Kartläggning av förutsättningar för delgivning av hemlig information

MAGNUS NORMARK, PER THUNHOLM, RUNAR VIKSTEN

FOI-R--4418--SE
ISSN 1650-1942 April 2017

Magnus Normark, Per Thunholm, Runar Viksten

Kartläggning av förutsättningar för delgivning av hemlig information

Titel	Kartläggning av förutsättningar för delgivning av hemlig information
Title	Mapping conditions for sharing confidential information between national authorities
Rapportnr/Report no	FOI-R--4418--SE
Månad/Month	April
Utgivningsår/Year	2017
Antal sidor/Pages	50
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	2. CBRN-frågor och icke-spridning
FoT-område	
Projektnr/Project no	E4280
Godkänd av/Approved by	Åsa Scott
Ansvarig avdelning	CBRN-skydd och säkerhet

Omslagsbild: iStockphoto, gjord av maxsattana

Sammanfattning

Denna rapport utgör resultatet av en studie som syftat till att kartlägga nationella förutsättningar för att hantera behovet av informationsdelgivning mellan underrättelse- och säkerhetstjänsterna och den breda kretsen av krisberedskapsmyndigheter avseende allvarliga antagonistiska hot.

Studien är fokuserad på relationer och förutsättningar för informationsdelning mellan centrala nationella underrättelse- och säkerhetstjänster visavi krisberedskapsmyndigheter. Verksamheten grundar sig på en genomgång av relevant regelverk samt dess förarbeten, strategiska dokument och inte minst intervjuer med representanter från nio centrala nationella myndigheter. Studiens resultat har en relevans och aktualitet i ljuset av det omfattande arbete som pågår inom regeringskansliet, Försvarsmakten och civila krisberedskapsmyndigheter avseende stärkande av samhällets förmåga att förebygga och hantera antagonistiska hot och angrepp av allvarlig karaktär inom ramarna för totalförsvarskonceptet.

En majoritet av de myndigheter som denna studieverksamhet interagerat med har gett uttryck för ett ökat behov av effektivare och utökad delgivning av underrättelser mellan nationella myndigheter. Detta behov bedöms öka i framtiden, bl.a. som en effekt av upprättandet av ett totalförsvarskoncept och ett påtagligt försämrat omvärldsläge. Bilden av hur existerande förutsättningar står i förhållande till detta utökade behov av samverkan och informationsdelning är mångfacetterad.

Baserat på den information och de perspektiv som inhämtats kan författarna konstatera att det finns ett etablerat nationellt regelverk som medger delgivning av underrättelser mellan nationella myndigheter under sådana omständigheter som denna studie syftar till att belysa. Det kan även konstateras att det existerar ett antal faktorer som begränsar förutsättningarna att utveckla informationsdelgivning i den riktning som en majoritet av de myndigheter som denna studie interagerat med anser är av stor vikt för att identifiera och möta existerande antagonistiska hot och säkerhetsutmaningar. Till dessa faktorer hör bristande gemensamma tekniska system för informationsöverföring, kulturella skillnader, begränsade resurser, avgränsade mandat samt en tydlig sektorsgräns mellan underrättelsesystemet och övriga myndigheter.

En grundläggande översyn behöver göras avseende hur det svenska systemet för underrättelseproduktion och delgivning kan utvecklas i ljuset av den trend av ökade behov och efterfrågan som råder, med hänsyn taget även till de centrala krisberedskapsmyndigheter som inte tillhör den existerande kretsen av myndigheter med inriktningsrätt. Detta gäller inte minst om tilldelade resurser i termer

av tekniska system för inhämtning, bearbetning och delgivning liksom tillgång till arbetskraft för den underrättelseproducerande verksamheten behöver förstärkas.

Nyckelord: underrättelsetjänst, underrättelser, sekretess, totalförsvar, krisberedskap, samverkan, informationsdelning, antagonistiska hot, kommunikation

Summary

This report constitutes the result of a study with the overall aim to identify current conditions for sharing confidential information between national authorities. The primary focus of this study is to bring forward the current state of capabilities and thresholds affecting national interagency cooperation in dealing with serious threats through sharing and coordinating classified information. This effort is carried out through an initial review of relevant regulations setting the framework for the work of the authorities with intelligence and other classified information as well as strategic government documents for the national intelligence system. The analysis and conclusions in this report are furthermore based on interviews and dialogue with representatives from nine authorities.

There is a common perception between the authorities of an increasing demand on dynamic and flexible information sharing in order to deal with current threats and security challenges. The authors of this report conclude that current regulations provide a good framework for sharing classified information between authorities but that there exists a range of different factors limiting the abilities to share information in an effective, dynamic and flexible manner, as required by the contemporary trend of escalating security challenges of increasingly complex nature. Some of the most pressing challenges are to develop a joint national information sharing system for classified information, confidence-building measures between intelligence agencies and the broader sector of relevant authorities, better transparency regarding mandates, resources and priorities limiting the ability to share classified information. There is therefore a pressing need for the Swedish government to initiate a comprehensive and in-depth review of how the national intelligence production system can adapt to an increasing demand of information from a broader set of authorities in the current threat environment.

Keywords: Intelligence, secret, classified, information sharing,
inter-agency co-operation

Innehåll

1 Inledning

Denna rapport utgör resultatet av studieverksamhet som genomförts av Totalförsvarets forskningsinstitut (FOI) i samverkan med Centrum för asymmetriska hot och terrorismforskning (CATS) vid Försvarshögskolan. Studien har finansierats av Myndigheten för samhällsskydd och beredskap (MSB) och genomförts under perioden april-december 2016.[1]

1.1 Bakgrund

Initiativet till denna studie grundar sig på resultatet av den tidigare genomförda FOI-studien Krisberedskap och antagonistiska CBRN-hot; förutsättningar för nationell samverkan mellan underrättelsesektorn och krisberedskapssystemet. Studien slutrapporterades i oktober 2014.

Studien från 2014 visar att det råder en klyfta mellan försvarsunderrättelse- och säkerhetstjänsterna och den breda kretsen av krisberedskapsmyndigheter med ansvar inom CBRN-området. Denna klyfta präglas bl.a. av strukturella barriärer där tjänsterna saknar konkreta instruktioner och uppdrag att stödja den bredare kretsen av myndigheter med underlag och där myndigheternas strategiska kontinuerliga riskbedömningsverksamhet är förhållandevis snävt avgränsat till myndigheternas individuella perspektiv. Detta medför att förutsättningarna för en utvecklad samverkan mellan tjänster och myndigheter i syfte att stärka samhällets förmåga att förebygga, upptäcka och hantera antagonistiska hot och kriser av allvarlig karaktär är bristfälliga.

En utveckling mot att stärka relationerna mellan tjänster och myndigheter inom detta område kräver åtgärder inom regeringen och regeringskansliet, tjänsterna och inte minst bland krisberedskapsmyndigheterna. Åtgärder som skulle kunna stödja en sådan utveckling behöver dock baseras på befintliga regelverk och strategiska inriktningar inom området. Av denna anledning har vi i denna studie genomfört, och till stor del utgått ifrån, en kartläggning av relevant nationell regelverk samt tolkning och implementering av dessa i sammanhang som berör delgivning av hemlig information mellan nationella myndigheter. Den övergripande ambitionen i studien är att lyfta perspektiv på existerande förutsättningar för informationsdelgivning till diskussion och att identifiera områden där åtgärder skulle kunna vidtas för att stärka förutsättningarna för samverkan mellan underrättelse- och säkerhetstjänster och en bredare krets av berörda myndigheter. Resultatet från studien har en relevans och aktualitet i ljuset av det omfattande

[1] M. Normark och F. Lindvall ”Krisberedskap och antagonistiska CBRN-hot; förutsättningar för nationell samverkan mellan underrättelsesektorn och krisberedskapssystemet”, FOI-RH--1460--SE, oktober 2014.

arbete som pågår inom regeringskansliet, Försvarsmakten och civila krisberedskapsmyndigheter avseende stärkande av samhällets förmåga att förebygga och hantera antagonistiska hot och angrepp av allvarlig karaktär inom ramen för totalförsvarskonceptet.

1.2 Studiens syfte och genomförande

Denna studie syftar till att kartlägga nationella förutsättningar för att hantera behovet av informationsdelgivning mellan underrättelse- och säkerhetstjänsterna och den breda kretsen av krisberedskapsmyndigheter avseende allvarliga antagonistiska hot.

De frågeställningar som vi sökt svar på är följande:

- I vilken utsträckning är identifierade brister inom CBRN-området generiska och överförbara på den övergripande nationella samverkan mellan sektorerna avseende delgivning av underrättelsebaserad information?
- Vilka juridiska förutsättningar finns för att framföra informationsbehov och för delgivning av underrättelsebaserad information mellan sektorerna?
- Utifrån de juridiska förutsättningarna för informationsdelning, vilka interna processer finns för att tillämpa sådan samverkan mellan sektorerna?

Genom att presentera svaren på ovanstående frågeställningar bidrar studien till att ge en tydligare bild över existerande förutsättningar för informationsdelning mellan underrättelse- och säkerhetssektorn visavi krisberedskapssektorn. Detta resultat utgör en vital förutsättning för att därefter identifiera och rekommendera relevanta åtgärder på central nationell nivå för att stärka framtida informationsdelning mellan sektorerna.

1.2.1 Metod och genomförande

Verksamheten har genomförts under 2016 under ledning av FOI och i samverkan med CATS vid Försvarshögskolan.

Studieverksamheten har genomförts i tre olika faser. Den första fasen har innefattat en genomgång av befintliga relevanta lagtexter och dess förarbeten samt tillgänglig litteratur avseende den strategiska styrningen av den nationella underrättelseverksamheten under de senaste 16 åren som är av relevans för studiens syfte.

Studiens andra verksamhetsfas har inkluderat inhämtning av perspektiv från ett urval av berörda tjänster och myndigheter avseende tolkning och tillämpning av

befintliga regelverk samt perspektiv på existerande förutsättningar för delgivning av hemlig information. Denna informationsinhämtning har genomförts genom enkäter med frågeställningar som tillställts berörda myndigheter, vars enkätsvar därefter kompletterats med intervjuer.

Följande myndigheter har responderat på studiens frågeställningar:

- Försvarets Radioanstalt (FRA)
- Kustbevakningen
- Migrationsverket
- Militära underrättelse- och säkerhetstjänsten (Must)
- MSB
- Polismyndigheten
- Säkerhetspolisen
- FOI
- Tullverket

Sista fasen av verksamheten har koncentrerats till dokumentation och rapportskrivning.

1.2.2 Avgränsningar

Studien är fokuserad på relationerna och förutsättningar för informationsdelning mellan centrala nationella underrättelse- och säkerhetstjänster visavi krisberedskapsmyndigheter. Detta innebär bl.a. att studien inte beaktat kontext relaterad till regionala och lokala aktörer eller myndigheters relationer med regeringskansliet annat än ur ett styrningsperspektiv.

Verksamheten är strikt begränsad till nationella förhållanden och förutsättningar, vilket innebär att studien inte beaktat myndigheters samverkan med partners i andra länder.

Denna studie har inte identifierat specifika tillämpningar eller åtgärder för ett utvecklat effektivt informationsutbyte mellan sektorerna.

2 Strategisk inriktning av svensk underrättelseverksamhet

I 2015 års inriktningsproposition betonar regeringen att det *”enskilt viktigaste under försvarsinriktningsperioden 2016 t.o.m. 2020 är att öka den operativa förmågan i krigsförbanden och att säkerställa den samlade förmågan i totalförsvaret”*. Det ställer förändrade krav på totalförsvaret och har sin bakgrund i det av regeringen konstaterade påtagligt försämrade omvärldsläget.

Den negativa utvecklingen aktualiserar enligt regeringen också behovet av en förstärkt försvarsunderrättelseförmåga, ett psykologiskt försvar anpassat efter dagens förhållanden m.m. Regeringen konstaterar också att försvarsunderrättelse- och cyberförsvarsförmågan är centrala för detta nya och osäkrare säkerhetspolitiska läge. Detta dels för att kunna skydda vitala system från angrepp, dels mer allmänt kunna vidmakthålla den svenska försvarsförmågan liksom möjligheterna för Sverige att föra en självständig och aktiv säkerhets-, utrikes- och försvarspolitik.

