Ds 2005:30

En anpassad försvarsunderrättelseverksamhet

REGERINGSKANSLIET
Försvarsdepartementet

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, 2003.
– En liten broschyr som underlättar arbetet för den som skall svara på remiss.

Broschyren är gratis och kan laddas ner eller beställas på
http://www.regeringen.se/remiss

Tryckt av XGS Grafisk Service
Stockholm 2005

ISBN 91-38-22401-1
ISSN 0284-6012

Innehåll

Förkortningar

AIVD	*Algemene Inlichtingen- en Veiligheistdienst*, holländsk civil underrättelse- och säkerhetstjänst
ANBw	*Amt für Nachrichtenswesen der Bundeswehr*, en särskild central myndighet under det tyska försvarsdepartementet
bet.	betänkande
BfV	*Bundesamt für Verfassungsschutz*, tysk civil inrikes säkerhets-tjänst
BND	*Bundesnachrichtendienst*, tysk civil underrättelsetjänst
BNDG	*Gesetz über den Bundesnach-richtendienst*, tysk lagstiftning som reglerar BND:s verksamhet
BSS	*The British Security Service (MI5)*, brittisk civil säkerhets-tjänst

CIA	*Central Intelligence Agency*, amerikansk civil underrättelsetjänst
DIA	*Defense Intelligence Agency*, amerikansk militär underrättelsetjänst
DIS	*The Defence Intelligence Staff*, brittisk militär underrättelsetjänst
Ds	Departementsskrivelse
ESFP	Europeiska säkerhets- och försvarspolitiken
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen	Europeiska konventionen (den 4 november 1950) om skydd för de mänskliga rättigheterna och de grundläggande friheterna
FBI	*Federal Bureau of Investigation*, amerikansk federal polismyndighet
FRA	Försvarets radioanstalt
FUN	Försvarets underrättelsenämnd
Fü SII	*Fürungsstab Zwei*, tysk militär underrättelsetjänst

FöU	Försvarsutskottet
GCHQ	*The Government Communications Headquarters*, brittisk signalspaningsorganisation
GUSP	EU:s gemensamma utrikes- och säkerhetspolitik
HUMINT	*Human Intelligence* (personbaserad inhämtning)
JIC	*The Joint Intelligence Committee*, brittiskt organ för inriktning av underrättelseinhämtning
KOS	Kommunikationsspaning
KSI	Kontoret för särskild inhämtning, vilket är en del av Militära underrättelse- och säkerhetstjänsten (MUST)
LWND	*Luftwaffen Nachrichtendienst*, schweizisk flygvapenunderrättelsetjänst
MAD	*Militärischer Abschirmdienst*, tysk militär säkerhetstjänst
MIVD	*Militäre Inlichtingen-Veiligheidsdienst*, holländsk militär underrättelsetjänst

MND	*Militärische Nachrichtendienst*, schweizisk militär underrättelsetjänst
MUST	Den militära underrättelse- och säkerhetstjänsten
NSA	*National Security Agency*, amerikansk signalspaningsorganisation
PKK	*Die Parlamentarische Kontrollkommission*, tysk kontrollfunktion av underrättelse- och säkerhetstjänsten
prop.	proposition
RIPA	*Regulation of Investigatory Powers Act 2000*
SIGINT	*Signal Intelligence* (signalspaning)
SIS	*Secret Intelligence Service* (MI6), brittisk civil underrättelsetjänst

Författningsförslag

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*

Försvarsunderrättelseverksamhet skall bedrivas av *Försvarsmakten och de andra* myndigheter som regeringen bestämmer.	*bestämmer ange en närmare inriktning av verksamheten.* 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.*
	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.*

Försvarsunderrättelsverksamhet 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.

2 Förslag till förordning om ändring i förordningen (2000:131) om försvarsunderrättelseverksamhet

Härigenom föreskrivs att 1, 2, 5 och 6 §§ förordningen (2000:131) om försvarsunderrättelseverksamhet skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
I denna förordning finns bestämmelser om verkställighet av lagen (2000:130) om försvarsunderrättelseverksamhet.	*Denna förordning innehåller föreskrifter som ansluter till vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet.*
	2 §
Försvarsunderrättelseverksamhet skall bedrivas, *förutom* av Försvarsmakten *enligt vad som sägs i 1 § lagen (2000:130) om försvarsunderrättelseverksamhet, även av* Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut.	Försvarsunderrättelseverksamhet skall bedrivas av Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut. *Inhämtning med särskilda metoder enligt 2 § lagen (2000:130) om försvarsunderrättelseverksamhet får bedrivas av Försvarsmakten och Försvarets radioanstalt. Av förordningen (2006:000) om signalspaning framgår att Försvarets radioanstalt bedriver teknisk inhämtning enligt lagen (2006:000) om signalspaning.*

5 §

Försvarsmakten skall underrätta Försvarets underrättelsenämnd i frågor om ledning av försvarsunderrättelseverksamheten, om frågorna är principiella eller annars av större vikt, och under förutsättning att inte verksamheten därigenom avsevärt försvåras. Om *Försvarsmakten* inte har kunnat lämna information, skall frågan utan dröjsmål lämnas till nämnden.

Försvarsmakten skall även informera nämnden om innehållet i den instruktion och de föreskrifter som gäller för den enhet inom myndigheten som inhämtar underrättelser med särskilda metoder.

Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Totalförsvarets forskningsinstitut skall informera Försvarets underrättelsenämnd i frågor som rör försvarsunderrättelseverksamhet, om frågorna är principiella eller annars av större vikt, och under förutsättning att inte verksamheten därigenom avsevärt försvåras. Om *myndigheterna* inte har kunnat lämna information, skall frågan utan dröjsmål lämnas till nämnden.

Försvarsmakten och Försvarets radioanstalt skall även informera nämnden om de bestämmelser som gäller för den verksamhet som inhämtar underrättelser med särskilda metoder.

6 §

De myndigheter som anges i 2 § skall informera Försvarets underrättelsenämnd om de principer som tillämpas för samarbete i underrättelsefrågor med andra länder och internationella organisationer samt lämna uppgift om med vilka länder och organisationer sådan samarbete sker. Myndigheterna skall sedan samarbetet etablerats informera nämnden om omfattningen av samarbetet och, när det bedöms påkallat, om resultatet, erfarenheterna och den fortsatta inriktningen av samarbetet. *Myndigheterna skall även i andra viktiga frågor som rör försvarsunderrättelseverksamhet lämna information till nämnden.*	De myndigheter som anges i 2 § skall informera Försvarets underrättelsenämnd om de principer som tillämpas för samarbete i underrättelsefrågor med andra länder och internationella organisationer samt lämna uppgift om med vilka länder och organisationer sådan samarbete sker. Myndigheterna skall sedan samarbetet etablerats informera nämnden om omfattningen av samarbetet och, när det bedöms påkallat, om resultatet, erfarenheterna och den fortsatta inriktningen av samarbetet.
Om informationen som avses i första stycket inte har kunnat lämnas, skall frågan utan dröjsmål anmälas för nämnden. Myndigheterna skall lämna informationen på det sätt nämnden bestämmer.	Om informationen som avses i första stycket inte har kunnat lämnas, skall frågan utan dröjsmål anmälas för nämnden. Myndigheterna skall lämna informationen på det sätt nämnden bestämmer.
Myndigheterna skall senast den 1 mars varje år lämna den	Myndigheterna skall senast den 1 mars varje år lämna den delen av årsredovisningen och budgetunderlaget som rör försvarsunderrättelseverksamheten till nämnden.

delen av årsredovisningen och budgetunderlaget som rör försvarsunderrättelseverksamheten till nämnden.

Denna förordning träder i kraft den 1 juli 2006.

3 Förslag till förordning om ändring i förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd

Härigenom föreskrivs i fråga om förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd

dels att 1–5, 8–10 och 13 §§ skall ha följande lydelse

dels att det skall införas en ny paragraf, 2 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Försvarets underrättelsenämnd har till uppgift att *följa underrättelsetjänsten inom Försvarsmakten och de övriga myndigheter* som enligt förordningen (2000:131) om försvarsunderrättelseverksamhet bedriver *försvarsunderrättelseverksamhet.*	Försvarets underrättelsenämnd har till uppgift att *kontrollera försvarsunderrättelseverksamheten hos den eller de myndigheter* som enligt förordningen (2000:131) om försvarsunderrättelseverksamhet bedriver *sådan verksamhet*. *Nämnden skall även granska behandlingen av uppgifter enligt lagen (2006:000) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt enligt lagen (2006:000) om behandling av personuppgifter i Försvarets radioanstalts underrättelseverksamhet.*

2 §

Nämnden skall särskilt	Nämnden skall särskilt
1. följa hur lagen (2000:130) om försvarsunderrättelseverksamhet och förordningen (2000:131) om försvarsunderrättelseverksamhet tillämpas,	1. följa hur lagen (2000:130) om försvarsunderrättelseverksamhet och förordningen (2000:131) om försvarsunderrättelseverksamhet tillämpas,
2. granska att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning som är bestämd,	2. granska att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning som är bestämd,
3. *ägna uppmärksamhet åt de enheter inom Försvarsmakten och Försvarets radioanstalt som inhämtar underrättelser med särskilda metoder,*	3. *granska de verksamheter där teknisk och personbaserad inhämtning med särskilda metoder ingår,*
4. granska de medel och metoder för inhämtning av underrättelser som används,	*4. granska de sökbegrepp som används och den rapportering som sker enligt lagen (2006:000) om signalspaning,*
5. *granska hur de register som behövs för försvarsunderrättelseverksamheten läggs upp och förs samt*	*5. granska principer för rekrytering och utbildning av personal*.
6. *granska principer för rekrytering och utbildning av personal*.	

2 a §

Nämnden har även till uppgift att ge tillstånd till sådan närmare inriktning som anges i lagen (2006:000) om signalspaning samt att kontrollera efterlevnaden av nämnda lag.

3 §

Nämnden 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.

Nämnden skall senast den 1 mars varje år till regeringen lämna en rapport över föregående års granskningsverksamhet.

Nämnden skall lämna *den eller de myndigheter som avses i 1 §* de synpunkter och de förslag till åtgärder som föranleds av granskningsverksamheten. Om det behövs, skall nämnden också lämna *dessa synpunkter och förslag* om åtgärder till regeringen.

Nämnden skall senast den 1 mars varje år till regeringen lämna en rapport över föregående års granskningsverksamhet. *I rapporten skall nämnden särskilt redogöra för tillståndsgivningen samt för den granskningsverksamhet som avser sökbegrepp enligt lagen (2006:000) om signalspaning.*

4 §

Nämnden består av sex personer. En av ledamöterna är ordförande.	*Nämnden består av en ordförande och sex övriga ledamöter. Minst två ledamöter skall vara eller ha varit ordinarie domare.*

5 §

Vid nämnden finns *en sekreterare.*	Vid nämnden finns *ett kansli under ledning av en kanslichef*.

8 §

Nämnden sammanträder på kallelse av ordföranden. *Nämnden skall sammanträda minst fyra gånger om året*. Nämnden skall dessutom sammanträda om någon ledamot eller någon av de myndigheter som bedriver försvarsunderrättelseverksamhet begär det.	Nämnden sammanträder på kallelse av ordföranden. Nämnden skall dessutom sammanträda om någon ledamot eller någon av de myndigheter som bedriver försvarsunderrättelseverksamhet begär det. *När en begäran om tillstånd enligt lagen (2006:000) om signalspaning kommit in till Försvarets underrättelsenämnd skall nämnden sammanträda så snart detta kan ske.* *Försvarets underrättelsenämnd skall fortlöpande granska de sökbegrepp som anges i lagen (2006:000) om signalspaning.*

9 §

Nämndens ordförande och *sekreterare* får pröva frågor om utlämnande av allmänna handlingar och överklagande av nämndens beslut.	Nämndens ordförande och *kanslichef* får *på nämndens vägnar* pröva frågor om utlämnande av allmänna handlingar och överklagande av nämndens beslut.

10 §

Nämnden är beslutför när ordföranden och minst tre av de andra ledamöterna är närvarande. När ärenden av större vikt handläggs skall om möjligt samtliga ledamöter vara närvarande.	Nämnden är beslutför när ordföranden och minst tre av de andra ledamöterna är närvarande. *Vid handläggning av ärenden som avser tillstånd enligt lagen (2006:000) om signalspaning skall minst en av nämndens juristledamöter närvara.* När ärenden av större vikt handläggs skall om möjligt samtliga ledamöter vara närvarande. *Om det framkommer skiljaktiga meningar vid handläggning av ärenden om tillstånd, tillämpas föreskrifterna i 18 § förvaltningslagen (1986:223) om omröstning.*

	13 §
Sekreterare utses av regeringen.	*Kanslichefen* utses av regeringen. *Övriga anställningar beslutas av X-myndigheten efter förslag från nämnden.*

Denna förordning träder i kraft den 1 juli 2006.

4 Förslag till lag (2006:000) 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 § 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 bestämmer 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 omedelbart anmälas till den myndighet som har att lämna tillstånd. Finner tillståndsmyndigheten att inriktningen inte borde ha verkställts skall den myndighet som avses i 4 § underrättas. Verksamheten med anledning av inriktningen skall då omedelbart avbrytas.

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 juli 2006.

5 Förslag till förordning (2006:000) om signalspaning

Härigenom föreskrivs följande.

1 § Denna förordning innehåller föreskrifter som ansluter till vad som föreskrivs i lagen (2006:000) om signalspaning.

2 § Försvarets radioanstalt skall bedriva sådan verksamhet som avses i lagen om signalspaning.

Försvarets radioanstalt bestämmer vilka sökbegrepp som enligt lagen om signalspaning skall användas. Sådana beslut fattas av myndighetens chef.

3 § Försvarets radioanstalt skall fortlöpande till Försvarets underrättelsenämnd redovisa vilka sökbegrepp enligt 3 § lagen om signalspaning som används.

4 § Försvarets radioanstalt får för den verksamheten som anges i 1 § andra stycket lagen om signalspaning samarbeta i signalspaningsfrågor med andra länder och internationella organisationer endast under förutsättning att syftet med samarbetet är att tjäna den svenska statsledningen och den nationella säkerheten. De uppgifter som myndigheten lämnar till andra länder och internationella organisationer får inte vara till skada för svenska intressen.

5 § Försvarets radioanstalt skall till Regeringskansliet (Försvarsdepartementet) anmäla frågor om att etablera och upprätthålla sådant samarbete som avses i 4 §. Myndigheten skall informera Regeringskansliet (Försvarsdepartementet) om viktiga frågor som uppkommer i samarbetet.

Denna förordning träder i kraft den 1 juli 2006.

6 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 (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 skall 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.

---

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.

7 Förslag till förordning om ändring i förordningen (2003:396) om elektronisk kommunikation

Härigenom föreskrivs att det i förordningen (2003:396) om elektronisk kommunikation skall införas en ny paragraf, 36 a §, med följande lydelse.

36 a § Post- och telestyrelsen får efter samråd med Försvarets radioanstalt meddela sådana föreskrifter om samverkanspunkter som avses i 6 kap. 19 a § lagen (2003:389) om elektronisk kommunikation. Operatörer som utser samverkanspunkter skall anmäla dessa till Försvarets radioanstalt.

Denna förordning träder i kraft den 1 juli 2006.

8 Förslag till förordning om ändring i förordningen (1994:714) med instruktion för Försvarets radioanstalt

Härigenom föreskrivs att 1 § förordningen (1994:714) med instruktion för Försvarets radioanstalt skall ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Försvarets radioanstalt är en central förvaltningsmyndighet med uppgift att bedriva *signalspaning enligt den inriktning som regeringen, Försvarsmakten och övriga uppdragsgivare anger*.	Försvarets radioanstalt är en central förvaltningsmyndighet med uppgift att bedriva *signalspaning*.

Denna förordning träder i kraft den 1 juli 2006.

1 Inledning

Föreliggande promemoria har utarbetats inom Regeringskansliet (Försvarsdepartementet). Hovrättspresidenten Johan Hirschfeldt, f.d. justitiekanslern Hans Regner och f.d. generaldirektören Rolf Holmquist har varit förordnade att biträda departementet vid utarbetandet av förslagen. Johan Hirschfeldt har varit förordnad under tiden den 12 december 2003 – 31 mars 2004, Hans Regner under tiden den 8 februari – 30 april 2005 och Rolf Holmquist under tiden den 1 juni 2003 – 31 mars 2004.

1.1 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 försvarsunderrättelsemyndigheterna 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 vidarebefordras. 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.

1.2 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.

2 Den svenska säkerhetspolitiska utvecklingen

Syftet med försvarsunderrättelseverksamheten är att ge underlag för beslut till stöd för svensk utrikes-, och säkerhetspolitik och för svensk försvarspolitik. Säkerhetspolitiken är en sammanfattande del av och benämning på de åtgärder som landets regering vidtar inom ramen för utrikes- och försvarspolitiken till skydd mot yttre hot mot landet och för att bevara landets fred och självständighet. Den svenska säkerhetspolitikens mål och inriktning är därmed avgörande för den grundläggande inriktningen av underrättelseverksamheten.

Mot bakgrund av detta bör översyn av lagen och överväganden i övrigt ta sin utgångspunkt i den svenska säkerhetspolitikens mål och inriktning och den aktuella svenska säkerhetspolitiska situationen. I föreliggande kapitel lämnas därför en översiktlig beskrivning av den säkerhetspolitiska utvecklingen efter det kalla krigets slut och av den svenska säkerhetspolitiken i dag. Regeringens syn på det säkerhetspolitiska läget utvecklas i större detalj i propositionen 2004/05:5 Vårt framtida försvar.

2.1 Den svenska säkerhetspolitikens mål och inriktning

Syftet med Sveriges säkerhetspolitik är 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 handlingsfrihet att, såsom enskild nation och i samverkan, kunna utveckla vårt samhälle.

Regeringen, Moderata Samlingspartiet Centerpartiet och Kristdemokraterna enades år 2002 om följande beskrivning av Sveriges säkerhetspolitiska linje (Utrikesdeklarationen 2002):

> Sveriges säkerhetspolitik syftar till att bevara fred och självständighet för vårt land, bidra till stabilitet och säkerhet i vårt närområde, samt stärka internationell fred och säkerhet.
>
> Sverige är militärt alliansfritt. Denna säkerhetspolitiska linje, med möjlighet till neutralitet vid konflikter i vårt närområde, har tjänat oss väl.
>
> För framtiden är det tydligare än någonsin att säkerhet är mer än avsaknad av militära konflikter. Hot mot freden och vår säkerhet kan bäst avvärjas i gemenskap och samarbete med andra länder. På det globala planet är det främsta uttrycket för detta vårt stöd till de Förenta nationerna. Genom vårt medlemskap i den Europeiska unionen deltar vi i en solidarisk gemenskap vars främsta syfte är att förhindra krig på den europeiska kontinenten.
>
> En betryggande försvarsförmåga är en central del av den svenska säkerhetspolitiken. Sverige verkar aktivt för att främja nedrustning och icke-spridning av massförstörelsevapen.

I beskrivningen konstateras bland annat att hot mot freden och vår säkerhet bäst kan avvärjas i gemenskap och samverkan med andra länder. Vårt deltagande i det internationella säkerhetspolitiska samarbetet ger oss också större möjligheter att påverka förhållandena i vår omvärld. Medlemskapet i Europeiska unionen innebär att Sverige deltar aktivt i en politisk allians, som är grundad på gemensamma värden och en solidarisk gemenskap. Unionens medlemsländer har en gemensam utrikes-

och säkerhetspolitik, GUSP. Inom ramen för GUSP bidrar Sverige till unionens civila och militära krishantering.

Sverige är militärt alliansfritt. Innebörden av den militära alliansfriheten är för svensk del att vi inte ingår avtal om bindande ömsesidiga försvarsgarantier. Vi ansvarar således självständigt för försvaret av Sveriges territorium. Den militära alliansfriheten utgör givetvis inget hinder för ett svensk brett och allsidigt deltagande i det internationella säkerhetssamarbetet. Det finns ingen motsättning mellan den militära alliansfriheten och den starka solidariteten mellan EU-länderna. Det är svårt att föreställa sig att Sverige skulle ställa sig neutralt i händelse av ett väpnat angrepp mot ett annat EU-land. Det är lika svårt att föreställa sig att övriga EU-länder inte skulle agera på samma sätt.

