Europeiska unionens råd

Bryssel den 28 juli 2017
(OR. en)

8188/1/17
REV 1 DCL 1

GENVAL 42
CYBER 57

BORTTAGANDE AV SÄKERHETSSKYDDSKLASSIFICERING

för dokument:	8188/1/17 REV 1 RESTREINT UE/EU RESTRICTED
Ny status:	Offentlig
Ärende:	Utvärderingsrapport om den sjunde omgången av ömsesidiga utvärderingar "Det praktiska genomförandet av europeisk politik för förebyggande och bekämpning av it-brottslighet" – Rapport om Sverige

För delegationerna bifogas ovannämnda dokument för vilket säkerhetsskyddsklassificeringen tagits bort.

Texten är identisk med föregående version.

Europeiska unionens råd

Bryssel den 18 maj 2017
(OR. en)

8188/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 42
CYBER 57

RAPPORT

Ärende:	Utvärderingsrapport om den sjunde omgången av ömsesidiga utvärderingar "Det praktiska genomförandet av europeisk politik för förebyggande och bekämpning av it-brottslighet" – Rapport om Sverige

BILAGA

Innehållsförteckning

1 SAMMANFATTNING

De svenska myndigheterna hade förberett besöket väl. Det innehöll bland annat möten med relevanta aktörer med ansvar dels för förebyggande och bekämpning av it-brottslighet, dels för genomförande och tillämpning av EU-politiken, t.ex. Justitiedepartementet, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Myndigheten för samhällsskydd och beredskap (MSB) och Ecpat Sverige.

Under besöket på plats försåg de svenska myndigheterna utvärderingsgruppen med tillräcklig information om rättsliga och operativa aspekter av förebyggande och bekämpning av it-brottslighet, gränsöverskridande samarbete och samarbete med EU-byråer. Därmed kunde utvärderingsgruppen utföra en tillfredsställande översyn av systemet och identifiera god praxis att utbyta med andra medlemsstater.

För Sverige är kampen mot it-brottslighet en prioritering och flera åtgärder har redan vidtagits som vittnar om detta. Dock har Sverige för närvarande ingen nationell strategi för cybersäkerhet. Sveriges regering håller på att utarbeta en sådan strategi, som ska innehålla prioriteringar för de olika fristående statliga organen samt fastställa uppföljningsförfaranden. Den bör även innebära att tillräcklig samordning mellan alla aktörer säkerställs.

Sverige har ännu inte ratificerat konventionen om it-brottslighet (undertecknad av Sverige den 23 november 2001). Under besöket på plats bekräftade myndigheterna sin avsikt att ratificera konventionen under den nuvarande mandatperioden, som löper ut 2018. En ratificering kommer med säkerhet att innebära ett starkare internationellt samarbete mellan Sverige och parterna i konventionen (51 stater).

Generellt anser Sverige att den nationella lagstiftning enligt vilken it-brottslighet straffas är tillräcklig och stämmer överens med EU-lagstiftningen. Överträdelserna beskrivs i så tekniskt neutrala termer som möjligt, snarare än utifrån definitionerna i EU-lagstiftningen. Detta kan innebära att lagstiftningen lösgörs från den vidare tekniska utvecklingen, men det kan även orsaka rättsosäkerhet och svårigheter i praktiken och när det gäller jämförbar statistik.

Sverige har inlett flera rättsliga undersökningar i syfte att förbättra den rättsliga ramen och anpassa den till problem som rör it-brottslighet. Mot bakgrund av att rättegångsbalken infördes 1942 och många avsnitt inte har ändrats sedan dess, framhöll åklagarna vissa problem när det gäller den praktiska tillämpningen av lagen, vilken ibland ger upphov till rättsosäkerhet.

Den statistik som har lagts fram för utvärderingsgruppen förefaller vara ofullständig. Bristen på detaljerad, uttömmande och standardiserad statistik om it-brottslighet kan leda till svårigheter att identifiera de främsta hoten mot den svenska cyberrymden. En utredning av hur statistik samlas in pågår dock.

Typiskt för ämnesområdet är också att ett stort antal it-brott inte anmäls. Den privata sektorn är inte förpliktad att anmäla brott, även när kritisk infrastruktur berörs. Sverige genomför för närvarande it-säkerhetsdirektivet[1].

[1] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Nationellt it-brottscentrum (SC3) har inrättats som en specialiserad byrå inom den svenska polisen. SC3 är inriktat på de mest komplexa fallen av it-brottslighet. Därtill kommer det på regionnivå att tillhandahålla tekniskt stöd, bästa praxis, utbildning, uppdateringar och underrättelseinsamling. SC3 samarbetar nära med specialiserade åklagare, på ett informellt och stödjande sätt.

Åklagarmyndigheten har genomfört åtgärder för att stärka kapaciteten att utreda it-brott och öka den allmänna kunskapen i detta avseende. 2015 inrättades ett särskilt nätverk för åklagare som hanterar fall av it-brottslighet. Åklagarna i nätverket har tillgång till en särskild webbplats där de kan diskutera olika operativa frågor och utbyta information om exempelvis ny lagstiftning och relevanta domar. De får avancerad utbildning om it-brottslighet och har särskilda erfarenheter på området.

De yrkesverksamma som man träffade under utvärderingen höll med om att juridisk utbildning och juridisk expertis för att bekämpa it-brottslighet måste förbättras.

I Sverige finns allmänt sett ett långtgående samarbete mellan den offentliga och den privata sektorn när det gäller bekämpning och förebyggande av it-brottslighet. Sverige fokuserar på både förebyggande arbete och insatser för att öka medvetenheten. När det gäller bekämpande av sexuellt utnyttjande av barn online, har Sverige en imponerande och väl integrerad strategi, och man samarbetar nära med olika statliga och privata aktörer. Material på internet som rör sexuellt utnyttjande av barn blockeras på lämpligt sätt, oavsett var värddatorn är lokaliserad.

På området ömsesidig rättslig hjälp bistår svenska myndigheter andra stater i största möjliga utsträckning och genom samma åtgärder som är tillgängliga för de svenska myndigheterna i inhemska utredningar eller förfaranden. I detta syfte har ett övergripande registreringssystem inrättats vid den svenska polismyndigheten. Tack vare detta tar det i allmänhet som längst två månader att behandla en begäran om ömsesidig rättslig hjälp.

Ett viktigt inslag i Sveriges framgångsrika insatser för att upprätta samarbete med privata motparter i USA har varit att hantera alla begäranden och svar genom en enda kontaktpunkt. Genom att tillämpa konceptet med en enda kontaktpunkt har behandlingen av begäranden kunnat ske friktionsfritt för både den svenska polisen och dess motparter i USA.

Med hänsyn till Sveriges ambitiösa inställning när det gäller bekämpande av it-brottslighet och landets avsikt att kontinuerligt stärka it-säkerheten anser utvärderingsgruppen att utsikterna i Sverige är lovande.

2 INLEDNING

Till följd av antagandet av gemensam åtgärd 97/827/RIF av den 5 december 1997[2] infördes en ordning för utvärdering av tillämpning och genomförande på nationell nivå av internationella åtaganden i kampen mot den organiserade brottsligheten. I enlighet med artikel 2 i den gemensamma åtgärden beslutade arbetsgruppen för allmänna frågor, inklusive utvärdering, den 3 oktober 2013 att den sjunde omgången av de ömsesidiga utvärderingarna skulle ägnas åt det praktiska genomförandet av europeisk politik för förebyggande och bekämpning av it-brottslighet.

Medlemsstaterna välkomnade att it-brott valts som ämne för den sjunde omgången av den ömsesidiga utvärderingen. På grund av den stora mängd överträdelser som omfattas av termen it-brottslighet enades man emellertid om att utvärderingen skulle riktas in på de överträdelser som medlemsstaterna ansåg behövde särskild uppmärksamhet. Därför omfattar utvärderingen tre särskilda områden: it-angrepp, sexuella övergrepp mot barn/barnpornografi online och betalkortsbedrägerier online. Utvärderingen skulle omfatta en utförlig granskning av de rättsliga och operativa aspekterna av hanteringen av it-brottslighet, gränsöverskridande samarbete och samarbete med relevanta EU-byråer. Direktiv 2011/93/EU om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi[3] (införlivandedatum: den 18 december 2013) och direktiv 2013/40/EU[4] om angrepp mot informationssystem (införlivandedatum: den 4 september 2015) äger särskild relevans i sammanhanget.

2 Gemensam åtgärd 97/827/RIF av den 5 december 1997, EGT L 344, 15.12.1997, s. 7.
3 EUT L 335, 17.12.2011, s. 1.
4 EUT L 218, 14.8.2013, s. 8.

I rådets slutsatser om EU:s strategi för cybersäkerhet från juni 2013[5] erinras dessutom om målet att så snart som möjligt ratificera Europarådets konvention om it-brottslighet (Budapestkonventionen)[6] av den 23 november 2001 och i ingressen betonas att "EU kräver därför inte att nya internationella rättsliga instrument skapas för cyberfrågor". Konventionen kompletteras med ett protokoll om rasistiska eller främlingsfientliga handlingar som utförs med hjälp av it-system[7].

Erfarenheter från tidigare utvärderingar visar att medlemsstaterna kommer att befinna sig på olika stadier när det gäller genomförandet av relevanta rättsliga instrument och den nuvarande utvärderingsprocessen kan utgöra ett värdefullt bidrag för medlemsstater som kanske inte har genomfört alla delar av de olika instrumenten. Målet med utvärderingen är ändå att den ska vara bred och tvärvetenskaplig och inte bara fokusera på genomförandet av olika instrument som rör bekämpandet av it-brottslighet, utan snarare på de operativa aspekterna i medlemsstaterna.

Förutom samarbete med åklagarmyndigheter kommer detta därför även att omfatta hur polismyndigheter samarbetar med Eurojust, Enisa och EC3 (Europol) och hur återkoppling från dessa aktörer dirigeras till den berörda avdelningen inom polisen eller socialtjänsten. Utvärderingen är inriktad på genomförandet av nationell politik med avseende både på stävjande av it-angrepp och bedrägeri samt på barnpornografi. Utvärderingen omfattar även operativ praxis i medlemsstaterna när det gäller internationellt samarbete och stöd till offer för it-brottslighet.

[5] 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

[6] CETS nr. 185, öppna för undertecknande den 23 november 2001, trädde i kraft den 1 juli 2004.

[7] CETS nr. 189, öppna för undertecknande den 28 januari 2003, trädde i kraft den 1 mars 2006.

Beslutet om i vilken ordning medlemsstaterna skulle besökas fattades av arbetsgruppen för allmänna frågor, inklusive utvärdering, den 1 april 2014. Sverige var den 28:e medlemsstaten som besöktes under denna utvärderingsomgång. I enlighet med artikel 3 i den gemensamma åtgärden upprättade ordförandeskapet en förteckning över experter med erfarenhet av de ämnen som utvärderingen gällde. I enlighet med den skriftliga begäran som ordföranden för arbetsgruppen för allmänna frågor, inklusive utvärdering, utfärdade den 28 januari 2014 utnämnde medlemsstaterna experter med fördjupad erfarenhet på området.

Utvärderingsgrupperna består av tre nationella experter, som bistås av två anställda från rådets generalsekretariat samt observatörer. Inför den sjunde omgången av ömsesidiga utvärderingar godtog arbetsgruppen för allmänna frågor, inklusive utvärdering, ordförandeskapets förslag att Europeiska kommissionen, Eurojust, Enisa och EC3 (Europol) skulle bjudas in som observatörer.

Följande experter gavs ansvaret för utvärderingen av Sverige: Cristina Schulman (Rumänien), Robrecht De Keersmaecker (Belgien) och Marcin Golizda-Bliziński (Polen). Följande observatörer närvarade också: Tjabbe Bos (Europeiska kommissionen) och Murat Ayilmaz (Eurojust), tillsammans med Michael Carlin och Sławomir Buczma från rådets generalsekretariat.

Denna rapport utarbetades av expertgruppen med bistånd av rådets generalsekretariat, baserat på resultaten av det utvärderingsbesök i Sverige som ägde rum mellan den 27 och 30 september 2016 samt de detaljerade svar på frågeformuläret och uppföljningsfrågorna som Sverige gav.

3 ALLMÄNNA FRÅGOR OCH STRUKTURER

3.1 Nationell strategi för cybersäkerhet

Utarbetandet av en nationell strategi för cybersäkerhet pågår för närvarande i Sverige. Målsättningen är bland annat att ytterligare öka Sveriges kapacitet och tillhandahålla en övergripande strategi för att bekämpa alla aspekter av it-brottslighet. Den nationella strategin för cybersäkerhet förväntas införas senast sommaren 2017.

Även om det vid tiden för besöket på plats inte fanns något utkast till dokument tillgängligt, uppgavs att den kommande strategin för cybersäkerhet kommer att innehålla en inledning och utgöra en övergripande vägledning för en rad pågående och planerade åtgärder.

3.2 Nationella prioriteringar avseende it-brottslighet

De senaste åren har särskild uppmärksamhet ägnats åt ett antal politikområden, däribland lagstiftning, organisation, utbildning, internationellt samarbete etc.

Det finns några kopplingar mellan EU:s prioritering för it-brottslighet och det arbete som den svenska polisen gör på området it-brottslighet. Sverige deltar i den internationella samarbetsöverenskommelse baserad på dessa prioriteringar. EU-direktiv och rekommendationer från EU ligger till grund för en del av det arbete som utförs inom ramen för Sveriges it-brottscentrum. Exempelvis används Europols hotbildsbedömning av internetstödd organiserad brottslighet (Iocta) som grund för underrättelsearbete när det gäller it-brottslighet.

De svenska myndigheterna är av åsikten att information om de aktuella prioriteringarna och kopplingen mellan EU:s prioriteringar och nationella prioriteringar skulle kunna synliggöras mer för personalen.

3.3 Statistik om it-brottslighet

Brottsförebyggande rådet (Brå) är en myndighet under justitiedepartementet som tar fram och offentliggör officiell brottsstatistik för Sverige. Brottsstatistiken omfattar bland annat antalet anmälda brott, personuppklaringar och domsstolsbeslut. Eftersom inte alla brott anmäls, speglar inte uppgifterna de verkliga nivåerna av kriminalitet. Statistiken påverkas även av förändringar av benägenheten att anmäla brott, av omfattande fall (dvs. fall som innebär ett ovanligt högt antal rapporterade brott) vissa år och av myndigheternas fokus på olika typer av brott, trots att de verkliga nivåerna av kriminalitet kan vara oförändrade. Det är Polismyndighetens ansvar att registrera anmälningar av misstänkta brott i systemet. Detta kan ske antingen på grundval av ett klagomål eller information från en privatperson eller ett företag eller, vilket ofta är fallet, med utgångspunkt i polisens eget arbete exempelvis i samband med övervakning.

Den officiella statistiken omfattar alla brott som enskilda individer eller den offentliga eller privata sektorn har anmält till brottsbekämpande myndigheter. Det är omöjligt att identifiera alla brott med koppling till it-brottslighet, men det finns uppgifter om brott som på olika sätt är it-relaterade. Mängden och/eller kategorierna av uppgifter som de olika aktörerna (polis, åklagare etc.) rapporterar är dock inte alltid heltäckande och förenliga. Brå har sammanställt en rapport där omfattningen av it-relaterade inslag bland anmälda brott kartläggs. Rapporten offentliggjordes i september 2016.

3.3.1 Huvudsakliga trender som leder till it-brottslighet

De senaste åren har förekomsten av datorrelaterade bedrägerier och bedrägeri som utförs via internet ökat. Olika typer av trakasserier och hot på internet, t.ex. på sociala medier, förefaller också hat, även om en sådan trend inte kan bekräftas i siffror, eftersom det inte finns belägg i form av officiella uppgifter. Exempel på huvudsakliga trender är ransomware, samordnade överbelastningsattacker (DDos) (isolerade attacker och attacker som omfattar utpressning), banksabotageprogram, "crime-as-a-service" och vd-bedrägerier (business email compromise (BEC)).

3.3.2 Antal anmälda fall av it-brottslighet

Uppgifter om olika typer av it-relaterade brott i Sverige 2014 och 2015.

Brottstyp	*Anmälda brott*	*Utredda brott*	*Personuppklaringar*[8]	*Domstolsbeslut*[9]	*Misstänkta personer*
Datorbedrägeri	42 883/ 67 085	13 136/ 14 570	745/391	Uppgifter ej tillgängliga	440/427
Bedrägerier via internet	23 528/ 24 124	13 483/ 13 012	2 674/ 2 537	Uppgifter ej tillgängliga	908/909
Internetrelaterade barnpornografibrott	738/488	865/502	617/307	Uppgifter ej tillgängliga	214/181
Obehörigt tillträde till eller utnyttjande av ett datorsystem	8 200/6 663	3 266/4 050	1 089/1 753	108/63	217/219

[8] Personuppklaring innebär att en misstänkt person har bundits vid brottet genom att åtal har väckts, strafföreläggande har utfärdats eller åtalsunderlåtelse har meddelats.

[9] Domstolsdomar (såsom fängelsestraff, skyddstillsyn och uppskjuten påföljd), strafföreläggande och åtalsunderlåtelse.

