EN GRANSKNINGSRAPPORT FRÅN RIKSREVISIONEN

It-relaterad brottslighet

– polis och åklagare kan bli effektivare

RIR 2015:21

RIKSREVISIONEN

Riksrevisionen är en myndighet under riksdagen med uppgift att granska den verksamhet som bedrivs av staten. Vårt uppdrag är att genom oberoende revision skapa demokratisk insyn, medverka till god resursanvändning och effektiv förvaltning i staten.

Riksrevisionen bedriver både årlig revision och effektivitetsrevision. Denna rapport har tagits fram inom effektivitetsrevisionen, vars uppgift är att granska hur effektiv den statliga verksamheten är. Effektivitetsgranskningar rapporteras sedan 1 januari 2011 direkt till riksdagen.

RIKSREVISIONEN

ISBN 978-91-7086-390-5
RIR 2015:21
FOTO: PLATTFORM/JOHNÉR
FORM: ÅKESSON & CURRY
TRYCK: RIKSDAGENS INTERNTRYCKERI, STOCKHOLM 2015

EN GRANSKNINGSRAPPORT FRÅN RIKSREVISIONEN

RiR 2015:21

It-relaterad brottslighet

– polis och åklagare kan bli effektivare

RIKSREVISIONEN

TILL RIKSDAGEN

DATUM: 2015-12-04
DNR: 31-2014-0837
RIR 2015:21

Härmed överlämnas enligt 9 § lagen (2002:1022) om revision av statlig verksamhet m.m följande granskningsrapport över effektivitetsrevision:

It-relaterad brottslighet – polis och åklagare kan bli effektivare

Riksrevisionen har granskat om Polismyndigheten och Åklagarmyndigheten har beredskap för att ändamålsenligt och effektivt handlägga och utreda it-relaterade brott. Resultatet av granskningen redovisas i denna granskningsrapport.

Företrädare för Polismyndigheten, Åklagarmyndigheten och Regeringskansliet (Justitidepartementet) har fått tillfälle att faktagranska och i övrigt lämna synpunkter på utkast till slutrapport.

Rapporten innehåller slutsatser och rekommendationer som avser Polismyndigheten och Åklagarmyndigheten samt regeringen.

Riksrevisor *Margareta Åberg* har beslutat i detta ärende. Revisionsledare *Tina Malmberg* har varit föredragande. Revisor *Helena Fröberg*, revisor *Tove Lindström* och revisionsdirektör *Anna Hansson* har medverkat vid den slutliga handläggningen.

Margareta Åberg Tina Malmberg

För kännedom:

Regeringen, Polismyndigheten och Åklagarmyndigheten.

Innehåll

forts.

Elektroniska bilagor

Till rapporten finns två ytterligare bilagor att ladda ned från Riksrevisionens webbplats www.riksrevisionen.se. Dessa kan också begäras ut från ärendets akt genom registraturen.

Sammanfattning och rekommendationer

Riksrevisionen har granskat om Polismyndigheten och Åklagarmyndigheten har beredskap för att ändamålsenligt och effektivt handlägga och utreda it-relaterade brott.

Granskningens bakgrund

It-relaterad brottslighet är ett växande problem. För all brottslighet har de personuppklarade brotten under perioden 2006–2014 sjunkit från 18 till 15 procent, vilken är den lägsta nivån hittills. Personuppklaringen för de granskade it-relaterade brotten ligger konstant lägre och var 7 procent år 2014. Det är viktigt att Polismyndigheten och andra delar av rättsväsendet förmår hålla jämna steg med utvecklingen på området för att det brottsutredande arbetet inte ska försämras. När människor drabbas av brott och ärendena skrivs av i stället för att utredas, finns det en risk att förtroendet för rättsväsendet påverkas negativt.

Granskningen omfattar tre brottskategorier; it-bedrägerier, internetrelaterade barnpornografibrott och attacker mot infrastruktur. Riksrevisionen gör bedömningen att dessa tre brottskategorier kan illustrera handläggning och utredning av it-relaterad brottslighet i stort. Huvudsakligt fokus i granskningen är processen från anmälan av brott till beslut om huruvida åtal ska väckas. Granskningen avser regeringen, Polismyndigheten och Åklagarmyndigheten.

Granskningens resultat

Sammantaget visar granskningen att bristen på vedertagna metodstöd, utvecklade arbetssätt, tillräcklig kompetens och specialisering inom området gör att polis och åklagare inte har beredskap och förmåga att utreda och handlägga it-relaterade brott på ett effektivt och ändamålsenligt sätt. De identifierade bristerna riskerar också att leda till att it-relaterade brott inte hanteras likvärdigt och enhetligt, och att det i högre grad blir personberoende hur ett ärende utreds. Samtidigt visar granskningen att det finns möjligheter till förbättrad personuppklaring med ett förändrat arbetssätt.

It-relaterad brottslighet kräver förändrade arbetssätt

Antalet anmälningar av it-relaterade brott ökar kraftigt samtidigt som personuppklaringen sjunker och många ärenden skrivs av utan utredning. It-relaterade brott är många gånger komplexa att utreda, digital bevisning är ofta svår att inhämta och internet gör det möjligt att begå brott anonymt. Polis och åklagare står därmed inför stora utmaningar för att kunna möta brottsutvecklingen.

Polisen och Åklagarmyndigheten har uppmärksammat den it-relaterade brottsligheten sent, först 2013 började området att lyftas fram mer i interna styrdokument och strategier. Den it-relaterade brottsligheten har därmed inte uppmärksammats i större utsträckning på ledningsnivå. Riksrevisionen ser positivt på att myndigheterna nu har börjat vidta flera åtgärder för att höja sin förmåga på området, men menar att det kommer att krävas ett långsiktigt och uthålligt arbete för att nå resultat.

Myndigheterna saknar nationella riktlinjer och metodstöd

Granskningen visar att det inom Polismyndigheten saknas metodstöd, vedertagna nationella riktlinjer och handböcker för utredning av it-relaterade brott. It-aspekten är till exempel inte en del av Polisens nationella utredningskoncept. De handböcker inom Åklagarmyndigheten som berör området är okända i många åklagarområden.

Kompetensen är låg inom myndigheterna

Utbildningsnivån för att utreda it-relaterad brottslighet är generellt sett låg inom Polismyndigheten och Åklagarmyndigheten. Endast ett fåtal förundersökningsledare, utredare, it-utredare, it-forensiker och åklagare har gått utbildningar på it-området. Dessutom innehåller grundutbildningen till polis som regel inte någon del som handlar om it-relaterad brottslighet. En del poliser är självlärda inom it-utredningar och har goda kunskaper på området. Utan ett större inslag av formell utbildning kommer enskilda poliser inte att ha den kompetens som krävs för att göra ett bra utredningsarbete och möjligheterna till enhetliga arbetsmetoder försvåras. Riksrevisionens enkät visar också att de utbildningar som finns inom Polismyndigheten och Åklagarmyndigheten inom it-området inte är tillräckliga. Det efterfrågas både mer om it-aspekten i grundutbildningen och fler vidareutbildningar, till exempel inom internetinhämtning. Tidsbrist, kostnader och ett begränsat antal utbildningsplatser utgör hinder för att gå de utbildningar som finns.

Specialiserade enheter kan vara en framgångsfaktor

Granskningen visar att 92 procent av de personuppklarade förundersökningarna utreddes vid en specialiserad enhet, jämfört med 30 procent för de nedlagda förundersökningarna. Till exempel har bedrägeriärenden ofta utretts vid bedrägerienheter. Riksrevisionen menar att detta tyder på att specialiseringar i den utredande verksamheten kan förbättra förutsättningarna för att klara upp brott.

Samverkan och internationellt utbyte måste öka

Många ärenden som Riksrevisionen har granskat skrevs av för att brottet hade begåtts utomlands. Inte i något ärende som ingick i aktgranskningen hade internationell rättslig hjälp dock begärts. Det verkar därmed finnas ett utrymme för att bättre utnyttja internationell hjälp i det brottsutredande arbetet, även om den internationella rättsliga hjälpen enligt företrädare för myndigheterna är tidskrävande och administrativt

komplicerad. Det finns också indikationer på att den svenska desken vid Europol i Haag skulle kunna användas i större utsträckning.