Den försämrade säkerhetspolitiska situationen visar tydligt på behovet av en god svensk förmåga att inhämta, bearbeta, analysera och delge försvarsunderrättelser och regeringen konstaterade också i inriktningspropositionen att försvarsunderrättelseförmågan ska förstärkas. Bland flera områden lyfts påverkanskampanjer som utgör ett brett spektrum av olika verksamheter och som används såväl i fredstid som i krig och som berör flera svenska myndigheter. Sverige ska även inom detta område kunna identifiera och möta just påverkanskampanjer, vilket måste kunna hanteras av berörda myndigheter och aktörer såväl under fredstida förhållanden som vid höjd beredskap.[2]

Försvarsunderrättelseverksamhet[3] syftar till att ge stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Sedan 2000 har Sverige också en lag om försvarsunderrättelseverksamhet, vilket det kommer att redogöras närmare för i nästa kapitel. Regeringen bestämmer försvarsunderrättelseverksamhetens inriktning och inom ramen för denna inriktning får också de myndigheter som regeringen bestämmer ange en närmare inriktning. Verksamheten bedrivs genom inhämtning, bearbetning och analys av information vilket leder till underrättelser som ska rapporteras till berörda myndigheter.[4]

[2] Prop. 2014/15:109
[3] Det är regeringen som bestämmer vilka myndigheter som ska bedriva Försvarsunderrättelseverksamhet och det är Försvarsmakten (Must), FRA, FOI och FMV.
[4] Lag (2000:130) om försvarsunderrättelseverksamhet.

Utöver försvarsunderrättelseverksamhet brukar Säkerhetspolisen och Polismyndigheten (NOA) omnämnas som underrättelseproducenter. Denna underrättelseverksamhet är till skillnad från försvarsunderrättelseverksamheten främst inriktad på att stödja det egna brottsförebyggande och brottsbekämpande arbetet och har inte heller en inriktning från regeringen på samma sätt som försvarsunderrättelseverksamheten. Därtill särskiljer sig Säkerhetspolisen och NOA jämfört med försvarsunderrättelsemyndigheterna genom att de inte har ett uppdrag att kommunicera sin kunskap genom en kontinuerlig produktion av underrättelserapporter. Deras underrättelseproduktion kommer istället mer indirekt övriga myndigheter till del genom myndighetssamverkan. De kan t.ex. genom analyser och rekommendationer stödja svenska myndigheter om hur de kan anpassa sitt skydd.

3 Regelverk för delgivning av sekretess mellan myndigheter

Enligt uppdraget ska en kartläggning göras av det nationella regelverk som styr delgivning av underrättelsebaserad information och behovsframställan. Det torde ligga i sakens natur att underrättelsebaserad information skyddas av sekretessregler och är hemlig. Öppen information är lätt tillgänglig för dem som behöver den och skyddas inte av några sekretessregler. En annan sak är att även hantering av öppna uppgifter under vissa förhållanden kan komma att omfattas av brott mot rikets säkerhet.

Enligt 2 kap. 1 § tryckfrihetsförordningen följer att varje svensk medborgare har rätt att ta del av allmänna handlingar som inte är hemliga. Rätten är inte begränsad till fysiska personer. Myndigheter och andra organ har enligt olika regelverk långtgående skyldigheter att medverka till att principen om allmänna handlingars offentlighet upprätthålls. Dessa regler kommer inte att beröras i det följande eftersom det är underrättelsebaserad information och hemliga handlingar som ligger i fokus. Vad som ska innefattas i ”underrättelsebaserad” är inte helt självklart. I första hand åsyftas i denna redovisning icke öppen information som inhämtats av något organ som har till uppgift att inhämta sådan information, t.ex. en försvarsunderrättelsemyndighet eller Säkerhetspolisen.

Även andra myndigheter ägnar sig dock åt att genom omvärldsbevakning eller på annat sätt inhämta information som ibland kan vara hemlig och hos myndigheten träffas av sekretessregler oavsett var informationen har sitt ursprung. Genomgången syftar till att ta upp de väsentligaste reglerna för överlämnande av underrättelsebaserad hemlig information mellan myndigheter. Även om uppdraget ställer krav på fullständighet är det inte möjligt att inom ramen för ett arbete av detta slag ta upp samtliga regler som kan vara av någon betydelse. Begränsningar måste även ske med hänsyn till att vi inom projektet i huvudsak använt oss av öppen information.

Det som i första hand tilldrar sig intresse är i vad mån information från myndigheter inom de stora områdena för inhämtning av hemligt material, dvs. försvarsunderrättelseverksamheten och det polisiära fältet, kan delges andra myndigheter. Givetvis är det också intressant att veta i vad mån regelverken tillåter att andra myndigheter lämnar information till myndigheterna inom nämnda områden. I det följande görs ingen principiell skillnad mellan att en myndighet självmant lämnar över en uppgift till en annan eller att överlämnandet aktualiseras först efter en uttrycklig begäran/behovsframställan. Anledningen är att de regler som styr om ett överlämnande kan ske inte gör någon principiell skillnad mellan dessa situationer.

Det finns dock, som kommer att framgå nedan, regler som anger att en myndighet på förfrågan är skyldig att lämna en uppgift i ett visst hänseende till en annan myndighet. För vissa ändamål finns också regler om rapporteringsskyldighet och om direktåtkomst till register för automatisk databehandling som ska belysas i det följande.

3.1 Försvarsunderrättelseverksamhet

Försvarsunderrättelseverksamhet ska enligt 1 § 1 st. lagen (2000:130) om försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Verksamheten ska enligt 2 § förordningen (2000:131) om försvarsunderrättelseverksamhet bedrivas av Försvarsmakten, FRA, FMV och FOI. Regeringen bestämmer försvarsunderrättelseverksamhetens inriktning enligt 1 § 2 st. nämnda lag och anger dess innehåll enligt 2a § nämnda förordning.

3.1.1 Gränsen mellan försvarsunderrättelse- och polisiär verksamhet

Sedan gammalt gäller att försvarsunderrättelseverksamheten, som framgår av 1 § 1 st. lagen om försvarsunderrättelseverksamhet, endast får avse utländska förhållanden, dvs. verksamheter och företeelser som har sin utgångspunkt i utlandet. Det hindrar inte att försvarsunderrättelseverksamhet kan beröra företeelser inom landet under förutsättning att dessa har sitt ursprung i utlandet, t.ex. främmande underrättelseverksamhet mot svenska intressen[5].

Inom försvarsunderrättelseverksamheten får det enligt 4 § 1 st. lagen om försvarsunderrättelseverksamhet inte vidtas åtgärder som syftar till att lösa uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet. Detta är en central bestämmelse som anger gränslinjen mellan försvarsunderrättelseverksamhet och polisiär verksamhet.

Mandatet för de myndigheter som bedriver försvarsunderrättelseverksamhet är begränsat till underrättelseverksamhet. I denna får inte företas åtgärder som inrymmer polisiära befogenheter som förundersökningsåtgärder enligt rättegångsbalken och tvångsmedelsanvändning, t.ex. hemlig avlyssning av elektronisk kommunikation[6]. Av det följer att signalspaning inte får användas för att stärka misstankarna mot en misstänkt sedan förundersökning inletts. Åtgärden skulle i så fall komma att få karaktären av ett hemligt tvångsmedel, för vilket det

[5] Se. t.ex. prop. 2006/07:63 s. 43
[6] Prop. 1999:2000:25 s. 17

gäller särskilda regler och vars användning exklusivt ankommer på brottsbekämpande myndigheter. I linje med detta riktade JO (dnr 4747-2009) också synnerligen allvarlig kritik mot Försvarsmakten för ett tillslag (i realiteten husrannsakan) mot en av Försvarsmakten ägd lägenhet som disponerades av en anställd som var misstänkt för brottslighet riktad mot rikets säkerhet. Det förtjänar att betonas att den gränslinje som 4 § lagen om försvarsunderrättelseverksamhet drar upp går vid användning av straffprocessuella tvångsmedel och annat utövande av polisiära befogenheter som riktas mot enskilda och som regleras i lag.

Det försvarsunderrättelsemyndigheterna ska ägna sig åt är just underrättelseverksamhet, och så länge denna inte tar sig uttryck i åtgärder som är exklusiva för de brottsbekämpande myndigheterna innebär nämnda 4 § inget hinder. Lagstiftaren har tvärtom betonat det angelägna i att denna verksamhet kan utnyttjas mot hela den vidgade säkerhetspolitiska hotbilden till nytta för en bredare krets av underrättelsemottagare.[7]

Enligt 4 § 2 st. framgår att, om det inte finns hinder enligt andra bestämmelser, får de myndigheter som bedriver försvarsunderrättelseverksamhet lämna stöd till andra myndigheters brottsbekämpande verksamhet.

3.1.2 Rapportering

Enligt 2 § lagen om försvarsunderrättelseverksamhet ska underrättelser rapporteras till berörda myndigheter. I första hand är det inte den färdiganalyserade bedömningen som ska rapporteras. I stället är det den information som framkommit som ska rapporteras i form av underrättelser. Den slutliga och samlade analysen bör följaktligen göras hos ansvariga myndigheter, där den kan anpassas efter myndighetens specifika behov.[8] Denna grundläggande princip hindrar dock inte att det finns särskilda regler som anger att rapporteringen ska avse just färdiga rapporter (se t.ex. avsnitt 3.1.4 under FRA nedan). I 7 § förordningen om försvarsunderrättelseverksamhet anges att försvarsunderrättelsemyndigheterna, innan de orienterar annan än regeringen eller informationsberättigad totalförsvarsmyndighet i underrättelsefrågor, ska samråda med regeringskansliet (Försvarsdepartementet).

Vilka som är berörda myndigheter anges inte annat än undantagsvis i författningar. Uppenbart är att bl.a. Regeringskansliet avses i 2 § lagen om försvarsunderrättelseverksamhet. Det är av naturliga skäl inte ovanligt att det i författningar anges att myndigheter i olika hänseenden har en rapporteringsskyldighet till Regeringskansliet. Att det gäller underrättelser som har betydelse för riket säkerhet ter sig självklart, se t.ex. avsnitt 3.2.1 nedan. Inom Försvarsmakten finns

[7] Prop. 2006/07:63 s. 39
[8] Prop. 2006/07 :63 s. 54

givetvis rutiner för hur relevant hemlig information delges berörda organisationsenheter. I den mån det bedöms att en myndighet, som enligt gällande regler och rutiner inte är informationsberättigad, bör få del av informationen, ska som framgått berörd försvarsunderrättelsemyndighet först samråda med Försvarsdepartementet. Därvid torde sekretessbrytande regler behöva övervägas, se avsnitt 3.3 nedan.

När det gäller signalspaning får de myndigheter som får inrikta signalspaning en återrapportering med anledning av de frågor man ställt. En särskild regel har införts i 8 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Bestämmelsen hänvisar till vad som gäller enligt lagen om försvarsunderrättelseverksamhet och anger dessutom att, om uppgifterna berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § i den lagen. Avsikten är att signalspaning inte ska få användas för sådana syften för vilka anvisats de särskilda redskap som står de brottsbekämpande myndigheterna till buds[9]. Med andra ord ska signalspaning inte få användas som ett substitut för hemliga tvångsmedel.

3.1.3 Sekretessregler för försvarsunderrättelseverksamhet

I försvarsunderrättelseverksamhet gäller ofta sekretess för de uppgifter som förekommer i verksamheten. Uppgifterna omfattas i många fall av reglerna om så kallad utrikes- och eller försvarssekretess i 15 kap. 1 § och 2 § offentlighets- och sekretesslagen (2009:400), fortsättningsvis benämnd OSL.

Enligt 15 kap. 1 § OSL gäller sekretess för uppgift som angår Sveriges förbindelser med annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs.

Av 1 a § framgår, beträffande direktåtkomst (se nedan 3.2.4), att sekretess gäller för uppgift som en myndighet har elektronisk tillgång till i en upptagning för automatiserad behandling hos en annan stat eller mellanfolklig organisation, om myndigheten inte får behandla uppgiften enligt en bindande EU-rättsakt eller ett av Sverige eller EU ingånget avtal med en annan stat eller mellanfolklig organisation.

Enligt 15 kap. 2 § OSL gäller sekretess för uppgift som angår verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

[9] Prop.2006/2007:63 s. 109

Utrikes- och försvarssekretessen gäller oavsett i vilken verksamhet eller hos vilken myndighet uppgiften förekommer. Dessa sekretesser inskränker, på det sätt som framgår av 15 kap. 6 § OSL, rätten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Av 38 kap. 4 § OSL framgår att sekretess gäller hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos FRA i underrättelse- och säkerhetsverksamheten för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider skada eller men. Bestämmelsen innebär alltså att det gäller en presumtion för sekretess beträffande de uppgifter som skyddas av denna.

Det finns sekretessbrytande bestämmelser som har stor betydelse i sammanhanget. De kommer att kortfattat redovisas gemensamt för alla verksamheter under avsnitt 3.5 nedan.

3.1.4 Direktåtkomst till vissa registeruppgifter inom försvarsunderrättelseverksamheten m.m.

Försvarsmakten

Av stor betydelse är lagen (2007:258) om personuppgiftsbehandling i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Beträffande den senare finns i lagen detaljerade regler om för vilka ändamål personuppgifter får behandlas och om villkoren för detta. I lagen finns vidare regler om utlämning av personuppgifter ur register.

I 14 § anges sålunda att endast enstaka personuppgifter får lämnas ut på medium för automatisk databehandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat att uppgifter får lämnas ut på sådant medium.