Två andra brott som ofta begås via internet, även om förekomsten inte kan fastställas utifrån den officiella brottsstatistiken, är kontakt med barn i sexuellt syfte (gromning) och utnyttjande av barn under 18 år för sexuell posering:

Brottstyp	*Anmälda brott*	*Utredda brott*	*Personuppklaringar*	*Domstolsbeslut*	*Misstänkta personer*
Kontakt med ett barn i sexuellt syfte (gromning)	143/140	130/110	12/4	0/1	25/12
Utnyttjande av barn under 18 år för sexuell posering	1 513/991	1 378/1 119	1 017/642	20/27	101/116

3.4 Nationellt budgetanslag för förebyggande och bekämpande av it-brottslighet samt stöd i form av EU-medel

I sitt årliga beslut om budgetanslag till organen vägleds regeringen av målsättningar och särskilda prioriteringar. Riksdagen och regeringen beslutar om inriktningen och villkoren för verksamhet på central myndighetsnivå samt om vilken verksamhet och vilka ansvarsområden de olika organen ska tilldelas. Organen har långtgående befogenheter i sitt dagliga operativa arbete och regeringen kan enligt grundlagen inte ingripa i individuella fall. Det är dock regeringens uppgift att styra organen och att se till att de fullgör sina skyldigheter, genom den reguljära tilldelningen av anslag, lagstiftning, regeringsuppdrag, utredningar osv.

It-brottslighet är en av de prioriteringar som fastställts inom ramen för det nationella programmet för genomförande av Fonden för inre säkerhet. Under de kommande åren kommer därför projekt om it-brottslighet och it-säkerhet som finansieras genom Fonden för inre säkerhet att genomföras. Den svenska polisen har deltagit och deltar därtill i vissa projekt som finansieras inom ramen för grenen säkra samhällen inom Horisont 2020. För närvarande deltar den svenska polisen i ett konsortium med österrikiska Bundeskriminalamt och dess tyska motsvarighet för att ta fram ett bud för säkra samhällen vad gäller virtuella valutor och darknet.

3.5 Slutsatser

- Sverige har ingen nationell strategi för cybersäkerhet, men man håller för närvarande på att utarbeta en sådan för att kunna tillhandahålla en övergripande strategi för att bekämpa it-brottslighet. Avsaknaden av en sådan strategi hindrar inte Sverige från att aktivt bekämpa och förebygga it-brottslighet. Experterna anser dock att dessa insatser riskerar att bli ett lappverk utan en övergripande nationell strategi för cybersäkerhet.

- Sverige saknar även en gemensamt överenskommen uppsättning prioriteringar när det gäller it-brottslighet, särskilt för att bekämpa it-brott som begås av organiserade kriminella grupper och som genererar stora vinster. Exempel på sådana är bedrägerier online och betalkortsbedrägerier, it-brott såsom sexuell exploatering av barn online, vilket allvarligt skadar offren, och it-attacker, som påverkar kritisk infrastruktur och informationssystem i EU.

- Justitiedepartementet är den institution som har huvudsakligt ansvar för att se till att dessa uppgifter utförs. Därtill sker samarbete med andra departement såsom Näringsdepartementet, Utrikesdepartementet och Utbildningsdepartementet, i enlighet med fastställda förfaranden och metoder. Som ett exempel har en departementsöverskridande arbetsgrupp formellt inrättats på området it-säkerhet.

- Den privata sektorn är inte direkt inblandad i utarbetandet av den kommande nationella strategin för cybersäkerhet, men intressenter från den privata sektorn deltar i det befintliga nätverket för rådgivande plattformar. Slutförandet av strategin inbegriper deras bidrag.

- Trots att viss statistik om it-brottslighet finns tillgänglig, verkar den ofta hänvisa till informationsteknik i allmänhet och inte till klart angivna kategorier it-brott. Det uppgavs att polisen samlar in alla uppgifter om anmälningar, men det är oklart varför de olika aktörerna (olika avdelningar inom polisen, åklagare etc.) uppger olika siffror och/eller kategorier.

- Sveriges regering genomför sina strategier genom att anslå resurser, snarare än på ett hierarkiskt sätt. Avsaknaden av en nationell cyberstrategi ser ut att hindra en klar överblick över de totala belopp som avsätts för att bekämpa och förebygga it-brottslighet.

4 NATIONELLA STRUKTURER

4.1 Domstolsväsende (åklagarmyndigheter och domstolar)

4.1.1 Intern struktur

Domstolar

It-brott handläggs av de allmänna domstolarna (tingsrätt, hovrätt och Högsta domstolen) på samma sätt som andra brottsliga handlingar. Det finns ingen formell inriktning på området it-brottslighet för domare, men det verkar som att domare som hanterar ärenden som rör it-brottslighet får viss utbildning eller stöd. De olika partnerna ansåg att bristen på fördjupade kunskaper bland domare utgör ett hinder för effektiv brottsbekämpning.

Åklagarmyndigheter

Brottsutredningar omfattas av åklagarväsendets verksamhet. It-brott handläggs av åklagarväsendet, men det finns även åklagare som är specialiserade på it-brottslighet och som har ett nära samarbete inom ramen för ett nätverk, med ett omfattande utbildningsprogram för varje åklagare och en avancerad kursplan för specialisterna. I åklagarväsendet ingår Åklagarmyndigheten och Ekobrottsmyndigheten.

Åklagarmyndigheten

Det finns sju geografiska åklagarområden och en nationell åklagaravdelning. Åklagarområdena består av 32 allmänna kammare, som har ett geografiskt arbetsfält ungefär motsvarande ett län. I myndigheten ingår även tre internationella åklagarkammare, som är belägna i Stockholm, Göteborg och Malmö.

Ekobrottsmyndigheten

Ekobrottsmyndigheten är en specialistmyndighet inom åklagarväsendet vars uppgift är att bekämpa ekobrott, såsom bokföringsbrott, skattebrott och brottslighet mot EU:s ekonomiska intressen. På myndighetens ansvar ligger även att samverka med andra myndigheter för att vidta åtgärder mot ekobrott. På myndigheten arbetar även poliser, ekorevisorer och analytiker.

4.1.2 Kapacitet och hinder för ett framgångsrikt åtal

Åklagarmyndigheten har nyligen genomfört åtgärder för att stärka kapaciteten att utreda it-brott och öka den allmänna kunskapen i detta avseende. Exempelvis inrättade Åklagarmyndigheten under 2015 ett nätverk av åklagare som hanterar it-brott. Nätverket består av 16 åklagare som företräder olika regioner och är geografiskt spridda över landet. Åklagarna har gått olika kurser om hur man hanterar it-brottslighet och har särskilda erfarenheter på detta område. Åklagarna i nätverket har tillgång till en särskild webbplats på Åklagarmyndighetens intranät där de kan diskutera olika frågor och problem och utbyta information om exempelvis ny lagstiftning och intressanta domar. De anordnar seminarier och samarbetar med polisen. Andra åklagare kan vända sig till åklagarna i nätverket med frågor som rör it-brottslighet.

Ytterligare ett exempel som nämns är den webbaserade vägledning för åklagare som lanserades 2015. Vägledningen innehåller information om bland annat tvångsåtgärder med anknytning till it-brottslighet, under vilka omständigheter användarinformation/IP-adresser kan erhållas från leverantörer av internettjänster, processen för ömsesidig rättslig hjälp och begäran om kvarstad etc. Vägledningen innehåller även kontaktuppgifter för internationella företag som tillhandahåller internettjänster (Facebook, Google m.fl.), vilket är viktigt eftersom bevismaterial ofta finns i dessa företags ägo och åklagarna behöver ta reda på om det finns möjlighet att ta del av dessa uppgifter och i så fall hur de ska gå till väga. It-brottsligheten förändras ständigt. Den webbaserade vägledningen kommer att ändras och uppdateras kontinuerligt.

Det främsta hinder som Åklagarmyndigheten rapporterade var att erhålla IP-adresser och grundläggande information om abonnenter från vissa leverantörer av internettjänster. Kanada är av visst intresse, eftersom applikationen KIK är kanadensisk och frivilligt utlämnande av uppgifter inte är tillåtet. Detta innebär att åklagarna måste använda sig av ömsesidig rättslig hjälp för att erhålla den information de behöver.

4.2 Brottsbekämpande myndigheter

Den 1 januari 2015 slogs Rikspolisstyrelsen och de 21 polismyndigheterna samman till en myndighet, samtidigt som Säkerhetspolisen blev en egen myndighet. Omorganisationen var den största inom den offentliga sektorn på många år och den största förändringen för den svenska polisen sedan verksamheten blev statlig 1965. Syftet med reformen var att ta tag i organisatoriska hinder inom polisen och därmed skapa bättre förutsättningar för polisen att förebygga, vidta åtgärder mot och utreda brott.

Myndigheten består av sju polisregioner, ett antal nationella avdelningar och ett kansli. De sju polisregionerna har helhetsansvar för polisverksamheten inom ett angivet geografiskt område. Ansvaret omfattar bland annat utredningsverksamhet, brottsförebyggande verksamhet och service. Varje region leds av en regionpolischef. Polismyndigheten leds av en rikspolischef, som utses av regeringen. Rikspolischefen bär ensam ansvaret för myndighetens verksamhet.

Den första oktober 2015 inrättade den svenska polisen ett **it-brottscentrum** (SC3) med huvudmålsättningen att bygga upp kapaciteten inom hela polisen att utreda alla typer av it-brott. SC3 kommer att byggas upp successivt och kommer att omfatta specialiserade utredare, analytiker, kriminaltekniker och experter. Underrättelseteamet vid nationellt it-brottscentrum ansvarar för att upptäcka, förebygga och förhindra allvarliga it-brott. Teamet strävar efter att utbyta information med relevanta partner om aktuella trender, hot och särskild teknisk information (IOC's – Indicators of Compromise, (riskindikatorer)).

Man rekryterar för närvarande medarbetare till SC3 och målet är att vara full personalstyrka senast i slutet av 2017. SC3 är kontaktpunkt för svenska åklagarkammare och domstolar, men även för privata enheter på området it-brottslighet. Det har även befogenhet att hantera de viktigaste och största fallen av it-brottslighet. För att kunna utföra sina uppgifter har SC3 mobila grupper som stöder de regionala polisavdelningarna i frågor som rör it-brottslighet. Avsikten är att skapa it-brottscentrum i samtliga sju polisregioner. SC3 har en egen utredningsenhet som hanterar internetövervakning, automatisk insamling av information i sociala medier, säkring av webbsidor och hemliga insatser. Utredningsenheten har underenheter som är specialiserade på begäranden till informationssändande stationer, underrättelse, kriminalteknisk analys av digitala medier, metodutveckling, samordning och skydd för barn samt en särskild polisenhet som bekämpar it-brott på darknet.

SC3 anordnar nationella utbildningar för brottsbekämpande myndigheter. Det har även byggt upp en särskild webbplats för brottsbekämpning, där erfarenheter och expertis kan utbytas och erhållas. Centrumet erbjuder även utbildningstillfällen med åklagare och brottsbekämpande myndigheter. SC3 samarbetar nära med EC3, i nordiska sammanhang, Interpol samt många internationella organ på bilateral nivå. Centrumet har jourtjänst dygnet runt via den ansvariga tjänstemannen vid den nationella operativa avdelningen. Denna funktion inrättades för många år sedan i samband med arbete som utfördes inom ramen för G8-ländernas Lyongrupp i syfte att genomföra konventionen om it-brottslighet (Budapestkonventionen)

År 2013 inrättades ett **nationellt bedrägericentrum**. Erfarna polistjänstemän från det nationella bedrägericentrumet ger regionalt och lokalt stöd till utredare och delar med sig av bästa praxis. För att kunna stå i främsta ledet samarbetar nationellt bedrägericentrum med Nationellt forensiskt centrum och nationellt it-brottscentrum. Centrumet genomför inte utredningar, utan bedriver enbart samordnande och stödjande verksamhet. För närvarande är arbetet inriktat på kortlösa bedrägerier (card not present-bedrägerier). Tidigare genomförde det en informationskampanj om vd-bedrägerier (business email compromise) riktad till verkställande direktörer.

Det nationella bedrägericentrumet har exempelvis en databas över bankkonton som redan har granskats i tidigare utredningar under de senaste två åren. Polisen söker i databasen innan man begär information om bankkonton. Databasen bygger på ett system med träff/icke träff. När en sökning ger träff får utredaren numret på det fall i samband med vilket den tidigare begäran gjordes och informationen kan erhållas via officiella kanaler. Om sökningen inte ger någon träff sänds en ny begäran automatiskt till banken. Begäran görs på standardformulär, så att svaren från bankerna kan automatiseras. Det nationella bedrägericentrumet har även utarbetat en handbok om virtuella valutor.

Enligt åklagarna behöver de svenska brottsbekämpande myndigheterna mer personal för att kunna analysera uppgifter snabbare. Sverige är redan medvetet om detta och har som målsättning att förbättra situationen genom att utöka personalstyrkan vid berörda enheter. Den svenska polisen nämnde att följande områden behöver förbättras för att man ska kunna utföra framgångsrika utredningar: den övergripande strukturen, riktlinjer, resurser och kompetens på området it-brottslighet och it-relaterade brott.

Exempel på hinder är att brott inte anmäls, att bevis och material såsom loggar och annan avgörande bevisning saknas eller är bristfälliga, att leverantörer inte lagrar eller inte kan tillhandahålla information om abonnenter, användning av olika tjänster för anonymisering och bristen på effektiva redskap för att utbyta information med andra länder. I Sverige är internetleverantörer inte skyldiga att lagra uppgifter i mer än sex månader.

4.3 Övriga myndigheter/institutioner/offentlig-privata partnerskap

Myndigheten för samhällsskydd och beredskap

Myndigheten för samhällsskydd och beredskap (MSB) arbetar förebyggande mot it-relaterad brottslighet. Myndigheten övervakas av justitiedepartementet och arbetar huvudsakligen utifrån de tre principerna om ansvar för stöd, ansvar för handling och ansvar för samverkan. MSB samarbetar med privata och offentliga intressenter och ansvarar för sektorerna energi, hälso- och sjukvård, livsmedel, offentliga tjänster, säkerhet, social trygghet, transport och trafik. MSB har fyra enheter (utbildning, samordning och samverkan, förebyggande arbete och utveckling). MSB arbetar fortlöpande med att förbättra sin strategi med utgångspunkt i den aktuella situationen vad beträffar angrepp och faror. MSB har även särskilda program för offentliga myndigheter för att öka medvetenheten hos deras personal. MSB har också skapat en särskild webbplats där medborgarna kan hitta information, öka sin kunskap, ställa frågor och anmäla angrepp. Alla offentliga organ måste lämna rapporter om it-relaterade risker till MSB så att MSB kan analysera rapporterna och vidta åtgärder i enlighet med sina principer.

MSB ansvarar för den nationella incidenthanteringsorganisationen som t.ex. kan informera om aktuella försök till bedrägeri och hur aktörer kan skydda sig. MSB kommer att vara den enda kontaktpunkten i situationer då Europaparlamentets och rådet direktiv 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (nedan kallat it-säkerhetsdirektivet) tillämpas. En rättslig utredning har redan inletts för att genomföra it-säkerhetsdirektivet.

Cert-SE

Den svenska civila incidenthanteringsorganisationen har ett nära samarbete med Sveriges militära incidenthanteringsorganisation. Det finns även ett nära samarbete med incidenthanteringsorganisationer från den privata sektorn. Inom ramen för detta samarbete utbyts och diskuteras information, trender, erfarenheter och sakkunskap.

Den svenska incidenthanteringsorganisationen har ett mycket intensivt och diversifierat varningssystem. Organisationen ansvarar för att varna allmänheten i händelse av ett angrepp. Den svenska incidenthanteringsorganisationen utarbetar och offentliggör veckovisa och ibland dagliga rapporter om aktuella angrepp samt lägessammanfattningar som skickas till andra offentliga och privata incidenthanteringsorganisationer. Detsamma gäller dagliga varningar i händelse av angrepp eller risker.

ECPAT

ECPAT Sverige grundades som en icke-statlig organisation 1996 och är medlem i ECPAT Internationals globala nätverk som är representerat i mer än 70 länder. ECPAT Sverige samarbetar med andra icke-statliga organisationer, myndigheter och delar av branschen för att bekämpa kommersiell sexuell exploatering av barn. ECPAT har ett nära samarbete med den svenska finansbranschen vid fall av barnpornografi i syfte att spåra pengar och identifiera förövarna med hjälp av ekonomiska utredningar. Ett internationellt samarbete med organ i andra länder har upprättats i samma syfte och utvecklas kontinuerligt. ECPAT har ett nära samarbete med svenska brottsbekämpande myndigheter och rättsväsendet.

4.4 Samarbete och samordning på nationell nivå

Riksdagen och regeringen beslutar om inriktningen och villkoren för verksamhet på central myndighetsnivå samt om vilken verksamhet och vilka ansvarsområden de olika organen ska tilldelas. Organen har långtgående befogenheter i sitt dagliga operativa arbete och regeringen kan enligt grundlagen inte ingripa i individuella fall. Det är dock regeringens uppgift att styra organen och att se till att de fullgör sina skyldigheter, genom den reguljära tilldelningen av anslag, lagstiftning, regeringsuppdrag, utredningar osv.

Uppgiftsfördelningen på området förebyggande och bekämpande av it-relaterad brottslighet och säkerställande av it-säkerhet i Sverige grundar sig på ansvarsprincipen. Detta innebär att ett organ som har tilldelats en uppgift via en instruktion, en lag, en förordning eller ett regeringsuppdrag är ansvarigt. Exempelvis har polisen enligt polislagen samt diverse andra lagar och förordningar tilldelats den allmänna uppgiften att utreda brott som fastställs i brottsbalken. Detta innebär i sin tur att polisen också har denna uppgift även om nya områden för brottsligheten uppstår eller om nya straffrättsliga bestämmelser fastställs.

Sedan SC3 inrättades har det ingått ett samarbetsavtal med säkerhetspolisen på området it-relaterad brottslighet. SC3 och MSB vidareutvecklar för närvarande samarbetsmekanismer på såväl operativ som strategisk nivå.