Polismyndigheten behöver ofta information från utländska företag för att kunna utreda it-relaterade brott. Delar av Polismyndighetens samarbete med utländska företag har underlättats av att myndigheten har utvecklat en samsyn för samarbete med vissa utländska företag som levererar internetbaserade tjänster, från vilka det ofta behövs information.

Riksrevisionens enkät visar att polisregionerna har olika uppfattning om hur samarbete och samverkan mellan regionerna fungerar. Företrädare för Polismyndigheten menar att det kan vara svårt att nå ut i polisorganisationen eftersom kontakter ofta bygger på personliga nätverk. Riksrevisionen menar att detta tyder på att det finns ett behov av tydligare strukturer för samarbete och samverkan inom Polismyndigheten. För att förbättra möjligheterna till utbyte av erfarenheter mellan it-kunniga åklagare har strukturerna för detta inom Åklagarmyndigheten nyligen förtydligats.

Många it-relaterade brott är svåra att utreda

Att många ärenden skrivs av beror ofta på att brott har begåtts utomlands, att spaningsuppslag saknas eller att brottet har varit för ringa för att vissa utredningsåtgärder, såsom hemliga tvångsmedel, skulle kunna vidtas. Gärningstypen har även en avgörande betydelse för om ett brott utreds. Några typer av dataintrång och bedrägerier som sker via internet utreds i stort sett inte alls. Dessa ärenden är en del av en brottslighet där möjligheten att nå framgång i ett enskilt ärende i det närmaste är obefintlig i dag. Riksrevisionen kan konstatera att det finns brottstyper där polis och åklagare med gällande lagstiftning och arbetssätt i stort sett saknar förutsättningar att vidta utredningsåtgärder.

Polis och åklagare kan arbeta effektivare och mer enhetligt

Riksrevisionen kan konstatera att många it-relaterade brott generellt är svårutredda. Samtidigt visar granskningen att det finns möjligheter till förbättringar i personuppklaringen med ett förändrat arbetssätt. Riksrevisionen noterar till exempel att polis och åklagare har lyckats vända trenden för internetrelaterat barnpornografibrott, där personuppklaringen har förbättrats kontinuerligt sedan 2006. Troliga bidragande faktorer till den ökande uppklaringen är ändrade förutsättningar i lagstiftningen, att Polishögskolan började ge en specialiserad utbildning på området 2006 och att denna brottstyp särskilt prioriterades av polisledningen under 2014.

Polis och åklagare måste komma igång snabbare med de inledande utredningsåtgärderna för att säkerställa att digitala bevis inte hinner försvinna. En förutsättning för att utredningsarbetet inte ska fördröjas eller försvåras är att anmälningarna innehåller all relevant information. Aktgranskningen visar att IP-adressen antecknades fel i cirka 20 procent av anmälningarna som innehöll en IP-adress. Detta får till följd att uppgiften inte

går att använda. Riksrevisionens aktgranskning visar också att utredningsåtgärder vidtogs snabbare i de personuppklarade förundersökningarna än i de nedlagda.

Polis och åklagare vidtar få it-relaterade åtgärder i förundersökningarna. I stället är det traditionella utredningsåtgärder som är vanligast, till exempel att spåra bankkonton. Det är inte alltid nödvändigt, eller ens möjligt, att vidta it-relaterade åtgärder i varje enskilt ärende för att klara upp ett brott. Riksrevisionens aktgranskning visar dock att det finns ett utrymme för att vidta fler it-relaterade utredningsåtgärder. Sådana åtgärder kan också bidra med information som kan vara värdefull för att nå framgång i Polisens underrättelsearbete. Till exempel skulle Polismyndigheten kunna samla IP-adresser på ett ställe för att ha möjlighet att arbeta mer systematiskt med seriebrottslighet och också förbättra förutsättningarna för att klara upp brott. Det kan även finnas skäl att involvera fler olika aktörer i förundersökningarna; till exempel har it-forensiker och företag varit delaktiga i större utsträckning i de personuppklarade förundersökningarna än i de nedlagda.

Riksrevisionens rekommendationer

Rekommendationer till Polismyndigheten

- Identifiera nationella utvecklingsbehov och utveckla den strategiska kompetensförsörjningen för att kunna säkerställa verksamhetens behov. Planera, uppmuntra och skapa utrymme för kompetenshöjande åtgärder inom it-området.
- Säkerställ att grundutbildningen till polis motsvarar verksamhetens behov med hänsyn till den tekniska utvecklingen och dess påverkan på brottsligheten.
- Utveckla och förankra nationella arbetssätt och metodstöd för utredning av it-relaterade brott.
- Se över strukturen för brottssamordning och samverkan mellan polisregionerna.
- Utnyttja de fora som finns för internationell samordning och samverkan.

Rekommendationer till Åklagarmyndigheten

- Identifiera nationella utvecklingsbehov och utveckla den strategiska kompetensförsörjningen för att kunna säkerställa verksamhetens behov. Planera, uppmuntra och skapa utrymme för kompetenshöjande åtgärder inom it-området.
- Utveckla och förankra metodstödet inom it-området och möjligheterna till erfarenhetsutbyte mellan åklagarområdena.

1 Inledning

1.1 Motiv till granskning

It-relaterad brottslighet ökar kraftigt och precis som för all brottslighet kan den leda till stort lidande för brottsoffren, både psykiskt, fysiskt och ekonomiskt. För all brottslighet har de personuppklarade[1] brotten under perioden 2006–2014 sjunkit från 18 till 15 procent, vilken är den lägsta nivån hittills. Personuppklaringen för de granskade it-relaterade brotten ligger konstant lägre och var 7 procent år 2014. Rikspolisstyrelsen har i en tillsynsrapport och en förstudie gjort bedömningen att det finns flera brister i handläggning och utredning av it-relaterade brott.[2] Om Polismyndigheten och Åklagarmyndigheten inte klarar av att utreda denna typ av brottslighet i tillräcklig utsträckning kan det leda till ett minskat förtroende för rättsväsendet och att brottsoffer avstår från att anmäla brott. En konsekvens av en sådan utveckling är att Polismyndigheten får en sämre överblick över brottsutvecklingen och de kriminella nätverken. I ett längre perspektiv kan den it-relaterade brottsligheten också leda till att människor får lägre tillit till att utföra till exempel transaktioner över internet och ändrar sitt beteende, vilket riskerar att påverka den ekonomiska utvecklingen i stort negativt.[3]

1.2 Syfte och revisionsfrågor

Syftet med granskningen är att undersöka om Polismyndigheten och Åklagarmyndigheten har beredskap för att ändamålsenligt och effektivt handlägga och utreda it-relaterade brott. Centralt i granskningen är att analysera vilka förutsättningar polis och åklagare har för att kunna klara upp denna typ av brottslighet, vilka åtgärder man har vidtagit samt vilka hinder och utmaningar som kvarstår. Granskningens revisionsfrågor är:

---

1 Personuppklarade brott är de brott för vilka beslutats om åtal, utfärdats strafföreläggande eller meddelats åtalsunderlåtelse (se även 1.6.5).

2 Rikspolisstyrelsen (2014), *Inspektion av polismyndigheternas förmåga att handlägga IT-brott,* tillsynsrapport 2014:2; Rikspolisstyrelsen (2013), *Förstudierapport, Polisens brottsbekämpande verksamhet, brott med internet-relevans,* dnr PoA480-5583/11, s. 4, 7–8. Förstudiens syfte är att peka på problem och brister samt att föreslå åtgärder för att förbättra Polisens förmåga att hantera detta problemområde.

3 Anderson m.fl. (2012), *Measuring the cost of cybercrime*, s. 5–10, 24.

- Hur arbetar Polismyndigheten och Åklagarmyndigheten med it-relaterade brott?
- Finns det en effektiv och ändamålsenlig organisering för att kunna handlägga och utreda it-relaterade brott?
- Har Polismyndigheten och Åklagarmyndigheten säkerställt kompetensförsörjningen för att kunna utreda och hantera it-relaterad brottslighet?
- Finns det en strukturerad samverkan inom området?

1.3 Avgränsningar

Granskningen omfattar tre brottskategorier:

- it-bedrägerier
- internetrelaterade barnpornografibrott
- brott som innebär attacker mot infrastruktur.

