för att möta de IT-relaterade yttre hoten mot den svenska tekniska infrastrukturen, inte minst tele- och datasystemen.

Det svenska informationssamhället utsätts för ett ständigt växande antal attacker och en ständig övervakning av såväl främmande stater som icke-statliga aktörer. Även om mörkertalet sannolikt är stort, ökar stadigt antalet rapporter om såväl spridning av datorvirus som andra och avsevärt mera kvalificerade hot i form av t.ex. olika typer av gränsöverskridande kriminell verksamhet eller stater som olovligen tillskansar sig information via de globala informationsnätverken.

Säkerhetspolisen konstaterade i sin verksamhetsberättelse för 2003 att den under året har ”uppmärksammat att ett stort antal aktörer fortsätter visa ökat intresse och förmåga att genomföra olika typer av IT-relaterade angrepp. De flesta aktörer använder oftast IT som arbetsredskap för t.ex. kommunikation, koordinering, informationsinhämtning, informationsspridning, intrång och informationsstöld.”

Post- och telestyrelsen framför i sin delrapport Strategi för ett säkrare Internet (PTS-ER-2004:37) att ett av de största hoten mot Internet idag är bristande säkerhet i användarnas miljöer, vilket leder till att deras datorer kapas och används som plattformar för attacker mot t.ex. kritiska delar av Internets infrastruktur.

En lång rad andra studier och rapporter från Krisberedskapsmyndigheten, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Informationssäkerhetsutredningen (SOU 2004:32) m.fl. visar hur sårbara vi är för angrepp från kvalificerade aktörer, t.ex. främmande länders underrättelsetjänster. Det kan t.ex. handla om företagsspionage eller andra typer av intrång i slutna nätverk för att tillskansa sig sekretessbelagd information. Mot denna typ av verksamhet har operatörer och andra många gånger svårt att värja sig, även om det är deras egna system som nyttjas. Dessa studier förstärker argumenteringen från t.ex. Informationssäkerhetsutredningen för att staten måste påta sig ett ytterligare ansvar på detta område, framförallt för att möta de IT-relaterade hot som är så allvarliga att de kan betecknas som yttre hot mot rikets säkerhet.

Det viktigaste skyddet mot de kvalificerade IT-hoten är det förebyggande arbetet, t.ex. tekniska och administrativa säkerhetsarrangemang. Underrättelseverksamheten kan bidra till dessa, men har också kompetens att tidigt möta de kvalificerade IT-hoten. Samma teknik som används för signalspaning i det globala nätet för traditionell underrättelseinhämtning kan också användas för att skydda mot kvalificerade attacker via det globala nätet mot våra IT-system. En förutsättning för detta är att såväl eter- som trådburen trafik får följas, och att signalspaningens unika metoder kan användas. Sverige riskerar annars att utnyttjas av främmande stater och andra aktörer, som vill begagna våra informationssystem. Dessa förhållanden har bl.a. framhållits av FRA-utredningen (SOU 2003:30), som betonar att detta kräver att Försvarets radioanstalt ges legala och tekniska förutsättningar att fullt ut kunna bevaka information i det globala kommunikationsnätet (a.a. s. 85).

7.1.2 En internationell jämförelse

De nya förutsättningarna för signalspaning berör alla länder och har i många av dem föranlett förändringar av lagstiftningen.

I Storbritannien infördes år 2000 en mycket omfattande lag, *Regulation of Investigatory Powers Act 2000 (RIPA)*. I första delen finns regler för övervakning och avlyssning av kommunikationer. Regelverket är teknikneutralt, dvs. samma regler gäller oavsett i vilket medium övervakningen sker. I *RIPA* finns en förteckning över de myndigheter som får bedriva övervakning av kommunikationer, bl.a. Försvarets radioanstalts motsvarighet, *Government Communications Headquarters (GCHQ)*.

Den tyska lagstiftningen är uppbyggd ungefär efter samma mönster som den brittiska och är även den teknikneutral. I en särskild lag föreskrivs i vilka fall intrång får äga rum i den grundlagsfästa rätten till skydd av kommunikationer, samt för vilka ändamål ett antal angivna myndigheter får övervaka och avlyssna kommunikationer, bl.a. den centrala underrättelsetjänsten *Bundesnachriechtendienst.* Avlyssningen får ske såväl i brottsutredningssyfte som i underrättelsesyfte. Tyskland antog i januari 2002 en förordning enligt vilken teleoperatörer och andra åläggs en långtgående skyldighet att anpassa sina tekniska system så att verkställighet av myndigheternas avlyssning/övervakning kan ske.

I Nederländerna antogs år 2002 lagstiftning om underrättelse- och säkerhetstjänsterna. Lagen innehåller detaljerade regler om förutsättningarna för myndigheternas övervakning av olika typer av kommunikationer. Regelverket är inte helt teknikneutralt, utan anger delvis olika förutsättningar för avlyssning/övervakning i etern och i kabel/nätburen trafik. Båda typerna av ”signalspaning” kan dock bedrivas av de myndigheter för vilka lagstiftningen gäller, bl.a. den militära (*MIVD)* och den civila *(AIVD)* underrättelsetjänsten.

I Australien finns ny lagstiftning från år 2001 som rör underrättelsetjänsten, inklusive signalspaningsorganisationens verksamhet. Den australiska signalspaningstjänsten, *Defence Signals Directorate (DSD),* har möjlighet att signalspana på elektromagnetisk energi, oavsett i vilket medium den förmedlas.

Nya Zeeland har en ny lag från år 2004, *Telecommunications Interception Capability Act 2004*. Lagstiftningen ger säkerhetstjänsten (*New Zealand Security Service*) och signalspaningsorganisationen (*Goverment Communications Security Bureau*) rätt att inhämta telekommunikation på ett teknikneutralt sätt.

7.2 Skyddet för den personliga integriteten

7.2.1 Allmänt om förhållandet mellan integritet och effektivitet

Frågor om personlig integritet är centrala i samband med överväganden om Försvarets radioanstalts tekniska inhämtning med särskilda metoder. Intresset av att värna enskildas integritet kan dock inte ses isolerat utan måste vägas mot andra befogade intressen, i detta sammanhang främst behovet av en effektiv underrättelseverksamhet.

En svårighet vid denna intresseavvägning är att definiera vad som egentligen avses med begreppet personlig integritet, för att därigenom kunna ringa in det skyddsvärda området. I svensk lagstiftning finns ingen definition av begreppet. Olika utredningar (se t.ex. Tvångsmedelskommitténs betänkande Tvångsmedel – Anonymitet – Integritet, SOU 1984:54 s. 42) har med utgångspunkt i bl.a. de grundläggande fri- och rättigheterna i regeringsformens andra kapitel försökt klargöra begreppet genom att skilja mellan den rumsliga integriteten (hemfriden), den materiella integriteten (egendomsskyddet), den kroppsliga integriteten (skydd för liv och hälsa samt mot ingrepp i eller mot kroppen), den personliga integriteten i fysisk mening (skyddet för den personliga friheten och rörelsefriheten) och den personliga integriteten i ideell mening (skyddet för privatlivet och för personligheten inklusive den privata ekonomin).

Ett annat sätt att bestämma begreppet personlig integritet är att ange vilka handlingar som utgör kränkningar av densamma (se Stig Strömholm i SvJT 1971 s. 695). Enligt denna modell kan kränkningarna delas in i tre huvudgrupper: 1) intrång i en persons privata sfär i fysisk eller annan mening; 2) insamlande av uppgifter om en persons privata förhållanden; 3) offentliggörande eller annan användning (t.ex. som bevisning i rättegång) av uppgifter om en persons privata förhållanden. Som konkreta exempel av intresse i detta sammanhang på olika slag av kränkningar har angetts intrång i en persons privata sfär genom skuggning, spionerande, telefonterror och dylikt; olovlig ljudupptagning, fotografering eller filmupptagning; brytande av brevhemlighet; telefonavlyssning samt utnyttjande av elektronisk avlyssningsapparatur.

Den personliga integriteten kan alltså kränkas på många olika sätt. Även om det inte finns någon entydig definition av begreppet kan sammanfattningsvis konstateras att kränkningarna innebär ett intrång i en fredad sfär eller zon som den enskilde bör vara tillförsäkrad.

Det är en svår uppgift att avväga integritetsintresset mot nödvändigheten av att tillse att myndigheterna har effektiva metoder till sin hjälp för att bedriva den verksamhet de är skyldiga att utföra. En utgångspunkt måste vara att ingen medborgare i varje situation kan hävda rätt till handlingsfrihet eller rätt att bli lämnad i fred. I syfte att tillförsäkra medborgarna ökad trygghet och säkerhet mot yttre och inre hot kan det vara

nödvändigt med vissa inskränkningar av integritetsskyddet. Integritetskommittén uttryckte saken på följande sätt (SOU 1970:47 s. 56).

> En individ som lever i ett samhälle och sålunda ingår i en gemenskap med andra människor kan självfallet inte göra gällande något absolut anspråk på att få leva i fred för andra individer eller ostört av samhällets organ. Eftersom gemenskapen med andra människor och samhörigheten med samhället är grundläggande för den enskilda människans villkor, är det tydligt att tanken på skydd för dylika anspråk står i motsats till åtskilligt som av andra skäl måste gälla. Regler som syftar till att skydda den enskildes personliga integritet måste sålunda förses med olika, i skilda situationer mer eller mindre vittgående undantag eller på annat sätt begränsas till sin giltighet, så att andra människors och samhällets intressen i övrigt inte träds för när.

En annan viktig utgångspunkt är att myndigheterna inte får ges sådana befogenheter att medborgarnas tilltro till dem påverkas negativt. Förtroendet kan skadas om medborgarna upplever att det finns risk för att myndigheterna utan deras vetskap samlar information om enskilda och deras privatliv utan att detta motiveras av tungt vägande allmänna intressen.

Medborgarnas bild av det allmännas verksamhet påverkas dock också av i vilken utsträckning myndigheterna ges förutsättningar att använda effektiva arbetsmetoder. Myndigheterna är samhällsorgan som ytterst har till uppgift att värna medborgarna. Om medborgarna upplever att myndigheterna inte har förmåga eller tillräckliga medel för att hantera hot mot samhället och enskilda kan även detta leda till ett minskat förtroende.

Skyddet för den personliga integriteten är i viss utsträckning fastställt i internationella konventioner och svensk rätt. Den rättsliga regleringen utgör den yttre ramen för en diskussion kring den personliga integriteten i samband med myndigheternas arbetsmetoder. En särskild metod är emellertid inte nödvändigtvis godtagbar från integritetssynpunkt enbart av den anledningen att användningen är lagligen grundad. Integritetsskäl kan göra sig så starkt gällande att en åtgärd som i och för sig ryms inom den legala ramen ändå inte bör godtas av hänsyn till bl.a. allmänhetens tilltro till verksamheten.

En parlamentariskt sammansatt kommitté arbetar för närvarande med skyddet för den personliga integriteten (Ju 2004:05, Integritetsskyddskommittén). Utredningens uppdrag är bl.a. att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten och att överväga om det, vid sidan av befintlig lagstiftning, behövs generellt tillämpliga bestämmelser till skydd för den personliga integriteten och i så fall lämna förslag till en sådan reglering. Kommittén skall redovisa sitt arbete senast den 20 december 2007.

7.2.2 Regeringsformen och andra grundlagsbestämmelser

En grundläggande bestämmelse om skydd för den enskildes personliga integritet finns i 1 kap. 2 § tredje stycket andra meningen regeringsformen. Där sägs bl.a. att det allmänna skall värna den enskildes privatliv och familjeliv. Bestämmelsen har inte karaktären av en rättsligt bindande föreskrift utan anger en målsättning för den offentliga verksamheten. Den målsättningen följs upp i 2 kap. regeringsformen som innehåller

regler om grundläggande fri- och rättigheter och där det återfinns rättsligt bindande föreskrifter som skyddar den personliga integriteten i förhållande till det allmänna. Bestämmelserna är bindande för lagstiftaren och i viss utsträckning för domstolarna och andra rättstillämpande organ.

I 2 kap. 6 § regeringsformen föreskrivs – såvitt här är av intresse – att varje medborgare gentemot det allmänna är skyddad mot kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Bestämmelsen ändrades senast år 1976, dock utan att någon saklig ändring var avsedd (prop. 1975/76:209 s. 147 f.). I lagstiftningsärendet anfördes bl.a. att det förhållandet att skyddet endast avser meddelanden som är förtroliga innebär att skyddet inte omfattar t.ex. samtal i en folksamling eller i radiosändningar. Skyddet omfattar däremot meddelanden som sänds med post eller på annat sätt som brev, telegram, bandinspelningar o.s.v. Skyddet omfattar såväl hemlig avlyssning som sker samtidigt med ett samtal som upptagning av ett samtal för senare avlyssning (Om buggning och andra hemliga tvångsmedel, SOU 1998:46 s. 51).

I begreppet ”husrannsakan och liknande intrång” torde inte innefattas intrång i datorer eller andra upptagningar för automatiserad behandling (se prop. 1987/88:65 s. 62 och SOU 1992:110 s. 351 f.).

Vissa av bestämmelserna i 2 kap. regeringsformen ger ett absolut skydd, vilket innebär att skyddet inte kan begränsas på annat sätt än genom grundlagsändring (se 2 kap. 2–5 §§). Beträffande andra bestämmelser gäller att skyddet är relativt i den meningen att det kan begränsas genom lag. Bestämmelsen i 2 kap. 6 § hör till den senare kategorin. Av 2 kap. 12 § framgår – förutom kravet på lagreglering – att begränsningar i skyddet får göras endast för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle. En begränsning får heller aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

De nu behandlade bestämmelserna i regeringsformen gäller för svenska medborgare. Om inte annat är föreskrivet är utlänning här i riket dock likställd med svenska medborgare i angivet avseende (2 kap. 22 § andra stycket 3 regeringsformen).

Vissa typer av kommunikationer skyddas vidare genom bestämmelserna i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Enligt 1 kap. 1 § tryckfrihetsförordningen har var och en frihet att i tryckt skrift yttra tankar och åsikter och meddela uppgifter och underrättelser i vilket ämne som helst såvida inte annat följer av förordningen. Uppgifter och underrättelser får vidare lämnas för publicering i tryckt skrift till författare, utgivare av en skrift eller en redaktion för skriften samt till nyhetsbyråer. Motsvarande bestämmelser finns i 1 kap. 2 § yttrandefrihetsgrundlagen när det gäller uppgifter för offentliggörande i bl.a. radioprogram, filmer samt ljud- och bildupptagningar. Meddelarfriheten garanteras genom ett anonymitetsskydd som bl.a. innebär att journalister och andra med vissa undantag har tystnadsplikt beträffande vem som lämnat meddelanden enligt 1 kap. 1 § tryckfrihetsförordningen eller 1 kap. 2 § ytt-

randefrihetsgrundlagen. I båda grundlagarna förbjuds det allmänna att efterforska vem som lämnat uppgifter för publicering i de olika medierna, med undantag för de fall då åtal eller annat ingripande mot honom eller henne kan ske med stöd av grundlagarna.

Den meddelarfrihet med åtföljande meddelarskydd som sålunda gäller är inte begränsad till publikationer, radioprogram m.m. som har anknytning till Sverige exempelvis därför att de ges ut här. Med vissa undantag gäller meddelarskyddet även den som lämnar uppgifter till utländska medier, i vart fall när uppgiftslämnandet sker i Sverige (SOU 2004:114 s. 143). Den som i publiceringssyfte sålunda kommunicerar med en utländsk tidningsredaktion eller ett utländskt radio- eller TV-företag får därför som regel inte efterforskas av det allmänna.

7.2.3 Europakonventionen

Skydd för den personliga integriteten

Europarådet antog den 4 november 1950 konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Ett antal tilläggsprotokoll har under åren öppnats för ratifikation. Genom lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna gäller Europakonventionen jämte tilläggsprotokoll sedan den 1 januari 1995 som svensk lag.

Enligt 2 kap. 23 § regeringsformen får lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden enligt konventionen.

Enligt artikel 8:1 i konventionen har var och en rätt till skydd för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Rätten till skydd för privatlivet är av mycket allmän art och omfattar skydd mot en mängd åtgärder. Med korrespondens avses olika former för att överföra meddelanden mellan individer. Överföring av meddelanden med hjälp av telefon, telefax, radio och datorer omfattas av konventionens skydd för korrespondens (se Danelius, Mänskliga rättigheter i europeisk praxis, 2002, s. 270). Ett ingrepp i skyddet för korrespondens är bl.a. när någon hindrar eller kontrollerar sådan kommunikation.

Av artikel 8:2 framgår under vilka förutsättningar inskränkningar i de angivna rättigheterna får ske. En inskränkning måste ske med stöd av lag och inskränkningen skall vara ägnad att tillgodose något av de i artikel 8:2 uppräknade allmänna eller enskilda intressena, däribland statens säkerhet, den allmänna säkerheten och förebyggande av oordning eller brott. Inskränkningen måste anses vara nödvändig i ett demokratiskt samhälle för att tillgodose detta intresse. Detta krav kan i huvudsak sägas innebära att det måste finnas ett angeläget samhälleligt behov av inskränkningen och att den måste stå i rimlig proportion till det syfte som skall tillgodoses genom ingreppet. Vidare måste undantaget vara utformat med sådan precision att inskränkningen av rättigheten är i rimlig utsträckning förutsebar.

I vilken utsträckning nationella organ ges frihet att avgöra vilka intressen som motiverar inskränkningar i grundläggande rättigheter beror på vilken typ av intressen det är fråga om. När det t.ex. gäller statens säker-

het är möjligheten att på nationell nivå göra avvägningar vidsträckt, och Europadomstolens kontroll följaktligen mindre omfattande (a.a. s. 264).

I Europadomstolens praxis har slagits fast att hemlig teleavlyssning och hemlig teleövervakning utgör intrång i såväl privatliv som korrespondens (SOU 1998:46 s. 53). Sådana inskränkningar har ansetts godtagbara då de är strängt nödvändiga för att skydda den nationella säkerheten eller för att förhindra oordning eller brott. Det måste dock finnas en effektiv kontroll av att systemet inte missbrukas (se bet. Om buggning och andra hemliga tvångsmedel, SOU 1998:46 s. 58 med hänvisningar). När teleavlyssning har ansetts utgöra en kränkning av artikel 8 har i de flesta fall bristande lagenlighet utgjort grunden för kränkningen.

I artikel 13 föreskrivs att var och en som anser sig ha fått sina fri- och rättigheter kränkta skall ha tillgång till ett effektivt rättsmedel inför en nationell myndighet. Detta gäller enligt artikeln även om kränkningen förövats av någon under utövning av offentlig myndighet. Konventionen kräver inte att prövningen skall utföras av domstol utan även administrativa rättsmedel, inklusive olika former av övervaknings- och kontrollåtgärder, kan vara tillräckliga för att uppfylla kravet.

Europakonventionen och lagstiftningen i andra länder

Europakonventionen gäller för det stora flertalet av Europas demokratiska stater. Motsvarande typ av reglering återfinns också i regel i olika länders konstitutioner. Ett flertal med Sverige jämförbara länder har lagstiftning som i olika grad tillåter inhämtning av telekommunikation i bland annat underrättelsesyfte. Medlemsländerna i den Europeiska unionen synes med varierande grad av utförlighet ha anpassat den nationella lagstiftningen som rör signalspaning mot elektronisk kommunikation till Europakonventionen. I t.ex. brittisk, nederländsk och tysk lagstiftning anges i enlighet med undantagsbestämmelsen i artikel 8:2 i konventionen att avlyssning av elektronisk kommunikation får bedrivas bl.a. för att skydda nationell säkerhet och landets ekonomiska välstånd samt för att bekämpa viss internationell brottslighet. Vissa medlemsländer har också i den nationella lagstiftningen uttryckligen angivit att avlyssningen endast får ske under förutsättning att åtgärden framstår som nödvändig i ett demokratiskt samhälle. Det har ibland också uttryckligen angivits att åtgärden måste stå i proportion till vad som är att vinna med den.

Medlemsländerna har alla olika nationella regler för kommunikationsspaningen beroende på om den riktas mot kommunikation inom eller utom landet och om den riktas mot landets medborgare eller mot utlänningar. I flera länder föreskrivs att spaningen inte får riktas mot det egna landets medborgare. I vissa medlemsländer finns regler om tillståndskrav för kommunikationsspaning. Medlemsländerna har särskilda organ för kontroll av att reglerna om kommunikationsspaningen efterlevs. I vissa länders lagstiftning anges att kontrollen skall utföras fortlöpande. Länderna har också särskilda regler om rättsmedel för att påtala fel i samband med signalspaningsverksamheten.

7.2.4 Brottsbalken

Det grundlagsfästa skyddet för den enskildes integritet gäller i förhållande till det allmänna. Integritetskränkningar från enskilda – men även tjänstemän hos det allmänna – regleras genom bestämmelser i annan lag, framförallt brottsbalken (BrB). De bestämmelser i brottsbalken som är av störst intresse ur integritetssynpunkt återfinns i 4 kap. om brott mot frihet och frid samt i 5 kap. om ärekränkningsbrott. Även 3 kap. om brott mot liv och hälsa, 6 kap. om sexualbrotten samt 20 kap. om tjänstefel innehåller regler som kan sägas utgöra ett skydd för den personliga integriteten. Signalspaningsverksamheten berörs dock främst av vissa bestämmelser i 4 kap. BrB, såsom brytande av post- eller telehemlighet (8 §), intrång i förvar (9 §) och olovlig avlyssning (9 a §). Verksamheten kan också komma att beröras av bestämmelsen om dataintrång i brottsbalken (9 c §). Sammanfattningsvis kan straffansvar för dessa brott endast komma i fråga om gärningen sker olovligen.

7.2.5 Reglering av personuppgiftsbehandling

Ett område på vilket det ansetts föreligga särskilda behov av integritetsskydd är vid behandling av personuppgifter på automatiserad väg i datorer eller manuellt i register. Automatiserad behandling och behandling i strukturerade samlingar är särskilt känslig med hänsyn till de möjligheter till sökning i och sammanställning av uppgifter som erbjuds. Bestämmelser till skydd mot integritetskränkningar genom sådan behandling finns i personuppgiftslagen (1998:204), som grundar sig på ett EG-direktiv, 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).

Personuppgiftslagen reglerar i vilka fall och under vilka förutsättningar personuppgifter får behandlas. Vid överträdelser av bestämmelserna kan en enskild som utsatts för kränkning bli berättigad till skadestånd. I vissa fall kan också straff komma i fråga. En särskild tillsynsmyndighet, Datainspektionen, övervakar tillämpningen och har i detta syfte fått långtgående befogenheter.

Dataskyddsdirektivet omfattar inte sådan behandling av personuppgifter som rör allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Personuppgiftslagen har däremot gjorts generellt tillämplig. Eftersom personuppgiftslagen har ett mycket brett tillämpningsområde som omfattar såväl privat som offentlig verksamhet av mycket skiftande karaktär är dess bestämmelser allmänna och beaktar inte alla frågeställningar som kan aktualiseras inom särskilda verksamheter. På många områden har därför införts särskilda registerförfattningar som närmare föreskriver vad som gäller för enskilda myndigheters personuppgiftsbehandling.

Personuppgiftsbehandlingen hos Försvarets radioanstalt regleras i förordningen (2001:703) om viss behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt. Regeringen bereder för närvarande en lagreglering av personuppgiftsbehandlingen. Ett lagförslag har varit föremål för lagrådsbehandling.

Europaparlamentets och rådets direktiv (2002/58/EG) av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation behandlar särskilt skyddet för personuppgifter som förmedlas elektroniskt. I likhet med dataskyddsdirektivet skall det emellertid inte tillämpas på verksamheter som avser bl.a. allmän säkerhet, försvar och statens säkerhet i övrigt (artikel 1.3). Av direktivet framgår vidare att rättigheter och skyldigheter enligt direktivet får begränsas genom lagstiftning när en sådan begränsning är nödvändig, lämplig och proportionell för att skydda bl.a. nationell säkerhet, försvaret och allmän säkerhet (artikel 15.1). Genom att signalspaning för försvarsunderrättelseändamål nu föreslås bli lagreglerad på sätt som tillgodoser kraven i artikel 15.1 får verksamheten anses bli förenlig med bestämmelserna i direktivet.

7.2.6 Regler om elektronisk kommunikation

I lagen (2003:89) om elektronisk kommunikation (LEK) finns i sjätte kapitlet regler till skydd för den enskildes integritet. Av 6 kap. 17 § andra stycket 3 framgår att förbudet mot avlyssning som uppställs i första stycket inte utgör hinder mot att i radiomottagare avlyssna eller på annat sätt med användande av sådan mottagare få tillgång till ett radiobefordrat elektroniskt meddelande som inte är avsett för den som avlyssnar eller för allmänheten. I 6 kap. 20 § anges att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av tillgång till vissa uppgifter om bl.a. innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande inte obehörigen får föra vidare eller utnyttja det han fått del av eller tillgång till. Tystnadsplikten gäller inte i förhållande till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller på annat sätt har sänt eller tagit emot meddelandet. I författningskommentaren (prop. 2002/03:110 s. 398) anförs att bestämmelsen i 6 kap. 17 § klargör den gällande principen om att etern är fri och att var och en i princip fritt kan lyssna till radiobefordrade meddelanden i en radiomottagare. Det konstateras att reglerna om tystnadsplikt dock kan vara tillämpliga.

I förarbetena (prop. 1992/93:200 s.166) till telelagen (1993:597) angav regeringen att den huvudsakliga utgångspunkten för den dåvarande regleringen av tystnadsplikten i 3 a § radiolagen (1966:755) för den som i mottagare avlyssnat ett telemeddelande var att etern är fri och att envar enligt radiolagstiftningen i princip fritt kan lyssna till radiobefordrade meddelanden. Regeringens bedömning i samband med införande av bestämmelsen i LEK var att rättsläget därigenom inte förändrades i detta avseende (prop. 2002/03:110 s. 255).

7.3 Effektivt utnyttjande av signalspaningsresursen

7.3.1 Utvidgning av signalspaningsmandatet

Regeringens förslag: Den myndighet som regeringen bestämmer skall få bedriva signalspaning i försvarsunderrättelseverksamhet oavsett om

signalerna befinner sig i etern eller i kabel, dvs. är trådburna. Detta skall regleras i en ny lag om signalspaning i försvarsunderrättelseverksamhet.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De allra flesta remissinstanserna tillstyrker förslaget eller lämnar det utan erinran. *Post- och telestyrelsen* har påtalat att det torde vara en väsentlig skillnad ur integritetssynpunkt att avlyssna ett radiomeddelande genom att passivt sätta upp en antenn i luften jämfört med att avlyssna ett meddelande genom att aktivt och fysiskt ta sig in i en operatörs kommunikationsnät och att det är märkligt att lägga denna skillnad i skyddsnivå till grund för att tillåta avlyssning i tråd. *Sveriges advokatsamfund* har fört fram att det inte är en given slutsats att om signalspaning i tråd tillåts detta skall få ske på samma villkor som för signalspaning i etern. Samfundet har också ifrågasatt om inte ett icke trådbundet telefonsamtal bör förtjäna samma skydd mot intrång från statsmakterna sida som ett trådbundet.

Skälen för regeringens förslag: Samhällets behov av en effektiv underrättelseverksamhet har beskrivits närmare i avsnitt 6 och 7.1.1, där det också framgår att inhämtning genom signalspaning är en av grunderna för Sveriges underrättelseförmåga. Alternativa inhämtningsmetoder kan sällan mäta sig med signalspaningen vid en effektivitets- och kostnadsjämförelse.

Signalspaningens viktigaste uppgift är att vara ett stöd för de säkerhetspolitiska beslutsfattarna i det löpande arbetet och att utgöra en försäkring mot överraskningar. Verksamheten ger oss möjlighet att följa den militära utvecklingen i vårt närområde och ger synnerligen angelägen information i samband med svenskt deltagande i internationella insatser för att ge ökat skydd för vår personal och bättre beslutsunderlag för berörda chefer. Signalspaningen kan också inhämta förtrolig kunskap om mellanstatligt agerande, spridning av massförstörelsevapen samt handel med vapen, människor och droger. Dessutom är signalspaning ett viktigt redskap i kampen mot internationell terrorism. När det gäller kartläggning av hot som innefattar brottslig verksamhet kan signalspaningen bidra med väsentlig strategisk information, men i enlighet med vad som framgår av avsnitt 6.3.2 gäller begränsningar i möjligheten att använda resursen i renodlat operativt brottsbekämpande syfte.

Eftersom signalspaningens inriktning, metoder och resultat behöver sekretesskyddas under lång tid kan mycket lite om den aktuella verksamheten offentliggöras. Vissa förhållanden från andra världskriget omfattas fortfarande av sekretess efter över sextio år. Med hänsyn till detta är det varken lämpligt eller möjligt att lämna närmare exempel på när och hur rapporterade underrättelser till följd av signalspaning har varit direkt avgörande för Sveriges säkerhet. Några exempel som belyser vikten av verksamheten lämnas dock nedan.

På 1940-talet forcerade den svenske matematikprofessorn Arne Beurling och hans medarbetare den tyska högsta ledningens kryptosystem, vilket ledde till att den svenska statsledningen under de första krigsåren i klartext kunde läsa ca 296 000 meddelanden ur den hemliga tyska militära och diplomatiska trafiken, varav många av synnerligen stor vikt för Sveriges säkerhet. Trafiken gick i kabel och gjordes tillgänglig för den svenska signalspaningen genom den förfogandelagstiftning som var i

tillämpning under kriget. Kryptoverksamheten inom svensk signalspaning växte kraftigt och var en bidragande orsak till att Försvarets radioanstalt bildades som en civil myndighet 1942.

Under det kalla kriget var en av signalspaningens huvuduppgifter att ge förvarning om krigsförberedelser eller andra militära hot mot Sverige samt händelser i omvärlden av betydelse för Sveriges säkerhet. Under Tjeckoslovakienkrisen 1968 följde signalspaningen uppmarschen av sovjetiska förband och gav värdefullt underlag för de svenska bedömningarna av riskerna för en sovjetisk intervention i Tjeckoslovakien. En liknande roll spelade signalspaningen i samband med Polenkrisen 1980-1981. Kunskaperna ledde då till att personal inkallades för beredskapstjänstgöring.

I samband med ubåtsincidenterna på 1980-talet kunde signalspaningsverksamheten bidra till att t.ex. vederlägga vissa vittnesuppgifter om ubåtsobservationer. Signalspaning har också med framgång använts i samband med andra typer av incidenter och haverier i Östersjöområdet, liksom för att följa andra staters materielutveckling.

Politiskt sett var signalspaning av stort värde i samband med det sovjetiska tillbakadragandet från Östeuropa och den baltiska frigörelsen, då fakta från signalspaningen kunde ställas mot rykten och gav möjlighet att bedöma hur parterna uppfyllde ingångna överenskommelser.

I samband med Sveriges deltagande i internationella insatser började signalspaning användas på Balkan 1995. En egen svensk signalspaningsförmåga i Bosnien och Kosovo bidrog till att öka säkerheten i området och gav, i samverkan med utländska enheter, taktiska underrättelser som ansågs mycket värdefulla av NATO, som ledde insatserna. Även vid svenska insatser i krisområden som Kongo, Liberia och Sudan har svensk signalspaning gett värdefulla bidrag.

Signalspaningen har också i decennier gett regeringen stöd med utrikespolitiskt relevanta underrättelser, t.ex. om internationella förhandlingar och allmän geopolitisk utveckling. Under senare år har spridning av massförstörelsevapen kunnat följas, liksom konventionell vapenhandel och exportkontroll av intresse för t.ex. Tullverket och Inspektionen för strategiska produkter.

I kampen mot terrorismen har information från svensk signalspaning mot utländska företeelser gett Säkerhetspolisen underrättelser av stor betydelse för det brottsförebyggande arbetet. Signalspaning har också använts framgångsrikt för att kartlägga annan grov organiserad brottslighet.

De djupgående förändringar som skett under de senaste åren avseende både den säkerhetspolitiska miljön och den tekniska utvecklingen har inneburit nya förutsättningar för underrättelseverksamheten. Behovet av underrättelser har ökat. Signalspaningen har fått en allt viktigare roll för att skydda vår kommunikation mot intrång av andra länder och aktörer. Därmed bidrar signalspaningen till att upprätthålla informationssäkerheten i samhället.

Mot den bakgrund som angetts ovan framstår det enligt regeringens mening som ett mycket angeläget allmänt intresse att signalspaningsmyndigheten även i framtiden skall kunna bedriva en ändamålsenlig verksamhet. En avgörande förutsättning för detta är dock att signalspaning kan genomföras oavsett med vilken teknik signalerna förmedlas. Att

kommunikationen idag till stor del har förflyttats från etern till tråd bör inte begränsa möjligheten att signalspana, särskilt som det sätt på vilket signalerna överförs ofta styrs av slumpen.

Det är således nödvändigt att anpassa förutsättningarna för signalspaningsverksamheten till utvecklingen på de säkerhetspolitiska och tekniska områdena. Starka skäl talar därför för att inhämtning av signaler i elektronisk form bör få ske även då signalerna befinner sig i tråd.

Signalspaning mot signaler i etern har sedan länge ansetts förenlig med det skydd gentemot det allmänna som 2 kap. 6 § regeringsformen uppställer, detta bl.a. mot bakgrund av förarbetsuttalanden med innebörden att skyddet för förtroliga meddelanden inte omfattar exempelvis samtal i folksamlingar eller radiosändningar (prop. 1975/76:209). Principen att etern är fri har också kommit till uttryck i 6 kap. 17 § andra stycket lagen (2003:389) om elektronisk kommunikation. Dock förhåller det sig annorlunda vad gäller inhämtning av signaler i tråd, för vilka särskilda regler är nödvändiga. Med hänsyn till hur verksamheten bedrivs skulle det innebära praktiska problem att behöva tillämpa olika rutiner beroende på från vilket medium kommunikation inhämtats. Likaså skulle kontrollen av verksamheten försvåras om olika regelverk tillämpas inom verksamheten. Regeringen anser att en lagreglering av signalspaningen i försvarsunderrättelseverksamheten därför bör vara teknikneutral på så sätt att signalerna rättsligt sett bör behandlas lika oavsett hur och från vilket medium kommunikationen inhämtas. Genom att signalspaningen i sin helhet ges uttryckligt stöd i lag tydliggörs också att den inte kommer i konflikt med de ovan redovisade bestämmelserna i brottsbalken. En utvidgning av signalspaningsmandatet till att även omfatta signaler i tråd innebär naturligtvis risk för intrång i den personliga integriteten. Hur skyddet för enskildas fri- och rättigheter skall utformas för att balansera denna risk behandlas i avsnitt 7.4.