Det svenska försvaret är sedan några år inne i en genomgripande omställning. Målet är ett modernt, flexibelt och rörligt insatsförsvar. Under det kalla kriget krävdes ett svenskt territorialförsvar som var starkt i relation till andra stater, för att Sverige inte med automatik skulle dras in i en stormaktskonflikt. Dagens hotbild är betydligt mer mångfacetterad. Försvarsmakten skall kunna möta väpnade angrepp riktade mot vår territoriella integritet, men den skall också förbättra sin förmåga att bidra till internationella fredsfrämjande insatser i samverkan med andra stater och för att kunna möta nya och oväntade hot.

2.2 En ny säkerhetspolitisk situation

2.2.1 Nya säkerhetshot och risker

Omvälvningarna i den internationella miljön under 1990-talet med det kalla krigets slut och ett slut på de tidigare stormaktsmotsättningarna har lett till omfattande förändringar i den säkerhetspolitiska omvärldssituationen. Ett nytt läge har uppstått, bl.a. i Europa och i Sveriges närområde.

Under det kalla kriget var ett storkrig mellan maktblocken i Europa det helt dominerande hotet. Då fokuserades den svenska

säkerhetspolitiken på att undvika att landet skulle dras in i ett sådant krig. Försvaret inriktades i grunden på att möta en invasion av landets territorium. Dagens verklighet ser helt annorlunda ut.

I försvarsbesluten under 1990-talet har framhållits att den internationella politiken och omvärldsutvecklingen i högre grad än tidigare präglas av föränderlighet och svårbedömbarhet. Förhållandena har delvis förklarats vara ett resultat av att den tidigare stormaktskonflikten och det kalla kriget har upphört. Samtidigt har de tidigare stormaktsmotsättningarna inte ersatts av någon annan jämförbar ordning. Det kalla krigets paradoxala kombination av politisk spänning och stabilitet har ersatts av ett förhållandevis rörligt och svårförutsägbart läge. Allmänt sett anses utvecklingen i världen karaktäriseras av ett större antal mer eller mindre inflytelserika aktörer, som sinsemellan är heterogena och långt ifrån jämbördiga. Även om risken för storkrig således har minskat och öppna krig mellan länder har blivit mindre vanliga, kan emellertid faran för även allvarligare och mer utbredda konflikter inte helt avskrivas.

I de nyss nämnda försvarsbesluten bedömer regeringen att ett enskilt militärt väpnat angrepp i alla dess former från en annan stat direkt mot Sverige är osannolikt under överskådlig tid (minst en tioårsperiod). Incidenter kopplade till territoriell integritet kan dock inte uteslutas. Nya säkerhetshot har uppstått. Den nya säkerhetspolitiska situation, som inträtt efter det kalla krigets slut, har medfört att ett bredare spektrum av tänkbara hot, risker och påfrestningar mot samhället måste kunna besvaras. I EU:s säkerhetsstrategi *Ett säkert Europa i en bättre värld* redovisas och sammanfattas de hot och utmaningar som vi står inför. Såsom hot identifieras särskilt terrorism, massförstörelsevapen, regionala konflikter, sönderfallande statsbildningar och organiserad brottslighet.

På olika håll i världen orsakas till exempel väpnade konflikter av såväl politiska som etniska, religiösa, ekonomiska, sociala och miljömässiga förhållanden. Ytterst utgör dessa konflikter ett hot mot den gemensamma säkerheten. Hotbilden består bland annat

av försörjningskriser, ekologiska obalanser, migrationsrörelser, nationalism, etniska och kulturella konflikter samt terrorism. Vidare medför den fördjupade integrationen vad gäller den ekonomiska och tekniska utvecklingen att sårbarheten och risken för störningar i samhället ökat.

Samtidigt bör pekas på att staterna i många avseenden närmat sig varandra genom ett ökat internationellt säkerhetssamarbete, bland annat i form av samverkan i fredsbevarande och humanitära insatser. I dag har Sverige ett mångfacetterat och brett internationellt säkerhetssamarbete, som ger betydligt större möjligheter att påverka förhållandena i omvärlden. Härvid spelar vårt medlemskap i EU en central roll, liksom arbetet inom FN och samarbetet med Nato. Detta har bland annat fört med sig att totalförsvarsresurserna anpassas för att bli bättre lämpade för internationell krishantering. För Sveriges del anses ett omfattande europeiskt och internationellt säkerhetssamarbete viktigt för den globala säkerheten och för att trygga vår egen säkerhet.

Attackerna mot New York och Washington den 11 september 2001 och i Madrid den 11 mars 2004 visar tydligt att hoten mot det öppna samhällets säkerhet idag kan vara andra än de traditionellt militära. Det moderna samhällets sårbarhet kräver därför en helhetssyn på säkerhet och beredskap. Den snabba teknikutvecklingen innebär att vi idag är betydligt mer beroende än någon gång tidigare av teknisk infrastruktur som elförsörjning, transportsystem, telekommunikationer och IT-system för att vårt samhälle ska fungera. Denna infrastruktur är i hög grad internationell. I vårt alltmer globaliserade samhälle är vi också i högre grad än tidigare sårbara för säkerhetshot som terrorism, massförstörelsevapen, narkotikahandel, organiserad brottslighet, miljö- och flyktingkatastrofer.

Den nya sortens hot är i hög grad gränsöverskridande och kan bara förebyggas och bekämpas genom internationellt samarbete. Det är över huvud taget svårt att föreställa sig ett allvarligt hot eller dåd mot en enskild stat som inte drabbar också andra stater genom den ökade ekonomiska, tekniska och politiska integrationen.

Följande exempel kan ges på så kallade nya hot och utmaningar, som skall kunna bemötas inom ramen för totalförsvaret och som kan ställa krav på information från en underrättelsefunktion.

Regionala konflikter orsakar stort lidande och kan dessutom spridas eller få följder för omvärlden i form av stora flyktingströmmar.

Spridning av massförstörelsevapen riskerar idag inte bara att ske till stater utan även till ickestatliga organisationer och terroristgrupper.

Stora flykting- och migrationsrörelser kan, oavsett om de orsakats av ekonomiska, ekologiska, etniska eller religiösa problem, medföra stora påfrestningar i mottagarländer och kan få såväl in- som utrikespolitiska konsekvenser.

Internationell terrorism och kriminalitet utgör idag hot mot både enskilda individer och stater. Detta framstår särskilt tydligt efter terroristattackerna den 11 september 2001 och den 11 mars 2004. Fenomenet internationell terrorism liksom åtgärderna för att bekämpa denna behöver analyseras i en utrikes- och säkerhetspolitisk kontext. En väl utvecklad underrättelseinhämtning och en god krishanteringsförmåga är viktiga komponenter för att förebygga terroristattacker och hantera konsekvenserna av en genomförd attack.

Ekonomiska utmaningar i form av valuta- och räntespekulationer, störningar i utrikeshandeln på grund av brist eller oro på råvarumarknader eller på de finansiella marknaderna eller i handelsavtal kan skapa utrikespolitiska spänningar. En sådan utveckling skulle ställa stora krav på förvarning för snabba, effektiva och samordnade åtgärder från statsmakternas sida.

Den tekniska utvecklingen inom framförallt informationsteknologin samt den framväxande globala kommunikationsstrukturen har framkallat ett beroende som medför att det moderna samhället har blivit avsevärt mer sårbart. De hot som härvidlag har uppstått är mångfacetterade och berör enskilda såväl som organisationer och stater.

2.2.2 Sveriges säkerhetspolitiska läge

Den nya säkerhetspolitiska situationen, målet för och inriktningen av den svenska säkerhetspolitiken samt det vidgade säkerhetsbegreppets konsekvenser för underrättelsetjänsten har behandlats bland annat i 1995 och 1996 års samlade försvarsbeslut (prop. 1995/96:12 och 1996/97:4), i 1999 års så kallade kontrollstationsproposition (prop. 1998/99:74), Försvarsberedningens rapporter Vårt militära försvar – vilja och vägval och Försvar för en ny tid (Ds 2003:8 resp. 2004:30). Frågorna har också behandlats i samband med de årliga statsbudgeterna.

Sveriges säkerhetspolitiska läge under 1990-talet och senare har bekräftats i 2004 års försvarsproposition, som omfattar perioden 2005-2007. Här framhåller regeringen att den internationella säkerhetspolitiska utvecklingen bekräftar och befäster att Sverige säkerhet på ett avgörande sätt har stärkts i och med den ökade europeiska integrationen. Ett militärt väpnat angrepp i alla dess former från annan stat direkt mot Sverige är osannolikt under överskådlig tid (minst en tioårsperiod). Incidenter kopplade till territoriell integritet kan dock inte uteslutas, inte heller att ett militärt hot mot Sveriges frihet och självständighet skulle kunna uppstå i framtiden. Regeringen har tidigare framfört att Sverige även fortsättningsvis behöver upprätthålla en grundläggande försvarsförmåga (se bl.a. prop. 2004/05:5 s. 23 ff.).

Dagens hot och utmaningar kan i många fall bäst mötas genom internationell samverkan. Om konfliktförebyggande åtgärder och krishantering skall få genomslag krävs internationell samordning och samarbete. Även inför asymmetriska och transnationella hot är internationellt samarbete, t.ex. bland säkerhets- och underrättelsetjänster, en förutsättning för framgång. Fenomenet internationell terrorism behöver analyseras i en säkerhetspolitisk kontext liksom svenskt agerande i kampen mot terrorism. Nationella underrättelsetjänster har här en viktig roll att spela. Informationsutbyte och koordinering mellan olika länder och myndigheter, såväl nationellt som internationellt, är avgörande för möjligheten att förebygga och

hantera dylika hot (prop. 2004/05:5 s. 25 f.). Vidare konstateras i propositionen att det är av stor vikt att vårt försvar och krishanteringsförmåga utvecklas för att ge långsiktig handlingsfrihet utifrån framtida behov och hot. Härvid fordras även en adekvat förmåga till tidig förvarning och en till den säkerhetspolitiska situationen anpassad underrättelsefunktion (prop. 2004/05:5 s. 28).

Våren 2004 utvidgades EU och Nato med nya medlemmar, vilket manifesterar en i grunden förändrad och förbättrad säkerhetspolitisk situation i Europa. EU är i sammanhanget unik i sin roll som politisk union, med en roll som global utrikes- och säkerhetspolitisk aktör. EU-länderna strävar efter att fördjupa samarbetet inom säkerhets- och försvarspolitiken, vilket manifesteras genom EU:s säkerhetsstrategi, där medlemsstaterna gemensamt formulerat en säkerhetsrelaterad syn på omvärlden, enats om strategiska målsättningar samt givit en inriktning om hur EU:s utrikes-, säkerhets- och försvarspolitik bör utformas (Ds 2004:30). I säkerhetsstrategin påpekas även behovet av ett förbättrat underrättelsesamarbete mellan medlemsstaterna och med partnerländer.

Utvecklingen av den europeiska säkerhets- och försvarspolitiken innebär nya förutsättningar för svensk säkerhetspolitik. Europeiska unionen är central för Sveriges säkerhet. Med EU:s utvidgning stärks säkerheten i hela Europa. Genom fördjupat samarbete med EU:s nya grannar driver vi ytterligare på denna utveckling. Samtidigt vill Sverige stärka EU:s förmåga att effektivt möta dagens säkerhetspolitiska hot både regionalt och globalt. En stärkt EU-förmåga kommer också Sverige till del. Därför ligger det i Sveriges, liksom i andra medlemsländers, intresse att öka EU:s kapacitet för krishantering.

Överväganden kring vår säkerhet måste utgå från den säkerhetspolitiska situationen där medlemskapet i EU är en central del. Sverige, tillsammans med övriga medlemsländer, har en vilja att solidariskt möta de hot Europa står inför. För att göra detta krävs en utvecklad förmåga och aktivt utnyttjande av tillgängliga instrument. Ett tidigt agerande från EU:s sida för att

förebygga hot och väpnade konflikter bidrar konkret till Europas säkerhet. Med ökad förmåga att gripa in i oroshärdar stärks också EU som aktör och därmed unionens politiska handlingsfrihet.

Försvarsberedningen lyfte i sin rapport Vårt militära försvar – vilja och vägval (Ds 2003:8) fram tre övergripande slutsatser avseende hotet om väpnat angrepp, vårt bidrag till fred och säkerhet i omvärlden och behovet av att minska samhällets sårbarhet.

Det internationella skeendet och utvecklingen av den europeiska säkerhets- och försvarspolitiken föranleder en fördjupad diskussion om den gemensamma hotbilden. Försvarsberedningen kvarstår i sin uppfattning att ett enskilt militärt väpnat angrepp i alla dess former från annan stat direkt mot Sverige är osannolikt under överskådlig tid (minst en tioårsperiod).

Incidenter kopplade till territoriell integritet kan dock inte uteslutas. Viktiga bedömningsgrunder är såväl politiska avsikter som den operativa förmåga som finns hos väpnade styrkor i vårt närområde, den bedömda utvecklingen av dessa samt det förbättrade strategiska läget och det fördjupade säkerhetssamarbetet i närområdet.

I ett långsiktigt perspektiv bedömer Försvarsberedningen att den grundläggande positiva säkerhetspolitiska situationen för Sverige fortsatt kommer att befästas och utvecklas. Försvarsberedningen konstaterar samtidigt att det inte går att utesluta att det i framtiden skulle kunna uppstå ett militärt hot mot Sverige. Att nu ha en klar uppfattning om karaktären av sådana hot är dock inte möjligt mot bakgrund av den snabba internationella, politiska, militärstrategiska och tekniska utvecklingen. Det är av stor vikt att kontinuerligt följa denna utveckling, som grund för successiva beslut om totalförsvarets utformning. I detta perspektiv blir långsiktig säkerhetspolitisk handlingsfrihet fundamental och därför krävs tillgång till kompetens, utvecklingsförmåga och flexibilitet.

Framväxten av eventuella framtida hot mot vår säkerhet måste bedömas också i ett vidare perspektiv än det nationella. Dessa,

ofta gränsöverskridande hot påverkar Sveriges säkerhetspolitiska läge. Dessa hot kan bäst mötas i samverkan med andra. Sambanden mellan denna typ av hot, bland annat terrorism, massförstörelsevapen, organiserad brottslighet, och risken för att de sprids, visar på nödvändigheten av att utnyttja hela bredden av tillgängliga instrument för att förebygga och bekämpa dem.

Omvärldens förändringar ställer hela tiden nya krav. Sverige skall aktivt delta i förbättringen och utvecklingen av det internationella systemet för att möta dagens hot. Genom att stärka vår egen förmåga att delta i internationellt arbete och krishanteringsinsatser stärks internationell fred och säkerhet både för Sverige, för EU som helhet och för vår omvärld. Det är av stor vikt att vårt försvar och vår krishanteringsförmåga utvecklas för att ge långsiktig handlingsfrihet utifrån framtida behov och hot. Härvid fordras även en adekvat förmåga till tidig förvarning och en till den säkerhetspolitiska situationen anpassad underrättelsefunktion.

Konflikter med allvarliga följder i och utanför konfliktområdet kommer att inträffa även i framtiden. Utvecklingen av asymmetriska metoder ökar denna risk. Dessa konflikter kan med ett relativt snabbt förlopp få konsekvenser även för internationell fred och säkerhet och i förlängningen också för EU och därmed Sverige. Genom konfliktförebyggande insatser och konflikthantering i det aktuella området kan spridningsrisken stävjas (se Ds 2003:08 och Ds 2004:30).

De nya icke-militära säkerhetshoten som uppstått i omvärlden påverkar den svenska säkerheten och samhällsutvecklingen. Internationella företeelser som terrorism, spridning av massförstörelsevapen, gränsöverskridande brottslighet och hot mot den tekniska infrastrukturen har gjort det nödvändigt att vidga det svenska säkerhetsbegreppet. I detta sammanhang har betydelsen av samordning mellan civil och militär underrättelseverksamhet ökat, såväl i ett nationellt som internationellt perspektiv. Både civil och militär underrättelseinformation måste beaktas för att det skall föreligga ett fullständigt underlag för beslut och åtgärder i ett vidgat säkerhetspolitiskt perspektiv.

Krav ställs därför på samarbete mellan myndigheterna inom försvarsunderrättelseverksamheten och andra ansvariga myndigheter för att hantera en bredare säkerhetspolitisk bild och för att förse statsmakterna med ett relevant och så fullständigt beslutsunderlag som möjligt.

När det gäller försvarsunderrättelseverksamheten framhåller regeringen i flera sammanhang att den säkerhetspolitiska tyngdpunktsförskjutningen från traditionell militär förvarning och heltäckande operativ samt taktisk förvarning mot strategiska och icke-militära underrättelser bör fortsätta. Det innebär en fortsatt utveckling av försvarsunderrättelsemyndigheternas förmåga att stödja regeringen med underrättelser som är relevanta för utrikes-, försvars- och säkerhetspolitiken. Omvärldsutvecklingen ställer alltså delvis andra krav på underrättelseunderlaget för att på ett relevant sätt bidra till bedömningar och beslut av skeenden. Dessa underrättelsebehov är främst, som nämnts, av civil, icke-militär, karaktär. Därutöver ställer det intensifierade internationella underrättelsesamarbetet, inte minst stödet till EU:s framväxande förmåga inom den gemensamma utrikes- och säkerhetspolitiken (GUSP) och den europeiska säkerhets- och försvarspolitiken (ESFP), nya krav på försvarsunderrättelseverksamheten. I takt med att Sveriges deltagande i internationella insatser ökas i enlighet med 2004-års försvarsbeslut är det också angeläget att ytterligare ansträngningar görs att stödja svensk trupp och annan personal i insatsområdet. Regeringen framhåller särskilt att det är av vikt att förbättra inriktningen, inhämtningsmetoderna och analyserna för att öka relevansen av producerade underrättelser (se t.ex. prop. 2003/04:1 Utgiftsområde 6 s. 66). I det senaste försvarsbeslutet pekade regeringen särskilt på att Sverige vid EU-ledda insatser deltar i hela besluts- och genomförandeprocesserna, vilket i sin tur ställer krav på ett mer omfattande engagemang både politiskt och resursmässigt än som hittills varit fallet vid FN- och Natoledda insatser. Stora krav ställs på att snabbt kunna fatta politiska beslut och på vår nationella förmåga att tillhandahålla resurser på alla nivåer i en insats från det att planeringen inleds tills dess att insatsen avslutas. Kopplingen

mellan underrättelsefunktionen och nationell planering på strategisk nivå samt genomförande av militära insatser måste utvecklas för att motsvara de krav som därmed ställs (prop. 2004/05:5, s. 28).

Regeringen understryker vidare att det är av stor vikt att vårt försvar och vår krishanteringsförmåga utvecklas för att ge långsiktig handlingsfrihet utifrån framtida behov och hot. Härvid fordras även en adekvat förmåga till tidig förvarning och en till den säkerhetspolitiska situationen anpassad underrättelsefunktion (prop. 2004/05:5 s. 28). Försvarsberedningen anförde dessutom att det i detta sammanhang var viktigt att Sverige som ett militärt alliansfritt land har en självständig underrättelseförmåga för att, även under de nya villkor som skildrats ovan, kunna göra egna bedömningar av viktiga säkerhetspolitiska händelser, förhållanden och skeenden. Inte minst det senaste årets internationella debatt om Irak har illustrerat detta (Ds 2004:30 s. 41).

3 Underrättelseverksamhet

3.1 Underrättelseverksamhet

Med underrättelsetjänst avses vanligtvis en verksamhet eller process för att med hemliga 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 underrättelsetjänst främst till att löpande bidra till kunskapsuppbyggnad, kompetenshöjning och förmåga att bekräfta eller vederlägga öppen information 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.