4.4.1 Rättsliga eller politiska skyldigheter

På regeringsnivå är justitiedepartementet den institution som har det huvudsakliga ansvaret. Inom departementet finns det enheter som ansvarar för kontakterna med polisen, åklagarmyndigheten, domstolarna, MSB, osv. Samarbete sker även med andra departement såsom näringsdepartementet, utrikesdepartementet och utbildningsdepartementet. Det finns fastställda förfaranden och praxis för detta samarbete och en arbetsgrupp med representanter från olika departement har formellt inrättats särskilt för området it-säkerhet.

Den svenska åklagarmyndigheten har i allmänhet inte direktkontakt med den privata sektorn, t.ex. internetleverantörer, finansinstitut, osv. Dessa kontakter handhas av polisen.

Polisen samarbetar t.ex. med ECPAT och länsstyrelsen, som har etablerat jourtelefoner till vilka allmänheten kan anmäla alla internetrelaterade sexuella övergrepp mot barn. Informationen vidareförmedlas direkt till polisen. Polisen och ECPAT är också aktiva partner i Finanskoalitionen.

Polisen har i vissa fall bett den privata sektorn om hjälp med frivilligt utbyte av information och vissa andra åtgärder. Ett samarbete har upprättats med de större bankerna för informationsutbyte och vidtagande av åtgärder. Vissa ärenden har hanterats i samarbete med Cert-SE och samarbetet med den privata sektorn (t.ex. internetleverantörer) är gott.

4.4.2 Resurser avsatta för att förbättra samarbetet

Den svenska polisen är à jour vad gäller utrustning och kunskap. År 2013 inrättades ett nationellt bedrägericentrum. Erfarna polistjänstemän från det nationella bedrägericentrumet ger regionalt och lokalt stöd till utredare och delar med sig av bästa praxis.

MSB har en årlig budget på 130 miljoner euro för samarbetsprojekt med den offentliga sektorn. Detta kan användas till att finansiera forskningsprojekt, informationskampanjer, forskningshjälpmedel, osv.

På området nät- och informationssäkerhet samordnar MSB ett nätverk, SAMFI, som består av Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen. SAMFI sammanträder regelbundet för att behandla bl.a. strategiska frågor, lagstiftning, utbildning, informationsåtgärder och tekniska frågor.

4.5 Slutsatser

- Domare erbjuds ingen systematisk utbildning om it-relaterad brottslighet. Utvärderarna anser att det med tanke på den höga komplexiteten i it-relaterad brottslighet krävs att domare som hanterar it-brott har goda kunskaper.

- Å andra sidan finns det specialiserade åklagare som hanterar it-brott. Alla åklagare ges en obligatorisk grundläggande utbildning om it-relaterad brottslighet och den specialiserade avancerade utbildningen är avsedd för de åklagare som hanterar it-brott. Utvärderingsgruppen var imponerad av specialiseringsgraden och nivån av kunskapshantering hos de åklagare man mötte.

- Dessutom finns det en webbaserad vägledning med en detaljerad och omfattande översikt över kunskap och bästa praxis vad gäller it-relaterad brottslighet. I vägledningen finns kontaktuppgifter till internationella företag som tillhandahåller internettjänster (Facebook, Google, m.fl.). Detta är viktigt eftersom det ofta finns bevisning lagrad som dessa företag har kontroll över, och åklagarna behöver veta om det är möjligt att få tillgång till denna information och hur man i så fall ska gå till väga. Den it-relaterade brottsligheten förändras ständigt. Den webbaserade vägledningen kommer att anpassas och uppdateras kontinuerligt. Utvärderingsgrupen anser att denna metod är bästa praxis.

- Det finns dessutom ett nationellt nätverk av åklagare som arbetar med it-relaterad brottslighet, i vilket varje åklagarområde företräds av två åklagare. Nätverket tillhandahåller särskilda utbildningsmoduler för åklagare samt de mest relevanta domarna på området it-relaterad brottslighet, och är en plattform där aktuella problem diskuteras. En medlem i detta nationella nätverk av åklagare med inriktning på it-relaterad brottslighet är medlem i Eurojusts europeiska rättsliga nätverk mot it-brottslighet.

- Det finns en mycket hög nivå av samarbete mellan olika organ och samordning mellan olika institutioner i Sverige, inom ramen för en unik uppsättning offentliga institutioner. Riksdagen och regeringen beslutar om inriktningen och villkoren för verksamhet på central myndighetsnivå samt om vilken verksamhet och vilka ansvarsområden de olika organen ska tilldelas.

- Många aktörer är delaktiga i att bekämpa it-relaterad brottslighet i Sverige. Organen har långtgående befogenheter i sitt dagliga operativa arbete och regeringen kan inte ingripa i individuella fall. Enligt utvärderarnas uppfattning skulle systemet kunna göras ännu mer effektivt genom en starkare samordning av de insatser som görs av alla aktörer som deltar i kampen mot it-relaterad brottslighet.

- Polisen ansvarar för att utreda brott som definieras i straffrätten, i vilket ingår nya brottsområden som uppstår eller nya straffrättsliga bestämmelser som fastställs. En omfattande polisreform har genomförts i Sverige i syfte att åtgärda organisatoriska hinder inom polisen och att förbättra möjligheterna att förebygga, vidta åtgärder mot och utreda brott. Polisen omorganiserades till en nationell polismyndighet på central nivå med flera regioner.

- Den 1 oktober 2015 inrättades dessutom ett nationellt it-brottscentrum (SC3) för att bygga upp kapaciteten att utreda alla typer av it-relaterad brottslighet. Centrumet ska gradvis utökas till att omfatta specialiserade utredare, analytiker, kriminaltekniker och experter. Det har en nationell enhet i Stockholm och sju regionala it-brottscentrum som fältkontor. SC3 skapades som ett centralt nav för samordning av alla insatser inom polisens avdelningar på området it-relaterad brottslighet, t.ex. när det gäller kunskaps- och kompetensbyggande, utbildning, forskning och utveckling och kontakter med andra parter (myndigheter, åklagare, internationellt, m.fl.). Eftersom centrumet fortfarande är i uppbyggnadsstadiet ligger fokus på SC3 och inte på de regionala centrumen (t.ex. vad gäller personalkapacitet).

- Utvärderarna anser dessutom att den svenska polisen som helhet skulle kunna förbättras på områdena övergripande struktur, riktlinjer, resurser och kompetens på området it-relaterad brottslighet. Bland de hinder som nämns av företrädare för de svenska brottsbekämpande myndigheterna finns följande: brott anmäls inte, bevis och material, t.ex. loggar och annan avgörande bevisning, saknas eller är bristfälliga, leverantörerna lagrar inte eller kan inte tillhandahålla information om abonnenter, användning av olika tjänster för anonymisering och brist på effektiva redskap för att utbyta information med andra länder, begränsade perioder för lagring av uppgifter, osv. (i Sverige är internetleverantörer inte skyldiga att lagra uppgifter i mer än sex månader).

5 RÄTTSLIGA ASPEKTER

5.1 Materiell straffrätt i fråga om it-relaterad brottslighet

5.1.1 Europarådets konvention om it-relaterad brottslighet

Sverige har ännu inte ratificerat konventionen om it-relaterad brottslighet (undertecknad av Sverige den 23 november 2001) och ingen tydlig förklaring av skälen till detta kunde lämnas. Under besöket på plats bekräftade Justitiedepartementet sin avsikt att ratificera konventionen under den nuvarande regeringens mandatperiod, som löper ut 2018.

5.1.2 Beskrivning av nationell lagstiftning

a) Rådets rambeslut 2005/22/RIF om angrepp mot informationssystem och direktiv 2013/40/EU om angrepp mot informationssystem

Sverige har införlivat direktiv 2013/40/EU i nationell lagstiftning. För att uppfylla kravet om maximistraff behövde en ny straffskala införas för grovt dataintrång (fängelse i lägst sex månader och högst sex år). Den nya lagstiftningen trädde i kraft i juli 2014.

Angrepp mot informationssystem, t.ex. olovlig tillgång till informationssystem, olovlig störning av system eller olovlig störning av användningen av uppgifter, straffbeläggs i första hand genom bestämmelserna om dataintrång (kapitel 4 paragraf 9 c i brottsbalken). För straffrättsligt ansvar krävs uppsåt. Vid bedömningen av huruvida ett dataintrång är grovt bör särskild uppmärksamhet ägnas frågan om huruvida gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Påföljden för dataintrång löper från böter till fängelse i högst två år. Om brottet anses vara grovt döms för ett sådant dataintrång till fängelse i lägst sex månader och högst sex år. Anstiftan, medhjälp och medverkan är straffbelagt. Försök att begå dataintrång är också straffbelagt förutom i lindriga fall.

Under vissa omständigheter kan angrepp mot informationssystem också vara straffbelagt i enlighet med bestämmelserna om skadegörelsebrott (kapitel 12 paragraf 1 eller 3) eller allmänfarliga brott (kapitel 13 paragraf 4 eller 5) eller om terroristbrott (paragraferna 2 och 3 i lagen om straff för terroristbrott).

Olovligt beredande av tillgång till datorbehandlingsbara uppgifter är straffbelagt enligt bestämmelserna om dataintrång (se ovan) samt bestämmelserna om brytande av post- eller telehemlighet (kapitel 4 paragraf 8 i brottsbalken). För straffrättsligt ansvar för brytande av post- eller telehemlighet krävs uppsåt. Påföljden är böter eller fängelse i högst två år. Den som anbringar tekniskt hjälpmedel med uppsåt att bryta telehemlighet kan dömas för förberedelse till sådant brott om han eller hon inte gjort sig skyldig till fullbordat brott (kapitel 4 paragraf 9 b i brottsbalken). Påföljden är böter eller fängelse i högst två år.

Missbruk av utrustning (tillverkning, distribution, anskaffande i syfte att använda, importera eller på annat sätt tillgängliggöra eller inneha utrustning för datormissbruk) är i första hand straffbelagt genom bestämmelserna om förberedelse att begå något av de beskrivna brotten, t.ex. förberedelse att begå dataintrång. Påföljden för förberedelse att begå ett brott är bestämd högst till vad som gäller för fullbordat brott och kan bestämmas till lägre än det lägsta straffet för fullbordat brott (kapitel 23 paragraf 2 i brottsbalken). Olika typer av missbruk av utrustning kan också straffbeläggas enligt bestämmelserna i kapitel 4 paragraf 9 b i brottsbalken.

Enligt svensk lag kan företagsbot åläggas juridiska personer för alla brott (inklusive it-relaterad brottslighet) som har begåtts i utövningen av näringsverksamhet. Företagsbot är en straffrättslig påföljd och kan fastställas till lägst fem tusen kronor och högst 10 miljoner kronor. Lagstiftningen om företagsbot, inbegripet nivån på påföljderna, har nyligen setts över av en utredningskommitté. När besöket genomfördes fick kommittén i uppdrag att lägga fram sin rapport i november 2016, och utvärderingsgruppen har underrättats om att rapporten lades fram i tid[10].

[10] När utvärderingsgruppen utarbetade sina resultat hade den inte kännedom om rapporten och tog inte hänsyn till den.

b) Direktiv 2011/93/EU om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi

Sverige har införlivat direktiv 2011/93/EU av den 13 december 2011 i nationell lagstiftning. Vid genomförandet av direktivet höll riksdagen med om regeringens slutsats att svensk lagstiftning, med undantag från vissa frågor gällande begränsning av påföljd och registerkontroll, uppfyllde bestämmelserna i direktivet. De nödvändiga ändringarna i lagstiftningen trädde i kraft 2013.

Kontakt med barn i sexuellt syfte (gromning)

Kontakt med barn i sexuellt syfte är straffbelagt enligt bestämmelserna i kapitel 6 paragraf 10 a i brottsbalken. Syftet med lagstiftningen är att förhindra att barn under femton år utnyttjas i sexuella syften vid sammanträffande med vuxna. För brottet krävs uppsåt.

Förutom att brottet kräver uppsåt vad gäller de åtgärder gärningsmannen faktiskt vidtar (t.ex. att kontakta barnet via internet, att komma överens om en tid och plats för mötet) krävs också att gärningsmannen har ett uppsåt att begå ett sexualbrott mot barnet vid sammanträffandet. Vid fastställandet av straffvärdet för en brottslig gärning ska de allmänna bestämmelserna om försvårande och förmildrande omständigheter i kapitel 29 paragraferna 2–3 i brottsbalken tillämpas.

Påföljderna omfattar böter eller fängelse i högst ett år. Stämpling, föreberedelse eller försök till *kontakt med barn i sexuellt syfte* är inte straffbelagt. Anstiftan, medhjälp och medverkan till ett brott är straffbelagt enligt den allmänna bestämmelsen om medhjälp och medverkan i kapitel 29 paragraf 4 i brottsbalken.

Barnpornografibrott

Det är brottsligt att skildra barn i pornografisk bild, att göra en sådan bild tillgänglig för någon annan, att förvärva eller bjuda ut en sådan bild, att på något sätt främja handel med sådana bilder eller att inneha en sådan bild (se bestämmelserna om *barnpornografibrott* och *grovt barnpornografibrott* i kapitel 16 paragraf 10 a i brottsbalken). För ansvar för *barnpornografibrott* eller *grovt barnpornografibrott* krävs uppsåt eller oaktsamhet. Sedan den 1 juli 2010 är också betraktande av en barnpornografisk bild som gärningsmannen har berett sig tillgång till straffbart som barnpornografibrott. Detta innefattar naturligtvis också betraktande på internet, utan innehav. I de straffrättsliga bestämmelserna om barnpornografi finns det tydligt uttryckt vad som utgör ett barnpornografibrott (se bestämmelserna om *barnpornografibrott* och *grovt barnpornografibrott*, kapitel 16 paragraf 10 a i brottsbalken). Vid tillämpningen av dessa bestämmelser avses med barn en person vars pubertetsutveckling inte är fullbordad eller som är under 18 år. I den straffrättsliga bestämmelsen föreskrivs att om pubertetsutvecklingen är fullbordad, ska ansvar för all handel med barnpornografiska bilder förutom själva skildrandet dömas ut bara om det av bilden och omständigheterna kring den framgår att den avbildade personen är under 18 år.

Barnpornografibrott är straffbart med fängelse i högst två år, eller om brottet är ringa, med böter eller fängelse i högst sex månader. *Grovt barnpornografibrott* är straffbelagt med fängelse i lägst sex månader och högst sex år. Försvårande aspekter som ska beaktas vid bedömningen av huruvida ett brott är grovt är bland annat om brottet har begåtts i vinstsyfte, utgjort ett led i brottslig verksamhet som utövats systematiskt eller i större omfattning, avsett en särskilt stor mängd bilder eller avsett bilder där barnen är särskilt unga, utsätts för våld eller tvång eller utnyttjas på annat särskilt hänsynslöst sätt (se bestämmelsen om *grovt barnpornografibrott*, kapitel 16 paragraf 10 a femte stycket i brottsbalken). Förmildrande omständigheter är bland annat om brottet bara avser en enstaka bild (se prop. 1997/98:43, s. 92).

De allmänna bestämmelserna om flera brott/återfall i brottsbalken gäller. Anstiftan, medhjälp och medverkan samt försök till *barnpornografibrott* enligt paragraf 10a första stycket eller *grovt barnpornografibrott* är straffbelagt.

c) Betalkortsbedrägerier på internet

Det finns ingen särskild lagstiftning som straffbelägger betalkortsbedrägerier på internet, eftersom det faller under definitionen av allmänt bedrägeri.

År 2013 inrättades ett nationellt bedrägericentrum. Erfarna polistjänstemän från det nationella bedrägericentrumet ger regionalt och lokalt stöd till utredare och delar med sig av bästa praxis. För att kunna stå i förgrunden samarbetar nationellt bedrägericentrum med nationellt forensiskt centrum och nationellt it-brottscentrum.

5.2 Procedurfrågor

5.2.1 Utredningsmetoder

Följande utredningsmetoder kan vara tillämpliga enligt svensk lagstiftning:

- Husrannsakan eller beslag av informationssystem/datorbehandlingsbara uppgifter.

Föremål som skäligen kan antas ha betydelse för utredning om brott får tas i beslag, t.ex. en dator (kapitel 27 paragraf 1 i rättegångsbalken). Husrannsakan får under vissa omständigheter beordras för att söka efter föremål som kan tas i beslag (kapitel 28 paragraf 1 i rättegångsbalken). Ett beslagtaget föremål får undersökas av de brottsbekämpande myndigheterna. Det innebär att information som t.ex. finns lagrad på en hårddisk är tillgänglig för myndigheterna.

- Avlyssning i realtid/insamling av uppgifter om trafik/innehåll.

Följande utredningsmetoder är tillåtna i form av hemliga tvångsmedel i enlighet med rättegångsbalken kapitel 27 paragraferna 18–19:

- Hemlig avlyssning av elektronisk kommunikation (paragraf 18).
- Hemlig övervakning av elektronisk kommunikation (paragraf 19).

Hemlig avlyssning av elektronisk kommunikation får användas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, eller
2. vissa särskilda allvarliga brott som nämns i paragraf 2 andra stycket punkterna 2–7,
3. försök, förberedelse eller stämpling till ett sådant brott, om en sådan gärning är belagd med straff, eller
4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Hemlig övervakning av elektronisk kommunikation får användas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader,
2. brott som särskilt nämns i paragrafen, såsom narkotikabrott enligt narkotikastrafflagen (1968:64), paragraf 1, narkotikasmuggling enligt lagen om straff för smuggling (1960:418), paragraf 1 eller barnpornografibrott enligt kapitel 16 paragraf 10 a i brottsbalken.
3. vissa särskilda allvarliga brott som nämns i paragraf 2 andra stycket punkterna 2–7,
4. försök, förberedelse eller stämpling till ett brott som avses i punkterna 1–3 ovan, om en sådan gärning är belagd med straff.