Signalspaningen enligt förslaget till lag om signalspaning i försvarsunderrättelseverksamhet skall bedrivas vid den myndighet som regeringen bestämmer. Den myndighet som regeringen avser att peka ut i förordning som ansvarig för verksamheten är Försvarets radioanstalt.

7.3.2 Inhämtningens omfattning

Regeringens förslag: Inhämtning av signaler i elektronisk form vid signalspaning skall få ske i försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet, dvs. underrättelseverksamhet som bedrivs till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. I verksamheten ingår också att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Försvarsunderrättelseverksamhet får endast avse utländska förhållanden.

Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller lämnar det utan erinran. *Kustbevakningen* har anfört att begreppet signaler i elektronisk form utgör en begränsning eftersom signalerna kan överföras på annat sätt än elektroniskt, t.ex. genom fiberoptik, och det kan ifrågasättas om den aktuella bestämmelsen borde göras inriktad på signaler eller uppgifter snarare än på teknik för överförande. *Stockholms universitet* har påpekat att det vid införandet av nya begrepp är viktigt att klargöra förhållandet till redan existerande begrepp. I 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation (LEK) definieras den informationsmängd som elektroniska kommunikationstjänster överför som ”signaler i elektroniska kommunikationsnät”. *Post- och telestyrelsen* har föreslagit att det i LEK definierade uttrycket ”elektroniskt meddelande” används för att beteckna innehållet i den elektroniska kommunikationen.

Skälen för regeringens förslag: I förslaget till ändring i lagen (2000:130) om försvarsunderrättelseverksamhet anges att försvarsunderrättelseverksamhet skall fullgöras genom inhämtning, bearbetning och analys av information. I verksamheten får användas teknisk och personbaserad inhämtning som sker med särskilda metoder. En sådan särskild metod är signalspaning, som innebär att signaler i elektronisk form inhämtas. I avsnitt 7.3.6 redogörs för begreppet elektronisk kommunikation. Begreppet definieras inte i LEK och anses där inte omfatta innehållet i kommunikationen. Därför är begreppet inte lämpligt att använda för att definiera föremålet för den inhämtning som signalspaningen innefattar. I 1 kap. 7 § LEK anges, såsom *Stockholms universitet* har anfört, att en elektronisk kommunikationstjänst utgörs av överföring av signaler i elektroniska kommunikationsnät.

Begreppet ”elektroniskt kommunikationsnät” definieras som ett system för överföring och i tillämpliga fall utrustning för koppling och dirigering samt andra resurser som medger överföring av signaler. Det bör dock i den nu aktuella lagen fokuseras på vad som får inhämtas, snarare än i vilket system signalerna överförs. I förslaget till lag om signalspaning i försvarsunderrättelseverksamhet avses med signaler i elektronisk form alla former av signaler som överförs bl.a. med hjälp av elektromagnetiska vågor. Det saknas därför enligt regeringens uppfattning anledning att gå ifrån den i promemorian föreslagna lydelsen.

Såväl intresset av att skydda den personliga integriteten som verksamhetens behov nödvändiggör att det av lagen framgår tydligt när signalspaning får ske, dvs. tillämpningsområdet måste vara klart avgränsat. I förslaget till ändring i lagen (2000:130) om försvarsunderrättelseverksamhet anges att försvarsunderrättelseverksamheten skall bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för att kartlägga yttre hot mot landet. I verksamheten ingår också att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Försvarsunderrättelseverksamheten får vidare enligt förslaget endast avse utländska förhållanden. Verksamheten inbegriper såväl traditionella militära frågor som andra säkerhetspolitiska hot. Signalspaningen är ett oundgängligt verktyg för att lösa samtliga de uppgifter som försvarsunderrättelseverksamheten omfattar. I förslaget till lag om signalspaning i försvarsunderrättelseverksamhet bör därför enligt regeringens mening anges

att signalspaning får ske i den verksamhet som anges i lagen om försvarsunderrättelseverksamhet.

Den signalspaning som bedrivs i försvarsunderrättelseverksamheten är för sin förmåga att tillhandahålla relevanta underrättelser beroende av att kunna följa utvecklingen på signalområdet och kontinuerligt anpassa sin teknik. För att Försvarets radioanstalt skall få tillräckliga förutsättningar för att kunna bedriva en effektiv försvarsunderrättelseverksamhet är det följaktligen viktigt att myndigheten har möjlighet att följa förändringar i signalmiljön i omvärlden, vilket bl.a. förutsätter inhämtning av metadata (data om data, såsom t.ex. kanalnummer och bärfrekvens). Likaså måste myndigheten kunna följa förändringar i den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten. Regeringen anser därför att lagen skall ge möjlighet till inhämtning av signaler i elektronisk form vid signalspaning också för dessa ändamål.

Inhämtning av information av teknisk karaktär enligt vad som beskrivits ovan sker för myndighetens egna behov av att kunna anpassa sina tekniska system till utvecklingen. Denna verksamhet genererar följaktligen inte någon underrättelserapportering. Den kompetens som byggs upp hos myndigheten på detta område kommer även andra myndigheter till del, men då inte i form av underrättelser eller motsvarande utan genom bistånd i tekniskt avseende. Verksamheten avser normalt inte innehållet i meddelanden som utväxlas mellan enskilda. Intrånget i den personliga integriteten blir därmed marginellt. Emellertid kan det inte uteslutas att verksamheten kan komma att innefatta inhämtning av information, t.ex. om mellan vilka viss kommunikation äger rum, som är känslig ur integritetssynpunkt. Regeringen anser därför att även denna verksamhet skall omfattas av de begränsningar som lagen uppställer.

7.3.3 Begränsning av inhämtningen i tråd

Regeringens förslag: Inhämtning som sker i tråd får endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör.

Promemorians förslag: Överensstämmer delvis med regeringens. I promemorian har förslagits att inhämtning som sker i tråd endast får avse signaler vilka förs över Sveriges gräns av operatörer som äger tråd.

Remissinstanserna: De flesta remissinstanser tillstyrker förslaget eller lämnar det utan erinran. *Kustbevakningen* har anfört att förslaget till 2 § är för begränsat, vilket kan leda till minskad möjlighet att inhämta signaler och uppgifter. Eftersom signaler även kan förmedlas via kabel för fiberoptik, kan det övervägas att föreskriva att inhämtning av signaler får ske i tråd och kabel om befogenheten även skall omfatta fiberoptik.

Säkerhetspolisen har påtalat att inhämtning om utländska förhållanden kan ske såväl i Sverige som utomlands. Den föreslagna begränsningen är därför oklar. De centrala aktörerna på telemarknaden är ofta internationella bolag, och Säkerhetspolisens erfarenhet är att inhemsk kommunikation därför i allt högre grad kan komma att passera nationsgränsen. När det gäller rättsäkerhet och andra aspekter på inhämtningen bör därför

förslagen ses som att de avser inhämtning av kommunikation mellan personer i Sverige.

Stockholms universitet menar att även om begreppet tråd har sitt ursprung i distinktionen mellan trådburen och trådlös kommunikation så är begreppet fasta nät etablerat inom telekommunikationssektorn. Innehavaren är nätägare, ett inarbetat begrepp som innefattar både fasta och mobila nät. I lagen om elektronisk kommunikation används begreppen fast respektive mobil när nätanslutningspunkterna beskrivs. Universitetet har vidare anfört att ett stort antal operatörer inte äger någon del av det fasta nätet utan endast hyr kapacitet. Universitetet framhåller också att förslaget till ny lag om signalspaning (2 §) innebär att av den trafik som de facto passerar genom samverkanspunkterna får avlyssning endast ske av signaler som de nätägande operatörerna förmedlar. Även *E.ON* har påtalat att förslaget till författningsreglering (2 §) kan tolkas som att signaler från en trådägande operatör som för trafik över rikets gräns via en hyrd förbindelse omfattas av lagen, medan signaler som kommer från operatör i Sverige som bedriver sin verksamhet över hyrda förbindelser inte omfattas.

Post- och telestyrelsen (PTS) har anfört att själva kommunikationssystemet i sig är uppbyggt kring mekanismer som skall göra det möjligt för kommunikation att fortgå obehindrat även om delar av kommunikationsnätet drabbas av störningar. PTS är vidare tveksam till slutsatsen att den inhemska trafiken endast sker i liten utsträckning över nationens gränser eller ens kan separeras från den utländska trafiken. PTS menar att det i dessa sammanhang inte går att tala om inhemsk respektive utländsk trafik eftersom näten inte är uppbyggda på ett sådant sätt att en klar skiljelinje går att dra.

Länsstyrelsen i Uppsala (administrativ värd för projektet Länssamverkan i bredband) har anfört att den elektroniska kommunikationen såväl inom som över landets gränser sker i allt större omfattning via Internet eller över det s.k. Internetprotokollet (IP). IP-kommunikation innebär att information delas upp i olika paket som transporteras olika vägar genom de fysiska näten och sätts samman till en enhet endast hos avsändaren, mottagaren eller i mellanliggande servrar. Ett informationspaket som skall nå en mottagare inom landet, och där sättas samman med övriga paket, kan lika väl transporteras över landets gränser som inom dessa. Förhållandena gör att det är mycket svårt att få en överblick över de olika näten samt att klart urskilja samt definiera vad som hör hemma i landet.

Skälen för regeringens förslag: Av föregående avsnitt framgår att försvarsunderrättelseverksamheten föreslås avse utländska förhållanden. I förslaget bör följaktligen finnas en reglering som ger Försvarets radioanstalt tillgång till sådana signaler som är av intresse för försvarsunderrättelseverksamheten men begränsar möjligheten att inhämta inhemsk kommunikation. Den övriga verksamhet för vilken signalspaning föreslås få bedrivas syftar till att skapa förutsättningar för inhämtning i försvarsunderrättelseverksamheten. Även sådan signalspaning riktas följaktligen huvudsakligen mot utländska förhållanden.

När det gäller signaler i tråd framgår av avsnitt 7.1.1 att trådbunden överföring sker via kablar i form av bl.a. fiberoptiska nät. Någon anledning att, såsom *Kustbevakningen* anfört, ändra begreppet ”tråd” saknas enligt regeringens mening därför. Det finns av lätt insedda skäl begrän-

sade möjligheter för signalspaningsmyndigheten att få tillgång till signaler som förmedlas i sådan tråd som i sin helhet befinner sig utomlands. För att kunna ta del av trafik som rör utländska förhållanden är verksamheten hänvisad till signaler till vilka myndigheten kan ges åtkomst. En sådan åtkomst är möjlig i fråga om signaler som förmedlas i tråd som passerar Sveriges gräns.

För att fånga in den trafik som är relevant för signalspaningen, men för att samtidigt i så stor utsträckning som det är möjligt utesluta inhemsk trafik, bör inhämtningen av signaler i tråd avse signaler som förs över Sveriges gräns. Regeringen är medveten om att, såsom flera *remissinstanser* har påpekat, även inhemsk trafik till följd av t.ex. kapacitets- eller kostnadsskäl kan komma att passera landgränsen. Kravet att signalerna skall passera Sveriges gräns innebär dock enligt regeringens bedömning de facto en begränsning av signalspaningens tillämpningsområde och en sådan bestämmelse bör därför föras in i lagen. Att signalerna passerar gränsen ökar också graden av relevans i förhållande till de ändamål för vilka försvarsunderrättelseverksamheten föreslås få bedrivas. Inhemsk kommunikation som av tekniska skäl förs över gränsen men som saknar koppling till utländska förhållanden skall enligt förslaget, om den överhuvudtaget skulle komma att inhämtas (se följande avsnitt), omedelbart förstöras (se avsnitt 7.4.4).

Det åligger följaktligen Försvarets radioanstalt att vidta åtgärder för att i så stor utsträckning som möjligt begränsa inhämtning av sådan kommunikation, att identifiera kommunikationen om den trots allt inhämtas och att i sådant fall se till att den inte kan bli föremål för vidare bearbetning eller lagring utan förstörs. Granskningen av att det finns fungerande system och rutiner för att säkerställa detta är en viktig uppgift för den kontrollfunktion som beskrivs i avsnitt 8. Till detta kommer att, enligt den nya sekretessbestämmelse till skydd för uppgifter om enskildas personliga och ekonomiska förhållanden i bl.a. Försvarets radioanstalts försvarsunderrättelseverksamhet som föreslås i avsnitt 9, sådana uppgifter om enskilda som inte förstörs kommer att omfattas av sekretess. Regeringen bedömer mot denna bakgrund att även om det inte är möjligt att helt utesluta att inhemsk information kommer att inhämtas, de kompletterande integritetsskyddande bestämmelser som föreslås (se avsnitt 7 och 8) sammantaget ger ett fullgott skydd för enskildas integritet.

För att signalspaningsmyndigheten skall få åtkomst till trådburna signaler som förs över Sveriges gräns krävs en reglering av hur överföringen av signalerna till myndigheten skall gå till. I syfte att skapa förutsättningar för en ändamålsenlig reglering av formerna för överföringen bör i förslaget till lag om signalspaning i försvarsunderrättelseverksamhet föreskrivas att inhämtningen endast får avse signaler i sådan tråd som ägs av en operatör. Med operatör avses detsamma som enligt 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation, dvs. den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation. Såsom *Stockholms universitet* och *E.ON* har påpekat behövs ett klargörande av den lagtext som föreslagits i promemorian för att tydliggöra att de trådägande operatörerna som för signaler i tråd över rikets gräns kan förmedla såväl egen som andra operatörers trafik. De bestämmelser av teknisk karaktär som enligt regeringens bedömning behövs för att åstadkomma nödvändig åtkomst till signaler i tråd i enlighet med det

ovan anförda beskrivs närmare i avsnitt 7.3.7, liksom skyldigheten för operatörerna att se till att signalerna enkelt kan tas omhand.

När det gäller signaler i etern förutsätter inte möjligheten till inhämtning att åtkomsten till signalerna sker under medverkan av någon operatör. Regeringen föreslår därför inte någon särskild reglering i detta avseende. Det finns inte heller någon möjlighet att på teknisk väg begränsa vilken eterburen kommunikation som skall göras tillgänglig för signalspaning.

7.3.4 Automatiserad inhämtning med sökbegrepp

Regeringens förslag: Inhämtning av signaler i tråd skall ske automatiserat. Sådan inhämtning skall endast få avse signaler som identifierats genom sökbegrepp.

När automatiserad inhämtning utnyttjas beträffande andra signaler än sådana som förmedlas i tråd skall också sökbegrepp användas för identifiering av signalerna.

Regeringens bedömning: Vid Försvarets radioanstalt bör ett integritetsskyddsråd inrättas med uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten.

Promemorians förslag överensstämmer i huvudsak med regeringens men innehåller inga överväganden kring inrättandet av ett integritetsskyddsråd.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslagen eller lämnar dem utan erinran. *Säkerhetspolisen* har anfört att argumenten för att låta Försvarets radioanstalt fastställa sökbegrepp tar sikte på två olika saker. Hur signalspaningen rent tekniskt skall genomföras är en verkställighetsfråga som givetvis måste ankomma på den verkställande myndigheten att fastställa. Beslutet att inom ramen för underrättelseverksamhetens inriktning använda sökbegreppen A eller B eller personnamnet C är däremot en fråga som med hänsyn till den personliga integriteten möjligen borde fastställas av en fristående oberoende myndighet, t.ex. Försvarets underrättelsenämnd. *Registernämnden* har påtalat att ett system där den myndighet som skall genomföra inhämtningen själv skall få fatta avgörande beslut om när sådan inhämtning skall ske genom att bestämma de s.k. sökbegreppen inte ter sig som rimligt vare sig från rättsäkerhetssynpunkt eller integritetsskyddssynpunkt. Den kontroll som föreslås äga rum i efterhand av Försvarets underrättelsenämnd är i avsaknad av ett system med rättssäkerhetsmässigt betryggande förhandsbeslut inte tillräcklig.

Kammarkollegiet har framfört att kollegiet anser att förhandstillstånd skall krävas, att allmänt ombud behövs för att ta till vara integritetsintresset i ärendet om tillstånd, att tillståndsgivande organ bör vara domstol eller ett domstolsliknande organ med en domare eller f.d. domare som ordförande samt att kriterierna för tillstånd bör vara fastlagda i lag. Det kan under inga omständigheter godtas att den myndighet som skall utföra signalspaningen själv skall få besluta helt eller delvis i dessa frågor eller att tillståndsfrågor skall prövas i efterhand. Det kan således inte komma i

fråga att Försvarets radioanstalt självt skall få bestämma sökbegreppen. Inte heller är det tillräckligt att Försvarets underrättelsenämnd först i efterhand skall kontrollera detta. Uppgiften passar över huvud taget inte för den nämnden med hänsyn till dess uppgifter i övrigt och sammansättning. Detta gäller även med beaktande av den föreslagna förändringen av nämnden.

Post- och telestyrelsen (PTS) har ansett att det är anmärkningsvärt att beslutet om att sökord som är direkt hänförligt till en viss fysisk person skall användas eller ej och i vilken utsträckning det i så fall skall ske bestäms självständigt av den organisation som utför avlyssningen. Att de angivna sökorden i efterhand kan granskas och kontrolleras av ett kontrollorgan påverkar inte PTS uppfattning. Vid en jämförelse med hemlig teleavlyssning och hemlig teleövervakning där det ansetts nödvändigt ur rättssäkerhetssynpunkt att varje avlyssning skall beslutas av en domstol med närvaro av ett särskilt ombud som skall tillvarata den berörde individens rättigheter torde de skyddsmekanismer som föreslås omgärda spaning i tråd anses vara mycket små.

Försvarets radioanstalt har poängterat att sökbegrepp med hög precision måste användas för att reducera risken för omotiverade intrång i den personliga integriteten.

Skälen för regeringens förslag och bedömning

Automatiserad inhämtning

Av den inledande redogörelsen för teknikutvecklingen har framgått att det är en oerhörd mängd trafik som förmedlas genom signaler i elektronisk form. För att inhämtning av signaler som är av relevans för signalspaningsverksamheten skall kunna ske på ett rationellt sätt måste den så gott som uteslutande ske automatiserat med hjälp av datorer. Manuell inhämtning är en betydligt mer resurskrävande metod som dessutom medför ökade risker för intrång i den personliga integriteten. När det gäller inhämtning av signaler i tråd finns varken något behov av eller någon praktisk möjlighet att bedriva manuell inhämtning. Av lagen bör därför framgå att inhämtning av sådana signaler skall ske automatiserat. I fråga om inhämtning i etern finns dock ett visst behov av att kunna bedriva manuell inhämtning, främst avseende traditionell militär radiokommunikation. Även om inhämtning i etern också huvudsakligen kommer att bedrivas automatiserat kan därför inte motsvarande begränsning uppställas beträffande sådan inhämtning.

Automatiserad inhämtning skulle i teorin kunna äga rum genom att all förekommande trafik inhämtas och lagras för senare bearbetning. Detta skulle dock innebära ett oproportionerligt intrång i den personliga integriteten. En sådan ordning skulle också ställa närmast orealistiska krav på kapacitet för lagring av information som endast till en ytterst begränsad del är av relevans för signalspaningsverksamheten. Inhämtning skall därför endast få ske av signaler genom urval som redan på förhand säkerställer att inhämtning endast sker av information som kan ha betydelse för verksamheten.

En metod för att åstadkomma en rimlig avgränsning är att begränsa den automatiserade inhämtningen till signaler som kan identifieras ge-

nom sökbegrepp. Genom att ange sökbegrepp kan man söka igenom en signal och hitta de poster eller uppgiftskonstellationer där begreppet förekommer. Detta innebär att endast en i förhållande till den totala kommunikationsvolymen ytterligt begränsad mängd information inhämtas och hanteras vidare av myndigheten. Den metoden används redan i dag i Försvarets radioanstalts signalspaningsverksamhet.

För att undvika att irrelevant information inhämtas måste sökbegrepp med hög precision användas. Den höga precisionen i sökbegreppen medför i sin tur att flera enskilda sökparametrar måste användas än om ett färre antal bredare och mer diffusa sökbegrepp utnyttjades. Antalet sökbegrepp som används inom signalspaningen är därför mycket stort. En viktig anledning till detta är också Försvarets radioanstalts omfattande arbetsuppgifter och den mångfacetterade inriktning som erhålls från de olika uppdragsgivarna. En annan anledning är de stora trafikvolymerna.

Att sökbegreppen utformas med hög precision är, såsom *Försvarets radioanstalt* påpekat, viktigt i syfte att reducera risken för omotiverade intrång i den personliga integriteten. Med ökad precision ökar också träffsäkerheten i urvalet och risken minskar för att irrelevant sidoinformation inhämtas och slutligen blir tillgänglig för ett mänskligt öga eller öra. Den dynamik som omgärdar signalspaningen gör dessutom att sökbegreppen ofta måste förändras. I takt med att en företeelse av betydelse för försvarsunderrättelseverksamheten kartläggs erhålls ny information som kan läggas till grund för utformandet av nya sökbegrepp med än större precision.

Utformningen av sökbegrepp för automatiserad inhämtning styrs av ändamålen för verksamheten såsom de angivits i lagen och inriktningen av verksamheten. Den närmare utformningen av sökbegrepp sker bl.a. genom väl avvägda kombinationer av teknisk data (såsom varifrån i världen signalerna inhämtas och med vilka transmissionsmedel de förmedlas) samt andra parametrar som nyckelord (t.ex. det särskilda namnet på ett vapensystem eller annan teknisk terminologi) och unika namn och språk.

Fastställande av sökbegrepp

För att kunna fastställa de sökbegrepp som begränsar inhämtningen till relevanta signaler krävs omfattande kunskap om den verksamhet som bedrivs hos Försvarets radioanstalt. Eftersom verksamheten ständigt måste anpassas efter utvecklingen kan sökbegreppen inte vara statiska utan måste kunna fastställas eller ändras fortlöpande, vilket i händelse av oförutsedda händelser i omvärlden måste kunna göras med största skyndsamhet. Hanteringen av sökbegreppen måste också tillgodose mycket högt ställda säkerhetskrav. De angivna kraven innebär att uppgiften inte utan stora svårigheter kan anförtros ett från myndigheten fristående organ på det sätt som flera remissinstanser förordat.

Av det sagda följer också att ett system med tillstånd till eller förhandskontroll av utnyttjande av enskilda sökbegrepp är förknippat med stora praktiska problem. Som flera remissinstanser har anfört bör det dock inte finnas möjlighet för den myndighet som skall utföra signalspaningen att fritt bestämma om denna. Någon form av förhandskontroll bör finnas. Förhandskontrollen bör enligt regeringens uppfattning dock om-

fatta inriktningarna av verksamheten, medan utformningen av sökbegreppen bör betraktas som en praktisk fråga om verkställighet av de inriktningar som ges för verksamheten. Regeringen återkommer i avsnitt 7.4.3 till denna fråga.

Fastställandet av sökbegreppen är en komplicerad uppgift som har stor betydelse för hur Försvarets radioanstalts verksamhet bedrivs. Det är därför viktigt att myndigheten har en väl fungerande rutin för fastställande och hantering av sökbegreppen. Denna rutin regleras lämpligen i myndighetens arbetsordning. Hur besluten om fastställande av sökbegrepp närmare utformas är beroende av karaktären på de uppgifter som skall inhämtas.

Även om fastställandet av sökbegreppen i allt väsentligt handlar om att på ett effektivt sätt verkställa inhämtning inom ramen för givna inriktningar, är naturligtvis fastställandet i sig en verksamhet som kräver överväganden i fråga hur enskildas integritetsskydd skall tillgodoses. Regeringen föreslår därför vissa begränsningar när det gäller utformningen av sökbegreppen, se avsnitt 7.4.2.

I syfte att säkerställa att de interna rutinerna vid Försvarets radioanstalt utformas på ett sätt som motsvarar högt ställda krav på integritetsskydd bör enligt regeringens bedömning också inrättas ett integritetsskyddsråd vid myndigheten. Rådet, vars ledamöter utses av regeringen, bör ha till uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten. Rådet bör få tillgång till all den information som behövs för att det skall kunna fullgöra sin uppgift. De närmare bestämmelser om rådets verksamhet som behövs bör meddelas i Försvarets radioanstalts instruktion.

Vid sidan av ett internt system för att säkerställa att hanteringen av sökbegreppen sker enligt tydliga och fasta riktlinjer finns också ett behov av utomstående efterhandskontroll av myndighetens hantering. Sökbegreppen skall därför fortlöpande redovisas för och granskas i särskild ordning av den myndighet som regeringen bestämmer (Försvarets underrättelsenämnd), se vidare om kontrollfunktionen i avsnitt 8. Därigenom säkerställs att en god utomstående kontroll kommer att ske av sökbegreppen. Inrättandet av ett integritetsskyddsråd inom Försvarets radioanstalt innebär inte att omfattningen av Försvarets underrättelsenämnds föreskrivna kontrolluppgift förändras.

7.3.5 Inriktning, rapportering och internationellt samarbete

Regeringens förslag: Signalspaningsverksamhet som bedrivs i syfte att utveckla signalspaningsmyndighetens inhämtningsförmåga skall inriktas av regeringen.

Inriktning som avser signalspaning i försvarsunderrättelseverksamheten skall inte få avse endast en viss fysisk person.

Rapportering av underrättelser skall ske enligt vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet.

Den myndighet som regeringen bestämmer får samarbeta med andra länder och organisationer för att kunna följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt

fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: Remissinstanserna tillstyrker förslagen i promemorian eller lämnar dem utan erinran.

Skälen för regeringens förslag

Inriktning av verksamheten

I 1 § andra stycket lagen om försvarsunderrättelseverksamhet anges att försvarsunderrättelseverksamhetens inriktning bestäms av regeringen. Den styrning som regeringen utövar med stöd av denna bestämmelse rör den övergripande inriktningen av verksamheten till stöd för utrikes-, säkerhets- och försvarspolitiken samt i övrigt för att kartlägga yttre hot mot landet och i fråga om medverkan i svenskt deltagande i internationellt säkerhetssamarbete. Detta görs årligen i regeringsbeslut om inriktning och i myndigheternas regleringsbrev. Enligt förslaget till ändring i lagen om försvarsunderrättelseverksamhet kan försvarsunderrättelseverksamheten också, inom ramen för regeringens övergripande inriktning, ges närmare inriktning av de myndigheter som regeringen bestämmer (se avsnitt 6.4). Bestämmelserna om inriktning gäller också för signalspaningsverksamheten. I lagen om signalspaning i försvarsunderrättelseverksamhet skall därför tas in en erinran om denna bestämmelse.

Förutom i den verksamhet som anges i lagen om försvarsunderrättelseverksamhet får signalspaningsverksamheten enligt vad som angetts i avsnitt 7.3.2. också bedrivas för att följa förändringen i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt att fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten. Även denna verksamhet bör inriktas av regeringen. Eftersom denna verksamhet syftar till att tillgodose Försvarets radioanstalts eget behov av att följa den tekniska utvecklingen saknas däremot anledning att ge andra myndigheter möjlighet att inrikta också den signalspaning som bedrivs för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Av de syften för vilken försvarsunderrättelseverksamheten får bedrivas och de begränsningar som anges i olika bestämmelser framgår att en inriktning skall gälla en företeelse och inte endast en viss fysisk person. Denna begränsning bör ändå klargöras för att undvika tveksamhet om för vilka uppgifter andra myndigheter kan använda signalspaningsresursen.

Begränsningen såvitt avser en viss fysisk person innebär att en inriktning inte får ha till syfte att endast kartlägga en utpekad person. Naturligtvis måste dock signalspaningen ibland beröra enskildas kommunikationer för att det skall vara möjligt att kartlägga en viss företeelse av relevans för verksamheten. Vid sådan kartläggning kan det vara nödvändigt att utnyttja information om fysiska personer som en utgångspunkt för vidare inhämtning. De begränsningar som gäller för i vilken utsträckning uppgifter som är hänförliga till fysiska personer i sådana sammanhang får användas som sökbegrepp behandlas i avsnitt 7.4.2.

Rapportering av underrättelser

Enligt förslaget till ändring i lagen om försvarsunderrättelseverksamhet skall rapportering av underrättelser ske till berörda myndigheter. Sådana myndigheter kan, utöver Regeringskansliet, vara t.ex. Försvarsmakten, Rikspolisstyrelsen (Säkerhetspolisen), Tullverket och Krisberedskapsmyndigheten. Bestämmelserna om rapportering gäller även underrättelser som erhållits genom signalspaning och en erinran om detta bör tas in i lagen om signalspaning i försvarsunderrättelseverksamhet. Nödvändiga begränsningar av rapporteringen behandlas i avsnitt 7.4.4.

Den signalspaning som sker för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, syftar till att tillgodose myndighetens egna behov och resulterar följaktligen inte i några underrättelser. Den omfattas därför inte av rapporteringsbestämmelsen.

Internationellt samarbete

Enligt lagen om försvarsunderrättelseverksamhet får den eller de myndigheter som bedriver försvarsunderrättelseverksamhet, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer. Samma skäl som gäller för behovet av möjligheten till internationellt samarbete på försvarsunderrättelseområdet gäller även för den information som inhämtas för att Försvarets radioanstalt skall kunna följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten. En bestämmelse med motsvarande innehåll föreslås därför även när det gäller sådan signalspaningsverksamhet.

7.3.6 Reglering av tillgången till signaler i tråd

Teknik för elektronisk kommunikation

Elektronisk kommunikation innebär överföring av signaler i elektronisk form. Signalerna bygger på data i analog eller digital form som kan överföras via elektromagnetiska svängningar. Innehållet i data är t.ex. text, ljud eller bild, eller kombinationer av dessa.

Elektronisk kommunikation omfattar telefoni, datakommunikation samt radio och TV (medier). En tydlig trend är att dessa tre sektorer gradvis växer samman genom den så kallade konvergensen. Konvergensen sker inom infrastruktur-, tjänste- och utrustningsområdena. Den har sin grund framförallt i digitaliseringen och i den standardisering som skett på Internetområdet. Utvecklingen på området för elektronisk kommunikation innebär att infrastrukturer och tekniker för överföring av kommunikation och tjänster smälter samman. Denna utveckling gör det exempelvis möjligt att telefonera via datorn, använda Internet via TV:n och se på TV i mobiltelefonen (prop. 2002/03:110 s. 58).

Via elektroniska kommunikationsnät befordras ständigt en ofantlig mängd information. Där förmedlas bl.a. telefonsamtal, telefaxmeddelan-

den, elektronisk post, datakommunikation och annan kommunikation som innehåller meddelanden

När det gäller så kallad fast telefoni har alla företag och hushåll som så vill i dag tillgång till analog taltelefoni. Även digital anslutning i form av ISDN (*Integrated Services Digital Network*) används för telefoni.

Dagens mobiltelefoni är till stor del en taltelefonitjänst. Nya tjänster och tekniker som SMS (*Short Message Service*) och WAP (*Wireless Application Protocol*) medger dock överföring av text samt webbliknande innehåll. GSM-näten har sedan sitt införande utvecklats tekniskt med bl.a. GPRS-teknik (*General Packet Radio Service*) och fått högre överföringskapacitet, vilket möjliggör nya tillämpningar och tjänster med större informationsinnehåll. Den tredje generationens system för mobil kommunikation, UMTS (*Universal Mobile Telecommunications System*), innebär att överföringskapaciteten ökar ytterligare.

De nationella stomnäten, dvs. rikstäckande allmänt tillgängliga nät som förbinder nationella noder och huvudnoder i landets olika delar med varandra, är främst baserade på optiska fiberkablar men även till en viss del radiolänk. Ortssammanbindande nät förbinder olika orter med varandra samt med huvudnoderna i nätet. Områdesnäten är spridningsnät som sammanbinder fastighetsnäten i en ort eller ett geografiskt avgränsat område med det ortssammanbindande nätet. I områdesnät kan även inräknas de nät som ofta benämns accessnät. En möjlighet till trådlös access med hög överföringskapacitet är fast yttäckande radioaccess som används för sändningar av datakommunikation, t.ex. LMDS (*Local Multipoint Distribution Service*). Även elnäten kan användas för elektronisk kommunikation, så kallad *Power Line Communication* (PLC). Därutöver används också uppgraderade telefonnät, satellit samt marknätet för digital-TV för datakommunikation. Leverantörerna är många, ofta små, och inriktar sig i hög grad på olika nischer och delsegment av marknaden där de erbjuder olika typer av anslutningsformer. De flesta erbjuder traditionella uppringda anslutningar över det vanliga metallbaserade accessnätet. Även kabel-TV-operatörer erbjuder anslutning till Internet via sina kabelnät, medan andra erbjuder anslutning till Internet med hög överföringskapacitet via fastighetsnät – LAN (*Local Area Network*) – framför allt i flerbostadshus. Det är Internet som i första hand driver fram nya typer av tjänster och skapar förutsättningar för ytterligare konvergens inom området. Det är främst användningen av telefon och TV som har minskat som en följd av den ökade Internetanvändningen.

Lagen om elektronisk kommunikation

Telelagen (1993:597) infördes i samband med att verksamheten i Televerket överfördes till Telia AB. Vissa av bestämmelserna i telelagen skulle enligt regeringen utgöra en huvudsaklig motsvarighet till vad som gällde enligt sekretesslagen för Televerkets verksamhet (se prop. 1992/93:200 s. 162 ff.).