Om direktåtkomst stadgas i 15 § att regeringen meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar och att regeringen, eller den myndighet som regeringen bestämmer, meddelar ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten.

Enligt 14 § ska tillgången till personuppgifter alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringens föreskrifter om bl.a. direktåtkomst finns i förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Av förordningen framgår att det vid Försvarsmakten får finnas uppgiftssamlingar för försvarsunderrättelseverksamhet, säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalkontroll. Det framgår även vad uppgiftssamlingarna får innehålla.

Enligt 8 § i förordningen anges att FRA får ha direktåtkomst till uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet i den omfattning som Försvarsmakten beslutar, och enligt 9 § ges på liknande sätt Säkerhetspolisen direktåtkomst till uppgifter i en uppgiftssamling för säkerhetsskyddstjänst.

Försvarsmakten bestämmer alltså vad som är tillgängligt för nämnda myndigheter genom direktåtkomst.

Försvarets radioanstalt

Lagen (2007: 259) om personuppgifter i FRA:s försvarsunderrättelse- och utvecklingsverksamhet innehåller regler om personuppgiftsbehandling i denna verksamhet. Enligt lagen får personuppgifter behandlas i uppgiftssamlingar. Vidare anges att regeringen meddelar närmare föreskrifter om dessa uppgiftssamlingar och vad de får innehålla. Av lagen framgår också när behandling av personuppgifter är tillåten.

Detaljerade regler ges i förordningen (2007:261) om behandling av personuppgifter i FRA:s försvarsunderrättelse- och utvecklingsverksamhetsregister. Enligt förordningen får det vid myndigheten finnas en rad olika uppgiftssamlingar. Det framgår också vad uppgiftssamlingarna får innehålla. I 4 § föreskrivs att det vid myndigheten får finnas uppgiftssamlingar för underrättelser. Dessa får endast innehålla färdiga underrättelserapporter.

Det är alltså FRA som beslutar om i vilken utsträckning direktåtkomst får ske. Det bör vidare observeras att direktåtkomsten endast kan gälla färdiga underrättelserapporter.

3.2 Polisens och Säkerhetspolisens brottsbekämpande verksamhet

I 1 § polislagen (1984:387) anges att, som ett led i samhällets verksamhet för att främja rättvisa och trygghet, polisens arbete ska syfta till att upprätthålla ordning och säkerhet samt i övrigt tillförsäkra allmänheten skydd och annan hjälp.

Enligt 2 § ingår i polisens uppgifter bl.a. att förebygga brott och andra störningar av den allmänna ordningen eller säkerheten, att övervaka den allmänna ordningen och säkerheten, hindra störningar därav och ingripa när sådana har inträffat samt bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

I 1 § förordningen (2014:1103) med instruktion för Säkerhetspolisen anges att Säkerhetspolisen i egenskap av säkerhetstjänst bedriver underrättelse- och säkerhetsarbete.

Enligt 3 § ansvarar Säkerhetspolisen bl.a. för att förebygga, förhindra och upptäcka brottslig verksamhet samt utreda och beivra bl.a. brott mot 18 eller 19 kap. brottsbalken eller annat brott mot rikets säkerhet, brott mot lagen (2003:148) om straff för terroristbrott samt en rad andra uppräknade brott av liknande art, däribland företagsspionerі understött av främmande makt samt brott som rör sanktionslagstiftningen, krigsmateriel eller produkter med dubbla användningsområden.

I 6 § polislagen anges att Polismyndigheten och Säkerhetspolisen ska samarbeta med varandra och med åklagarmyndigheterna. De ska också samarbeta med andra myndigheter och organisationer vilkas verksamhet berör polisverksamheten.

3.2.1 Rapportering

I 8 § förordningen med instruktion för Säkerhetspolisen föreskrivs att underrättelser som kan ha betydelse för Sveriges säkerhetspolitik eller som av annan anledning bör komma till regeringens kännedom utan dröjsmål ska rapporteras till Regeringskansliet (Justitiedepartementet).

I förordningen finns vidare regler för samverkan med Polismyndigheten. Enligt 12 § bör Säkerhetspolisen, i den utsträckning sekretess inte hindrar det, upplysa Polismyndigheten om förhållanden som kan ha betydelse för dess verksamhet.

3.2.2 Sekretessregler av särskild betydelse för brottsbekämpning

Enligt 18 kap. 1 § OSL gäller sekretess för bl.a. uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

Av samma kap. 2 § framgår att sekretess gäller för bl.a. uppgifter som hänför sig till personuppgifter som får behandlas i polisens eller Säkerhetspolisens arbete för att förebygga, förhindra eller upptäcka brottslig verksamhet, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

Bestämmelsen är alltså utformad som en presumtion för sekretess.

Enligt 3 § gäller sekretessen enligt 1 och 2 §§ också hos en myndighet som biträder vissa angivna brottsbekämpande myndigheter i deras verksamhet.

I 35 kap. OSL regleras ett omfattande sekretesskydd för enskild i verksamhet som syftar till att förebygga eller beivra brott. Sålunda gäller enligt 1 § sekretess

för uppgift om enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider skada eller men och uppgiften förekommer i ett antal uppräknade angelägenheter och register, bl.a. förundersökning i brottmål och användning av tvångsmedel.

Bestämmelsen är, liksom nämnda 18 kap. 2 § OSL, sålunda utformad som en presumtion för sekretess.

Enligt lagen (2016:774) om uppgiftsskyldighet vid samverkan mot grov organiserad brottslighet, som trädde i kraft den 15 augusti 2016, ska en myndighet trots sekretess lämna uppgift till en annan myndighet om det behövs för den mottagande myndighetens deltagande i samverkan mot grov organiserad brottslighet. Endast de myndigheter som regeringen bestämmer ska vara skyldiga att lämna eller få ta emot uppgifter enligt denna lag.

Genom förordningen(2016:775) med samma namn har regeringen bestämt att dessa myndigheter är: Arbetsförmedlingen, Ekobrottsmyndigheten när den bedriver polisiär verksamhet, Försäkringskassan, Kriminalvården, Kronofogdemyndigheten, Kustbevakningen, Migrationsverket, Polismyndigheten, Skatteverket, Säkerhetspolisen och Tullverket.

Beträffande sekretessbrytande regler se nedan under 3.5.

3.2.3 Direktåtkomst till vissa register inom brottsbekämpning

Av 1 kap. polisdatalagen (2010:361) framgår lagens syfte och tillämpningsområde. I 2 kap. 7 § anges att personuppgifter får behandlas om det behövs för att 1. förebygga, förhindra eller upptäcka brottslig verksamhet, 2. utreda eller beivra brott, eller 3. fullgöra förpliktelser som följer av internationella åtaganden.

Enligt 8 § får personuppgifter som behandlas enligt 7 § även behandlas när det är nödvändigt för att tillhandahålla information som behövs bl.a. i brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket. Bland övriga verksamheter uppräknas verksamhet hos Kriminalvården samt verksamhet hos Migrationsverket för kontroll av fingeravtryck.

Behandling av personuppgifter får även ske när det är nödvändigt att tillhandahålla information som behövs i en myndighets verksamhet om det enligt författning åligger Polismyndigheten att bistå myndigheten med viss uppgift eller om information tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott.

Beträffande utlämnande av personuppgifter och uppgiftsskyldighet stadgas i 16 § att Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket,

Kustbevakningen och Skatteverket, trots sekretess enligt 21 kap. 3 § 1 st. och 35 kap. 1 § OSL, har rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga, om den mottagande myndigheten behöver uppgiften i sin brottsbekämpande verksamhet.

Enligt 17 § har samma myndigheter som anges i 16 § utom Skatteverket rätt att ta del av uppgifter om huruvida personer förekommer i register över DNA-profiler enligt 4 kap. i lagen. Migrationsverket har motsvarande rätt att ta del av uppgifter som behandlas i fingeravtrycks- och signalelementsregistret.

I 3 kap. återfinns särskilda bestämmelser om personuppgifter som får göras gemensamt tillgängliga i den brottsbekämpande verksamheten. I 1 § sägs bl.a. att uppgifter som endast ett fåtal personer har rätt att ta del av inte anses som gemensamt tillgängliga. Under 2 § ges detaljerade regler om vilka personuppgifter som får göras gemensamt tillgängliga. I 8 -13 §§ regleras frågor om direktåtkomst till registren och om när personuppgifterna inte längre får behandlas. Enligt 8 § får Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomst får endast avse uppgifter som gjorts gemensamt tillgängliga.

I lagen (2010:362) om polisens allmänna spaningsregister finns regler om vad som gäller för detta register, bl.a. om andra myndigheters rätt att ta del av uppgifter och om direktåtkomst.

I 18 § stadgas bl.a. följande: Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket har trots sekretess enligt 21 kap. 3 § 1st. och 35 kap. 1§ OSL rätt att ta del av uppgifter i register, om myndigheten behöver uppgifterna i sin brottsbekämpande verksamhet. Regeringen meddelar föreskrifter om att uppgifter får lämnas ut i andra fall än som anges i första stycket.

Enligt 19 § får enstaka personuppgifter lämnas ut på medium för automatiserad behandling och regeringen meddela föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall. Denna begränsning gäller inte de myndigheter som anges i följande paragraf.

Av 20 § framgår bl.a. följande: Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till registret. En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Kompletterande föreskrifter om behandling av personuppgifter som omfattas av lagen ges i förordningen (2010:1157) om polisens allmänna spaningsregister. I förordningens 3 § anges att direktåtkomst inte får ges innan Polismyndigheten har försäkrat sig om att den mottagande myndigheten uppfyller Polismyndighetens krav på behörighet och säkerhet.

Utlänningsdatalagen (2016:27) syftar till att ge Migrationsverket, Polismyndigheten och utlandsmyndigheterna möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin verksamhet enligt utlännings- och medborgarskapslagstiftningen och att skydda människor mot integritetskränkningar vid sådan behandling. Enligt 11 § får dessa myndigheter behandla personuppgifter för en rad behov, bl.a. kontroll av utlänning i samband med inresa och utresa samt kontroll under vistelsen i Sverige.

Enligt 14 § får Migrationsverket föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8 § utlänningslagen (2005:716). I 19 § anges vilka myndigheter som får ges direktåtkomst till personuppgifter hos Migrationsverket. Dessa är Polismyndigheten, Säkerhetspolisen, utlandsmyndigheterna, Försäkringskassan, Pensionsmyndigheten och Skatteverket. Lagen innehåller vidare begränsningar om sökningar. I utlänningsdataförordningen (2016:30) ges ytterligare begränsningar beträffande direktåtkomst av personuppgifter hos Migrationsverket.

Som framgår i denna rapport har inte försvarsunderrättelsemyndigheter direktåtkomst till polisens register.

3.3 Övriga myndigheter och underrättelsebaserad information

De myndigheter som, vid sidan av försvarsunderrättelseverksamheten och det polisiära fältet, har ett särskilt intresse av underrättelsebaserad information är de civila myndigheter som enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap har ett särskilt ansvar. Förordningen hänvisar till lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap och till förordningen (2006:637) med samma rubrik. Det geografiska områdesansvaret vid höjd beredskap ankommer på länsstyrelser, landsting och kommuner. Eftersom denna rapport är begränsad till centrala organ lämnas regler som tar sikte på regionala och lokala organ utanför genomgången.

Enligt 7 § 1 st. i förordningen 2015:1052 indelas ett antal myndigheter som redovisas i en bilaga till förordningen i s.k. samverkansområden. Enligt 7 § 3 st. ska MSB i samverkan med myndigheterna i samverkansområdena utveckla samarbetsformerna för arbetet i områdena. Vikten av samverkan mellan berörda

aktörer betonas i 5 §. Länsstyrelsernas sammanhållande roll inom sitt geografiska område framhålls i 6 §. Myndigheterna i samverkansområdena har enligt 8 § ett särskilt ansvar att vidta förberedelser för och verksamhet under krissituationer. I detta ingår att göra sårbarhets- och riskanalyser. De har också enligt 10 § ett särskilt ansvar för att planera och vidta förberedelser för att skapa förmåga att hantera en kris, förebygga sårbarhet och motstå hot och risker.

Det geografiska områdesansvaret omfattar alla länsstyrelser och MSB.

Samverkansområdena är utöver det geografiska områdesansvaret: *Teknisk infrastruktur* med sex myndigheter*, Transporter* med fem myndigheter, *Farliga ämnen* med 11 myndigheter, *Ekonomisk säkerhet* med fem myndigheter samt *Skydd undsättning och vård* med sju myndigheter.

Det är givet att MSB i sin roll kan ha anledning att ge samverkande myndigheter underrättelsebaserad hemlig information och att generalklausulen i 10 kap. 27 § OSL därvid kan komma att tillämpas.

3.3.1 Rapportering

Enligt 13 § förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska en ansvarig myndighet vid en i 8 § 2 st. beskriven situation (kris) hålla regeringen informerad om händelseutvecklingen, tillståndet, den förväntade utvecklingen och tillgängliga resurser inom respektive ansvarsområde samt om vidtagna och planerade åtgärder. Vid höjd beredskap har dessa bevakningsansvariga myndigheter enligt 18 § en fortlöpande rapporteringsplikt till regeringen.