För Sveriges del finns en rad moderna exempel på viktiga frågor där underrättelser haft en konkret betydelse.

Underrättelsetjänst kan i många fall bidra med ett mervärde av information. Alla med Sverige jämförbara länder bedriver underrättelsetjänst. I den kamp som förs mot de nya hoten, till exempel terrorism, spridning av massförstörelsevapen och grov organiserad brottslighet är underrättelser av avgörande betydelse.

Det är särskilt viktigt för ett alliansfritt land att förfoga över en förmåga att självständigt göra bedömningar i säkerhetspolitiska frågor och att kritiskt kunna granska andra aktörers

argumentation och agerande. Förmågan till elektronisk inhämtning, som en del av underrättelseverksamheten, är nödvändig för att Sverige skall kunna skydda sina egna kommunikationssystem. På samma sätt är säkerhetsunderrättelsetjänsten en förutsättning för att kunna skydda det egna landet mot bland annat spionage.

3.1.1 Närmare om lagregleringen

Lagen om försvarsunderrättelseverksamhet innehåller bestämmelser om uppgifter och arbetsformer för försvarsunderrättelseverksamheten.

Beträffande begreppet försvarsunderrättelseverksamhet anförde regeringen att eftersom det i den militära underrättelseverksamheten ingår att medverka i internationellt säkerhetssamarbete och att stärka samhället vid svåra påfrestningar på samhället i fred är det erforderligt med ett begrepp för verksamheten som inte bara täcker underrättelseverksamhet till stöd för det militära försvaret. Regeringen ansåg därför att en lämplig benämning för den beskrivna underrättelseverksamheten var försvarsunderrättelseverksamhet (prop. 1999/2000:25 s. 7).

Försvarsunderrättelseverksamheten 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 (1 § första stycket). Försvarsunderrättelseverksamheten får emellertid inte avse uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete (4 §).

Det ankommer på regeringen att bestämma försvarsunderrättelseverksamhetens inriktning (1 § andra stycket).

Försvarsunderrättelsemyndigheterna skall fullgöra sina uppgifter genom inhämtning, bearbetning och analys av information. Analyser av hotbilder och bedömningar i underrättelsefrågor

skall rapporteras till Regeringskansliet och andra berörda myndigheter (2 §).

I lagen finns bestämmelser om utlandssamarbete i underrättelsefrågor (3 §). Det anges vidare i lagen att det skall finnas en särskild nämnd under regeringen som skall ha insyn i försvarsunderrättelseverksamheten (5 §).

3.1.2 Närmare om försvarsunderrättelsemyndigheternas uppgifter

Försvarsunderrättelseverksamhet

Försvarsunderrättelseverksamhetens syfte 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. Försvarsunderrättelsetjänsten skall tidigt identifiera och redovisa eller ge förvarning om sådana förändringar i omvärldsläget att informationen kan ligga till grund för ett politiskt beslut om totalförsvarets anpassning. Underrättelsetjänsten 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. Underrättelsetjänsten 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 försvarsunderrättelseverksamhetens uppgifter ingår att medverka i det svenska deltagandet i internationellt säkerhetspolitiskt samarbete samt att, enligt regeringens bestämmande, medverka i uppgiften att stärka samhället vid svåra påfrestningar

på samhället i fred. Enligt regeringen kan det i sistnämnda fall röra sig om att medverka med information och analys i fråga om sådant som t.ex. internationell terrorism och gränsöverskridande miljöhot. Ansvarsförhållandena på sådana områden påverkas inte av försvarsunderrättelsetjänstens medverkan. Regeringen tillade att det självfallet är viktigt att försvarsunderrättelsetjänstens 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 (se prop. 1999/2000:25 s. 14 f.).

Arbetsmetoder

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

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.

Försvarsunderrättelseverksamheten skall styras av landets säkerhetspolitiska intressen. Detta innebär naturligtvis att regeringen bestämmer om försvarsunderrättelsetjänstens samarbete i underrättelsefrågor med andra länder och internationella organisationer. 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 visavi utrikesministern (se prop. 1999/2000:25 s. 16).

Förhållandet till polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete

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

Bestämmelsens utformning överensstämmer inte med Underrättelsekommitténs förslag, utan har fått sin slutliga formulering efter att regeringen instämt i de synpunkter som Rikspolisstyrelsen och Säkerhetspolisen lämnat i sina remissyttranden (se prop. 1999/2000:25 s. 17 f.).

Underrättelsekommittén föreslog att det i försvarsunderrättelseverksamhet inte fick utövas verksamhet som krävde polisiära befogenheter. Genom denna formulering ville kommittén erinra om den naturliga konsekvens som följer av lagar och andra föreskrifter, att det är andra samhällsfunktioner än förvarsunderrättelsetjänsten som svarar för den inre nationella säkerheten. Att det i försvarsunderrättelsetjänst inte får utövas verksamhet som inrymmer polisiära befogenheter såsom förundersökningsåtgärder enligt rättegångsbalken och polisiär tvångsmedelsanvändning enligt polislagen, anförde kommittén, följer också av den andra grundprincipen för försvarsunderrättelseverksamhet. (I prop. 1999/2000:25 redogörs för försvarsunderrättelseverksamhetens fyra grundprinciper).

Rikspolisstyrelsen och Säkerhetspolisen invände att förslaget inte överensstämde med andra grundprinciper för försvarsunderrättelseverksamheten, nämligen den att verksamheten inte får vara inriktad på uppgifter som ligger inom ramen för polisens brottsbekämpande och brottsförebyggande arbete. Säkerhetspolisen ifrågasatte om kommitténs förslag innebar nya gränser för underrättelsetjänstens verksamhet, och avstyrkte i den mån förslaget. Regeringen, som instämde i de synpunkter som lämnats av bland annat Rikspolisstyrelsen och

Säkerhetspolisen, ansåg att det uttryckligen i lagen bör framgå att försvarsunderrättelseverksamheten inte får avse uppgifter som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete.

Regeringen framhöll emellertid att regleringen inte syftar till att utgöra något hinder mot att myndigheter som sysslar med försvarsunderrättelseverksamhet, enligt regeringens bestämmande, skall kunna lämna andra myndigheter biträde. Den tekniska utrustning som kan finnas hos en myndighet som är verksam med till exempel signalspaning inom försvarsunderrättelseverksamheten skall med stöd av regeringens uppdrag 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 talar också att teknisk utrustning som det allmänna anskaffat används på ett rationellt sätt. Enligt regeringen skall det även finnas utrymme för att ge sådant stöd i andra avseenden. Regeringen tillade vidare att myndigheter som ägnar sig åt försvarsunderrättelseverksamhet, i enlighet med regeringens bestämmande, skall kunna syssla med uppdragsverksamhet för annan myndighets räkning.

Insyn

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.

3.1.3 Särskilt om underrättelseverksamhet avseende yttre icke-militära hot

Som redogjorts för i kap. 2 har den nya säkerhetspolitiska situationen medfört att man inom totalförsvarets ram i fortsättningen skall utgå från en vidgad säkerhetssyn för att kunna möta ett bredare spektrum av hot, risker och påfrestningar. Det kan till exempel röra sig om hot och utmaningar i form av bland annat ekonomiska kriser, försörjningskriser, ekologiska obalanser, nationalism (extremism), etniska och kulturella konflikter, gränsöverskridande brottslighet och terrorism, samt flyktingeller migrationsrörelser. Även om dessa nya hot och utmaningar har ett icke-militärt ursprung, kan de ändå vara av så allvarlig art att de utvecklas till att beröra hela samhällsstrukturen. Härvid kan militär förmåga komma att erfordras för att skydda samhället och nationella intressen.

Underrättelsekommittén konstaterade att det vidgade säkerhetsbegreppet väckte frågor om och i vad mån det ankom på den militära underrättelsetjänsten att ta sig an sådana icke-militärt anknutna säkerhetsproblem i form av nya hot. Enligt kommittén borde ansvaret för hanteringen av de nya hoten såväl i fredstid som i krig enligt gängse princip ankomma på den myndighet som har ansvaret i fredstid och att det först i den mån en sådan myndighet saknar egen kapacitet för underrättelseinhämtning det 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 avse bland annat att enligt vad regeringen bestämmer, medverka i uppgiften att stärka samhället vid svåra påfrestningar i fred. Enligt Underrättelsekommittén skulle den militära underrättelsetjänsten bidra med främst en militär aspekt på den vidgade säkerhetspolitiska hotbilden. Behovet av att från den militära underrättelsetjänsten därutöver erhålla ett självständigt på eget initiativ utarbetat bidrag till ett mer allsidigt, icke-militärt präglat underlag såsom

stöd för ”svensk utrikes- och säkerhetspolitik” ifrågasattes. 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 sammanhanget kan nämnas att Säkerhetspolisen i sitt remissyttrande över Underrättelsekommitténs betänkande framförde vissa betänkligheter när det gäller de nya hoten, särskilt avseende ansvaret för bekämpning av terrorism och samordningsansvaret för icke-spridningsfrågor. Enligt Säkerhetspolisen framstod som oklart om kommitténs förslag innebar att underrättelsetjänsten mot bakgrund av det vidgade säkerhetsbegreppet skulle bygga upp egna resurser inom området. Säkerhetspolisen erinrade också om vad regeringen uttalat i sin skrivelse till riksdagen om beredskapen mot svåra påfrestningar på samhället i fred (skr. 1998/99:33 s. 18). Regeringen underströk där att ett samarbete mellan Försvarsmakten och ansvarig civil myndighet förutsätter att den civila myndigheten uttryckligen anger att ett behov av ett sådant stöd föreligger.

Regeringens förslag till lag om försvarsunderrättelseverksamhet innehöll inte någon särskild skrivning såvitt avsåg yttre icke-militära hot mot landet. Frågan om försvarsunderrättelseverksamheten skulle omfatta sådana hot berördes under utskottsbehandlingen i riksdagen (bet. 1999/2000:FöU3 s. 10 f.).

3.2 Vissa särskilda underrättelsemetoder

Grunden för den nationella underrättelseförmågan beror på hur effektiv inhämtningen med särskilda metoder är. Utan en effektiv särskild inhämtningsförmåga kan den efterföljande bearbetningen och grundanalysen endast bygga på öppen insamlad information, till exempel UD- och försvarsattachérapportering, med de begränsningar detta innebär. 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 ger det kompletterande mervärdet.

3.2.1 Personbaserad inhämtning

En viktig metod för underrättelseinhämtning är personbaserad inhämtning med särskilda metoder. Sådan inhämtning utförs av Kontoret för särskild inhämtning (KSI), vilket är ett organ inom Militära underrättelse- och säkerhetstjänsten (MUST) som enbart arbetar med inhämtning av underrättelser mot utländska förhållanden. På grundval av inhämtat material upprättas rapporter, som överlämnas till Militära underrättelse- och säkerhetstjänsten, där dessa sedan bearbetas tillsammans med annat underrättelsematerial. Personbaserad inhämtning utförs även åt andra myndigheter, t.ex. de 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 dessutom försvåra eller omöjliggöra fortsatt underrättelseinhämtning.

3.2.2 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 verksamheten 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. Såsom reglerna i lagen om försvarsunderrättelseverksamhet är formulerade faller viss del av Försvarets radioanstalts verksamhet således utanför försvarsunderrättelseverksamheten.

Enligt 2 § i Försvarets radioanstalts instruktion anges att Försvarets radioanstalt 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 och
- utföra matematiska bedömningar av kryptosystem för totalförsvaret.

Vidare skall Försvarets radioanstalt enligt 3 a § ha hög teknisk kompetens inom informationssäkerhetsområdet. Försvarets radioanstalt får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig 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.

I nämnda bestämmelse anges också att Försvarets radioanstalt skall samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

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

En övergripande uppgift för Försvarets radioanstalt, såsom den anges i lagstiftning och regleringsbrev, 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.

3.2.2.1 Signalspaning

Försvarets radioanstalts signalspaning syftar, som redan framgått, bland annat till att ge underlag för bedömning i fråga om sådan förvarning om förhållanden i omvärlden, som kan påverka landet i säkerhetspolitiska och militära hänseenden. Signalspaningen bedrivs som kommunikationssignalspaning (KOS) mot utländsk radiokommunikation och som så kallad teknisk signalspaning (TES) mot vissa sändningar av annan karaktär. De utförs från stationer, som med hänsyn till radiovågornas utbredning är placerade på lämpliga platser i Sverige. Spaning bedrivs även från flygburna stationer och från fartyg.

KOS riktas mot såväl civila som militära eterburna signaler över kommunikationssatelliter och jordbundna system (t.ex. radiolänkar). Sändande källor lägesbestäms med hjälp av pejlanläggningar. I förlängningen kan intentioner hos olika internationella aktörer kartläggas såväl som en eventuell militär motståndares organisation, stridsindelning, taktik och beredskap med mera. I en allt större utsträckning har det också vid signalspaningen utvecklats en förmåga att följa de ”nya hoten” såsom terrorism, gränsöverskridande organiserad brottslighet med mera.

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 bland annat 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 egen offensiv så kallad

telekrigföring. Utvecklingen inom området för telekrigföring med elektroniska stridsmedel utgör ett allt större hot, eftersom sådana stridsmedel helt kan såväl förstöra vitala civila informations- och kommunikationssystem som slå ut påkostade militära lednings- och vapensystem. Utvecklingen ställer ökande krav på signalkunskap hos Försvarets radioanstalt. Myndigheten måste bland annat kunna förse Försvarsmakten med aktuella så kallade signalreferensbibliotek, som kan utnyttjas i varnar- och motmedelssystem bl.a. på örlogsfartyg och i militära flygplan. Genom att avlyssna en signal skapas möjligheter att följa främmande stridskrafters rörelser och att identifiera dessa. Genom TES kan en motståndares vapensystem avlyssnas och ge underlag för att bedöma dessas prestanda.

Inhämtade signaler i både KOS- och TES-funktionen bearbetas, analyseras och ställs samman till underrättelserapporter som sänds till Försvarets radioanstalts uppdragsgivare. Inhämtning sker genom registrering (avlyssning) av utvalda signaler. Den sändande parten söker ofta skydda innehållet i kommunikationen genom ett utvecklat signalskydd, bland annat i form av kryptering. Bearbetningen inom ramen för KOS-verksamheten syftar till att forcera signalskyddet och frilägga eller beskriva sändningarnas innehåll. Teknisk analys, trafikbearbetning och kryptoforcering är verktyg för detta. En fortsatt analys ger de faktiska underrättelserna.

I Försvarets radioanstalts uppgift att bedriva signalspaningsverksamhet till stöd för utrikes-, försvars- och säkerhetspolitiken ingår att ge stöd åt Försvarsmakten och att medverka i det svenska deltagandet i internationellt säkerhetssamarbete. Försvarets radioanstalt har i sistnämnda hänseende att på uppdrag av Försvarsmakten stödja svenska förband i internationell tjänst med signalspaningsutrustning och metodik som behövs bland annat för att förvarna om hot mot förbanden. Försvarets radioanstalt skall också lämna stöd i form av underrättelser till svenska förband som är engagerade i internationell tjänst.

Stödet till Försvarsmakten innebär bland annat att på uppdrag av Försvarsmakten stödja förbandsproduktion och därvid utveckla och anskaffa signalspaningssystem samt att utveckla metodik och att fackutbilda personal. En väsentlig och övergripande uppgift är att på uppdrag stödja Försvarsmakten med underrättelseinformation när det gäller Försvarsmaktens huvuduppgift att försvara landet mot väpnat angrepp och hävda landets territoriella suveränitet.

Försvarets radioanstalt har vidare att på uppdrag av olika myndigheter medverka med underrättelser i uppgiften att stärka samhället vid svåra påfrestningar i fred. Försvarets radioanstalt har enligt sin instruktion i övrigt att bedriva signalspaning i enlighet med vad de inriktande myndigheterna anger.

Enligt instruktionen skall Försvarets radioanstalt ha hög teknisk kompetens inom informationssäkerhetsområdet. Myndigheten skall på begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känsliga ur sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

3.2.2.2 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, som utgör målet för Försvarets radioanstalts kommunikationsspaning – så som telefoni, dataöverföring med mera – har dock 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 avgörande begränsning för att myndigheten nu och i framtiden skall kunna bedriva en ändamålsenlig inhämtningsverksamhet. Däri ingår bland annat att bistå till att

upprätthålla ett trovärdigt signalskydd och framgent för att kunna upprätthålla skyddet mot kvalificerade IT-relaterade hot.

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

Dessa frågor berörs vidare i kap. 5.

3.3 Underrättelseverksamhet internationellt

3.3.1 Internationellt samarbete inom underrättelseverksamheten

Det internationella samarbetet när det gäller underrättelseverksamhet på det säkerhetspolitiska området är av stor betydelse för enskilda länder. I dagens föränderliga och svårbedömda 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, bland annat internationell terrorism och gränsöverskridande brottslighet.

I den senaste budgetpropositionen framhåller regeringen att det intensifierade internationella underrättelsesamarbetet ställer nya krav på underrättelseverksamheten. I sammanhanget nämns särskilt betydelsen av stödet till EU:s framväxande förmåga inom ramen för den gemensamma utrikes- och säkerhetspolitiken (GUSP) och den europeiska säkerhets- och försvarspolitiken (ESFP). Samarbetet med andra staters underrättelsetjänster understryks också i samband med Sveriges allt större deltagande i fredsfrämjande och andra internationella insatser (jfr prop. 2003/04:1 Utgiftsområde 6 s. 66).

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 att lagreglera underrättelseverksamheten var enligt Underrättelsekommittén att detta skulle kunna bidra till att den viktiga och ofta uppmärksammade verksamheten kom att åtnjuta ett högt förtroende hos medborgarna. Lagen om försvars-underrättelseverksamhet anger således ramarna för verksamheten och ger en viss anvisning om underrättelsetjänstens uppbyggnad och funktion. Även om det med hänsyn till syftet med verksamheten aldrig är möjligt att ge en helt komplett och rättvisande bild av verksamheten hos landets underrättelse-organisation kan dagens lagstiftning på så sätt sägas öka allmänhetens insyn i och förståelse för verksamheten.

Sverige skiljer sig emellertid alltjämt från många andra länder där man valt att ha en än mer öppen redovisning av underrättelseverksamheten. Det förekommer att lagstiftningen tydligt och detaljerat anger vilka uppgifter och befogenheter de olika underrättelseorganen har i sin verksamhet samt hur styrning och kontroll utformats.

Med hänsyn härtill förefaller det naturligt att som bakgrund till de kommande övervägandena redovisa hur underrättelse-verksamheten till stöd för utrikes-, säkerhets- och försvarspolitik bedrivs i vissa andra jämförbara länder. Av särskilt intresse är då i första hand styrning och kontroll samt hur underrättelse-verksamheten har lagreglerats. Här följer således en översiktlig redovisning av förhållandena i dessa avseenden hos några andra länder samt en kortfattad beskrivning av underrättelsesamarbetet inom EU.

3.3.2 Underrättelseverksamhet i några andra länder

3.3.2.1 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). Båda tjänsterna styrs och kontrolleras på ett samordnat sätt och skall enligt lagen samarbeta med varandra.

Lagen är väsentligt utvidgad i förhållande till tidigare lagreglering. Detta har bland annat 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. I och med lagen har vidare ett nytt tillsynsorgan inrättats för att förstärka kontrollen av verksamheterna och behandlingen av klagomål mot dessa.

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 så kallad 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 nämnda bestämmelser har AIVD och MIVD befogenhet att under vissa villkor utnyttja ett antal olika arbetsmetoder. Dessa metoder innefattar allt i 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 härvid 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.

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

3.3.2.2 Schweiz

Sedan år 1991 är underrättelsetjänsten och den militära säkerhetstjänsten i Schweiz delad. Underrättelsetjänsten är knuten till försvarsmakten och försvarsdepartementet, medan den militära säkerhetstjänsten 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 bland annat 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 artikel 1 i Nach-

richtendienstverordnung omfattar underrättelsetjänsten den strategiska underrättelsetjänsten (SND), den militära underrättelsetjänsten (MND) och flygvapenunderrättelsetjänsten (LWND).