År 2000 presenterade EG-kommissionen ett förslag till nytt regelverk för elektronisk kommunikation i syfte att modernisera gemenskapens lagstiftning på området. Förslaget lades fram mot bakgrund av den snabba tekniska och marknadsmässiga utvecklingen. Kommissionens förslag behandlades av Europaparlamentet och rådet. Det regelverk som senare

beslutades omfattar flera direktiv, bl.a. direktivet (2002/21/EG) om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet), direktivet (2002/20/EG) om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektivet), direktivet (2002/19/EG) om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter (tillträdesdirektivet), direktivet (2002/22/EG) om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster (USO-direktivet) och direktivet (2002/58/EG) om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

För att genomföra EG-direktiven tillkallades under år 2001 en utredning, e-komutredningen. På grundval av utredningens arbete infördes lagen (2003:389) om elektronisk kommunikation, LEK. Lagen ersatte i juli 2003 telelagen och lagen (1993:599) om radiokommunikation.

E-komutredningen angav i sitt betänkande Lag om elektronisk kommunikation (SOU 2002:60 s. 267) att elektronisk kommunikation ofta används som en samlande benämning på den verksamhet som bedrivs inom det nya område som växer fram mot bakgrund bl.a. av konvergensutvecklingen och Internet och att en sådan beskrivning inte är speciellt klargörande. E-komutredningen ansåg att begreppet elektronisk kommunikation behövde konkretiseras ytterligare men konstaterade också att varken ramdirektivet eller de s.k. särdirektiven innehåller någon definition av begreppet. Däremot definieras vad som menas med elektroniska kommunikationsnät och elektroniska kommunikationstjänster i ramdirektivet.

Lagen om elektronisk kommunikation gäller elektroniska kommunikationsnät och kommunikationstjänster med tillhörande installationer och tjänster samt annan radioanvändning. I 1 kap. 7 § LEK definieras elektroniskt kommunikationsnät som system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs. Enligt samma bestämmelse avses med elektronisk kommunikationstjänst en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät.

Till skillnad från telelagen är den nya lagen tillämplig inte endast på telefoni och datakommunikation utan även på utsändningar till allmänheten av program i ljudradio och TV. Riksdagen har i samband med att lagen om elektronisk kommunikation antogs beslutat om nya mål för sektorn elektronisk kommunikation. Enligt riksdagens beslut är målen att enskilda och myndigheter skall få tillgång till effektiva och säkra elektroniska kommunikationer med största möjliga utbyte när det gäller urvalet av överföringstjänster samt deras pris och kvalitet. Sverige skall i ett internationellt perspektiv ligga i framkanten i dessa avseenden (prop. 2002/03:110 s. 9 och 101 f. och bet. 2002/03:TU6 s. 6).

Vissa bestämmelser i LEK knyter an till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. Enligt 6 kap. 19 § LEK skall en verksamhet bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte

röjs. Innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden skall göras tillgängliga så att informationen enkelt kan tas om hand. Med detta avses den så kallade anpassningsskyldigheten.

7.3.7 Nya regler för att möjliggöra inhämtning

Regeringens förslag: De trådägande operatörerna skall till särskilda samverkanspunkter överföra all trafik som förs över Sveriges gräns.

Samverkanspunkter väljs av de trådägande operatörerna och skall anmälas av dem till den myndighet som regeringen bestämmer.

Samtliga operatörer som för signaler i tråd över Sveriges gräns skall lämna sådan information de innehar som gör det enklare att ta hand om signalerna.

Regeringen eller tillsynsmyndigheten enligt lagen (2003:389) om elektronisk kommunikation får meddela föreskrifter om samverkanspunkter.

Samtliga operatörer skall utföra uppgiften så att verksamheten inte röjs.

Tystnadsplikt för samtliga operatörer skall gälla för uppgift som hänför sig till angelägenhet som avser inhämtning av signaler i elektronisk form enligt förslaget till lag om signalspaning i försvarsunderrättelseverksamhet.

Promemorians förslag överensstämmer i huvudsak med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslagen eller lämnar dem utan erinran. *Post- och telestyrelsen* (PTS) har instämt med promemorian om lämpligheten av att i så stor utsträckning som möjligt begränsa antalet operatörer som omfattas av skyldigheter att möjliggöra inhämtning. PTS är dock tveksam till var promemorian egentligen avser dra denna gräns. I flera fall ägs kommunikationsnätet av ett bolag vars enda verksamhet utgörs av uthyrning av s.k. svart fiber, dvs. ett helt oförädlat nät. De operatörer som nyttjar sådana nät förfogar förvisso över detta nät och torde i praktiken tillföra all väsentlig teknik till nätet, men kan knappast sägas äga tråden. Lagförslaget kan därmed komma att träffa aktörer som i praktiken inte tillhandahåller några förädlade kommunikationsnät eller tjänster. Det ter sig enligt PTS uppfattning mindre rimligt att en förhållandevis liten operatör skall föreläggas att anpassa sin verksamhet för miljonbelopp endast för att den operatören t.ex. har verksamhet i ett ytterligare land och därigenom även äger kommunikationsnät mellan dessa länder. Enligt PTS uppfattning är bakgrunden till föreskriftsrätten oklar och det är otydligt på vilket sätt föreskrifterna skall fylla ut lagstiftningen.

Justitiekanslern och Tryck- och yttrandefrihetsberedningen har påpekat att tystnadsplikten enligt 6 kap. 21 § lagen (2003:389) om elektronisk kommunikation är upptagen bland de kvalificerade tystnadsplikterna som räknas upp i 16 kap. sekretesslagen (1980:100) och som har försteg framför meddelarfriheten (jfr. 7 kap. 3 § tryckfrihetsförordningen). Om avsikten är att även den nya tystnadsplikten som avses gälla för uppgifter som inhämtas genom signalspaning skall vara av kvalificerad art och sålunda bryta meddelarfriheten, krävs ett tillägg i 16 kap 1 § 9 sekretesslagen.

Skälen för regeringens förslag

Trådägande operatörers skyldigheter

Förslaget till lag om signalspaning i försvarsunderrättelseverksamhet ger möjlighet för signalspaningsmyndigheten att inhämta signaler både i etern och i tråd (kabel). För att inhämtning av signaler i elektronisk form vid signalspaning skall vara möjlig krävs att operatörerna medverkar till detta. Med operatör avses enligt 1 kap. 7 § LEK den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation. Det finns ett antal operatörer som äger tråd (i 1 kap. 7 § LEK anges att överföring av signaler kan ske bl.a. via tråd). Verksamheterna bedrivs på många håll i landet. För att signalspaningsmyndigheten skall kunna ta emot signalerna krävs givetvis att dessa överförs dit. Av övervägandena i avsnitt 7.3.3 framgår att inhämtning av signaler i tråd endast skall avse signaler vilka förs över Sveriges gräns.

De trådägande operatörerna föreslås därför föra all trafik som förs över Sveriges gräns till särskilda samverkanspunkter (se nedan). *Post- och telestyrelsen* har anfört att det är oklart vilka operatörer som omfattas av promemorians lagförslag. Uttrycket ”äger tråd” avser att peka ut att skyldigheten att överföra signalerna till samverkanspunkter avser just de trådägande operatörerna. Detta får till följd att skyldigheten omfattar både sådana trådägare som endast äger s.k. svartfiber och sådana trådägare som tillhandahåller förädlade kommunikationsnät. Trafiken kan bestå av såväl egen som andra operatörers trafik. En trådägare kan exempelvis hyra ut hela eller delar av sin tråd till andra operatörer eller förmedla andra operatörers trafik.

Antalet trådägande operatörer vars tråd korsar riket gräns är litet (ett tiotal) i förhållande till antalet andra operatörer (t.ex. *Internet Service Providers*), dvs. det är bara ett fåtal operatörer som träffas av skyldigheten. De icke trådägande operatörerna varierar mer i antal över tiden och det är därför inte rimligt att en ständig samverkan kring överföringen skall ske med alla dessa. Om skyldigheten att överföra trafik skulle gälla för alla typer av operatörer skulle – med hänsyn till såväl tekniska som administrativa aspekter – en orimlig och samhällsekonomisk mycket kostsam situation uppstå. Ytterligare en fördel med att endast trådägare i vars tråd trafik förs över Sveriges gräns skall ha skyldigheten att överföra trafik till samverkanspunkterna är att verkställigheten i ett tekniskt avseende endast behöver genomföras vid ett fåtal tillfällen, dvs. när lagen träder i kraft och därefter när nya trådägare tillkommer. Skyldigheten att överföra trafiken till samverkanspunkter skall därför endast gälla för trådägaren.

Vad är en samverkanspunkt?

En samverkanspunkt är den plats där trafiken överlämnas från den trådägande operatören till myndigheten. Operatören har ansvaret för att trafiken förs till samverkanspunkten, som också väljs av operatören. Operatören kan därmed välja en för denne lämplig och kostnadseffektiv plats för samverkanspunkten. Operatören har dock inget ansvar för att samverkanspunkten uppförs och svarar inte heller för några kostnader för denna.

Från samverkanspunkterna har myndigheten ansvar för att överföra signalerna till sina system. Detta innebär att myndigheten inte kan hållas ansvarig för eventuella störningar i trådägande operatörers system och att operatörerna inte får kännedom om vilka signaler som myndigheten är intresserad av. Operatörerna bär kostnaderna för att signalerna förs till samverkanspunkter som de valt och därefter har signalspaningsmyndigheten det totala kostnadsansvaret. Signalspaningsmyndigheten skall således, utöver att bygga upp samverkanspunkter, svara för kostnaderna för uppsättande och drift av nödvändig utrustning vid samverkanspunkterna.

De samverkanspunkter som de trådägande operatörerna valt ut, skall anmälas till den myndighet som regeringen bestämmer. Som framgår av avsnitt 7.3.1 avser regeringen att i förordning peka ut Försvarets radioanstalt för denna verksamhet. I Sverige finns ett antal anläggningar i en säker miljö där de flesta av dessa operatörer bedriver verksamhet. Det är därför lämpligt att sådana operatörer förlägger samverkanspunkterna i dessa anläggningar. Vissa operatörer har dock ingen verksamhet i anläggningarna och kan därför inte förväntas anmäla samverkanspunkter där. För dessa operatörer är det rimligt att de anmäler punkter som är belägna på platser med motsvarande säkerhetsnivå som operatörer har i sina nät i övrigt för säkra trafikpunkter. Om det motiveras av ett påtagligt behov hos operatören, kan denne anmäla en ny plats för samverkanspunkten.

Regeringen ser att det kan komma att finnas behov av att det utfärdas föreskrifter på området. I lagen bör därför införas en bestämmelse om att regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om samverkanspunkter. Dessa kan innefatta generella krav på antal och belägenhet i förhållande till trafikmängd, säkerhet som motsvarar operatörernas säkerhet för sina trafikpunkter, förutsättningar för byte av samverkanspunkt och åtkomlighet för myndigheten. Föreskrifterna skall utformas med utgångspunkt i att operatörernas verksamhet påverkas så lite som möjligt, men samtidigt så att Försvarets radioanstalts kostnader för att upprätta och driva nödvändig utrustning vid samverkanspunkterna hålls på en rimlig nivå. Ytterligare beskrivning kring kostnadsaspekter finns i avsnitt 10.

Hur skall signalerna enkelt kunna tas om hand?

Utöver vad som gäller för operatörer som äger tråd föreslås alla operatörer som för signaler över landets gräns vara skyldiga att se till att signalerna enkelt kan tas om hand av myndigheten (Försvarets radioanstalt), vilket sker efter begäran från myndigheten. Med operatör avses den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation (se 1 kap. 7 § LEK). Detta gäller således trådägare, *Internet Service Providers* (ISP) m.fl.

För att en ändamålsenlig signalspaning skall kunna ske måste signaler i elektronisk form enkelt kunna tas om hand av myndigheten, vilket bl.a. betyder att datareduktion behöver genomförs. Detta innebär att huvuddelen av de levererade signalerna sållas bort. För att myndigheten skall kunna göra detta behövs vissa ingångsvärden från operatörerna, dvs. även från sådana operatörer som inte äger tråd. Dessa ingångsvärden kan exempelvis bestå av förbindelsernas benämning, arkitektur, bandbredd,

riktning, typ av signalering, vilka som hyr förbindelser av operatören m.m., dock inte detaljuppgifter om speciella skydd för konfidentialitet som operatörerna exklusivt tillhandahåller slutkunder. Uppgifterna behövs också för myndighetens vidare förädling av informationen. Den information som skall överföras till Försvarets radioanstalt är sådan som operatörerna redan har i sina system. Någon skyldighet för operatörerna att anpassa denna information skall inte föreskrivas. För att signalerna enkelt skall kunna tas om hand skall operatörerna informera om kommande förändringar i sina system för att myndigheten i god tid skall kunna förbereda sig. Med god tid avses den tid som operatören normalt använder för att besluta om ändring i sitt nät.

Röjandeförbud och tystnadsplikt

Operatören skall – oavsett om denne är trådägare eller inte (jfr. 6 kap. 19 a § tredje stycket LEK) – utföra uppgiften enligt den föreslagna bestämmelsen så att verksamheten inte röjs.

I 6 kap. 21 § LEK finns regler om tystnadsplikt för operatörerna vad gäller angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken. Liknande regler fanns tidigare i telelagen och överfördes med endast mindre ändringar till LEK (jfr prop. 2002/03:110 . 271 f.).

Även om den underrättelseinhämtning som Försvarets radioanstalt bedriver i många betydelsefulla avseenden skiljer sig från de brottsbekämpande myndigheternas verksamhet, är det av avgörande betydelse för Försvarets radioanstalts verksamhet att motsvarande regler som gäller vid hemlig teleavlyssning och hemlig teleövervakning i fråga om röjandeförbud och tystnadsplikt även kommer att gälla för angelägenhet som avser inhämtning av signaler i elektronisk form vid signalspaning. Ett sådant tillägg bör därför införas i 6 kap. 21 § LEK.

Tystnadsplikten enligt 6 kap. 21 § LEK finns upptagen bland de meddelandefrihetsbrytande tystnadsplikterna i 16 kap. 1 § 9 sekretesslagen. Regeringen anser att det, med hänsyn till att de uppgifter som rör signalspaning inte direkt kan röja mot vem eller vilka verksamheten riktas, saknas anledning att införa motsvarande regler avseende inhämtning av signaler i elektronisk form vid signalspaning.

7.4 Regeringsformens och Europakonventionens krav på en reglering om utvidgad signalspaning

I föregående avsnitt har redovisats vilka anpassningar av regelverket som krävs för att få till stånd en signalspaningsverksamhet som på ett effektivt sätt kan tillgodose samhällets underrättelsebehov. I detta avsnitt behandlas de kompletterande bestämmelser som behövs för att regelverket skall tillgodose de krav som regeringsformen, andra grundlagar och Europakonventionen ställer och som presenterats i avsnitt 7.2.

7.4.1 Rättighetsskyddsgarantier – utgångspunkter

En utvidgning av möjligheten att signalspana innebär att mer kommunikation än tidigare kan bli föremål för signalspaning. Många människor kan därmed komma att utsättas för sådant intrång i den personliga integriteten som verksamheten innefattar, i synnerhet som alltmer av den enskildes kommunikation sker i det globala nätet. De bestämmelser i regeringsformen till skydd mot intrång i enskildas personliga integritet som redovisats i avsnitt 7.2. gäller, såvida inte annat är föreskrivet, inte bara svenska medborgare utan också andra som befinner sig i Sverige (2 kap. 22 § andra stycket 3 regeringsformen). Inte heller Europakonventionens rättighetsskydd är begränsat till konventionsstaternas medborgare, utan gäller enligt artikel 1 i konventionen var och en som befinner sig under en sådan stats jurisdiktion.

Oavsett tillämpningsområdet för de aktuella regelverken saknas dessutom sakliga skäl för att i fråga om integritetsskydd göra åtskillnad på personer beroende på medborgarskap eller i vilket land de vistas. Vid bedömningen av vilka bestämmelser som behövs för att lagen om signalspaning i försvarsunderrättelseverksamhet skall uppfylla kraven på tillräckligt skydd för enskilda bör därför svenska medborgare och medborgare i andra länder behandlas lika.

Som framgår av redogörelsen i avsnitt 7.2 uppvisar regeringsformen och Europakonventionen likheter när det gäller skyddet för den privata sfären. Detta har sin förklaring bl.a. i att grundlagsbestämmelserna har utformats med hänsyn tagen till konventionens bestämmelser. Konventionen anses kräva, förutom lagform, att inskränkningarna är förutsebara i viss utsträckning. Enskilda skall skyddas mot godtyckliga ingrepp inom ramen för det tolkningsutrymme som lämnas nationella myndigheter. Om en rättighetsinskränkning är nödvändig anses staten ha en viss frihet att bestämma tolkningsutrymmet. Denna frihet står i relation till behovet av inskränkningen på så sätt att ju angelägnare statens intresse är desto större anses tolkningsutrymmet vara. Inskränkningen av en rättighet måste dock alltid stå i proportion till syftet med begränsningen.

Inhämtning av signaler i elektronisk form som sänds i tråd och som innefattar kommunikationer mellan enskilda innebär ett ingrepp i den privata sfär som skyddas av både 2 kap. 6 § regeringsformen och artikel 8 i Europakonventionen. Skyddet är inte absolut utan kan i princip brytas igenom när syftet bl.a. är att skydda en stats säkerhet. En avvägning måste dock ske mellan behovet av sådana åtgärder och integritetsskyddsintresset. Som tidigare påpekats (se särskilt avsnitt 7.3.1) finns det ett angeläget behov av en utvidgad möjlighet till signalspaning för att tillgodose nödvändiga underrättelsebehov. Det saknas andra metoder för underrättelseinhämtning som har förutsättningar att mäta sig med signalspaningen när det gäller effektivitet och praktiskt värde. Som företeelse får alltså signalspaning anses i princip acceptabel förutsatt att den inskränkning av rättighetsskyddet som uppkommer står i rimlig proportion till det syfte som skall uppnås genom förfarandet. Tillämpningsområdet blir därmed av stor betydelse, liksom rättighetsskyddsgarantierna.

En första fråga blir då när det intrång i den privata sfären som signalspaningen medför rent faktiskt kan sägas äga rum. Skyddet för integriteten avser innehållet i de meddelanden som utväxlas liksom uppgifter om

vilka som kommunicerar med varandra samt när och hur detta sker. Det är följaktligen först när en myndighet kan ta del av sådan information som ett integritetsintrång sker.

Som beskrivits i avsnitt 7.3.4 kommer signalspaning med stöd av det utvidgade mandatet i allt väsentligt att ske automatiserat med hjälp av sökbegrepp. När det gäller inhämtning i tråd är detta den enda föreskrivna inhämtningsmetoden. Det innebär att inhämtningen endast avser en mycket begränsad del av den totala trafikvolymen. De signaler som inte sorteras ut genom sökbegreppen lagras inte utan försvinner och är inte åtkomliga för myndigheten. Tydligast illustreras detta av trådburen trafik. Denna består till övervägande del av signaler i form av rent ljus. Ljuset är bärare av data (ettor och nollor). Först när ljuset fångas in och lagras i ett datasystem går det att hantera ljuset och söka ut information. Det ljus som inte hanteras på detta sätt försvinner och är därmed borta.

Av ovanstående följer att något integritetsintrång inte kan anses äga rum redan då Försvarets radioanstalt får tillgång till kommunikationsvägarna. Det är först när vissa signaler med datorhjälp, och utan möjlighet för myndigheten att dessförinnan ta del av innehållet, lagrats och därmed blivit tillgängliga för vidare bearbetning som ett integritetsintrång uppstår.

Ovanstående resonemang är även tillämpligt på sådan inhämtning i etern av signaler i elektronisk form som sker med automatiserad behandling. Den inhämtning i etern som sker manuellt är av begränsad omfattning och avser trafik (huvudsakligen militär radiokommunikation) beträffande vilken integritetsaspekterna inte gör sig gällande på samma sätt som i fråga om kommunikation mellan enskilda.

Sammanfattningsvis kan alltså konstateras att, såvitt gäller den sfär som skyddas av regeringsformen och Europakonventionen, automatiserad inhämtning av uppgifter vid signalspaning inte kommer att avse alla de meddelanden som sänds i etern eller i tråd, utan kommer att inskränkas till meddelanden som väljs ut genom sökbegrepp på det sätt som beskrivits i avsnitt 7.3.4. En viktig omständighet är också att signalspaning i försvarsunderrättelseverksamhet endast får bedrivas beträffande utländska förhållanden. Ur integritetsskyddssynpunkt förtjänar också att framhållas att inom verksamheten skall inte få vidtas åtgärder som syftar till att lösa uppgifter som enligt lagar och andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet (se avsnitt 6.3.2).

7.4.2 Reglering av användningen av sökbegrepp

Regeringens förslag: Sökbegrepp skall utformas och användas så att de medför ett så begränsat intrång som möjligt i den personliga integriteten. Sökbegrepp får inte vara direkt hänförliga till en viss fysisk person om det inte är av synnerlig vikt för verksamheten.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: *Post- och telestyrelsen* har anfört att det kan ifrågasättas om den tekniska funktionen av Försvarets radioanstalts signalspaning verkligen kan fungera på så sätt att det ”ljus som inte hanteras”

försvinner. *Krisberedskapsmyndigheten* har påtalat att vid stödjande insatser kring informationssäkerhet, exempelvis vid nationella kriser med IT-inslag, kan det vara av stor vikt med en skyndsam medverkan för att identifiera inblandade aktörer i IT-relaterade hot mot samhällsviktiga system. Detta innebär riktad sökning där sökbegreppen ofta är direkt relaterade till en viss fysisk person, exempelvis IP-adresser och e-postadresser.

Skälen för regeringens förslag: Såsom anförts i avsnitt 7.3.4 och 7.4.1 kommer sådan trafik som inte sorterats ut genom sökbegrepp inte att lagras utan försvinna och inte vara åtkomlig för signalspaningsmyndigheten. Myndigheten kommer inte, såsom *Post- och telestyrelsen* ifrågasatt, få tillgång till all kommunikation som sker, utan endast den som träffas av de i förväg fastställda sökbegreppen. Då all automatiserad inhämtning av signaler i elektronisk form skall ske genom användning av sökbegrepp (se avsnitt 7.3.4), kommer en ytterst liten andel av alla de personer som kommunicerar genom signaler i elektronisk form att bli föremål för inhämtning. Bakom all kommunikation ligger dock människor och det är därför ofrånkomligt att den inhämtning som regleras i lagen i enskilda fall kan komma att medföra intrång i den personliga integriteten. I dessa fall är det angeläget att signalspaningen inte inkräktar på den personliga integriteten i större utsträckning än som är absolut nödvändigt för att uppnå syftet med verksamheten. Det bör därför föreskrivas att sökbegreppen skall utformas och användas så att de medför ett så begränsat intrång som möjligt i den personliga integriteten.

För att så värdefull information som möjligt skall kunna erhållas genom signalspaningen måste inhämtningen ibland ske med hjälp av sökbegrepp som är hänförliga till en viss individ. Sådan inhämtning medför naturligtvis särskilda risker ur integritetsskyddsperspektiv och bör endast komma i fråga under speciella förutsättningar. För att säkerställa att inhämtningen har föregåtts av en grundlig behovsprövning bör det därför krävas att sökbegreppen får vara direkt hänförliga till en fysisk person endast när det är av synnerlig vikt för verksamheten. Innan ett sådant sökbegrepp används som urvalsparameter måste det alltså göras en bedömning av om den information som därigenom kan erhållas är av sådan vikt att det motiverar åtgärden.

Bestämmelsen innebär att användning av sådana sökbegrepp som exempelvis inkluderar personnamn samt telefonnummer, e-postadresser, IP-adresser etc. och som kan knytas till en fysisk person måste föregås av noggranna överväganden. Om det är av synnerlig vikt att kunna använda sökbegrepp direkt hänförliga till fysisk person får bedömas utifrån olika faktorer. Den situationen som *Krisberedskapsmyndigheten* tar upp kan vara en sådan som kräver att sökbegrepp som är direkt hänförlig till en enskild individ används (se även avsnitt 7.3.4).

Kontroll av att sökbegreppen endast används på det sätt som anges i lagen, och i synnerhet att de används på ett sätt som inte medför otillbörligt intrång i den personliga integriteten, skall vara en viktig del i den särskilda granskningen av verksamheten (se avsnitt 8).

För den begränsade inhämtning som kommer att ske med manuella metoder, dvs. traditionell signalspaning mot radiotrafik (t.ex. kortvågsspaning mot militär radiokommunikation), finns av naturliga skäl inte möjlighet att fastställa sökbegrepp. Integritetsskyddet upprätthålls här

genom föreskriften att information omedelbart skall förstöras om den saknar betydelse för verksamheten (se avsnitt 7.4.4). Även efterlevnaden av denna föreskrift är en naturlig och central del av den särskilda granskningen.

7.4.3 Tillståndsförfarande

Regeringens förslag: De myndigheter som enligt regeringens bestämmande får ge närmare inriktning för signalspaningsverksamheten, skall först få tillstånd av tillståndsmyndigheten. I brådskande fall får inriktningen ges utan tillstånd, men skall då omedelbart anmälas till tillståndsmyndigheten. Om myndigheten finner att inriktningen inte borde ha getts¨, skall signalspaningsmyndigheten underrättas och inhämtningen omedelbart avbrytas.

Ett tillstånd skall gälla i högst sex månader och skall efter förnyad prövning kunna förlängas med högst sex månader i taget.

Tillstånd får endast lämnas för inriktning som avser sådan verksamhet för vilken signalspaning får bedrivas och som är förenlig med lagen (2000:130) om försvarsunderrättelseverksamhet. Tillstånd får endast lämnas om syftet med inriktningen väger klart tyngre än det integritetsintrång som inhämtning i enlighet med inriktningen kan innebära och detta syfte inte kan tillgodoses på ett mindre ingripande sätt. Tillstånd får inte lämnas om inriktningen endast avser en viss fysisk person.

Regeringens bedömning: Försvarets underrättelsenämnd skall fullgöra uppgiften som tillståndsmyndighet. Tillståndsprövningen skall ske i en särskild avdelning inom nämnden, i vilken en ledamot med domarerfarenhet eller motsvarande juridisk kompetens skall vara ordförande.

Promemorians förslag överensstämmer i huvudsak med regeringens, men innehåller inte uttryckligen den proportionalitetsbedömning som tillståndsmyndigheten skall göra. Inte heller föreslogs i promemorian att tillstånden skall vara tidsbegränsade. I promemorian har vidare inte gjorts några överväganden i fråga om Försvarets underrättelsenämnds sammansättning vid tillståndsprövningen.

Remissinstanserna: *Säkerhetspolisen* har anfört att när Försvarets underrättelsenämnd meddelar tillstånd till närmare inriktning av Försvarets radioanstalts signalspaningsverksamhet kommer nämnden att få insyn i och i praktiken pröva bl.a. Säkerhetspolisens operativa verksamhet som ytterst gäller myndighetsutövning mot enskild och med stöd av gällande lagstiftning. Att Försvarsunderrättelsenämnden på detta sätt ges insyn i och påverkan på polisiär och annan civil verksamhet utgör enligt Säkerhetspolisens mening en från konstitutionella utgångspunkter oacceptabel lösning. Tillstånd skall istället meddelas av ett för ändamålet kompetent organ skiljt från försvarsunderrättelseverksamheten, såsom en allmän domstol.

Registernämnden har framfört att beslut om tillstånd som krävs för signalspaning mot trådburen trafik bör fattas i förväg. Det föreslagna systemet med tillstånd för inriktning innebär inte ett rättsäkerhetsmässigt betryggande system för förhandsprövning. Besluten bör fattas av en

domstol eller domstolsliknande organ med möjligheter för ett allmänt ombud att medverka. *Kammarkollegiet* har anfört att förhandstillstånd skall krävas och att sådant tillstånd skall prövas i domstol eller domstolsliknande organ med en domare eller f.d. domare som ordförande samt att kriterierna för tillstånd bör vara fastlagda i lag. *Lunds universitet* har ansett att det inte framgår tydligt av lagen om signalspaning när signalspaning får ske.

Skälen för regeringens förslag och bedömning

Generella krav på tillstånd

Vid regleringen av förutsättningarna för signalspaning är frågan om i vilken utsträckning inhämtning skall föregås av tillstånd av vitalt intresse. Det primära syftet med ett system för tillståndsgivning måste vara att säkerställa att det intrång i den personliga integriteten som signalspaning i vissa fall kan innebära bara skall få ske när viktiga intressen för det svenska samhället berörs. Ett tillståndsförfarande ger vissa garantier för att signalspaningen bedrivs inom ramen för de ändamål och förutsättningar i övrigt som gäller för verksamheten. Mot detta måste vägas att ett krav på förhandstillstånd kan innebära negativa effekter på möjligheten att snabbt rikta verksamheten mot oförutsedda företeelser som kan utgöra yttre hot mot Sverige.

Signalspaning i försvarsunderrättelseverksamhet innefattar inhämtning av information av mycket varierande karaktär, alltifrån uppgifter som helt saknar intresse ur integritetssynpunkt till kommunikation mellan enskilda. En reglering av signalspaningen måste vara utformad så att den kan tillämpas på verksamheten i hela dess bredd.

När behovet av ett särskilt tillståndskrav för signalspaning skall bedömas är det väsentligt att beakta att försvarsunderrättelseverksamhetens syfte är att förse regeringen och berörda myndigheter med underrättelser på en övergripande nivå om utländska förhållanden och att verksamheten inte innefattar några befogenheter av tvångsmedelskaraktär i förhållande till enskilda. Detta innebär bl.a. att det, till skillnad från när hemliga tvångsmedel används i brottsbekämpande verksamhet, inte handlar om att utgå från en enskild person för att kartlägga denne. Signalspaning innebär att man söker efter det i förväg okända. Det huvudsakliga syftet är inte att bekräfta befintlig kunskap eller misstanke. Inhämtning måste därför – inom ramen för de inriktningar som ges för verksamheten och som anger relevanta hotbilder – kunna inledas brett och förutsättningslöst, för att efterhand koncentreras mot relevant kommunikation. Snävt begränsade tillstånd gör att flexibiliteten och utrymmet för kontinuerlig anpassning efter ändrade förhållanden minskar. Detta innebär att det är svårt att definiera ramen för tillståndsprövning på ett sådant sätt att prövningen blir meningsfull. Det är t.ex. inte möjligt att relatera ett tillstånd till en enskild kommunikationskälla, eftersom detta måste kunna förändras under inhämtningsprocessen i takt med att helhetsbilden blir tydligare.

Av de skäl som redovisas i avsnitt 7.3.4 är det inte heller möjligt att använda de sökbegrepp som används för utsållning av relevant information som utgångspunkt för tillståndsprövning. För att av såväl kapacitetsskäl som integritetsskäl kunna avgränsa inhämtningen ur den oerhörda

mängden elektroniska signaler till det som är relevant för verksamheten, måste sökbegrepp med stor precision och detaljeringsgrad användas. Tillstånd för varje enskilt sökbegrepp skulle förutom oerhörda praktiska svårigheter, med hänsyn till det mycket stora antal sökbegrepp som används, innebära så långtgående begränsningar av möjligheten att snabbt anpassa inhämtningen efter ändrade förhållanden att verksamhetens syfte skulle förfelas. Ett tillståndskrav avseende sökbegrepp skulle framtvinga användandet av mer generella och obestämda sökbegrepp. Följden av detta blir minskad precision i inhämtningen, vilket leder till att fler människor berörs och att mer ovidkommande information inhämtas – integritetsintrånget kommer alltså att drabba fler.

En viktig aspekt att beakta är vidare att den myndighet som bedriver signalspaning i försvarsunderrättelseverksamhet inte har något eget intresse av verksamhetens resultat. Försvarets radioanstalt är en renodlat underrättelseproducerande myndighet som inte använder underrättelserna för egna behov. Utöver den yttre ram som uppställs i lagen om försvarsunderrättelseverksamhet styrs verksamheten av de inriktningar som regeringen – och enligt förslaget också berörda myndigheter – lämnar till myndigheten. Inriktningarna omsätts i underrättelseprojekt, varvid det uteslutande är beställarnas intressen som står i fokus. Försvarets radioanstalt initierar inte inhämtning om det inte föreligger en inriktning som föranleder inhämtningen. Det är följaktligen i allt väsentligt de externa inriktningarna som avgör omfattningen och avgränsningen av inhämtningen. Detta förhållande påverkar i hög grad bedömningen av om, och i förekommande fall hur, ett tillståndssystem skall utformas.

Det anförda leder enligt regeringens mening till slutsatsen att det inte är möjligt att – så som några remissinstanser förordat – utforma ett tillståndssystem efter mönster av den ordning som tillämpas när det gäller användning av hemliga tvångsmedel i brottsbekämpande verksamhet. Verksamheterna är alltför olika såväl när det gäller ändamål och syfte som formerna för bedrivandet. I den brottsbekämpande verksamheten är omfattningen förhandsbestämd såväl när det gäller person (den som är skäligen misstänkt för visst brott, 27 kap. 20 § rättegångsbalken) som ändamål (förundersökning angående särskilt angivna brott, 27 kap. 19 § rättegångsbalken) och användningen av hemliga tvångsmedel syftar till att lagföra enskilda. Signalspaning i försvarsunderrättelseverksamheten handlar däremot som angetts om att inom ramen för en inriktning söka efter på förhand okända företeelser som avser utländska förhållanden och verksamheten syftar inte till att kartlägga enskilda. Inom försvarsunderrättelseverksamheten saknas helt möjlighet att vidta andra åtgärder mot enskilda än sådana som består i renodlad informationsinhämtning. När det gäller signalspaning i försvarsunderrättelseverksamhet är dessutom de frågeställningar som aktualiseras vid en prövning inte av renodlat judiciell karaktär. Om en modell för tillståndsprövning skall införas måste den därför utformas självständigt med utgångspunkt från de speciella förutsättningar som gäller.