Frågor om ovannämnda åtgärder prövas av rätten på ansökan av åklagaren. Varaktigheten för avlyssningen eller övervakningen får inte vara längre än nödvändig och får inte överstiga en månad från dagen för beslutet (paragraf 21).

I brådskande situationer och om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse att inhämta rättens tillstånd får tillfälligt tillstånd ges av åklagaren. Ett sådant beslut måste anmälas till rätten så snart som möjligt (paragraf 21 a).

Telefonsamtal eller andra meddelanden mellan den misstänkte och dennes försvarare får inte vara föremål för hemlig avlyssning av elektronisk kommunikation. Om det under avlyssningen kommer fram att det är fråga om ett sådant samtal eller sådan meddelande ska övervakningen avbrytas. Detsamma gäller samtal mellan den misstänkte och personer som inte får vittna i enlighet med rättegångsbalken, kapitel 36 paragraf 5 punkterna 2–6 (t.ex. advokater, läkare och präster). Upptagningar och uppteckningar från sådan kommunikation ska omedelbart förstöras (paragraf 22).

Ovannämnda hemliga tvångsmedel får endast användas om någon är skäligen misstänkt för ett brott och åtgärden är av synnerlig vikt för utredningen. Åtgärderna får endast avse ett telefonnummer eller en adress som innehas av den misstänkte eller som kan antas komma att användas av den misstänkte. Hemlig övervakning och avlyssning av elektronisk kommunikation får under vissa omständigheter ske i syfte att utreda personer som är skäligen misstänkta.

- Säkrande av datorbehandlingsbara uppgifter.

I svensk lagstiftning föreskrivs inte nationella beslut om säkrande. Myndigheterna rapporterade dock att framställningar om säkrande skickas till andra länder.

Myndigheten får säkra datorbehandlingsbara uppgifter under en husrannsakan i fall då en dator och dess innehåll inte kan beslagtas. Det gäller fall då ett beslagtagande skulle vara oproportionerligt i förhållande till det misstänkta brottet eller då följderna för den berörda parten/utrustningens ägare anses bli för allvarliga.

- Order om lagrade trafikuppgifter/innehållsuppgifter.

Enligt kapitel 6 paragraferna 16a och 16d i lagen om elektronisk kommunikation (2003:389) är internetleverantörer skyldiga att lagra trafikuppgifter i sex månader. (Efter sex månader måste uppgifterna utplånas.)

För att få tillgång till trafikuppgifter för en förundersökning krävs normalt sett tillstånd från rätten och vissa krav måste uppfyllas (se ovannämnda kapitel 27 paragraferna 18 och 19 i rättegångsbalken).

- Order om användaruppgifter.

Enligt kapitel 6 paragraferna 16a och 16d i lagen om elektronisk kommunikation (2003:389) är internetleverantörer skyldiga att lagra användarinformation (såsom namn, adress, telefonnummer osv.) i sex månader. Efter sex månader måste uppgifterna utplånas. Om det finns misstanke om brott måste internetleverantören på begäran lämna denna information till en åklagarmyndighet eller polismyndighet (kapitel 6 paragraf 22.2 i lagen om elektronisk kommunikation). I enlighet med skyldigheten att lagra uppgifterna i fråga i sex månader, måste begäran följaktligen göras inom denna tid.

Det är emellertid en särskild utmaning att utredningar inom Sverige hämmas av det faktum att det internationella samarbetet vad gäller tillgång till information och bevis som innehas av privata företag i en annan jurisdiktion än den svenska är alldeles för underutvecklat. Ofta måste svenska brottsutredningar läggas ned på grund av att uppgifter som inte avser innehåll inte lämnas ut av privata företag i sådana jurisdiktioner. Enligt Sveriges erfarenheter är samarbete med i synnerhet Förenta staterna och företag baserade där avgörande om vi ska kunna nå framgång i kampen mot it-relaterad brottslighet. Eftersom det ligger inom dessa företags rättsliga befogenheter att på frivillig basis lämna ut uppgifter som inte avser innehåll, har Sverige försökt att komma överens med ett antal företag baserade i Förenta staterna om metoder och förfaranden för att begära och få tillgång till sådan information. I vissa fall har dessa ansträngningar krönts med framgång. Sedan 2013 har den svenska polisen i detta sammanhang inrättat en enda kontaktpunkt i förhållande till Facebook, Instagram, Ask.fm, Google och Apple. För närvarande pågår arbete med att uppnå en liknande överenskommelse med Twitter och Periscope.

Konceptet med en enda kontaktpunkt har många fördelar för både den svenska polisen och en privat motpart i Förenta staterna. För den svenska polisen innebär detta att avdelningen vid det svenska nationella it-brottscentrumet, SC3, skapar sig en överblick och tillägnar sig erfarenhet över tid om hur man förvaltar samarbetet på bästa sätt. Det möjliggör också en lämplig övervakning av dataskyddsfrågor. För den privata motparten i Förenta staterna möjliggör utnyttjandet av en enda kontaktpunkt en smidigare behandling eftersom denna kontaktpunkt vid den brottsbekämpande myndigheten kan tillhandahålla de uppgifter som krävs för att begära ut uppgifter som inte avser innehåll och ta emot information som lämnas ut på frivillig basis.

För utredning av it-relaterad brottslighet krävs ett team av olika specialister, it-forensiker, utredare och åklagare. Bland de särskilda utredningsteknikerna finns en tydlig inriktning på taktik vid husrannsakningar (kriminalteknik i verkliga livet) för att få så goda resultat som möjligt vad gäller digitala bevis, it-forensisk analys av loggar och beslagtagna datorer, laglig avlyssning av kommunikation (både telefoni och datatrafik), avancerad underrättelseinhämtning från öppna källor och hemliga insatser.

5.2.2 Kriminalteknik och kryptering

Kryptering används både vid datalagring och kommunikation via internet. Enligt polisen används allt mer kryptering och det blir allt svårare att ta sig förbi krypteringen. Därför krävs bättre taktiska insatser från polisen vid gripanden.

I allmänhet utförs dekryptering internt. Samarbetet med andra myndigheter anses vara väletablerat och effektivt. Vissa av organen kan anses vara specialiserade. Följande problem har rapporterats i samband med kryptering:
– Krypteringsformat (eller krypterade behållare) som inte stöds.
– Appar med okända krypteringsrutiner:
– Vid lösenordsbaserad kryptering, överdrivet komplexa lösenord som är svåra att knäcka.
– iPhone är ett bra exempel som visar på problemen med kryptering.

En mer intelligent analys av en misstänkts mönster för skapande av lösenord och dynamisk aggregering av datorkraft har lyfts fram som möjliga lösningar på problemen ovan. De företrädare som utvärderingsgruppen mötte föreslog dessutom att gruppen med olika specialister borde arbeta tillsammans, även med it-forensiker. Under en husrannsakan är det god praxis att ha nära kontakt med åklagaren. Under förhör med en misstänkt kan en it-forensisk specialist vara närvarande för att se till att man förstår alla tekniska detaljer.

5. 2.3 E-bevisning

Det finns inga regler om tillåtlighet för e-bevisning, eller för annan bevisning. Fri bevisprövning är en grundläggande princip i den svenska rättegångsbalken. Rättssystemet innehåller inte några formella regler om bevisföring eller bevisvärdering. Allting som kan ha bevisvärde i ett mål kan, i princip, läggas fram i rätten.

Svenska rättegångsregler är i huvudsak teknikneutrala, vilket innebär att det inte finns några särskilda regler för e-bevisning. Regeringen har nyligen tillsatt en utredning i syfte att undersöka vissa aspekter relaterade till beslag och husrannsakan. Bestämmelserna om beslag och husrannsakan trädde i kraft på 1940-talet. Lagstiftningen är inriktad på fysiska föremål och skriftliga handlingar. I uppdraget ingår att analysera hur lagstiftningen kan anpassas till modern teknik. Utredningen förväntas redovisa sitt uppdrag i september 2017.

Skydd av mänskliga rättigheter/grundläggande friheter

Grundläggande fri- och rättigheter är skyddade i grundlagen. I grundlagen anges också under vilka omständigheter begränsningar kan införas. Sådana begränsningar kan t.ex. göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Samma regler gäller på internet som utanför.

Skyddet av de grundläggande fri- och rättigheterna är även det lika starkt på internet som utanför. Polisen kan alltså inte ingripa enklare på internet än i verkliga livet.

5.4 Jurisdiktion

5.4.1. Principer som tillämpas för att utreda it-relaterade brott

I enlighet med territorialitetsprincipen och ubikvitetsprincipen kan svensk domstol fastställa sin behörighet över (hela) brottet om någon del av brottet begåtts i Sverige. Om ett it-relaterat brott begås i sin helhet utanför svenskt territorium kan svensk domstol fastställa sin behörighet över brottet om det har begåtts av en svensk medborgare eller av en utländsk medborgare med hemvist i Sverige (personalitetsprincipen), under förutsättning att gärningen omfattas av straffrättsligt ansvar enligt den lagstiftning som gäller där gärningen begicks (dubbel straffbarhet). Vad gäller barnpornografibrott där den brottsliga gärningen består i att skildra barn i pornografisk bild och grova barnpornografibrott gäller dock inte kravet på dubbel straffbarhet.

Behörighet kan också fastställas för brott som begåtts utanför svenskt territorium om brottet begås mot den svenska staten, en svensk kommunal myndighet eller annan församling eller mot en svensk offentlig institution (skyddsprincipen).

5.4.2 Bestämmelser i fråga om behörighetskonflikter och hänskjutande till Eurojust

Ofta är problemet inte att två eller fler medlemsstater vill lagföra, utan att inget land vill utreda och lagföra. I fall då mer än en medlemsstat utreder ett brott eller en del av ett brott löses ofta frågan om var den misstänkte ska åtalas genom en förhandsöverenskommelse under utredningen. Detta kan innebära ett av följande alternativ:

- Överföring av förfarandet från ett land till ett annat. Detta gjordes i ett fall beträffande dataintrång i flera länder som hade begåtts av en svensk medborgare i Sverige. Andra stater överförde sina förfaranden till Sverige.

- Uppdelning av fallet mellan medlemsstaterna, dvs. att ett land utreder de brottsoffer som är bosatta i den staten och vice versa. Detta gjordes i ett fall beträffande dataintrång där personen ursprungligen dömdes i Sverige och därefter överfördes till Danmark.
- Varje land utreder den person som är bosatt inom dess territorium, även om de alla är del av en organisation. Detta gjordes i ett fall beträffande framställande av barnpornografi där fotografen åtalades i ett land och de personer som beställt bilderna åtalades i sina hemländer (Spanien, Sverige och Förenta staterna).

Rådets rambeslut 2009/948/RIF av den 30 november 2009 om förebyggande och lösning av tvister om utövande av jurisdiktion i straffrättsliga förfaranden har genomförts, men Sverige för inte register över tillämpningen av EU-instrument. Det finns ingen erfarenhet av hänskjutande till Eurojust för att lösa tvister om jurisdiktion.

5.4.3 Jurisdiktion för it-relaterade brott som begåtts i "molnet"

Brott som begåtts "i molnet" kan ofta knytas både till var gärningsmannen befann sig när han eller hon begick brottet och till var följderna uppstod. Beroende på typ av it-relaterat brott kan följderna knytas till flera medlemsstater, vilket kan leda till tvister om jurisdiktion när två eller fler medlemsstater kan fastställa behörighet för brottet.

När myndigheterna mottar en framställning om ömsesidig rättslig hjälp som rör information i molnet, har informationen vanligtvis spårats till en server i Sverige. I sådana fall finns det inte några problem med att tillhandahålla ömsesidig rättslig hjälp avseende informationen i molnet. Ibland har dock informationen i fråga försvunnit vid den tidpunkt framställan mottas och i sådana fall är det problematiskt att tillhandahålla ömsesidig rättslig hjälp eftersom det saknas rättslig grund för att göra en formell sökning i "molnet".

Denna situation blir allt mer problematisk eftersom till exempel redovisningstjänster tillhandahålls som molntjänster. För tillfället diskuterar Ekobrottsmyndigheten med molntjänstleverantörer frågan om möjligheten att i samband med brottsutredningar få tillgång till redovisning som lagras i molnet.

5.4.4 Den svenska uppfattningen vad gäller den rättsliga ramen för att bekämpa it-relaterad brottslighet

Enligt de svenska myndigheterna är framställningar om ömsesidig rättslig hjälp ofta tidskrävande och ibland mottas svaren för sent för att vara till någon verklig hjälp. Processen för ömsesidig rättslig hjälp vad gäller e-bevisning behöver förbättras.

Det finns brister vad gäller tillgång till uppgifter som är lagrade på fjärrservrar (oavsett om de tillhör utländska företag eller inte). Detta område behöver förbättras och samarbetet med utländska tjänsteleverantörer bör förstärkas. Otillräckliga regler för lagring av uppgifter i vissa länder är också ett problem.

Det finns i synnerhet tre områden där förbättringar krävs. Det första gäller harmonisering av den relevanta lagstiftningen i medlemsstaterna (inklusive lagring av uppgifter). Det andra gäller en förbättrad process för ömsesidig rättslig hjälp. Det tredje gäller tydliga riktlinjer och krav (skyldigheter) gällande framställningar från andra länder. Detta innefattar stöd dygnet runt, svarstider och förtydliganden om för vilka typer av uppgifter ömsesidig rättslig hjälp krävs och i vilka fall en kontakt mellan poliser är tillräcklig.

5.5 Slutsatser

- Sverige har ännu inte ratificerat konventionen om it-relaterad brottslighet och ingen tydlig förklaring av skälen till detta kunde lämnas. Under besöket på plats uttryckte Justitiedepartementet sin avsikt att ratificera konventionen under den nuvarande mandatperioden, som löper ut 2018. Det bör understrykas att åklagare och poliser betonade behovet av en ratificering, inbegripet för beslut om säkrande.

- Med undantag för säkrandebefogenheter uppgavs det att den svenska lagstiftningen tillgodoser genomförandet av konventionen. Anslutning till fördraget kommer dock troligen att ha en betydande påverkan på andra områden, inbegripet bättre möjligheter till internationellt samarbete. Berörda parter, t.ex. åklagare och polisen, betonade behovet av att skyndsamt ratificera Budapestkonventionen.

- På området materiell straffrätt är bestämmelserna i brottsbalken, så långt möjligt, allmänna och teknikneutrala, då avsikten är att tillämpa dem oavsett om ett brott har begåtts i en it-miljö eller inte. Syftet med denna rapport är inte att bedöma om en sådan strategi är genomförbar i praktiken mot bakgrund av den enorma utvecklingen på teknikområdet.

- Sverige rapporterade att man har införlivat direktiv 2013/40/EU i nationell lagstiftning. För att uppfylla kravet om maximistraff behövde en ny straffskala införas för grovt dataintrång (fängelse i lägst sex månader och högst sex år). Den nya lagstiftningen trädde i kraft i juli 2014. De brott som anges i direktiv 2013/40/EU straffas inte som separata brott och det kan därmed bli problematiskt att samla in och rapportera in uppgifter i enlighet med direktivet.

- Sverige rapporterade även att man har införlivat direktiv 2011/93/EU. Det finns ingen särskild lagstiftning som straffbelägger betalkortsbedrägerier på internet, eftersom det förefaller omfattas av den allmänna lagstiftningen.

- Vad gäller processrätten är strategin att i första hand vara teknikneutral, vilket innebär att det inte finns några särskilda regler för e-bevisning. Fri bevisprövning är en grundläggande princip i den svenska rättegångsbalken som kan utgöra bästa praxis. Rättssystemet innehåller inte några formella regler om bevisföring eller bevisvärdering. Allting som kan ha bevisvärde i ett mål kan, i princip, läggas fram i rätten.

- Regeringen har nyligen tillsatt en utredning i syfte att undersöka vissa aspekter relaterade till beslag och husrannsakan. Bestämmelserna om beslag och husrannsakan trädde i kraft på 1940-talet. Lagstiftningen är inriktad på fysiska föremål och skriftliga handlingar. I uppdraget ingår att analysera hur lagstiftningen kan anpassas till modern teknik. Utredningen förväntas redovisa sitt uppdrag i september 2017.

- Sverige har för närvarande flera pågående utredningar som syftar till att förbättra bestämmelser i brottsbalken och i rättegångsbalken, bl.a. med avseende på beslag. Detta är nödvändigt eftersom den befintliga lagstiftningen inte är praktisk. Ny lagstiftning kommer även att införas beträffande övergrepp på nätet och sökningar på internet i enheter. Vad gäller det senare är Sverige medvetet om problemet med kryptering och vill använda resultaten av utredningen om sökning på internet och åtgärder för beslagtagande även för att tillägna sig erfarenhet och förbättra de tekniska utredningsmetoderna.

- Vad gäller lagring av uppgifter väntade Sverige på ett beslut från domstolen. Vid tidpunkten för besöket var teletjänstföretag skyldiga enligt lag att lagra uppgifter i sex månader[11].

- Utvärderarna anser att säkrandebefogenheterna måste införlivas i nationell lagstiftning som en separat åtgärd.[12]

- Hantering av bevis i molnet (ur lagstiftningsperspektiv) förefaller vara en särskild utmaning för åklagare eftersom det saknas tydliga regler. För närvarande är det endast möjligt att säkra bevis om servern kan lokaliseras och ömsesidig rättslig hjälp kan utnyttjas. Med tanke på osäkerheten vad gäller åtkomst till bevis i molnet för de som arbetar med detta, skulle det vara till hjälp att på nationell nivå upprätta tydliga regler (ändringar eller tolkningar av tillämpningen av befintlig lagstiftning och deltagande i internationella forum, t.ex. den kommitté inom Europarådet som övervakar Europarådets konvention om it-relaterad brottslighet (T-CY), där Sverige skulle kunna delta som observatör och där lösningar på dessa problem diskuteras.