Vidare ska varje myndighet enligt 14 §, efter förfrågan från Regeringskansliet eller MSB, lämna den information som behövs för samlade lägesbilder. MSB kan alltså inhämta information från myndigheterna inom samverkansområdena för att få underlag för en samlad lägesbild. Det rör sig om en skyldighet för dessa myndigheter att tillhandahålla för ändamålet relevanta uppgifter som även kan omfatta sekretessbelagda uppgifter. Det ankommer på MSB att överväga i vad mån samlade lägesbilder och underrättelser bör delges myndigheter inom samverkansområdena. Det kan givetvis handla om underrättelsebaserad hemlig information.

Utöver nu nämnda regler om rapportering finns i de instruktioner som gäller för myndigheter inom samverkansområdena särskilda regler om rapporteringsskyldighet och regler om samverkan med andra myndigheter. Det kan i detta sammanhang finnas skäl att nämna några.

I 3 § p 5 förordningen (2007:119) med instruktion för Svenska kraftnät föreskrivs en särskild skyldighet att till regeringen senast den 1 juli varje år rapportera bl.a. hur kraftbalansen den senaste vintern har upprätthållits. Enligt 10 § ankommer

det på styrelsen för Svenska kraftnät att bestämma hur rapportering och samordning mellan Svenska kraftnät och koncernens företag ska ske samt se till att regeringen får det underlag som behövs för att ta ställning till omfattningen och inriktningen av verksamhetens olika delar.

Av förordningen (2007:853) med instruktion för Kustbevakningen anges i 2 § att det i Kustbevakningens uppgift att bedriva sjöövervakning ingår att ansvara för eller bistå andra myndigheter med övervakning, brottsbekämpande verksamhet samt kontroll och tillsyn enligt vad som anges i förordningen.

Enligt 9 § förordningen (2010:185) med instruktion för Trafikverket ska verket för att säkerställa att totalförsvarets krav beaktas i den fredstida verksamheten samråda med Försvarsmakten, MSB och övriga berörda totalförsvarsmyndigheter.

I 8 § punkten 6 förordningen (2009: 1243) med instruktion för Socialstyrelsen anges att Socialstyrelsen ska medverka i totalförsvaret och krisberedskap i enlighet med förordningen om krisberedskap och höjd beredskap samt samordna och övervaka planläggningen av den civila hälso- och sjukvårdens, smittskyddets och socialtjänstens beredskap.

För fullgörandet av nu nämnda myndighetsåligganden torde det kunna bli aktuellt med utbyte av underrättelsebaserad och hemlig information.

3.3.2 Sekretessregler inom samverkansområdena enligt förordningen om krisberedskap och höjd beredskap

Olika regler i OSL kan givetvis vara tillämpliga beroende på vilken verksamhet det rör sig om. När det gäller totalförsvarsplanering blir det naturligt att reglerna om försvarssekretess är tillämpliga. I övrigt kan en rad olika sekretessregler vara tillämpliga för myndigheterna inom samverkansområden. För informationsutbyte mellan myndigheter inom dessa områden torde, när det gäller underrättelsebaserad information, de sekretessregler som uppställts till skydd för berörd verksamheten vara intressantare än det skydd som gäller till förmån för enskilds personliga och ekonomiska förhållanden. I det här sammanhanget bör det vara tillräckligt att peka på några av dessa bestämmelser.

Värt att observera är att skyddet för förundersökning och underrättelseverksamhet i 18 kap. 1 och 2 §§ OSL, enligt 3 § , även gäller hos en myndighet som biträder Åklagarmyndigheten, Polismyndigheten, Skatteverket, Tullverket eller Kustbevakningen med att bekämpa brott.

Vidare bör i samma kapitel observeras skyddet för säkerhets- och bevakningsåtgärd i 8 §, chiffer och koder i 9 §, körkorts referensnummer i 10 §, spridning av kärnvapen m.m. i 12 § och risk- och sårbarhetsanalyser m.m. i 13 §.

När det gäller en myndighets affärs- och driftförhållanden bör också skyddet i 19 kap.1 § OSL uppmärksammas.

Även om sekretessreglerna till skydd för uppgifter om enskilds personliga och ekonomiska förhållandenen inte torde komma i fråga så ofta när det gäller utbyte av underrättelsebaserad information inom samverkansområdena kan det säkert inträffa. Det gäller i första hand reglerna i 35 kap. OSL till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott. Därvid är reglerna i 1 §, som skyddar uppgifter om enskild i verksamhet som syftar till att bekämpa brott, liksom uppgifter i vissa register om enskilda enligt reglerna i 3 och 4 §§ av intresse.

Beträffande sekretessbrytande regler, se nedan under 3.5.

3.4 Särskilda samverkansgrupper

Olika former av samverkan mellan myndigheter har blivit allt vanligare. Bakgrunden till detta är bl.a. att regeringen genom regleringsbrev och separata regeringsuppdrag uppmanat myndigheterna att samverka och att effektivisera den samverkan som redan finns etablerad. För att möta vissa typer av hot har det mellan myndigheter, som har ett särskilt ansvar att identifiera och bekämpa hotet i fråga, bildats särskilda samverkansgrupper. Ett viktigt led i alla former av samverkan är möjligheten att kunna utbyta information.

3.4.1 Samverkansrådet mot terrorism

Samverkansrådet mot terrorism är ett samarbete mellan 14 svenska myndigheter som syftar till att stärka Sveriges förmåga att motverka och hantera terrorism. Rådet har inte någon egen juridisk status eller formellt uppdrag men har ett uttalat stöd från regeringen, exempelvis i den nationella strategin mot terrorism. Rådet har tillkommit på initiativ av Säkerhetspolisen. Det leds och kallas samman av säkerhetspolischefen. De ingående myndigheterna representeras på myndighetschefsnivå. Följande myndigheter ingår i rådet:

Säkerhetspolisen, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Kriminalvården, Migrationsverket, Försvarsmakten, FRA, MSB, Kustbevakningen, FOI, Tullverket, Strålsäkerhetsmyndigheten och Transportstyrelsen.

3.4.2 Nationellt centrum för terrorhotbedömning (NCT)

NCT är en sedan 2009 permanent arbetsgrupp med personal från Säkerhetspolisen, FRA och Must. I arbetsgruppen ingår medarbetare från de tre myndigheterna. Styrgrupp för arbetsgruppen är cheferna för myndigheterna. Chefen för

NCT leder den dagliga verksamheten enligt styrgruppens inriktning. Chefskapet roterar mellan myndigheterna. Uppgiften är att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen på kort och lång sikt.

NCT är ett exempel på myndighetssamverkan som syftar till att förbättra Sveriges förmåga att förebygga, avvärja, hindra och hantera konsekvenserna av terrorangrepp mot Sverige och svenska intressen. NCT bedömer hotnivån för Sverige och chefen för Säkerhetspolisen beslutar om denna. NCT:s bedömningar av terrorhotet mot Sverige bygger på information som är sekretessbelagd. NCT:s produktion av rapporter berör och distribueras till samtliga deltagande myndigheter i Samverkansrådet mot terrorism och till regeringskansliet.

3.4.3 Samverkansgruppen för informationssäkerhet (SAMFI)

Den nationella handlingsplanen för samhällets informationssäkerhet togs fram 2012 av MSB i samråd med övriga myndigheter som nu ingår i SAMFI. Dessa är FMV, Sveriges certifieringsorgan för IT-säkerhet (CSEC), FRA, Post- och telestyrelsen, Polismyndigheten, Säkerhetspolisen och Försvarsmakten. I den nationella handlingsplanen ingår ett stort antal åtgärdspunkter. Myndigheterna i SAMFI och flera andra aktörer har under de senast åren genomfört ett betydande antal aktiviteter för att öka samhällets informations- och cybersäkerhet.

3.4.4 Nationell samverkan till skydd mot allvarliga IT-hot (NSIT)

NSIT är en samverkansform mellan Must, Säkerhetspolisen och FRA. Samarbetet började som ett pilotprojekt som slutfördes hösten 2014. Projektet bedömdes som lyckat och ledde till att samarbetet permanentades. NSIT analyserar och bedömer hot och sårbarheter som gäller de mest skyddsvärda nationella intressena. Samverkan syftar till att försvåra för en kvalificerad angripare att komma åt eller skada skyddsvärda civila och militära resurser. MSB deltar sedan 2014 som observatör i NSIT-samverkan.

3.4.5 Övriga myndighetssamarbeten

Det finns även andra exempel på mer eller mindre formaliserande samarbeten mellan myndigheter. Ett exempel är arbetsgruppen för arbete mot icke spridning och exportkontroll, ISEK. I den ingår Must, FOI, Inspektionen för strategiska produkter (ISP), Säkerhetspolisen och Tullverket.

Inom det brottsbekämpande området finns Samverkansrådet, Operativa rådet samt Nationellt underrättelsecentrum (NUC) och regionala underrättelsecenter (RUC). I dessa organ ingår tolv myndigheter med uppgifter inom området. I de olika underrättelsecentren deltar myndigheterna med samgrupperade samverkanspersoner, vilket underlättar att delge varandra relevant information. En redovisning av resultatet av den särskilda satsningen mot den grova organiserade

brottsligheten finns i den årliga publikationen Myndigheter i samverkan mot den organiserade brottsligheten.

3.4.6 Sekretessregler inom samverkansgrupperna

En rad olika sekretessregler kan tillämpas beroende på vilka verksamhetsområden och myndigheter det gäller i enlighet med vad som redovisats ovan. Försvarsunderrättelsemyndigheterna och de brottsbekämpande myndigheterna intar dock en särställning inom dessa samverkansgrupper, i synnerhet när det gäller att tillföra underrättelsebaserad information. Utrikes- och försvarssekretessen liksom förundersökningssekretessen och underrättelsesekretessen inom det polisiära fältet torde oftast vara tillämpliga.

För samverkan inom de olika underrättelsecentren inom den brottsbekämpande verksamheten gäller bl.a. de sekretessregler som redovisats under avsnitt 1.2.

I samverkanshänseende bör vidare erinras om att försvars- och utrikessekretessen gäller oavsett i vilken verksamhet eller hos vilken myndighet uppgiften förekommer. Det borde ofta göra det lättare att till annan myndighet lämna över uppgifter som omfattas av detta sekretesskydd under förutsättning av att det finnas stöd för att uppgiften kan lämnas ut.

I underrättelsesammanhang torde det för övrigt vara vanligt att uppgifter, oavsett slag av myndighet, omfattas av utrikessekretess. När sekretess inte med automatik följer med en uppgift som lämnas över från en myndighet till en annan torde det ofta vara så att uppgiften ändå träffas av en sekretessregel som gäller för den verksamhet och den myndighet till vilken den överlämnas. En uppgift som rör en enskild person och skyddas av förundersökningssekretess hos Säkerhetspolisen kan t.ex. komma att träffas av sekretess i underrättelseverksamhet m.m. enligt 18 kap. 2 § OSL om den lämnas över till Must eller FRA.

När myndigheter delger varandra sekretesskyddade uppgifter inom ramen för arbetet i olika samverkansgrupper kan det, på samma sätt som inom MSB:s samverkansområden, bli aktuellt att tillämpa generalklausulen i 10 kap. 27 § OSL, se nedan under 3.5.

Frågan om direktåtkomst till varandras register uppkommer när det gäller arbetet i samverkansgrupperna. Det gäller inte minst samarbetet i NCT. För närvarande använder medarbetarna sina egna myndigheters IT-system och har inte tillgång till varandras system. Det finns en gemensam NCT-mapp, som medarbetarna från alla tre myndigheter har tillgång till. Den innehåller utkasten till de rapporter som ännu inte färdigställts.

Säkerhetspolisen har i skrivelse till regeringen (Ju 2015/05096/L4) föreslagit att myndigheten ska ge Försvarsmakten och FRA direktåtkomst till personuppgifter

som gjorts gemensamt tillgängliga för NCT-samarbetet i Säkerhetspolisens verksamhet, om uppgifterna behövs för att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen. En utredning (Ju 2015/07312/P) har undersökt frågan liksom hur myndigheterna i dag delger varandra information inom ramen för samarbetet i NCT. Utredaren föreslår att varje myndighet inom NCT ska få medge övriga myndigheter inom samarbetet direktåtkomst till sådana uppgifter som behövs för att analytikerna vid myndigheterna ska kunna göra bedömningar på strategisk nivå om terrorhot mot Sverige och svenska intressen.

Direktåtkomsten ska inte omfatta fler uppgifter än vad myndigheterna i dag kan lämna ut till varandra på papper eller muntligen. Förslaget innehåller också en teknikneutral bestämmelse som ska ge Säkerhetspolisen samma möjlighet som Försvarsmakten och FRA att lämna ut uppgifter elektroniskt på annat sätt inom samarbetet. Förslaget föreslås träda i kraft den 1 januari 2018.