Internationell jämförelse

Beträffande de länder som i sin lagstiftning har infört närmare regleringar av förutsättningarna för signalspaning kan konstateras att i den ut-

sträckning krav på förhandstillstånd ställs är detta krav i regel inte generellt för all signalspaning. Vilken verksamhet som omfattas av tillståndskravet och hur dessa krav utformas varierar i hög grad. I den nederländska lagstiftningen *(Intelligence and Security Services Act* från 2002) undantas t.ex. signalspaning i etern. Signalspaning mot trådburna kommunikationer får ske efter tillstånd av den ansvarige ministern och ett tillstånd avser inte enstaka fall eller viss person, specificerade teleadresser, m.m. utan gäller all sådan spaning under en tremånadersperiod med möjlighet till förlängning.

I den australiensiska lagstiftningen (*Telecommunications Interception Act* från 1979 och *Intelligence Services Act* från 2001) regleras underrättelseorganisationen, men den innehåller inga närmare regler om underrättelseorganens olika aktiviteter t.ex. i form av signalspaning. Lagstiftningen gäller bara förhållanden utanför Australien. Om verksamheten skall riktas mot en australisk medborgare som befinner sig utomlands krävs tillstånd av ansvarig minister. Tillståndsbegäran görs av generaldirektören för myndigheten till den federala justitieministern, och kan avse viss kommunikation eller viss person och beviljas för en period om upp till 6 månader, med möjlighet att förlänga genom nytt beslut. Vid fara i dröjsmål medges generaldirektören att, i avvaktan på justitieministerns beslut om tillstånd, själv bevilja sådant tillstånd, om han förutser positivt besked på den begäran som behandlas. Myndighetschefen skall inom 3 månader efter avslutad inhämtning meddela justitieministern om åtgärden som beviljats varit verksamheten till gagn.

De brittiska underrättelse- och säkerhetstjänsternas verksamhet och inbördes ansvarsfördelning regleras i *Intelligence Services Act* från 1994. Befogenheterna för inhämtning regleras där generellt. I *Regulation of Investigatory Powers Act (RIPA)* från 2000, regleras avlyssning och inhämtning av telekommunikationer i detalj, avseende såväl underrättelse- och säkerhetsorgan som brottsbekämpande organ. Tillstånd för avlyssning och inhämtning på det egna territoriet beslutas av inrikesministern, på ansökan av myndighetschef för någon av underrättelse- och säkerhetstjänsterna, poliskårerna eller tullen. Tillstånd krävs för all avlyssning och inhämtning på brittiskt territorium. Två typer av tillstånd regleras i *RIPA*. Vid inhämtning/avlyssning mot visst känt objekt används s.k. ”line access warrant”, medan ”external warrants” används när ett särskilt objekt inte specificerats. Den sistnämnda tillståndstypen kan användas för såväl transittrafik som trafik med källa eller mål i Storbritannien. Tillståndens längd är tre månader, med möjlighet till förnyat tillstånd av samma längd eller, om ministern så specificerat, sex månader. (Ministern kan delegera tillståndsbeslut till högre tjänstemän; sådana beslut får fem dagars giltighet.).

Den tyska lagregleringen avseende inhämtning på det egna territoriet för underrättelsebehov återfinns i den särskilda lagen för landets civila underrättelsetjänst, *Bundesnachrichtendienstgesetz (BNDG*) i lagen om post- och telehemlighet från 2001 samt i lagen om elektroniska kommunikationer från 2004. Regleringen i *BNDG* avser endast underrättelsetjänst bedriven av *Bundesnachtrichtendienst (BND*) men stödjer sig i vissa avseenden på motsvarande befogenhetsregleringar för den civila säkerhetstjänsten, i författningsskyddslagen. *BNDG* medger inhämtning på det egna territoriet. Om inhämtningen innebär att post- och telehem-

lighet bryts skall chefen för BND begära tillåtelse vid det federala inrikesministeriet. Ministerns tillstånd skall underställas den s.k. G 10-kommissionnen (se avsnitt 5.3.2). Vid omedelbar fara får dock inhämtning påbörjas enligt ministerns tillstånd. Kommissionen prövar inhämtningens författningsenlighet och nödvändighet samt anger i fråga om strategisk övervakning av telekommunikationer bl.a. vilka sökbegrepp som får användas.

Den amerikanska lagstiftningen (*US Code Chapter 36*), omfattar auktorisering för samtliga berörda federala organ – *National Security Agency* (*NSA), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA) och Federal Bureau of Investigation (FBI*) – med avseende på övervakning av utländsk underrättelseverksamhet eller motsvarande. Två former av tillståndsgivning föreskrivs; normalfallet för tillståndsgivning för inhämtning i det egna landet består i ett ansökningsförfarande inför specialdomstol (med särskild andrainstansrätt och ytterst hänvändelse till högsta domstolen). Federal tjänsteman ansöker om tillståndet, med godkännande av landets justitieminister. Tillståndets längd kan vara upp till nittio dagar. Presidenten kan besluta, genom landets justitieminister, om tillstånd för inhämtning på det egna territoriet riktat mot främmande makt för perioder upp till ett år, under vissa förutsättningar såsom att inget inhemskt rättssubjekt berörs. Den särskilda domstolen skall underrättas om sådan åtgärd.

Av ovanstående framgår att någon generell modell för tillståndsgivning inte kan urskiljas vid en jämförelse mellan olika länder. Lösningarna varierar beroende på respektive lands lagstiftnings-, förvaltnings- och inhämtningstradition.

Krav på tillstånd gäller i regel inte för all inhämtning utan förekommer framförallt i de fall då lagstiftningen även omfattar inhämtning i brottsbekämpande syfte eller på det egna territoriet. I många länder regleras signalspaning för sådana ändamål som försvarsunderrättelseverksamheten omfattar i samma författning som signalspaning för mer uttalat brottsbekämpande ändamål, vilket naturligtvis påverkar regleringens utformning.

Det kan mot denna bakgrund inte anses föreligga någon enhetlig internationell standard – ens bland de stater som är bundna av Europakonventionen – som ställer krav på viss utformning av ett system för förhandsprövning. Frågan måste därför bedömas med utgångspunkt från nationella förutsättningar när det gäller t.ex. förhållandet mellan regering och myndigheter, de begränsningar som föreslås beträffande de syften för vilka signalspaning får bedrivas och de förutsättningar i övrigt som gäller för verksamheten.

Tillstånd för myndigheter att ge närmare inriktning m.m.

Som regeringen har konstaterat ovan måste ett system för tillståndsgivning utformas med beaktande av verksamhetens särskilda förutsättningar. Regeringens bedömning är som berörts i avsnitt 7.4.1 att försvarsunderrättelseverksamheten – så som den avgränsas genom de förslag som här lämnas – är ett sådant angeläget ändamål att det nödvändiggör vissa inskränkningar i grundläggande fri- och rättigheter. Syftet med ett system för tillståndsgivning måste följaktligen vara att säkerställa att signalspa-

ningsverksamheten endast bedrivs för att tillgodose de i lag angivna ändamålen och att det sker på ett sätt som är proportionerligt med hänsyn till ändamålen.

I promemorian har föreslagits ett system enligt vilket detta syfte uppnås genom en prövning av de inriktningar som andra myndigheter ger för signalspaningen. Regeringen kan se flera fördelar med en sådan modell. Den innebär att prövningen sker av vad som i realiteten avgränsar signalspaningens omfattning, nämligen de externa behovsframställningar som utgör utgångspunkten för verksamhetens bedrivande. Samtidigt innebär en sådan modell att Försvarets radioanstalts verkställande åtgärder med anledning av en inriktning påverkas i begränsad utsträckning och kan utföras med bibehållen flexibilitet och anpassningsförmåga. Fokus läggs på den ur integritetssynpunkt viktiga frågan *vad* som får inhämtas, inte på den av huvudsakligen tekniska och praktiska parametrar betingade frågan *hur* inhämtningen skall genomföras.

Ett tillståndskrav för myndigheternas inriktning kan dessutom underlätta såväl Försvarets radioanstalts som den inriktande myndighetens arbete genom att det i samband med inhämtningens genomförande inte behöver råda någon tvekan om en närmare inriktnings förenlighet med de i lag angivna förutsättningarna för verksamheten. Därigenom behöver inte heller några resurser avsättas hos Försvarets radioanstalt för att annat än i brådskande fall (se nedan) mer ingående pröva i vilken utsträckning en närmare inriktning kan läggas till grund för inhämtningen. Har tillstånd däremot lämnats kan den bedömningen göras mer övergripande.

Som föreslås i promemorian bör tillståndsprövningens syfte vara att pröva den närmare inriktningens förhållande till de ramar för verksamheten som uppställs genom bestämmelserna i lagen (2000:130) om försvarsunderrättelseverksamhet, lagen om signalspaning i försvarsunderrättelseverksamhet och regeringens inriktning. Därtill anser regeringen att prövningen också bör innefatta en proportionalitetsbedömning, uttryckt på så sätt att tillstånd endast får lämnas om syftet med inriktningen väger klart tyngre än det integritetsintrång som inhämtning i enlighet med inriktningen kan innebära och detta syfte inte kan tillgodoses på ett mindre ingripande sätt. Proportionalitetsbedömningen får göras utifrån det underlag som den inriktande myndigheten förser tillståndsorganet med. När det gäller uppskattningen av det integritetsintrång som inhämtning enligt en inriktning kan komma att innebära kan en sådan bedömning naturligtvis inte göras med exakthet, eftersom det ankommer på Försvarets radioanstalt att närmare bestämma formerna för inhämtningen. En inriktning bör dock i allmänhet vara så utformad att tillståndsorganet kan skaffa sig en välgrundad uppfattning i stort om omfattningen av de inhämtningsåtgärder som kan komma att vidtas med anledning av inriktningen.

Även om det inte finns anledning att hysa farhågor för att en myndighet skulle komma att vilja utnyttja signalspaningsresurserna för andra ändamål än de som anges i lagen är inhämtning av uppgifter för myndigheternas räkning mer ägnad att komma i konflikt med integritetsskyddet än inhämtning som sker i enlighet med inriktning för regeringens egna underrättelsebehov. Regeringens inriktning avser övergripande företeelser av strategiskt utrikes-, säkerhets- och försvarspolitiskt intresse. Systemen för att säkerställa inriktningarnas förenlighet med lag bör därför utformas olika. För myndigheternas närmare inriktning av signalspaning-

en föreslår regeringen det system som redovisas närmare i följande avsnitt.

När det gäller regeringens inriktning avseende de egna behoven av underlag för t.ex. utrikespolitiska ställningstaganden, är det naturligtvis angeläget att det också beträffande denna finns mekanismer för att på förhand säkerställa att inriktningen är förenlig med de krav som uppställs i lag och alltså uppfyller samma kriterier som gäller för en myndighets närmare inriktning. I detta syfte bör den kompetens och erfarenhet på försvarsunderrättelseområdet som tillståndsmyndigheten tillägnar sig genom tillståndsförfarandet tillvaratas. Regeringen avser därför att i samband med sitt beslut om inriktningen låta tillståndsmyndigheten ta ställning till dess förenlighet med lag, enligt motsvarande kriterier som vid tillståndsprövning för myndigheternas närmare inriktning. Därigenom garanteras att ingen signalspaningsverksamhet initieras utan att all inriktning först blivit föremål för betryggande bedömning av inriktningens förenlighet med lag.

Som framgår av avsnitt 8.2 föreslår regeringen att den myndighet som skall kontrollera signalspaningsverksamheten dessutom skall få besluta att viss inhämtning skall upphöra eller att upptagning eller uppteckning av inhämtade uppgifter skall förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med lagen eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten. Den möjligheten gäller oavsett vilken inriktning som ligger till grund för inhämtningen.

Regeringens beslut om inriktning av försvarsunderrättelseverksamheten är därtill naturligtvis underkastat samma parlamentariska kontroll genom riksdagens konstitutionsutskott som regeringens beslut i övrigt.

När det gäller regeringens inriktning har naturligtvis också Försvarets radioanstalt ett ansvar för att, innan verkställande åtgärder vidtas, pröva om signalspaning kan ske enligt inriktningen; myndigheten kan inte verkställa en inriktning som strider mot lag. Det i avsnitt 7.3.4 föreslagna integritetsskyddsrådet fyller därvid en viktig funktion för att säkerställa att verksamheten är lagenlig.

Försvarets radioanstalts ansvar för att innan inhämtning påbörjas ta ställning till dess laglighet innefattar självfallet att kontrollera att inhämtning för regeringens eget underrättelsebehov inte avser endast en viss enskild person eller åtgärder som syftar till att lösa uppgifter som ligger inom ramen för brottsbekämpande verksamhet. Integritetsskyddsrådet, som har en i förhållande till inhämtningsverksamheten fristående roll, skall ha ett särskilt ansvar för att förhindra att inhämtning sker som inte är förenlig med lag eller vars syfte inte kan anses stå i rimlig proportion till det integritetsintrång som den medför.

Integritetsskyddsrådet fyller också, vilket närmare berörs i avsnitt 8.2, en viktig funktion för påtalande av behov av närmare granskningsåtgärder. Genom den löpande utomstående kontrollen av verksamheten säkerställs ytterligare att inhämtning som sker enligt regeringens inriktning verkställs i enlighet med lagens krav. Denna kontroll gäller all signalspaning, oavsett enligt vilken inriktning den bedrivs.

Vilken myndighet skall pröva frågor om tillstånd?

Ett tillståndsförfarande förutsätter att tillståndsgivningen kan anförtros ett självständigt och oberoende organ som är ägnat att upprätthålla ett brett allmänt förtroende för verksamheten. Organet bör också ha kunskap om verksamheten och goda möjligheter att hantera sekretessbelagt material. Några remissinstanser har ansett att uppgiften att ge tillstånd bör anförtros en domstol eller ett domstolsliknande organ.

För ett domstolsförfarande talar rättssäkerhetsskäl och att det system med offentliga ombud som nu finns vid domstolsprövningen av hemlig teleavlyssning och hemlig teleövervakning skulle kunna utnyttjas också vid frågor om signalspaning i försvarsunderrättelseverksamheten. Det finns emellertid flera skäl som talar mot ett domstolsförfarande. Ett skäl är att det vid signalspaning inte rör sig om användning av straffprocessuella tvångsmedel utan om inhämtning som sker för andra syften och som skall tillgodose olika behov på ett flertal myndigheters verksamhetsområden. Det blir då fråga om en prövning av huruvida behoven kan tillgodoses genom signalspaning och inom de ramar som dragits upp genom lag och regeringens inriktningsbeslut. Prövningen innefattar däremot inte åtgärder som vidtas inom ramen för ett processrättsligt system och som utgör förberedande åtgärder till mål som senare kan komma att handläggas av domstol i ordinarie ordning. I stället kommer handläggningen av tillståndsärendena att ställa särskilda krav på erfarenhet av verksamhet som är främmande för en domstol, eftersom den innebär prövning av inriktningar som avser behov av mycket skiftande karaktär och som innefattar bedömningar av utrikes-, säkerhets- och försvarspolitisk karaktär. *Registernämndens* och *Kammarkollegiets* uppfattning att prövningen bör göras av domstol delas därför inte av regeringen.

Ett alternativ till domstolsprövning är att anförtro tillståndsprövningen till en ny myndighet som inrättas uteslutande för att fullgöra denna uppgift. Mot att tillskapa en ny myndighet endast för denna fråga talar att myndighetens uppgift blir av begränsad omfattning. Som har framhållits i den förvaltningspolitiska propositionen (prop. 1997/98:136 s. 38 f) och i budgetpropositionen för år 2006 (prop. 2005/06:1 bilaga 1 s. 7) bör myndigheter av denna karaktär inte inrättas om det finns andra alternativ. När så är möjligt bör i stället särskilda beslutsfunktioner inom befintliga myndigheter användas. Mot att tillskapa ett nytt organ endast för denna fråga talar också tidsåtgången för att från grunden bygga upp organisationen och skaffa nödvändig kompetens. Att inrätta en ny myndighet bör följaktligen övervägas först om det kan konstateras att det inte finns möjlighet att inrymma tillståndsprövningsfunktionen i en befintlig myndighet.

Om uppgiften att pröva frågor om tillstånd för inriktning av signalspaningen skall anförtros en redan befintlig myndighet bör denna, utöver kompetens att hantera försvarsunderrättelsefrågor, också ha kunskap om andra berörda myndigheters arbetsuppgifter och behov.

Registernämnden har i förhållande till Säkerhetspolisen en sådan funktion att det skulle kunna övervägas att anförtro även tillståndsgivning i nu aktuellt avseende till nämnden. Flertalet av de myndigheter som har intresse av signalspaningens resultat saknar dock motsvarande anknytning till ett organ av denna karaktär. Det framstår därför med hänsyn till myn-

digheternas skiftande behov som mindre ändamålsenligt att göra Registernämnden till generellt tillståndsorgan. Registernämnden har heller inte den bredare kompetens på det utrikes-, säkerhets- och försvarspolitiska området som är nödvändig.

Ett annat alternativ är Försvarets underrättelsenämnd. Nämnden är en självständig myndighet under regeringen som – utan någon beroendeställning till de myndigheter som bedriver försvarsunderrättelseverksamhet – skall kontrollera signalspaningsverksamheten och annan försvarsunderrättelseverksamhet och som därigenom har detaljerad insikt i förutsättningarna för verksamheten. Det kan mot denna bakgrund anses att nämnden är den redan befintliga myndighet som idag bäst lämpar sig för att få till uppgift att lämna tillstånd till signalspaningen. Mot att anförtro tillståndsgivningen till Försvarets underrättelsenämnd talar att detta kan uppfattas som om Försvarets underrättelsenämnd därigenom får dubbla roller som dels tillståndsgivare, dels tillsynsorgan. Som regeringen inledningsvis anfört är det viktigt att tillståndsfunktionen är självständig och oberoende och att såväl tillstånds- som kontrollfunktionen åtnjuter ett stort förtroende.

Som framhålls i promemorian kan detta skenbara problem dock avhjälpas genom att tillståndsgivningen utformas på ett sådant sätt att någon konflikt mellan den tillståndsgivande och kontrollerande funktionen inte uppstår. Det kan ske genom att de beställande myndigheterna söker tillstånd hos Försvarets underrättelsenämnd innan de lämnar sin närmare inriktning till Försvarets radioanstalt, och att det följaktligen inte är Försvarets radioanstalt som inhämtar tillstånden. Försvarets radioanstalt är som framhållits ovan ett renodlat inhämtningsorgan och bedriver inte signalspaning för egna underrättelsebehov. När ett tillstånd har lämnats kan Försvarets radioanstalts egen prövning av att inhämtning lagligen kan ske i enlighet med den givna inriktningen vara av mer övergripande karaktär. Den kontroll som granskningsmyndigheten därefter utövar av signalspaningsverksamheten inriktas på Försvarets radioanstalts verksamhet och omfattar följaktligen inte innehållet i inriktningen, utan endast i vilken utsträckning inhämtning utförts i enlighet med inriktningen samt formerna för denna inhämtning, t.ex. utformningen av sökbegrepp. När det gäller den inriktande myndigheten begränsar sig Försvarets underrättelsenämnds prövning till den närmare inriktningens förhållande till de ramar för verksamheten som uppställs genom bestämmelserna i lagen (2000:130) om försvarsunderrättelseverksamhet, lagen om signalspaning i försvarsunderrättelseverksamhet – i vilken bl.a. finns begränsningen att inriktningen inte får avse endast en viss fysisk person – och regeringens inriktning samt till en proportionalitetsbedömning.

En sådan utformning av tillståndsgivningen skulle inte på något sätt innebära att den inriktande myndighetens verksamhet underställs nämndens granskning. Regeringen delar således inte *Säkerhetspolisens* uppfattning att Försvarets underrättelsenämnd skulle komma att pröva Säkerhetspolisens operativa verksamhet i samband med tillståndsförfarandet. Nämndens uppgift är i ett sådant fall endast att ta ställning till om Försvarets radioanstalt kan inhämta underrättelser enligt en inriktning från Säkerhetspolisen. Däremot kan den ordningen att inriktande myndigheter begär tillstånden bidra till att underlaget för prövningen blir så brett som möjligt, eftersom det rimligen är den inriktande myndigheten

som bäst kan belysa behovet av att erhålla de underrättelser som inriktningen avser. Det är dessutom den inriktande myndigheten som har bäst förutsättningar att förse tillståndsmyndigheten med material för den proportionalitetsbedömning som skall göras.

Enligt regeringens bedömning är det fullt möjligt att med en sådan utformning av tillståndsprövningen som beskrivits ovan inrymma såväl tillståndsfunktionen som den kontrollerande funktionen inom ramen för Försvarets underrättelsenämnds verksamhet. För att ytterligare markera tillståndsprövningens självständighet avser regeringen att reglera Försvarets underrättelsenämnds organisation på sådant sätt att tillståndsprövningen skall ske i en särskild avdelning inom nämnden, i vilken en ledamot med domarerfarenhet eller motsvarande juridisk kompetens skall vara ordförande. Därigenom förstärks också den rättsliga karaktären av tillståndsprövningen.

Sammantaget anser regeringen att en tillståndsfunktion inom Försvarets underrättelsenämnd utformad på det sätt som angetts tillgodoser behovet av en självständig och oberoende förhandsprövning i syfte att säkerställa skyddet för enskildas fri- och rättigheter.

Närmare om tillståndsprövningen

Den nya uppgift som tillståndsprövningen innebär reser krav på en förstärkning av Försvarets underrättelsenämnds organisation. I avsnitt 8 beskrivs vissa organisatoriska förändringar av Försvarets underrättelsenämnd som krävs för att de nya uppgifter som åläggs nämnden skall kunna lösas. Bl.a. måste nämnden tillföras ytterligare juridisk kompetens. Förändringarna innebär att nämnden kommer att ha kapacitet för att snabbt och rationellt kunna hantera de framställningar som kommer från olika myndigheter. Det kan emellertid uppstå situationer av så brådskande karaktär att ett tillstånd inte kan avvaktas utan att det skulle medföra allvarliga konsekvenser för väsentliga nationella intressen. I sådana situationer bör det enligt regeringens mening finnas en möjlighet att ge en närmare inriktning utan att tillstånd först inhämtats. En sådan situation kan t.ex. vara plötsliga hot mot rikets säkerhet, som en från utlandet härrörande omedelbart förestående terroristattack i Sverige. Ett annat exempel kan vara ett akut hot mot svensk trupp eller personal utomlands. Den myndighet som gett inriktningen skall i sådana fall i efterhand omedelbart anmäla den givna inriktningen till tillståndsmyndigheten. Om tillståndsmyndigheten finner att tillstånd till inriktning inte borde ha getts skall Försvarets radioanstalt underrättas och inhämtningen omedelbart avbrytas. Ansvaret för att inhämtningen avbryts vilar således på Försvarets radioanstalt och omfattas av tillståndsmyndighetens kontroll.

En inriktning skall, oavsett om den är av brådskande karaktär eller inte, avse en företeelse eller ett förhållande som är relevant med avseende på de ändamål för vilka signalspaningen får bedrivas. Inriktningen skall också i övrigt vara förenlig med lagen (2000:130) om försvarsunderrättelseverksamhet. I tydliggörande syfte bör detta framgå av bestämmelsen om tillstånd, liksom att tillstånd inte får ges för inriktning som endast avser en fysisk person. Det senare följer visserligen redan av de syften för vilken verksamheten får bedrivas och de begränsningar i övrigt som framgår av regelverket, men bör ändå klargöras för att undvika tveksam-

het om för vilka uppgifter andra myndigheter kan använda signalspaningsresursen.

Begränsningen såvitt avser fysiska personer innebär att en inriktning inte får ha till syfte att endast kartlägga en viss person. Naturligtvis måste dock signalspaningen ibland beröra enskildas kommunikationer för att det skall vara möjligt att kartlägga en viss företeelse som avser utländska förhållanden av relevans för verksamheten. Vid sådan kartläggning kan det vara nödvändigt att utnyttja information om fysiska personer som en utgångspunkt för vidare inhämtning. De begränsningar som gäller för i vilken utsträckning uppgifter som är direkt hänförliga till fysiska personer i sådana sammanhang får användas som sökbegrepp behandlas i avsnitt 7.4.2.

Som redogjorts för ovan skall prövningen dessutom innefatta en proportionalitetsbedömning på grundval av de uppgifter som lämnas av den inriktande myndigheten.

Ett tillstånd bör vara tidsbegränsat. Med hänsyn till karaktären av de företeelser som är av intresse för verksamheten kan giltighetstiden inte sättas alltför kort. Regeringen bedömer att en tidsram om högst sex månader kan vara en lämplig. Om inhämtningen är av mer kortsiktig art skall tillståndet naturligtvis ges för en kortare tid. Om det efter utgången av tiden för tillstånd föreligger fortsatt behov av inhämtningen, skall möjlighet finnas att efter förnyad prövning förlänga tillståndet i ytterligare perioder om högst sex månader. Genom tidsbegränsningen och kravet på förnyad prövning säkerställs att det sker en kontinuerlig omprövning av behovet av inhämtningen.

Sammanfattningsvis innebär det som regeringen ovan har anfört om tillståndsprövningen att Försvarets underrättelsenämnd, innan inhämtning enligt en närmare inriktning påbörjas, skall göra en prövning i flera steg och därvid bedöma om den närmare inriktningen är förenlig med en rad olika kriterier. Det första steget består i att pröva att inriktningen avser kartläggning av något förhållande som är av intresse för svensk utrikes-, säkerhets- och försvarspolitik eller i övrigt avser yttre hot mot landet. Därvid skall också kontrolleras att inriktningen avser utländska förhållanden. Vid denna prövning har myndigheten till stöd för sin bedömning den exemplifiering av ändamål som finns i författningskommentaren till 1 § lagen om signalspaning i försvarsunderrättelseverksamhet, se avsnitt 12.2.

I tillståndsprövningen ingår som ett nästa steg att bedöma om den närmare inriktning som en myndighet önskar ge ryms inom regeringens inriktning av verksamheten. Regeringen samordnar och prioriterar genom sin inriktning de behov som försvarsunderrättelseverksamheten skall tillgodose och anger på det sättet ytterligare en ram för prövningen. Regeringens inriktning kan snäva in den ram inom vilken signalspaningen kan bedrivas, men naturligtvis inte utvidga den utöver vad lagen medger.

Ett ytterligare steg i prövningen är att kontrollera att den närmare inriktningen avser en företeelse och inte endast en viss fysisk person. Denna bedömning syftar bl.a. till att säkerställa att inriktningen inte avser 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. Som regeringen tidiga-

re har framhållit är det av yttersta vikt att hålla isär signalspaning i försvarsunderrättelseverksamhet och sådana åtgärder.

Härefter skall tillståndsmyndigheten göra en proportionalitetsbedömning av syftet med den närmare inriktningen i förhållande till det integritetsintrång som inhämtning genom signalspaning i enlighet med inriktningen kan komma att medföra.

Slutligen skall tillståndsmyndigheten, om det finns förutsättningar för att lämna tillstånd till den närmare inriktningen, ange för hur lång tid tillståndet skall gälla.

7.4.4 Upptagningar och uppteckningar som skall förstöras samt rapportering av underrättelser

Regeringens förslag: Upptagning eller uppteckning av uppgifter som inhämtats genom signalspaning skall omgående förstöras om innehållet
1. berör en viss fysisk person och har bedömts sakna betydelse för den verksamhet som regleras i lagen,
2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 4 § tryckfrihetsförordningen eller 2 kap. 4 § yttrandefrihetsgrundlagen, eller
3. omfattar uppgifter i meddelanden som avses i 27 kap. 22 § rättegångsbalken.

Rapportering av underrättelser som inhämtats genom signalspaning och som berör en viss fysisk person får endast avse förhållanden som är av betydelse för ändamålet med verksamheten såsom den formulerats i 1 § lagen (2000:130) om försvarsunderrättelseverksamhet.

Regeringens bedömning: Någon bestämmelse om förstöring av upptagning eller uppteckning som omfattar annan kommunikation behövs inte.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorians förslag har dock inte förstöringsskyldigheten respektive rapporteringsbegränsningen begränsats till att endast avse uppgifter som berör en viss fysisk person. Promemorians förslag innehåller heller ingen bestämmelse om förstöring av kommunikation mellan en misstänkt och dennes försvarare.

Remissinstanserna: De flesta remissinstanser som har yttrat sig har tillstyrkt förslaget eller lämnat det utan erinran. *Justitiekanslern* har anfört att den föreslagna lösningen får godtas under förutsättning att alla uppgifter som omfattas av grundlagsskyddet förstörs och inte vidarerapporteras, oavsett om upptagningen i övrigt innehåller uppgifter av intresse ur underrättelsesynpunkt. Justitiekanslern har vidare ifrågasatt riktigheten av slutsatsen att begränsningar avseende annan privilegierad kommunikation inte behövs och anfört att det bör övervägas om inte också uppgifter som avser kommunikation mellan en misstänkt och dennes försvarare skall omfattas av kravet på omgående förstöring.

Även *Tryck- och yttrandefrihetsberedningen* har pekat på behovet av ett förtydligande när det gäller kravet på att förstöra upptagningar eller uppteckning som innehåller såväl grundlagsskyddad information som information av intresse för försvarsunderrättelseverksamheten. *Tidningsutgivarna* har ifrågasatt om förslaget löser den grundlagsmässiga problematiken, eftersom brottet mot anonymitetsskyddet och efterforskningsförbudet är fullbordat redan genom inhämtningen och inte läks genom förstöring i efterhand, och har anfört att förfarandet för att bli godtagbart måste legitimeras genom bestämmelser i berörda grundlagar.

Försvarets radioanstalt har anfört att det i förslaget saknas en bestämmelse motsvarande den som återfinns i myndighetens regleringsbrev och enligt vilken ett undantag från kravet på att information utan betydelse skall förstöras görs för material som har ett sådant innehåll att det bör komma till polisens kännedom. *Säkerhetspolisen* har, utifrån sin syn på gränsdragningen mellan försvarsunderrättelseverksamhet och polisiär verksamhet (se avsnitt 6), påpekat att den föreslagna begränsningen skulle innebära att information av intresse för de brottsbekämpande myndigheterna kan komma att förstöras och anfört att det därför bör finnas utrymme för att överlämna information som den mottagande myndigheten själv skulle ha kunnat inhämta.

Skälen för regeringens förslag och bedömning

Information utan betydelse för verksamheten

I avsnitt 7.3.4 behandlas hur sökning med fastställda sökbegrepp skall användas för att begränsa inhämtningen med automatiserad behandling av signaler i elektronisk form. Urval med hjälp av sökbegrepp begränsar i hög grad antalet personer som berörs av inhämtningen. Användningen av sökbegrepp utgör dock inte någon fullständig garanti för att det inte bland de uppgifter som erhålls genom automatiserad inhämtning kan komma att finnas andra uppgifter om fysiska personer än de som är intressanta ur underrättelsesynpunkt. I den signalspaning som sker med manuella metoder sker inget förhandsurval genom sökbegrepp, varför det även i den information som inhämtas på detta sätt kan komma att finnas sådana uppgifter om fysiska personer som saknar relevans för underrättelseverksamheten. Förekomsten av sådana uppgifter i upptagningar eller uppteckningar är inte nödvändig för verksamhetens behov.

Det kan därför, vid en avvägning mot intresset av skydd för den personliga integriteten, inte anses motiverat att de hanteras inom signalspaningsverksamheten. Det föreslås därför att upptagning eller uppteckning av uppgifter som erhållits genom inhämtning av signaler i elektronisk form omgående skall förstöras om innehållet berör en viss fysisk person och har bedömts sakna betydelse för verksamheten. Ett exempel på upptagningar eller uppteckningar som typiskt sett saknar betydelse för verksamheten är sådana som avser kommunikation som faller helt utanför ramen för verksamhetens ändamål, t.ex. därför att de rör inhemska förhållanden. Det finns inte anledning att låta förstöringsskyldigheten avse andra uppgifter än de som kan vara integritetskänsliga, dvs. uppgifter som berör viss fysisk person.

När det gäller upptagningar eller uppteckningar som innehåller både relevanta uppgifter och sådana uppgifter som saknar betydelse behandlas denna frågeställning närmare nedan i samband med förslagen som berör rapportering av underrättelser.

Relationen till tryck- och yttrandefriheten

En viktig utgångspunkt är vidare att regler om signalspaning inte får strida mot det skydd för meddelarfriheten som gäller enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Även om signalspaningen inte riktas mot personer som är verksamma på massmedieområdet kommer det inte att gå att helt undvika risken för att exempelvis ett meddelande mellan en journalist och en meddelare inhämtas. Anonymitetsskyddet som garanteras genom journalistens tystnadsplikt bryts då igenom. En upptagning eller uppteckning kan också innefatta ett brott mot det s.k. efterforskningsförbudet. Det ideala skulle vara om inhämtning som berörde massmedieområdet förbjöds. Vid automatiserad inhämtning är det dock inte möjligt att upprätthålla ett sådant förbud. Av praktiska och tekniska skäl kan det inte heller krävas att inhämtningen omedelbart skall avbrytas. Problemet kan inte lösas på annat sätt än genom en föreskrift om att upptagningar eller uppteckningar som står i konflikt med tryckfrihetsförordningen och yttrandefrihetsgrundlagen omedelbart skall förstöras.