- Sveriges erfarenheter beträffande hur man har organiserat samarbetet med privata motparter i Förenta staterna är god praxis. Konceptet med en enda kontaktpunkt har många fördelar för både den svenska polisen och den privata motparten i Förenta staterna. För den svenska polisen innebär detta att avdelningen vid det svenska nationella it-brottscentrumet, SC3, skapar sig en överblick och tillägnar sig erfarenhet över tid om hur man förvaltar samarbetet på bästa sätt. Det möjliggör också en lämplig övervakning av dataskyddsfrågor. För den privata motparten i Förenta staterna möjliggör utnyttjandet av en enda kontaktpunkt en smidigare behandling eftersom denna kontaktpunkt vid den brottsbekämpande myndigheten kan tillhandahålla de uppgifter som krävs för att begära ut uppgifter som inte avser innehåll och ta emot information som lämnas ut på frivillig basis.

---

[11] Efter domstolens dom i december 2016 i de förenade målen C-203/15 och C-698/15 informerades utvärderingsgruppen om att den svenska regeringen hade tillsatt en offentlig utredning som skulle se över bestämmelserna om datalagring i lagen om elektronisk kommunikation. Vid översyn ska full hänsyn tas till domstolens dom i de förenade målen C-203/15 och C-698/15. Ett betänkande med förslag beräknas komma senast den 9 oktober 2017.

[12] Ett förtydligande av skillnaderna mellan de två åtgärderna finns i utvärderingsrapporten om genomförandet av säkrandebestämmelserna i Budapestkonventionen om it-relaterad brottslighet som antogs av den kommitté inom Europarådet som övervakar Europarådets konvention om it-relaterad brottslighet (T-CY) vid dess åttonde plenarsammanträde (den 5–6 december 2012) samt i den förklarande rapporten (149–162) till Budapestkonventionen.

6 OPERATIVA ASPEKTER

6.1 It-angrepp

6.1.1 Typen av it-angrepp

Det finns för närvarande ingen statistik över den exakta typen av it-angrepp, men angreppen brukar följa internationella trender: Samordnade överbelastningsattacker (DDoS-attacker), identitetsstöld, riktat nätfiske (spearphishing) och kortlösa bedrägerier (Card not present-bedrägerier) håller på att öka.

Polisen får sin information från de polisanmälningar som görs. Många it-angrepp anmäls inte eller anmäls till andra myndigheter än polisen.

6.1.2 Mekanism för att reagera på it-angrepp

Vid bedömningen av om ett brott är grovt beaktar man huruvida gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Straffet för grovt dataintrång (minst sex månaders och högst sex års fängelse) antogs 2014 för att man skulle kunna uppfylla kraven vad gäller påföljder enligt direktiv 2013/40/EU.

Den 1 april 2016 trädde en förordning i kraft i Sverige som rör obligatorisk rapportering av allvarliga it-incidenter vad gäller statliga myndigheter. Detta innebär att de svenska myndigheterna får en bättre överblick över hoten och en möjlighet att vidta rätt skyddsåtgärder.

I enlighet med EU-lagstiftningen är telekomoperatörer skyldiga att rapportera säkerhetsbrott och dataintrång till den nationella regleringsmyndigheten för elektronisk kommunikation. Vilken orsaken bakom dessa brott är (till exempel ett kriminellt it-angrepp) är irrelevant i detta sammanhang. Förfarandena för detta fastställs i EU:s sekundärlagstiftning. Det finns ingen skyldighet att rapportera direkt till brottsbekämpningsmyndigheter.

MSB har utarbetat en nationell hanterandeplan för allvarliga it-incidenter. Att skapa situationsmedvetenhet och arbeta med en nationell samarbetsmekanism utgör de två viktigaste processerna. Mekanismen bygger på ansvarsprincipen, vilket betyder att ingen inblandad aktör tar över en annan aktörs ansvar när det gäller att hantera incidenten. En viktig grund för mekanismen är den nationella incidenthanteringsorganisationen (Cert). Både myndigheter och privata företag kan delta i mekanismen.

Det är operatörens ansvar att se till att det egna företaget är tillfredsställande skyddat. Operatörerna samarbetar också med andra operatörer inom sina respektive sektorer för utbyte av information. Ett sektorssamarbete har upprättats, bland annat inom telekommunikationssektorn och den finansiella sektorn.

Att offren visar inget eller mycket litet intresse ses som ett hinder. Detta gäller särskilt privata företag men även statliga organ och myndigheter. It-brottslighet bör rapporteras och det krävs samarbete när en utredning väl har inletts. Därför förekommer underrapportering av incidenter.

Enligt de svenska myndigheterna måste den svenska polisen få mer erfarenhet av dessa typer av brott.

6.2 Åtgärder mot barnpornografi och sexuella övergrepp mot barn på internet

6.2.1 Programdatabaser för identifiering av offer och åtgärder för att undvika upprepad viktimisering

Sveriges polis använder programdatabaser, såsom Griffeye, ICSE och NetClean, som är särskilt utformade för att identifiera offer. Interpols databas ICSE (The International Child Sexual Exploitation Database) används dagligen.

Endast ett begränsat antal anställda har tillgång till bilderna i databasen. Konfiskerat material förstörs alltid.

6.2.2 Åtgärder för att ta itu med sexuell exploatering/övergrepp på internet, sexting och mobbning på nätet

Sexuell utpressning är enligt de svenska myndigheterna ett problem som måste uppmärksammas och som kräver motåtgärder.

Samhällets och teknikens utveckling har lett till att möjligheterna att kommunicera och sprida information har ökat och således även möjligheten att begå handlingar som inbegriper hot och kränkningar.

En utredningskommitté har nyligen genomfört en omfattande översyn av det straffrättsliga skyddet av enskilda personers privatliv, särskilt i fråga om hot och andra kränkningar. Kommittén föreslår att det straffrättsliga skyddet av den personliga integriteten stärks och moderniseras, till exempel genom att man inför en ny straffbestämmelse om olaglig kränkning av den personliga integriteten. Den nya bestämmelsen kommer i vissa fall att medföra ett straffrättsligt ansvar för den som kränker en annan persons personliga integritet genom att sprida bilder eller annan information på ett sätt som är avsett att förorsaka påtaglig skada för den person som informationen gäller. Förslagen behandlas för närvarande av regeringen.

Den 17 juni 2014 utsågs en utredningskommitté för att se över tillämpningen av bestämmelsen om kontakt med barn i sexuellt syfte (sexuell gromning) i kapitel 6 paragraf 10a i brottsbalken. Kommittén lade fram sin rapport för regeringen i oktober 2015. Rapporten behandlas för närvarande vid justitiedepartementet.

Dessutom håller en statlig utredningskommitté ("2014 års sexualbrottskommitté") på att genomföra en översyn av våldtäktsbrottet. I översynen ingår också en analys av huruvida straffrätten ger ett tillräckligt starkt skydd mot vissa typer av sexuella övergrepp som begås på internet. Utvärderingsgruppen har underrättats om att kommittén rapporterade om sina resultat den 1 oktober 2016[13].

Polisen samarbetar med barn- och ungdomsforum, särskilt populära webbplatser och sociala forum för barn i Sverige. När barn och ungdomar ser eller får information om sexuella övergrepp eller sexuell exploatering ger de oss de upplysningar vi behöver för att inleda en utredning. Polisen arbetar också för att skapa en "stoppknapp" som barn kan trycka på när de behöver eller vill göra en anmälan om att de har kontaktats av vuxna i sexuellt syfte.

[13] Det bör nämnas att utvärderingsgruppen inte tog hänsyn till kommitténs resultat.

6.2.3 Förebyggande åtgärder mot bland annat sexturism och barnpornografiska föreställningar

År 2009 tillsattes i Sverige en särskild arbetsgrupp som skulle ha ett landsomfattande ansvar för att utreda barnsexturism. För att upptäcka och förebygga barnsexturism har man inlett kampanjer för att öka allmänhetens medvetenhet. Man har också tillhandahållit utbildning för tjänstemän vid de brottsbekämpande myndigheterna och för personer verksamma inom resesektorn osv. samt utvecklat samarbetet med utländska brottsbekämpande myndigheter och inhemska och utländska icke-statliga organisationer, vilket bland annat inbegriper deltagande i gemensamma insatser och gemensamma utredningsgrupper.

Den 22 juni antog regeringen en ny handlingsplan till skydd för barn mot människohandel, exploatering och sexuella övergrepp. Handlingsplanen innehåller ett antal åtgärder som är relevanta för kampen mot barnsexturism, till exempel åtgärder som rör turism- och reseindustrin och utrikesförvaltningen och som syftar till att förbättra upptäckt.

Under de senaste åren har en rad framgångsrika utredningar om direktströmning av sexuell exploatering genomförts som har lett till fällande domar för anstiftan till grov våldtäkt mot barn. Samarbete har upprättats med Finanskoalitionen och internetbaserade betaltjänstleverantörer för att upptäcka och stoppa penningflödet i sådana fall.

Den svenska polisen samarbetar med ECPAT och får information från dess telefonjour. På polisens hemsida kan ett offer eller en person som har information om denna typ av brott anmäla brottet till polisen. På samma sida kan man också läsa om brotten, hur man kan skydda sig och vad man ska göra om man själv eller någon man känner utsätts för ett sådant brott. I samarbete med icke-statliga organisationer har man utarbetat särskilt informationsmaterial som är riktat både till barn och till deras föräldrar.

Det svenska medierådet är ett statligt organ med uppgift att stärka barn och unga som medvetna medieanvändare och skydda dem mot skadlig mediepåverkan. Därför tar medierådet fram utbildningsmaterial som kan användas i klassrummet eller hemma av lärare, bibliotekarier, föräldrar och elever. En del av detta utbildningsmaterial har översatts till engelska, somaliska och arabiska med tanke på invandrarbefolkningen i Sverige. En del av materialet har också getts ut särskilt för barn med intellektuella och psykiska funktionsnedsättningar.

Mellan 2013 och 2015 genomförde det svenska medierådet Europarådets kampanj No Hate Speech Movement i syfte att förebygga rasism, sexism och andra former av hat på internet. Sedan 2015 har man fortsatt med kampanjen, men denna gång på nationell nivå, med en ytterligare aspekt som rör förebyggande av våldsbejakande extremism och propaganda på internet. Inom ramen för denna kampanj har medierådet tagit fram utbildningsmaterial, poddsändningar och onlinematerial där bestämmelser och rättsliga frågor som rör internet förklaras av en rättslig expert. Kampanjen ger också ungdomar och föräldrar råd om hur man ska hantera olagligt och/eller skadligt innehåll som har producerats av andra.

I september 2015 gav regeringen även Skolverket i uppdrag att föreslå nationella IKT-strategier för det svenska skolväsendet. Strategierna ska innehålla målsättningar och insatser för att stärka förutsättningarna för en likvärdig tillgång till IKT inom skolväsendet, en stärkt digital kompetens hos elever och lärare och en IKT-strategisk kompetens hos skolledare.

Strategierna ska säkerställa att digitaliseringens möjligheter tas till vara för skolutveckling och för utveckling av undervisningen. I förslagen ingår skolornas arbete för att förebygga mobbning på nätet och främja integritet och säkerhet online och en kritisk informationsbedömning.

Skolverket fick redan 2008 i uppdrag att främja en säker användning av IKT i skolorna, inbegripet skydd av den personliga integriteten och ett kritiskt förhållningssätt till digital information och onlineinformation. Inom ramen för detta uppdrag har Skolverket publicerat undervisningsmaterial och stöd online för skolor och lärare i dessa frågor. Denna information finns på: www.skolverket.se/kollakallan.

6.2.4 Aktörer och åtgärder mot webbplatser som innehåller eller sprider barnpornografi

Lagen om ansvar för elektroniska anslagstavlor (1998:112) innehåller regler som syftar till att förhindra spridning av barnpornografi. Med elektronisk anslagstavla avses en tjänst för elektronisk förmedling av meddelanden i form av text, bild, ljud eller information i övrigt. Den som tillhandahåller en elektronisk anslagstavla är skyldig att ha uppsikt över dess innehåll. Tillhandahållaren är också skyldig att ta bort ett meddelande från tjänsten eller på annat sätt förhindra vidare spridning av meddelandet, om det är uppenbart att innehållet är barnpornografi. Den som uppsåtligen eller av grov oaktsamhet bryter mot denna skyldighet kan dömas till böter eller fängelse i högst sex månader.

Dessutom sker blockering av webbplatser med barnpornografiskt innehåll i Sverige genom frivilligt samarbete mellan polisen och internetleverantörerna. 85–90 % av internetabonnenterna i Sverige omfattas av detta frivilliga samarbete.

Samarbetet fungerar så att polisen får information om barnpornografiska webbplatser via olika kanaler såsom Europol, Interpol, organisationer för barns rättigheter eller allmänheten. Polisen samlar också in information i sitt dagliga arbete för att bekämpa barnpornografi på internet.

Informationen kontrolleras och förmedlas sedan till internetleverantörerna, som vidtar de tekniska arrangemangen för blockering på slutanvändarnivå. Detta innebär att den som försöker få tillgång till webbplatsen i fråga i stället ser ett meddelande (se bilaga) om att webbplatsen är blockerad på grund av sitt barnpornografiska innehåll.

EU:s formella gränser har ingen betydelse för huruvida en internetleverantör i samarbete med den svenska polisen kommer att blockera en webbplats eller inte. Med andra ord kommer webbplatser med barnpornografiskt innehåll att blockeras och göras otillgängliga i Sverige oberoende av om webbplatsen ligger inom eller utanför EU.

Vid kontrollen om en webbplats innehåller barnpornografiskt material kontrollerar polisen också var webbplatsen är lokaliserad. I samband med blockeringen och på grundval av den skickas information till den behöriga rättsliga eller brottsbekämpande myndigheten i det land där webbplatsen är lokaliserad. Tack vare denna information får myndigheten vetskap om att en webbplats på dess territorium innehåller olagligt material. Inga andra åtgärder vidtas emellertid, eftersom åtgärderna skulle kunna påverka till exempel en pågående utredning i det landet.

Sveriges nationella it-brottscentrum har specialiserade tjänstemän som uteslutande arbetar med material med sexuella övergrepp mot barn, i syfte att identifiera barn och gärningsmän. Utredningarna genomförs inom polisregionerna och oftast av för ändamålet utbildade tjänstemän. Sedan 2006 har omkring 300 tjänstemän utbildats i att identifiera offer och ca 500 har fått utbildning och särskild skolning i att hantera utredningar som rör barn (personerna är inte alltid desamma och alla arbetar inte längre med sexuell exploatering av barn.)

Vissa regioner, men ännu inte alla sju, har specialiserade enheter som enbart hanterar material och utredningar som rör sexuella övergrepp mot barn. Det finns dock ingen centraliserad statistik med uppgifter om de regionala enheternas sammansättning och storlek.

6.3 Betalkortsbedrägerier på internet

6.3.1 Onlinerapportering

Det finns inget onlineverktyg för rapportering av it-brott till den svenska polisen. I nästan alla fall får polisen endast information från polisanmälningar som gjorts. Många it-angrepp anmäls inte eller anmäls bara till andra myndigheter än polisen. Polisen är skyldig att göra en anmälan när den blir medveten om ett eventuellt brott. Därför tvekar ofta offren (t.ex. verkställande direktörer eller företag) att kontakta polisen i händelse av it-angrepp, av rädsla för att lida ytterligare skada till följd av oönskad publicitet. För att minska denna underrapportering har det nationella bedrägericentret möjlighet att "spärra" ett ärende och således inte informera polisen.

Medborgarna anmäler ofta dessa fall till polisen eftersom svenska banker i allmänhet kräver att en polisanmälan har gjorts innan den ersätter förlusterna. Privata företag tenderar att inte göra anmälan lika ofta. En möjlig orsak till detta kan vara att de uppskattar att tidsåtgången och kostnaderna av anmälan är större än sannolikheten för att brottet reds ut.

Uppgifter om kortlösa bedrägerier (Card not present-bedrägerier (CNP)): under de sex första månaderna av 2016 gjordes totalt 38 700 polisanmälningar angående CNP. Under 2015 gjordes 21 100 anmälningar under samma tidsperiod.

Information om personuppgifter och finansiella uppgifter i Sverige finns relativt öppet och tillgängligt tillhanda. Polisen informerar regelbundet berörda parter om att detta är ett problem och att det krävs lagstiftningsändringar för att förhindra att brottslingar får tillgång till informationen.

6.3.2 Den privata sektorns roll

Sveriges polis, banker, betaltjänstleverantörer, bensinbolag och logistikföretag har i flera år idkat ett nära samarbete. Information om ett nytt tillvägagångssätt utbyts alltid mellan båda parter.

Den svenska polisen är engagerad i kortsäkerhet online och magnetremsans sårbarhet och samarbetar med svenska banker på detta område.

Genom olika kommittéer, diskussionsgrupper och forum deltar den privata sektorn aktivt i att samordna insatserna för att bekämpa it-brottslighet och öka medvetenheten. Exempelvis samarbetade den privata sektorn med MSB för att utveckla utbildningsverktyg för användare i både offentliga och privata organisationer.

6.4 Slutsatser

- MSB har utarbetat en nationell hanterandeplan för allvarliga it-incidenter. För närvarande har enheter inom kritisk infrastruktur i den privata sektorn ingen rättslig skyldighet att anmäla it-angrepp till polisen. Detta kommer dock att ändras när it-säkerhetsdirektivet genomförs. Offentliga myndigheter i Sverige har en skyldighet att anmäla it-angrepp, medan privata enheter inte har det.