3.5 Sekretessbrytande regler

I 10 kap. OSL finns allmänna sekretessbrytande regler och bestämmelser om undantag från sekretess. Regeringen har en allmän dispensbefogenhet. Sålunda anges i 6 § att regeringen för ett särskilt fall får besluta att en sekretessbelagd uppgift i ett regeringsärende får lämnas ut och att regeringen även i övrigt för ett särskilt fall får besluta om undantag från sekretess om det är motiverat av synnerliga skäl. Regeringen kan alltså inte generellt undanta vissa uppgifter eller viss rapportering från sekretess. Befogenheten tar sikte på ett särskilt fall. Av 7 § framgår att regeringen får förena ett utlämnande av hemlig handling med villkor och att ett sådant villkor inskränker den grundlagsskyddade meddelarfriheten.

Enligt 15 § hindrar sekretess inte att en uppgift lämnas till riksdagen eller regeringen.

27 § innehåller den s.k. generalklausulen. Enligt den får en sekretessbelagd uppgift lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda. Från bestämmelsen finns vissa undantag. Bestämmelsen får stor betydelse när det gäller samverkan mellan myndigheter, särskilt när det saknas särskilda författningsmässiga bestämmelser om rapportering.

3.6 Inskränkningar i yttrande- och informationsfriheten

Det skulle vara att gå för långt att här närmare gå in på inskränkningarna i de grundläggande bestämmelserna om den yttrande- och informationsfrihet som får göras med hänsyn till rikets säkerhet m.m. I 7 kap. 3 § tryckfrihetsförordningen

(TF) och 5 kap. 3 § yttrandefrihetsgrundlagen (YGL) anges dock tre undantagsfall, då en meddelare eller annan medverkande till en grundlagsskyddad framställning kan hållas straffrättsligt ansvarig för sin medverkan. I stället för TF och YGL ska alltså vanlig lag tillämpas i dessa fall.

Det första undantaget är när gärningen utgör bl.a. spionerі, grovt spionerі, grov obehörig befattning med hemlig uppgift eller försök, förberedelse eller stämpling till sådant brott.

Det andra undantaget omfattar uppsåtligt utlämnande av hemlig allmän handling.

Det tredje undantaget avser uppsåtligt åsidosättande av tystnadsplikt i de fall som anges i särskild lag, dvs. OSL. Detta rör sig om åsidosättande av s.k. kvalificerad sekretess. Exempel på en sådan regel i OSL är 15 kap. 6 §, som inskränker den grundläggande friheten att meddela och offentliggöra uppgifter i grundlagsskyddade media när det är fråga om en uppgift vars röjande kan antas sätta rikets säkerhet i fara eller annars skada landet allvarligt.

Med stöd av 2 kap. 14 § tryckfrihetsförordningen föreskrivs i 1 § offentlighets- och sekretessförordningen en särskild ordning för hur en begäran av en enskild att utfå en allmän handling ska prövas om uppgiften är av synnerlig betydelse för rikets säkerhet.

Enligt bestämmelsen ska prövningen göras av någon av cheferna för Justitiedepartementet, Utrikesdepartementet eller Försvarsdepartementet, beroende på vilka sekretessregler som är tillämpliga på uppgifterna i fråga.

Det ligger i sakens natur att en myndighet måste göra en noggrann prövning innan en uppgift av synnerlig betydelse för rikets säkerhet med stöd av generalklausulen kan lämnas över till en annan myndighet. Någon tvekan om att uppgiften kan skyddas hos den mottagande myndigheten torde inte få råda.

3.7 Brott mot tystnadsplikten m.m.

För utlämnande av hemliga handlingar är det inte oviktigt för den enskilde att känna till vilket ansvar som kan följa med ett oriktigt utlämnande.

Om någon röjer en uppgift som han är pliktig att hemlighålla, eller olovligen utnyttjar en sådan hemlighet, kan denne enligt 20 kap. 3 § brottsbalken dömas för brott mot tystnadsplikten till böter eller fängelse i högst ett år. Även ett röjande av oaktsamhet är straffbart och kan medföra böter.

Det finns även särskilda bestämmelser om brott mot tystnadsplikt i 19 kap. brottsbalken (5-9 §§) om brotten mot rikets säkerhet. Det rör sig här bl.a. om spioneri och obehörig befattning med hemlig uppgift, alltså allvarlig brottslighet som har företräde framför brottet i 20 kap. 3 § brottsbalken. Den som åsidosätter en domstols eller undersökningsledares förordnande om yppandeförbud kan straffas enligt regler i 9 kap. 6 § rättegångsbalken och 39 § förvaltningsprocesslagen.

4 Perspektiv från myndigheterna

I detta kapitel redogörs för perspektiv och erfarenheter som deltagande myndigheter har gett uttryck för i samband med enkätsvar och intervjuer inom ramen för denna studieverksamhet. Frågeställningarna som tillställts respektive myndighet utgår i grunden från studiens centrala frågeställningar, men varierar något beroende på myndighetens funktion och mandat.[10]

Den information som myndigheterna delgivit är av varierad karaktär, till del beroende på att de myndighetsrepresentanter som besvarat studiens frågeställningar kan representera olika funktioner på respektive myndighet. I merparten av fallen har myndigheterna representerats av personer som har ett övergripande ansvar för myndighetens underrättelseverksamhet, i enstaka fall har myndigheter representerats på handläggarnivå respektive juridisk funktion.

Sammanställningen av de perspektiv som myndigheterna delgivit redovisas utifrån tematiska områden, där uttryck avseende likartade möjligheter och begränsningar som lyfts av flera myndigheter har getts större prioritet och utrymme.

4.1 Övergripande perspektiv på behovet av informationsdelning

En klar majoritet av de myndigheter som denna studieverksamhet interagerat med har gett uttryck för ett ökat behov av effektivare och utökad delgivning av underrättelser mellan nationella myndigheter. En skiljelinje går dock mellan de myndigheter som traditionellt betraktats som underrättelseproducenter och övriga myndigheter.

Underrättelseproducenterna[11] inklusive Säkerhetspolisen har framfört att efterfrågan och intresse för myndighetens information samt förväntningar på ökad delgivning har varit påtaglig, inte bara från andra myndigheter utan även från delar inom Regeringskansliet. Övriga myndigheter har tydliggjort att behovet av utökad samverkan är påtaglig och att förutsättningarna för mer flexibel och dynamiskt informationsutbyte behöver utvecklas.

Bilden av hur existerande förutsättningar står i förhållande till detta utökade behov av samverkan och informationsdelning är mångfacetterad, men på många sätt förhållandevis likartad mellan myndigheterna liksom bilden av vilka områden som behöver utvecklas. De områden som präglat diskussionerna och enkätsvaren berör allt från mandat, inriktning och regelverk till existerande rutiner,

[10] Se bifogade exempel på enkät i bilaga 1
[11] Must, FRA, FOI, FMV och Säkerhetspolisen

resurser, tekniska system och kulturskillnader. De aspekter som denna studieverksamhet har uppfattat som mest väsentlig i sammanhanget redovisas nedan.

Gemensamma perspektiv från myndigheterna talar även för att behovet av utvecklade förutsättningar för informationsdelning sannolikt kommer att växa även i framtiden. Några aspekter som uppges ligga till grund för det växande behovet är bl.a. den förändrade och mer komplexa hotbilden mot Sverige och svenska intressen, Försvarsmaktens ökade fokus på närområdet i kombination med kravet på civila myndigheter att planera för ett nationellt totalförsvar. Även pågående verksamhet inom EU för en utökad internationell samverkan för att stärka säkerhet och gränsbevakning förutspås få implikationer för samverkan på nationell nivå.

4.2 Gällande nationell inriktning och uppdrag sätter begränsningar

Samverkan och delgivning kostar alltid resurser, så samtidigt som de producerande underrättelsemyndigheterna betonar vikten av den information som kommer fram inom ramen för underrättelseproduktionen är till för att användas, är det ständigt prioriteringar om vilka behov som kan och bör tillgodoses och i vilken omfattning. Därtill är även inriktningsrätten begränsad med hänsyn till den personliga integriteten, varför extra hänsyn till, och proportionalitet med avseende på, integritetsintrånget ställt mot nyttan och behovet av den efterfrågade informationen måste beaktas. Som tidigare nämnts är det regeringen som bestämmer inriktningen för försvarsunderrättelseverksamheten. Emellertid skiljer det sig mellan signalspaning å ena sidan och övrig försvarsunderrättelseverksamhet å den andra.

Vad avser signalspaningen är det endast regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och NOA, som enlig lag får ge en närmare inriktning och då endast inom ramen för regeringens inriktning. De två sistnämnda, Säkerhetspolisen och NOA, återfick sin inriktningsrätt 2013 efter ett fyraårigt uppehåll sedan tillkomsten av Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet, där bl.a. inriktningsrätten lagreglerades för att förstärka integritetsskyddet vid signalspaning. Tullverket, ISP och MSB, som tillstyrkte förslaget om att utöka inriktningsrätten för Säkerhetspolisen och NOA, framhöll i sitt remissvar ett behov av att även själva återfå möjligheten att inrikta signalspaningen, vilket emellertid inte skedde.

För övriga försvarsunderrättelsemyndigheter är det hemligt vilka myndigheter som enligt regeringens bestämmande får komma med en närmare inriktning. Däremot framgår det som beskrivits tidigare tydligt i försvarsunderrättelselagen med dess förarbeten, att underrättelser ska rapporteras till berörda myndigheter.

FRA:s delgivningspraxis skiljer sig till del från övriga försvarsunderrättelsemyndigheter och de polisiära underrättelsemyndigheterna och FRA skickar vid behov sina underrättelserapporter till andra berörda myndigheter även om de inte har inriktningsrätt. Detta förefaller dock inte vara vanligt förekommande. Must däremot delger spontant inte några andra myndigheter än de som har inriktningsrätt, däremot kan det förekomma att om någon myndighet kommer med en framställning om ett informationsbehov kan de i vissa fall delge redan utgivna rapporter. Must förhållningssätt har också blivit mer restriktivt under senare år, framför allt utifrån resursskäl p.g.a. allt fler förfrågningar om såväl skriftlig som muntlig rapportering, men även av försiktighetsskäl då de fått frågor från Regeringskansliet om varför de rapporterat till myndigheter utan inriktningsrätt.

Både FRA och Must för ett liknande resonemang om hur de skiljer mellan samarbete, dialog, inriktning och delgivning. Båda myndigheterna menar att det först blir en de facto-inriktning om hänsyn tas till den myndighetens behov genom att FRA eller Must justerar inhämtning, bearbetning och/eller analys för att tillmötesgå behovet. Om det däremot aktivt eller passivt framkommer ett legitimt behov hos en myndighet som inte leder till någon justering av just inhämtning, bearbetning och analys och som stämmer överens med någon annan inriktande myndighets inriktning, kan informationen delges även den myndighet som inte har inriktningsrätt om den anses vara berörd.

För att nämna några exempel på samarbeten som tidigare beskrivits i studien och som har eller har haft inslag av myndigheter som saknat en närmare inriktningsrätt kan nämnas:

- NCT (Säkerhetspolisen, Must och FRA), som bildades som en arbetsgrupp 2005 och som permanentades 2009 och där Säkerhetspolisen saknade inriktningsrätt 2009-2013.
- NSIT (Säkerhetspolisen, Must och FRA), som bildades månaden innan Säkerhetspolisen åter fick sin närmare inriktningsrätt vad avser signalspaning, och där MSB, som fortfarande saknar en närmare inriktningsrätt vad avser signalspaning, sedan 2014 har en plats som observatör. Initiativet kom till stånd som en följd av att IT-hotet inte anpassar sig efter myndighetsstrukturer, vilket medförde att NSIT växte fram ur ett samarbetsbehov som de tre myndigheterna sett under en längre tid. [12]

[12] Pressmeddelande från Säkerhetspolisen, *Säpo, Must och FRA i nytt samarbete för att stärka den nationella säkerheten,* 2013, http://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt-arkiv/2013-01-14-sapo-must-och-fra-i-nytt-samarbete-for-att-starka-den-nationella-sakerheten.html

Detta är bara två exempel men de visar ändå på ett tydligt sätt att det går att samverka inom ramen för försvarsunderrättelseverksamhetens inriktning om incitamenten är tillräckligt starka. Den polisiära underrättelseverksamhet, som bedrivs av Säkerhetspolisen och NOA, skiljer sig från försvarsunderrättelseverksamheten, som tidigare nämnts, såväl avseende lagstiftningen som hur regering och riksdag valt att inrikta verksamheten.