Justitiekanslern och *Tryck- och yttrandefrihetsberedningen* har anfört att kravet på förstöring bör gälla oavsett om en upptagning eller uppteckning i övrigt innehåller information av relevans för försvarsunderrättelseverksamheten. När det gäller sådana upptagningar eller uppteckningar som berör det grundlagsskyddade området kan det naturligtvis förekomma att innehållet är sådant att det i och för sig är av intresse för försvarsunderrättelseverksamheten. Detta saknar dock betydelse när det gäller tillämpningen av den föreslagna bestämmelsen; en sådan upptagning eller uppteckning skall förstöras så snart det har konstaterats att den är av sådant slag som anges i bestämmelsen, innehållet i det som omfattas av grundlagsskyddet saknar därvid all betydelse. Att så skall vara fallet följer redan av promemorians författningsförslag. I detta avseende skiljer sig situationen från vad som gäller i fråga om uppgifter som saknar betydelse för verksamheten – den upptagning eller uppteckning som innehåller sådana uppgifter behöver inte förstöras om den också innehåller relevanta uppgifter, eftersom det som framgår av följande avsnitt ofta inte är praktiskt möjligt att ta bort de förra uppgifterna. Däremot får de uppgifter som saknar betydelse inte rapporteras vidare, se nedan.

Regeringen delar inte *Tidningsutgivarnas* bedömning att det föreslagna systemet skulle kräva grundlagsreglering. Enbart den omständigheten att informationen inhämtas kan nämligen inte anses innebära ett brott mot anonymitetsskyddet och efterforskningsförbudet om inte något sådant syfte föreligger.

Förbudet mot att röja identiteten hos en författare, meddelare eller utgivare av icke periodisk skrift riktas enligt 3 kap. 3 § första stycket tryckfrihetsförordningen mot den som har tagit befattning med tillkomsten eller utgivningen av tryckt skrift eller med framställning avsedd att införas i tryckt skrift och den som varit verksam inom företag för utgivning

av tryckta skrifter eller inom företag för utgivning av tryckta skrifter eller inom företag för yrkesmässig förmedling av nyheter eller andra meddelanden till periodiska skrifter. Yttrandefrihetsgrundlagens bestämmelse om tystnadsplikt riktas mot motsvarande kategorier på yttrandefrihetsgrundlagens område, 2 kap. 3 § första stycket yttrandefrihetsgrundlagen. Bestämmelserna är följaktligen inte riktade direkt mot det allmänna. Tystnadsplikten för de angivna kategorierna syftar till att skydda författare och meddelare, som i princip åtnjuter ansvarsfrihet från tryck- och yttrandefrihetsbrott, också från andra påföljder, t.ex. obehag från omgivningen (Håkan Strömberg och Hans-Gunnar Axberger, Yttrandefrihetsrätt, 2004, s. 36). Den föreslagna bestämmelsen har samma syfte och innebär följaktligen att anonymitetsskyddet tryggas.

När det gäller förbudet – med vissa undantag – mot att efterforska författare, utgivare eller meddelare (3 kap. 4 § tryckfrihetsförordningen och 2 kap. 4 § yttrandefrihetsgrundlagen) riktar sig detta visserligen uttryckligen mot myndigheter och andra allmänna organ. För att en överträdelse av förbudet skall anses föreligga torde emellertid krävas att syftet med åtgärden från det allmännas sida varit att efterforska författaren, utgivaren eller meddelaren. När sådan information i stället råkar inhämtas av en myndighet som en icke avsedd bieffekt av annan verksamhet kan det inte anses att efterforskningsförbudet överträtts, i synnerhet inte om det åvilar myndigheten en uttrycklig skyldighet att förstöra upptagning eller uppteckning med sådan information och anonymitetsskyddet följaktligen garanteras.

Regeringens uppfattning är sammanfattningsvis att genom förslaget tillgodoses anonymitetsskyddet och meddelarfriheten på ett sätt som, vilket också *Justitiekanslern* anfört, får anses godtagbart med hänsyn till den intresseavvägning som är nödvändig.

Annan kommunikation som åtnjuter särskilt skydd

I anslutning till skyddet för sådan kommunikation som omfattas av tryck- och yttrandefriheten finns anledning att överväga behovet av att föreskriva om förstöring av upptagningar eller uppteckningar som innehåller andra typer av kommunikation som i annan lagstiftning åtnjuter ett särskilt skydd.

Ett sådant skydd finns, såvitt avser hemlig teleavlyssning, i 27 kap. 22 § rättegångsbalken för telefonsamtal eller andra telemeddelanden mellan en misstänkt och dennes försvarare. Sådan kommunikation får inte avlyssnas, och om det framkommer under avlyssning att det är fråga om ett sådant samtal eller meddelande skall avlyssningen avbrytas. Upptagningar och uppteckningar som omfattas av förbudet skall omedelbart förstöras.

Bestämmelsen har tillkommit mot bakgrund av principen att det bör råda överensstämmelse mellan begränsningarna i vittnesplikt och begränsningarna i möjligheten att få fram motsvarande uppgifter genom tvångsmedelsanvändning (prop. 1988/89:124 s. 46). Enligt 36 kap. 5 § rättegångsbalken får inte bl.a. försvarare höras som vittne om vad som anförtrotts honom för uppdragets fullgörande. Det har ansetts att den misstänkte skall kunna förlita sig på att det han anförtror sin försvarare

inte skall komma till de brottsutredande organens kännedom utan hans samtycke oavsett på vilket sätt han meddelat sig med försvararen.

I samband med tillkomsten av skyddet för samtal mellan den misstänkte och hans försvarare i 27 kap. 22 § rättegångsbalken har utgångspunkten alltså varit att det skall föreligga korrespondens mellan begränsningarna i vittnesplikten och begränsningarna i möjligheten att erhålla information genom tvångsmedelsanvändning. Det skall följaktligen inte vara möjligt att som bevis i rättegång åberopa uppgifter som avlyssnats när de lämnats under ett samtal eller i ett meddelande mellan den misstänkte och en person som inte kunnat höras som vittne om samma förhållande och därigenom kringgå bestämmelserna i 36 kap. 5 § rättegångsbalken.

I promemorian har inte föreslagits någon bestämmelse om skyldighet att förstöra sådan information, med motiveringen att i fråga om signalspaning föreligger den grundläggande skillnaden i förhållande till de ovan behandlade situationerna att de uppgifter som inhämtas inte är avsedda att åberopas som bevis vid en rättegång eller ligga till direkt grund för något annat ingripande eller någon annan åtgärd riktad mot den enskilde från myndigheternas sida. Signalspaningen utgör följaktligen inte något straffprocessuellt tvångsmedel. I den utsträckning underrättelser baserade på signalspaning överlämnas till polismyndigheter utgörs dessa av bearbetade och analyserade underrättelser och inte av upptagningar eller uppteckningar av de uppgifter som inhämtats genom signalspaningen. I promemorian görs därför bedömningen att det inte är möjligt att med hjälp av sådana underrättelser kringgå bestämmelserna om begränsningar av vittnesplikten och att det inte heller föreligger någon risk för att integritetskänsliga uppgifter skall spridas i offentligheten på det sätt som sker under en rättegång.

Justitiekanslern har påtalat att rapporteringsförbudet inte hindrar att genom signalspaning inhämtade uppgifter som berör förhållandet mellan en misstänkt och dennes advokat skulle kunna åberopas i rättegång och därmed användas för att kringgå vittnesförbudet. Justitiekanslern har därför ansett att det bör övervägas att föreskriva om förstöring även av sådana uppgifter.

Av de grundläggande principer som gäller för gränsdragningen mellan försvarsunderrättelseverksamhet och brottsbekämpande verksamhet som behandlas i avsnitt 6.3.2. framgår att signalspaning i försvarsunderrättelsesyfte inte får bedrivas kring en företeelse om vilken förundersökning pågår, eftersom det då finns förutsättningar att i den brottsbekämpande verksamheten använda sådana hemliga tvångsmedel som regleras i rättegångsbalken. Som *Justitiekanslern* påpekar kan det dock inte garanteras att sådan kommunikation inte ändå blir föremål för signalspaning och att den, även om den inte heller rapporteras i form av underrättelser, kan komma att användas på ett sätt som innebär att vittnesförbudet kringgås. Regeringen anser därför att det trots vad som anförts i promemorian finns skäl att införa en bestämmelse som helt utesluter denna risk. På så sätt tydliggörs ytterligare att signalspaning inte kan användas för att kringgå restriktioner som gäller användning av hemliga straffprocessuella tvångsmedel utan är en inhämtningsmetod avsedd för helt andra ändamål. Även sådana uppgifter som avses i 27 kap. 22 § rättegångsbalken bör följaktligen omfattas av förstöringsskyldigheten. Liksom i fråga om grundlagsskyddade meddelanden (se föregående avsnitt) skall en upptagning eller

uppteckning förstöras om den innehåller sådana uppgifter, även om innehållet i kommunikationen i och för sig också avser andra uppgifter.

När det gäller övriga kategorier som omfattas av rättegångsbalkens vittnesförbud finner dock inte regeringen skäl att frångå den bedömning som gjorts i promemorian att de bestämmelser som nu föreslås om verksamhetens ändamål, användning av sökbegrepp, tillstånd för viss inriktning, förstöring av upptagningar eller uppteckningar samt rapporteringsbegränsningar utgör ett fullgott skydd mot att särskilt skyddsvärd kommunikation inhämtas och bearbetas utan att det är oundgängligen nödvändigt för verksamheten. Att därutöver helt undanta vissa privilegierade kategorier från signalspaningens tillämpningsområde – oberoende av deras faktiska relevans för underrättelseverksamheten – skulle mot bakgrund av vad som anförts ovan utgöra en omotiverad inskränkning av verksamhetens förutsättningar. Någon motsvarande begränsning eller förstöringsskyldighet gäller heller inte enligt rättegångbalkens regler om hemlig teleavlyssning.

Rapportering av underrättelser

Som tidigare redovisats blir sökbegreppen avgörande för vilken information om enskilda som kommer att samlas in genom automatiserad inhämtning. Hur sofistikerade sökbegreppen än görs går det inte att undvika att inhämtningen kommer att omfatta både relevant och irrelevant information, särskilt inte när informationen förmedlas vid ett och samma kommunikationstillfälle. När det gäller uppgifter om fysiska personer omfattar den ovan nämnda bestämmelsen om förstöring av upptagning eller uppteckning bara upptagningar som innehåller betydelselösa uppgifter. Bestämmelsen riktar sig däremot inte mot upptagningar med både relevant och irrelevant information; en sådan upptagning har ju faktiskt – i vart fall till viss del – betydelse för verksamheten och skall då inte förstöras.

Problemet med olika typer av uppgifter i en och samma upptagning kan inte lösas genom ett krav på att upptagningen eller uppteckningen skall redigeras så att endast betydelsefull information får kvarstå. En sådan ordning är inte praktiskt genomförbar. Med utgångspunkt i integritetsskyddet återstår då att försöka förhindra att informationen förs vidare. I lagen om signalspaning i försvarsunderrättelseverksamhet bör därför föras in en bestämmelse om att rapportering av underrättelser som inhämtats genom signalspaning och som innefattar uppgifter som berör viss fysisk person endast får avse förhållanden som är av betydelse för ändamålet med verksamheten såsom den formulerats i 1 § lagen om försvarsunderrättelseverksamhet. Det blir därmed en viktig uppgift för kontrollorganet att ha tillsyn över vilka underrättelser som rapporteras.

I likhet med vad som föreslås gälla för förstöring anser regeringen, till skillnad från vad som föreslagits i promemorian, att det finns anledning att precisera rapporteringsförbudet till att omfatta särskilt skyddsvärda uppgifter, dvs. sådana som berör en viss fysisk person.

Regeringen har i avsnitt 6 behandlat frågan om försvarsunderrättelseverksamhetens mandat och gränsdragningen gentemot de brottsförebyggande och brottsbekämpande myndigheternas arbete. De uppgifter för försvarsunderrättelseverksamheten som regeringen föreslår skall anges i

lagen om försvarsunderrättelseverksamhet utgör också, vid sidan av inhämtning för Försvarets radioanstalts teknikutvecklingsbehov, den yttre ramen för de ändamål för vilket signalspaning skall få ske och som preciseras i avsnitt 7.4.3. Inom ramen för ändamålet ryms också de brottsförebyggande och brottsbekämpande myndigheternas behov av underrättelser om yttre hot mot landet. Sådana myndigheter kommer som angetts ovan också ha möjlighet att inrikta signalspaningen inom ramen för försvarsunderrättelseverksamheten.

Som regeringen har framhållit är det av stor vikt att hålla gränsen klar mellan inhämtning för försvarsunderrättelseändamål och de brottsbekämpande myndigheternas användning av hemliga tvångsmedel. Förutsättningarna för verksamheterna och de restriktioner till skydd för enskildas fri- och rättigheter som omgärdar dem skiljer sig i flera avseenden, beroende på att syftena med verksamheterna är olika. Signalspaning i enlighet med den här föreslagna lagstiftningen skall inte kunna användas för sådana syften för vilka anvisats de särskilda redskap som står de brottsbekämpande myndigheterna till buds. Av detta följer att det inte vid sidan av den generella rapporteringsregleringen finns utrymme för något uppgiftslämnande i särskild ordning till polisen eller andra brottsförebyggande och brottsbekämpande myndigheter. Mot denna bakgrund saknas anledning att överväga någon sådan bestämmelse som *Försvarets radioanstalt* och *Säkerhetspolisen* har berört.

7.4.5 Effektiva rättsmedel

Regeringens bedömning: Förslagen uppfyller Europakonventionens krav på att den enskilde skall ha tillgång till effektiva rättsmedel.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna delar promemorians bedömning eller lämnar det utan erinran. *Göteborgs universitet* har anfört att det i preskriptionsreglerna för rätten till skadestånd bör införas en bestämmelse av innebörden att preskriptionstiden räknas från tidpunkten som den skadelidande får kännedom om den skadebringande handlingen och inte, som normalt vid brott, från tidpunkten då den skadebringande handlingen företogs.

Skälen för regeringens bedömning: Europakonventionen ställer krav på att det skall finnas effektiva rättsmedel för den enskilde som anser sig ha fått sina fri- och rättigheter kränkta. En enskild som anser sig utsatt för signalspaning som går utöver de ramar som lagstiftningen uppställer kan alltid anmäla saken till åtal eller väcka talan om skadestånd och därigenom få sin sak prövad. De straffbestämmelser som då kan tillämpas är de som nämns i avsnitt 7.2.4. Eftersom signalspaning, när den riktar sig mot enskilda, under vissa förhållanden skulle kunna anses utgöra myndighetsutövning kan också bestämmelsen i 20 kap. 1 § brottsbalken aktualiseras. En enskild har också möjlighet att anföra klagomål hos Justitieombudsmannen, som har möjlighet att väcka åtal för det fall att brott begåtts.

När det gäller skadeståndsmöjligheten bör det noteras att skadeståndslagen (1972:207) ger rätt till ersättning inte bara vid sakskador,

personskador och förmögenhetsskador utan också vid lidande som orsakats genom vissa brott mot den personliga integriteten. Möjlighet till skadestånd finns också enligt de bestämmelser om behandling av personuppgifter som gäller för verksamheten. Preskriptionstiden i fråga om fordringar i allmänhet är som huvudregel 10 år från fordringens tillkomst, 2 § preskriptionslagen (1981:130). Preskriptionstiden avseende fordringar på skadestånd räknas normalt från den dag den skadegörande handlingen begås. Den fråga som *Göteborgs universitet* har väckt rör de grundläggande principerna om beräkning av preskriptionstid för fordringar på skadestånd. Frågan bör lösas på ett gemensamt sätt, åtminstone för de myndigheter som bedriver underrättelseverksamhet. Några överväganden eller förslag som avviker från vad som gäller idag i denna del kan inte göras inom ramen för detta lagstiftningsarbete.

I verksamhetens karaktär ligger emellertid att den som upplever sig ha anledning att anföra klagomål inte alltid själv har, eller kan få, kännedom om de förhållanden som kan innefatta en integritetskränkning. Problematiken har uppmärksammats av Europadomstolen, som i anslutning till ett fall avseende hemlig telefonavlyssning har framhållit att ett effektivt rättsmedel i dessa speciella sammanhang måste förstås som ett så effektivt rättsmedel som möjligt med hänsyn till de särskilda omständigheterna (målet Klass m.fl. mot Tyskland, dom 1978-09-06). Domstolen har också i andra sammanhang där svårigheter att kommunicera uppgifter till klaganden förelegat uttalat att de rättsmedel som kan krävas under sådana speciella omständigheter måste bli av relativt begränsad effektivitet (målet Leander mot Sverige, dom 1987-03-27). I samband med det senare avgörandet ansågs de olika tillsynsmöjligheter som stod till buds genom bl.a. JO, JK och parlamentarisk kontroll tillräckliga för att uppfylla kravet. Domstolen har också senare upprepat att såvitt avser hemlig övervakning kan ett objektivt övervakningssystem vara tillräckligt så länge som de åtgärder som riktas mot enskilda förblir hemliga, och att det är först när åtgärderna har blivit kända som egentliga rättsmedel måste bli tillgängliga för den enskilde (målet Rotaru mot Rumänien, dom 2000-05-04).

I ett senare avgörande mot Sverige (målet Segerstedt-Wiberg m.fl mot Sverige, dom 2006-06-06) som bl.a. gällde möjligheten att utverka beslut om radering av uppgifter i Säkerhetspolisens register, ansågs dock inte Sverige uppfylla konventionens krav genom den tillsyn som JO, JK, Datainspektionen och Registernämnden bedriver, varken sammantaget eller var och en för sig.

Vid bedömningen av i vilken utsträckning den här föreslagna regleringen uppfyller kraven på tillgång till effektiva rättsmedel måste beaktas verksamhetens speciella karaktär. Försvarsunderrättelseverksamheten inbegriper inte i sig några åtgärder mot enskilda av motsvarande karaktär som kan bli resultatet av användning av hemliga tvångsmedel i brottsbekämpande syften. Verksamheten får endast avse utländska förhållanden och det ligger i sakens natur att det finns mycket begränsade möjligheter att ge enskilda insyn i verksamheten, ens på mycket lång sikt. Intresset av att hemlighålla såväl de åtgärder som vidtas som resultatet av dessa gör sig gällande under mycket lång tid och verksamheten är organiserad på ett sätt som säkerställer att sådan information inte sprids. De mekanismer som skall tillgodose enskildas integritetsintresse

måste därför i huvudsak utgöras av generella kontrollfunktioner som verkar i huvudsak på eget initiativ och därvid granskar såväl att inte andra uppgifter behandlas än sådana som har betydelse för verksamheten som att uppgifter inte bevaras längre än nödvändigt.

Försvarets underrättelsenämnd ges enligt förslaget en särskild uppgift att kontrollera verksamheten, särskilt med avseende på användningen av sökbegrepp, förstöring av vissa typer av uppgifter och rapportering av underrättelser. Nämnden skall också kunna besluta att viss inhämtning skall upphöra eller att upptagning eller uppteckning av inhämtade uppgifter skall förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med denna lag eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten. Även om det med hänsyn till den begränsade möjligheten att ge insyn i verksamheten inte är meningsfullt att införa en formell anmälningsmöjlighet till nämnden innebär detta ändå att det finns en funktion för att stoppa rättighetsinskränkande åtgärder. Försvarets underrättelsenämnd kan naturligtvis också agera på annat sätt, t.ex. genom att vidarebefordra sina iakttagelser vid kontrollen till JO, som kan pröva om det finns anledning att väcka åtal mot någon befattningshavare, eller till Datainspektionen.

Mot bakgrund av den aktuella verksamhetens speciella karaktär, den heltäckande kontroll som skall utföras av Försvarets underrättelsenämnd och nämndens möjlighet att få inhämtning att upphöra, anser regeringen att den tillsyn som JO, JK och Datainspektionen utövar kompletteras i sådan utsträckning att kravet på effektiva rättsmedel får anses tillgodosett.

7.4.6 Behovet av rättighetsskyddsgarantier och lagen om elektronisk kommunikation

Regeringens bedömning: Skyldigheten för trådägande operatörer att till samverkanspunkter överföra trafik som förs över Sveriges gräns kommer inte i konflikt med egendomsskyddet i regeringsformen eller Europakonventionen.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: Remissinstanserna delar promemorians bedömning eller lämnar den utan erinran.

Skälen för regeringens bedömning

Skyldigheten att överföra trafik till samverkanspunkter

Den föreslagna skyldigheten för trådägande operatörer att till samverkanspunkter överföra trafik som förs över Sveriges gräns aktualiserar frågan om skyddet för egendom. Av 2 kap. 18 § regeringsformen framgår att varje medborgares egendom är tryggad genom att ingen kan tvingas avstå sin egendom till det allmänna eller till någon enskild genom expropriation eller annat sådant förfogande eller tåla att det allmänna inskränker användningen av mark eller byggnad utom när det krävs för att tillgodose angelägna allmänna intressen. Den som genom expropriation

eller liknade förfogande tvingas avstå från sin egendom tillförsäkras ersättning för förlusten. Under vissa närmare angivna förutsättningar tillförsäkras sådan ersättning också den för vilken det allmänna på visst sätt inskränker användningen av mark eller byggnad.

Ett skydd för enskildas egendom återfinns också i Europakonventionen. Enligt artikel 1 i första tilläggsprotokollet till konventionen har varje fysisk eller juridisk person rätt till respekt för sin egendom. Ingen får berövas sin egendom annat än i det allmännas intresse och under förutsättningar som anges i lag och i folkrättens grundsatser. Av artikeln framgår vidare att egendomsskyddet inte inskränker en stats rätt att genomföra sådan lagstiftning som staten finner nödvändig för att reglera nyttjandet av egendom i överensstämmelse med det allmännas intresse eller för vissa andra angivna ändamål. Rätten till ersättning berörs inte i tilläggsprotokollet, men i Europadomstolens praxis anses möjligheten för den enskilde att få ersättning vid ett ingrepp utgöra en viktig faktor att beakta vid bedömningen av om ingreppet är proportionerligt (Danelius, Mänskliga rättigheter i europeisk praxis, 2002, s. 377).

Den skyldighet som genom förslaget åläggs trådägande operatörer att till samverkanspunkter överföra trafik som förs över Sveriges gräns utgör inte något egendomsberövande eller någon inskränkning i förfoganderätten över egendom. Inte heller kan förpliktelsen för operatörerna anses innebära att det allmänna i något annat avseende gör anspråk på att förfoga över operatörernas egendom på sådant sätt att förfarandet kan uppfattas som en sådan inskränkning av egendomsskyddet enligt 2 kap. 18 § regeringsformen eller respekten för egendom enligt artikel 1 i första tilläggsprotokollet till Europakonventionen att det därför föreligger hinder mot att ålägga operatörerna en sådan skyldighet. Det kan visserligen diskuteras om inte den skyldighet som åläggs operatörerna i sig innebär en ekonomisk belastning som kan sägas beröra egendomsskyddet i Europakonventionen. Under alla omständigheter får underrättelseverksamheten dock anses utgöra ett så angeläget allmänt intresse att inskränkningen i vart fall måste tolereras.

Hur kostnadsansvaret för bl.a. nödvändig teknisk anpassning skall fördelas behandlas närmare i avsnitt 10.

Tillgodogörandet av information

Regelverket till skydd för egendom aktualiserar också frågan om informationen som sådan kan anses utgöra ett självständigt objekt (jfr. Christina Wainikka i SvJT 2003 s. 577) och om det tillgodogörande av informationsinnehåll – oavsett informationsbärare – som signalspaningsverksamheten innefattar kan anses komma i konflikt med egendomsskyddet.

Avgörande för denna bedömning är att även om den myndighet som bedriver signalspaningsverksamheten tillgodogör sig informationsinnehållet innebär inte detta att informationsinnehavarens – i regel avsändaren, men i vissa fall mottagaren eller båda – tillgång till informationen påverkas i något avseende. Signalspaningen medför följaktligen inte något intrång i en ägande- eller säkerhetsrätt. Vad som möjligen skulle kunna aktualiseras är i stället intrång i ensamrätt till immateriell egendom (jfr. NJA 2001 s. 362). För att en kränkning av ensamrätten till en immateriell tillgång skall anses föreligga krävs dock, utöver tillgodogö-

rande av informationsinnehållet, utnyttjande eller någon annan åtgärd som utgör intrång i ensamrätten. Hanteringen av information som inhämtas genom signalspaning kan inte anses innefatta någon sådan åtgärd.

8 Kontrollfunktionen

8.1 Allmänt

Uppgiften att följa underrättelsetjänsten inom Försvarsmakten och de övriga myndigheter som bedriver försvarsunderrättelseverksamhet, alltså Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut, åligger Försvarets underrättelsenämnd. Detta framgår av 1 § förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd.

I betänkandet Den militära underrättelsetjänsten (SOU 1976:19) uttalade Underrättelseutredningen följande i samband med sitt förslag om att inrätta en Försvarets underrättelsenämnd (s. 29).

> En djup sekretess är nödvändig kring stora delar av det militära underrättelseväsendet av hänsyn till landets säkerhet och förhållandet till främmande makter. Enskilda medborgare har därför små möjligheter att själva informera sig om underrättelsetjänsten och bilda sig en uppfattning i frågor som rör denna verksamhet. Under sådana förhållanden är det betydelsefullt att begränsningarna i den enskilda insynen uppvägs av en effektivt verkande kontroll genom statsmakternas försorg.

Som en följd av Underrättelseutredningens förslag inrättades därför Försvarets underrättelsenämnd den 1 juli 1976. Syftet med nämnden var att den skulle utgöra regeringens insyns- och kontrollorgan med uppgift att fortlöpande följa verksamheten hos den militära underrättelsetjänsten och lämna de förslag som föranleddes av granskningen. Försvarets underrättelsenämnd skall enligt sin nuvarande instruktion följa underrättelsetjänsten vid de myndigheter som omfattas av lagen (2000:130) om försvarsunderrättelseverksamhet. Nämnden skall särskilt

- följa hur lagen och förordningen (2000:131) om försvarsunderrättelseverksamhet tillämpas,
- granska att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning som är bestämd,
- ägna uppmärksamhet åt de enheter inom Försvarsmakten och Försvarets radioanstalt som inhämtar underrättelser med särskilda metoder,
- granska de medel och metoder för inhämtning av underrättelser som används,
- granska hur de register som behövs för försvarsunderrättelseverksamheten läggs upp och förs, samt
- granska principer för rekrytering och utbildning av personal.

Försvarets underrättelsenämnd skall lämna Försvarsmakten och de övriga myndigheter som bedriver försvarsunderrättelseverksamhet de synpunkter och de förslag till åtgärder som föranleds av granskningsverksamheten. Om det behövs skall nämnden också lämna förslag om åtgärder till regeringen. Försvarets underrättelsenämnd skall senast den 1 mars

varje år till regeringen lämna en rapport över föregående års granskningsverksamhet.

Försvarets underrättelsenämnd består av sex ledamöter, varav en är ordförande, som alla utses av regeringen för en bestämd tid. Vid nämnden finns en sekreterare. Nämnden sammanträder på kallelse av ordföranden minst fyra gånger per år.

Utöver Försvarets underrättelsenämnd finns naturligtvis även för försvarsunderrättelseverksamheten, som i övrigt för den offentliga sektorn, ett antal särskilda tillsynsorgan med olika granskningsområden och befogenheter. Genom riksdagens ombudsmän (JO) har riksdagen ett instrument för att kontrollera att tjänstemän och andra som utövar offentlig verksamhet i sin tjänsteutövning efterlever lagar och andra författningar och i övrigt fullgör sina åligganden. Motsvarande organ för regeringens del är Justitiekanslern (JK). Det bör vidare framhållas att även Riksrevisionen och Datainspektionen är kontrollorgan vilkas ansvar omfattar den aktuella verksamheten.

I detta sammanhang kan som jämförelse nämnas att inom polisens område har en särskild myndighet, Registernämnden, vissa tillsynsuppgifter. Nämnden skall i första hand pröva frågor om utlämnande av uppgifter från vissa av polisens register i samband med registerkontroll. Registernämnden har emellertid därutöver också till uppgift att granska Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (1998:622), särskilt med avseende på behandlingen av känsliga personuppgifter.

8.2 En förstärkt kontroll av försvarsunderrättelseverksamheten

Regeringens förslag: Försvarsunderrättelseverksamheten skall kontrolleras av den myndighet som regeringen bestämmer.

Myndigheten skall kontrollera att lagen om signalspaning i försvarsunderrättelseverksamhet följs och särskilt granska användning av sökbegrepp, förstöring av uppgifter och rapportering enligt den lagen.

Myndigheten skall få besluta att viss inhämtning skall upphöra eller att upptagning eller uppteckning av inhämtade uppgifter skall förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med lagen eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten.

Promemorians förslag överensstämmer delvis med regeringens. I promemorian saknas förslag om att Försvarets underrättelsenämnd skall kunna besluta om att inhämtning skall upphöra eller uppgifter förstöras.

Remissinstanserna: De flesta remissinstanserna tillstyrker förslaget eller lämnar det utan erinran. *Hovrätten för Övre Norrland* och *Kammarrätten i Jönköping* har anfört att kontrollmyndigheten inte har getts befogenheter att ingripa om nämnden anser att regleringen inte följs annat än genom att lämna synpunkter och förslag till myndigheten och till regeringen. Detta förutsätter att den kontrollerade myndigheten eller regeringen delar nämnden uppfattning. Om den kontrollerade myndigheten väljer att inte göra någon förändring har nämnden inte getts någon befogenhet

att vidta ytterligare åtgärder, varför den i praktiken inte kan anses vara någon stark garant för att den enskildes rättigheter inte träds förnär.

Skälen för regeringens förslag

Behovet av utökad kontroll

Den underrättelseverksamhet som bedrivs till stöd för landets utrikes-, säkerhets- och försvarspolitik måste av naturliga skäl omgärdas av en sträng sekretess. Den begränsade insyn som följer härmed kan i kombination med arten av den verksamhet som bedrivs leda till farhågor hos enskilda medborgare om att verksamheten inte bedrivs på ett korrekt sätt. Att underrättelseverksamheten är föremål för en effektiv och ändamålsenlig insyn och kontroll är mot denna bakgrund ett viktigt element för att skapa förtroende för denna centrala och ibland känsliga verksamhet.

Försvarets underrättelsenämnds uppgift är idag att följa underrättelsetjänsten inom de myndigheter som utövar försvarsunderrättelseverksamhet. När mandatet för försvarsunderrättelseverksamhet utökas finns anledning att ytterligare betona betydelsen av en utomstående granskning av dessa myndigheters verksamhet. Försvarets underrättelsenämnd har redan idag den grundläggande kompetens som behövs för att utöva den granskning som verksamheten kräver. Regeringens uppfattning är därför att det är lämpligt att utöka nämndens arbetsuppgifter till att *kontrollera* försvarsunderrättelseverksamheten hos de myndigheter som bedriver sådan verksamhet.

Mot bakgrund av det förändrade mandatet för försvarsunderrättelseverksamheten är det av stor vikt att den särskilda inhämtningen, såväl teknisk som personbaserad, kontrolleras och granskas närmare. Det utvidgade signalspaningsmandatet innebär också att behovet av kontroll ökar.

Särskilt om kontroll enligt lagen om signalspaning

Det förhållandet att signalspaningsmandatet nu utvidgas till att även omfatta inhämtning av trådburna signaler i elektronisk form innebär inte att den hittills gällande ordningen för kontroll av verksamheten behöver förändras i grunden. Försvarets underrättelsenämnd har ingående kunskaper om inhämtning med särskilda metoder och det är därför naturligt att nämndens granskning också omfattar den utvidgade signalspaningsverksamheten.

Enligt förslaget till lag om signalspaning i försvarsunderrättelseverksamhet skall Försvarets underrättelsenämnd också få till uppgift att ge tillstånd till den närmare inriktningen av signalspaningsverksamheten. Tillståndsprövningen skall ske i en särskild avdelning inom nämnden, se avsnitt 7.4.3. Den kontroll som Försvarets underrättelsenämnd därefter utövar i fråga om Försvarets radioanstalts inhämtning i enlighet med en sådan inriktning omfattar inte innehållet i den närmare inriktningen, däremot kommer granskningen att omfatta att inhämtningen utförts i enlighet med inriktningen, samt formerna för denna inhämtning. En väsentlig del i kontrollen är att säkerställa spårbarheten, dvs. att den inhämtning

som genomförs kan kopplas till en viss given inriktning och att ingen inhämtning bedrivs utan att en inriktning föreligger.

Det är naturligtvis särskilt angeläget att kontrollen omfattar sådan verksamhet i samband med signalspaningen som särskilt medför att enskildas integritetsintresse kan komma att påverkas. Regeringen anser därför att det i lagen särskilt bör anges att Försvarets underrättelsenämnd skall granska de sökbegrepp som Försvarets radioanstalt enligt vad som är närmare föreskrivet skall använda i inhämtningssystemen. Som ett led i kontrollverksamheten skall Försvarets radioanstalt fortlöpande lämna en redogörelse till Försvarets underrättelsenämnd om vilka sökbegrepp som används. Detta förfarande inskränker naturligtvis inte nämndens möjlighet att även på annat sätt som nämnden finner lämpligt utföra sin kontroll, t.ex. genom att vid besök hos Försvarets radioanstalt granska sökbegreppsanvändningen. Nämnden skall vid sin granskning av sökbegreppen särskilt kontrollera att de är förenliga med de syften som anges i lagen om signalspaning och att de utformas på ett sätt som inte medför otillbörligt intrång i enskildas personliga integritet.

Försvarets underrättelsenämnd skall även granska att uppgifter förstörs i den utsträckning som följer av lagen och att rapporteringen av underrättelser som inhämtats genom signalspaning är förenlig med ändamålet för verksamheten såsom det formulerats i lagen om försvarsunderrättelseverksamhet och lagen om signalspaning. Genom denna kontroll säkerställs att det under hela underrättelseprocessen sker kontinuerliga bedömningar av uppgifters relevans för verksamheten och att de åtgärder som lagen föreskriver när det gäller förstöring av uppgifter och rapportering av underrättelser utförs på ett korrekt sätt.

Den återrapportering som nämnden skall göra avseende sin granskning regleras i nämndens instruktion. I promemorian har inte föreslagits att nämnden skall kunna vidta några andra åtgärder med anledning av de iakttagelser som görs i kontrollverksamheten. *Hovrätten för Övre Norrland* och *Kammarrätten i Jönköping* har efterlyst andra möjligheter för nämnden att agera om den anser att reglerna för verksamheten inte följs.