Riksrevisionen gör bedömningen att dessa tre brottskategorier kan illustrera handläggning och utredning av it-relaterad brottslighet i stort. Brottskategorierna har även till stor del lyfts fram i arbetet vid EU-centret European Cybercrime Centre (EC3).[4]

Av praktiska skäl bryts de tre brottskategorierna ned i fem brottstyper, så som de är indelade i den officiella kriminalstatistiken:[5]

- datorbedrägerier (it-bedrägerier)
- bedrägerier med hjälp av internet (it-bedrägerier)
- internetrelaterade barnpornografibrott
- dataintrång (attacker mot infrastruktur)
- datasabotage (attacker mot infrastruktur).[6]

Statistiken för de fem brottstyperna avser perioden 2006–2014.

Huvudsakligt fokus i granskningen är processen från anmälan av brott till beslut om huruvida åtal ska väckas. Granskningen omfattar regeringen, Polismyndigheten och Åklagarmyndigheten.

---

4 Se bilaga 1 för mer information om European Cybercrime Center vid Europol (EC3).

5 Det är dessa fem brottstyper som kodas som it-relaterade i den officiella statistiken. Informationsteknik används även i andra typer av brott men detta kodas inte särskilt i statistiken. Även brottstyperna brott mot upphovsrätten genom fildelning och brott mot det industriella rättsskyddet med hjälp av internet kodas särskilt i den officiella kriminalstatistiken sedan 2010. Eftersom Riksrevisionen granskar en längre period och dessa brott omfattar få anmälningar har dessa inte ingått i Riksrevisionens urval (2013 registrerades totalt 42 anmälningar inom dessa brottstyper).

6 Datorbedrägerier och bedrägerier med hjälp av internet: 9 kap. 1–3 §§ brottsbalken (1962:700). Dataintrång och datasabotage: 4 kap. 9 c § brottsbalken (1962:700). Internetrelaterat barnpornografibrott: 16 kap. 10 a § brottsbalken (1962:700).

1.4 Genomförande

Nedan följer en kort beskrivning av granskningens huvudsakliga metoder. För en mer detaljerad redogörelse, se bilaga 2.

Riksrevisionen har haft avstämningar med en *extern referensgrupp* bestående av poliser och åklagare med särskild kompetens inom it-relaterad brottslighet. I början av granskningen har problemindikationer stämts av med referensgruppen, som även har bistått Riksrevisionen med information om vilka arbetsmoment som omfattas av förundersökningsarbetet. Referensgruppen har även lämnat synpunkter på de iakttagelser som Riksrevisionen gjorde efter genomförd aktgranskning.

Riksrevisionen har *granskat akter* gällande it-relaterade ärenden som avslutades under 2013. Granskningen avsåg totalt 350 beslut (ett ärende kan innehålla flera beslut) inom de tre brottskategorierna. Granskningen omfattar dels 175 beslut som har lett till att åtal har väckts, åtalsunderlåtelse[7] meddelats, eller strafföreläggande[8] utfärdats, och dels 175 beslut som har lett till att ärendet har skrivits av (se vidare 1.6.4). Urvalsmetoden innebär att resultatet är generaliserbart för it-relaterade brott som helhet, men inte för respektive brottskategori, undantaget it-bedrägerier där urvalet är tillräckligt stort. Vidare har en person med åklagarkompetens granskat de polisledda avskrivna ärendena och en överåklagare vid Åklagarmyndigheten de åklagarledda avskrivna ärendena. Syftet var att bedöma om mer hade kunnat göras i ärendena för att nå lagföring[9] och om avskrivningsgrunderna använts enhetligt och ändamålsenligt.

En *enkät* har även genomförts avseende kompetens, arbetssätt och organisering som samtliga polisregioner och åklagarområden har besvarat.

Vidare har Riksrevisionen gått igenom *statistik* från Brå och Polismyndigheten, genomfört *dokumentstudier* och *intervjuer* med företrädare för de granskade myndigheterna (främst operativ personal i form av förundersökningsledare, utredare och it-forenisker, men även personal på strategisk nivå) samt besökt European Cybercrime Center (EC3) i Haag.

---

7 20 kap. 7 § rättegångsbalken (1942:740). Åtalsunderlåtelse innebär en möjlighet att under vissa i lagen särskilt angivna förutsättningar inte väcka åtal. Något väsentligt allmänt eller enskilt intresse får inte åsidosättas.

8 48 kap. rättegångsbalken (1942:740). Fråga om ansvar för brott kan tas upp av åklagare genom strafföreläggande. Ett strafföreläggande har samma verkan som en dom. Eftersom åklagaren inte väcker åtal prövas inte ansvarsfrågan i domstol.

9 Enligt Åklagarmyndigheten betyder lagföring att en person har ställts till svars för sin handling genom åtal, strafföreläggande och åtalsunderlåtelse. Detta innebär inte nödvändigtvis att personen har blivit dömd. I den officiella kriminalstatistiken som publiceras av Brottsförebyggande rådet innebär lagföring att personen har dömts i tingsrätt, godkänt strafföreläggande eller åtalsunderlåtelse. http://www.aklagare.se/Om-oss/Fragor-och-Svar1/Statistik/Vad-innebar-begreppet-lagforing-/. Riksrevisionen använder Åklagarmyndighetens definition i denna rapport.

1.5 Bedömningsgrunder

En övergripande utgångspunkt för granskningen är riksdagens och regeringens mål för kriminalpolitiken att minska brottsligheten och att öka människors trygghet.[10] Målen för utredning och lagföring är att verksamheten ska bedrivas med högt ställda krav på rättssäkerhet, kvalitet och effektivitet och att antalet brott som klaras upp ska öka.[11]

Förundersökningsarbetet

Förundersökningar ska enligt rättegångsbalken (1942:740) bedrivas så skyndsamt som möjligt.[12] En annan utgångspunkt för Polismyndighetens förundersökningsarbete är Polisens nationella utredningskoncept (PNU)[13] som identifierar följande fyra faktorer för en effektiv brottsutredning: adekvata inledande utredningsåtgärder, aktiva förundersökningsledare, effektiv brottssamordning och forensik (kriminalteknik).

Kompetensförsörjning

Både riksdagen och regeringen har uppmärksammat ett behov av att stärka rättsväsendets kompetens i arbetet mot brottslighet på internet eftersom en allt större del av brottsligheten är it-relaterad.[14]

Samverkan

Polismyndigheten och Åklagarmyndigheten har olika roller och ansvar, med krav på samverkan och att arbeta effektivt i rättskedjan.[15] I EU:s strategi för cybersäkerhet framhålls också att de nationella myndigheterna bör främja samverkan med andra medlemsstaters myndigheter, privata företag och EU-organ för att förbättra möjligheterna att bekämpa it-relaterad brottslighet.[16] Strategin är inte ett bindande dokument men visar ändå på vad medlemsstaterna bör göra.

---

10 Prop. 2014/15:1, utgiftsområde 4, s. 15; prop. 2015/16:1, utgiftsområde 4, s. 13.

11 Prop. 2014/15:1, utgiftsområde 4, s. 46; prop. 2015/16:1, utgiftsområde 4, s. 38.

12 23 kap. 2 och 4 § rättegångsbalken (1942:740).

13 Rikspolisstyrelsen (2004), dnr USE 400-0653/04.

14 Bet. 2014/15:JuU1; prop. 2014/15:1, utgiftsområde 4, s. 18.

15 Se bland annat 6 § polislagen (1984:387).

16 Europeiska kommissionen och Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik JOIN(2013) 1 slutlig.

1.6 Definitioner och preciseringar av centrala begrepp

1.6.1 It-relaterad brottslighet

Det finns ingen enhetlig och vedertagen definition av it-relaterad brottslighet. Ett synsätt är att dela in denna brottslighet i tre typer av brott:

- brott mot en it-enhet (*computer integrity crimes*, exempelvis dataintrång och överbelastningsattacker)
- brott där en it-enhet används (*computer-related crimes*, exempelvis försäljning av icke-existerande varor på internet och phishing)
- brott som består i att sprida digitalt material (*computer content crimes*, såsom barnpornografibrott eller spridning av våldspropaganda).[17]