Detta beskrivs enklast just genom den skillnad som finns i försvarsunderrättelsemyndigheternas uppdrag som underrättelsetjänster i klassisk mening, där underrättelsebehoven finns utanför den egna myndigheten. Säkerhetspolisen och NOA bedriver ett underrättelsearbete främst för sina egna behov. Detta är också något som tydligt kom fram i intervjuerna, och om det finns någon önskan att förändra detta förhållande måste det ske genom regeringens styrning, t.ex. genom att Säkerhetspolisen skulle åläggas att instifta en rapporterings- och delgivningsfunktion till stöd för andra berörda myndigheter. Detta skulle röra sig om en mycket stor förändring i, eller tillägg till, dagens grunduppdrag, och skulle i betydande omfattning påverka såväl metodik som organisation, vilket skulle kräva både tid och resurser.

4.3 Iakttagelser om regeltillämpning

Det tankeutbyte som förts inom utredningen och med berörda myndigheter om regelverket har bl.a. medfört följande iakttagelser, som avser att vara rent beskrivande och inte ett uttryck för utredningens värderingar.

Grundläggande är den under avsnitt 3.1 nämnda skillnaden mellan försvarsunderrättelseverksamhet och polisiär verksamhet. Polisiär verksamhet har ett tydligt fokus på brottsmisstanke och individer, medan försvarsunderrättelseverksamhet inte har någon koppling till brottsmisstanke och främst tar sikte på strategiska förhållanden. Det gör att försvarsunderrättelseverksamhet i allmänhet är ett för grovt instrument för brottsbekämpning. Visserligen har Säkerhetspolisen och NOA behov av information från signalspaning, men där lägger signalspaningslagstiftningen betydande restriktioner för användningen genom att spaningen, med vissa i sammanhanget ointressanta undantag, inte får avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige.

Vidare är FRA förhindrad att lämna ut information som gäller personer som är föremål för en förundersökning. Dessa förbud, där det senare som följer av 4 § lagen om försvarsunderrättelseverksamhet även gäller övrig försvarsunderrättelseverksamhet, är uppställda av integritetsskäl och för att utgöra en tydlig gräns mot polisiär verksamhet. Från försvarsunderrättelsehåll brukar vidare

anföras att ett utnyttjande av försvarsunderrättelseverksamhet för brottsutredningar skulle resa krav på offentliggöranden i rättegångar av bl.a. operatörer, källor och metoder, vilket allvarligt skulle kunna äventyra verksamheten.

I övrigt synes regelverken inte innebära några påtagliga hinder för försvarsunderrättelsemyndigheterna att lämna relevant information inbördes eller till andra myndigheter, även om försvarssekretessen och andra sekretessregler som angetts under avsnitt 1.1 givetvis måste beaktas. Försvarsmakten har framhållit att försvarssekretessen kan hindra att uppgifter lämnas till andra nationella myndigheter för att användas i internationella sammanhang (EU IntCent gavs som exempel). I det sammanhanget kan hänvisas till förordningen (2010:649) om utlämnande av sekretessbelagda uppgifter vid samarbete med utländsk myndighet och 8 kap. 3 § OSL. Man har vidare pekat på att det förekommit tveksamheter, om ifall information som inhämtats på begäran av myndigheter som får inrikta försvarsunderrättelseverksamhet, kan lämnas till myndigheter som inte får inrikta sådan verksamhet men har behov av informationen. Inom Försvarsmakten har frågan besvarats jakande.

Försvarsmakten kan, som framgått av avsnitt 3.1.4, ge såväl FRA som Säkerhetspolisen direktåtkomst till vissa angivna registeruppgifter. En liknande möjlighet har, som också framgått av detta avsnitt, FRA i förhållande till en rad uppräknade myndigheter. För att det ska få ske har FRA ställt upp en rad kriterier och för närvarande har möjligheten inte utnyttjats. FRA anser att berörda myndigheter kan delges behövd information på annat sätt utan olägenhet.

Polisens möjligheter att lämna information inom det brottsbekämpande området är, som framgått av avsnitt 3.2, goda, bl.a. genom den nya lagen och förordningen om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet. I diskussion med NOA:s företrädare har framkommit att personal vid NOA vid ett par tillfällen ansett att Säkerhetspolisen varit alltför restriktiv med att lämna ut information som NOA behövt, trots att varken lagstiftning eller hänsyn till andra samverkande parter, enligt NOA:s uppfattning, lagt hinder i vägen.

Vi har i utredningen har lagt ner viss möda på att få reda på i vad mån berörda myndigheter anser att nuvarande sekretessregler utgör ett beaktansvärt hinder för att ge samverkande myndigheter den information som dessa behöver med hänsyn till sina uppgifter. Frågan har generellt besvarats nekande.

4.4 Tillgängliga system för informationsöverföring

Det finns en variation av tillgängliga tillvägagångssätt för att överföra hemlig information mellan två parter nationellt, från bud/kurir, kryptotelefon, kryptofax och meddelanden genom Swedish Government Secure Intranet (SGSI) till det mer avancerade system såsom Försvarsmaktens informationssystem för militära underrättelser och säkerhetstjänst (IS UndSäk). Detta innebär att vilket tillvägagångssätt som ska användas rimligen inte borde utgöra ett oöverstigligt hinder för att informationsdelning ska ske. Trots detta är brister i tillgängliga system för överföring av hemlig information en aspekt som samtliga myndigheter, med ett undantag, har lyft som en betydande begränsning för förutsättningarna att delge hemlig information till andra nationella myndigheter. System för informationsdelning är naturligtvis gränssättande för hur snabbt, säkert och formatanpassad information kan överföras, liksom förutsättningarna för spårbarhet.

Responderande myndigheters perspektiv på hur och i vilken utsträckning tillgängliga system sätter begränsningar skiljer sig åt, framför allt mellan kretsen av försvarsunderrättelsemyndigheter och övriga myndigheter. Försvarsunderrättelsemyndigheterna kan i hög grad utnyttja IS UndSäk för snabb och säker kommunikation, via krypterade meddelanden och delgivning av hemliga handlingar med övriga mottagare, som har en IS UndSäk-klient. En tydlig begränsning med systemet är dock att antalet klienter utanför kretsen av försvarsunderrättelsemyndigheter är mycket begränsad.[13] Systemet är också begränsat till att endast överföra elektroniska dokument (e-post och handlingar), men har däremot en mycket hög säkerhetsnivå (upp till kvalificerat hemlig information). Av denna anledning har även försvarsunderrättelsemyndigheter uttryckt synpunkten att det finns utvecklingsbehov inom området.

Övriga myndigheter har på ett tydligare sätt problematiserat dessa förutsättningar. Tullverket har meddelat att de inom en nära framtid ska installera en IS UndSäk-klient, vilket kommer att förbättra förutsättningarna något. De flesta myndigheter använder framför allt kryptotelefon, kryptofax och fysiska möten samt till viss del e-post genom SGSI. SGSI uppges hålla en tillräckligt hög säkerhetsnivå för information under förundersökningssekretess men inte för försvarssekretess. [14]

Ytterligare perspektiv på begränsningar i system för elektronisk delgivning är att behovet av ökad och mer effektiv samverkan ställer högre krav på tillgängliga

[13] Det har framgått under studiearbetet att MSB och Säkerhetspolisen har en IS UndSäk klient samt att Tullverket kommer att få tillgång till en i en nära framtid.
[14] SGSI Handbok, Myndigheten för samhällsskydd och beredskap, diarienr 2015-4350, 2016-07-01

system för informationsdelning. Detta gäller framför allt i de sammanhang där det inte finns etablerade samverkansforum där myndigheter kontinuerligt eller regelbundet träffas fysiskt för att delge information.

Uttalade behov av utvecklade system kretsar kring lösningar som medger en dynamisk, säker och flexibel kommunikationslösning som skulle medföra en mer effektiv samverkan. Denna typ av uttalade behov kan relateras till flexibilitet avseende vilka myndigheter man behöver kommunicera med, möjligheten att kommunicera med flera samtidigt samt att systemet har kapacitet att hantera olika format på informationsutbytet såsom bild, film, text och ljud. Ett säkert system innebär i detta sammanhang att en hög sekretessnivå ska kunna hanteras, att systemet är driftssäkert även i kris och att det alltid ska gå att nå en relevant representant vid den myndighet man behöver samverka med.

Utmaningarna i att möta uttalade behov om ett dynamiskt och flexibelt gemensamt system för överföring av hemlig information mellan nationella myndigheter är många och komplexa. Dialogen med myndighetsrepresentanter inom ramen för denna studie har dock inte utrett denna problematik på djupet, även om detta helt uppenbart utgör en av de främsta begränsningarna för effektiv informationsdelning mellan myndigheter i dag.

4.5 En förtroendebransch med betydande kulturella skillnader

Studieverksamheten har visat på att delgivning av underrättelsespecifik information är omgärdat av en komplex lagstiftning som är till för att skydda såväl statens skyddsintressen samtidigt som den ska skydda den personliga integriteten. Det går samtidigt att med stöd av intervjuerna och offentliga uttalande från framför allt GD Säkerhetspolisen och C Must, men även GD FRA, konstatera att samarbetet mellan deras respektive myndigheter aldrig har varit så bra som det är nu. Det goda samarbetet har emellertid inte kommit av sig själv och underrättelsemyndigheterna och övriga intervjuade krisberedskapsmyndigheter lyfter också fram olika samarbetsinitiativ som växt fram på initiativ från underrättelsemyndigheterna.

Att förtroende rent generellt är avgörande för väl fungerande organisationer inom många områden är på intet sätt revolutionerande[15]. Lägger man därtill till hemligstämplar och sekretess är förtroende särskilt betydelsefullt. [16]

Studien visar på två tämligen distinkta lager med en inre och en yttre kärna, där underrättelsemyndigheterna är den inre kärnan, vilket är en grupp som till stora delar har uppnått ett gott och förtroendefullt samarbete över myndighetsgränserna. Den yttre kärnan, det mellan underrättelsemyndigheterna och övriga krisberedskapsmyndigheter, har i varierande grad inte lika goda förutsättningar för samarbete och delgivning av information. I det senare fallet har i studien konstaterats att de legala hindren i sammanhanget får anses, med några få undantag, som försumbara. Däremot är tillit och förtroende avgörande och på det området finns det både mjuka och hårda utmaningar.

Bland de hårda faktorerna redovisades ovan avsaknaden av tillräckligt säkra IT-system, då framför allt i den yttre kärnan och såväl för säker kommunikation mellan krisberedskapsmyndigheterna som för den myndighetsinterna IT-infrastrukturen, som ska vara dimensionerad och ackrediterad för att klara av hotet från en kvalificerad statlig aktör. Bland de mjuka utmaningarna gäller det om den inre kärnan har förtroende för huruvida den yttre kärnan verkligen förstår magnituden och komplexiteten när det gäller att hantera sekretessbelagd underrättelseinformation.

Information och underrättelser skapas för att användas, men när de används i verksamheten är det inte bara den enskilda informationen som har ett skyddsvärde. Det verkliga skyddsvärdet är snarare de bakomliggande faktorerna som de förmågor, metoder och källor som måste skyddas. Då detta är vitalt för underrättelsemyndigheternas förmåga och verksamhet, liksom till skyddet av den personliga integriteten, tillämpas det i den inre kärnan en försiktighetsprincip då det helt enkelt inte finns något utrymme för misstag. En viktig slutsats blir att hindren för delgivning av underrättelsespecifik information till stor del är kulturella snarare än strukturella (trots IT-utmaningen).

Detta förhållande ger upphov till en barriär som blir särskilt tydlig när det gäller underrättelser av sällankaraktär, svaga signaler och mer diffusa iakttagelser och

---

[15] Jämför t.ex. Marsh, Stephen, 94-112, *Trust in Distributed Artificial Intelligence*, i Cristiano Castelfranchi, Eric Werner, Artificial Social Systems - Lecture Notes in Computer Science, (1994), Hofstede, Geert. *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations*. (2001)
Hofstede, Geert, Hofstede, Gert Jan & Minkov, Michael, *Cultures and Organizations: Software of the Mind.* Revised and Expanded 3rd Edition, (2010). Schein, Edgar H, 17, *Organizational Culture and Leadership,* 3rd edition. (2004).

[16] Omand, David, 300-302, *Securing the State* (2010), Lowenthal, Mark M, 1-7, *Intelligence – From Secrets to Policy,* 6th edition 2015.

information, där ansvaret är delat mellan många intressenter såsom kan vara fallet inom områdena terrorism, IT-säkerhet och cyberoperationer och informationspåverkan, för att bara nämna några. För att till del underlätta och effektivisera informationsdelning har myndigheterna vidtagit extra åtgärder för att stärka samarbetet och arbetat mer aktivt genom NCT och NSIT. Flera intervjupersoner varnade emellertid för att i alltför stor grad förlita sig på och/eller skapande av nya institutionaliserade samarbeten, som är mycket resurskrävande.