Den strategiska underrättelsetjänsten svarar för de erforderliga 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. Därvid ger försvarsministern även riktlinjer för den fortsatta verksamheten.

Kontroll

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

3.3.2.3 Storbritannien

Det centrala brittiska underrättelseväsendet består dels av den militära underrättelsetjänsten, the Defence Intelligence Staff (DIS), dels av de tre civila underrättelse- och säkerhetstjänsterna, Secret Intelligence Service (SIS), Government Communications Headquarters (GCHQ) och Security Service (BSS). De tre sistnämnda tjänsterna - Intelligence and Security Agencies, brukar kort benämnas the Agencies (se National Intelligence Machinery, Crown copyright 2000).

Teknisk och personbaserad inhämtning

SIS, även kallad MI6, 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, the Intelligence Services Act 1994. Lagen innehåller också regler om bl.a. tillsyn och kontroll över SIS och GCHQ samt även över BSS.

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

SIS:s inhämtning av underrättelser sker främst genom personbaserad inhämtning (HUMINT) men även genom tekniska förfaranden. GCHQ:s inhämtning sker genom signalspaning (SIGINT), mot bland annat 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 finansministeriet samt BSS och andra myndigheter är mottagare av information från SIS och GCHQ. 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, the Ministerial Committee on the Intelligence Services. Kommittén består av premiärministern såsom ordförande och av bland andra utrikes-,

försvars-, inrikes- och finansministrarna. Kommittén bevakar mera övergripande de policyfrågor som berör tjänsterna. Ministrarna biträds i tillsynen och kontrollen av en statssekreterargrupp, the Permanent Secretaries' Committee on the Intelligence Services.

År 1994 inrättades en parlamentarisk underrättelsenämnd, the 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 avger en årlig rapport till premiärministern som även presenteras i öppna delar för parlamentet. Nämnden lämnar även under året på ad hoc-basis rapporter 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 från parlamentets sida. Kontrollen och granskningen av DIS sker således genom the Select Committee for Defence.

De tre underrättelse- och säkerhetstjänsterna är även underkastade tillsyn genom särskilda av premiärministern utsedda tjänstemän, the Security Service Commissioner, the Intelligence Service Commissioner och the Interception Commissioner. De två förstnämnda funktionerna upprätthålls av en hög jurist. Denne 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 en motsvarande funktion med avseende på givna tillstånd för underrättelse- och säkerhetstjänsterna att ta del av post- och telekommunikation.

3.3.2.4 Tyskland

Det centrala tyska underrättelseväsendet består dels av den civila underrättelsetjänsten Bundesnachrichtendienst (BND), dels av två militära underrättelsetjänster i form av en avdelning inom försvarsstaben (Fü SII), som ingår i försvarsdepartementet, och en särskild central myndighet under samma departement, Amt für Nachrichtenwesen der Bundeswehr (ANBw). Det centrala säkerhetsväsendet består dels av den civila inrikes säkerhetstjänsten Bundesamt für Verfassungsschutz (BfV), dels av den militära säkerhetstjänsten Militärischer Abschirmdienst (MAD).

Civil underrättelseverksamhet

BND är en fristående myndighet, som lyder under den tyska statsrådsberedningen, Bundeskanzleramt. Den legala basen för BND:s verksamhet är reglerad i den tyska grundlagen. Därutöver är verksamheten reglerad genom särskild lagstiftning, Gesetz über den Bundesnachrichtendienst – BNDG.

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. Regler finns vidare, 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 så kallad överskottsinformation samt regler om kontroll av information och om skydd för BND:s personal, utrustning, källor med mera. Det ges även regler om gränsdragningen mellan underrättelsetjänstens och polisens och säkerhetstjänstens uppgifter. BND har inte någon exekutiv befogenhet.

BND:s uppgifter är att bedriva underrättelseverksamhet med avseende på utrikespolitiska och utländska militära och ekonomiska förhållanden. BND skall i övrigt utföra underrättelseuppdrag utomlands i enlighet med anvisningar från förbundskanslern och förbundsregeringen samt bevaka utländsk underrättelseverksamhet i Tyskland. BND skall även ta emot underrättelseuppdrag från olika departement, som rör omvärldsbevakning bl.a. med avseende på 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, såsom ”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 nyssnämnda tre underrättelse- och säkerhetstjänsterna är förhållandevis omfattande. Kontrollen är lagreglerad och utövas i första hand av die Parlamentarische Kontrollkommission (PKK). PKK:s kontroll omfattar dock inte den militära verksamheten och den är inte heller en legalitetskontroll utan en politisk kontroll. Kontrollen innefattar tillgång till arkiv och förhör med personalen vid underrättelse- och säkerhetstjänsterna. Det sistnämnda medför också möjlighet för personalen att ta upp frågor med PKK om verksamhetens utövande. Kontrollen innefattar även förhör med ansvariga ministrar och med

koordinatorn. PKK granskar också förslagen till budget för underrättelse- och säkerhetstjänsterna.

Underrättelse- och säkerhetstjänsterna kan även underkastas sedvanlig kontroll av olika parlamentsutskott. PKK ges emellertid särskilda möjligheter till kontroll i frågor, som är underkastad speciell sekretess. En särskild parlamentarisk kontroll utövas med anledning av de tillstånd, som skall ges för underrättelse- och säkerhetstjänsterna om de önskar ta del av post- och telekommunikation. Sådana tillstånd kan ges för att avvärja hot mot landets säkerhet men också bland annat för att inhämta information om terrorism, om illegal handel med vapen och teknologi och om ”penningtvätt”.

3.3.3 Underrättelsesamarbetet inom EU

Utvecklandet av den gemensamma utrikes- och säkerhetspolitiken (GUSP) och den europeiska säkerhets- och försvarspolitiken (ESFP) har lett fram till ett behov av vissa analys- och underrättelsefunktioner på EU-nivå. Även EU:s fredsfrämjande och humanitära insatser har visat på ett underrättelsebehov. Det är naturligtvis av största vikt att EU kan göra en korrekt hotbildsanalys för till exempel ett område dit man kan komma att skicka civil eller militär personal.

Underrättelseverksamheten inom EU är fortfarande i ett uppbyggnadsskede, och det finns till exempel alltjämt utrymme för att stärka informations- och underrättelseinhämtning samt att utveckla styrning, samverkan och kontroll, särskilt i jämförelse med hur verksamheten vanligen är organiserad på det nationella planet inom de olika medlemsstaterna. Vissa funktioner med underrättelseuppdrag har dock inrättats.

Inom EU:s militära stab har upprättats en underrättelsefunktion (intelligence division). Detta är en formell rådsfunktion i vilken alla medlemsstater deltar. Funktionen 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 om inrättandet av en enhet för politisk planering och tidig förvarning, sägs att medlemsstaterna och kommissionen skall understödja den politiska planeringen genom att i största möjliga utsträckning tillhandahålla relevanta upplysningar, inbegripet förtroliga upplysningar.

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.

Regeringen har i regleringsbrev för budgetåret 2005 avseende de myndigheter som bedriver försvarsunderrättelseverksamhet, uttalat att dessa myndigheter inom ramen för EU:s gemensamma utrikes- och säkerhetspolitik och bidrag till EU:s krishanteringsförmåga, skall bidra till en stärkt underrättelsefunktion.

Regeringen har även i den senaste budgetpropositionen understrukit att försvarsunderrättelseverksamheten bör vidareutveckla förmågan att bidra till det internationella underrättelsesamarbetet, särskilt såvitt avser det stöd som kan lämnas till EU, varmed avses främst EU:s framväxande förmåga inom ramen för GUSP och ESFP (se prop. 2003/04:1 Utgiftsområde 6 s. 65 f.).
En särskild uppgift inom ramen för stärkandet av EU:s krishanteringsförmåga gäller utvecklingen av bidrag till en gemensam europeisk förmåga på strategisk nivå inom underrättelseverksamheten och ett stärkt europeiskt underrättelsesamarbete. Till detta syfte har Sverige, som en bland flera medlemsstater, bland annat ställt en svensk tjänsteman med gedigen erfarenhet från underrättelseverksamhet och säkerhetstjänst till lägescentralens förfogande. Skälet för detta är att lägescentralen bedöms få en central roll för informations- och underrättelseutbyte för GUSP och konfliktförebyggande åtgärder samt att Sverige vill kunna bidra till att skapa en stärkt och effektivare gemensam utrikes- och säkerhetspolitik.

4 Anpassning av försvarsunderrättelseverksamheten

4.1 Behovet av en förändrad försvarsunderrättelseverksamhet

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, den samhälleliga kontrollen samt viss anpassning av mandatet för verksamheten.

Den svenska försvarsunderrättelseverksamheten utvecklades efter det 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. Trots att något invasionshot inte föreligger, eller kan skönjas på mindre än tio års sikt, kan risken för väpnade konflikter, incidenter och kränkningar av Sveriges territoriella integritet inte uteslutas. Att bevaka den militära utvecklingen i vårt närområde förblir därför en viktig uppgift för den svenska försvarsunderrättelsetjänsten.

En annan uppgift för försvarsunderrättelseverksamheten är att förse regeringen och Regeringskansliet med underlag för beslut i utrikes-, försvars- och säkerhetspolitiska frågor. Den säkerhetspolitiska utvecklingen under det senaste decenniet, som har redovisats i kapitel 2, 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;

- terrorism;
- spridning av massförstörelsevapen;
- internationell kriminalitet som t.ex. smuggling av vapen, droger eller människor;
- flykting- och migrationsrörelser, orsakade t.ex. av 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 som kan få säkerhetspolitiska konsekvenser.

Den säkerhetspolitiska utvecklingen har inneburit att Regeringskansliet blivit en allt större och viktigare konsument av underrättelser, medan Försvarsmaktens relativa andel har minskat. Därtill kommer växande underrättelsebehov till stöd för verksamheten inom Säkerhetspolisen, Tullverket och

kriminalunderrättelsetjänsten, samt till 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. Ett förändringsarbete pågår för att stärka underrättelsetjänsternas kapacitet och relevans.

En adekvat underrättelsetjänst mot dagens transnationella säkerhetspolitiska hot förutsätter 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.

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

- Mandatet för försvarsunderrättelseverksamhet ändras från ”yttre militära hot” till ”yttre hot” (avsnitt 4.3).
- Gränsdragning mellan polisiär verksamhet och försvarsunderrättelsetjänst förtydligas med anledning av förslag från 11 september-utredningen och remissinstanser (avsnitt 4.3).
- Tydligare reglering av inriktning, rapportering av underrättelser och inhämtningen med särskilda metoder (avsnitt 4.4).
- Införande av ett uttryckligt lagstöd för signalspaningen i syfte att anpassa verksamheten till den tekniska utvecklingen (kapitel 5).
- En förstärkning av samhällets funktioner för inriktning och kontroll av underrättelseverksamheten (kapitel 6).

4.2 Lagreglering av försvarsunderrättelseverksamheten

Underrättelsekommittén (SOU 1999:37, s. 204 f.) konstaterar att regeringsformen inte uppställer något formellt krav på lagreglering av underrättelseverksamhet som avser landets yttre säkerhet och dess säkerhetspolitik. Detta krävs däremot vad avser fri- och rättighetsbegränsande åtgärder, regler som gäller åligganden för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden.

Kommittén påpekar att staten enligt Europakonventionen har en skyldighet att garantera att konventionens fri- och rättigheter upprätthålls i lagstiftning, rättstillämpning och annan form av maktutövning, Konventionen medger dock inskränkningar, t.ex. i fråga om vad som ”i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet”.

I förarbetena till lagen (2000:130) om försvarsunderrättelseverksamhet anförde regeringen att en lagreglering 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.

Eftersom de förändringar som föreslås i denna promemoria vad gäller försvarsunderrättelseverksamhet, tar sikte på utländska förhållanden är de nämnda övervägandena tillämpliga också i detta sammanhang. Även om särskilda lagregler således inte behövs för stora delar av underrättelseverksamheten ligger det även här ett värde i att riksdagen tar ställning till bestämmelserna.

4.3 Gränsdragning mellan yttre och inre hot, mellan civilt och militärt samt mellan underrättelse- och polisiär verksamhet

4.3.1 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 menar att uttrycket ”kartlägga yttre militära hot” i lagen om försvarsunderrättelseverksamhet inte kan anses innefatta icke-militär terrorism. Utredningen föreslår därför att uttrycket ändras till ”yttre väpnade hot mot landet”.

Utredningen pekar 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 föreslår därför ett tillägg till 4 § i lagen om försvarsunderrättelseverksamhet med innebörd att den angivna gränsen mellan polisiär och underrättelseverksamhet (se ovan) inte skall gälla för försvarsunderrättelseverksamhet som ”bedrivs utomlands eller med inriktning på utländska förhållanden”.

I sitt remissvar på utredningens betänkande pekar Rikspolisstyrelsen på att förslaget kan leda till att gränsen luckras upp mellan ”civila och militära myndigheters roll i samhället”. Det finns ingenting som hindrar samarbete mellan Försvarsmakten och Säkerhetspolisen, anser styrelsen, och avstyrker utredningens förslag till tillägg till 4 §. Försvarsmakten skall inte bearbeta och analysera underrättelseinformation som har betydelse i polisens brottsbekämpande arbete. Sådan information skall omgående överlämnas till behörig polismyndighet, anser Rikspolisstyrelsen.

Säkerhetspolisen påpekar det olämpliga i att inom Försvarsmakten bygga upp en med Säkerhetspolisen parallell

kompetens för inhämtning, bearbetning och analys, och avstyrker också förslaget till ändring av 4 §.

Även Försvarsmakten avstyrker den föreslagna ändringen av 4 §. Regeringen bör på annat sätt än genom lagstiftning klara ut vilka säkerhetspolitiska aspekter som terrorism har, och hur underrättelsebehovet skall tillgodoses. Försvarsmakten understryker 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 av remissinstanserna redovisar tvekan eller avstyrker utredningens förslag om att ge Försvarsmakten underrättelseuppgifter i terroristbekämpningen. Däremot betonar många remissinstanser vikten av nära samarbete och ett effektivt utbyte av information mellan underrättelse- och säkerhetsorganisationerna. Bland remissinstanserna finns 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 varnar för oklarheter i ansvars- och befogenhetsfrågor mellan de myndigheter som bedriver försvarsunderrättelseverksamhet och Säkerhetspolisen.

4.3.2 Förslag till gränsdragningar

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.

Försvarsunderrättelseverksamheten får inte innefatta åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande uppgifter enligt lagar och föreskrifter. Detta gäller dock inte när verksamheten, utan att avse fysisk person, bedrivs för kartläggning av förhållanden utomlands som innebär yttre hot.

Det finns ingen anledning att frångå den sedan länge rådande huvudprincipen, nämligen att yttre militära hot skall hanteras av Försvarsmakten, medan terrorism och annan gränsöverskridande brottslighet är kriminella handlingar, som det ankommer på myndigheterna inom rättsväsendet och andra organ att förebygga och bekämpa.

Denna princip löser emellertid inte gränsdragningsfrågor som uppkommer när det gäller att tillgodose behovet av underrättelser som behövs mot bakgrund av den säkerhetspolitiska utvecklingen.

Yttre hot och utländska förhållanden

Den första gränsdragningsfrågan gäller vilken typ av hot som försvarsunderrättelseverksamheten skall ha mandat att ägna sig åt. Idag föreskriver 1 § i lagen om försvarsunderrättelseverksamhet att det skall vara fråga om ”yttre militära hot”. Detta begrepp är alltför snävt eftersom en betydande del av den moderna hotbilden består av icke-militära hot. 11 september-

utredningen föreslår att uttrycket byts ut mot ”yttre väpnat hot” som en markering av att även terrorism skall omfattas. Den formuleringen täcker emellertid inte 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 teknisk kompetens, som måste tas till vara. Det är dessutom angeläget att försvarsunderrättelseverksamhetens unika särskilda metoder kan nyttjas mot hela den vidgade säkerhetspolitiska hotbilden till nytta för en bredare krets av mottagare.

Med tanke på den komplexa hotbilden, med betydande inslag av icke-militära och icke-väpnade hot, bör verksamheten avse ”yttre hot”, oavsett deras karaktär och ursprung. Därmed omfattas hela den säkerhetspolitiska hotbilden.

Försvarsunderrättelseverksamheten bör vidare förbli inriktad uteslutande på utländska förhållanden, dvs. verksamheter eller företeelser som har sin utgångspunkt i utlandet. Det rör sig således inte om verksamhet som är av inhemsk karaktär. Det innebär att försvarsunderrättelseverksamheten skall inhämta, bearbeta och delge sådan information om företeelser och förhållanden i andra länder som bl.a. ger svenska säkerhetspolitiska beslutsfattare ett förbättrat underlag för beslut och bedömningar i utrikes-, säkerhets- och försvarspolitiska frågor eller att skydda svensk personal som deltar i internationella insatser.

Gränsdragningen mellan försvarsunderrättelseverksamhet och polisiär verksamhet

Den andra frågan gäller gränsen mellan försvarsunderrättelseverksamhet och polisiär verksamhet. 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. Det bör t.ex. noteras att de myndigheter som omfattas av lag (2000:130) om försvarsunderrättelseverksamhet under det senaste decenniet kommit att ge ett ökat stöd till svenska polisiära myndigheter.

Även om försvarsunderrättelseverksamheten uteslutande skall avse utländska förhållanden har den sin fysiska bas inom landet. Polisiär verksamhet är däremot inriktad på inhemska förhållanden men en ökande del av den underrättelseinformation som polisen inhämtar och analyserar avser utländska förhållanden. Det finns därför anledning att vid gränsdragningen i första hand beakta verksamhetens ändamål. Av betydelse är härvid att försvarsunderrättelseverksamheten i första hand är inriktad på att ge sådan strategisk information som Regeringskansliet och andra myndigheter behöver för planering, beslut och andra åtgärder.

Allvarliga yttre hot måste bli föremål för en aktiv underrättelseverksamhet och får inte riskera att falla mellan stolarna. Som 11 september-utredningen påpekar 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. Ytterligare ett förhållande som bör kunna minska risken för oklarheter mellan försvarsunderrättelseverksamheten och polisiär verksamhet är att försvarsunderrättelseverksamheten nu mer skall fokusera på att rapportera underrättelser och inte utföra övergripande analyser (se avsnitt 4.4 *Rapportering av underrättelser*). Det nyligen inrättade 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.

Försvarsunderrättelseverksamheten bör inte heller i fortsättningen avse åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete enligt lagar eller andra föreskrifter. Självklart är exempelvis att det i försvarsunderrättelseverksamheten inte skall bedrivas verksamhet som inrymmer straffprocessuella tvångsmedel eller polisiära befogenheter i övrigt. Inte heller inhämtning i brottsförebyggande syfte av information om inhemska förhållanden bör ingå i försvarsunderrättelseverksamheten.

I 4 § lagen om försvarsunderrättelseverksamhet regleras 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 varit tämligen klar. Vid ett utvidgat mandat för försvarsunderrättelseverksamheten kan dock avgränsningen vålla problem. Det framstår exempelvis som osäkert om och i vilken utsträckning försvarsunderrättelseverksamheten kan avse 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. Ett nytt och utvidgat mandat för försvarsunderrättelseverksamheten kan därför komma i konflikt med den begränsning som följer av 4 § i dess nuvarande lydelse. 4 § lagen om försvarsunderrättelseverksamhet behöver alltså förtydligas så att terrorism och andra yttre hot i form av internationell kriminalitet inte utesluts från tillämpningsområdet för försvarsunderrättelseverksamheten.

I enlighet med det sagda bör det i paragrafen anges att försvarsunderrättelseverksamheten inte får innefatta åtgärder ”som ligger inom ramen för polisens och andra myndigheters brottsförebyggande och brottsbekämpande uppgifter enligt lagar och andra föreskrifter”. Det bör vidare anges att denna inskränkning inte gäller när försvarsunderrättelseverksamheten, utan att avse fysisk person, bedrivs för kartläggning av förhållanden utomlands som innebär yttre hot. Genom en sådan reglering uppnås en rimlig avvägning mellan dels intresset av att brottsförebyggande och brottsbekämpande arbetsuppgifter förbehålls polisen och andra berörda myndigheter, dels intresset av att försvarsunderrättelseverksamheten ändå kan inriktas på yttre hot i form av kriminalitet.