Polismyndigheten har traditionellt använt termerna it-brott och it-relaterad brottslighet, och framhåller att det i svensk lagstiftning finns två definierade it-brott: dataintrång[18] och datorbedrägeri.[19] Båda brotten är inriktade på register och system för automatisk behandling och informationsteknik är ett rekvisit för att kunna begå brottet, som riktas mot en it-enhet. Den andra termen, it-relaterad brottslighet, används som ett samlingsbegrepp på brottslighet som begås med hjälp av informationsteknik. Själva begreppet it-relaterad brottslighet finns inte i lagstiftningen och de brottstyper som avses faller in under olika straffbestämmelser som är teknikneutrala, det vill säga de särskiljer inte om brottet sker med informationsteknik.[20] I andra sammanhang kan andra begrepp och termer användas, såsom it-kriminalitet och internetbrott, som i stort beskriver samma fenomen. Vissa menar att definitionsfrågan av it-brott och it-relaterad brottslighet har förlorat i betydelse i takt med samhällets teknikutveckling och användandet av informationsteknik i allt fler brottstyper.[21] I dag är i stort sett all brottslighet mer eller mindre it-relaterad.[22]

I denna rapport använder vi genomgående begreppet it-relaterad brottslighet. Betydelsen är då brottslighet där informationsteknik antingen är ett hjälpmedel, en brottsarena eller ett nödvändigt rekvisit för att begå brottet. Med denna definition omfattas Polismyndighetens båda termer it-brott och it-relaterad brottslighet. Däremot omfattas inte brott där gärningspersonen har lämnat digitala spår men inte använt informationsteknik för att begå brottet, exempelvis

---

17 Wall, David (2007/11),"Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (Revised Feb. 2011)", *Police Practice & Research: An International Journal*, 8(2): 183 205, s. 186 f.

18 4 kap. 9 c § brottsbalken (1962:700).

19 9 kap. 1 § andra stycket brottsbalken (1962:700).

20 Brå (2000), *IT-relaterad brottslighet*, rapport 2000:2, s. 12.

21 Kronqvist, Stefan (2013), *Brott och digitala bevis. En handledning*. Tredje upplagan, Norstedts Juridik, s. 22; Politiet, Politidirektoratet, Norge (2015), *Datakrimstrategien*, s. 31.

22 Intervju med Rikspolisstyrelsen 2014-11-17.

när gärningsmannen kan knytas till en brottsplats genom GPS. Som tidigare nämnts får tre brottskategorier illustrera den it-relaterade brottsligheten.

1.6.2 It-forensik

Med it-forensik menas undersökning av beslagtagna datorer, mobiler och liknande teknik, analys av videor och bildmaterial samt säkring av bevisning från internet. Detta utförs främst av så kallade it-forensiker eller Nationellt forensiskt center, och ibland av andra anställda inom Polismyndigheten, främst inom utredningsverksamheten.

1.6.3 Förundersökning

Brottmålsprocessen består i huvudsak av följande grundläggande delar:

1. utredning av brott (polis och åklagare)
2. åtalsprövning (åklagare)
3. lagföring (åklagare och domstol)
4. verkställighet av påföljd (exempelvis Kriminalvården).

Riksrevisionens granskning omfattar del 1 och 2.

Polis och åklagare svarar för förundersökningsfasen där brottet ska utredas och bevisning säkras. I Polismyndighetens uppgifter ingår bland annat att ta emot och upprätta anmälningar om brott och utreda brottsmisstankar. Åklagaren leder förundersökningar, beslutar om åtal, utfärdar strafföreläggande, meddelar åtalsunderlåtelser och för talan vid domstol.

Brottsutredningar bedrivs i form av förundersökningar.[23] En förundersökning ska inledas om det finns anledning att anta att ett brott som hör under allmänt åtal har begåtts. En förundersökning behöver däremot inte inledas om brottet uppenbart inte går att utreda, till exempel om spaningsuppslag saknas, eller om kostnaderna för utredningen inte står i rimligt förhållande till sakens betydelse och brottets straffvärde understiger fängelse i tre månader. Polis eller åklagare beslutar om att inleda en förundersökning. Förundersökningen leds normalt av en polis fram till dess att någon skäligen kan misstänkas för brottet. Då övertas förundersökningen av en åklagare. Vid brott av enkel beskaffenhet kan hela förundersökningen vara polisledd.[24] Förundersökningsledaren ansvarar för utredningen i dess helhet, och ska bland annat se till att den bedrivs effektivt samt ge direktiv för arbetet till övriga som är delaktiga i förundersökningen. Vid åklagarledda förundersökningar ska Polismyndigheten utifrån åklagarens

[23] De grundläggande bestämmelserna om förundersökning finns i 23 kap. rättegångsbalken (1942:740).

[24] 23 kap. 3 § första stycket rättegångsbalken (1942:740). Riktlinjer för vem som ska leda en förundersökning finns i Åklagarmyndighetens föreskrifter och allmänna råd (ÅFS 2005:9) om ledning av förundersökning i brottmål och Rikspolisstyrelsens föreskrifter och allmänna råd (RPSFS 2014:5) om ledning av förundersökning i brottmål.

direktiv vidta åtgärder, till exempel hålla förhör, genomföra husrannsakan, utföra spaning eller övervakning.

Under förundersökningen ska polis och åklagare utreda och besluta om det finns skäl för åtal och förbereda ärendet inför en eventuell domstolsprövning. Om det inte finns anledning till att förundersökningen fullföljs ska den läggas ned. Förundersökningsledaren beslutar om att lägga ned förundersökningen. Åtal ska alltid väckas om man på objektiva grunder kan motse en fällande dom.[25]

1.6.4 Avskrivna ärenden

Med avskrivna ärenden avses i denna granskning två typer av avskrivningar: dels brottsanmälningar som avslutats genom beslut om att inte inleda en förundersökning (direktavskrivning), dels ärenden som avslutats genom beslut att lägga ned förundersökningen. När någon av dessa två typer av avskrivningar redovisas separat i granskningen preciseras det genom att termerna direktavskrivning respektive nedlagd förundersökning används.

1.6.5 Begrepp ur den officiella kriminalstatistiken

Med *personuppklaring* menas att en person har bundits till brottet genom att åtal har väckts, att strafföreläggande har utfärdats eller att åtalsunderlåtelse har meddelats. *Personuppklaringsprocenten* redovisar personuppklarade brott under ett år i procent av antal anmälda brott under samma period.[26] I denna granskning beräknas personuppklaringsprocenten utifrån beslut, till skillnad från Brå:s beräkningar som utgår från brott (flera beslut kan kopplas till samma brott). Detta eftersom brottstypen datasabotage, som ingår i denna granskning, inte redovisas i den officiella kriminalstatistiken. Riksrevisionens beräkningar ligger dock mycket nära Brå:s beräkningar.

1.7 Disposition

I kapitel 2 presenteras utvecklingen av den it-relaterade brottsligheten, större förändringar inom rättsväsendet samt politikens inriktning. I kapitel 3 redovisas hur Polismyndigheten och Åklagarmyndigheten hanterar it-relaterade brott. I kapitel 4–6 redovisas olika förutsättningar som myndigheterna har för att handlägga och utreda it-relaterade brott.

---

[25] 20 kap. 6 § rättegångsbalken (1942:740); prop. 1984/85:3, s. 10. Se dock bestämmelserna om åtalsunderlåtelse i 20 kap. 7 § rättegångsbalken (1942:740).

[26] Brå har en ny definition sedan 2014, nämligen personuppklarade brott under ett år i procent av handlagda brott under samma period. Med handlagda brott menas brott där polis, åklagare eller annan utredande myndighet fattat ett beslut gällande brottet under redovisningsåret. Brå, Handlagda brott, http://www.bra.se/bra/brott-och-statistik/statistik/handlagda-brott.html (hämtad 2015-11-16).

2 Den it-relaterade brottsligheten

2.1 Brottsligheten förändras

Den snabba tekniska utvecklingen har öppnat upp för nya sätt, möjligheter och arenor för att begå brott, både för enskilda och för den organiserade brottsligheten.[27] Med hjälp av informationsteknik kan kriminella begå många brott samtidigt på distans med en relativt liten insats, till exempel genom att sprida sabotageprogram som angriper hundratusentals datorer samtidigt. Möjligheten att begå brott på distans och agera anonymt på internet med hjälp av olika anonymiseringstjänster gör att it-relaterade brott många gånger är mindre riskfyllda för förövarna än traditionell brottslighet.[28] Internet har även bidragit till att skapa en större och mindre riskfylld marknad för kriminella. Illegala varor och tjänster, såsom droger och vapen, assistans att begå mord och it-relaterade brott, bjuds numera ut på handelssidor på internets mörkare och hemliga delar, även kända som deep web och darknet.[29] Virtuella valutor eller kryptovalutor, till exempel bitcoin, är vanliga betalmedel på dessa marknader eftersom transaktioner som görs med dessa betalningsmedel inte går att ångra och är mycket svåra att spåra.[30]

Det ökande tekniska inslaget i brottsligheten har även lett till att de kriminella nätverken inte längre är lika fasta. Utvecklingen är att kriminella personer specialiserar sig på en viss del av ett brott och säljer denna tjänst vidare till andra kriminella. Detta fenomen, känt som ”Crime as a Service” (CaaS), eller brottstjänster, tillåter kriminella personer och nätverk att begå sofistikerade brott utan att de behöver ha någon djupare teknisk kunskap. Kontakterna mellan köpare och säljare av sådana tjänster knyts ofta på olika fora på internet, främst på darknet eller deep web.[31]

---

[27] Intervju med Rikspolisstyrelsen 2014-11-17; Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014*.