Det är också därför som framför allt underrättelsemyndigheterna istället under de senaste åren i allt högre grad satsat på samverkanspersoner som arbetar med att söka upp och tillmötesgå olika behov. Men även detta kostar i resurser och det går inte att vara överallt utan att det får konsekvenser för respektive myndighets kärnuppgifter. Det kan därför bara konstateras att det blir lite av ett moment 22, då förtroende bara kan byggas genom engagemang och tid, och detta verkar inte i linje för en bredare samverkan, utan det finns en risk att det snarare blir de redan etablerade strukturerna som förstärks och fördjupas, medan de mer perifera kan riskera att halka efter.

Om en ökad förståelse kan uppnås för de värderingar och incitament som ligger till grund för förtroende torde det inte vara omöjligt att till del ändra invanda rutiner och antaganden. Positiva förändringar kommer inte att uppstå genom att myndigheter tvingas att bete sig annorlunda, men genom att skapa förutsättningar för att utveckla personliga och förtroendefulla relationer går det att komma en bit. Men återigen, detta kräver tid och resurser och framför allt kräver det en strategisk drivkraft och en förståelse för att de positiva effekterna kommer först på lång sikt.

4.6 Otydlighet gällande rutiner och processer

De rutiner och processer som diskuterats med myndighetsrepresentanter har berört sådana som är direkt kopplade till förfaranden med syfte att efterfråga och delge hemlig information, liksom förfaranden för att utreda förutsättningarna för att delge hemlig information.

Det är tydligt att vissa underrättelsemyndigheter inte regelbundet delger hemlig information till alla de myndigheter som ingår i denna studieverksamhet och i synnerhet inte till Migrationsverket och Kustbevakningen. Detta förhållande avspeglas i att dessa myndigheter och till viss del även Tullverket framfört behov av att tydliggöra rutiner och utveckla strategier för samverkan och informationsutbyte med underrättelseproducenterna. Behoven gäller bland annat att tydliggöra rutiner och kontaktvägar för att framföra underrättelsebehov och inhämta information om andra myndigheters prioriteringar. Detta utgör främst ett problem

för myndigheter som inte ingår i inriktningsprocessen för försvarsunderrättelseverksamheten, där det varje år under ledning av Försvarsdepartementet, genomförs en särskild dialog avseende prioriteringar och diskussioner om förutsättningar för underrättelseproduktion.

En motsvarande process för civila krisberedskapsmyndigheter saknas. Detta innebär att det inte finns något forum för regelbundna och övergripande diskussioner om förutsättningar, behov och perspektiv avseende informationsdelning kopplad till civila krisberedskapsmyndigheter. Det medför även att gränssnittet mellan denna krets av myndigheter och de som ingår i inriktningsprocessen avseende underrättelseverksamheten fortsatt kommer att präglas av kulturskillnader och brister i förståelsen för prioriteringar och förutsättningar för delgivning.

Etablerade och tydliga rutiner för informationsdelning kopplas främst till den informationsdelning som sker inom ramen för existerande samverkansforum såsom arbetet mot grov organiserad brottslighet (NUC/RUC), ISEK, Samverkansrådet mot terrorism etc. Ett flertal myndigheter anger dock att en stor del av informationsdelningen utanför dessa forum sker ad hoc, inte sällan beroende på förekomsten av personliga kontakter mellan berörda myndigheter. Ad hoc-baserad informationsdelning kan medföra en rad olika risker, däribland att information som kanske bör delges inte delges i sådana situationer där individer inte har etablerade kontakter eller att information delges till andra personer än de som främst bör ta del av den.

Andra utmaningar kopplat till rutiner och processer gäller när hemlig information från underrättelseproducenter kan behöva delges myndigheter som normalt inte anses utgöra ”berörd myndighet” enligt 2 § lagen om försvarsunderrättelseverksamhet.

Begreppet ”berörd myndighet” uppges vara otydligt, vilket lett till en viss skillnad i tolkningen av detta mellan underrättelsemyndigheterna. Must gör en förhållandevis snäv tolkning av begreppet genom att utgå ifrån de myndigheter som anges i regeringens inriktning för försvarsunderrättelseverksamheten. FRA gör en något vidare tolkning av begreppet genom att relatera det till ”informationsberättigad totalförsvarsmyndighet i underrättelsefrågor”, där den avgörande betydelsen för att identifiera mottagare av underrättelser baseras på underrättelsens innehåll, vilket avgörs i varje enskilt fall.

En förutsättning för att underrättelsemyndigheterna ska kunna delge underrättelser till andra myndigheter är att samråd inhämtas från regeringskansliet. Hur detta samråd ska inhämtas har varit otydligt, vilket föranlett Must att hemställa hos Försvarsdepartementet om instruktioner för detta förfarande.

5 Slutsatser

5.1 Perspektiv på förutsättningar för delgivning av sekretess

Baserat på den information och de perspektiv som inhämtats kan författarna konstatera att det finns ett etablerat nationellt regelverk som medger delgivning av underrättelser mellan nationella myndigheter under sådana omständigheter som denna studie syftar till att belysa. Det kan även konstateras att det existerar ett antal faktorer som begränsar förutsättningarna för att utveckla informationsdelgivning i den riktning som en majoritet av de myndigheter som denna studie interagerat med anser är av stor vikt för att identifiera och möta existerande antagonistiska hot och säkerhetsutmaningar.

Vi kan samtidigt konstatera att den problematik som lyftes fram i studien avseende Krisberedskap och antagonistiska CBRN-hot: förutsättningar för samverkan mellan Underrättelsesektorn och krisberedskapssystemet inte är specifik för CBRN-relaterade utmaningar och hot. Begränsande faktorer för nationella förutsättningar för effektiv samverkan är mer generisk till sin natur. Dessa faktorer är av varierande karaktär, vilket kräver en rad olika åtgärder och resurser på olika nivåer för att hanteras under förutsättning att det på nationell central nivå finns ambitioner och målsättningar för att möjliggöra effektivare samverkan och informationsdelning.

Denna studie syftar främst till att kartlägga och lyfta fram de begränsningar och möjligheter som existerar. Det innebär att de slutsatser som dragits i studien inte presenterar några lösningar på de begränsande faktorer som identifierats. Däremot finns det anledning att vidareutveckla perspektiven avseende de områden som vi anser är centrala för att vidareutveckla förutsättningarna för informationsdelning mellan centrala myndigheter, vilket vi gör i detta avslutande kapitel.

Gränsdragningar mellan verksamhetsområden

Som framgått av avsnitt 3.1.1 finns en klar gräns mellan å ena sidan den brottsbekämpande verksamhet som bedrivs av Polismyndigheten och andra myndigheter med uppgifter inom samma område och å andra sidan den verksamhet som får bedrivas inom ramen för försvarsunderrättelseverksamhet. Denna skillnad har traditionella orsaker som att försvarsunderrättelsemyndigheterna haft monopol på underrättelseinhämtning utomlands och att polisiära myndigheter har monopol på maktutövning mot den enskilde, bl.a. genom att använda hemliga tvångsmedel. Givetvis har skiljelinjen också sin grund i skäl som hänger samman med grundläggande rättssäkerhetskrav och skydd av den personliga integriteten.

Signalspaningslagstiftningen är ett exempel på hur lagstiftaren försökt upprätthålla denna skillnad inom områden där det ansetts viktigt att även vissa myndigheter utanför försvarsunderrättelsesfären får del av resultat från signalspaning. Skillnaderna kommer till uttryck även på andra sätt, bl.a. genom de sekretessregler som beskrivits i avsnitt 3.2.2 och som innebär gränser för i vad mån de polisiära myndigheterna kan delge information utanför denna krets. Liknande detaljerade begränsningar finns inte när det gäller försvarsunderrättelsemyndigheternas möjligheter att lämna information till myndigheter utanför försvarsområdet, även om givetvis försvarssekretessen kan utgöra ett klart hinder.

Inte minst bekämpningen av terrorism har gjort det svårt att i alla delar upprätthålla en tydlig gränslinje mellan försvarsunderrättelseverksamhet och polisiär verksamhet. Denna svårighet är också tydlig i många andra länder. Enligt *guidelines* för FBI från 2008 sägs att utvecklingen går mot en eliminering av den traditionella väggen mellan utrikes underrättelseinhämtning, utförd av främst CIA, och *domestic law enforcement*, som varit FBI:s fält. I Storbritannien gör en ny *Investigatory Powers Act* det möjligt för såväl polisen som säkerhets- och underrättelsetjänsterna att själva samla in eller bereda sig tillgång till olika former av elektronisk information. I Finland har en arbetsgrupp i betänkandet *Riktlinjer för finsk underrättelselagstiftning* föreslagit att inte bara Försvarsmakten utan även skyddspolisen ska få befogenheter för inhämtning av underrättelser utomlands.

I Sverige har från moderat håll förts fram att Säkerhetspolisen bör få tillgång till signalspaning även inom ramen för en förundersökning, vilket skulle göra det möjligt att bedriva signalspaning i brottsutredande syfte. Förslaget har inget stöd hos regeringspartierna. Däremot råder inte någon tvekan om att statsmakterna anser det angeläget att myndigheterna blir bättre på att delge varandra behövlig information. Ett exempel på det är den under avsnitt 3.2.2 nämnda lagen om uppgiftsskyldighet vid samverkan mot grov organiserad brottslighet som trädde i kraft den 15 augusti 2016. Det är för tidigt att nu dra några slutsatser om lagens effekter.

När det gäller de brottsförebyggande myndigheternas möjligheter att delge information till myndigheter utanför det brottsbekämpande området är möjligheterna, delvis som en följd av den nyss nämnda gränsen mellan försvarsunderrättelseverksamhet och polisiär verksamhet, klart mer begränsade. Ett undantag är samarbetet inom NCT där ett förslag nu, som framgått av avsnitt 3.4.6, går ut på att ytterligare förbättra samarbetet genom att myndigheterna ges viss direktåtkomst till varandras register. Notabelt är att samma utredning föreslår att Säkerhetspolisen även ska kunna lämna ut uppgifter elektroniskt på annat sätt till Försvarsmakten och FRA. Avsikten är att de uppgifter som kan lämnas genom direktåtkomst även ska kunna lämnas på annat sätt digitalt. Det är en teknikneutralitet som eftersträvas och inte en utvidgning av informationsdelningsmöjligheten. Även med beaktande av detta innebär förslaget, om det genomförs,

något av ett trendbrott beträffande Säkerhetspolisens möjligheter att delge information till myndigheter utanför det brottsbekämpande området.

Trots vad som nu sagts bör betonas att varken i de skriftliga svar som erhållits under kartläggningen eller under de diskussioner som förts med myndighetsföreträdarna har det framkommit att nuvarande regelsystem utgör något betydande hinder för möjligheterna att delge varandra behövd information.

Begränsade resurser och ökad efterfrågan kräver skarpa prioriteringar

Liksom i många andra sammanhang står det klart att begränsade resurser vid de underrättelseproducerande myndigheterna i kombination med ökad efterfrågan av rapportering och delgivning skapar en tröskel mot att aktivt beakta en bredare krets av berörda myndigheters informationsbehov. Detta gäller sannolikt även i sådana fall där dessa behov ligger i linje med inriktande myndigheters behov, och i synnerhet när dessa uttrycks från den krets av myndigheter som kräver ett samrådsförfarande med Försvarsdepartementet innan delgivning kan genomföras. Dessa förhållanden kan som en konsekvens medföra att viktig information kanske inte delges berörda funktioner vid andra myndigheter i tid.

Begränsade resurser skapar även ett behov av att tillgängliga resurser koncentreras till sådana problemområden som är av högsta prioritet. Detta är nödvändigt i syfte att upprätthålla en hög kvalitet på den underrättelseproduktion som genomförs, men får konsekvensen att många problemområden inte bevakas i en utsträckning som kan vara av betydelse i en tid av diffusa, komplexa hot och säkerhetspolitiska skeenden i vårt närområde. Denna problematik utgör därför ytterligare en omständighet som begränsar möjligheterna för en ökad samverkan och informationsdelgivning, då skarpa prioriteringar begränsar sannolikheten för att andra myndigheters informationsbehov överensstämmer med inriktande myndigheters aktuella inriktning.

I takt med underrättelseverksamhetens ökade betydelse i ljuset av en alltmer osäker omvärld finns det små utsikter för att det som i dag betecknas som ett ökat tryck från inriktande myndigheter ska avta inom överskådlig framtid. En översyn behöver göras avseende hur det svenska systemet för underrättelseproduktion och delgivning kan utvecklas i ljuset av den trend av ökade behov och efterfrågan som råder, med hänsyn taget även till de centrala krisberedskapsmyndigheter som inte tillhör den existerande kretsen av myndigheter med inriktningsrätt. Detta gäller inte minst huruvida tilldelade resurser i termer av tekniska system för inhämtning, bearbetning och delgivning liksom tillgång till arbetskraft för den underrättelseproducerande verksamheten behöver förstärkas.