Det nu framlagda förslaget rörande gränsdragningen mellan polisiär verksamhet och försvarsunderrättelsetjänst, 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 som omfattas av den vidgade säkerhetspolitiska hotbilden och andra företeelser som innebär svåra påfrestningar för samhället. Utifrån detta synsätt bör försvarsunderrättelseverksamheten ses som samverkande serviceorgan för att tillgodose behov hos Regeringskansliet som t.ex. Försvarsmakten, Rikspolisstyrelsen, Säkerhetspolisen, Tullverket, Kustbevakningen eller Krisberedskapsmyndigheten.

4.4 Ytterligare anpassningar av försvarsunderrättelseverksamheten

Förslag: I lagen om försvarsunderrättelseverksamhet skall 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 Regeringskansliet och andra berörda myndigheter.

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

Inriktning av försvarsunderrättelseverksamhet

I 1 § lagen om försvarsunderrättelseverksamhet anges att regeringen skall bestämma försvarsunderättelseverksamhetens inriktning. Utgångspunkten är således att regeringen skall inrikta och styra försvarsunderrättelseverksamheten. Även om regeringen bestämmer inriktningen krävs emellertid att de behovsställande myndigheterna ges möjlighet att närmare inrikta verksamheten inom den ram som regeringen fastställt, dock endast 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.

Vilka bedriver försvarsunderrättelseverksamhet?

Försvarsunderrättelseverksamhet skall enligt 1 § tredje stycket lagen om försvarsunderrättelseverksamhet bedrivas av Försvarsmakten och de andra myndigheter som regeringen

bestämmer, nämligen 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 försvarsunderrättelesverksamhet. I lagen bör 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 Regeringskansliet och 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. Den slutliga och samlade analysen, bör göras hos ansvariga myndigheter. Underrättelser 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. Underrättelserapporteringen omfattas självklart av den kontroll av verksamheten som skall genomföras (se vidare kap. 6).

För att tydliggöra att det 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. Inget bör dock hindra t.ex. Försvarsmakten eller Totalförsvarets forskningsinstitut (FOI) från att producera mer aggregerade analyser eller hotbildsbedömningar inom ramen för sina ansvarsområden. Hur resultaten av denna verksamhet skall rapporteras behöver inte lagregleras.

Inhämtning med särskilda metoder

Underrättelserna skall i huvudsak grunda sig på 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 4.2 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. Ytterligare förslag vad gäller den tekniska inhämtningen redogörs för i kapitel 5.

5 Signalspaning

5.1 Behov av effektiv signalspaning

I tidigare avsnitt har behovet av en effektiv underrättelseverksamhet redovisats. Signalspaning som bedrivs mot eterburen trafik står traditionellt för huvuddelen av det inhämtade underrättelseunderlaget. I dag sker dock allt mer av den elektroniska kommunikationen via tråd (kabel). Signalspaningens möjligheter att inhämta relevanta underrättelser är därför på väg att urholkas, vilket på sikt kan medföra allvarliga men för underrättelseproduktionen till stöd för Sveriges utrikes-, säkerhets- och försvarspolitik. För att underrättelseverksamheten framöver skall kunna producera relevanta underrättelser måste övervägas att ge signalspaningen tillgång till såväl etersom trådburen kommunikation. Flera jämförbara länders underrättelsetjänster har redan denna möjlighet eller håller på att skaffa sig den (se vidare avsnitt 5.1.2).

I detta avsnitt redogörs närmare för den tekniska utvecklingen och de anpassningar av regelverket som behövs för en fortsatt effektiv verksamhet. Därefter behandlas det regelverk till skydd för den personliga integriteten som måste beaktas vid de överväganden som en anpassning av signalspaningsverksamhetens förutsättningar föranleder.

5.1.1 Nuvarande begränsningar och framtida behov

Teknikutvecklingen

Den tekniska utvecklingen på kommunikationsområdet går mycket snabbt. Komplexiteten hos olika kommunikationssystem liksom variationen av signalsystem och volymen av kommunikation ökar. 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, såsom också föreskrivs i 2 § i instruktionen för myndigheten, fortlöpande utveckla den teknik och metodik som behövs för att bedriva signalspaningsverksamheten.

Som har framgått ovan av avsnitt 3.2.2 bedrivs Försvarets radioanstalts signalspaning i dagsläget mot alla typer av trådlös kommunikation, t.ex. telefoni, telegrafi, dataöverföring och tjänster via Internet. Den nuvarande tekniken bygger helt på de förutsättningar som rådde ända in på 1990-talet, då överföring av stora mängder kommunikation vid längre avstånd oftast skedde helt eller delvis trådlöst via radio (i ”etern”). Den tekniska utvecklingen har emellertid inneburit att kommunikationssignaler numera i allt högre grad överförs trådbundet. I andra jämförbara länder har inhämtningstekniken vid signalspaning därför i huvudsak kommit att inriktats mot sådan kommunikation.

Det globala nätet

Trådlös överföring sker via radionät på marken (radiolänkar) samt via kortvåg och kommunikationssatelliter (radiokommunikation). Trådbunden överföring sker via kablar i form av bl.a. fiberoptiska nät. De olika kommunikationsvägar som utnyttjas 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 transmissionsmedel (radiolänk, satellit eller tråd [kabel]) för kommunikationen styrs av de operatörer – statliga eller privata kommunikationsföretag – som tillhandahåller kommunikationskapacitet på det samlade globala nätet. Valet av kommunikationsväg är i princip helt automatiskt och den som använder nätet för kommunikation eller tjänster kan inte bestämma vilken väg eller vilken kombination av transmissionsmedel som skall användas vid ett visst kommunikationstillfälle. Det är inte heller säkert att den geografiskt sett närmaste vägen för överföring används. Valet av kommunikationsväg och medel sker helt utifrån företagsekonomiska bedömningar med hänsyn till befintlig kommunikationskapacitet och pris.

Det globala nätet förmedlar all sorts kommunikation och utnyttjas av en mängd olika typer av användare; offentliga organ, företag och enskilda. Som exempel använder operatörerna 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 m.m. 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 allt större utsträckning.

Volymen av den kommunikation som överförs via det globala nätet ökar ständigt och har redan i dag oerhörda 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 försvarsunderrättelse-perspektiv. Nätet används dock även för sådana 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 stora 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. Samtidigt krävs en mycket selektiv sökprocess för att skilja ut den mycket begränsade trafik som skall få inhämtas i underrättelsearbetet. Utsorteringen av rätt information ur den gigantiska trafikmängden ställer stora krav på de tekniska systemen.

IT-relaterade hot

I kapitel 4 anges att hot mot den tekniska infrastrukturen, inte minst tele- och datasystem, måste ges ökad uppmärksamhet i underrättelseverksamheten. I samband med den diskussion som förs i avsnitt 4.3.2. om försvarsunderrättelseverksamhetens gränser konstateras följdriktigt att försvarsunderrättelseverksamhetens resurser måste kunna användas också för att möta kvalificerade IT-relaterade hot och att sådana företeelser därför skall omfattas av begreppet ”yttre hot”.

Eftersom signalspaning är den metod i försvarsunderrättelseverksamheten som framförallt står till buds för att i ett tidigt skede kunna möta de IT-relaterade hoten, finns det anledning att i detta kapitel närmare beskriva denna hotbild och dess konsekvenser för signalspaningen.

Sveriges framväxande informationssamhälle utsätts ständigt för attacker och övervakning av såväl främmande stater som icke-statliga aktörer. Även om mörkertalet är stort och långtifrån allt blir känt kommer ständigt nya rapporter om t.ex. spridning av datorvirus och andra mer kvalificerade hot som olika typer av gränsöverskridande kriminell verksamhet eller stater som tillskansar sig information via de globala informationsnätverken.

Säkerhetspolisen konstaterar i sin verksamhetsberättelse för 2003 att ”SÄPO har under 2003 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 – Tänkbara åtgärder för att säkra Internets infrastruktur (PTS-ER-2004:37) följande.

> Samhället blir allt mer beroende av säker och fungerande kommunikation över Internet. Internet är idag verksamhetskritiskt för näringslivet och en viktig motor för Sveriges tillväxt. Den offentliga sektorn tar även allt större steg mot Internetberoende bland annat i och med satsningar på 24-timmarsmyndigheter. Samtidigt ökar incidenter i form av bland annat avbrott samt överbelastnings- och intrångsattacker. Om vitala delar av Internet skulle slås ut kan det få stora konsekvenser för samhället. Internet som sådant bedöms till sin natur vara en relativt säker infrastruktur men den generella skyddsnivån ökar inte lika mycket som riskerna. Internets nuvarande säkerhet sätts utifrån operatörernas kommersiella överväganden på en konkurrerande marknad.
>
> /---/ Ett av de största hoten mot Internet idag är bristande säkerhet i användares miljöer vilket leder till att deras datorer kapas och används som plattformar för attacker mot bland annat kritiska delar av Internets infrastruktur.

Andra studier och rapporter visar hur sårbara vi är för angrepp från kvalificerade aktörer som kan bedriva t.ex. företagsspionage eller begå intrång i slutna nätverk för att tillskansa sig sekretessbelagd information. Sådana aktörer kan t.ex. vara främmande länders underrättelsetjänster. Mot denna typ av verksamhet har teleoperatörer och andra många gånger svårt att värja sig, trots att det är deras system som ofta nyttjas.

Förhållandet illustreras i t.ex. Krisberedskapsmyndighetens årliga rapport avseende Samhällets informationssäkerhet – Lägesbedömning 2004, Totalförsvarets forskningsinstituts användarrapport En studie om det kvalificerade IT-hotet (FOI-R-1182-SE) i februari 2004, Försvarets radioanstalts löpande IT-kontrollverksamhet och Informationssäkerhetsutredningens rapport Informationssäkerhet i Sverige och internationellt (SOU 2004:32). Dessa och andra studier förstärker intrycket av att staten måste ta ytterligare ansvar, framförallt för att möta de kvalificerade IT-relaterade hoten av säkerhetspolitisk dignitet. Informationssäkerhetsutredningen (SOU 2004:32 sid. 27) konstaterar bl.a. att det finns kvalificerade IT-relaterade hot som, mot bakgrund av den framväxande globala kommunikationsstrukturen och den nya informationstekniken, i en förlängning också skulle kunna innebära ett hot mot rikets säkerhet.

Det förebyggande arbetet genom t.ex. tekniska och administrativa säkerhetsarrangemang, är det effektivaste medlet för att kunna skydda sig mot de kvalificerade hoten. Underrättelsetjänsten kan bidra till detta arbete men är också ett viktigt verktyg för att tidigt kunna möta de kvalificerade IT-relaterade hoten. Samma teknik som kan användas för signalspaning i det globala nätet för traditionell underrättelseinhämtning kan också fylla en viktig funktion som skydd mot kvalificerade attacker via det globala nätet mot våra IT-system. I propositionen 2001/02:158 Samhällets säkerhet och beredskap konstateras att underrättelse- och säkerhetstjänstens arbete bör förstärkas för att förhindra allvarliga informationsattacker mot Sverige (sid. 103). Det framstår följaktligen som en angelägen uppgift för underrättelseverksamheten att bidra till säkerheten mot kvalificerade IT-relaterade hot och att skydda enskilda och samhället mot obehörig användning av kommunikationssystemen. En förutsättning för detta är dock att såväl eter- som trådburen trafik kan följas och att det ges möjlighet att använda de unika metoder som signalspaningen representerar i detta syfte. Sverige riskerar annars att i allt större utsträckning 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 i detta avseende anför följande (sid. 85).

> Utredningen vill i dessa sammanhang peka på att i omvärlden prioriteras signalspaningsorganens verksamhet till skydd för IT-system mycket högt. Signalspaningsorganens möjligheter att spela en avgörande roll för skyddet mot kvalificerade IT-relaterade hot bedöms i dessa sammanhang som stora. Möjligheterna för FRA att kunna fylla en roll i IT-sammanhang kräver emellertid, som nyss har nämnts, att FRA ges legala och tekniska förutsättningar för att fullt ut kunna bevaka information i det globala kommunikationsnätet.

Informationssäkerhetsutredningen konstaterar också i sin rapport Säker information Förslag till informationspolitik (SOU 2005:42) att signalspaningsorganens möjligheter att spela en avgörande roll för skyddet mot kvalificerade IT-relaterade hot bedöms som stora (s. 212).

5.1.2 En internationell jämförelse

De ändrade förutsättningar för signalspaning som den tekniska utvecklingen inneburit är inte en företeelse som är begränsad till Sverige. I många länder har problematiken uppmärksammats och på flera håll även lett till lagstiftning som möjliggör signalspaning även mot trådburen kommunikation.

I Storbritannien infördes år 2000 en mycket omfattande lag benämnd ”Regulation of Investigatory Powers Act 2000” (RIPA). I första delen första kapitlet finns regler för övervakning och avlyssning av kommunikationer. Regelverket är teknikneutralt, det vill säga det gör ingen åtskillnad i fråga om i vilket medium övervakningen/avlyssningen äger rum. I del 6(2) av RIPA finns en förteckning över de myndigheter som får bedriva övervakningen av kommunikationer. Försvarets

radioanstalts motsvarighet Government Communications Headquarters (GCHQ) finns upptagen i den förteckningen.

Den tyska lagstiftningen är uppbyggd ungefär efter samma mönster som den brittiska. I en särskild lag föreskrivs enligt vilka förutsättningar intrång får äga rum i den grundlagsfästa rätten till skydd av kommunikationer. Vidare anges för vilka ändamål ett antal olika myndigheter får övervaka/avlyssna kommunikationer. Avlyssningen får ske såväl i brottsutredningssyfte som i underrättelsesyfte. Bundesnachriechtendienst, som inom sig har en signalspaningsorganisation, är en av de myndigheter som ges befogenhet i lagen. Tyskland antog vidare i januari 2002 en förordning enligt vilken teleoperatörer med flera ålades långtgående skyldigheter att anpassa sina tekniska system så att verkställighet av myndigheternas avlyssning/övervakning kan ske.

I Nederländerna antogs år 2002 lagstiftning rörande underrättelse- och säkerhetstjänsterna. Lagen innehåller detaljerade regler om förutsättningarna för myndigheternas övervakning av olika typer av kommunikationer. Regelverket är inte som det brittiska utformat på ett teknikneutralt sätt 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, Allgemene Inlichtingen en Veiligheids Dinst (underrättelse- och säkerhetstjänsten) och Militaire Inlichtingen en Veilgheidsdienst (militära underrättelse- och säkerhetstjänsten).

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

Nya Zeeland har en ny lag från 2004 (Telecommunications [Interception Capability] Act 2004) nyligen antagits. Lagstiftningen ger deras säkerhetstjänst (New Zealand Security

Service) och deras signalspaningsorganisation (Goverment Communications Security Bureau) rätt till inhämtning av telekommunikation. Lagen innehåller detaljerade regler om förutsättningarna för hur övervakning av olika typer av kommunikationer skall gå till. Regelverket är teknikneutralt, det vill säga det gör ingen åtskillnad i fråga om i vilket medium övervakningen/avlyssningen äger rum.

5.2 Skyddet för den personliga integriteten

5.2.1 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 samhällsmedborgarna. 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 på den grunden 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 30 mars 2007.

5.2.2 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 (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 radioprogram, filmer och ljudupptagningar. Meddelarfriheten garanteras bl.a. 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 § yttrandefrihetsgrundlagen. 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 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. 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.

5.2.3 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 (SOU 1998:46 s. 52).

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.

Bestämmelserna i artikel 8 innebär inte bara att konventionsstaterna skall avhålla sig från ingrepp i den skyddade rättigheten. Det åligger också staten att vidta positiva åtgärder för att skydda den enskildes privatsfär (a.a. s. 261).

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 (jfr Danelius s. 263). Vidare måste undantaget vara utformat med sådan precision att inskränkningen av rättigheten är i rimlig utsträckning förutsebar.

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 det är strängt nödvändigt 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 SOU 1993:40 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 demokratiska stater och införlivades genom Maastricht-fördraget i samtliga EU-medlemsstaters lagstiftning. 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 av att åtgärden framstår som nödvändig i ett demokratiskt samhälle. Det har 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.

5.2.4 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 är 4 kap. om brott mot frihet och frid samt 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.

Enligt 4 kap. 8 § BrB är det straffbart som *brytande av post- eller telehemlighet* att olovligen bereda sig tillgång till ett meddelande som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller telemeddelande. Det saknar betydelse om telemeddelandet förmedlas via det allmänna telenätet eller på annat sätt. För att bestämmelsen skall vara tillämplig förutsätts att försändelsen innehåller ett meddelande. Det är inte straffbart att lyssna på telemeddelanden som befordras endast med radio (t.ex. mobiltelefoni som inte sker via kabel, SOU 1992/93:200 s. 166 f.). En förutsättning för straffbarhet är att gärningen sker olovligen. Även utan samtycke kan en gärning anses vara fri från ansvar, exempelvis om förfarandet utgör tvångsmedelsanvändning såsom beslag av brev eller hemlig teleavlyssning.

Den som olovligen bryter ett brev eller ett telegram eller annars bereder sig tillgång till något som förvaras "tillslutet eller under lås" kan dömas för *intrång i förvar* enligt 4 kap. 9 § BrB. Bestämmelsen är subsidiär i förhållande till 4 kap. 8 § BrB. Straffskyddet gäller inte bara brev och meddelanden utan också annat som förvaras tillslutet. Liksom vid tillämpning av 4 kap.

8 § BrB kan gärningen vara fri från ansvar på grund av att den enligt särskilda bestämmelser är lovlig.

I 4 kap. 9 a § BrB regleras *olovlig avlyssning*. För det brottet döms den som i annat fall än som sägs om brytande av post- eller telehemlighet olovligen medelst tekniskt hjälpmedel för återgivning av ljud i hemlighet avlyssnar eller upptar tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst, vartill allmänheten inte äger tillträde och som han själv inte deltar i eller som han obehörigen berett sig tillträde till.

Bestämmelsen om *dataintrång* i 4 kap. 9 c § BrB, som motsvarar 21 § i den numera upphävda datalagen (1973:289), innebär att det är straffbart att olovligen bereda sig tillgång till en upptagning för automatisk databehandling. Med upptagning för automatisk databehandling avses en hantering av uppgifter som sker med hjälp av dator som försetts med ett program som anger vilka åtgärder som skall vidtas, det vill säga en programstyrd behandling. Det är enligt samma bestämmelse också straffbart att olovligen ändra eller utplåna eller i register föra in upptagning för automatisk databehandling. Även om tillgången till en upptagning är lovlig är det alltså straffbart att olovligen ändra i eller utplåna en sådan upptagning. Bestämmelsen om dataintrång är subsidiär i förhållande till brytande av post- eller telehemlighet och intrång i förvar (4 kap. 8 och 9 §§ BrB).

5.2.5 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 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 generell 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. I Försvarsdepartementet bereds för närvarande en departementspromemoria om lagreglering av ifrågavarande verksamhet.

Europarlamentets och rådets direktiv (2002/58EG) 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 i bestämmelserna i direktivet.

5.3 En lagstiftning som tillgodoser verksamhetens behov

5.3.1 Reglering av signalspaningsverksamheten vid Försvarets radioanstalt

5.3.1.1 En utvidgning av signalspaningsmandatet

Förslag: Försvarets radioanstalt skall få bedriva signalspaning oavsett om signalerna befinner sig i etern eller i kabel, dvs. är trådbundna. Detta skall regleras i en ny lag om signalspaning.

Samhällets behov av en effektiv underrättelseverksamhet har beskrivits närmare i kap. 4 och i avsnitt 5.1.1, 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.