- De svenska myndigheterna har vidtagit flera olika åtgärder för att ta itu med sexuella övergrepp och sexuell exploatering av barn, bland annat preventions- och informationskampanjer samt lagstiftningsåtgärder och blockering av webbplatser med olagligt innehåll. Dessa åtgärder syftar till att upplysa allmänheten, föräldrar och barn om riskerna med skadliga/olagliga beteenden på internet.

- Strategierna ska säkerställa att digitaliseringens möjligheter tas till vara för skolutveckling och för utveckling av undervisningen. Nya förslag som är under behandling syftar till att förebygga mobbning på nätet och främja integritet och säkerhet online och en kritisk informationsbedömning.

- Sveriges nationella it-brottscentrum har specialiserade tjänstemän som uteslutande arbetar med material med sexuella övergrepp mot barn, i syfte att identifiera barn och gärningsmän, och vissa regioner har specialiserade enheter som enbart hanterar material och utredningar som rör sexuella övergrepp mot barn.

- Under de senaste åren har en rad framgångsrika utredningar om direktströmning av sexuell exploatering genomförts som har lett till fällande domar för anstiftan till grov våldtäkt mot barn.

- Polisen arbetar med ECPAT och länsstyrelsen, som har etablerat jourtelefoner till vilka allmänheten kan anmäla alla internetrelaterade sexuella övergrepp mot barn. Informationen vidareförmedlas direkt till polisen. Polisen och ECPAT är också aktiva partner i Finanskoalitionen. Det övergripande tillvägagångssättet och de åtgärder som har vidtagits av de svenska myndigheterna på detta område utgör god praxis som bör spridas till andra medlemsstater.

- När det gäller betalkortsbedrägerier på nätet idkar de svenska brottsbekämpande myndigheterna nära samarbete med banksektorn (t.ex. automatiserade och standardiserade förfrågningar). I allmänhet utreds bedrägerier lokalt och ofta saknar utredarna erfarenhet av gränsöverskridande utredningar och samarbete.

- Samarbete har upprättats med Finanskoalitionen och internetbaserade betaltjänstleverantörer för att upptäcka och stoppa penningflödet i sådana fall. Detta samarbete sker dock på frivillig basis och således är det möjligt att de svenska myndigheterna inte är tillräckligt medvetna om it-bedrägeriernas omfattning.

- Utvärderarna anser att it-brottsutredningar som omfattar vinning måste åtföljas av ekonomiska utredningar för eftersökning, beslagtagande och förverkande av sådan vinning. På motsvarande sätt måste ekonomiska utredningar som omfattar brott mot och med hjälp av datorer åtföljas av it-brottsutredningar. Rent praktiskt innebär detta tätt samarbete mellan enheter som utreder it-brott, finansutredningsgrupper och finansunderrättelseenheter

- Information om personuppgifter och finansiella uppgifter i Sverige finns relativt öppet och tillgängligt tillhanda. Polisen informerar regelbundet berörda parter om att detta är ett problem. Möjligen krävs det lagstiftningsändringar för att förhindra att brottslingar får tillgång till informationen.

- Utvärderarna anser att utredningsresurserna eventuellt inte är tillräckliga med tanke på det stora antalet ärenden.

7 INTERNATIONELLT SAMARBETE

7.1 Samarbete med EU-byråer

7.1.1 Formella krav för samarbetet med Europol/EC3, Eurojust och Enisa

Åklagarmyndigheten har samarbetat med EU-byråer vid flera tillfällen, bland annat i samband med följande:

- Operation Onymous – samarbete med Europol/EC3 och Eurojust. Brott begångna på darknet – Silk road.
- Operation Black Shades – samarbete med bland annat EC3 och Eurojust. Sabotageprogram och bedrägerier.
- Operation Ateljé – samarbete med stöd av Eurojust. Produktion av barnpornografi.

Den svenska polisen har deltagit i flera operationer och ett antal projekt med två eller flera involverade medlemsstater. I de flesta ärenden har Europol tillhandahållit stöd och samordning. Ibland har även Eurojust varit involverad. Ett bra exempel på en operation är Onymous från november 2014. Syftet med operationen var att stänga ner flera marknadsplatser på det dolda Tor-nätverket. Det EU-finansierade projektet avseende olaglig handel på marknadsplatser online (Itom, Illegal Trade on Online Marketplaces) är kopplat till denna operation. Sverige deltog både på strategisk och operativ nivå.

Ett annat fallexempel från polisen är den multinationella operationen Bygbyte/Shrouded Horizon där ett av de största kriminella hackerforumen stängdes ner medan arresteringar, husrannsakningsorder och beslagtagningar verkställdes samtidigt i flera länder runtom i världen. Samarbete om banktrojaner genomfördes också under ledning av EC3, till exempel i fråga om Retafe och Dridex.

Inga sådana krav eller förfaranden finns med avseende på Enisa.

När det gäller sexuell exploatering av barn används databasen ICSE regelbundet och det görs många förfrågningar om olika typer av information. Sveriges polis deltar även i alla expertmöten.

Eurojust används också på grund av dess förbindelser till länder som USA, Norge och Schweiz, vilket underlättar kontakterna och samarbetet. Dessutom fungerar enligt Åklagarmyndigheten förfarandet för att bjuda in tredjeländer till samarbetsmöten i Eurojusts utrymmen bra.

Många tredjeländer och myndigheter är företrädda vid Europol i Haag, vilket har främjat samarbetet. Tredjeländerna/parterna deltar i olika forum och arbetsgrupper. Sverige har goda bilaterala förbindelser med många av dessa parter, men det faktum att de är företrädda vid Europol underlättar samarbetet.

7.1.2 Utvärdering av samarbetet med Europol/EC3, Eurojust och Enisa

Eurojust har vid flera tillfällen spelat en viktig roll i ärenden som rör fler än en medlemsstat.

Samarbete förekommer med Enisa och Europol.

Enisa kan bidra med sin tekniska expertis inom nät- och informationssäkerhetsfrågor och samla in och sprida expertis från andra källor. Mervärdet rör snarare förebyggande arbete och informationsspridning än begränsningsåtgärder eller utredningar. Enisas nätverk av personer med kunskap om nät- och informationssäkerhet är en tillgång. Det har inte samlats några erfarenheter av samarbete med Enisa i fråga om it-brottsfall.

Europols arbete baserar sig på medlemsstaternas bidrag när det gäller tillhandahållna uppgifter men även på riktlinjer i fråga om prioriteringar. För att uppnå goda resultat av samarbetet med Europol måste Sverige inte enbart bidra med information från pågående och avslutade utredningar och underrättelseärenden, utan också sända tydliga och specifika förfrågningar till Europol. Den svenska polisen skulle kunna använda expertisen hos EC3 i högre grad än den gör i dag.

När det gäller Enisa och Europol anser de svenska myndigheterna att en ändring av förfarandena eller mandaten förmodligen skulle ha begränsad inverkan. En ökning av resurserna skulle antagligen ha större effekt, om det fanns en möjlighet att öronmärka dessa resurser för detta syfte.

Enligt de svenska myndigheterna är Sveriges deltagande i J-CAT absolut nödvändigt för att man ska kunna arbeta på ett mer strukturerat, effektivt och smidigt sätt i it-brottsfall. Brott känner inga gränser, och Sverige måste spela en aktivare roll i det internationella samfundets arbete.

Utöver detta konstaterades det att det finns ett behov av att sända flera anställda i allmänhet till EC3, där de kan lära sig av den internationella brottsbekämpningen och samtidigt bidra till en gemensam, internationell insats samt främja specifika svenska intressen och den svenska polisen.

7.1.3 De gemensamma utredningsgruppernas och it-övervakningens operativa resultat

Operation Ateljé gällde produktion och anskaffande av barnpornografi. En gemensam utredningsgrupp med tre medlemsstater inrättades och det hölls flera möten. Eurojust anordnade samordningsmöten som den gemensamma utredningsgruppens medlemmar och flera andra länder deltog i. Samarbetet mellan den gemensamma utredningsgruppens medlemmar fungerade mycket bra och den gemensamma utredningsgruppen spelade en viktig roll för operationens framgång.

Sedan 2014 har Sveriges nationella it-brottscentrum varit engagerat i en verksamhet vid EMPACT (prioritet G, it-angrepp), vars syfte är att inrätta internetövervakning. Denna verksamhet har utvecklats från en operativ idé till en mer teoretisk sådan med ett kapacitetsuppbyggande ändamål.

Enligt Åklagarmyndigheten är en gemensam utredningsgrupp ett utmärkt verktyg för att underlätta samarbetet mellan medlemsstaterna. Det är viktigt att det fortsättningsvis finns en möjlighet att ansöka om och få finansiering för utredningarna.

7.2 Samarbete mellan de svenska myndigheterna och Interpol

De svenska myndigheterna rapporterade att viss operativ information har sänts från Interpol, men att det inte rörde sig om särskilt mycket information och att informationen inte heller ansågs vara särskilt relevant. Några ärenden har inletts och samordnats av Interpol och samtliga har till en början sett lovande ut, men de har också varit tidskrävande och alltför diffusa. De yrkesverksamma som intervjuades anser att Sverige, för att undvika missförstånd och dubbelarbete, i mån av möjlighet bör sträva efter att arbeta på det internationella planet via Europol. Förbindelsen till Interpol kan upprättas med hjälp av Interpols sambandsman vid Europol.

7.3 Samarbete med tredjeländer

Till exempel när det gäller ömsesidig rättslig hjälp är den underliggande principen att de svenska myndigheterna bistår främmande stater i möjligaste mån och med alla åtgärder som finns tillgängliga för de svenska myndigheterna i inhemska utredningar eller förfaranden.

Flera framställningar har skickats till och mottagits från USA och Kanada. Den rättsliga grunden är bilaterala avtal med USA respektive Kanada. Dessa framställningar gäller flera olika typer av ömsesidig rättslig hjälp och har lett till varierande resultat.

I fråga om både USA och Kanada tar det vanligtvis en lång tid innan man får ett svar.

7.4 Samarbete med den privata sektorn

NetClean eller Griffeye har installerats på datorerna vid många privata företag i syfte att upptäcka om de anställda använder barnpornografi.

Internetbaserade betaltjänstleverantörer anmäler misstänkt verksamhet till polisen. Polisen har i vissa fall bett den privata sektorn om hjälp med utbyte av information och vissa andra åtgärder, trots att ingen skyldighet föreligger. Samarbete har upprättats med de större bankerna för att de ska kunna tillhandahålla information och vidta åtgärder. Vissa ärenden har hanterats i samarbete med Cert-SE och samarbetet med den privata sektorn (till exempel internetleverantörer) är gott.

Enligt kapitel 6 paragraferna 16a och 16d i lagen om elektronisk kommunikation (2003:389) är internetleverantörer skyldiga att lagra trafikuppgifter och användarinformation (såsom namn, adresser, telefonnummer osv.) i sex månader. Efter sex månader måste uppgifterna utplånas. För att få tillgång till trafikuppgifter för användning i förundersökningar behövs vanligtvis ett tillstånd av domstol, och vissa krav måste vara uppfyllda. Om det finns misstanke om brott måste internetleverantören på begäran lämna användarinformation till en åklagarmyndighet eller polismyndighet (kapitel 6, paragraf 22.2 i lagen om elektronisk kommunikation). Internetleverantörer är också bundna av tystnadsplikt bland annat när det gäller begäranden från brottsbekämpande myndigheter. Om en internetleverantör inte uppfyller sina skyldigheter kan Post- och telestyrelsen utfärda ett föreläggande. En webbplats som innehåller barnpornografi blockeras vanligen frivilligt av internetleverantören efter det att polisen har informerat denne om webbplatsens innehåll.

När informationen är lagrad i ett tredjeland eller när åklagaren behöver få utredningsåtgärder utförda i ett tredjeland måste åklagaren vanligtvis begära ömsesidig rättslig hjälp och vända sig till de rättsliga myndigheterna i det landet. Det är inte alltid möjligt att gå via en lokal filial för att få denna information. Till exempel har Facebook servrar i Sverige och en lokal filial, men för att få information från dessa servrar måste åklagaren ändå gå via huvudkvarteret i USA. När det är möjligt att ha direkt kontakt sker detta vanligtvis via polisen.

Tvångsåtgärder mot privata företag i tredjeländer omfattas alltid av ömsesidig rättslig hjälp. Sådana åtgärder har utförts vid flera tillfällen. Det är vanligt med tvångsåtgärder mot privata företag i Sverige, både när någon som arbetar vid företaget är misstänkt och när informationen är lagrad där.

I vissa fall har det emellertid inte ansetts vara möjligt eftersom mängden information är så enorm och det är omöjligt för en utomstående att veta var informationen är lagrad och att hitta den.

SC3 skulle vilja se att mer resurser tilldelades för förbättring av samarbetet med den privata sektorn. Det är sist och slutligen inom privatägda och privatdrivna infrastrukturer som it-brott begås och det är där som de bevis och spår som behövs för en utredning finns.

I kampen mot barnpornografi på internet samarbetar polisen med ECPAT Sverige och inom den finansiella sektorn och telekommunikationssektorn med Finanskoalitionen i syfte att stoppa och spåra betalningar för sådant material.

När det gäller betalkortsbedrägerier har det kunnat konstateras att svenska polisen, banker, betaltjänstleverantörer, bensinbolag och logistikföretag har idkat ett nära samarbete i flera år.

Vad gäller it-angrepp framhäver man i det nationella programmet för fonden för inre säkerhet även ett förbättrat samarbete och en förbättrad samordning mellan alla aktörer när det gäller att skydda informations- och kommunikationsinfrastrukturen.

Åklagarmyndigheten har inga direkta kontakter till den privata sektorn, såsom internetleverantörer, finansiella institut osv. Dessa kontakter handhas av polisen.

7.5 Verktyg för internationellt samarbete

7.5.1 Ömsesidig rättslig hjälp

Den myndighet som ansvarar för mottagande av framställningar om ömsesidig rättslig hjälp i samband med utredningar som rör it-brottslighet är Åklagarmyndigheten. Framställningarna handläggs vanligtvis av en av de internationella åklagarkamrarna i Stockholm, Göteborg och Malmö. En åklagare fattar beslut om huruvida framställningen ska verkställas. Om framställningen inte kan verkställas, t.ex. på grund av att brottet i fråga är av politisk eller militär karaktär, eller om det skulle stå i strid med grundläggande rättsliga rättigheter i Sverige att tillmötesgå framställnigen, fattar regeringen beslut om att neka rättslig hjälp.

Framställningar från andra medlemsstater kan skickas direkt till de internationella åklagarkamrarna. Framställningar från länder utanför EU bör sändas till justisdepartementet.

Den åklagare som ansvarar för förundersökningen ansvarar även för att sända framställningar om ömsesidig rättslig hjälp. Åklagaren skickar framställningen direkt till den behöriga rättsliga myndigheten i de andra medlemsstaterna. Åklagaren använder ofta den europeiska rättsliga atlasen för att fastställa vilken den korrekta adressen är. Om framställningen ska skickas till ett land utanför EU skickas den via justisdepartementet.

Alla inkommande framställningar förs in i Åklagarmyndighetens registreringssystem (Cåbra). Detta system gör det möjligt att följa ett fall från registreringen till dess att svaret skickas till det ansökande landet. Därtill har Internationella åklagarkammaren i Stockholm (som är den åklagarkammare som handlägger de flesta inkommande framställningarna om ömsesidig rättslig hjälp) skapat ett ännu bättre och mer detaljerat system där varje fall av ömsesidig rättslig hjälp följs upp separat.

Inkommande framställningar som mottas av Internationella åklagarkammaren i Stockholm handläggs på ett allt effektivare sätt så att handläggningstiden för de flesta ärenden är högst två månader. Tillfälliga förseningar i att besvara en framställning beror inte på en brist på resurser eller prioritering, utan snarare på den tid det tar att samla in information (t.ex. bankuppgifter eller krypterade servrar), oförmåga att kontakta den relevanta personen, framställningens komplexitet eller behovet av att komplettera informationen från det ansökande landet.

Enligt kapitel 2 paragraf 10 i lagen om internationell rättslig hjälp i brottmål ska inkommande ansökningar om rättslig hjälp behandlas skyndsamt. Enligt kapitel 2 paragraf 3 i Åklagarmyndighetens interna föreskrifter (ÅFS 2007:12) bör handläggningstiden för ansökningar om rättslig hjälp inte överstiga två månader.

Om den medlemsstat som har sänt framställningen anger en orsak till att framställningen är särskilt brådskande försöker man handlägga den så snabbt som möjligt. Enligt kapitel 2 paragraf 10 i lagen om internationell rättslig hjälp i brottmål ska ansökningar om rättslig hjälp behandlas skyndsamt.

Statistiska uppgifter samlas in från registreringssystemet. I detta system finns det inga uppgifter om det internationella instrument enligt vilket en framställning om ömsesidig rättslig hjälp har gjorts, eftersom internationella instrument införlivas i nationell rätt. Med andra ord är den rättsliga grunden för att göra en framställning eller för att svara på en framställning den nationella rätten, inte det internationella instrumentet. Det är inte heller möjligt att få fram statistiska uppgifter om vilken typ av it-brott en framställning gäller. Det totala antalet framställningar om ömsesidig rättslig hjälp som avsändes från Åklagarmyndigheten under 2015 var 491. Under samma period mottogs 836 framställningar.

Alla åtgärder som kan vidtas vid andra brott kan också vidtas med avseende på it-brott. Vissa typer av hjälp, t.ex. avlyssning, kan emellertid förutsätta ett visst minimistraff. Den vanligaste orsaken till att göra framställningar om ömsesidig rättslig hjälp är spårning av IP-adresser.

När myndigheterna mottar en framställning om ömsesidig rättslig hjälp som rör information i molnet, har denna information vanligtvis spårats till en server i Sverige. I sådana fall har man inte upptäckt några allvarliga problem när det gäller att tillhandahålla ömsesidig rättslig hjälp avseende information i molnet.