[28] Intervju med EC3, Europol 2015-06-02; Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014;* Polismyndigheten, Noa (2015), *Polisens rapport om organiserad brottslighet 2015*, dnr A185.830/2015.

[29] Deep web är de delar av internet som inte nås av vanliga sökmotorer. Darknet är ett krypterat nätverk inom deep web som avsiktligt hålls undangömt. En särskild programvara, till exempel TOR (The Onion Router) som är en slags anonymiseringstjänst, behövs för att navigera på darknet. Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014*.

[30] Polismyndigheten, Noa (2015), *Polisens rapport om organiserad brottslighet* 2015, dnr A185.830/2015, s. 53.

[31] Intervju med EC3, Europol 2015-06-02; Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014;* Polismyndigheten, Noa (2015), P*olisens rapport om organiserad brottslighet 2015,* dnr A185.830/2015 s. 52.

Den it-relaterade brottsligheten är internationell till sin karaktär. Kriminella personer och nätverk som medverkar till att begå samma brott är ofta stationerade i olika länder och kan med hjälp av informationsteknik begå brott i länder där de inte befinner sig fysiskt.[32] Sverige och övriga länder inom EU är attraktiva måltavlor för it-brottslingar på grund av sitt relativa välstånd, den utbredda användningen av informationsteknik och internet hos befolkningen samt de många tjänster som erbjuds över internet inom till exempel bank- och finanssektorn.[33]

EXEMPEL PÅ VANLIGA IT-RELATERADE BROTT OCH TILLVÄGAGÅNGSSÄTT FÖR ATT BEGÅ DESSA BROTT

Bedrägerier av olika slag med skiftande komplexitet, till exempel kortbedrägerier eller falska annonser på handelsplatser på internet. *Phishing* (nätfiske) går ut på att få offret att lämna ifrån sig exempelvis användarnamn, lösenord, uppgifter om bankkort som bedragaren kan utnyttja eller sälja vidare. *Skimning* är en form av kontokortsbedrägeri där någon kopierar innehållet i magnetremsan på ett kontokort. Informationen läggs över på ett annat kort, som bedragaren använder för att betala med men som belastar den ursprungliga ägarens konto.

Social manipulation är när ett offer manipuleras till att skicka känslig information eller pengar.

Id-kapningar är när en bedragare köper varor eller tar krediter i någon annans namn.

Hot, kränkningar och trakasserier (näthat) begås ofta via till exempel internetforum, social media, e-post och sms.

Internetrelaterat barnpornografibrott innebär innehav och/eller spridning av barnpornografiskt material. Det är även vanligt med så kallad livestreaming (direktsändning över internet) av sexuella övergrepp och våldtäkter mot barn.

Grooming är när en gärningsman tar kontakt med barn under 15 år i sexuellt syfte. Den första kontakten tas ofta via ett chattforum.

Dataintrång är till exempel när en angripare olovligen tar sig in i en it-enhet, till exempel för att få tag i känsliga uppgifter eller hemlig information. Dataintrång sker både mot privatpersoner, företag, myndigheter, banker, sjukhus och annan samhällsviktig infrastruktur.

Sabotageprogram *(malware)* är datorprogram som innehåller en skadlig kod som stör it-systemet eller samlar in information. Exempel på vanliga sabotageprogram är virus, trojaner och ransomware. Virus sprids via andra program, så kallade värdprogram, och körs enbart när värdprogrammet körs. *Trojaner* är fristående filer och sprids oftast via e-post eller fildelningsprogram. För att bli infekterad av en trojan måste den som fått filen själv köra programmet. Trojaner kan till exempel öppna en dator så att andra personer får tillgång till den utan användarens vetskap, eller registrera lösenord,

[32] Intervju med EC3, Europol 2015-06-02; Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014.*

[33] Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014,* s. 11, 67.

exempelvis till offrets bankkonto på internet. *Ransomware*, hindrar användaren av den infekterade datorn från att använda den utan att betala en lösensumma. Det finns även sabotageprogram som skapar *botnets*. Ett botnet sammanlänkar datorer som via en central nod får uppgifter, till exempel att sprida skräppost (*spam*, oönskad e-post som skickas ut till mängder av mottagare för att sprida reklam, sabotageprogram eller nätfiskeattacker). Ett botnet kan bestå av hundratusentals datorer där ägarna inte vet om att datorerna är infekterade.

Överbelastningsattacker (DDoS-attacker) riktas mot stordatorsystem eller datornätverk, exempelvis en myndighet eller ett företag, och leder till att systemet överbelastas. Endast en liten kapacitet blir kvar för övrig kommunikation och systemet eller hemsidan riskerar att bli helt utslagen under en tid. Attackerna görs ofta med hjälp av botnets.

2.1.1 *It-brottsligheten omsätter stora belopp*

Under de senaste decennierna har den it-relaterade brottsligheten utvecklats till en industri där kriminella personer och nätverk omsätter miljarder kronor årligen.[34] Det är svårt att uppskatta exakt hur stora belopp som är i omlopp och hur stora samhällets kostnader för den it-relaterade brottsligheten är eftersom mörkertalen av brott som aldrig anmäls bedöms vara stora. Några beräknade uppskattningar har dock tagits fram, bland annat hänvisar European Cybercrime Center (EC3) till att brottstjänster inom it-relaterad brottslighet globalt omsätter mer än 300 miljarder amerikanska dollar varje år.[35] Kostnaden för den it-relaterade brottsligheten uppskattas vara mångdubbelt större än brottslighetens omsättning. Ett exempel är ett botnet som under 2010 skickade spam där ägarna tjänade ungefär 2,7 miljoner dollar på detta, medan kostnaderna för utveckling och användning av spam-filter beräknades till över en miljard dollar.

Samhällets direkta och indirekta kostnader kopplade till den it-relaterade brottsligheten innefattar flera delar. Dels uppstår kostnader för att skydda sig mot it-relaterad brottslighet med hjälp av till exempel antivirus och försäkringar. Dels uppstår direkta kostnader som en följd av själva brottet i form av förluster och kompensation till utsatta. Det uppstår även indirekta kostnader för drabbade myndigheter, banker och företag genom att deras anseenden och varumärken skadas.[36]

---

34 Polismyndigheten, Noa (2015), *Polisens rapport om organiserad brottslighet 2015*, dnr A185.830/2015, s. 51.

35 McAfee (2013), *The Economic Impact of Cybercrime and Cyber Espionage*, refererad i Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014*, s. 19.

36 Anderson m.fl. (2012), *Measuring the cost of cybercrime,* s. 1-4, 26.

2.2 Utmaningar med it-relaterade brott

It-relaterade brott medför flera specifika och svåra utmaningar för rättsväsendet, utöver de som finns för alla typer av brott. I detta avsnitt redovisas några av dessa utmaningar.