Organ som utövar kontroll och tillsyn över offentlig verksamhet har i regel inte några möjligheter att vidta direkta åtgärder mot en annan myndighet. Den tillsyn som Riksdagens ombudsmän utövar kan t.ex. resultera i ett uttalande i frågan om en åtgärd av en myndighet eller tjänsteman strider mot lag eller annan författning eller annars är felaktig eller olämplig (en s.k. erinran) eller i åtal mot en enskild befattningshavare, men kan inte på annat sätt stoppa eller förhindra viss verksamhet. Inte heller Justitiekanslern har någon sådan möjlighet. När det gäller tillsyn på begränsade områden kan konstateras att Datainspektionens befogenhet enligt 44 § personuppgiftslagen (1998:204) att vid vite förbjuda viss behandling av personuppgifter inte ansetts vara lämplig att använda i förhållande till andra myndigheter beträffande vilka personuppgiftsbehandlingen reglerats i särskild lag, eftersom vite som sanktionsmedel enligt allmänna rättsgrundsatser inte bör användas som sanktionsmedel mellan statliga myndigheter (se t.ex. prop. 2004/05:164 s. 54). Datainspektionen är då hänvisad till att genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Ett beslut om att olagligt behandlade personuppgifter skall utplånas kan inte fattas av Datainspektionen, utan myndigheten

är hänvisad till att hos länsrätt ansöka om detta, 47 § personuppgiftslagen.

En möjlighet för Försvarets underrättelsenämnd att agera mer påtagligt i förhållande till signalspaningsmyndigheten med anledning av iakttagelser i samband med sin kontroll kan inte utan ytterligare överväganden förenas med någon form av sanktion. Redan en i lagen uttryckt rätt för nämnden att genom beslut meddela anvisningar för signalspaningsmyndigheten skulle dock kunna fungera som en tydlig markering av att nämndens kontrollverksamhet kan och skall resultera i omedelbara reaktioner. Även utan en reglerad sanktionsmöjlighet är det för övrigt självklart att signalspaningsmyndigheten skall rätta sig efter nämndens beslut.

Mot denna bakgrund delar regeringen den bedömning som Hovrätten för Övre Norrland och Kammarrätten i Jönköping gjort att en möjlighet för nämnden att vidta åtgärder i de fall då kontrollen utvisar att regelverket inte följs skulle bidra till ett förstärkt skydd för enskilda. Försvarets underrättelsenämnd bör därför ges en rätt att fatta beslut om att vissa typer av åtgärder skall vidtas om det vid kontroll framkommer att inhämtningen inte är förenlig med lag eller annars utgör ett intrång i enskildas rättigheter som inte står i rimlig proportion till syftet med verksamheten.

De åtgärder som nämnden bör kunna besluta om bör dels vara att en viss närmare angiven pågående inhämtning skall avbrytas, dels att en upptagning eller uppteckning av redan inhämtade uppgifter skall förstöras. Nämnden får i varje enskilt fall avgöra omfattningen av åtgärden. Ett beslut om avbrytande av en inhämtning skulle t.ex. kunna avse alltifrån att en viss företeelse överhuvudtaget inte skall vara föremål för kartläggning till att vissa sökbegrepp inte skall få användas.

Beslut av Försvarets underrättelsenämnd kan aktualiseras i samband med löpande kontroll på nämndens eget initiativ eller efter särskilda kontrollåtgärder som föranletts av upplysningar som t.ex. lämnats av det integritetsskyddsråd inom FRA som regeringen enligt vad som närmare redovisas i avsnitt 7.3.4 avser att inrätta. Det är med hänsyn till verksamhetens syfte och karaktär dock inte meningsfullt att införa en formaliserad möjlighet för enskilda att framföra klagomål på signalspaningsverksamhet. Signalspaning får endast avse utländska förhållanden och det ligger i verksamhetens natur att den inte skall bli känd. Det står dock naturligtvis nämnden fritt att agera på grundval av information oavsett varifrån den kommer.

För att Försvarets underrättelsenämnd skall kunna utföra en reell tillståndsprövning och effektiv kontroll krävs att nämnden förstärks med ytterligare juridisk kompetens och en utbyggd kanslifunktion. Vilka förändringar som behövs beskrivs närmare avsnitt 11.1 Regeringen avser att i nämndens instruktion närmare föreskriva om regler avseende kontroll, organisation och handläggning.

9 Sekretess till skydd för enskilds personliga eller ekonomiska förhållanden

Regeringens förslag: I sekretesslagen (1980:100) skall införas en bestämmelse om att sekretess gäller för uppgift om enskilds personliga eller ekonomiska förhållanden hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos Försvarets radioanstalt i underrättelse- och säkerhetsverksamheten.

Sekretess för sådan uppgift skall gälla om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till den enskilde lider skada eller men.

I fråga om uppgift i allmän handling skall sekretessen gälla i högst sjuttio år.

Den nya sekretessbestämmelsen skall inte ha företräde framför meddelarfriheten.

Utredningens förslag innebär att en sekretessbestämmelse till skydd för den enskilde skall gälla hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten. Bestämmelsen skall enligt förslaget innehålla ett omvänt skaderekvisit, vilket innebär att det skall råda en presumtion för sekretess. Utredningen föreslår däremot inte någon motsvarande sekretess för Försvarets radioanstalts underrättelse- och säkerhetsverksamhet. Utredningen har inte berört frågan om meddelarfrihet.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt eller inte haft något att erinra mot utredningens förslag. Med undantag av *Kammarrätten i Stockholm* har remissinstanserna inte yttrat sig över behovet av en sekretessbestämmelse i Försvarets radioanstalts underrättelse- och säkerhetsverksamhet. Kammarrätten konstaterar att det av utredningens redovisning angående behovet av en sådan bestämmelse inte går att utläsa att motsvarande förhållanden inte är för handen hos Försvarets radioanstalt. För det fall förhållandena är likartade bör, enligt kammarrätten, det föreslagna sekretesskyddet för enskild gälla även hos Försvarets radioanstalt.

Bakgrund

Försvarsmakten och Försvarets radioanstalt är två av de myndigheter som bedriver försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet. Försvarets radioanstalt bedriver också viss annan verksamhet av teknisk karaktär som syftar till att tillgodose myndighetens behov av anpassning av sina tekniska system. Försvarsunderrättelseverksamheten har beskrivits i avsnitt 5.

Myndigheterna bedriver också säkerhetsskyddsverksamhet enligt säkerhetsskyddslagen (1996:627). Med säkerhetsskydd avses dels skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet, dels

skydd i andra fall av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet. Vidare avses med säkerhetsskydd även skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet. Försvarsmakten skall med stöd av 4 § 2 förordningen (2000:555) med instruktion för Försvarsmakten leda och bedriva militär säkerhetstjänst.

Den militära säkerhetstjänstens uppgift är att upptäcka, identifiera och möta säkerhetshot som riktas mot Försvarsmakten och dess säkerhetsintressen såväl inom som utom landet. Häri ingår bl.a. att biträda polisen i dess ansvar beträffande skyddet av rikets säkerhet. Försvarsmaktens säkerhetsintressen kan hänföras till personal, materiel, anläggningar, information samt planering och planer i vid bemärkelse.

Den säkerhetshotande verksamhet som riktas mot Försvarsmakten brukar delas in i underrättelseverksamhet, sabotage, subversiv verksamhet, terrorism samt annan kriminalitet. Den kan riktas mot hela eller delar av Försvarsmakten, viss funktion eller verksamhet och förband samt verksamhet inom Försvarsmaktens intresseområde, t.ex. försvarsindustri. Underrättelseverksamhet riktad mot Försvarsmakten kan bedrivas av såväl främmande makt som olika organisationer, företag och kriminella personer. Främmande makts underrättelseverksamhet kan ske på svenskt territorium, utanför landet eller riktas mot Försvarsmakten i samband med internationell verksamhet eller uppträdande utomlands i andra sammanhang.

Den militära säkerhetstjänsten omfattar säkerhetsunderrättelsetjänst och säkerhetsskyddstjänst. Säkerhetsunderrättelsetjänsten har till uppgift att klarlägga den säkerhetshotande verksamhetens omfattning, inriktning samt medel och metoder. Dess syfte är att utifrån aktuella säkerhetsunderrättelsebehov lämna underlag för beslut om t.ex. säkerhetsskyddsåtgärder, beredskap eller förbandsproduktion. Säkerhetsskyddstjänstens uppgift är att ta fram åtgärder som syftar till att hindra eller försvåra säkerhetshotande verksamhet. Den arbetar med att förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Säkerhetsskyddstjänsten skyddar också materiel och anläggningar mot sabotage och stöld samt personal, anläggningar och materiel mot terrorism. Säkerhetsskyddstjänsten omfattar informationssäkerhet inklusive IT-säkerhet, säkerhetsprövning, tillträdesbegränsning, utbildning och kontroll av säkerhetsskyddet.

Även Försvarets radioanstalt bedriver för egna behov viss säkerhetsunderrättelse- och säkerhetsskyddstjänst enligt vad som angetts ovan. Därutöver bedriver myndigheten inom ramen för sin säkerhetsverksamhet också sådan verksamhet på informationssäkerhetsområdet som framgår av 3 a § i förordningen (1994:714) med instruktion för Försvarets radioanstalt. Myndigheten skall därvid bl.a. stödja myndigheter som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller ur ett säkerhets- eller försvarspolitiskt avseende.

Skälen för regeringens förslag

Behovet av en sekretessbestämmelse

I den försvarsunderrättelseverksamhet och militära säkerhetstjänst som Försvarsmakten bedriver samt i Försvarets radioanstalts underrättelse- och säkerhetsverksamhet behandlas uppgifter som kan vara känsliga med hänsyn till enskildas personliga och ekonomiska förhållanden. I såväl försvarsunderrättelseverksamheten som säkerhetstjänsten kan det t.ex. förekomma uppgifter om en persons politiska åsikter. Sådana uppgifter kan inom försvarsunderrättelseverksamheten vara relevanta för att bedöma utländska beslutsfattares bevekelsegrunder eller vara av intresse inom säkerhetstjänsten för att kartlägga potentiella hot mot verksamheten. I dessa sammanhang kan det även komma ifråga att behandla uppgifter om lagöverträdelser eller uppgifter som på annat sätt gör en person sårbar ur säkerhetssynpunkt, t.ex. uppgifter om familjeförhållanden, ekonomisk situation eller sexuell läggning. Ett utlämnande av sådana personliga uppgifter kan naturligtvis vara till skada eller men för såväl den enskilde själv som för närstående till den som uppgifterna rör.

De personer om vilka det förekommer uppgifter i försvarsunderrättelseverksamheten och säkerhetstjänsten är ofta politiska beslutsfattare eller militära befattningshavare i andra stater. Även uppgifter om andra enskilda privatpersoner kan dock förekomma, t.ex. sådana som uppträtt som uppgiftslämnare eller på annat sätt haft anknytning till verksamheten.

Uppgifter hos Försvarsmakten respektive Försvarets radioanstalt inom de berörda verksamheterna omfattas i många fall av reglerna om så kallad utrikes- och/eller försvarssekretess i 2 kap. 1 och 2 §§ sekretesslagen (1980:100). Enligt 2 kap. 1 § sekretesslagen gäller sekretess för uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Enligt 2 kap. 2 § gäller sekretess för uppgift som angår verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Sekretessen enligt 2 kap. 1–2 §§ sekretesslagen gäller vanligtvis i högst 40 år.

Den utrikes- och försvarssekretess som gäller i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och säkerhetsverksamhet syftar endast till att skydda verksamheten hos myndigheterna och utgör inget skydd för enskilda individer och deras personliga eller ekonomiska intressen. I det fall sekretess inte kan göras gällande till skydd för det allmänna finns det ingen regel om sekretess som direkt omfattar uppgifter om enskilds personliga och ekonomiska förhållanden. Det saknas följaktligen sekretessskydd för sådana uppgifter som lämnats eller inhämtats om en person och som inte är av den karaktären att de skyddas av försvarssekretessen men som om de utlämnas kan vara till skada eller men för den enskilde eller närstående.

De uppgifter om enskilda som förekommer i de aktuella verksamheterna är av känslig karaktär. Uppgifter om politisk åskådning omfattas exempelvis av absolut sekretess i samband med val (7 kap. 49 § sekretesslagen) och uppgifter om lagöverträdelser eller sexuell läggning får anses vara integritetskänsliga uppgifter. Även uppgifter om att en enskild har ekonomiska problem får betraktas som känsliga. Till detta kommer att uppgifterna i den här aktuella verksamheten ofta har inhämtats utan den enskildes vetskap. Ovanstående talar för att enskildas integritetsskydd bör ges företräde framför insynsintresset beträffande de uppgifter som nu är ifråga.

Den begränsning i möjligheten till insyn som en sådan reglering skulle innebära kan till viss del uppvägas av den kontroll som utövas av Försvarets underrättelsenämnd. Det skall vidare nämnas att det följer av 14 kap. 4 § sekretesslagen att den föreslagna sekretessen till skydd för enskild inte kommer att gälla mot den enskilde själv. En uppgift som inte omfattas av annan sekretess, t. ex sekretessen enligt 2 kap. 2 § sekretesslagen, kommer alltså att kunna lämnas ut till den som sekretessen avser att skydda i samma utsträckning som idag.

Mot angiven bakgrund bör i enlighet med utredningens förslag en sekretessbestämmelse införas som innebär att uppgifter i de aktuella verksamheterna om enskilds personliga eller ekonomiska förhållanden skall få sekretesskydd. Sekretessen skall endast gälla i verksamheten hos de angivna myndigheterna. Uppgifter som rapporteras till andra myndigheter omfattas av den sekretess som gäller i den mottagande myndighetens verksamhet. För uppgifter av sådan betydelse att de blir föremål för rapportering gäller dock i regel sekretess också enligt 2 kap. 2 § sekretesslagen, som är tillämplig oavsett hos vilken myndighet uppgiften finns.

Vad gäller styrkan av sekretesskyddet är det av intresse hur skaderekvisiten utformats i fråga om den sekretess som gäller till skydd för enskildas personliga eller ekonomiska förhållanden i bland annat Säkerhetspolisens verksamhet enligt 9 kap. 17 § sekretesslagen samt hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddade verksamhet enligt 9 kap. 26 § sekretesslagen. Dessa sekretessbestämmelser innehåller ett så kallat omvänt skaderekvisit, vilket innebär att det finns en presumtion för sekretess. Utredningen har föreslagit att även den nya bestämmelsen skall innehålla ett omvänt skaderekvisit. Inga remissinstanser har invänt mot detta. Regeringen delar utredningens uppfattning att det med hänsyn till integritetsskyddsintresset får anses föreligga övervägande skäl för att sekretess skall vara utgångspunkten för uppgifter om enskildas personliga och ekonomiska förhållanden som förekommer i de nu aktuella verksamheterna.

Behovet av sekretesskydd gör sig, som *Kammarrätten i Stockholm* påpekat och som regeringen redogjort för ovan, gällande inte bara i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst utan också i Försvarets radioanstalts underrättelse- och säkerhetsverksamhet. Bestämmelsen bör därför omfatta även denna verksamhet. Eftersom bestämmelsen skall skydda såväl enskilds personliga som ekonomiska förhållanden bör den placeras i sekretesslagens nionde kapitel.

Sekretesstiden

I fråga om sekretess till skydd för det allmännas verksamhet varierar sekretesstiderna. Utrikes- och försvarssekretessen gäller, såsom ovan nämnts, enligt sekretesslagen i högst 40 år. När det gäller uppgifter som omfattas av försvarssekretess har emellertid regeringen bemyndigats att föreskriva att sekretessen skall gälla under längre tid. Regeringen har i 1 § sekretessförordningen (1980:657) föreskrivit att sekretessen gäller i högst 70 år om uppgifterna i en allmän handling angår bl.a. underrättelseverksamheten inom underrättelsetjänsten.

I propositionen om ny sekretesslag föreslogs att en sekretesstid om 70 år skulle gälla för de viktigaste bestämmelserna om skydd för enskilds personliga förhållanden (prop. 1979/80:2 del A s. 493f.). Som framgått ovan hanteras inom Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt Försvarets radioanstalts underrättelse- och säkerhetsverksamheten uppgifter som kan vara av mycket känslig natur för vilka sekretess gäller i högst sjuttio år när de förekommer i allmän handling i annan verksamhet. Ett sådant exempel är den tidigare berörda sekretessbestämmelsen avseende uppgifter hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet (9 kap. 26 § sekretesslagen).

Sekretesstiden bör därför också i fråga om uppgifter i allmän handling om enskilds personliga eller ekonomiska förhållanden hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos Försvarets radioanstalt i underrättelse- och säkerhetsverksamheten vara högst 70 år.

Sedan den 1 mars 2003 gäller att sekretess till skydd för enskildas personliga och ekonomiska förhållanden enligt 9 kap. 17 § första stycket 1–4 och 5 sekretesslagen inte skall gälla avseende uppgifter hos Säkerhetspolisen från tiden före 1949 (prop. 2001/02:191). Syftet med undantaget är att allmänheten skall ges möjlighet till insyn i de handlingar som finns hos Säkerhetspolisen avseende svenska myndigheters och enskildas förhållningssätt till Tyskland och nazismen under andra världskriget (a. prop. s. 88). De skäl som ligger bakom undantaget gör sig i viss mån också gällande i förhållande till uppgifter i den verksamhet som avses med den här föreslagna sekretessbestämmelsen. Regeringen bedömer emellertid att frågan om undantag från den nu föreslagna sekretessbestämmelsen måste lösas tillsammans med frågan om motsvarande undantag från försvarssekretessen i 2 kap. 2 § sekretesslagen. Beträffande den senare frågan pågår ett arbete i Regeringskansliet. Tillräckligt underlag för att nu ta ställning till omfattningen och utformningen av ett sådant undantag föreligger dock inte. Regeringen avser mot denna bakgrund att så snart som möjligt återkomma med förslag om hur forskningens intressen skall tillgodoses när det gäller möjligheten till tillgång till uppgifter i den militära underrättelse- och säkerhetstjänstens arkiv.

Meddelarfrihet

Med meddelarfrihet avses rätten enligt 1 kap. 1 § tredje stycket tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen att lämna uppgift i vilket ämne som helst för publicering i de medier som de båda

grundlagarna omfattar. Meddelarfriheten är dock inte oinskränkt. Det är inte tillåtet att uppsåtligen lämna ut en allmän handling som omfattas av sekretess. Det är inte heller tillåtet att åsidosätta tystnadsplikt i de fall som anges antingen i tryckfrihetsförordningen och yttrandefrihetsgrundlagen eller i 16 kap. 1 § sekretesslagen. Bestämmelsen om försvarssekretess i 2 kap 2 § sekretesslagen anges inte i uppräkningen av sekretessbestämmelser som har företräde framför meddelarfriheten i 16 kap. 1 § sekretesslagen. Däremot följer av 7 kap. 3 § första stycket 1 tryckfrihetsförordningen att meddelarfrihet inte föreligger i fråga om meddelanden som innebär att någon gör sig skyldig till högförräderi, spionerі, grovt spionerі, grov obehörig befattning med hemlig uppgift, uppror, landsförräderi, landssvek eller försök, förberedelse eller stämpling till sådant brott. Motsvarande bestämmelse återfinns också i yttrandefrihetsgrundlagen. Detta innebär att meddelarfriheten är starkt begränsad på försvarssekretessens område.

Eftersom försvarsunderrättelseverksamheten redan omgärdas av ett starkt sekretesskydd är det angeläget att i samband med att en ny sekretessbestämmelse införs överväga om det finns skäl att låta även den tystnadsplikt som följer av den nya bestämmelsen ha företräde framför meddelarfriheten. Därvid måste beaktas att möjligheten till insyn i och granskning av verksamheten ytterligare försvåras med en sådan ordning. Det kan visserligen hävdas att när det gäller uppgifter som omfattas av den nu aktuella bestämmelsen – uppgifter om enskildas personliga eller ekonomiska förhållanden – är behovet av insyn mer begränsat än när det gäller uppgifter om verksamheten som sådan. Mot detta kan emellertid anföras att den allmänna debatten kring en myndighets verksamhet inte sällan utgår från enskilda fall.

Vid en jämförelse med andra områden kan konstateras att beträffande den sekretess till skydd för enskildas personliga och ekonomiska förhållanden som enligt 9 kap. 17 § sekretesslagen gäller för bl.a. uppgifter i Säkerhetspolisens verksamhet föreskrivs inte något undantag från meddelarfriheten.

Sammantaget finner regeringen att övervägande skäl talar emot att låta den tystnadsplikt som följer av den föreslagna bestämmelsen ha företräde framför meddelarfriheten. Någon ändring i 16 kap. sekretesslagen föreslås därför inte.

10 Ikraftträdande och övergångsbestämmelser

Regeringens förslag: Ändringarna i lagen om försvarsunderrättelseverksamhet och sekretesslagen samt den nya lagen om signalspaning i försvarsunderrättelseverksamhet skall träda i kraft den 1 juli 2007.

Även ändringarna i lagen om elektronisk kommunikation skall träda i kraft den 1 juli 2007. Skyldigheten för operatörer som äger tråd att överföra signaler till samverkanspunkter enligt 6 kap. 19 a § skall dock gälla från och med den 1 juli 2008.

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten enligt lagen (2003:389) om elektronisk kommunikation får

meddela föreskrifter om att bestämmelserna om skyldigheten skall börja tillämpas senare.

Promemorians förslag överensstämmer delvis med regeringens. Promemorian föreslog att skyldigheten för de trådägande operatörerna att överföra signaler till samverkanspunkter skall gälla från och med den 1 januari 2007.

Remissinstanserna: *Swedish Network User Society* och *Vetensakpsrådet* har anfört att det finns risk att tiden om sex månader innan driftssättning av systemet är för snävt för operatörerna. *Telia Sonera AB* har påpekat att bolaget skulle tvingas till en större del manuell omkoppling om det beslutas om en snabb implementering.

Skälen för regeringens förslag: Den föreslagna regleringen bör träda i kraft den 1 juli 2007.

Som framhålls i promemorian är det rimligt att de operatörer som äger tråd får en viss tid på sig för att förbereda sina system så att överföringen av trafiken skall kunna ske till samverkanspunkterna. I och med att bestämmelserna i LEK föreslås träda i kraft den 1 juli 2007 är det därför befogat att de trådägande operatörerna ges ytterligare viss tid på sig för att förbereda systemen för den första samverkanspunkten. Regeringen anser med hänsyn till vad som anförts av remissinstanserna och till kostnaderna för operatörerna att det är skäligt att bestämma en längre tid för detta än vad som angetts i promemorian. Skyldigheten i detta hänseende för operatörerna föreslås därför tidigast gälla från och med den 1 juli 2008. Det kan även härefter finnas skäl att senarelägga skyldigheten, exempelvis för överföring till ytterligare punkter, eller om Försvarets radioanstalt inte har färdigställt de utsedda samverkanspunkterna. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten bör därför kunna meddela föreskrifter om när bestämmelserna om skyldighet för operatörer som äger tråd att överföra signaler till samverkanspunkter i 6 kap. 19 a § skall tillämpas första gången.

11 Konsekvenser och genomförande

11.1 Myndigheterna

Regeringens bedömning: De merkostnader som förslaget innebär för Försvarets radioanstalt bör finansieras genom omföringar från andra anslag inom utgiftsområde 6 Försvar samt beredskap mot sårbarhet och genom omprioriteringar och besparingar inom den egna verksamheten. Kostnaderna för förstärkningen av Försvarets underrättelsenämnd bör finansieras genom omprioriteringar inom utgiftsområde 6. De ekonomiska konsekvenserna för Post- och telestyrelsen bedöms bli små och bör finansieras genom omföringar från utgiftsområde 6.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser som har yttrat sig har delat bedömningen eller lämnat den utan erinran. *Försvarets radioanstalt* har anfört att det i promemorian angivna investeringsbehovet är förknip-

pat med viss osäkerhet när det gäller den totala kostnadsbilden, eftersom denna påverkas av flera faktorer. Om syftet med inhämtningen är underrättelseproduktion behöver myndigheten endast göra investeringar där det kan finnas trafik av högt underrättelsevärde, vilket begränsar investeringsbehovet. Om syftet är att även kunna detektera IT-relaterade hot mot Sverige behöver utbyggnaden vara mera komplett och heltäckande i riket. De långsiktiga kostnaderna är också beroende av omsättningstakten av utrustning hos trådägarna. Försvarets radioanstalt måste uppgradera eller omsätta sin utrustning för inhämtning i takt med att trådägarna omsätter sin utrustning. Sammanfattningsvis har myndigheten anfört att det angivna behovet måste ses som ett första steg i uppbyggnaden.

Skälen för regeringens bedömning

Försvarets radioanstalt

För Försvarets radioanstalt innebär möjligheten att inhämta signaler i tråd en betydande ökning av den tillgängliga trafiken. Inhämtning av signaler i tråd är från en teknisk synvinkel en komplex verksamhet. I avsnitt 7 har formerna för den beskrivits. Nedan följer en beskrivning av kostnaderna.

En ny generation datastöd för bearbetning av trafik håller på att utvecklas vid Försvarets radioanstalt. Den första delen tas snart i drift och följs av kompletterande system de närmaste åren. Kostnaderna för bearbetningsstödet kan förenklat delas in i tre delar: utveckling, hårdvara samt lagringskapacitet. Kostnaderna för utveckling och hårdvara låg i huvudsak under 2005-2006 och påverkades endast marginellt av en eventuell trådaccess. Däremot följer behovet av lagringskapacitet mer eller mindre direkt från processkapaciteten – ju fler signaler som kan processas av Försvarets radioanstalt desto mer lagringskapacitet behövs. Detta kommer också att medföra betydande kostnader.

Sammantaget skulle de investeringar som hänför sig till att få tillgång till signaler i elektronisk form genomföras under en femårsperiod och uppgå till drygt 200 miljoner kronor. Det första året skulle investeringarna uppgå till cirka 30 miljoner kronor. Kapitalkostnaden för de beskrivna investeringarna beräknas uppgå till drygt 25 miljoner kronor i genomsnitt per år under avskrivningstiden.

Driftkostnaderna består till största del av sambandskostnader, lokalhyra för samverkanspunkter samt löner. Dessa beräknas under det första året till cirka 4 miljoner kronor för att när investeringarna är slutförda och fullt ut kan nyttjas beräknas till cirka 25 miljoner kronor.

Som *Försvarets radioanstalt* har anfört är beloppen förknippade med viss osäkerhet. Regeringen anser dock att de kan läggas till grund för en grundläggande bedömning av de ekonomiska konsekvenserna för myndigheten.

Försvarets radioanstalt bör delvis kompenseras för de ökade kapital- och driftskostnaderna genom omföringar från andra anslag och genom omprioriteringar och besparingar inom den egna verksamheten.

Försvarets underrättelsenämnd

Försvarets underrättelsenämnd har i dag en granskande myndighetsfunktion men är inte en förvaltningsmyndighet i traditionell mening, nämnden har t.ex. inga anställda. Försvarets underrättelsenämnd får i de föreslagna författningarna fler uppgifter än i dag. Kravet på att utföra en fortlöpande och mer ingående kontroll medför behov av organisatoriska förändringar, liksom uppgiften att pröva tillstånd till inriktning av signalspaning.

Försvarets underrättelsenämnd skall ha en självständig kontrollfunktion och vara fristående från de myndigheter som nämnden har att granska. Med beaktande av nämndens avgränsade ansvarsområde, organisationens ringa storlek och för att vinna ekonomiska och administrativa fördelar bör dock Försvarets underrättelsenämnd ges stöd i administrativt avseende och när det gäller t.ex. lokaler från någon annan myndighet. Nämndens ansvar och uppgifter skall dock beslutas av regeringen.

Merkostnaderna för de kanslifunktioner som Försvarets underrättelsenämnd kommer att behöva beräknas uppgå till sammanlagt cirka 5 miljoner kronor när verksamheten är i full drift. Det första året behöver dock ytterligare ett par miljoner kronor tillföras för att säkerställa ett fullgott säkerhetsskydd och initiala investeringar.

Därutöver behöver Försvarets underrättelsenämnd tillföras medel för arvodering, eftersom den nya uppgiften att fungera som tillståndsorgan föranleder viss utökning av nämndens sammansättning med ytterligare juridisk kompetens. Dessa kostnader beräknas uppgå till sammanlagt cirka 2 miljoner kronor. Kostnaden för nämndens verksamhet uppgår i dag till 1 miljon kronor. Finansieringen av de utökade kostnaderna för nämnden skall ske genom omprioriteringar inom utgiftsområde 6 Försvar samt beredskap mot sårbarhet.

Post- och telestyrelsen

Post- och telestyrelsen är central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, inom postområdet och området för elektronisk kommunikation.

För Post- och telestyrelsens del kommer förslaget till inhämtning av signaler i elektronisk form enligt lagen om signalspaning i försvarsunderrättelseverksamhet att innebära att myndigheten kan komma att utöva tillsyn och meddela föreskrifter inom området. Regeringen gör bedömningen att denna verksamhet och dess kostnader kommer att vara av mindre omfattning och bör finansieras genom omprioritering från anslag inom utgiftsområde 6.

11.2 Operatörerna

Regeringens förslag: De trådägande operatörerna skall stå för kostnaden för den tekniska anpassning som krävs för att signaler i elektronisk form i tråd skall kunna föras till samverkanspunkterna. Såväl trådägande som andra operatörer skall stå för kostnaden för att lämna sådan information som kan göra det enklare att ta hand om signalerna.

Regeringens bedömning: Förslaget innebär inte några beaktansvärda konkurrensnackdelar för de operatörer som berörs. Regeringen avser emellertid att göra en utvärdering av förslagets påverkan på den aktuella marknaden.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser som har yttrat sig har tillstyrkt förslaget eller lämnat det utan erinran. *Post- och telestyrelsen* har invänt mot bedömningen att de kostnader som kommer att uppstå kommer vara av engångskaraktär och efter denna initiala investering plana ut och endast omfatta vissa löpande kostnader. Styrelsen har framhållit att telekommarknaden är en mycket dynamisk verksamhet som är stadd i konstant förändring och att det därför är troligt att tekniken avseende samverkanspunkterna måste förändras i takt med teknikutvecklingen i övrigt. Styrelsen har jämfört med operatörers kostnader för anpassningsskyldigheten avseende hemlig teleavlyssning och hemlig teleövervakning, vilket visat sig vara en fortlöpande kostnad som hela tiden, allteftersom ny teknik innebär nya anpassningsbehov, belastar operatörerna. Styrelsen har vidare framfört att det ter sig mindre rimligt att en liten operatör föreläggs att anpassa sin verksamhet för miljonbelopp, och då framhållit fall där en operatör endast äger och tillhandahåller s.k. svartfiber, medan andra operatörer i praktiken förfogar över denna fiber.

Svenska IT-företagens organisation, Telia Sonera AB och *E.ON* har motsatt sig förslaget att teleoperatörerna skall stå för kostnaden av att leverera trafiken till de s.k. samverkanspunkterna och framhållit det som självklart att renodlat statliga angelägenheter till fullo skall finansieras via statsbudgeten. Svenska IT-företagens organisation har anfört att en annan ordning kan leda till ett överutnyttjande samt att en ur samhällsekonomisk synvinkel lämplig prioritering av resurser försvåras genom att den som beslutar kring prioriteringarna inte själv står för kostnaden. I det fall de trådägande operatörerna åläggs att själva stå för kostnaderna, uppstår därtill en komplicerad situation hur dessa operatörer i sin tur ska få kompensation från andra operatörer som hyr utrymme i ledningarna.

IT-Företagen har vidare anfört att mängden trafik, och därmed kostnaderna, grovt underskattats och att de kostnadsskattningar som redovisas saknar all trovärdighet. IT-företagen har påpekat att en stor mängd renodlat utländsk trafik passerar Sverige, vilket betyder att trafiken är ofantligt mycket större än vad som anges i promemorian och kommer att öka ytterligare. Det innebär att investeringarna i utrustning och sökprogram måste bli betydligt större än vad som anges för att spaningen ska kunna bli effektiv och proportionerlig. I den mån inte samma reglering införs i andra länder, så innebär förslaget en konkurrensnackdel för de operatörer vars trafik – inhemsk såväl som utländsk – passerar rikets gränser. Om trafiken avlyssnas kan dessa operatörer inte garantera sitt kanske viktigaste åtagande inför sina abonnenter, nämligen telehemligheten.

E.ON har anfört det inte kan uteslutas att avnämare av kommunikationstjänster kan komma att välja operatör utifrån kriteriet huruvida operatörens tekniska lösning innebär att även inhemsk kommunikation förs utomlands för bearbetning, vilket skulle kunna ha en hämmande inverkan på den tekniska utvecklingen och tillskapandet av effektiv konkurrens på kommunikationsområdet. Denna problematik förstärks ytterligare om

operatörerna åläggs att bekosta investeringar etc. i enlighet med förslaget, då mindre operatörer har sämre förutsättningar att bära sådana kostnader.

Telia Sonera AB har anfört att det är fel att vältra över kostnader som är direkt hänförliga till ett klart och uttalat samhälleligt behov, i detta fall behov av underlag för underrättelseverksamhet, på marknadens aktörer, framförallt när utgifterna inte ger de drabbade aktörerna någon direkt nytta. Den principiella utgångspunkten måste vara att kostnader för samhälleliga behov skall synliggöras. Sådana kostnader bör därför täckas genom anslag i statsbudgeten. Kostnader och nytta kan då vägas mot varandra, mot andra åtgärder för att främja säkerhet samt mot andra mål, såsom dem för elektroniska kommunikationer. Telia Sonera AB har vidare påtalat att förslaget föranleder en rad åtgärder och kostnader för operatörerna som inte synes beaktade, bl.a. att en snabb implementering fordrar större inslag av manuell omkoppling. Bolaget har också påtalat att det kan bli tvunget att hålla sig i närheten av samverkanspunkterna i all ny och tilläggsetablering samt att detta medför verksamhetspåverkan, inflexibilitet och kostnadsökningar.