Ibland har dock informationen på en server försvunnit i det skedet när framställningen mottas. Om informationen är försvunnen är det besvärligt att tillhandahålla ömsesidig rättslig hjälp – det finns nämligen ingen rättslig grund för att genomföra en formell rannsakan av "molnet". Detta är ett problem, särskilt eftersom det blir allt vanligare att till exempel redovisningstjänster tillhandahålls som molntjänster. För tillfället diskuterar Ekobrottsmyndigheten med molntjänstleverantörer möjligheten att i samband med brottsutredningar få tillgång till redovisning som lagras i molnet.

Utgående framställningar om ömsesidig rättslig hjälp är ofta problematiska eftersom det i många fall är svårt att avgöra vart en framställning ska sändas.

Åklagarmyndigheten använder sig av framställningar om ömsesidig rättslig hjälp när detta är möjligt. Processen är dock ofta alltför långsam.

7.5.2 Instrument för ömsesidigt erkännande

Statistiska uppgifter samlas in från registreringssystemet. Det finns ingen uppgift om vilket internationellt instrument som har använts för internationellt samarbete i detta system. Det är inte heller möjligt att få statistiska uppgifter om huruvida ett fall av internationellt samarbete gällde it-brottslighet. Det kan noteras att erkännande av ekonomiska påföljder i praktiken mer eller mindre uteslutande tillämpas på trafikbrott.

7.5.3 Överlämnade/utlämning

Ett brott behöver inte finnas på förteckningen för den europeiska arresteringsordern för att kunna leda till överlämnande. Andra brott kan också leda till överlämnande (eller utlämning) förutsatt att de betraktas som brott i Sverige. När det gäller utlämning måste brottet dessutom enligt svensk rätt kunna bestraffas med ett fängelsestraff eller en frihetsberövande åtgärd på minst 12 månader eller, om dom har avkunnats eller en frihetsberövande åtgärd har dömts ut, med en dom på minst fyra år. De flesta it-brott uppfyller detta kriterium, med undantag för t.ex. lindrigare fall av bedrägeri.

Vissa svenska it-brott omfattas av förteckningen för den europeiska arresteringsordern men uppfyller inte kravet på att kunna bestraffas med fängelsestraff på minst tre år (t.ex. lindrigare eller normala fall av bedrägeri eller smärre brott i samband med barnpornografi). Allvarliga eller grova fall av bedrägeri eller barnpornografi uppfyller också treårskravet.

Sverige har ett multilateralt avtal med Finland, Norge, Danmark och Island om den nordiska arresteringsordern som tillämpas i stället för avtalet mellan EU:s medlemsstater, Island och Norge. Detta avtal tillämpas ofta.

Den europeiska arresteringsordern och den nordiska arresteringsordern utfärdas - beträffande alla typer av brott - av en allmän åklagare om det rör sig om lagföring. Rör det sig om verkställighet av en dom utfärdades arresteringsordern av den nationella polismyndigheten på begäran av Kriminalvården.
Till följd av domstolens dom i målet Poltorak, C-452-16 PPU, har Åklagarmyndigheten nyligen utsetts att utfärda arresteringsorderna i sådana fall.
Framställningar om utlämning utfärdas av en allmän åklagare eller av Kriminalvården och går via Justitiedepartementet.

Inkommande europeiska arresteringsorder och nordiska arresteringsorder handläggs - beträffande alla typer av brott - av en allmän åklagare. En domstol beslutar om framställningarna. När det gäller nordiska arresteringsorder kan åklagaren under vissa omständigheter fatta beslut. Framställningar om utlämning mottas av Justitiedepartementet och översänds sedan till åklagarmyndigheten för handläggning, men det är Sveriges regering som fattar beslut om ansökningar om utlämning.

Europeiska och nordiska arresteringsorder kan skickas direkt mellan de behöriga myndigheterna. SIS används också. Det europeiska rättsliga nätverket och Eurojust kan också användas för att finna den rätta mottagande myndigheten.
Framställningar om utlämning kan skickas direkt till Justitiedepartementet.

Statistiska uppgifter samlas in från registreringssystemet. I detta system finns det ingen uppgift om det internationella instrument enligt vilket en framställning om överlämnande eller utlämning har gjorts. Det är inte heller möjligt att få fram statistiska uppgifter om vilken typ av it-brott en framställning gäller.

Det totala antalet europeiska arresteringsorder som utfärdades av svenska åklagare under 2015 var 258. Under samma period mottogs 142 europeiska arresteringsorder. Det totala antalet nordiska arresteringsorder som utfärdades av svenska åklagare under 2015 var 33. Under samma period mottogs 47 nordiska arresteringsorder. Det totala antalet framställningar om utlämning som avsändes från Sverige under 2015 var 30. Under samma period mottogs 21 framställningar om utlämning.

Det finns inga särskilda förfaranden som ska följas eller villkor som ska uppfyllas vad avser framställningar med koppling till it-brottslighet. Framställningar om överlämnande eller utlämning med koppling till it-brottslighet handläggs, liksom alla framställningar om överlämnande och utlämning, snabbt. Provisoriska gripanden är möjliga och i de flesta fall genomförs sådana gripanden. Under 2015 var den genomsnittliga tiden för ett fullständigt överlämandeförfarande enligt den europeiska arresteringsordern när personen samtyckte till överlämnande 13 dagar. Den genomsnittliga tiden är personen inte samtyckte var 35 dagar.

7.6 Slutsatser

- Sverige samarbetar nära med EU-organ, särskilt Europol, EC3, J-Cat och Eurojust. De svenska rättsliga myndigheterna anlitar ofta den sakkunskap och de möjligheter som tillhandahålls av Eurojust, vilket ofta är avgörande när det gäller it-brottslighet. Sverige betraktar samarbetet med EU-organ som både nödvändigt och tillfredsställande vad beträffar kampen mot it-brottslighet, även vid samarbete med tredjestater, där dessa organ kan verka som mellanhänder.

- Även om samarbetet med Interpol på området it-brottslighet befanns vara tillfredsställande, är svenska polisen mycket mer aktiva i samarbetet inom Europol.

- Sverige har ett multilateralt avtal med Finland, Norge, Danmark och Island om den nordiska arresteringsordern som tillämpas i stället för avtalet mellan EU:s medlemsstater.

- Sverige samarbetar med andra länder på grundval av internationella eller bilaterala avtal (t.ex. med USA och Kanada). De rättstillämpare man träffade tog dock upp be3hovet av större svensk medverkan i samarbetet inom olika internationella forum. Eftersom brott inte vet av några gränser anser utvärderarna att Sverige bör spela en mer aktiv roll i arbetet i det internationella samfundet både för att lära sig av andra länder och för att utbyta erfarenheter med dem.

- Vad beträffar samarbetet med internetleverantörer och andra länder har Sverige upprättat mycket goda kontakter med de viktigaste intressenterna i den offentliga och den privata sektorn, särskilt genom att ha en enda kontaktpunkt för framställningar. Systemet med en enda kontaktpunkt har hittills visat sig mycket fruktbart, särskilt vad beträffar att bygga upp förtroende, vinna erfarenheter och ständigt försöka förbättra informationsutbytet eller verkställigheten av framställningar. Detta system innebär också mervärde vad avser sakkunskap och sammankoppling. Ett svar från Facebook tar för närvarande – i genomsnitt – två veckor.

- När det gäller ömsesidig rättslig hjälp är den underliggande principen att de svenska myndigheterna bistår främmande stater i möjligaste mån och med alla åtgärder som finns tillgängliga för dem i inhemska utredningar eller förfaranden.

- Även om polisen har starka informella kontakter med USA-baserade internationella tjänsteleverantörer inom den privata sektorn måste vissa rättsliga framställningar gå via officiella kanaler för ömsesidig rättslig hjälp. Detta tar ofta lång tid.

- Sverige har en enda databas för registrering och uppföljning av inkommande framställningar om ömsesidig rättslig hjälp (SPA), vilket avsevärt minskar den tid som går till att handlägga dem. I detta system är det möjligt att följa ett fall från registreringen till dess att svaret skickas till det ansökande landet. Därtill har Internationella åklagarkammaren i Stockholm (som är den åklagarkammare som handlägger de flesta inkommande framställningar om ömsesidig rättslig hjälp) skapat ett ännu mer förbättrat och detaljerat system där varje fall av ömsesidig rättslig hjälp följs upp separat. Detta praktiska verktyg kunde rekommenderas som ett exempel på bästa praxis.

8 UTBILDNING, SKAPANDE AV ÖKAD MEDVETENHET OCH FÖREBYGGANDE

8.1 Särskild utbildning

Domare

Domarakademin i Sverige tillhandahåller vidareutbildning för domare. Det finns inte någon särskild utbildning i frågor som rör it-brottslighet. Däremot anordnar Domarakademin årliga seminarier i straffrätt rörande aktuella teman.

Från 2010 erbjöd Domarakademin en serie utbildningssessioner om it-brottslighet. Den bestod av tre olika utbildningssessioner på två dagar var. Tretton domare deltog i den första delen 2010 och elva domare deltog i den andra delen som hölls 2011. 2012 erbjöds åter den första och den andra delen, men tyvärr var antalet domare som ansökte för litet och utbildningssessionerna annullerades. Den tredje delen av serien med utbildningssessioner annullerades av samma orsak. Därtill anordnades 2015 ett tvådagarsseminarium för domare om it-brottslighet och it.

Akademin har också årliga utbildningsprogram om teknisk bevisning och it-forensik. I genomsnitt deltar 50-60 domare i dessa straffrättsliga seminarier och utbildningsprogram varje år. 2016 planerade Domarakademin att skicka domare till det europeiska rättsliga nätverkets seminarium Linguistics seminar on the Vocabulary of Cybercrime i Madrid.

Dessutom inbegriper utbildningsprogrammen för domare under utbildning en utbildningssession om teknisk bevisning som äger rum i Nationellt forensiskt centrum i Linköping. Denna utbildningssession är av samma typ som den som erbjuds ordinarie domare och beskrivs i vårt förra svar. Under denna utbildningssession har deltagarna möjlighet att delta i föreläsningar och förevisningar som hölls av experter vid Nationellt forensiskt centrum, bland dessa en expert på it-forensik. Utöver denna utbildningssession ingår ingen särskild utbildning om it-brottslighet i programmen för domare under utbildning.

Åklagarmyndigheten

Svenska åklagarmyndighetens utbildningsenhet tillhandahåller en kurs med anknytning till it-brottslighet inom den obligatoriska grundutbildningen och inom vidareutbildningen för åklagare.

Under grundutbildningen hålls totalt 8 + 6 lektioner som omfattar särskild utbildning med anknytning till it-brottslighet. Exempel på teman som ingår: internets grundstruktur, tvångsåtgärder i it-miljö, IP-spårning, sexualbrott på internet och barnpornografi.

Inom vidareutbildningen består den it-relaterade straffrättsliga kursen av en enveckasutbildning för 25 åklagare som hålls två gånger om året. Ämnena är: internets struktur och olika spårningstekniker, tvångsåtgärder och digital bevisning, rättsliga instrument inom ramen för rättegångsbalken, barnpornografi på internet, nya metoder för betalning på internet och ett studiebesök hos polisen.

Under hösten 2016 hölls en ny enveckaskurs för erfarna åklagare i samarbete med den svenska polisen och detta kommer i framtiden att fortsätta en gång om året. Den fokuserade på mer komplexa fall och på hur man ska planera och genomföra utredningar och på användning av olika tvångsåtgärder i it-miljö.

Den interna webbaserade handledningen om it-brottslighet lanserades 2015. Handledningen är tillgänglig för all personal vid Åklagarmyndigheten. Med anledning av de ständiga förändringarna på detta område kommer handledningen att ändras och uppdateras kontinuerligt - så som redan skett.

Polisen

Polisen tillhandahåller utbildning för åklagare, domare och brottsbekämpande tjänstemän som arbetar med barnpornografi och står dessutom värd för en årlig konferens om it-brottslighet för brottsbekämpande tjänstemän som arbetar på området it-brottslighet och identifiering av offer. Antalet deltagare ökade från 200 till 300 mellan 2015 och 2016, ett tecken på att de mänskliga resurserna växer.

Svenska polisen håller på att inrätta en ny plattform för utbildning som också inbegriper utredare av it-brottslighet.

Nationellt forensiskt centrum och SC3 arbetar på att ytterligare utveckla utbildningsmöjligheterna. I framtiden kommer även externa aktörer såsom universitet att involveras.

Svenska polisen har inte några lättillgängliga siffror som specifikt rör utbildning med anknytning till it-brottslighet.

Det har hållits några kurser om gemensamma utredningsgrupper där personal från SC3 har deltagit. Cepol tillhandahöll olika typer utbildning, t.ex. webinarseminarier (ca 60-90 minuter) och vanliga utbildningskurser (fem dagar).

SC3 genomför intern utbildning för sju polisregioner. Den utbildningsplattform som nu håller på att utvecklas av SC3 och Nationellt forensiskt centrum är avsedda att i framtiden involvera externa aktörer, t.ex. från akademier.

Det finns särskilt utformade treåriga högskolekurser i it-forensik och informationssäkerhet, t.ex. vid Högskolan i Halmstad och Högskolan i Skövde i väster, Blekinge Tekniska Högskola i söder och Luleå Tekniska Universitet i norr.

8.2 Skapande av ökad medvetenhet

Statens medieråd har fått i uppgift av regeringen att analysera den offentliga sektorns, privata aktörers och det civila samhällets roll när det gäller att skydda barn från rasism, sexism och extremism på nätet. Syftet med analysen är att se vad som ytterligare kunde göras av dessa aktörer för att öka skyddet för barn mot sådana skadliga inflytelser. Arbetet med denna uppgift pågår under 2016-2017.

Statens medieråd framställer utbildningsmaterial för lärare och skolbibliotekarier som de kan diskutera med eleverna i eller utanför klassrummet. Forskning som genomförts av medierådet visar att barn i Sverige börjar använda internet vid två års ålder. Därför har medierådet inlett ett partnerskap med mödravårdscentraler i Stockholm för att informera föräldrar till barn på 0-2 år om barns beteende online och om hur man kan övervaka/skydda dem.

8.3 Förebyggande

8.3.1 Nationell lagstiftning/politik och andra åtgärder

Den 22 juni 2016 antog regeringen en ny handlingsplan för skydd av barn mot människohandel, exploatering och sexuella övergrepp. Handlingsplanen omfattar 23 åtgärder, inbegripet en rad viktiga åtgärder för att skydda barn mot brott med anknytning till internet.

Polisen

Gemensamma åtgärder pågår med ECPAT och länsstyrelsen: informationsbroschyrer har framställts, brottsbekämpande tjänstemän får utbildning, samarbete med icke-statliga organisationer utvecklas, och riktade åtgärder används inom resesektorn.

Informationskampanjer (för att öka medvetenheten) som riktar sig till allmänheten planeras. Nyligen fick kampanjen RESEKURAGE mot barnsexturism, ett kooperativt initiativ från länsstyrelsen, en utmärkelse.

En ny metod för förebyggande har inletts och införlivats med det arbete som utförs av utredningsgruppen för it-brott. Som en del av en förebyggande strategi förutsätts den taktiska interventionen "proaktiva samtal" användas mot enskilda personer (ungdomar) som riskerar att i framtiden begå it-brott (det bör finnas specifika indikatorer, men inte så allvarliga eller så många att personen utreds eller rentav åtalas).

Skolverket

Skolverket i Sverige fick sommaren 2015 i uppdrag att förse lärare, rektorer och tillhandahållare av utbildning inom den obligatoriska utbildningen och gymnasieutbildningen med omfattande kontinuerlig vidareutbildning inom yrket, s.k. nationella utvecklingsprogram, på olika områden. Ett av de utvalda områdena är digitala färdigheter - för att stärka den digitala kompetensen inom undervisningen. Uppgiften innefattar också tillhandahållande av stöd för skolor i arbetet med de grundläggande värdena i skollagen och i skolornas kursplaner, t.ex. jämställdhet och ett normkritiskt perspektiv i skolorna, liksom förebyggande av mobbning och trakasserier.

De mänskliga rättigheterna, i form av grundläggande demokratiska värden, utgör grunden för det svenska skolsystemet. I enlighet med skollagen (2010:800) och de nationella läroplanerna bör alla som arbetar i skolor utan undantag främja respekt för varje enskild persons inneboende värde och den miljö som är gemensam för oss alla.

Kapitel 6 i skollagen (2010:800) innehåller också bestämmelser om aktiva åtgärder för att förebygga mobbning i skolorna och ålägger skolorna ansvaret för utredning av och lämpliga åtgärder mot förnedrande behandling. Detta kan inbegripa mobbning på nätet i anslutning till skolutbildningen.

Statens skolinspektion granskar skolorna. Barn- och elevombudet utgör en del av Skolinspektionen och övervakar den del av skollagen som rör förnedrande behandling.

8.3.2 Offentlig- privata partnerskap (PPP)

Sverige använder offentlig-privata partnerskap vid förebyggande och bekämpning av it-brottslighet. I kampen mot barnpornografi på internet t.ex. samarbetar polisen med ECPAT Sverige och med den finansiella sektorn och telekommunikationssektorn genom Finanskoalitionen i syfte att stoppa och spåra betalningar för sådant material. Polisen arbetar tillsammans med internetleverantörer inom ramen för en samarbetsöverenskommelse som syftar till frivillig blockering enligt vad som beskrivs ovan.

Sveriges polis, banker, betaltjänstleverantörer, bensinbolag och logistikföretag har i flera år idkat ett nära samarbete jfr avsnitt 6.3.1.).