2.2.1 Digitala bevis är svåra att säkra

Polismyndigheten måste agera snabbt och på rätt sätt för att kunna säkra flyktiga digitala bevis. Tidspressen blir bland annat tydlig vid så kallade IP-spårningar.[37] Svenska internetoperatörer ska enligt lag spara trafikinformation i sex månader.[38] Om inte polisen hinner få fram en IP-adress till den misstänkte inom denna tid är det inte längre möjligt att spåra den misstänkte via IP-adressen.[39]

De data som utgör bevisning är dessutom ofta mycket omfattande och svåråtkomliga. Polismyndigheten är exempelvis förhindrad att genomsöka uppgifter som en misstänkt har lagrad i en molntjänst vars server är placerad utanför Sverige.[40] I sådana fall måste istället rättslig hjälp begäras från den stat på vars territorium servern är placerad.[41] En annan svårighet är den ökande användningen av kryptering, som kan göra data oåtkomlig för brottsutredande myndigheter såvida inte den enhet som ska genomsökas, exempelvis en dator, är igång och upplåst när den tas i beslag. Detta ställer nya krav på hur husrannsakningar genomförs, så att den misstänkte inte får möjlighet att stänga ned eller låsa den eftersökta enheten. Att kunna genomföra en it-forensisk undersökning[42] på plats under husrannsakan, så kallad live forensics, blir allt viktigare.[43] Den digitala bevisningen måste också säkras på rätt sätt för att inte förstöras eller förvanskas, vilket kräver särskilda kunskaper hos den som hanterar detta. Den snabba tekniska utvecklingen gör att det behövs en bred kunskap inom Polismyndigheten och Åklagarmyndigheten om informationsteknik, internet och it-forensik för att kunna utreda brott tillfredsställande och ha förmåga att värdera och hantera digital bevisning.[44]

---

37 En IP-adress eller ett IP-nummer (Internet Protocol address) identifierar en anslutning mot internet och används för att information som skickas på internet ska nå fram till rätt dator. IP-adressen kan spåras till en operatör, som kan lämna abonnentuppgifter för IP-adressen, så kallad IP-spårning.

38 6 kap. 16 § lag (2003:389) om elektronisk kommunikation. De svenska datalagringsbestämmelserna är föremål för prövning, se avsnitt 2.6.2.

39 Intervju med EC3, Europol 2015-06-02; intervju med Åklagarmyndigheten 2014-11-14.

40 Detta skulle vara att betrakta som en husrannsakan i utlandet, se Ds. 2005:6, s. 131.

41 Se 3 kap. lag (2000:562) om rättslig hjälp i brottmål.

42 Se avsnitt 1.6.2.

43 Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014;* intervju Polismyndigheten 2015-03-12; Kronqvist, Stefan (2013), *Brott och digitala bevis. En handledning. Tredje upplagan,* Norstedts Juridik, s. 51.

44 Politiet, Politidirektoratet, Norge (2015), *Datakrimstrategien*, s. 159; intervju med Rikspolisstyrelsen 2014-11-17; intervju med Polismyndigheten 2015-03-12.

2.2.2 *Svårt att identifiera misstänkta personer*

När brottsligheten flyttar ut på internet krävs ofta ett omfattande spaningsarbete både på internet och i den fysiska världen för att kunna binda en misstänkt person till ett visst brott.[45] Att hämta bevis från internet kan vara tekniskt komplicerat och kräva genomgång av stora mängder information. Polismyndigheten kan inhämta öppen information från internet oavsett var den lagras fysiskt. För att Polismyndigheten ska kunna genomföra hemlig avlyssning eller övervakning av misstänkta personers elektroniska kommunikation krävs däremot domstolsbeslut.[46]

Även så kallade anonymiseringstjänster gör det svårare för de brottsutredande myndigheterna att spåra internetaktivitet till en viss enhet eller person . När en misstänkt it-enhet har kunnat identifieras är det en utmaning att knyta en viss person till användandet av samma enhet.[47] Specialiseringen bland de kriminella på vissa delar av ett brott har också gjort det svårare för de brottsutredande myndigheterna att identifiera alla inblandade parter i ett brott. De olika specialiserade personerna känner sällan varandra personligen, utan bara till de smeknamn som används på de fora där tjänsterna säljs. Även om Polismyndigheten kan identifiera en deltagare i brottet innebär det inte att samtliga i det kriminella nätverket kan identifieras.[48]

2.3 Utvecklingen för de granskade brottstyperna

Mellan åren 2006 och 2014 ökade antalet anmälda it-relaterade brott[49] med 767 procent, att jämföra med cirka 18 procent för all brottslighet.[50] Under samma period ökade andelen it-relaterade brott av det totala antalet anmälda brott i Sverige från 0,7 till 5,2 procent. År 2014 anmäldes totalt 75 369 it-relaterade brott. Det finns inga tecken på att den it-relaterade brottsligheten kommer att avta.

Personuppklaringsprocenten för samtliga brott har minskat från 18 procent 2006 till 15 procent 2014. Personuppklaringsprocenten för de granskade it-relaterade brotten följer i stort samma kurva, men ligger konstant 6–10 procentenheter lägre än personuppklaringen för samtliga brott, se diagram 1.

---

45 Intervju med EC3, Europol 2015-06-02; Polismyndighetens konferens om it-relaterad brottslighet i Nynäshamn i april 2015.

46 Kronqvist, Stefan (2013), *Brott och digitala bevis. En handledning. Tredje upplagan*, Norstedts Juridik, s. 55, 86-88, 91-95. Se 27 kap. 18-19 §§ rättegångsbalken (1942:740) för regler om hemliga tvångsmedel.

47 Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014;* intervju med Åklagarmyndigheten 2014-11-10.

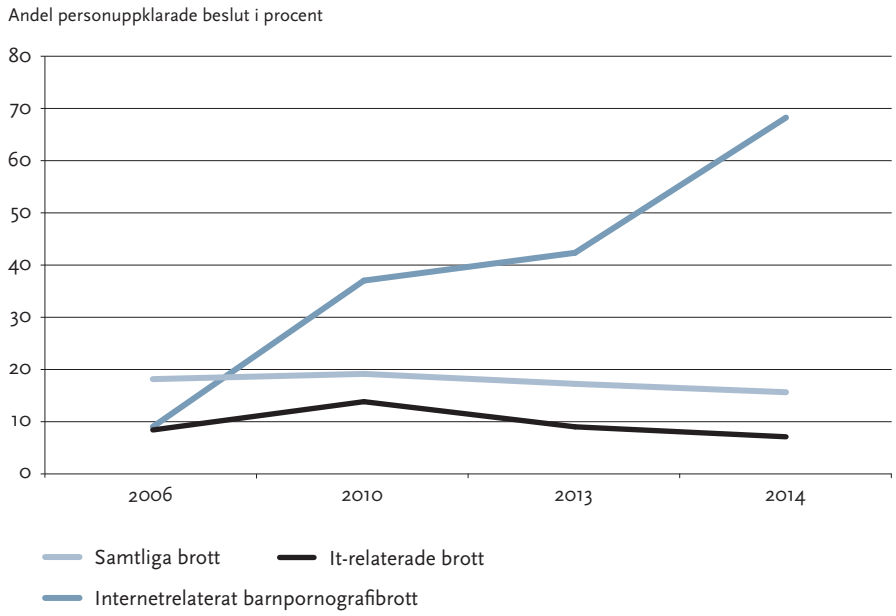
48 Intervju med EC3, Europol 2015-06-02.

49 Se avsnitten 1.3 och 1.6.1 för precisering av it-relaterad brottslighet.

50 Uppgifter från Brå och Riksrevisionens egna beräkningar.

Personuppklaringskurvan för internetrelaterat barnpornografibrott redovisas särskilt i diagram 1 eftersom den visar på en avvikande och mycket bättre utveckling jämfört med de andra brotten. Under perioden 2006–2014 ökade personuppklaringen för dessa brott från 9 till 68 procent. Troliga bidragande faktorer till att personuppklaringen började förbättras 2006 är ändringar i lagstiftningen och att Polishögskolan 2006 började ge en specialiserad utbildning på området.[51] Den största ökningen var mellan åren 2013 och 2014 när personuppklaringsprocenten steg från 38 till 68 procent. En trolig bidragande faktor till denna förbättring är att rikspolischefen 2014 beslutade om att tillfälligt särskilt prioritera utredning av internetrelaterade barnpornografibrott. Målsättningen var att det inte skulle finnas några sådana ärenden öppna när den nya Polismyndigheten bildades i januari 2015.[52] Den 31 december 2014 fanns det 170 öppna internetrelaterade barnpornografiärenden, vilket är en minskning med knappt 24 procent från året innan.[53]

Diagram 1 Andel personuppklaringsbeslut av totalt antal beslut under perioden 2006–2014



Källa: Uppgifter från Brå samt Riksrevisionens egna beräkningar.

Anm: Det har sent i granskningen framkommit att statistiken för internetrelaterat barnpornografibrott för 2014 har påverkats av ett stort ärende. Om personuppklaringsprocenten 2014 justeras för det stora ärendet uppgår den till 48 procent. I Brå:s officiella statistik redovisas siffran 68 procent.