Svenska stadsnätsföreningen har anfört att eftersom försvarsunderrättelseverksamheten är en fråga om nationens säkerhet måste eventuella kostnader för nätägarna också bekostas av samhället. Föreningen har påtalat att situationen är mycket olika mellan nätägarna där vissa t.ex. redan är etablerade i ”samverkanspunkter” medan andra endast har trunktrafik genom sina nät. Föreningen har vidare påpekat vissa tekniska förhållanden som bör föranleda ytterligare överväganden.

Vetenskapsrådet (huvudman för SUNET) har framhållit att det är svårt att på grundval av det underlag som presenteras bedöma om kostnadsberäkningarna är realistiska och anfört att kostnaderna kan ha underskattats, inte minst när det gäller operatörernas anpassningsskyldighet. I det sammanhanget har rådet bl.a. påpekat att underlaget är knapphändigt beträffande tekniken och att det t.ex. är oklart vad som menas med att operatörerna måste lämna ifrån sig signaler som FRA "lätt" kan hantera.

Skälen för regeringens förslag och bedömning: För operatörerna kommer inhämtning av signaler i tråd enligt detta förslag att innebära en kostnad för teknisk anpassning samt vissa löpande kostnader. Dessa kostnader kommer framförallt att beröra de trådägande operatörerna. Kostnaderna kommer efter ett antal år att plana ut och därefter i princip endast omfatta vissa löpande kostnader. I avsnitt 7 beskrivs operatörernas skyldigheter.

Att göra en exakt uppskattning av de trådägande operatörernas kostnader för att göra den trafik som passerar rikets gräns tillgänglig för Försvarets radioanstalt är som flera *remissinstanser* påpekat svårt i och med att telekommunikationsindustrin är en mycket dynamiskt verksamhet som är stadd i konstant förändring. Det viktiga är dock att beräkningen görs utifrån så goda utgångspunkter som möjligt. I utarbetandet av de kostnadsberäkningar som här föreligger har därför Post- och telestyrelsen, Försvarets radioanstalt samt operatörer och andra aktörer bidragit med information om såväl egna som mer allmänna förhållanden. Regeringen menar därför till skillnad från några av *remissinstanserna* att de beräkningar som presenteras i promemorian kan läggas till grund för bedömningarna av förslagens ekonomiska konsekvenser.

När det gäller fördelningen av kostnaderna för anpassningen finns flera tänkbara alternativ. Kostnaden kan bäras av signalspaningsmyndigheten eller av operatörerna eller fördelas mellan dem. En annan möjlighet är att kostnaden bärs av det allmänna utan att direkt belasta signalspaningsmyndighetens anslag.

En allmän utgångspunkt när det gäller kostnader för försvarsunderrättelseverksamheten är att de myndigheter som bedriver verksamheten skall svara för dessa. Detta argument har också framförts av de remissinstanser som är kritiska mot promemorians förslag. Signalspaningsverksamheten är enligt dessa remissinstanser en statlig angelägenhet som bör bekostas av staten och inte av de enskilda operatörerna.

Som regeringen framhållit i andra sammanhang (prop. 1995/96:180 s. 32 f.) finns det emellertid flera verksamhetsområden där samhället som förutsättning för att enskilda skall få bedriva viss verksamhet kräver att vissa allmännyttiga intressen beaktas. Ett exempel är arbetsgivares skyldighet att uppbära, redovisa och inbetala preliminär skatt för anställda. Ett annat exempel är de krav som ställs på företag som bedriver miljöfarlig verksamhet. Ytterligare ett exempel, som ligger nära den nu aktuella verksamheten, är operatörers skyldighet att anpassa sina system så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas. Enligt regeringens mening finns det ingen principiell skillnad mellan dessa förpliktelser och en förpliktelse att bekosta anpassning av systemen för att möjliggöra signalspaning. Regeringen delar följaktligen inte den principiella inställning som *Svenska IT-företagens organisation, Telia Sonera AB, E.ON* och *Svenska stadsnätsföreningen* har anfört.

En betydelsefull omständighet att beakta vid valet av vem som skall stå för kostnaden för att styra ut trafiken är också vad som blir den samhällsekonomiskt mest effektiva lösningen. Den som drabbas av kostnaderna har naturligtvis ett starkt incitament att söka hålla kostnaderna nere. Detta innebär att det är samhällsekonomiskt effektivare att låta de trådägande operatörerna stå för kostnaderna vad avser utstyrning och leverans av signalerna till samverkanspunkterna.

De trådägande operatörerna kan som huvudsakliga inköpare av de hård- och mjukvaror som krävs påverka priset på ett annat sätt än vad en statlig myndighet kan. De har en förhandlingsposition som bör kunna leda till att största kostnadseffektivitet uppnås i detta hänseende. Teknik som möjliggör en utstyrning av information från de trådägande operatörernas system kommer nämligen att omfattas av förhandlingar om nya system och om ny teknik i befintliga system som en mycket liten del i ett större paket. Ifrågavarande kostnader kan hållas nere om den aktuella funktionaliteten beaktas på ett så tidigt stadium som möjligt. Slutsatsen är att om det finns ett eget ekonomiskt incitament för de trådägande operatörerna att förhandla fram ett så fördelaktigt pris som möjligt kommer detta att bli den samhällsekonomiskt mest lämpliga lösningen.

Ett liknande resonemang kan föras vad avser kommunikationskostnaden, d.v.s. kostnaden för att föra trafiken från operatörernas system till samverkanspunkterna. I och med att de trådägande operatörerna har ett incitament att överföra trafiken till så låg kostnad som möjligt kommer de att överföra trafiken till samverkanspunkterna på det mest kostnadseffektiva sättet.

Svenska IT-företagens organisation har anfört att om operatörerna skall bära kostnaden kan detta leda till ett överutnyttjande samt att en ur samhällsekonomisk synvinkel lämplig prioritering av resurser försvåras genom att den som beslutar kring prioriteringarna inte själv står för kostnaden. Regeringen anser inte att detta resonemang är tillämpligt i fråga om signalspaning. Det handlar i dessa sammanhang om att styra ut all trafik som passerar Sveriges gräns för att signalspaningsmyndigheten därefter skall kunna inhämta relevanta signaler. Den skyldighet som åvilar operatörerna påverkas följaktligen inte av i vilken utsträckning signalspaningsmyndigheten därefter inhämtar och bearbetar de utstyrda signalerna. Regeringens uppfattning är därför att någon risk för överutnyttjande inte föreligger; de kostnader som är relaterade till omfattningen av signalspaningsmyndighetens verksamhet bärs i sin helhet av denna.

Regeringen delar inte den uppfattning som framförts av *Telia Sonera AB* att ett skäl för att staten skall bära kostnadsansvaret är att utgifterna inte ger de drabbade aktörerna någon direkt nytta. Regeringen menar tvärtom att operatörerna i hög grad har nytta av den försvarsunderrättelseverksamhet som syftar till att skydda Sverige mot IT-relaterade hot, se avsnitt 7.1.1.

Sammanfattningsvis anser regeringen att övervägande skäl talar för att de trådägande operatörerna skall bära kostnaden för den tekniska anpassning som krävs för att inhämtning av signaler i elektronisk form i tråd skall kunna genomföras. Det ankommer därefter på de trådägande operatörerna att med beaktande av förutsättningarna på marknaden bedöma hur kostnaden vidare skall fördelas.

Regeringen finner dock rimligt mot bakgrund av vad remissinstanserna anfört angående kostnader att en utvärdering sker avseende vilken påverkan förslaget kan komma att ha på marknaden och dess aktörer. Vidare bör införandet av skyldigheterna för operatörerna senareläggas. Genom att föreskriva att bestämmelserna om dessa skall tillämpas från och med den 1 juli 2008 ges operatörerna möjlighet att i större utsträckning utnyttja de fördelar i form av att vara huvudsaklig inköpare och ha en stark förhandlingsposition som angetts ovan

Uppskattning av kostnader för operatörerna

Ett resonemang kring kostnader för operatörer måste utgå från vissa grundläggande principiella resonemang och ett antagande avseende tid för implementering. I nedanstående resonemang utgår beräkningen från en implementeringstid på fem år från den dag lagen träder i kraft.

Vad som först kan konstateras är att omsättningstakten för aktuella typer av kommunikationsutrustning är hög och att huvuddelen av utrustningen inom en femårsperiod kan förvänts vara utbytt eller kraftigt uppgraderad.

En annan central aspekt att beakta är att de tekniska investeringskostnaderna för de trådägande operatörerna efterhand kommer att minska kraftigt. Huvudorsaken till detta är att eftersom det legala kravet på dessa operatörer (d.v.s. att styra ut all trafik som förs över Sveriges gräns till samverkanspunkterna) finns kommer all beställning av ny utrustning av de trådägande operatörerna att innehålla krav på denna typ av funktionalitet. Denna extra funktionalitet kommer då att vara en mindre del av de

krav som ställs på ny utrustning och eftersom den byggs in från början kommer kostnaden att vara begränsad (jmf. resonemanget i föregående avsnitt).

Generellt består kostnaderna för de trådägande operatörerna av följande delar: Investeringar i ny utrustning, drift- och underhållskostnader, kompetensuppbyggnad (om operatören måste investera i ny typ av utrustning), sambandkostnader (för att transportera trafik från access- till samverkanspunkt) och informationsplikt (att förse Försvarets radioanstalt med nödvändig information om främst förändringar i nätstruktur och trafikinnehåll). Som flera *remissinstanser* påpekat är det mot bakgrund av den snabba utvecklingen på området svårt att uppskatta hur den löpande anpassningskostnaden kommer att utvecklas i förhållande till de initiala investeringarna. Regeringen delar dock promemorians bedömning att tyngdpunkten när det gäller kostnadsansvaret kommer att ligga i samband med de inledande investeringarna.

Utöver de ovan angivna kostnaderna tillkommer vissa mindre kostnader för att lämna information som kan göra det enklare att ta hand om signalerna, vilket omfattar såväl trådägare som andra operatörer som utan att äga tråden för signaler i tråd över Sveriges gräns. Dessa kostnader är ringa eftersom det rör sig om att överföra sådan kringinformation som operatörerna redan har i sina system. Det finns heller inget krav på att denna information skall anpassas. Vilka åtgärder hos operatörerna som är nödvändiga för att göra det enklare att ta hand om signalerna behandlas i avsnitt 7.3.7.

Det torde också vara ömsesidigt fördelaktigt om Försvarets radioanstalts behov, när så är möjligt, kopplas till av operatören planerade uppgraderingar och förändringar – kostnaden för operatören kan därmed reduceras samtidigt som Försvarets radioanstalt kan få mer trafik tillgänglig i samverkanspunkterna.

Utifrån hypotesen att all trafik som förs över Sveriges gräns i tråd ska vara tillgänglig för Försvarets radioanstalt inom fem år efter lagens ikraftträdande kan följande beräkning göras.

Det finns ca 10 trådägande operatörer som för trafik över rikets gräns. Utifrån detta kan en teoretisk modell för kostnaderna byggas enligt följande. I ett tänkt fall med en trådägande operatör som har 20 procent av trafiken vilken passerar rikets gräns skulle den tekniska anskaffningskostnaden om man räknar högt bli ca 15 miljoner kronor för att göra all trafik från dessa trådar tillgänglig för Försvarets radioanstalt. Utöver detta tillkommer drift och underhållskostnader samt kostnader för förbindelse mellan operatörens system och samverkanspunkten. Kostnaden för samband är dock generellt ringa i och med att samverkanspunkten troligtvis kommer att ligga i ett utrymme mycket nära de trådägande operatörerna.

Omräknat för alla 10 trådägare innebära detta en totalkostnad på högst 75 miljoner kronor för att göra all trafik vilken passerar rikets gräns tillgänglig. Den genomsnittliga kostnaden per år, är då 15 miljoner kronor (utslaget på alla trådägande operatörer). Den tillkommande kostnaden för att lämna information som kan göra det enklare att ta hand om signalerna, en skyldighet som också omfattar de operatörer som inte äger tråd men för signaler i tråd över Sveriges gräns, är som angetts ovan obetydlig i sammanhanget.

Konkurrensfrågor

E.ON och *Svenska IT-Företagens organisation* har uttalat farhågor för att förslaget kan leda till en snedvridning av konkurrensen i den mån inte samma reglering införs i andra länder. Som framgår av redogörelsen i avsnitt 7.1.2 är signalspaning avseende signaler i tråd långtifrån någon unik svensk företeelse; tvärtom har många länder redan denna möjlighet sedan tidigare. Även om förutsättningarna för verksamheten varierar mellan olika länder kan förslaget därför enligt regeringens mening inte anses innebära några beaktansvärda konkurrensnackdelar för svenska operatörer. I sammanhanget förtjänar att framhållas att *Konkurrensverket* inte haft några invändningar mot förslaget.

11.3 Övriga konsekvenser

Förslaget bedöms inte ha några konsekvenser när det gäller kostnader eller intäkter för kommuner och landsting. Inte heller bedöms förslaget ha några konsekvenser för den kommunala självstyrelsen, sysselsättningen, den offentliga servicen i olika delar av landet, jämställdheten mellan män och kvinnor och möjligheterna att nå de integrationspolitiska målen.

12 Författningskommentarer

12.1 Förslag till lag om ändring i lagen (2000:130) om försvarsunderrättelseverksamhet

1 §

Lagens *första paragraf* har ändrats på flera sätt. I den *första meningen* markeras att försvarsunderrättelseverksamheten främst skall ge stöd till svensk utrikes-, säkerhets- och försvarspolitik. I förhållande till paragrafens nuvarande lydelse har ordningsföljden på de politikområden som försvarsunderrättelseverksamheten skall stödja ändrats. Ändringen har gjorts för att åstadkomma en överensstämmelse med den begreppsbildning som används för att bl.a. inom budgetpolitiken ange politikområden och knyter an till gängse språkbruk. Vidare innebär ändringarna att verksamheten breddas från att omfatta yttre militära hot mot landet till att omfatta även andra yttre hot mot landet än rent militära. I lagtexten slås därför fast att försvarsunderrättelseverksamheten skall avse yttre hot mot landet. Detta innebär att bl.a. internationell terrorism och annan kvalificerad gränsöverskridande brottslighet med säkerhetspolitiska konsekvenser omfattas av underrättelseverksamheten. Det utvidgade mandatet behandlas utförligt i avsnitt 6.3.1.

Av *andra meningens* sista led framgår idag att det i verksamheten ingår att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred. Eftersom det ifrågavarande området i huvudsak täcks av uttrycket ”yttre hot mot landet” är uppgiften inte nödvändig och finns därför inte med i förslaget till ändrad paragraf.

I *tredje meningen* anges att försvarsunderrättelseverksamheten endast får avse utländska förhållanden. Genom användningen av uttrycket utländska förhållanden ges försvarsunderrättelseverksamheten sin inriktning i sak och avgränsas mot inhemska förhållanden. Med uttrycket utländska förhållanden betonas även den grundläggande roll som försvarsunderrättelseverksamheten är avsedd att ha för landets samlade säkerhetspolitik och till stöd för statsledningen. Ändringen motiveras närmare i avsnitt 6.3.1.

Andra stycket första meningen har inte ändrats. *Andra meningen* är ny. Där regleras de uppdragsgivande myndigheternas möjlighet att närmare inrikta försvarsunderrättelseverksamheten inom den ram som regeringen fastställt. Frågan behandlas i avsnitt 6.4.

Ändringen i *tredje stycket* innebär att ingen av de myndigheter som skall bedriva försvarsunderrättelseverksamhet anges i lag. Myndigheterna anges i stället i förordning.

2 §

Första stycket har ändrats i flera avseenden. I *första meningen* görs en språklig anpassning till den föreslagna ändringen av 1 § första stycket.

Därefter görs en ändring i *andra meningen* för att betona att försvarsunderrättelseverksamheten i första hand skall vara inriktad på att inhämta, bearbeta och genomföra grundanalys av information. Resultatet av denna process är de underrättelser som skall rapporteras. För att tydliggöra att graden av analys måste varieras med hänsyn bl.a. till mottagarens behov och egen analyskapacitet och att det inte i första hand är en färdiganalyserad bedömning som skall rapporteras, har formuleringen om att analyser av hotbilder och bedömningar i underrättelsefrågor skall rapporteras utgått. Eftersom Regeringskansliet är en myndighet behöver den inte anges särskilt i författningstexten. Att ordet ”Regeringskansliet” utgår innebär således inte att kretsen av mottagare av underrättelser förändras. Regeringskansliet skall även fortsättningsvis vara mottagare av underrättelser avsedda för regeringens underrättelsebehov.

I *andra stycket,* som är nytt, anges att i försvarsunderrättelseverksamheten får användas teknisk och personbaserad inhämtning med särskilda metoder, se vidare avsnitt 6.4. Bestämmelsen är av informationskaraktär och ger inte några tvångsmedelsliknande befogenheter i förhållande till enskilda. Begreppet särskilda metoder återfinns också i 2 § tredje punkten lagen (2006:939) om kvalificerade skyddsidentiteter och behandlas i prop. 2005/06:149 s. 28.

I stycket finns en hänvisning till lagen om signalspaning i försvarsunderrättelseverksamhet, i vilken lagstödet för signalspaningsverksamheten återfinns. Signalspaning utgör teknisk inhämtning.

3 §

Paragrafen har ändrats. Ändringen är av redaktionell karaktär, och innebär att bestämmelsen anpassas till den ändrade lydelsen av 1 § tredje stycket.

4 §

I paragrafen regleras avgränsningen mellan försvarsunderrättelseverksamhet och polisiär verksamhet. Bestämmelsen har fått en annan lydelse för att förtydliga att begränsningen syftar på sådana åtgärder som vidtas i syfte att lösa en i lag eller annan föreskrift föreskriven uppgift i polisens och andra myndigheters brottsförebyggande och brottsbekämpande arbete. Den grundläggande principen att försvarsunderrättelseverksamheten inte får innefatta förfarande i samband med förundersökning, vissa arbetsmetoder som är förbehållna polisman och användning av straffprocessuella tvångsmedel kvarstår och behöver inte uttryckligen anges, eftersom detta följer av andra bestämmelser.

Bestämmelsens nya lydelse omfattar andra konkreta åtgärder som vidtas i den brottsförebyggande och brottsbekämpande verksamheten med det direkta syftet att lösa uppgifter som föreskrivs för denna verksamhet. Som närmare redovisas i avsnitt 6.2 handlar det om sådana åtgärder som, om de vidtogs av andra myndigheter, skulle kunna störa utövandet av den brottsbekämpande eller brottsförebyggande verksamheten. Begränsningen träffar endast sådana åtgärder för inhämtning av information som tar sig mer konkreta uttryck än t.ex. inhämtning av signaler i elektronisk form vid signalspaning. Gränsdragningsfrågor i övrigt får behandlas inom ramen för regeringens inriktning av försvarsunderrättelseverksam-

heten. Utanför det område som omfattas av bestämmelsen ligger det följaktligen i regeringens hand att genom sin inriktning överväga gränsdragningen mellan myndigheternas ansvarsområden, på motsvarande sätt som regeringen i andra sammanhang reglerar frågor om relationen mellan olika myndigheter i t.ex. instruktioner och delegeringsföreskrifter.

Genom bestämmelsen kompletteras 1 §, i vilken försvarsunderrättelseverksamhetens mandat anges och begränsningen till utländska förhållanden regleras. Bestämmelsen snävar således ytterligare in verksamheten i förhållande till lagen i övrigt.

Paragrafens *andra stycke* syftar till att klargöra att gränsdragningen i det första stycket inte innebär någon begränsning av möjligheten för de myndigheter som bedriver försvarsunderrättelseverksamhet att till de brottsbekämpande och brottsförebyggande myndigheterna lämna stöd utanför försvarsunderrättelseverksamheten. Förutsättningarna för stöd till annan myndighet avgörs av vad som gäller för verksamheten hos den myndighet som begär och mottar stödet. Det handlar följaktligen om att inom ramen för en sådan myndighets verksamhet biträda med åtgärder som den mottagande myndigheten i och för sig haft rätt att vidta på egen hand, men har otillräckliga resurser för. I syfte att klarlägga detta anges att en förutsättning för stöd är att det inte finns hinder enligt andra bestämmelser.

Exempel på sådan verksamhet som kan komma i fråga är biträde med kryptoforcering, tekniskt stöd på informationssäkerhetsområdet och stöd i andra situationer då det är särskilt angeläget att resurserna hos de myndigheter som bedriver försvarsunderrättelseverksamhet kan användas för samhällsviktiga ändamål.

Paragrafen har behandlats närmare i avsnitt 6.3.2.

5 §

Paragrafen har ändrats. Hänvisningen till ”En särskild nämnd under regeringen” har bytts ut mot ”Den myndighet som regeringen bestämmer” för att anpassa lagen till de förslag som lämnats i betänkandet SOU 2004:23 Från verksförordning till myndighetsförordning. För att understryka att den aktuella myndighetens roll skall stärkas har uttrycket ”ha insyn i” ersatts av ”kontrollera”. Se vidare avsnitt 8.

12.2 Förslag till lag om signalspaning i försvarsunderrättelseverksamhet

1 §

Inhämtning av signaler i elektronisk form vid signalspaning är en sådan särskild metod för teknisk inhämtning som nämns i lagen (2000:130) om försvarsunderrättelseverksamhet. I paragrafen anges att sådan inhämtning får bedrivas i försvarsunderrättelseverksamheten. Möjligheten att inhämta signaler i elektronisk form är inte knuten till var signalerna befinner sig, utan är teknikneutral. Därmed kan inhämtning ske oavsett om signalerna befinner sig i etern eller i kabel (d.v.s. är trådbunden) eller någon

annan stans. Beträffande uttrycket ”signaler i elektronisk form”, se vidare avsnitt 7.3.2.

I paragrafens *första stycke* slås fast att signaler i elektronisk form får inhämtas i försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet. Det innebär att inhämtning får ske i försvarsunderrättelseverksamhet som bedrivs till stöd för svensk utrikes-säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. I verksamheten ingår också att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Verksamheten får endast avse utländska förhållanden. Beträffande försvarsunderrättelseverksamhet, se vidare avsnitt 7.3.2 och kommentaren till de förslagna ändringarna i lagen (2000:130) om försvarsunderrättelseverksamhet, avsnitt 11.1.

Att den verksamhet som regleras i lagen får bedrivas för försvarsunderrättelseändamål innebär att inhämtning t.ex. får ske av uppgifter av relevans för att kartlägga militära hot mot landet och förhållanden som är relevanta för svenskt deltagande i fredsfrämjande och humanitära internationella insatser samt kartläggning under pågående insatser av hot mot svensk personal eller svenska intressen i övrigt. Vidare får inhämtningen avse strategisk kartläggning av internationell terrorism eller annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen. Det är dock inte försvarsunderrättelseverksamhetens uppgift att kartlägga verksamheten i operativt brottsbekämpande syfte.

Andra exempel på ändamål för vilka signalspaning får bedrivas är kartläggning av utveckling och spridning av massförstörelsevapen och krigsmateriel, yttre hot mot samhällets tekniska infrastrukturer i form av t.ex. kvalificerade IT-relaterade hot, konflikter utomlands med konsekvenser för internationell säkerhet och internationella företeelser i övrigt av betydelse för svensk utrikes-, säkerhets- och försvarspolitik.

Inhämtningen enligt denna lag skall emellertid även få bedrivas för vissa andra särskilda syften som inte omfattas av försvarsunderrättelseverksamheten men som utgör en förutsättning för att denna skall kunna bedrivas, se avsnitt 7.3.2. I paragrafens *andra stycke* beskrivs dessa syften i två punkter.

I *första punkten* anges att inhämtning får ske för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet. I *andra punkten* anges att inhämtning genom signalspaning får ske för att fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt lagen. Vad som regleras i detta stycke återfinns idag i förordningen med instruktion för Försvarets radioanstalt, och överförs nu till lagen.

Eftersom inhämtning som sker med stöd av andra stycket inte utgör underrättelseverksamhet – verksamheten bedrivs för signalspaningsmyndighetens egna behov av teknik- och kompetensutveckling och genererar inte underrättelser – omfattas den inte av lagen (2000:130) om försvarsunderrättelseverksamhet. De begränsningar som uppställs i lagen om signalspaning i försvarsunderrättelseverksamhet gäller dock även för denna inhämtning, se avsnitt 7.3.2.

2 §

Av paragrafen framgår att inhämtning som sker i tråd endast får avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör. Med operatör avses detsamma som enligt 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation, d.v.s. den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation. Paragrafen behandlas i avsnitt 7.3.3 och i avsnitt 7.3.7.

3 §

I paragrafen *första mening* slås fast att ett villkor för att få bedriva inhämtning av signaler i tråd är att inhämtningen sker automatiserat. Vid sådan inhämtning skall signalerna ha identifierats genom sökbegrepp. Med sökbegrepp avses här att man genom att ange ett eller flera begrepp kan söka igenom en informationsmängd och hitta de poster eller uppgiftskonstellationer där begreppet förekommer. Sökbegrepp kan också innefatta parametrar som utesluter större informationsmängder. Krav på att använda sökbegrepp uppställs också för sådan automatiserad inhämtning som sker i etern. Detta framgår av *andra meningen*. Bestämmelsen tar enbart sikte på sådan inhämtning som sker automatiserat, vilket innebär att inhämtning i etern som bedrivs med manuella metoder inte omfattas av begränsningen (se vidare avsnitt 7.3.4).

I *andra stycket* slås fast att sökbegreppen skall utformas och användas så att de medför ett så begränsat intrång som möjligt i den personliga integriteten samt att sökbegreppen inte får vara direkt hänförliga till en viss fysisk person om det inte är av synnerlig vikt för verksamheten (se vidare avsnitt 7.4.2).

Att sökbegreppen skall granskas i särskild ordning framgår av 10 §.

4 §

I paragrafens *första stycke* erinras om att regeringens och myndigheters inriktning av sådan signalspaning som är försvarsunderrättelseverksamhet regleras i lagen (2000:130) om försvarsunderrättelseverksamhet. När det gäller inriktning av verksamhet som gäller signalspaning anges att en sådan inriktning inte får avse endast en viss fysisk person. Signalspaningsverksamheten måste visserligen i vissa fall beröra enskildas kommunikationer för att det skall vara möjligt att följa en viss företeelse av relevans för verksamheten. Den skall dock inte inriktas endast mot en enskild utpekad individ.

I *andra stycket* finns bestämmelser om att även sådan signalspaningsverksamhet enligt 1 § andra stycket som inte är försvarsunderrättelseverksamhet men utgör en nödvändig förutsättning för denna skall inriktas av regeringen.

Bestämmelsen behandlas vidare i avsnitt 7.3.5.

5 §

I paragrafens *första stycke* slås fast att det krävs tillstånd för att de myndigheter som regeringen bestämmer skall kunna ge närmare inriktning av signalspaningsverksamheten. Kravet på tillstånd gäller inte för inriktning som avser regeringens eget underrättelsebehov, d.v.s. sådan inriktning

som avser beslutsunderlag för regeringens ställningstaganden i utrikes-, säkerhets- och försvarspolitiska frågor. Tillståndet lämnas av den myndighet som regeringen bestämmer (Försvarets underrättelsenämnd). Ett tillstånd gäller för högst sex månader och kan efter förnyad prövning förlängas med högst sex månader i taget. Omfattningen av en sådan förnyad prövning får anpassas till vad tillståndet avser, inhämtningens dittillsvarande resultat och eventuella nytillkomna omständigheter av betydelse för prövningen.

Av *andra stycket* framgår att en inriktning skall avse en företeelse eller ett förhållande som är relevant med avseende på de ändamål för vilka signalspaningen får bedrivas. Inriktningen skall också i övrigt vara förenlig med lagen (2000:130) om försvarsunderrättelseverksamhet. Tillstånd får endast lämnas om syftet med inriktningen väger klart tyngre än det integritetsintrång som inhämtning i enlighet med inriktningen kan innebära och detta syfte inte kan tillgodoses på ett mindre ingripande sätt. Tillståndsmyndigheten skall följaktligen göra en proportionalitetsbedömning på grundval av de uppgifter som den ansökande myndigheten lämnar.

Tillstånd får inte ges för inriktning som endast avser en fysisk person. Detta följer redan av 4 §, i vilken anges att en närmare inriktning inte får avse endast en viss fysisk person. Här understryks ytterligare att detta skall prövas i samband med tillståndsgivningen. Signalspaningsverksamheten måste dock i vissa fall beröra enskildas kommunikationer för att det skall vara möjligt att följa en viss företeelse av relevans för verksamheten, vilket skall vara möjligt så länge inte det enda syftet med en inriktning är att kartlägga en viss fysisk person

I *tredje stycket* begränsas skyldigheten att inhämta tillstånd. Tillstånd krävs inte i brådskande fall. Med detta avses situationer då det skulle medföra allvarliga konsekvenser för väsentliga nationella intressen att avvakta tillståndet. Om en närmare inriktning givits utan tillstånd skall den omedelbart anmälas till den myndighet som skall lämna tillstånd (Försvarets underrättelsenämnd). Om tillståndsmyndigheten finner att tillstånd till inriktning inte borde ha getts skall Försvarets radioanstalt underrättas och inhämtningen omedelbart avbrytas.

Bestämmelsen behandlas i avsnitt 7.4.3.

6 §

Enligt paragrafens *första punkt* skall upptagning eller uppteckning av uppgifter som inhämtats enligt lagen omgående förstöras om innehållet i upptagningen eller uppteckningen berör en viss fysisk person och har bedömts sakna betydelse för den verksamhet som avses i 1 §, dvs. för försvarsunderrättelseverksamheten eller för den verksamhet som beskrivs i 1 § andra stycket. Detta gäller givetvis oavsett om inhämtningen skett med hjälp av automatiserad behandling eller med manuella metoder. En situation då det finns anledning att förstöra upptagningar eller uppteckningar är om en inhämtning avbrutits enligt 5 § tredje stycket på grund av att den avser en företeelse som saknar betydelse för försvarsunderrättelseverksamheten.

Krav på förstöring gäller också om upptagningen eller uppteckningen omfattar uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfri-

hetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 4 § tryckfrihetsförordningen eller 2 kap. 4 § yttrandefrihetsgrundlagen. Även upptagning eller uppteckning av uppgifter i sådana meddelanden som avses i 27 kap. 22 § rättegångsbalken, dvs. mellan en misstänkt och dennes försvarare, skall förstöras. I de senare fallen skall överhuvudtaget ingen annan bedömning göras av innehållet i upptagningen eller uppteckningen än vad som är nödvändigt för att konstatera om ett sådant förhållande som anges i den andra eller tredje punkten föreligger. Bestämmelsen behandlas i avsnitt 7.4.4.

7 §

I paragrafens *första mening* erinras om att underrättelser med uppgifter som inhämtats genom signalspaning i försvarsunderrättelseverksamheten skall rapporteras till berörda myndigheter i enlighet med vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet. Den verksamhet som sker med stöd av 1 § andra stycket syftar till att möjliggöra signalspaning i försvarsunderrättelseverksamheten genom att tillgodose myndighetens egna behov av teknik- och kompetensutveckling och resulterar inte i några underrättelser. Den omfattas därför inte av denna bestämmelse. Första meningen behandlas i avsnitt 7.3.5.

I *andra meningen* görs en begränsning av vad som får rapporteras från signalspaning i försvarsunderrättelseverksamheten. Där anges att om uppgifterna berör en viss fysisk person får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § lagen om försvarsunderrättelseverksamhet. Bestämmelsen innebär ett förbud mot rapportering av sådan överskottsinformation rörande enskilda som saknar relevans ur försvarsunderrättelsesynpunkt. Begränsningen behandlas i avsnitt 7.4.4.

8 §

Paragrafen medger att den myndighet som regeringen bestämmer (Försvarets radioanstalt) får bedriva internationellt signalspaningssamarbete för sådan verksamhet som regleras i 1 § andra stycket, dvs. för sådan inhämtning som inte är försvarsunderrättelseverksamhet. När det gäller försvarsunderrättelseverksamhet finns bestämmelser om internationellt samarbete i 3 § lagen (2000:130) om förvarsunderrättelseverksamhet. Bestämmelsen behandlas i avsnitt 7.3.5.

9 §

Enligt paragrafen skall den myndighet som regeringen bestämmer (Försvarets underrättelsenämnd) kontrollera att lagen följs, på motsvarande sätt som myndigheten gör i fråga om försvarsunderrättelseverksamheten i stort, se avsnitt 8. De sökbegrepp som avses i 3 §, förstöring enligt 6 § och den rapportering som avses i 7 § skall granskas särskilt.

I andra stycket ges myndigheten möjlighet att med anledning av sina iakttagelser i samband med kontrollen vidta åtgärder riktade mot Försvarets radioanstalt. Åtgärderna består i att myndigheten kan fatta beslut om att viss inhämtning skall upphöra eller att upptagning eller uppteckning

av inhämtade uppgifter skall förstöras. Nämnden får i varje enskilt fall avgöra omfattningen av åtgärden. Ett beslut om avbrytande av en inhämtning kan t.ex. avse att vissa sökbegrepp inte längre skall få användas.

Bestämmelsen behandlas i avsnitt 7.3.5 och 8.

10 §

Paragrafen innehåller en hänvisning till de bestämmelser i lagen (2003:389) om elektronisk kommunikation som reglerar operatörernas skyldighet att överföra signaler för att möjliggöra inhämtning enligt lagen om signalspaning i försvarsunderrättelseverksamhet. Se avsnitt 7.3.7 och kommentaren till de föreslagna ändringarna i lagen om elektronisk kommunikation, avsnitt 12.3.

11 §

I paragrafen slås fast att beslut som fattas enligt lagen om signalspaning i försvarsunderrättelseverksamhet inte får överklagas.