När det gäller it-angrepp bör den nationella hanteringsplanen omnämnas (jfr. avsnitt 6.1.2). I det nationella programmet för fonden för inre säkerhet framhävs även ett förbättrat samarbete och en förbättrad samordning mellan alla aktörer när det gäller att skydda informations- och kommunikationsinfrastrukturen.

8.4 Slutsatser

- Sverige har ett utförligt utbildningsprogram för åklagare och poliser på området it-brottslighet, med obligatorisk grundläggande utbildning för vanliga åklagare och mer avancerade kurser för dem som arbetar på specialistavdelningar. Domarna förefaller dock inte att ha någon sådan utbildning eftersom det bara förekommer sessioner för enskilda specialändamål och korta "lösryckta" sessioner.

- Det sätt på vilket utbildningen för åklagare är organiserad - inklusive det specialiserade nätverket för åklagare - bör särskilt noteras som bästa praxis. Diskussionerna avslöjade att domare ofta inte har de nödvändiga färdigheterna för att döma denna typ av brott. Dessutom visade det sig att andra enheter inom polisen saknar kunskaper om it-brottslighet och elektronisk bevisning trots att it-brottslighet ingick i den grundläggande utbilningen. Dessutom kunde domares och åklagares kunskaper förbättras om man i större utsträckning anlitade it-experter i pågående mål rörande it-brott.

- Enligt utvärderarnas uppfattning behövs utbildning om it-brottslighet och elektronisk bevisning inom hela domstolsväsendet för att säkerställa den nödvändiga straffrättsliga kapaciteten för att samla in, analysera och använda elektronisk bevisning inte bara i fråga om brott med anknytning till datorer utan i fråga om alla brott. Eftersom elektronisk bevisning kan förekomma rörande vilket brott som helst behövs det utbildning för nästan alla brottsbekämpande tjänstemän, inte bara för några få.

- Sverige har en nationell plan för att öka medvetenheten och fokuserar särskilt på barn, redan från två års ålder. Programmet är välintegrerat och bygger på samarbete mellan ett stort antal statliga institutioner med involvering av byråer och privata aktörer.

- Ytterligare samarbete mellan Socialdepartementet, Kulturdepartementet och kommunerna inrättades för att förbättra arbetet i skolorna. Sverige har för närvarande inte något program som syftar till att öka äldre personers medvetenhet. På detta område förlitar sig Sverige på den privata sektorn och dess initiativ.

- När det gäller förebyggande har Sveriges kulturdepartement ett program som är inriktat på att öka barns medvetenhet, t.ex. med poddsändningar, med Facebook-projekt för att bekämpa och förebygga rasism och hatspråk. I detta syfte inrättades ett nära samarbete med internetleverantörer. Nära samarbete med de baltiska länderna inrättades också för att analysera och förebygga det inflytande som utövas av nättroll som försöker påverka den allmänna opinionen genom falsk information.

- I Sverige finns allmänt sett ett mycket långtgående samarbete mellan den offentliga och den privata sektorn i kampen mot och förebyggandet av it-brottslighet.

9 AVSLUTANDE ANMÄRKNINGAR OCH REKOMMENDATIONER

9.1 Förslag från Sverige

Sveriges åklagarmyndighet har framgångsrikt utrett och lagfört ett stort antal olika it-brott. Exempelvis har ett antal seriesexförbrytare lagförts och dömts. I många fall fanns det över 50 målsägande. I dag har åklagarmyndigheten flera experter på it-brottslighet med omfattande kunskaper och erfarenhet på området. Emellertid ökar it-brotten och frågorna med anknytning till detta område. Därför arbetar åklagarna på att förbättra utbildningen, sakkunskapen och erfarenheten hos ett stort antal åklagare för att ytterligare förstärka kapaciteten på detta område.

Sverige bedömer att polisen har låg till måttlig kapacitet. Det beror på bristen på resurser, kapacitet, prioriteringar och vissa frågor rörande den rättsliga ramen. Otillräckliga utredningsresurser i förhållande till det stora antalet fall nämndes också som ett av hindren för gränsöverskridande samarbete särskilt beträffande kortbedrägerier på nätet.

Dessutom är förbättrat externt samarbete för Sveriges it-brottscentrum mycket viktigt när det gäller att förebygga och utreda it-brott. Detta behöver förbättras och inte bara genomföras på lägre nivå (mellan enskilda tjänstemän).

Sverige anser dock att vissa av landets politiska riktlinjer är att betrakta som bästa praxis.
Särskilt specialiseringen för åklagare och poliser tillsammans med verksamt samarbete och utbyte av know-how mellan dem och mellan de berörda medlemsstaterna är nyckeln till en effektiv process.

För att bygga vidare på de framgångsfaktorer som brottsbekämpningen har att tillgå kan man inte starkt nog betona vikten av begreppet grupparbete. Sannolikheten för framgång ökar redan genom att man har en samordnad insats för underrättelsetjänstemän, utredare, åklagare, en insatsstyrka och experter på it-forensik.

Vad beträffar att förstärka förebyggandet och bekämpningen av it-brottslighet är samarbete det viktigaste och mest verksamma verktyget för de brottsbekämpande organen, särskilt för polisen, när det gäller att verkligen bekämpa it-brottsligheten. Först och främst handlar det om att mer aktivt medverka i arbetet inom det internationella samfundet.

Sverige anser att landet bör ansluta sig till J-CAT och härigenom och via andra kanaler verkligen kunna påverka och lära av EU:s bekämpning av it-brott. Detta skulle också bidra till och förenkla utrednings- och underrättelseverksamhet i Sverige. Andra relevanta forum, såsom NCFTA i USA där polistjänstemän från flera länder (även i Europa) arbetar tillsammans med och i samma byggnad som företag inom den privata sektorn och andra organ är också viktiga.

Det nationella it-brottscentrumet förväntas vara främst i ledet vad beträffar samarbetet i kampen mot it-brottslighet samt inleda och stå värd för olika aktiviteter som relevanta partner kan delta i. Det bör finnas ett strukturerat sätt att arbeta med privata enheter och andra former av samarbete. Det nationella it-brottscentrumet bör också vara öppet för medverkan av privatföretag och andra organ när gemensamma fall pågår.

9.2 Rekommendationer

Vad beträffar det praktiska genomförandet och förverkligande av rambeslutet och direktivet kunde den expertgrupp som medverkade i utvärderingen av Sverige på ett tillfredsställande sätt granska systemet i Sverige.

Sverige bör följa upp rekommendationerna i denna rapport inom 18 månader efter utvärderingen och rapportera om framstegen till arbetsgruppen för allmänna frågor, inklusive utvärdering.

Utvärderingsgruppen ansåg det lämpligt att göra ett antal förslag riktade till de svenska myndigheterna. Därtill framförs även på grundval av olika former av bästa praxis rekommendationer till EU, dess institutioner och organ, särskilt Europol.

9.2.1 Rekommendationer till Sverige

1. Sverige bör slutföra och anta sin nationella strategi för it-säkerhet och ta med den i ett kapitel om it-brottslighet. (Jfr 3.1 och 3.5.)

2. Sverige bör på strategisk nivå säkerställa en konsekvent politik och adekvata åtgärder mot it-brottslighet, såsom genomföra ett online-rapporteringssystem för it-brottslighet, förbättra den institutionella strukturen (t.ex. genom att förstärka enheten mot högtekniska brott och andra specialiserade enheter på lokal nivå), tillhandahålla brottsbekämpningsutbildning samt utbildning för domare och åklagare rörande it-brottslighet och elektronisk bevisning, främja det offentlig-privata samarbetet, vidta åtgärder för att skydda barn på nätet, särskilt mot sexuell exploatering på nätet, genomföra finansiella utredningar samt ha goda ramar och mekanismer för effektivt internationellt samarbete vid utredningar av it-brott. (Jfr 3.2, 3.5 och 6.4.)

3. Sverige bör förbättra insamlingen av statistik om it-brott och göra den mer detaljerad, standardiserad och övergripande samt förbättra hanteringen av statistiska data, både på utrednings- och lagföringsnivå å ena sidan och beträffande fällande domar för it-brott å den andra. Sådana data skulle ge en fullständig bild för strategiska ändamål, t.ex. nationell strategi och utbildningsstrategi. De statistiska uppgifter som samlas in bör omfatta data rörande åtminstone vart och ett av de brott som begärs kriminaliserade enligt direktiv 2013/40/EU. (Jfr 3.3, 3.5 och 5.1.2.)[14]

4. Sverige bör överväga att förstärka den svenska polisens kapacitet och förmåga, t.ex. Den övergripande strukturen, riktlinjer, resurser och kompetens på området it-brottslighet och it-relaterade brott, med tillräckliga mänskliga resurser för att hantera det stora antalet fall. (Jfr 4.3 och 4.5.)

5. Sverige bör på central nivå förstärka samordningen mellan de olika aktörer som medverkar i kampen mot och förebyggandet av it-brottslighet. (Jfr 4.4 och 4.5.)

6. Sverige bör så snart som möjligt ratificera konventionen om it-brottslighet och särskilt genomföra artiklarna 16 och 29 (skyndsamt bevarande) samt artiklarna 17 och 30 om skyndsamt bevarande respektive delvis utlämnande. (Jfr 5.1 och 5.5.)

7. Sverige bör säkerställa att processrätten är anpassad till modern teknik, bl.a. vad beträffar tillgång till bevisning som finns lagrad i molnet och skyndsamt erhållande av information om abonnenter. (Jfr 5.2.1, 5.2.3, 5.4.3 och 5.5.)

8. Sverige bör överväga att spela en mer aktiv roll inom det internationella samfundets arbete, både för att lära av och utbyta erfarenheter med andra länder och för att förbättra kapaciteten för gränsöverskridande utredningar och samarbete. (Jfr 7.6 och 9.1.)

[14] Efter besöket underrättades utvärderingsgruppen om att Brottsförebyggande rådet håller på att analysera lösningen på behovet att samla in fullständiga och heltäckande statistiska uppgifter om it-relaterad brottslighet. Brå har föreslagit att det rikstäckande uppföljningssystemet ska inrättas för it-forensisk verksamhet inom polisen.

9. Sverige bör tillhandahålla utbildning om utredning av bedrägeri och elektronisk bevisning genom att ge det straffrättsliga systemet den nödvändiga kapaciteten för att samla in, analysera och använda elektronisk bevisning, inte bara i fråga om brott med anknytning till datorer utan i fråga om alla brott. (Jfr 8.1 och 8.4.)

10. Sverige bör också inrätta ett övergripande och strukturellt utbildningssystem för domare och åklagare och utvidga utbildningsmöjligheterna för polistjänstemän. Man bör också överväga att göra det möjligt att i större utsträckning anlita it-experter för att förbättra domarkårens kunskaper när det gäller it-relaterade mål. (Jfr 8.1 och 8.4.)

9.2.2 Rekommendationer till Europeiska unionen och dess institutioner samt till andra medlemsstater

1. Medlemsstaterna bör överväga att inrätta ett övergripande och strukturellt utbildningssystem rörande it-brottslighet för åklagare, av samma typ som det svenska systemet för utbildning av åklagare och den webbaserade handledningen för åklagare. (Jfr 4.1.2 och 4.5.)

2. Medlemsstaterna rekommenderas att utveckla eller förstärka det faktiska samarbetet mellan polisen och åklagarna i kampen mot it-brottslighet, i linje med vad som är fallet i Sverige. (Jfr 4.1.2 och 4.5.)

3. Medlemsstaterna rekommenderas att använda offentlig-privata partnerskap för att bekämpa övergrepp mot barn och barnpornografi på nätet genom att utveckla verktyg för att blockera olagligt innehåll på nätet, såsom är fallet i Sverige. (Jfr 6.2.4 och 6.4.)

4. Medlemsstaterna rekommenderas att stärka kommunikationsprocessens effektivitet med andra medlemsstater och tredjeländer genom att inrätta ett registreringssystem för ömsesidig rättslig hjälp och ett hanteringssystem för ömsesidig rättslig hjälp som gör det möjligt att följa fall från registrering till dess att svaret skickas till det ansökande landet, som hos Åklagarmyndigheten i Sverige. (Jfr 7.5.1 och 7.6.)

5. Medlemsstaterna rekommenderas att intensifiera samarbete med grannländerna för att förstärka sin politik för bekämpning av it-brottslighet, i enlighet med modellen för Sveriges samarbete med de övriga nordiska länderna samt med Lettland, Litauen och Estland. (Jfr 7.5.3 och 7.6.)

6. Medlemsstaterna rekommenderas att utveckla kampanjer i syfte att öka medvetenheten hos föräldrar och barn vad beträffar tryggt användande av internet, som Statens medieråd i Sverige har gjort. (Jfr 8.2 och 8.4.)

7. EU-institutionerna bör snarast möjligt ta itu med frågan om datalagring. (Jfr 5.5.)

8. EU bör överväga en gemensam europeisk strategi för gränsöverskridande tillgång till elektronisk bevisning, inklusive överenskommelser med stora privata företag om att underlätta samarbetet i straffrättsliga frågor (t.ex. Facebook och Google). (Jfr 7.5.1 och 7.6.)

9.2.3 Rekommendationer till Eurojust/Europol/Enisa

1. Europol, Eurojust och Enisa bör i relevanta fall säkerställa och öka medvetenheten om deras kapacitet att stödja utredningar av it-brott på nationell nivå och i synnerhet i anslutning till det gränsöverskridande samarbetet. (Jfr 7.1.1 och 7.1.2.)

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

Tuesday 27 September

09:30-12:00	Ministry of Justice
Location:	*Government Offices, Jakobsgatan 24, Kajutan, floor 7*
12:30-13:30	Lunch at the Government Offices
Location:	*Government Offices, Rosenbad*
13:45-16:30	The Swedish Prosecution Authority and the Swedish Economic Crime Authority
Location:	*Government Offices, Jakobsgatan 24, Cittran, ground floor*
18:30	Dinner at Brasserie Godot
Location:	*Grev Turegatan 36*

Wednesday 28 September

10:00-16:00	Swedish Police Authority
Location:	*Polhemsgatan 30*
12:00-13:00	Lunch at the Swedish Police

Thursday 29 September

10.00-12:00 Swedish Civil Contingencies Agency

Location: *Fleminggatan 14*

12:00-13:00 Lunch at the Swedish Civil Contingencies Agency

Friday 30 September

10.00-12:15 Round-up and further questions

Location: *Government Offices, Jakobsgatan 24, Kajutan, floor 7*

Including participation in part by Secretary-General of ECPAT Sweden, Mr Anders Pettersson

12:30- Lunch at the Government Offices

Location: *Government Offices, Rosenbad*

ANNEX B: PERSONS INTERVIEWED/MET

Meetings 27 September 2016

Venue: The Ministry of Justice

Person interviewed/met	Organisation represented
Mr Nils Hänninger	Director, Ministry of Justice
Mr Henrik Sjölinder	Deputy Director, Ministry of Justice
Mr Mikael Kullberg	Deputy Director, Ministry of Justice
Mr Jonas Brunberg	Legal Adviser, Ministry of Justice
Mr Emil Karlsson	Legal Adviser, Ministry of Justice
Ms Jenny Engvall	Legal Adviser, Ministry of Justice
Ms Homa Abdolrasouli	Administrator, Ministry of Culture
Ms Julia Berglund	Administrator, the Swedish Police Authority

Venue: The Swedish Prosecution Authority

Person interviewed/met	Organisation represented
Mr Jan Tibbling	Vice Chief Prosecutor, Economic Crimes Authority
Mr Christer Dahlström	Prosecutor, Economic Crimes Authority
Mr Per Hedvall	Head of Bureau, The Prosecution Authority
Mr Niklas Lagrell	Head of Training, The Prosecution Authority
Mr Henrik Olin	Vice Chief Prosecutor
Ms Ingmarie Olsson	Specialist Prosecutor
Ms Cathrine Rudström	Specialist Prosecutor

Meetings 28 September 2016

Venue: The Swedish Police Authority

Person interviewed/met	Organisation represented
Mr Richard Ahlgren	Head, Cyber Crime Intelligence Unit
Mr Tommy Nordström	Head, High-Tech Unit
Mr Lena Larsson	Head, Cyber Crime Investigation Unit
Mr Per-Åke Wecksell	Desk officer Child Sex Exploitation online
Ms Bo Norgren	Desk officer, Desk Unit
Mr Jörgen Härberg	Head, Desk Unit
Ms Julia Berglund	Administrator

Meetings 29 September 2016

Venue: Swedish Civil Contingencies Agency

Person interviewed/met	Organisation represented
Ms Linda Ericson	Head of Strategic Support and Analysis Section
Ms Anne-Marie Alverås	Head of Section (cert.se).
Mr Christoffer Karsberg	Head of Section

Meetings 30 September 2016

Venue: The Ministry of Justice

Person interviewed/met	Organisation represented
Mr Henrik Sjölinder	Deputy Director, Ministry of Justice
Mr Anders Pettersson	Secretary General of ECPAT Sweden
Mr Mikael Kullberg	Deputy Director, Ministry of Justice
Mr Jonas Brunberg	Legal Adviser, Ministry of Justice
Mr Emil Karlsson	Legal Adviser, Ministry of Justice

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	SWEDISH OR ACRONYM IN ORIGINAL LANGUAGE	SWEDISH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
Brå	*Brå*		The Swedish National Council for Crime Prevention
ECPAT	*ECPAT*		End Child Prostitution in Asian Tourism
IOC's	*IOC's*		Indicators of Compromise
MSB	*MSB*		The Civil Contingencies Agency of Sweden
NAE	*SV*		The National Agency for Education
NFC	*NBC*		The National Fraud Centre
SC3	*SC3*		The Swedish Cybercrime Centre
SPA	*ÅM*		The Swedish Prosecution Authority