[51] E-post från Polismyndigheten 2015-11-25.

[52] Gruppdiskussion med Riksrevisionens referensgrupp 2015-09-23.

[53] Uppgifter om ärendebalanser från Polismyndigheten september 2015.

Det finns ingen entydig förklaring till varför personuppklaringen inte förbättras, men Brå menar att försämringen inte enbart kan förklaras av ett ökat antal anmälningar. Möjliga förklaringar som ges är att enskilda brottstyper ändrar karaktär, att åklagare och domare ställer högre krav på teknisk bevisning eller att kvaliteten i Polisens utredningsarbete har försämrats, men detta har ännu inte studerats av Brå.[54] En låg personuppklaringsnivå kan innebära att poliser och åklagare i för stor utsträckning lägger ned förundersökningar som hade kunnat klaras upp. I ett flertal rapporter konstaterar Brå även att Polisen väljer att lägga ned förundersökningar som hade kunnat klaras upp.[55] Antalet avskrivna it-relaterade ärenden har ökat från 6 633 stycken år 2006 till 70 014 år 2014, vilket är en ökning med 955 procent. Andelen it-relaterade brott som skrivs av har däremot legat relativt konstant och var 93 procent 2014.[56]

2.3.1 Antalet öppna it-relaterade ärenden ökar

När ärenden är öppna under en längre tid i väntan på att utredas finns en ökad risk att misstänkta personer hinner begå fler brott. Det finns även en risk att brott hinner preskriberas.[57] Polismyndigheten kallar öppna ärenden för ärenden i balans. Ett ärende i balans vid Polismyndigheten kan alltså dels vara ett ärende där det pågår aktiva utredningsåtgärder, och dels ett ärende där det finns förutsättningar att utreda ärendet men där så inte sker av någon anledning.

Ärendebalanserna för it-relaterade brott vid Polisen ökade kraftigt mellan åren 2006 och 2008, och har sedan dess legat på en jämn men hög nivå. Undantaget är 2011 när antalet it-relaterade ärenden i balans tillfälligt minskade med 20 procent. Det är i huvudsak bedrägerier med hjälp av internet som ligger i ärendebalansen. Andelen ärenden i balans i förhållande till antalet anmälda it-relaterade brott har dock minskat under perioden, från cirka 29 procent år 2006 till cirka 13 procent år 2014. Samtidigt kan noteras att andelen it-relaterade ärenden som varit öppna i mer än 12 månader har ökat från 15 procent år 2006 till 22 procent år 2014.[58] Polismyndigheten har inte definierat hur stor andel öppna ärenden som är acceptabelt. I en tillsynsrapport från Rikspolisstyrelsen 2009 rekommenderade inspektionsgruppen att en sådan gräns högst borde uppgå till 9 procent av antalet inkomna ärenden totalt per år, men denna rekommendation har inte antagits.[59]

---

54 Brå (2014), *Varför gav fler poliser inte ökad personuppklaring? Slutrapport i uppdraget "Satsningen på fler poliser"*, rapport 2014:17, s. 35–50.

55 Brå (2014), *Handläggningstider i rättskedjan 2009–2012*, rapport 2014:7, s. 53.

56 Uppgifter från Brå samt Riksrevisionens egna beräkningar.

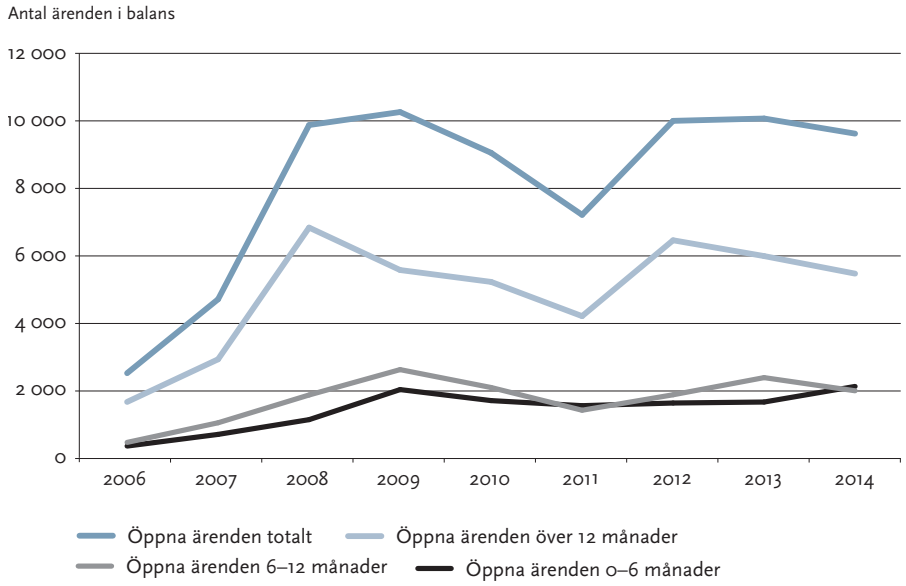
57 Intervju med Åklagarmyndigheten 2015-03-12.

58 Uppgifter från Polismyndigheten och Riksrevisionens egna beräkningar. Sifferuppgifterna ger en bild av hur situationen såg ut i december månad under åren 2006–2014.

59 Rikspolisstyrelsen (2013), *Uppföljning av inspektion av polismyndigheternas ärendebalanser i den brottsutredande verksamheten*, tillsynsrapport 2013:3, s. 41.

Ett annat sätt att värdera Polismyndighetens resultat är att titta på handläggningstider. Medeltiden för att handlägga[60] it-relaterade brottsanmälningar har sjunkit mellan åren 2006 och 2014. Förklaringen till detta är att ärenden skrivs av fortare.[61] Detta skulle även kunna förklara varför andelen ärenden i balans i förhållande till antalet anmälda it-relaterade brott sjunker. Parallellt med denna utveckling har dock medeltiden för att handlägga personuppklarade it-relaterade brott ökat under samma period. För utredningar som har lett till åtal ökade medelhandläggningstiden med cirka 14 procent, för utredningar som har lett till strafföreläggande med 40 procent och för utredningar som har lett till åtalsunderlåtelse med 33 procent. Det ska dock noteras att medeltiden sjönk något under 2014 till cirka 300 dagar.

Diagram 2 Antal it-relaterade öppna ärenden (dvs. i balans) vid Polisen



Källa: Polismyndighetens uppgifter om ärendebalanser

[60] Med handläggningstid menas här tid från inkommen anmälan till beslut om avskrivning eller åtal.

[61] Uppgifter från Brå samt Riksrevisionens egna beräkningar.

2.4 Myndigheterna har uppmärksammat it-relaterad brottslighet relativt sent

Polismyndigheten och Åklagarmyndigheten har relativt sent uppmärksammat den it-relaterade brottsligheten i interna styrdokument och budgetunderlag. Först 2013 börjar området lyftas fram i en ökad utsträckning.[62] Myndigheterna konstaterar att de behöver stärka sin förmåga på området. Inom Polisen tydliggör man att it-aspekten ska beaktas i alla delar av den brottsbekämpande verksamheten. En förklaring till att Polisen tidigare inte har uppmärksammat den it-relaterade brottsligheten i någon större omfattning är, enligt flera företrädare för Polismyndigheten, att det har tagit lång tid att få gehör och förståelse för omfattningen av den it-relaterade brottsligheten och på vilka sätt informationsteknik och internet används för att begå brott.[63] En försvårande omständighet är att Polismyndigheten har svårt att överblicka den it-relaterade brottsligheten. Detta beror bland annat på att it-relaterade brott är svåra att särskilja i den officiella statistiken, att mörkertalen för dessa brott antas vara stora och på att det saknas ett nationellt samordnat underrättelsearbete om it-relaterad brottslighet.[64] Riksrevisionen noterar att flera andra länder betonar vikten av att rättsväsendet har en uppdaterad lägesbild av den it-relaterade brottsligheten. Detta för att man effektivt ska kunna anpassa till exempel lagstiftning, arbetsmetoder och strategier till brottsutvecklingen (se bilaga 1).