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 och signalspaningen har fått en allt viktigare roll för att skydda vår kommunikation mot utnyttjande från andra länder och aktörer och därigenom bidra till att upprätthålla informationssäkerheten i samhället. Det är följaktligen ett angeläget allmänt intresse att Försvarets radioanstalt 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.

Mot bakgrund av ovanstående framstår det som nödvändigt att anpassa förutsättningarna för signalspaningsverksamheten till utvecklingen på de säkerhetspolitiska och tekniska områdena. Starka skäl talar därför för att Försvarets radioanstalt bör ges möjlighet att inhämta signaler i elektronisk form vid signalspaning 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. Mot bakgrund av att det är tillfälligheter som avgör hur ett meddelande förmedlas – trådlöst eller trådbundet – kan det dock ifrågasättas om det är rimligt att i detta sammanhang föreslå en ordning enligt vilken ett och samma meddelande kan hämtas in fritt när det befordras trådlöst medan inhämtningen är omgärdad av skyddsmekanismer när det befordras trådbundet. Den lagstiftning som behovet av ett utvidgat signalspaningsmandat aktualiserar bör därför vara teknikneutral på så sätt att signalerna rättsligt sett bör behandlas lika oavsett hur och från vilket medium kommunikationen inhämtas. Genom att signalspaningsverksamheten vid Försvarets radioanstalt i sin helhet ges uttryckligt stöd i lag tydliggörs också att den är förenlig med de ovan redovisade bestämmelserna i brottsbalken, vilka endast kan tillämpas i fråga om verksamhet som bedrivs olovligen.

Sammanfattningsvis kan konstateras att signalspaning bör få bedrivas även avseende signaler i tråd. Den lagstiftning som behovet av ett utvidgat signalspaningsmandat aktualiserar bör

vara teknikneutral och följaktligen också omfatta inhämtning av signaler i etern. Genom att signalspaningsverksamheten i sin helhet ges uttryckligt stöd i lag tydliggörs att den är förenlig med de ovan redovisade bestämmelserna i brottsbalken, vilka endast kan tillämpas i fråga om verksamhet som bedrivs olovligen.

Signalspaningen skall bedrivas vid den myndighet som regeringen bestämmer (Försvarets radioanstalt).

5.3.1.2 Inhämtningens omfattning

Förslag: Inhämtning av signaler i elektronisk form vid signalspaning vid Försvarets radioanstalt skall få ske för försvarsunderrättelseverksamhet, det vill säga 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.

Inhämtning av signaler i elektronisk form vid signalspaning skall vidare få ske för att myndigheten skall följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten.

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. Således måste signaler i elektronisk form kunna inhämtas. I avsnitt 5.3.2 redogörs för begreppet elektronisk kommunikation. Begreppet definieras inte i lagstiftningen men anses inte omfatta innehållet i kommunikationen. Därför är begreppet inte lämpligt att använda för

att definiera föremålet för den inhämtning som signalspaningen innefattar. I stället skall det teknikneutrala och heltäckande uttrycket signaler i elektronisk form användas.

Det skall tydligt framgå av den nya lagen när signalspaning får ske, d.v.s. tillämpningsområdet skall 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 endast avse utländska förhållanden. I lagen om signalspaning skall anges att signalspaning skall få ske för motsvarande ändamål. Verksamheten inbegriper såväl traditionella militära frågor som de nya hoten.

Den signalspaningsverksamhet som bedrivs för försvarsunderrättelseändamål 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 verksamhet är det följaktligen viktigt att den 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. Denna verksamhet är även nödvändigt för att myndigheten skall kunna bistå med skydd mot signalspaning och teknisk informationssäkerhet. Lagen skall därför ge möjlighet till inhämtning av signaler i elektronisk form vid signalspaning också för dessa ändamål, som inte utgör försvarsunderrättelseverksamhet.

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. 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, till skillnad från den signalspaningsverksamhet som bedrivs i försvarsunderrättelsesyfte, 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. Även denna verksamhet skall därför omfattas av huvuddelen av de begränsningar som lagen uppställer.

Inhämtning av signaler i elektronisk form sker också vid de IT-säkerhetsanalyser som utförs av Försvarets radioanstalt och som syftar till att stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig ur sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Denna typ av analyser genomförs på begäran av olika myndigheter och statligt ägda bolag. Analyserna syftar till att upptäcka tekniska brister (sårbarheter) i uppdragsgivarnas interna nätverk, vilka sker bl.a. genom s.k. aktiv IT-kontroll. De signaler i elektronisk form som därvid inhämtas förmedlas i slutna nätverk. En förutsättning för denna verksamhet är att den sker med uppdragsgivarens tillstånd och att tillgång till kommunikationsnätet ges av den som råder över detta. För sådan inhämtning krävs följaktligen inte något lagstöd och den faller därmed utanför tillämpningsområdet för den föreslagna lagen.

5.3.1.3 Begränsning av inhämtningen i tråd

Förslag: Inhämtning som sker i tråd får endast avse signaler vilka förs över Sveriges gräns av operatörer som äger tråd.

Av föregående avsnitt framgår att försvarsunderrättelseverksamheten avser utländska förhållanden. I lagen 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 får bedrivas syftar till att skapa goda förutsättningar för inhämtning för försvarsunderrättelseändamål. Även sådan signalspaning riktas följaktligen mot utländska förhållanden.

När det gäller signaler i tråd finns det av lätt insedda skäl begränsade möjligheter för Försvarets radioanstalt 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 Försvarets radioanstalt 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 samtidigt utesluta inhemsk trafik, bör inhämtningen av signaler i tråd följaktligen avse signaler som förs över Sveriges gräns. Visserligen kan även inhemsk trafik, till följd av t.ex. kapacitets- eller kostnadsskäl, komma att passera landgränsen. Detta förekommer dock i så liten utsträckning att den föreslagna regleringen i praktiken utgör en begränsning av signalspaningens tillämpningsområde till sådan trådburen trafik som är relevant i förhållande till de ändamål för vilka försvarsunderrättelseverksamheten får bedrivas.

För att Försvarets radioanstalt 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 lagen om signalspaning 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, d.v.s. den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation. De

bestämmelser av teknisk karaktär som behövs för att åstadkomma nödvändig åtkomst till signaler i tråd i enlighet med det ovan anförda beskrivs närmare i avsnitt 5.3.2.

När det gäller signaler i etern förutsätter inte möjligheten till inhämtning att åtkomsten till signalerna regleras särskilt. Det finns inte heller någon möjlighet att på teknisk väg begränsa vilken eterburen kommunikation som skall göras tillgänglig för signalspaning.

5.3.1.4 Automatiserad inhämtning med sökbegrepp

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.

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. En sådan ordning skulle ställa närmast orealistiska krav på kapacitet för lagring av information som endast till en ytterst begränsad del är av relevans för signalspaningsverksamheten. För att på ett rimligt sätt avgränsa denna inhämtning är det därför nödvändigt att begränsa den till signaler som kan identifieras genom 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 kommer att inhämtas och hanteras vidare av myndigheten.

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. Det är följaktligen inte enkla variabler såsom namnet på en terroristorganisation som nyttjas utan mycket specifika och väl avvägda kombinationer.

I avsnitt 5.4.1.2 behandlas de särskilda bestämmelser som skall gälla vid användning av sökbegrepp som är direkt hänförliga till viss fysisk person.

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.

Av det sagda följer också att ett system med tillstånd till eller förhandskontroll av utnyttjande av olika sökbegrepp är förknippat med stora praktiska problem. Till saken hör också att verksamheten handlar om inhämtning av strategiskt viktig information för Regeringskansliet och andra myndigheters räkning och inte information som kan läggas till direkt grund för ingripanden mot enskilda här i Sverige. Från denna utgångspunkt synes någon förhandskontroll inte heller nödvändig. Den rimligaste modellen för fastställande av sökbegrepp är istället att lägga uppgiften på den myndighet som utför verksamheten d.v.s. Försvarets radioanstalt. En sådan beslutsprocess tillgodoser de angivna kraven på säkerhet, kunskap om verksamheten samt förmåga att fortlöpande och skyndsamt fastställa sökbegreppen. Den överensstämmer också med principen att en myndighet som har ansvaret för en verksamhet också får fatta alla de beslut som är nödvändiga för att bedriva verksamheten, så länge den inte innefattar sådana åtgärder mot enskilda att rättssäkerheten kräver utomstående prövning.

Fastställandet av sökbegreppen är en komplicerad uppgift som har stor betydelse för hur Försvarets radioanstalts verksamhet bedrivs. Med hänsyn till frågans speciella karaktär bör sådana beslut fattas av myndighetens chef, vilket därför bör regleras i förordning. Det är också viktigt att myndigheten även i övrigt har en väl fungerande rutin för hanteringen av sökbegreppen. Denna rutin regleras lämpligen i myndighetens arbetsordning. 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 kontroll 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 kap. 6.

5.3.1.5 Inriktning, rapportering, internationellt samarbete och kontroll

Förslag: Även signalspaningsverksamhet som inte är försvarsunderrättelseverksamhet skall inriktas av regeringen.

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

Försvarets radioanstalt 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.

En särskild myndighet (Försvarets underrättelsenämnd) skall kontrollera efterlevnaden av lagen om signalspaning. I kontrollen skall särskilt ingå en granskning av sökbegreppen och av rapporteringen.

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 4.4). Bestämmelserna om inriktning gäller också för signalspaningsverksamheten. I lagen om signalspaning skall därför tas in en erinran om denna bestämmelse.

Förutom för de ändamål som anges i lagen om försvarsunderrättelseverksamhet får signalspaningsverksamheten enligt vad som angetts i avsnitt 5.3.1.2. 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 dessa ändamål 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 inte utgör försvarsunderrättelseverksamhet.

Rapportering av underrättelser

Enligt förslaget till ändring i lagen om försvarsunderrättelseverksamhet skall rapportering av underrättelser ske till berörda myndigheter. Sådana myndigheter är, förutom Regeringskansliet, 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. Nödvändiga begränsningar av rapporteringen behandlas i avsnitt 5.4.1.5. 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 direkt 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 försvarsunderrättelsesidan 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 som bedrivs enligt 1 § andra stycket lagen om signalspaning.

Kontroll av verksamheten

En effektiv och ändamålsenlig insyn i och kontroll av underrättelseverksamheten är ett viktigt element för att skapa förtroende för denna centrala men också känsliga verksamhet. Försvarets underrättelsenämnd granskar idag den signalspaningsverksamhet som Försvarets radioanstalt bedriver. När Försvarets radioanstalts mandat för signalspaning nu anpassas till den säkerhetspolitiska och tekniska utvecklingen finns anledning att ytterligare betona betydelsen av en utomstående granskning av verksamheten. Försvarets underrättelsenämnd skall därför nära följa och kontrollera signalspaningsverksamheten. I kontrollen skall särskilt ingå granskning av de sökbegrepp som används och den rapportering av underrättelser som sker. I kap. 6 ges en närmare beskrivning av kontrollverksamheten. I kap. 3 redogörs för hur kontrollen av verksamheten genomförs i ett antal andra länder som är jämförbara med Sverige.

5.3.2 Reglering av tillgången till signaler i tråd

5.3.2.1 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 olika 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, telefaxmeddelanden, elektronisk post, datakommunikation och annan kommunikation som innehåller meddelanden, det vill säga information i form av text, bild eller ljud.

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 mobiltelesystem, UMTS (Universal Mobile Telecommunications System), innebär att överföringskapaciteten ökar ytterligare.

Beträffande *informationsteknik och datakommunikation* kan följande nämnas. 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.

5.3.2.2 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, EkomL. 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-komutred-

ningen 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 § EkomL 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 2002/03:TU6 s. 6).

Vissa bestämmelser i lagen om elektronisk kommunikation knyter an till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. Enligt 6 kap. 19 § EkomL 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.

5.3.2.3 Nya regler för att möjliggöra inhämtning

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

Samverkanspunkter skall utses och anmälas av de trådägande operatörerna till den myndighet som regeringen bestämmer (Försvarets radioanstalt).

Samtliga operatörer som för signaler i tråd över Sveriges gräns skall se till att dessa enkelt kan tas om hand.

Regeringen eller tillsynsmyndigheten enligt lagen (2003:389) om elektronisk kommunikation (Post- och telestyrelsen) 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.

Trådägande operatörers skyldigheter

Förslaget till lag om signalspaning ger möjlighet för Försvarets radioanstalt 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 § EkomL den som innehar eller på annat sätt råder över ett allmänt kommunikationsnät eller tillhörande installation. Det finns ett antal opera-

törer som äger tråd (i 1 kap. 7 § EkomL anges att överföring av signaler kan ske bl.a. via tråd). Verksamheterna bedrivs på många håll i landet. För att Försvarets radioanstalt skall kunna ta emot signalerna krävs givetvis att dessa överförs till myndigheten. Av övervägandena i avsnitt 5.3.1.3 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). 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.

Det finns ett mindre antal (ett tiotal) trådägande operatörer i förhållande till antalet andra operatörer (t.ex. Internet Service Providers). Dessa andra operatörer varierar mer i antal över tiden. 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 som för trafik 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, det vill säga när lagen träder i kraft och därefter när nya trådägare tillkommer. Det är dock den trådägande operatören som väljer överföringssätt fram till samverkanspunkten. 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 det fulla ansvaret att föra trafiken till samverkanspunkten, som också utses av operatören. Från samverkanspunkterna har myndig-

heten 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 utsett och därefter har Försvarets radioanstalt det totala kostnadsansvaret. Försvarets radioanstalt skall vidare svara för kostnaderna för uppsättande och drift av nödvändig utrustning vid samverkanspunkterna.

Samverkanspunkter skall, sedan de trådägande operatörerna utsett dem, anmälas till den myndighet som regeringen bestämmer (Försvarets radioanstalt). 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 viktigt att de anmäler punkter som är belägna på platser med motsvarande säkerhetsnivå som operatörer har i sina nät i övrigt för säkra trafikpunkter.

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten (Post- och telestyrelsen) 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 och åtkomlighet för myndigheten. Föreskrifterna skall utformas 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 kap. 7.

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 § EkomL). Detta gäller således trådägare, Internet Service Providers (ISP) med flera.

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, d.v.s. 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. 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 EkomL) – utföra uppgiften enligt den föreslagna bestämmelsen så att verksamheten inte röjs.

I 6 kap. 21 § EkomL 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 EkomL (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 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 § EkomL.

Ikraftträdande och övergångsbestämmelser

Förslag: Ändringarna i lagen om elektronisk kommunikation föreslås träda i kraft den 1 juli 2006. Skyldigheten för operatörer som äger tråd att överföra signaler till samverkanspunkter enligt 6 kap. 19 a § föreslås dock gälla från och med den 1 januari 2007.

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.

Det är 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 ändringarna i EkomL föreslås träda i kraft den 1 juli 2006 är det därför befogat att de trådägande operatörerna ges ytterligare sex månader för att förbereda systemen för den första samverkanspunkten. Skyldigheten i detta hänseende för operatörerna föreslås därför tidigast gälla från och med den 1 januari 2007. 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.

5.4 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 5.2.

5.4.1 Rättighetsskyddsgarantier i den nya lagen om signalspaning

5.4.1.1 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 sådan kränkning av 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 5.2.1 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 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 5.2 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 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 rättssäkerhetsgarantierna.

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 5.3.1.4 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 kommer automatiserad inhämtning av uppgifter vid signalspaning inte 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 5.3.1.4. Tillämpningsområdet begränsas vidare av de syften för vilka signalspaning skall få bedrivas, vilka redovisats i avsnitt 5.3.1.2. En viktig omständighet är också att signalspaning i försvarsunderrättelseverksamhet endast får bedrivas beträffande utländska förhållanden och att sådan verksamhet inte skall få innefatta åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete enligt lagar och förordningar (se avsnitt 4.3.3). Ett på detta sätt begränsat tillämpningsområde får anses fylla kravet på skydd mot godtyckliga ingrepp.

Av betydelse i sammanhanget är vidare att syftet med förvarsunderrättelseverksamhet främst är att införskaffa strategisk information som Regeringskansliet och andra myndigheter behöver för planering, beslut och andra åtgärder. I mångt och mycket är det alltså fråga om övergripande information som inte angår den personliga sfären. Integritetsaspekterna kan dock göra sig gällande också vid inhämtning av sådan information och naturligtvis i ännu högre grad när det är fråga om uppgifter som hänför sig till viss person. I integritetshänseende blir därmed utformningen av sökbegreppen av stor betydelse.

5.4.1.2 Reglering av användningen av sökbegrepp

Förslag: Sökbegrepp får inte vara direkt hänförliga till viss fysisk person såvida det inte är av synnerlig vikt för verksamheten. Sökbegreppen skall granskas i särskild ordning.

Eftersom all automatiserad inhämtning av signaler i elektronisk form skall ske genom användning av sökbegrepp (se avsnitt

5.3.1.5), kommer en ytterst begränsad 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 kommer 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.

För att så värdefull information som möjligt skall kunna erhållas genom signalspaningen måste inhämtningen ibland inriktas mot personer 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 krävas att sökbegreppen får vara direkt hänförliga till en fysisk person endast när det är av synnerlig vikt för verksamheten. Bestämmelsen innebär att användning av sådana sökbegrepp som personnamn samt telefonnummer, e-postadresser, IP-adresser etc. som kan knytas till en fysisk person måste föregås av noggranna överväganden.

Kontroll av att sökbegreppen endast används på det sätt som stadgas i lagen, och i synnerhet att de används på ett sätt som inte medför otillbörligt intrång i den personliga integriteten, bör vara en viktig del i den särskilda granskning som skall ske av verksamheten.

För den begränsade inhämtning som kommer att ske med manuella metoder, d.v.s. 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 5.4.1.4). Även efterlevnaden av denna föreskrift är en naturlig och central del av den särskilda granskningen.

5.4.1.3 Tillståndsförfarande

Förslag: En myndighet som enligt regeringens bestämmande får ge närmare inriktning för signalspaningsverksamheten, skall innan inriktningen ges, inhämta tillstånd av Försvarets underrättelsenämnd. Om tillstånd inte utan väsentlig olägenhet kan avvaktas får inriktningen ges utan tillstånd, men skall då omedelbart anmälas till nämnden. Om nämnden finner att inriktningen inte borde ha verkställts skall Försvarets radioanstalt underrättas och inhämtningen omedelbart avbrytas.

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 inte lämnas om inriktningen endast avser viss fysisk person.

Generella krav på tillstånd

När det gäller de rättssäkerhetsgarantier som är nödvändiga vid signalspaning skulle det ur ett renodlat rättssäkerhetsperspektiv givetvis vara att föredra om inhämtningen endast fick ske efter särskilt tillstånd i varje enskilt fall. Ett sådant generellt krav på tillstånd skulle dock leda alltför långt med hänsyn till att inhämtningen kan avse såväl uppgifter som helt saknar betydelse i integritetshänseende som uppgifter av mer integritetskänslig natur. Mot bakgrund av den föreslagna regleringen av verksamhetens omfattning och de ändamål för vilka den skall få ske är en sådan ordning inte heller praktiskt genomförbar. Ett skäl är att signalspaning som bedrivs i enlighet med lagen i stor utsträckning syftar till att inhämta kommunikation som inte är känd i förväg. Saken kan uttryckas så att man spanar efter det okända. Ett tillstånd skulle följaktligen behöva innefatta så vida ramar för signalspaningen att prövningen skulle te sig föga meningsfull från rättssäkerhetssynpunkt. Ett annat skäl är att

verksamheten måste präglas av så stor flexibilitet att man i varje ögonblick kan anpassa spaningen till det relevanta.

Ett annat alternativ för att tillgodose rättsäkerhetskraven skulle kunna vara att sökbegreppen blir föremål för en förhandskontroll. Det alternativet är dock inte genomförbart av skäl som redovisats i avsnitt 5.3.1.4.

När det gäller de länder som i sin lagstiftning på området har infört krav på förhandstillstånd är det att märka att tillståndskravet inte är generellt för all signalspaning. 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 australiska 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 telehemlighet bryts skall chefen för BND begära tillåtelse vid det federala inrikesministeriet.