12.3 Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation

6 kap. 19 a §

Paragrafen är ny. För att möjliggöra en ändamålsenlig inhämtning av signaler i elektronisk form enligt lagen (2007:000) om signalspaning i försvarsunderrättelseverksamhet föreskriver den vissa skyldigheter för operatörerna. Skyldigheterna avseende överföring m.m. gäller endast sådana signaler som förs över Sveriges gräns. Beträffande övervägandena i denna del, se avsnitt 7.3. Begreppet operatör definieras i 1 kap. 7 §.

I *första stycket* åläggs de operatörer som äger tråd i vilka signaler förs över Sveriges gräns en skyldighet att överföra dessa till samverkanspunkter. De överförda signalerna kan bestå av såväl egen som andra operatörers trafik. De samverkanspunkter som de trådägande operatörerna valt skall anmälas till den myndighet som regeringen bestämmer (Försvarets radioanstalt). En samverkanspunkt är en plats där trafiken överlämnas från den trådägande operatören till myndigheten, se avsnitt 7.3.7. Om det motiveras av ett reellt behov hos operatören, kan denne anmäla en ny plats för samverkanspunkten. I stycket finns slutligen ett bemyndigande för regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten att meddela föreskrifter om samverkanspunkter. Enligt 2 § förordningen (2003:396) om elektronisk kommunikation är Post- och telestyrelsen tillsynsmyndighet enligt lagen om elektronisk kommunikation.

Andra och tredje stycket gäller både sådana operatörer som är trådägare och sådana som inte är det. Det *andra stycket* innehåller en skyldighet för alla operatörer som för signaler i tråd över Sveriges gräns att lämna sådan information de har som kan göra det enklare att ta hand om signalerna. Det innebär bl.a. att en operatör skall informera den myndighet som skall ta emot anmälningarna om samverkanspunkterna (Försvarets radioanstalt) om förändringar i sina system för att myndigheten i god tid

skall kunna förbereda sig. Skyldigheten omfattar endast sådan information som operatören innehar och innebär inte något krav på anpassning av informationen.

Av *tredje stycket* framgår att samtliga operatörer skall utföra uppgiften enligt den föreslagna bestämmelsen så att verksamheten inte röjs.

6 kap. 21 §

Paragrafen, som reglerar tystnadsplikt beträffande vissa uppgifter för den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst fått del av eller tillgång till dessa, har ändrats på så sätt att en ny *tredje punkt* har införts. Enligt denna skall tystnadsplikt även gälla för uppgift som hänför sig till angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2007:000) om signalspaning i försvarsunderrättelseverksamhet. Ändringen innebär att motsvarande regler som gäller för hemlig teleavlyssning och hemlig teleövervakning enligt 6 kap. 21 § 2 även kommer att gälla för angelägenhet som avser inhämtning av signaler i elektronisk form, signalspaning, i försvarsunderrättelseverksamhet.

Ikraftträdande

Lagändringen träder ikraft den 1 juli 2007. För de operatörer som äger tråd föreskrivs en skyldighet att föra signalerna till samverkanspunkter. Denna skyldighet träder ikraft den 1 juli 2008, vilket innebär att dessa operatörer har tolv månader på sig att efter lagens ikraftträdande förbereda sina system för detta. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten enligt lagen (2003:389) om elektronisk kommunikation (Post- och telestyrelsen) får meddela föreskrifter om att bestämmelserna om skyldigheten skall börja tillämpas senare. Bestämmelsen behandlas i avsnitt 11.

12.4 Förslag till lag om ändring i sekretesslagen (1980:100)

9 kap. 32 §

Paragrafen är ny och innebär att det i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt hos Försvarets radioanstalt i underrättelse- och säkerhetsverksamheten gäller sekretess för uppgifter om enskildas personliga och ekonomiska förhållanden. Bestämmelsen utgör ett komplement till utrikes- och försvarssekretessen enligt 2 kap. 1 och 2 §§ sekretesslagen, som skyddar verksamheten men inte de enskilda om vilka uppgifter kan förekomma i de angivna verksamheterna. Beträffande vilka verksamheter hos myndigheterna som omfattas av bestämmelsen, se avsnitt 9.

Sammanfattning av betänkandet SOU 2003:32 i nu aktuell del

Försvarsmaktens underrättelseverksamhet

Försvarsunderrättelseverksamhet skall enligt 1 § första stycket lagen (2000:130) om försvarsunderrättelseverksamhet bedrivas för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars-, och säkerhetspolitik. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred. I lagens 4 § anges generellt att försvarsunderrättelseverksamheten inte får avse uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete. Enligt utredningens bedömning är det mycket tveksamt om nämnda lag kan anses ge någon fristående befogenhet för Försvarsmakten att inom ramen för den egna underrättelseverksamheten inhämta, bearbeta och analysera underrättelser om internationell terrorism.

När det gäller sådana yttre väpnade hot som kan utgöra en direkt fara för landet, anser utredningen det ofrånkomligt att de i viss utsträckning blir föremål för en aktiv underrättelseverksamhet. Annars skulle en viktig del av skyddet för landets säkerhet riskera att falla mellan stolarna. Frågan kan emellertid ställas om underrättelseverksamhet av detta slag bör inbegripas i försvarsunderrättelseverksamheten eller ankomma på den civila säkerhetstjänsten eller, eventuellt, vara en uppgift för båda organisationerna.

Säkerhetspolisen arbetar i princip inte utanför Sveriges gränser. Enligt internationell praxis anses det nämligen inte böra förekomma att en polisorganisation utan särskilt tillstånd arbetar i en främmande stat. Som framgår av det följande föreslår utredningen att Säkerhetspolisen ombildas till en icke-polisiär civil säkerhetstjänst. Därmed skulle något hinder inte finnas mot att underrättelseoperationer utomlands sker genom den civila säkerhetstjänsten. Utredningen är dock tveksam till en sådan förändring och anser sig i varje fall inte ha underlag för att föreslå denna i nuvarande läge.

Försvarsmakten har till skillnad från Säkerhetspolisen personal utomlands, vilket innebär att vissa slags spaningsinsatser exempelvis i anslutning till konflikthärdar i främmande länder rimligen måste vara en uppgift för Försvarsmakten. Den lagstiftning om Försvarsmaktens medverkan i terrorismbekämpningen som utredningen har föreslagit medför också att det framstår som naturligt att viss underrättelseverksamhet av aktuellt slag ankommer på Försvarsmakten. Det är av flera skäl knappast tillrådligt att mer än ett organ skulle ha till uppgift att bedriva permanent underrättelse- verksamhet utanför landets gränser, en ordning som inte heller förekommer i sådana länder som vi brukar jämföra oss med. När det gäller en så viktig fråga som landets säkerhet är det nödvändigt att ansvarsförhållandena är klarlagda och ändamålsenliga.

Den del av försvarsunderrättelseverksamheten som bedrivs till stöd för svensk utrikes-, försvars-, och säkerhetspolitik har kommit att få allt större betydelse. Utredningen har svårt att se att det beträffande denna del av verksamheten behövs några särskilda avgränsningar i lag utöver att den skall bedrivas utomlands eller med sikte på utländska förhållanden.

Utredningen föreslår därför att lagen om försvarsunderrättelseverksamhet ändras så att det står klart att försvarsunderrättelsemyndigheterna får inhämta underrättelser utomlands som är av betydelse för skyddet mot terroristangrepp samt bearbeta och analysera sådan information. Detsamma gäller i fråga om andra underrättelser, om de behövs till stöd för svensk utrikes-, försvars- och säkerhetspolitik. Sådan verksamhet får dock endast bedrivas utomlands eller med sikte på utländska förhållanden.

Lagförslag i betänkandet SOU 2003:32

Förslag till lag om ändring i lagen (2000:130) om försvarsunderrättelseverksamhet

Härigenom föreskrivs att 1 och 4 §§ lagen (2000:130) om försvarsunderrättelseverksamhet skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre *militära* hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred.	Försvarsunderrättelseverksamhet skall bedrivas för att kartlägga yttre *väpnade* hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred.

Regeringen skall bestämma försvarsunderrättelseverksamhetens inriktning.

Försvarsunderrättelseverksamhet skall bedrivas av Försvarsmakten och de andra myndigheter som regeringen bestämmer.

4 §	
Försvarsunderrättelseverksamheten får inte avse uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete.	Försvarsunderrättelseverksamheten får inte avse uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete. *Detta gäller dock inte försvarsunderrättelseverksamhet som bedrivs utomlands eller med inriktning på utländska förhållanden.*

Denna lag träder i kraft den 1 januari 2004.

Förteckning över remissinstanserna

Följande remissinstanser har beretts tillfälle att yttra sig över 11 september-utredningens betänkande (SOU 2003:32) Vår beredskap efter den 11 september: Riksdagens ombudsmän, Svea hovrätt , Hovrätten för Nedre Norrland, Stockholms tingsrätt, Malmö tingsrätt, Göteborgs tingsrätt, Kammarrätten i Sundsvall, Kammarrätten i Jönköping, Justitiekanslern, Riksåklagaren, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Registernämnden, Datainspektionen, Statskontoret, Migrationsverket, Utlänningsnämnden, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Krisberedskapsmyndigheten, Statens räddningsverk, Styrelsen för psykologiskt försvar, Kustbevakningen, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets pliktverk, Försvarets underrättelsenämnd, Socialstyrelsen, Smittskyddsinstitutet, Tullverket, Finansinspektionen, Riksskatteverket, Länsstyrelsen i Stockholms län, Länsstyrelsen i Uppsala län, Länsstyrelsen i Södermanlands län, Länsstyrelsen i Kalmar län, Länsstyrelsen i Skåne län, Länsstyrelsen i Hallands län, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Gotlands län, Göteborgs universitet, samhällsvetenskapliga fakulteten, Stockholms universitet, samhällsvetenskapliga fakulteten, Lunds universitet, juridiska fakulteten, Uppsala universitet, juridiska fakulteten, Statens jordbruksverk, Livsmedelsverket, Statens veterinärmedicinska anstalt, Statens strålskyddsinstitut, Statens kärnkraftinspektion, De lokala säkerhetsnämnderna vid kärntekniska anläggningar, Post- och telestyrelsen, Banverket, Vägverket, Sjöfartsverket, Luftfartsverket, Affärsverket svenska kraftnät, Statens energimyndighet, Elsäkerhetsverket, Svenska Kommunförbundet, Stockholms kommun, Göteborgs kommun, Malmö kommun, Landstingsförbundet, Sveriges advokatsamfund, Tjänstemännens Centralorganisation, Sveriges Akademikers Centralorganisation, Landsorganisationen i Sverige, Föreningen Svenskt Näringsliv, Facket för service och kommunikation, Svensk Handel, Svenska polisförbundet, ST-Polisväsende, Officersförbundet, Sveriges Reservofficersförbund, Värnpliktsrådet, Civilpliktsrådet, Försvarsförbundet, TULL-KUST och Utrikespolitiska Institutet.

Yttrande har vidare inkommit från utredningen om Utveckling av området civil säkerhet inom Östersjöstaternas råd (Fö2002:03).

Sammanfattning av promemorian Ds 2005:30

Bakgrund

Promemorians utgångspunkt är att Sverige behöver en väl fungerande och effektiv underrättelseverksamhet. Den förändrade säkerhetspolitiska situationen har medfört att vi idag måste möta ett bredare spektrum av hot, risker och påfrestningar mot samhället. Det kan gälla bl.a. terrorism, spridning av massförstörelsevapen, etniska och religiösa konflikter samt den sårbarhet som den tekniska utvecklingen och informationsteknologin för med sig. Detta ställer nya krav på försvarsunderrättelseverksamheten, vilket har understrukits i t.ex. betänkandet Vår beredskap den 11 september (SOU 2003:32) från 11 september-utredningen.

Sedan det kalla krigets slut har det skett en gradvis tyngdpunktsförskjutning från traditionell militär, operativ och taktisk förvarning i riktning mot strategiska och icke-militära underrättelser. 11 september-utredningen framhöll att detta kräver att nya metoder utvecklas och att samarbetet utökas, såväl nationellt mellan de myndigheter som bedriver försvarsunderrättelseverksamhet och andra underrättelseorgan, som internationellt mellan olika länders underrättelsetjänster. Mot denna bakgrund föreslog utredningen att lagen (2000:130) om försvarsunderrättelseverksamhet ändras så att försvarsunderrättelseverksamhet inriktas på yttre väpnade hot mot landet, vare sig de är militära eller inte. Vidare föreslog utredningen att sådan försvarsunderrättelseverksamhet som bedrivs utomlands, eller med sikte på utländska förhållanden, inte borde vara underkastad begränsningen att den inte får avse uppgifter som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete.

Regeringen har i flera sammanhang, bl.a. de senaste budgetpropositionerna, pekat på det ökande behovet av strategiska underrättelser av civil karaktär med relevans för utrikes-, säkerhets- och försvarspolitiken. Försvarsunderrättelseverksamheten bör också inriktas på att utveckla det internationella underrättelsesamarbetet, särskilt det inom EU. Ytterligare ansträngningar bör göras för att stödja svensk trupp och personal i internationella insatser. Regeringens bedömning är att det förändringsarbete som har inletts för att förbättra inriktning, inhämtningsmetoder och analyser bör fortsätta. Regeringen har också pekat på behoven av att anpassa lagen om försvarsunderrättelseverksamheten till de nya förhållandena.

I betänkandet Försvarets radioanstalt – en översyn (SOU 2003:30) konstaterar FRA-utredningen att frågan om den rättsliga regleringen av Försvarets radioanstalts verksamhet borde övervägas i annan ordning än inom ramen för den utredningen. Utredningen framhöll bl.a. att den tekniska utvecklingen har medfört att signaler i allt större utsträckning förmedlas i tråd, medan Försvarets radioanstalts signalspaning med nuvarande lagstiftning är begränsad till eterburna signaler. För att Försvarets radioanstalt i framtiden skall kunna bedriva en ändamålsenlig verksamhet till rimliga kostnader är det, enligt utredningen, väsentligt att signalspaning kan bedrivas oavsett med vilken teknik signalerna vidarebeford-

ras. Utredningen underströk att signalspaning mot trådbunden trafik måste ges ett uttryckligt stöd i lagstiftningen. Detta är idag fallet i flera med Sverige jämförbara länder, t.ex. Nederländerna, Storbritannien och Tyskland.

Sammanfattning av författningsförslagen

För att anpassa försvarsunderrättelseverksamheten till de växande underrättelsebehoven inom utrikes-, försvars- och säkerhetspolitiken, föreslås i denna promemoria följande förändringar av den rättsliga regleringen för verksamheten:

- Mandatet för försvarsunderrättelseverksamheten ändras från ”yttre militära hot” till ”yttre hot” (kapitel 4);
- gränsdragning mellan polisiär verksamhet och försvarsunderrättelsetjänst förtydligas med anledning av förslag från 11 september-utredningen och remissinstanser (kapitel 4);
- tydligare reglering av inriktning, rapportering av underrättelser och inhämtningen med särskilda metoder (kapitel 4);
- ett uttryckligt lagstöd för signalspaningen i syfte att anpassa verksamheten till den tekniska utvecklingen (kapitel 5); samt
- en förstärkning av samhällets funktioner för inriktning och kontroll av underrättelseverksamheten (kapitel 6).

Mandatet för försvarsunderrättelseverksamhet ändras från ”yttre militära hot” till ”yttre hot”

Idag föreskriver 1 § i lagen (2000:130) om försvarsunderrättelseverksamhet att verksamheten skall avse ”yttre militära hot”. Detta begrepp är alltför snävt eftersom en betydande del av den nya hotbilden består av icke-militära hot. Förutom att tjäna som ett stöd för svensk utrikes-, säkerhets- och försvarspolitik, skall försvarsunderrättelseverksamheten därför avse ”yttre hot”, oavsett deras karaktär och ursprung. I verksamheten skall också ingå att medverka i svenskt deltagande i internationellt säkerhetssamarbete.

Den är angeläget att bevara den sedan länge rådande huvudprincipen att yttre militära hot skall hanteras av Försvarsmakten, medan det ankommer på myndigheterna inom rättsväsendet att förebygga och bekämpa terrorism och annan gränsöverskridande brottslighet.

Försvarsunderrättelseverksamheten bör vidare förbli inriktad uteslutande på utländska förhållanden, dvs. verksamheter eller företeelser som har sin utgångspunkt i utlandet. Försvarsunderrättelseverksamheten skall följaktligen inhämta, bearbeta och delge sådan information om företeelser och förhållanden i andra länder som t.ex. ger svenska beslutsfattare ett förbättrat underlag för beslut och bedömningar i utrikes-, säkerhets- och försvarspolitiska frågor eller för att skydda svensk personal som deltar i internationella insatser.

Gränsdragning mellan polisiär verksamhet och försvarsunderrättelsetjänst förtydligas med anledning av förslag från 11 september-utredningen och remissinstanser

Den tekniska utvecklingen och de gränsöverskridande hoten har gjort att skiljelinjen mellan inre/polisiär och yttre/militär säkerhet är mer oklar än tidigare. Det är därför angeläget att säkerställa att ett nytt och utvidgat mandat för försvarsunderrättelseverksamheten inte kommer i konflikt med den begränsning som följer av den nuvarande regleringen av förhållandet mellan försvarsunderrättelseverksamheten samt de brottsbekämpande och brottsförebyggande myndigheternas arbete. I detta syfte föreslås ett förtydligande så att terrorism och andra yttre hot i form av t.ex. internationell kriminalitet inte utesluts från försvarsunderrättelseverksamheten.

Tydligare reglering av inriktning, rapportering av underrättelser och inhämtningen med särskilda metoder

Regeringen skall liksom hittills bestämma försvarsunderrättelseverksamhetens inriktning. Det bör dock som tidigare också finnas en möjlighet för de myndigheter som är konsumenter av underrättelserättelser att närmare inrikta verksamheten inom den ram som regeringen har fastställt. I förtydligande syfte föreslås att det av lagen om försvarsunderrättelseverksamhet skall framgå att en närmare inriktning av verksamheten får anges av de myndigheter som regeringen bestämmer.

Lagregleringen av försvarsunderrättelseverksamheten bör i första hand vara inriktad på att inhämta, bearbeta och genomföra grundanalys av information. Det som kommer ut ur denna process är underrättelser. För att tydliggöra att det inte i första hand är den färdiganalyserade bedömningen som omfattas av lagens rapporteringsskyldighet som skall rapporteras bör föreskriften om att analyser av hotbilder och bedömningar i underrättelsefrågor skall rapporteras till Regeringskansliet och andra berörda myndigheter utgå. I konsekvens därmed föreslås en ändring i lagen med innebörden att det i första hand är underrättelser som skall rapporteras.

Av lagen om försvarsunderrättelseverksamhet bör i förtydligande syfte framgå vilka särskilda verktyg som får användas för att bedriva verksamheten. I promemorian föreslås att lagen skall ange att försvarsunderrättelseverksamheten får använda sig av teknisk och personbaserad inhämtning som sker med särskilda metoder.

Införande av ett uttryckligt lagstöd för signalspaningen i syfte att anpassa verksamheten till den tekniska utvecklingen

Inhämtning genom signalspaning är en av grunderna för Sveriges försvarsunderrättelseförmåga. Alternativa inhämtningsmetoder kan sällan mäta sig med signalspaningen vid en effektivitets- och kostnadsjämförelse. Den tekniska utvecklingen har dock inneburit att signaler i allt större utsträckning förmedlas genom tråd. Den signalspaningsverksamhet som Försvarets radioanstalt bedriver mot eterburna signaler framstår mot denna bakgrund som otillräcklig. I promemorian föreslås därför att Försvarets radioanstalt skall få bedriva signalspaning oavsett om signalerna

befinner sig i etern eller är trådbundna. Detta skall enligt förslaget regleras i en ny lag om signalspaning.

Den nya lagen bör tydligt ange när signalspaning får ske, d.v.s. tillämpningsområdet skall vara klart avgränsat. Inhämtning av signaler i elektronisk form skall få ske för försvarsunderrättelseverksamheten. Signalspaningen skall vidare få ske för att följa förändringar i signalmiljön i omvärlden, i den tekniska utvecklingen och inom signalskyddet samt för att fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

Eftersom signalspaning kan medföra intrång i enskildas personliga integritet föreslås en rad bestämmelser som syftar till att säkerställa skyddet för den enskilde.

Inhämtning som sker i tråd skall enligt förslaget endast få ske av signaler, vilka förs över Sveriges gräns av operatörer som äger tråd. Den skall ske automatiserat och får endast avse signaler som har identifierats genom sökbegrepp. När automatiserad inhämtning sker av andra signaler än sådana som förmedlas i tråd skall också sökbegrepp användas för att identifiera signalerna. Sökbegreppen får inte vara direkt hänförliga till viss fysisk person, såvida det inte är av synnerlig vikt för verksamheten. Sökbegreppen skall granskas i särskild ordning. Förslaget innebär att en myndighet som enligt regeringens bestämmande har rätt att inrikta signalspaningen skall inhämta tillstånd av Försvarets underrättelsenämnd innan inriktningen sker. Om tillstånd inte utan väsentlig olägenhet kan inväntas kan inriktningen ske utan tillstånd, men skall då anmälas till nämnden. Tillstånd skall endast lämnas för inriktning som avser sådan verksamhet för vilken signalspaning får bedrivas, och som är förenlig med lagen om försvarsunderrättelseverksamhet. Tillstånd får inte ges om inriktningen endast avser viss fysisk person.

För att säkerställa att information inhämtad genom signalspaning inte används för andra syften än de som anges i lagen föreslås att en upptagning eller uppteckning av uppgifter som inhämtats i elektronisk form omgående skall förstöras om den t.ex. bedömts sakna betydelse för den verksamhet som regleras i lagen. I samma syfte föreslås att rapportering av underrättelser som baseras på information inhämtad genom signalspaning endast skall få avse förhållanden som är av betydelse för ändamålet med verksamheten såsom den har formulerats i lagen om försvarsunderrättelseverksamhet.

En särskild myndighet (Försvarets underrättelsenämnd) skall kontrollera efterlevnaden av lagen om signalspaning. I kontrollen skall särskilt ingå en granskning av sökbegreppen och av rapporteringen.

För att Försvarets radioanstalt skall få tillgång till signaler som förmedlas i tråd föreslås en bestämmelse i lagen (2003:389) om elektronisk kommunikation med innebörd att de trådägande operatörerna skall till särskilda samverkanspunkter överföra all trafik som förs över Sveriges gräns.

En förstärkning av samhällets funktioner för inriktning och kontroll av underrättelseverksamheten

Försvarets underrättelsenämnds uppgift är idag att följa verksamheten inom de myndigheter som bedriver försvarsunderrättelseverksamhet. När

mandatet för försvarsunderrättelseverksamheten utökas finns anledning att ytterligare betona betydelsen av en utomstående granskning av dessa myndigheters verksamhet genom att utvidga nämndens mandat till att också omfatta kontroll av försvarsunderrättelseverksamheten.

Som tidigare har nämnts föreslås också att nämnden skall ge tillstånd till sådan närmare inriktning som anges i förslaget till lag om signalspaning samt kontrollera efterlevnaden av den lagen och därvid särskilt granska användning av sökbegrepp och rapportering.

En utvidgad kontrollfunktion kräver att Försvarets underrättelsenämnd utökas med en ledamot och att nämnden förstärks med ett permanent kansli under ledning av en kanslichef.

Lagförslagen i Ds 2005:30

Förslag till lag om ändring i lagen (2000:130) om försvarsunderrättelseverksamhet

Härigenom föreskrivs att 1-5 §§ lagen (2000:130) om försvarsunderrättelseverksamhet skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Försvarsunderrättelseverksamhet skall bedrivas *för att kartlägga yttre militära hot mot landet och till stöd för svensk utrikes-, försvars- och säkerhetspolitik.* I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete *och att, enligt vad regeringen närmare bestämmer, medverka med underrättelser för att stärka samhället vid svåra påfrestningar på samhället i fred.*	Försvarsunderrättelseverksamhet skall bedrivas *till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet.* I verksamheten ingår *också* att medverka i svenskt deltagande i internationellt säkerhetssamarbete. *Försvarsunderrättelseverksamhet får endast avse utländska förhållanden.*
Regeringen skall bestämma försvarsunderrättelseverksamhetens inriktning.	Regeringen skall bestämma försvarsunderrättelseverksamhetens inriktning. *Inom ramen för denna inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten.*
Försvarsunderrättelseverksamhet skall bedrivas av *Försvarsmakten och de andra* myndigheter som regeringen bestämmer.	Försvarsunderrättelseverksamhet skall bedrivas av *den eller de* myndigheter som regeringen bestämmer.
	2 §
Uppgifterna som anges i 1 § skall fullgöras genom inhämtning, bearbetning och analys av information. *Analyser av hotbilder och bedömningar i underrättelsefrågor* skall rapporteras till *Regeringskansliet och andra* berörda myndigheter.	*Verksamheten enligt* 1 § skall fullgöras genom inhämtning, bearbetning och analys av information. *Underrättelser* skall rapporteras till berörda myndigheter. *I verksamheten får användas teknisk och personbaserad inhämtning med särskilda metoder.* *Vissa bestämmelser om teknisk inhämtning finns i lagen (2006:000) om signalspaning i*

	3 §
De myndigheter som skall bedriva försvarsunderrättelseverksamhet får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer.	*Den eller* de myndigheter som skall bedriva försvarsunderrättelseverksamhet får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer.
	4 §
Försvarsunderrättelseverksamheten får inte *avse uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete.*	Försvarsunderrättelseverksamhet får inte *innefatta åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete enligt lagar och förordningar.* *Utan hinder av första stycket får försvarsunderrättelseverksamhet, utan att riktas mot fysisk person, bedrivas för kartläggning av utländska förhållanden som innebär yttre hot mot landet.*
	5 §
En särskild nämnd under regeringen skall ha insyn i försvarsunderrättelseverksamheten enligt vad regeringen närmare föreskriver.	*Den myndighet som regeringen bestämmer skall kontrollera försvarsunderrättelseverksamheten.*

Denna lag träder i kraft den 1 juli 2006.

Förslag till lag (2005:000) om signalspaning

Härigenom föreskrivs följande.

1 § För den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet får signaler i elektronisk form inhämtas vid signalspaning.

Inhämtning av signaler i elektronisk form vid signalspaning får, även om den inte omfattas av den verksamhet som anges i första stycket, ske för att

1. följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt

2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

2 § Inhämtning som sker i tråd får endast avse signaler vilka förs över Sveriges gräns av operatörer som äger tråd.

3 § Inhämtning av signaler i tråd skall ske automatiserat. Sådan inhämtning får endast avse signaler som identifierats genom sökbegrepp. Även vid annan automatiserad inhämtning skall sökbegrepp användas för identifiering av signaler. Sökbegreppen får inte vara direkt hänförliga till viss fysisk person såvida det inte är av synnerlig vikt för verksamheten.

4 § Endast den myndighet som regeringen bestämmer får bedriva inhämtning enligt 1 §.

5 § I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet.

Regeringen skall bestämma inriktningen av den verksamhet som bedrivs enligt 1 § andra stycket.

6 § Annan myndighet än Regeringskansliet får inte utan tillstånd ge närmare inriktning av signalspaning enligt 1 § första stycket. Tillstånd lämnas av den myndighet som regeringen bestämmer. Tillstånd får endast avse inriktning som är förenlig med lagen (2000:130) om försvarsunderrättelseverksamhet. Tillstånd får inte lämnas om inriktningen endast avser viss fysisk person.

Om tillstånd inte utan väsentlig olägenhet kan avvaktas får inriktning ges utan att tillstånd har lämnats. Inriktningen skall då anmälas till den myndighet som har att lämna tillstånd.

7 § Upptagning eller uppteckning av uppgifter som erhållits genom inhämtning enligt denna lag skall omgående förstöras om

a) den bedömts sakna betydelse för verksamhet som avses i 1 §,

b) den omfattar uppgifter beträffande vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen eller inhämtningen är oförenlig med 3 kap. 4 § tryckfrihetsförordningen eller 2 kap. 4 § yttrandefrihetsgrundlagen.

8 § Rapportering av underrättelser som erhållits vid signalspaning i försvarsunderrättelseverksamhet regleras i lagen (2000:130) om försvarsunderrättelseverksamhet. Sådan rapportering får endast omfatta förhållanden som är av betydelse i de hänseenden som anges i 1 § den lagen.

9 § Den myndighet som regeringen bestämmer får för den verksamhet som anges i 1 § andra stycket, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.

10 § Den myndighet som regeringen bestämmer skall kontrollera efterlevnaden av denna lag. I kontrollen skall särskilt ingå granskning av sökbegrepp som avses i 3 § och rapportering som avses i 8 §.

11 § I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om operatörers skyldighet att överföra trafik för att möjliggöra inhämtning enligt denna lag.

12 § Beslut enligt denna lag får inte överklagas.

Denna lag träder i kraft den 1 januari 2006.

Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2003:389) om elektronisk kommunikation

dels att 6 kap. 21 § skall ha följande lydelse,

dels att det skall införas en ny paragraf, 6 kap. 19 a §, av följande lydelse.

6 kap.

19 a §

För att inhämtning av signaler i elektronisk form enligt lagen (2006:000) om signalspaning skall kunna ske, är operatörer som äger tråd i vilka signaler förs över Sveriges gräns skyldiga att överföra dessa till samverkanspunkter. Varje sådan operatör skall utse en eller flera samverkanspunkter och anmäla dessa till den myndighet som regeringen bestämmer. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om samverkanspunkter.

Samtliga operatörer som för signaler i tråd över Sveriges gräns ska l se till att dessa enkelt kan tas om hand.

Samtliga operatörer skall utföra uppgiften enligt denna bestämmelse så att verksamheten inte röjs.

21 §

Tystnadsplikt enligt 20 § första stycket gäller även för uppgift som hänför sig till

1. åtgärden att kvarhålla försändelser enligt 27 kap. 9 § rättegångsbalken,

2. angelägenhet som avser användning av hemlig teleavlyssning eller hemlig teleövervakning enligt 27 kap. 18 eller 19 § rättegångsbalken, och

3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2006:000) om signalspaning i försvarsunderrättelseverksamhet.

---

1. Denna lag träder i kraft den 1 juli 2006.

2. Skyldigheten för operatörer som äger tråd att överföra signaler till samverkanspunkter enligt 6 kap. 19 a § skall tillämpas första gången den 1 januari 2007. Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om att bestämmelserna om skyldigheten skall börja tillämpas senare.

Förteckning över remissinstanserna

Följande remissinstanser har beretts tillfälle att yttra sig över departementspromemorian Ds 2005:30 En anpassad försvarsunderrättelseverksamhet: Riksdagens ombudsmän, Hovrätten över Skåne och Blekinge, Hovrätten för Övre Norrland, Kammarrätten i Stockholm, Kammarrätten i Jönköping, Stockholms tingsrätt, Malmö tingsrätt, Göteborgs tingsrätt, Justitiekanslern, Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Registernämnden, Inspektionen för strategiska produkter, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Krisberedskapsmyndigheten, Försvarshögskolan, Totalförsvarets forskningsinstitut, Försvarets underrättelsenämnd, Statens räddningsverk, Kustbevakningen, Tullverket, Finansinspektionen, Ekonomistyrningsverket, Skatteverket, Premiepensionsmyndigheten, Datainspektionen, Kammarkollegiet, Stockholms universitet, Örebro universitet, Göteborgs universitet, Umeå universitet, Riksarkivet, Radio- och TV-verket, Statens kärnkraftsinspektion, Affärsverket svenska kraftnät, Elsäkerhetsverket, Statens energimyndighet, Konkurrensverket, Post- och telestyrelsen, Banverket, Luftfartsstyrelsen, Verket för näringslivsutveckling, Sveriges advokatsamfund, Svenska polisförbundet, Tryck- och yttrandefrihetsberedningen (Ju 2003:04), Amnesty International, Länssamverkan Bredband, Svenska bankföreningen, Svenska IT-företagens organisation, Svenska Journalistförbundet, Tidningsutgivarna, Svenska Stadsnätsföreningen, Svenskt näringsliv, Swedish Network Users Society, Swedish University Network, E ON AB, Stokab AB, TeliaSonera AB och Vattenfall AB.

Yttrande har vidare inkommit från Sveriges Riksbank.

Sammanfattning av förslaget i SOU 2003:34 om en ny bestämmelse i sekretesslagen

I Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten finns uppgifter som kan vara mycket integritetskänsliga för enskilda och deras närstående och som inte skyddas av gällande sekretessregler. Det kan t.ex. gälla uppgifter som avslöjar en persons fysiska eller psykiska hälsotillstånd. Den sekretess som i dag gäller för uppgifter i den militära underrättelse- och säkerhetstjänsten syftar endast till att skydda själva verksamheten hos myndigheten och utgör därmed inget skydd för enskilda individer och deras personliga eller ekonomiska intressen. Mot bakgrund härav föreslår vi att det i sekretesslagen (1980:100) införs en bestämmelse om sekretess hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten, till skydd för uppgift om enskilds personliga eller ekonomiska förhållanden. Sekretess för sådan uppgift skall enligt vår mening gälla om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men. Sekretess bör gälla i högst 70 år.

Lagförslag i betänkandet SOU 2003:34 angående sekretess

Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att det i sekretesslagen (1980:100) skall införas en ny paragraf, 9 kap. 27 §, av följande lydelse.

9 kap.

27 § Sekretess gäller hos Försvarsmakten i den militära underrättelse- och säkerhetstjänsten för uppgift om enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 juli 2004.

Förteckning över remissinstanserna

Efter remiss har följande instanser lämnat yttrande över departementspromemorian Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt (Ds 2005:50): Riksdagens ombudsmän, Hovrätten för Övre Norrland, Kammarrätten i Stockholm, Länsrätten i Uppsala län, Justitiekanslern, Försvarsmakten, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Försvarets underrättelsenämnd, Datainspektionen, Göteborgs universitet och Riksarkivet.

Försvarets materielverk och Uppsala universitet har avstått från att yttra sig.