Anpassade system för överföring av hemlig information

En grundförutsättning för delgivning av information mellan myndigheter är att det finns information hos en part som andra behöver få tillgång till och att den myndighet som har tillgång till informationen är medveten om att andra parter

har behov av den. Den pågående processen för återupprättande av totalförsvarsplanering bland militära och civila myndigheter kommer sannolikt att leda till att bredden av berörda myndigheter gör en grundlig översyn av sin roll och funktion vid krissituationer och höjd beredskap i denna kontext, och som en effekt av detta även identifierar vilken typ av information som myndigheterna är beroende av för att leva upp till detta. I ljuset av den komplexa hotbild som vuxit fram under de senaste åren, där skalan av utmaningar omfattar diffusa informationssäkerhetsincidenter, spionage och påverkanskampanjer blandat med mer konkreta aspekter som terrorhot och allt mer aggressivt uppträdande av militära plattformar i närområdet, kommer behovet av information kopplat till hotperspektiv att öka.

För många myndigheter, både militära och civila, kommer behovet av information som man själv inte har tillgång till att vara betydande. Det är därför inte förvånande att den gemensamma grundsyn för en sammanhängande planering för totalförsvaret som MSB och Försvarsmakten presenterat har identifierat att förmågan att kunna dela information med krav på robusthet och sekretess är viktig.[17] Som i denna studie belysts finns det lösningar för delgivning av information med hög sekretessnivå, men att brister i tillgänglighet, tillämpning, kunskap och teknik medför att existerande förutsättningar för informationsdelning och samverkan inte är anpassad för dagens behov och än mindre framtida utmaningar.

Identifierade brister utgör dock ingen ny insikt då det i ett flertal underlag inom olika verksamhetsområden har pekats på liknande utmaningar. Ett exempel är utvärderingarna av fem nationella ickespridningsövningar, som bedrevs under 2007-2013, där tillgång till tekniska system, bristande insikt om olika myndigheters system och praxis avseende användning av dessa, orsakade påtagliga kommunikationsproblem vid hantering av skyndsamma ickespridningsärenden.[18] Riksrevisionen har i en granskning konstaterat att arbetet med informationssäkerhet inom den civila statsförvaltningen inte är ändamålsenlig i ljuset av en ökad hotbild. I denna kritik framförs bl.a. att det saknas en samlad lägesbild över existerande hot och risker avseende informationssäkerhet, att vidtagna åtgärder för att stärka förmågan är otillräckliga, att roller och ansvar är otydliga och att resurstilldelningen inom området är otillräcklig.[19]

[17] Sverige kommer att möte utmaningarna: Gemensamma grunder för en sammanhängande planering av totalförsvaret, FM2016-13584:3, 2016-06-10.
[18] UD Övrigt stöd, uppdragsprojekt: genomförd projektverksamhet och resultat, FOI-R-4005, december 2014, sid 14.
[19] Informationssäkerheten i den civila statsförvaltningen, Riksrevisionen, RIR 2014:23, 2014-11-10

Tillgänglighet av system som medger säker och flexibel överföring av information med hög sekretess mellan försvarsunderrättelsesystemet och berörda krisberedskapsmyndigheter är en grundförutsättning för att ett totalförsvarssystem ska kunna försörjas med insikter om och förhålla sig till utvecklingen av hot och risker i dag och i framtiden. Krisberedskapsförordningens krav enligt 30a § om att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller krav avseende säkerhet och funktion är synnerligen otillräckligt för att säkerställa att respektive myndighet kan genomföra sin verksamhet inom ramarna för ett samlat totalförsvar anpassat efter dagens hot och kriser. Att utveckla och driftsätta ett nationellt gemensamt och tillgängligt system för säker och flexibel överföring av information med hög sekretess kommer att bli dyrt, svårt och komplicerat. Ett grundläggande förarbete krävs där en kompetent funktion utreder existerande behov och förutsättningar för ett system, där erfarenheter och lösningar från andra relevanta länder med fördel kan utgöra en delkomponent.

En förtroendebransch där försiktighetsprincip tillämpas

Studien har tydligt visat att delgivning av försvarsunderrättelser är en förtroendebransch, och det oaktat om det berör den inre (underrättelsemyndigheterna) eller yttre (övriga krisberedskapsmyndigheter) kärnan. Det som också är tydligt är att det måste råda en försiktighetsprincip och det är ingen av de intervjuade myndigheterna som uttrycker något i linje att verkan får gå före skydd. Som ett tydligt exempel kan nämnas Försvarsmakten/Musts svar på den avslutande enkätfrågan[20], där de skrev att myndigheternas behov av försvarsunderrättelseinformation måste vägas mot behovet av att skydda information och källor.

Studiens slutsats och konstaterande är att försiktighetsprincipen är obestridlig, då det är tre aspekter som alltid måste skyddas:

1) den personliga integriteten
2) statens behov att skydda sina förmågor, metoder och källor
3) den faktiska underrättelsen eller informationen

Underrättelsemyndigheterna tar detta på stort allvar och de överlämnar heller enligt egen utsago aldrig information om de inte försäkrat sig om att den kan hanteras utifrån alla dessa tre aspekter. Detta leder givetvis till en inte obetydlig tröskel när det gäller distribution och nyttjande av underrättelser.

Tydligast blir denna tröskel när underrättelserapporteringen delas upp i vag eller konkret underrättelseinformation och om underrättelserapportering sker löpande

[20] Är existerande regelverk, rutiner och processer anpassade och effektiva för att möta ökat behov av informationsutbyte mellan statliga myndigheter? Om inte - vad skulle kunna utvecklas för att förbättra förutsättningarna för delgivning av underrättelsebaserad information på central nationell nivå?

eller sällan. Tröskeln blir som störst när underrättelserapporteringen ska ut till den yttre kärnan av berörda myndigheter och än större när informationen är både vag och sällan förekommande. Med vag information menar vi underrättelserapportering som är vag i sitt innehåll och vag ifråga om vem eller vilka som kan anses vara just berörd myndighet. Med respekt för försiktighetsprincipen blir studiens slutsats att det framför allt är bland dessa potentiella vaga sällanhändelser som det bör ske en analys för att se i vilka fall det kan finns skäl och behov för ett fördjupat samarbete för att därigenom bygga förtroende och tillit.

Ett område som kan vara aktuellt att studera djupare skulle t.ex. kunna vara det psykologiska försvaret och dess förmåga att identifiera, förstå och möta påverkans- och informationsoperationer. Här kan informationen, både till innehåll och avsändare, vara vag. Och även om den på bredden är vanligt förekommande kan den för olika berörda myndigheter i den yttre kärnan vara mer av sällankaraktär.

Regeringen har också i den försvarspolitiska inriktningens motivering om varför området psykologiskt försvar bör anpassas efter dagens förhållanden pekat på att en särskild utmaning vad avser påverkanskampanjer är att såväl öppna som dolda metoder kan nyttjas. Regeringens pekar också på att berörda myndigheter och aktörer redan under fredstid också ska kunna utföra försvarsåtgärder, att berörda aktörers samverkan stärks och utvecklas och att MSB:s stödjande roll är viktig för denna samverkan.[21]

När det gäller den inre kärnan blir slutsatsen att delgivning av underrättelserapportering synes fungera på avsett sätt, även om det kanske inte är orimligt att anta att en vag underrättelseinformation som sker förhållandevis sällan kan löpa en viss risk att hamna mellan stolarna. Däremot pekar studien på vikten av en tydlig styrning från regeringen att det är tydligt vilka som kan ha behov av underrättelseinformation. Detta är särskilt viktigt när det gäller försvarsunderrättelseinformation, då denna av Must endast delges till dem med inriktningsrätt.

[21] Prop. 2014/15:109, s. 109f

Bilaga 1 - Exempel på enkät

Möjligheter och begränsningar i överföring av underrättelsebaserad information mellan statliga myndigheter

FOI genomför på uppdrag av MSB i samverkan med CATS vid Försvarshögskolan en studie under 2016. Syftet med studien är att belysa förutsättningarna, med dess möjligheter och begränsningar, för underrättelse- och säkerhetstjänster att delge underrättelsebaserad information till totalförsvarsmyndigheter och andra berörda myndigheter. För att komplettera studien av offentligt tryck genomför studiegruppen en skriftlig enkätundersökning som under hösten följs upp med intervjuer.

Studiegruppen hemställer därför om ert stöd i detta arbete och skulle uppskatta om ni har möjlighet att besvara nedanstående frågeställningar.

Bakgrund

Studien har initierats mot bakgrund av de förändrade och mer komplexa säkerhetsutmaningar samt den ökade osäkerhet som råder avseende framtida antagonistiska hot mot samhället. En mer oförutsägbar utveckling ökar betydelsen av att underrättelseverksamhet utifrån sina förutsättningar och gällande regelverk kan bidra till och stödja beslutsfattandet inom den nationella krisberedskapen. En väl fungerande informationsdelning mellan aktörer inom ett nationellt totalförsvar utgör en grundläggande förutsättning för att förhindra, upptäcka och hantera allvarliga antagonistiska hot. I en tidigare studie (FOI-RH-1460, okt 2014) framkom att det inom CBRN-området råder en klyfta mellan försvarsunderrättelse- och säkerhetstjänsterna och den breda kretsen av krisberedskapsmyndigheter som till del har sin förklaring i strukturella barriärer.

Denna studie söker därför belysa nationella förutsättningar genom att söka svar på följande övergripande frågeställningar:

Vilka huvudsakliga delar av nationellt regelverk styr delgivning av underrättelsebaserad information?

Hur tolkas regelverket av nationella underrättelse- och säkerhetstjänster?

Vilka processer och rutiner finns för delgivning av information till statliga myndigheter som normalt inte på regelbunden basis tar emot sådan information?

Frågor avseende tolkning av regelverk:

1. Enligt 2 § lagen(2000:130) om försvarsunderrättelseverksamhet ska underrättelser rapporteras till *berörda myndigheter.* Hur tolkar myndigheten detta begrepp?

2. I 7 § förordningen (2000:131) om försvarsunderrättelseverksamhet talas om *informationsberättigad totalförsvarsmyndighet.* Hur tolkar myndigheten detta begrepp? Ange om möjligt vilka myndigheter som i den egna myndighetens perspektiv är mest relevanta.
3. I 7 § förordningen om försvarsunderrättelseverksamhet anges att försvarsunderrättelsemyndigheten ska samråda med Regeringskansliet om myndigheten vill orientera annan än informationsberättigad totalförsvarsmyndighet. När kan en sådan åtgärd bli aktuell? Exemplifiera gärna med verkligt eller tänkt exempel. Är det några särskilda författningsbestämmelser som mera frekvent försvårar/förhindrar att en orientering sker till annan myndighet?
4. Har det förekommit att 15 kap. 1 § eller 2 § offentlighets- och sekretesslagen (2009:400) hindrat att underrättelsebaserad information lämnats till annan myndighet trots att det vid er myndighet bedömts att annan myndighet skulle ha behövt uppgiften i sin verksamhet? Är detta en vanlig eller ovanlig situation?
5. Har det förekommit att 38 kap. 4 § offentlighets- och sekretesslagen hindrat att underrättelsebaserad information lämnats till annan myndighet trots att det vid er myndighet bedömts att annan myndighet skulle ha behövt uppgiften i sin verksamhet? Är detta en vanlig eller ovanlig situation?
6. Enligt 8 § förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet anges att Försvarets radioanstalt får ha direktåtkomst till uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet *i den omfattning som Försvarsmakten beslutar.* Vilka principer styr i huvudsak de överväganden som blir aktuella i detta sammanhang?
7. På liknande sätt som under fråga 7 beslutar Försvarsmakten om Säkerhetspolisens direktåtkomst till uppgifter i en uppgiftssamling för säkerhetsskyddstjänst. Vilka principer styr i huvudsak de överväganden som blir aktuella i detta sammanhang?

Frågor angående tillämpning och rutiner av informationsdelning:

8. Vilka existerande rutiner styr hur underrättelsebaserad information kan delges andra berörda myndigheter?
9. Vilka beslut behöver tas och på vilken nivå för att möjliggöra sådan delgivning?

10. Kan ni ge exempel på när sådan delgivning skett och/eller exempel på när sådan delgivning inte varit möjlig och i så fall varför?
11. Hur tillgänglig är information om existerande rutiner för informationsdelgivning för andra berörda myndigheter som normalt inte erhåller information från Försvarsmakten?
12. Är existerande regelverk, rutiner och processer anpassade och effektiva för att möta ökat behov av informationsutbyte mellan statliga myndigheter? Om inte - vad skulle kunna utvecklas för att förbättra förutsättningarna för delgivning av underrättelsebaserad information på central nationell nivå?

Fortsatt arbete

Studiegruppen önskar svar på frågorna i skriftlig form som skickas till undertecknad, senast den 27 juni 2016.

Studiegruppen önskar även följa upp enkätsvaret genom en muntlig dialog med relevanta representanter från er organisation. Tidsramarna för uppföljande dialog är planerad till perioden 29 augusti-16 september 2016.

Studiens resultat delges MSB i skriftlig form i december 2016.

Med vänlig hälsning

Magnus Normark
Tel: 076-102 41 61
E-post: magnus.normark@foi.se

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se