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), 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. Mot bakgrund av de begränsningar som föreslås beträffande de syften för vilka signalspaning får bedrivas och vilka förutsättningar i övrigt som gäller för verksamheten, kan det därför inte heller med beaktande av andra länders system anses föreligga något behov av ett generellt tillståndskrav i lagen om signalspaning.

Tillstånd för myndigheter att ge närmare inriktning

Av ovanstående följer att något generellt krav på tillstånd till signalspaning inte bör ställas upp. Detta utesluter dock inte möjligheten att ändå kräva ett visst mått av förhandsprövning. Vad som då främst aktualiseras är sådan signalspaning som bedrivs i enlighet med en av annan myndighet bestämd närmare inriktning av verksamheten. 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 av uppgifter i andra fall. Några hinder av

konstitutionell art mot ett mera begränsat tillståndssystem torde inte föreligga och inte heller torde en sådan ordning medföra några praktiska problem. Ett tillståndskrav för sådan inriktning kan dessutom underlätta såväl Försvarets radioanstalts som den inriktande myndighetens arbete genom att det aldrig 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) pröva i vilken utsträckning en närmare inriktning kan läggas till grund för inhämtningen.

Ett tillståndsförfarande förutsätter att tillståndsgivningen kan anförtros ett självständigt och oberoende organ med kunskap om verksamheten och möjligheter att hantera sekretessbelagt material. Ett möjligt alternativ skulle kunna vara att ge uppgiften till en domstol. 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 nu aktuell 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 regeringens inriktningsbeslut. En sådan prövning skulle kunna anses främmande för både de allmänna domstolarna och de allmänna förvaltningsdomstolarna.

En annan tänkbar ordning är att tillståndsprövningen anförtros en myndighet. Mot att tillskapa ett nytt organ endast för denna fråga talar tidsåtgången för att från grunden bygga upp organisationen och skaffa nödvändig kompetens. Ett annat tänkbart alternativ är att slå samman några myndigheter som idag har liknande uppgifter, såsom Försvarets underrättelse-

nämnd och Registernämnden. Det finns dock idag inte tillräckliga skäl för en sådan omfattande förändring av dessa funktioner. Ytterligare ett alternativ är att uppgiften att pröva frågor om tillstånd för inriktning av signalspaningen anförtros en redan befintlig myndighet. En sådan myndighet bör förutom kompetens att hantera försvarsunderrättelsefrågor också ha kunskap om andra 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. Men flertalet av de myndigheter som har intresse av signalspaningens resultat saknar motsvarande anknytning till ett organ av denna karaktär. Det framstår med hänsyn till myndigheternas skiftande behov som mindre ändamålsenligt att göra Registernämnden till generellt tillståndsorgan.

Ett i förhållande till försvarsunderrättelsemyndigheterna självständigt organ med god kunskap om försvarsunderrättelseverksamheten och dess förutsättningar är Försvarets underrättelsenämnd. Nämnden är den myndighet som skall kontrollera signalspaningsverksamheten och har därigenom 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 inriktning av signalspaningen. Den nya uppgift som tillståndsprövningen innebär reser krav på en förstärkning av nämndens organisation. För att tillföra nämnden fördjupad kunskap om en inriktande myndighets verksamhetsförutsättningar för ställningstagande till en närmare inriktning kan det övervägas om behovet kan tillgodoses t.ex. genom adjungering av ledamöter från respektive myndigheter.

Eftersom Försvarets underrättelsenämnds funktion i övrigt är inriktad på försvarsunderrättelsemyndigheternas verksamhet, kan det förefalla lämpligt att de inriktande myndigheterna vänder sig till Försvarets radioanstalt, som i sin tur begär tillstånd hos nämnden att få verkställa inriktningen. Tillståndsförfarandet bör dock organiseras på ett sätt som inte kan medföra att det kan

anses som om Försvarets underrättelsenämnd uppfattas ha dubbla roller som dels tillståndsgivare, dels tillsynsorgan. Det kan ske genom att det blir de beställande myndigheterna som skall söka tillstånd innan en inriktning ges till Försvarets radioanstalt. När ett tillstånd lämnats skall Försvarets radioanstalt kunna förlita sig på att inhämtning lagligen kan ske i enlighet med den givna inriktningen. Den kontroll som granskningsmyndigheten därefter utövar över signalspaningsverksamheten kommer följaktligen inte att omfatta innehållet i inriktningen, utan endast i vilken utsträckning inhämtning utförts i enlighet med inriktningen samt formerna för denna inhämtning. 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 om försvarsunderrättelseverksamhet och signalspaningslagen. Nämndens tillståndsgivning innebär inte på något sätt att den inriktande myndighetens verksamhet underställs nämndens granskning.

I kap. 6 beskrivs de organisatoriska förändringar av Försvarets underrättelsenämnd som krävs för att de nya uppgifter som åläggs nämnden skall kunna lösas. 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 innebära allvarliga problem för myndigheternas verksamhet. I sådana situationer skall 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, såsom en 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 verkställts 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, t.ex. i 4 § lagen (2000:130) om försvarsunderrättelseverksamhet, men bör ändå klargöras för att undvika tveksamhet om för vilka uppgifter andra myndigheter kan använda signalspaningsresursen.

Begränsningen såvitt avser fysiska personer innebär endast att en inriktning inte får ha till syfte att kartlägga en viss 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 direkt hänförliga till fysiska personer i sådana sammanhang får användas som sökbegrepp behandlas i avsnitt 5.4.1.2.

5.4.1.4 Upptagningar och uppteckningar som skall förstöras

Förslag: Upptagning eller uppteckning av uppgifter av signaler i elektronisk form skall omgående förstöras om den bedömts sakna betydelse för den verksamhet som regleras i lagen, 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.

Bedömning: Någon bestämmelse om förstöring av upptagning eller uppteckning som omfattar kommunikation med någon av de övriga kategorier som avses i 36 kap. 5 § rättegångsbalken behövs inte.

Information utan betydelse för verksamheten

I avsnitt 5.4.1.2 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 uppgifter 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 den 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.

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 undvika att exempelvis ett samtal mellan en journalist och en meddelare spelas in. 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.

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 bl.a. försvarare inte 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 lagrådsremissen med anledning av Buggningsutredningens förslag (SOU 1998:46) till reglering av hemlig teknisk avlyssning (buggning) föreslogs att hemlig avlyssning inte skulle få avse en plats som stadigvarande används eller är särskilt avsedd att användas för sådan verksamhet som bedrivs av personer som avses i 36 kap. 5 § andra–sjätte stycket rättegångsbalken, såvida inte synnerlig anledning fanns att anta att platsen användes för vissa närmare angivna brott. Vidare föreslogs att hemlig avlyssning inte skulle få omfatta samtal eller annat tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte stycket rättegångsbalken, inte skulle ha kunnat höras som vittne om det som sagts eller på annat sätt uttryckts. I anslutning härtill föreslogs en bestämmelse om under vilka förutsättningar avlyssning skulle avbrytas och förstöring av upptagningar eller upptagningar ske, motsvarande vad som följer av 27 kap. 22 § rättegångsbalken.

36 kap. 5 § andra–sjätte stycket rättegångsbalken reglerar begränsningar i vittnesplikten för advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter, familjerådgivare, präster eller personer med motsvarande ställning i ett trossamfund samt den som har tystnadsplikt enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen till skydd för meddelarfriheten.

Lagrådet delade uppfattningen att det vid avgränsningen av tillämpningsområdet för hemlig avlyssning kunde vara naturligt

att knyta an till reglerna i 36 kap. 5 § om undantag från vittnesplikten, men anförde synpunkter på den föreslagna regleringens utformning bl.a. i fråga om dess tillämpningsområde såvitt avsåg advokater samt präster och motsvarande personer (prop. 2002/03:74 s. 91 f.f.). Lagrådsremissen har inte föranlett lagstiftning.

I samband med såväl tillkomsten av skyddet för samtal mellan den misstänkte och hans försvarare i 27 kap. 22 § rättegångsbalken som övervägandena kring införande av möjlighet till hemlig avlyssning, har utgångspunkten 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 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. Det är följaktligen inte möjligt att med hjälp av sådana underrättelser kringgå bestämmelserna om begränsningar av vittnesplikten. Inte heller föreligger någon risk för att integritetskänsliga uppgifter skall spridas i offentligheten på det sätt som sker under en rättegång.

De allmänna bestämmelser som föreslås om användning av sökbegrepp, tillstånd för viss inriktning och förstöring av

upptagningar eller upptecknings etc. utgör ett fullgott skydd mot att sådan kommunikation som här avses 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. Det kan sammanfattningsvis inte anses föreligga något behov av att i fråga om signalspaningen göra några begränsningar utöver de som behandlats ovan såvitt avser de kategorier som nämns i 36 kap. 5 § rättegångsbalken.

5.4.1.5 Begränsningar av rapporteringen

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

Som tidigare redovisats blir sökbegreppen avgörande för vilken information om enskilda som kommer 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 t.ex. ett och samma telefonsamtal. Den ovan nämnda bestämmelsen om förstöring av upptagning eller uppteckning omfattar bara förstörande av betydelselösa upptagningar men riktar sig inte mot en upptagning 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 bör därför föras in en bestämmelse om att rapportering av underrättelser som inhämtats genom signalspaning 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 lämnas.

5.4.1.6 Effektiva rättsmedel

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

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 5.2.4. 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. 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.

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 med liknande

förhållanden (hemlig telefonavlyssning) 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).

Mot den angivna bakgrunden får den kontroll som sker genom Försvarets underrättelsenämnd, sammantaget med den tillsyn som JO och JK utövar, anses tillgodose kravet på effektiva rättsmedel i de fall då de ovan beskrivna möjligheterna till domstolsprövning inte kan utnyttjas direkt av den enskilde.

5.4.2 Behovet av rättighetsskyddsgarantier med anledning av de förslag som avser lagen om elektronisk kommunikation

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.

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. Under alla omständigheter får underrättelseverksamheten 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 kap. 7.

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 tillgodogörande 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.

6 Kontrollfunktionen

6.1 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.

6.2 En förstärkt kontroll av försvarsunderrättelseverksamheten

Förslag: Försvarets underrättelsenämnd skall vara ett kontrollorgan för försvarsunderrättelseverksamheten.

Nämnden skall ge tillstånd till sådan närmare inriktning som anges i förslaget till lag om signalspaning.

Nämnden skall kontrollera efterlevnaden av förslaget till lag om signalspaning och särskilt granska användning av sökbegrepp och rapportering enligt den lagen.

Nämnden skall granska personuppgiftsbehandlingen i Försvarsmaktens försvarsunderrättelseverksamhet och den militära säkerhetstjänsten samt i Försvarets radioanstalts underrättelseverksamhet.

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.

Nämndens 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 skall därför ha till uppgift 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.

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. När det gäller förslagen i lagen om signalspaning beskrivs nämndens uppgifter närmare nedan.

I samband med överväganden om Försvarets radioanstalts arbetsmetoder har självfallet frågor om personlig integritet en central betydelse. Behovet av en effektiv verksamhet måste därför alltid ställas i relation till det eventuella integritetsintrång som kan befaras uppkomma. Det framstår därför som angeläget att frågor med anknytning till enskildas personliga integritet kan bli föremål för en rättssäker prövning. I avsnitt 7.3 behandlas de överväganden i fråga om nämndens organisation som detta föranleder.

Tillstånd till närmare inriktning enligt lagen om signalspaning

I förslaget till lag om signalspaning anges att de myndigheter som regeringen bestämmer får ge närmare inriktning av signalspaningsverksamheten. För att sådan närmare inriktning skall få ske måste ett tillstånd ges av Försvarets underrättelsenämnd. Det innebär att en myndighet som enligt föreskrift eller beslut har rätt att ange inriktning av signalspaningsverksamheten först måste vända sig till nämnden och avvakta dess prövning innan inriktningen kan lämnas till Försvarets radioanstalt. Nämnden skall pröva om inriktningen är förenlig med de villkor som anges i förslaget till lag om signalspaning.

Det kan emellertid uppstå situationer av så brådskande karaktär att ett tillstånd inte kan avvaktas utan att det skulle innebära allvarliga problem för myndigheternas verksamhet. I sådana situationer skall finnas en möjlighet att ge en närmare inriktning utan att tillstånd först inhämtats. Den myndighet som gett inriktningen skall i sådana fall i efterhand anmäla den givna inriktningen till Försvarets underrättelsenämnd, som skall göra en efterhandskontroll av inriktningens förenlighet med de angivna villkoren. Om inriktningen är oförenlig med lagens villkor skall nämnden rapportera detta, se avsnittet nedan om återrapportering.

Särskilt om kontroll enligt lagen om signalspaning

Utöver vad som anges i förslaget till ändring i lag om försvarsunderrättelseverksamhet skall Försvarets underrättelsenämnd kontrollera efterlevnaden av lagen om signalspaning.

Som angivits ovan har Försvarets underrättelsenämnd till uppgift att ge tillstånd till den närmare inriktningen av signalspaningsverksamheten. 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.

Vidare skall Försvarets underrättelsenämnd särskilt granska de sökbegrepp som Försvarets radioanstalt enligt vad som är närmare föreskrivet skall använda i inhämtningssystemen. Försvarets radioanstalt skall fortlöpande lämna en redogörelse till Försvarets underrättelsenämnd om vilka sökbegrepp som används. Nämnden skall fortlöpande granska dessa sökbegrepp och 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 rapporteringen av underrättelser som inhämtats genom signalspaning är förenlig med ändamålet för verksamheten såsom det formulerats i lagen om försvarsunderrättelseverksamhet och lagen om signalspaning.

Försvarets underrättelsenämnds återrapportering

Såsom framgår av 3 § i Försvarets underrättelsenämnds instruktion i dess nuvarande lydelse skall nämnden lämna de myndigheter som omfattas av lagen om försvarsunderrättelseverksamhet de synpunkter och de förslag till åtgärder som föranleds av granskningsverksamheten. Om det behövs, skall nämnden också lämna förslag om åtgärder till regeringen. Denna informationsskyldighet till regeringen bör utökas till att vid behov även omfatta de synpunkter som lämnas till myndigheterna.

Nämnden skall också senast den 1 mars varje år till regeringen lämna en rapport över föregående års granskningsverksamhet. Den kontrollverksamhet som avser tillstånd, sökbegrepp och rapportering av underrättelser vid Försvarets radioanstalt är av sådan karaktär att utfallet av granskningen skall rapporteras särskilt i den årliga rapporten. Rapporteringen i dessa frågor skall

därutöver göras till regeringen när nämnden anser det nödvändigt.

6.3 Nämndens organisation

Förslag: Nämnden skall utökas med en ledamot. Minst två av ledamöterna skall vara eller ha varit ordinarie domare.

För att kunna utföra en fortlöpande och mer ingående kontroll skall nämnden förstärkas med ett permanent kansli under ledning av en kanslichef.

Minst en av juristledamöterna skall närvara vid handläggningen av ärenden som avser tillstånd för närmare inriktning vid signalspaning.

Om det framkommer skiljaktiga meningar vid handläggning av tillståndsärenden skall reglerna i förvaltningslagen (1986:223) avseende omröstning tillämpas.

Nämnden skall fortlöpande bedriva en effektiv och ändamålsenlig kontroll av försvarsunderrättelseverksamheten. Med den organisation Försvarets underrättelsenämnd har i dag är förutsättningarna för en sådan granskning som föreslås begränsad. Vissa förändringar framstår därför som nödvändiga. Avsikten är att göra det möjligt för nämnden att bedriva en mer ingående kontroll av underrättelseverksamheten. Nämnden skall därför utökas med en ledamot.

Många av de frågor och överväganden som aktualiseras i nämndens verksamhet ställer krav på juridisk kompetens hos såväl nämndens ledamöter som dess kansli. Försvarets underrättelsenämnd har i dag en ledamot med domarkompetens. Med hänsyn till att nämnden skall besluta om tillstånd för inriktning av signalspaningsverksamheten och även granska sökbegreppen enligt lagen om signalspaning ökar behovet av sådan kompetens. För att de nya uppgifter som tillförs nämnden skall kunna hanteras med bibehållen hög rättsäkerhetsnivå skall det därför finnas minst två jurister i nämnden. Dessa skall vara eller ha varit ordinarie domare. Minst en av juristledamöterna

skall närvara vid handläggningen av ärenden som avser tillstånd för närmare inriktning vid signalspaning.

Om det framkommer skiljaktiga meningar vid handläggning av tillståndsärenden skall reglerna i förvaltningslagen (1986:223) avseende omröstning tillämpas.

För att kunna utföra en fortlöpande och mer ingående kontroll av underrättelseverksamheten skall nämnden ha ett permanent kansli. Kansliets personal bör ha god kunskap om underrättelsearbete och juridisk kompetens. Kansliet skall ledas av en kanslichef som utses av regeringen. Övriga anställningar hos kansliet beslutas av nämnden. För att understryka att kontrollverksamheten skall bedrivas fortlöpande bör den bestämmelse som i dag anger att nämnden skall ha minst fyra (4) sammanträden per år tas bort. Med ett permanent kansli och ett uttalat uppdrag att fortlöpande granska underrättelseverksamheten kommer en mer frekvent verksamhet än fyra nämndsammanträden per år följa som en naturlig konsekvens. Förändringarna innebär att nämnden kommer att ha kapacitet för att snabbt och rationellt kunna hantera de framställningar som kommer från olika myndigheter. Som en följd av att nämnden tillförs ett kansli bör ordföranden och kanslichefen på nämndens vägnar kunna pröva frågor om utlämnande av allmänna handlingar och överklagande av nämndens beslut.

Att nämnden bl.a. får ett fast kansli kommer att medföra vissa kostnadskonsekvenser. Beskrivning kring kostnadsaspekter finns i kap. 7.

7 Konsekvenser och genomförande

7.1 Inledning

Detta avsnitt behandlar organisatoriska och finansiella konsekvenser av de föreslagna författningarna.

7.2 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 kap. 5 har formerna för den beskrivits. Nedan följer en beskrivning av kostnaderna.

En initial installation av den tekniska utrustningen för en samverkanspunkt, samt det som behövs för att överföra signalen till Försvarets radioanstalt och för att processa signalerna bedöms röra sig om en investering på ca 35 miljoner kronor. Under en period av fyra år skulle sådana installationer behöva göras vid ytterligare minst två anläggningar för att uppnå önskad effekt.

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 i tre delar: utveckling, hårdvara samt lagringskapacitet. Kostnaderna för utveckling och hårdvara ligger i huvudsak under 2005-2006 och påverkas 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.

Driftkostnaderna består till största del av sambandskostnader samt lokalhyra för samverkanspunkter.

Sammantaget skulle de investeringar som hänför sig till att få tillgång till signaler i elektronisk form genomföras under en femårsperiod och uppgå till omkring 200 miljoner. Det första året skulle investeringarna uppgå till ca 30 miljoner kronor för att sedan successivt öka något under de följande fyra åren.

Genom sitt anslag finansierar Försvarets radioanstalt kapitalkostnaden för den teknikutveckling som behövs för dess verksamhet. Kapitalkostnaden för de beskrivna investeringarna skulle belasta anslaget med mellan 10 och 20 miljoner kronor per år under avskrivningstiden. Därefter kommer resursbehovet att avse vidmakthållande av förmågan, vilket får ske inom gängse ramar för Försvarets radioanstalts verksamhet.

De ökade kostnaderna för trådaccess finansieras genom omprioriteringar inom utgiftsområde 6. Försvar samt beredskap mot sårbarhet.

För Försvarets radioanstalt bedöms inte den föreslagna regleringen medföra några organisatoriska konsekvenser.

7.3 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 ett permanent kansli. Detta har beskrivits i kap. 6.

Med beaktande av underrättelsenämndens avgränsade ansvarsområde, organisationens ringa storlek och för att vinna ekonomiska och administrativa fördelar bör Försvarets

underrättelsenämnd ombildas till en nämndmyndighet och knytas till en värdmyndighet. Nämndens ansvar och uppgifter bör beslutas av regeringen och framgå av värdmyndighetens instruktion. Nämndens ledamöter samt dess kanslichef bör utses av regeringen. Värdmyndigheten bör liksom Försvarets underrättelsenämnd sortera under Försvarsdepartementet, men bör med hänsyn till övervakningsfunktionens krav på integritet inte vara en av de myndigheter som kommer att granskas av nämnden. Värdmyndigheten och Försvarets underrättelsenämnd bör heller inte ha en stark personalunion. Den bör slutligen ligga inom rimligt avstånd till de granskade myndigheterna, dvs. i Stockholmsområdet.

Värdmyndigheten bör ansvara för Försvarets underrättelsenämnds lokaler, personal och administrativa funktioner.

Lokalerna behöver inrymma kanslipersonalen, ordföranden samt ev. tillkommande experter. Det behöver finnas gemensamma utrymmen samt konferensrum, kommunikationer och arkiv. Kraven på tillträdesskydd blir höga. Detta kan dock åstadkommas i de flesta fastigheter, även i sådana som i dag har låg skyddsnivå.

Merkostnaderna för kanslifunktionen uppskattas till mellan fem och tio miljoner per år, något högre det första året p.g.a. initiala investeringar. Nämndens anslag år 2005 uppgår till 1 miljon kronor och skulle således behöva höjas. Detta bör ske genom överföringar av anslag från de myndigheter som nämnden granskar, dvs. försvarsunderrättelsemyndigheterna.

Värdmyndigheten bör ges i uppdrag från regeringen att organisera de administrativa formerna för verksamheten.

7.4 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 att innebära att myndigheten kan komma att utöva tillsyn och meddela föreskrifter inom området. Denna verksamhet och dess kostnader bedöms vara av mindre omfattning och bör därför kunna inrymmas i myndighetens ordinarie verksamhet. Om så inte skulle vara fallet får kostnaderna istället finansieras genom höjda tillsynsavgifter enligt lagen om elektronisk kommunikation.

7.5 Operatörer

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 kap. 5 beskrivs operatörernas skyldigheter.

Att göra en exakt uppskattning av kostnaderna för de trådägande teleoperatörerna i syfte att göra den trafik som passerar rikets gräns tillgänglig för Försvarets radioanstalt är 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.

En betydelsefull omständighet att beakta vid valet av vem som skall stå för kostnaden att styra ut trafiken är 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 upphandlare av de hård- och mjukvaror som krävs

påverka priset på ett annat sätt än vad Försvarets radioanstalt 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 sina system till samverkanspunkterna. I och med att de trådägande operatörerna har ett incitament att överföra trafiken till så låg kostnad som möjligt kommer de, om de har ansvaret att hitta det mest kostnadseffektiva sättet, att överföra trafiken till samverkanspunkterna.

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 telekommunikationsutrustning är hög och att huvuddelen av utrustningen inom en femårsperiod kan förväntas 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 stycke).

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).

Utöver detta tillkommer vissa mindre kostnader för att trafiken enkelt skall kunna tas omhand, vilket omfattar såväl trådägare som andra operatörer. Dessa kostnader är ringa eftersom det rör sig om att överföra sådan (kring-) information som operatörerna redan har i sina system. Det finns heller inget krav på att denna information skall anpassas.

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 år 2005 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 teleoperatör som har 20 % 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).

7.6 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.

8 Författningskommentarer

8.1 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 förhållandet till paragrafens nuvarande lydelse har ordningsföljden ändrats på de politikområden som försvarsunderrättelseverksamheten skall bedrivas till stöd för. 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 gränsöverskridande brottslighet med säkerhetspolitiska konsekvenser omfattas av underrättelseverksamheten. 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 täcks av uttrycket ”yttre hot mot landet” är beskrivningen överflödig 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 4.3.2.

Andra stycket första meningen har inte ändrats. *Andra meningen* är ny. Där regleras de behovsställande myndigheternas möjlighet att närmare inrikta försvarsunderrättelseverksamheten inom den ram som regeringen fastställt. Frågan behandlas i avsnitt 4.4.

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 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. I styckets *sista mening* som är ny anges de två primära metoderna för inhämtning av försvarsunderrättelser, teknisk och personbaserad inhämtning. Se vidare avsnitt 4.4.

Andra stycket, som är nytt, hänvisar till lagen om signalspaning. Signalspaning utgör teknisk inhämtning. Se avsnitt 5.3.1.2.

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 i det nuvarande första stycket har fått en delvis annan lydelse och ett nytt andra stycke har förts in i paragrafen. Ändringen i *första stycket* innebär att försvarsunderrättelseverksamheten inte skall få innefatta åtgärder som ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande arbete såsom det bestämts i andra lagar och föreskrifter.

I andra stycket anges att inskränkningen för försvarsunderrättelseverksamheten som uppställs i paragrafens första stycke inte gäller när verksamheten, utan att avse fysisk person, bedrivs för kartläggning av förhållanden utomlands som innebär yttre hot. Genom bestämmelsen markeras att avgränsningen mot den polisiära verksamheten inte skall hindra att försvarsunderrättelseverksamheten ändå kan inriktas mot yttre hot i form av kriminalitet så länge som den inte bedrivs på ett sätt som kan jämföras med de polisiära myndigheternas mera personinriktade underrättelseverksamhet. Paragrafen har behandlats närmare i avsnitt 4.3.2.

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 kap. 6.

8.2 Förslag till förordning om ändring i förordningen (2000:131) om försvarsunderrättelseverksamhet

1 §
Paragrafen har ändrats. Förordningen (2000:131) om försvarsunderrättelseverksamhet innehåller med de ändringar som nu föreslås dels verkställighetsföreskrifter till lagen (2000:130) om försvarsunderrättelseverksamhet, dels bestämmelser som anknyter till denna lag och som regeringen meddelat med stöd av den s.k. restkompetensen. Ändringen avspeglar detta förhållande.

2 §
Första stycket har ändrats på så sätt att förordningstexten anger samtliga de myndigheter som skall bedriva försvarsunderrättelseverksamhet. Ändringen är en följd av den föreslagna lydelsen av 1 § tredje stycket lagen (2000:130) om försvarsunderrättelseverksamhet.

Andra stycket är nytt. Där anges vilka myndigheter som får bedriva inhämtning med särskilda metoder enligt 2 § lagen om försvarsunderrättelseverksamhet (Försvarsmakten och Försvarets radioanstalt). Vidare görs en hänvisning till förordningen (2006:000) om signalspaning, i vilken Försvarets radioanstalt pekas ut som den myndighet som får bedriva teknisk inhämtning enligt lagen (2006:000) om signalspaning.

5 §
Ändringen i *första stycket* har sin grund i de förändringar som föreslås i lagen (2000:130) om försvarsunderrättelseverksamhet, innebärande ett utvidgat mandat som också föranleder en förstärkt kontroll. Samtliga försvarsunderrättelsemyndigheter skall nu underrätta Försvarets underrättelsenämnd i frågor som rör försvarsunderrätteleverksamhet om frågorna är principiella

eller annars av större vikt, och under förutsättning att inte verksamheten därigenom avsevärt försvåras.

Även *andra stycket* har ändrats av det skäl som nämnts ovan. Enligt bestämmelsen skall både Försvarsmakten och Försvarets radioanstalt informera nämnden om de interna bestämmelser som gäller för den verksamhet som inhämtar underrättelser med särskilda metoder.

6 §

I bestämmelsens *första stycke* har *sista meningen* utgått. Detta är en följd av en ändring i 5 § första stycket denna förordning.

Andra och *tredje stycket* har inte ändrats.

8.3 Förslag till förordning om ändring i förordningen (1988:552) med instruktion för Försvarets underrättelsenämnd

Ändringarna i Försvarets underrättelsenämnds instruktion grundar sig i behovet av att förstärka nämnden till följd av att nämnden enligt förslaget till ändring i lagen (2000:130) om försvarsunderrättelseverksamhet skall kontrollera försvarsunderrättelseverksamheten.

Genom förändringarna tillförs nämnden ytterligare en ledamot. Minst två av ledamöterna skall vara eller ha varit ordinarie domare. Vidare stärks nämnden genom att tillföras ett kansli som leds av en kanslichef. Särskilda regler om handläggning av tillstånd enligt lagen om signalspaning införs i instruktionen.

8.4 Förslag till lag om signalspaning

1 §

Inhämtning av signaler i elektronisk form vid signalspaning är en sådan särskild metod för teknisk och personbaserad inhämtning som nämns i lagen (2000:130) om försvarsunderrättelse-

verksamhet. Paragrafen beskriver när, d.v.s. för vilka syften, sådan inhämtning får bedrivas. 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 5.3.2.

I paragrafens *första stycke* slås fast att signaler i elektronisk form får inhämtas för den verksamhet som anges i 1 § lagen (2000:130) om försvarsunderrättelseverksamhet. Det innebär att inhämtning får ske för försvarsunderrättelseverksamhet, d.v.s. 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. Verksamheten får endast avse utländska förhållanden. Beträffande försvarsunderrättelseverksamhet, se vidare avsnitt 5.3.1.2. och kommentaren till de förslagna ändringarna i lagen (2000:130) om försvarsunderrättelseverksamhet, avsnitt 8.1.

Inhämtningen enligt denna lag skall emellertid även få bedrivas för vissa andra särskilda syften som inte omfattas av försvarsunderrättelseverksamheten, se avsnitt 5.3.1.2. 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 verksamheten. Vad som regleras i detta stycke finns idag i förordningen med instruktion för Försvarets radioanstalt, och överförs nu till lagen. Se avsnitt 5.3.1.2.

Eftersom inhämtning som sker med stöd av andra stycket inte utgör försvarsunderrättelseverksamhet omfattas den inte av lagen (2000:130) om försvarsunderrättelseverksamhet. Huvuddelen av de begränsningar som uppställs i lagen om signalspaning gäller dock även för denna inhämtning, se avsnitt 5.3.1.2.

2 §

Av paragrafen framgår att inhämtning som sker i tråd endast får avse signaler vilka förs över Sveriges gräns av operatörer som äger tråd. 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 5.3.1.3 och i avsnitt 5.3.2.3.

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. 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. Paragrafens två första meningar behandlas i avsnitt 5.3.1.4. I *tredje meningen* slås fast att sökbegreppen inte får vara direkt hänförliga till viss fysisk person såvida det inte är av synnerlig vikt för verksamheten. Meningen behandlas i avsnitt 5.4.1.2.

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

4 §

Paragrafen slår fast att den myndighet som regeringen bestämmer (Försvarets radioanstalt) får bedriva inhämtning enligt 1 §.

5 §

I paragrafens *första stycke* erinras om att regeringens och myndigheters inriktning av sådan signalspaning som är försvarsunderrättelseverksamhet regleras i lagen (2000:130) om försvarsunderrättelseverksamhet. I *andra stycket* finns bestämmelser om att sådan signalspaningsverksamhet som *inte* är försvarsunderrättelseverksamhet skall inriktas av regeringen. Se avsnitt 5.3.1.5.

6 §

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 Regeringskansliet. Tillståndet lämnas av den myndighet som regeringen bestämmer (Försvarets underrättelsenämnd). 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 vara förenlig med lagen (2000:130) om försvarsunderrättelseverksamhet. Tillstånd får inte ges för inriktning som endast avser en fysisk person. Signalspaningsverksamheten måste dock i vissa fall beröra enskildas kommunikationer för att det skall vara möjligt att följa en viss företeelse av relevans för verksamheten.

I *andra stycket* begränsas skyldigheten att inhämta tillstånd. Tillstånd krävs inte om det skulle innebära en väsentlig olägenhet för den inriktande myndighetens verksamhet att avvakta tillståndet. Om en närmare inriktning givits utan tillstånd skall den omedelbart anmälas till den myndighet som har att lämna tillstånd (Försvarets underrättelsenämnd). Om tillståndsmyndigheten finner att tillstånd till inriktning inte borde ha verkställts skall Försvarets radioanstalt underrättas och inhämtningen omedelbart avbrytas.

Bestämmelsen behandlas i avsnitt 5.4.1.3.

7 §

Upptagning eller uppteckning av uppgifter som erhållits genom inhämtning enligt lagen skall omgående förstöras om uppgiften bedömts sakna betydelse för den verksamhet som avses i 1 §, d.v.s. för försvarsunderrättelseverksamheten eller för den verksamhet som beskrivs i 1 § andra stycket 1-2. Detta gäller givetvis oavsett om inhämtningen skett med hjälp av automatiserad behandling eller med manuella metoder. Motsvarande gäller om upptagningen eller uppteckningen 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. Bestämmelsen behandlas i avsnitt 5.4.1.4.

8 §

I paragrafens *första mening* erinras om att rapportering av underrättelser som erhållits vid signalspaning i försvarsunderrättelseverksamheten regleras i lagen (2000:130) om försvarsunderrättelseverksamhet. Av 2 § första stycket i förslaget till ändringen i den lagen framgår att sådana underrättelser skall rapporteras till berörda myndigheter. Den verksamheten som sker med stöd av 1 § andra stycket lagen om signalspaning syftar till att tillgodose myndighetens egna behov och resulterar inte i några direkta underrättelser. De omfattas därför inte av bestämmelsen. Första meningen behandlas i avsnitt 5.3.1.5. I *andra meningen* görs en begränsning av vad som får rapporteras från signalspaningsverksamhet. Där anges att rapporteringen endast får omfatta förhållanden som är av betydelse i de hänseenden som anges i 1 §. Begränsningen behandlas i avsnitt 5.4.1.5.

9 §

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 5.3.1.5.

10 §
Enligt paragrafen skall en myndighet som utses av regeringen (Försvarets underrättelsenämnd) kontrollera efterlevnaden av lagen. De sökbegrepp som avses i 3 § och den rapportering som avses i 8 § skall granskas särskilt. Bestämmelsen behandlas i avsnitt 5.3.1.5 och kap. 6.

11 §
Paragrafen innehåller en hänvisning till de bestämmelser i lagen (2003:389) om elektronisk kommunikation som reglerar operatörernas skyldighet att överföra trafik för att möjliggöra inhämtning enligt lagen (2006:000) om signalspaning. Se avsnitt 5.3.2.3 och kommentaren till de föreslagna ändringarna i lagen om elektronisk kommunikation, avsnitt 8.5.

12 §
I paragrafen slås fast att beslut som fattas enligt lagen om signalspaning inte får överklagas.

8.5 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 (2006:000) om signalspaning föreskriver den vissa skyldigheter för de s.k. operatörerna. Skyldigheterna avseende överföring m.m. gäller endast sådana signaler som förs över Sveriges gräns. Beträffande övervägandena i denna del, se avsnitt 5.3. 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. Samverkanspunkterna skall, sedan de trådägande operatörerna utsett dem, anmälas till den myndighet regeringen bestämmer (Försvarets radioanstalt). En samverkanspunkt är en plats, där trafiken överlämnas från den trådägande operatören till myndigheten, se avsnitt 5.3.2.3. 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 se till att signalerna enkelt kan tas om hand. 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.

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 (2006:000) om signalspaning. 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.

Ikraftträdande

Lagändringarna träder ikraft 1 juli 2006. För de operatörer som äger tråd föreskrivs en skyldighet att föra signalerna till samverkanspunkter. Denna skyldighet träder ikraft 1 januari 2007, vilket innebär att dessa operatörer har sex månader på sig att efter lagens ikraftträdande att 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 5.3.2.3.

Departementsserien 2005

Kronologisk förteckning

1. Finansiella konglomerat. Fi.
2. Kungörande i PoIT. Redovisning av uppdrag om elektroniskt kungörande. Ju.
3. Svensk rätt i integrationspolitisk belysning. Ju.
4. Avräkning av utländsk skatt. Fi.
5. Angrepp mot informationssystem. Ju.
6. Brott och brottsutredning i IT-miljö. Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll. Ju.
7. Iakttagelser om landsting. Fi.
8. Inriktning på filmpolitiken från 2006. U.
9. En moderniserad rättsprövning, m.m. Ju.
10. Arbetstagarinflytande i europakooperativ. N.
11. Den europeiska exekutionstiteln för obestridda fordningar. Ju.
12. Makten och mångfalden. Eliter och etnicitet i Sverige. Ju.
13. Försäkringsbolags tillgång till patientjournaler. Ju.
14. Olovlig befattning med narkotikaprekursorer. EU:s rambeslut om olaglig narkotikahandel. Ju.
15. Förstärkning och förenkling – ändringar i anställningsskyddslagen och föräldraledighetslagen. N.
16. Att fånga kunnandet om lärande och undervisning. Om villkoren för skolledare och lärare att ta del av systematiskt framtagen kunskap om utbildningsverksamhet. U.
17. Internationell insolvens. Ju.
18. Säkerhet i vägtunnlar. N.
19. De projektbaserade mekanismerna enligt Kyotoprotokollet och länkdirektivet. M.
20. Svenskt värdskap för ESS. U.
21. Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet. Ju.
22. Småskalig livsmedelsförädling. Jo.
23. Ett förnyat strandskydd. M.
24. Tidsbegränsat uppehållstillstånd för offer för människohandel m.fl. UD.
25. Förhandsavgörande från EG-domstolen. Ju.
26. Utökat informationsutbyte mellan arbetslöshetskassorna och inom Arbetsmarknadsverkets verksamhet. N.
27. Arbetsgivares informationsskyldighet – ändringar i anställningsskyddslagen. N.
28. Skattefusk, effektivitet och rättvisa – utökad skattekontroll i vissa branscher och diskussioner rörande schabloniserade inslag i beskattningen. Fi.
29. Förslag om ett utvecklat elcertifikatsystem. M.
30. En anpassad försvarsunderrättelseverksamhet. Fö.

Departementsserien 2005

Systematisk förteckning

Justitiedepartementet

Kungörande i PoIT. Redovisning av uppdrag om elektroniskt kungörande. [2]
Svensk rätt i integrationspolitisk belysning. [3]
Angrepp mot informationssystem. [5]
Brott och brottsutredning i IT-miljö. Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll. [6]
En moderniserad rättsprövning, m.m. [9]
Den europeiska exekutionstiteln för obestridda fordningar. [11]
Makten och mångfalden. Eliter och etnicitet i Sverige. [12]
Försäkringsbolags tillgång till patientjournaler. [13]
Olovlig befattning med narkotikaprekursorer. EU:s rambeslut om olaglig narkotikahandel. [14]
Internationell insolvens. [17]
Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet. [21]
Förhandsavgörande från EG-domstolen. [25]

Utrikesdepartementet

Tidsbegränsat uppehållstillstånd för offer för människohandel m.fl. [24]

Försvarsdepartementet

En anpassad försvarsunderrättelseverksamhet. [30]

Finansdepartementet

Finansiella konglomerat. [1]
Avräkning av utländsk skatt. [4]
Iakttagelser om landsting. [7]
Skattefusk, effektivitet och rättvisa – utökad skattekontroll i vissa branscher och diskussioner rörande schabloniserade inslag i beskattningen. [28]

Utbildnings- och kulturdepartementet

Inriktning på filmpolitiken från 2006. [8]
Att fånga kunnandet om lärande och undervisning. Om villkoren för skolledare och lärare att ta del av systematiskt framtagen kunskap om utbildningsverksamhet. [16]
Svenskt värdskap för ESS. [20]

Jordbruksdepartementet

Småskalig livsmedelsförädling. [22]

Miljö- och samhällsbyggnadsdepartementet

De projektbaserade mekanismerna enligt Kyotoprotokollet och länkdirektivet. [19]
Ett förnyat strandskydd. [23]
Förslag om ett utvecklat elcertifikatsystem. [29]

Näringsdepartementet

Arbetstagarinflytande i europakooperativ. [10]
Förstärkning och förenkling – ändringar i anställningsskyddslagen och föräldraledighetslagen. [15]
Säkerhet i vägtunnlar. [18]
Utökat informationsutbyte mellan arbetslöshetskassorna och inom Arbetsmarknadsverkets verksamhet. [26]
Arbetsgivares informationsskyldighet – ändringar i anställningsskyddslagen. [27]