2.5 Större förändringar inom rättsväsendet

Under senare år har rättsväsendet tillförts ökade resurser. Mellan åren 2006 och 2014 har anslaget för Polisen ökat med 36,5 procent och för Åklagarmyndigheten med 47 procent.[65] Särskilda satsningar har gjorts inom rättsväsendet under perioden, till exempel uttalade regeringen år 2006 ett mål om att Sverige skulle ha 20 000 poliser år 2010. Det innebar att antalet poliser skulle öka med drygt

---

62 Åklagarmyndigheten nämner redan i sin verksamhetsplan år 2007 att it-bedrägerier är ett prioriterat område och att myndigheten ska se över möjligheterna att säkra bevis i it-miljö. Se Polisens och Åklagarmyndighetens budgetunderlag, verksamhetsplaner och årsredovisningar åren 2006–2014 samt Rikspolischefens inriktning år 2014.

63 Intervju med Rikspolisstyrelsen 2014-11-17; intervju Polishögskolan 2014-11-18; Rikspolisstyrelsen (2013), *Förstudierapport, polisens brottsbekämpande verksamhet, brott med internet-relevans*, dnr PoA480-5583/11, s. 4.

64 Intervju med Rikspolisstyrelsen 2014-11-17; intervju med Polismyndigheten 2015-03-16. Polismyndigheten har velat ändra kodningen i statistiken för att lättare kunna urskilja it-relaterade brott. Brå och Åklagarmyndigheten är dock tveksamma och menar att det finns en risk för att ett för stort antal koder kan försvåra användningen av koder och leda till missvisande statistik. Brå ska nu se över möjligheterna att skapa ett system för att kunna följa utvecklingen av it-inslaget i brottsligheten, se avsnitt 2.6.3.

65 År 2014 var anslaget för Polisen 21 079 mnkr och för Åklagarmyndigheten 1 310 mnkr. Inga medel är särskilt avsatta för att utreda och handlägga it-relaterad brottslighet. Prop. 2015/16:1, utgiftsområde 4.

2 500 från år 2006 till och med år 2010.[66] Regeringens målsättning var att satsningen bland annat skulle leda till en högre personuppklaring.[67]

2.5.1 Polisen

Den nya Polismyndigheten

I januari 2015 bildades Polismyndigheten, som består av de tidigare 21 polismyndigheterna, Rikspolisstyrelsen och Statens kriminaltekniska laboratorium. I samband med detta blev även Säkerhetspolisen (Säpo) en egen myndighet. Omorganisationen ska öka förutsättningarna för ett bättre verksamhetsresultat och en högre kvalitet i polisarbetet. Den nya Polismyndigheten ska vara närmare medborgarna och fungera mer enhetligt.[68] Polismyndigheten är uppdelad i sju geografiska regioner; Syd, Väst, Öst, Stockholm, Mitt, Bergslagen och Nord. Under dessa finns 35 polisområden, som i sin tur är uppdelade i 99 lokalpolisområden. Det finns även nationella avdelningar med olika funktioner som ska stödja den operativa verksamheten.[69]

Polisregionerna har ett helhetsansvar för polisverksamheten inom ett angivet geografiskt område och ska, så långt det är möjligt och effektivt, ha en liknande organisatorisk grundstruktur. De regionala utredningsenheterna ansvarar bland annat för utredningar av vissa it-brott, för större bedrägeriärenden utan direkt lokal anknytning samt för barnpornografibrott. Polisområdenas utredningsenheter handlägger bland annat vissa bedrägeribrott och mängd- och seriebrott av större omfattning.[70]

Nationella operativa avdelningen (Noa) är en central funktion som ansvarar för internationellt polissamarbete och internationell samverkan och är nationell kontaktpunkt mot bland annat Säkerhetspolisen. Noa ska endast bedriva egeninitierad verksamhet när det gäller de specifika ärendetyper som ska utredas av Noa, och därutöver stödja regionerna i deras utredningsarbete vid särskilda behov.[71]

Som ett led i ombildningen av Polisen till en enda myndighet har det införts ett nationellt processansvar på flera områden. Det finns bland annat för it-forensik,

---

66 Brå (2013), *Satsningen på fler poliser – vad har den lett till,* rapport 2013:12, s. 6. I realiteten ökade antalet poliser med närmre 3 000 fram till slutet av 2011, vilket ledde till att det i december 2011 fanns cirka 20 400 poliser. Detta korrigerades följande år för att komma tillbaka till en nivå på 20 000 poliser.

67 Se bland annat prop. 2005/06:1, utgiftsområde 4 och prop. 2009/10:1, utgiftsområde 4.

68 Genomförandekommittén för nya Polismyndigheten (2014), *Beslut om huvuddragen i den nya Polismyndighetens detaljorganisation – med medborgare och medarbetare i centrum*, dnr JU 2012:16/2014/51, s. 7f.

69 Polismyndigheten, Organisation, https://polisen.se/Om-polisen/Organisation/ (hämtad 2015-11-12).

70 Genomförandekommittén för nya Polismyndigheten (2014), *Beslut om huvuddragen i den nya Polismyndighetens detaljorganisation – med medborgare och medarbetare i centrum,* dnr JU 2012:16/2014/51, s. 19–21.

71 Ibid, s. 27–30.

utredningar av komplex it-brottslighet och barnpornografibrott.[72] Nationellt forensiskt center (NFC, tidigare Statens kriminaltekniska laboratorium, SKL) ansvarar för den it-forensiska arbetsprocessen medan Noa ansvarar för komplex it-brottslighet och barnpornografibrott.[73] Polismyndigheten arbetar nu med att ta fram processbeskrivningar.

Många centrala beslut i förändringsarbetet i och med omorganisationen saknas fortfarande, bland annat på grund av att flera nyckelpersoner, som ska leda olika arbetsprocesser och verksamheter inom Polismyndigheten, ännu inte har rekryterats.[74]

I denna rapport används Polisen för att hänvisa till den tidigare polisorganisation och Polismyndigheten efter ombildningen.

Nationellt bedrägericentrum bildades 2013

Sedan 2013 finns Nationellt bedrägericentrum (NBC) som en enhet under bedrägerisektionen i Stockholm. Centret ska samordna resurserna inom Polismyndigheten mot bedrägeribrott för att kunna upptäcka brottsmönster som sträcker sig över flera regioner. I uppdraget ingår metodutveckling, brottsförebyggande insatser samt operativt arbete i form av samordning.[75] Nationellt bedrägericentrum arbetar med alla typer av bedrägerier, alltså inte enbart it-bedrägerier.

Nationellt it-brottscenter bildades i oktober 2015

Inom Polismyndigheten finns från och med den 1 oktober 2015 ett Nationellt it-brottscenter, som ligger i Stockholm och är en del av Noa. Där finns i dagsläget cirka 45 medarbetare, men siktet är på att ha det dubbla 2017. Syftet med centret är att bidra till en kompetenshöjning för svensk polis generellt och att fungera som knutpunkt för it-relaterad brottslighet på nationell nivå. Centret är också tänkt att fungera som en plattform för samarbete med exempelvis Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap, Åklagarmyndigheten och Nationellt Forensiskt Center, samt vara en internationell kontaktpunkt.[76]

---

[72] Ibid, s.16; intervjuer med Polismyndigheten 2015-03-16 och 2015-03-24. Processansvaret omfattar att skapa, förvalta och implementera enhetlighet, informationskanaler samt utveckling och uppföljning av processen från ansvarsnivån till alla nivåer där verksamheten ska utföras.

[73] Genomförandekommittén för nya Polismyndigheten (2014), *Beslut om huvuddragen i den nya Polismyndighetens detaljorganisation – med medborgare och medarbetare i centrum*, dnr JU 2012:16/2014/51, s. 27, 34.

[74] Telefonintervju med Polismyndigheten 2015-10-07.

[75] Polismyndigheten Stockholm (2014), *Nationell lägesbild bedrägerier,* s. 2; intervju med Polismyndigheten 2015-08-20.

[76] Genomförandekommittén för nya Polismyndigheten (2014), beslutsprotokoll, dnr Ju 2012:16/2013/4; intervju med Rikspolisstyrelsen 2014-11-17; Polismyndigheten, It-brottscentrum verklighet i oktober, https://polisen.se/Aktuellt/Nyheter/2015/Juli/IT-brottscentrum-verklighet-i-oktober/ (hämtad 2015-07-08).

2.5.2 *Åklagarmyndigheten*

Åklagarmyndigheten är från och med oktober 2014, liksom Polismyndigheten, indelad i sju geografiska områden med en nationell avdelning.[77] Ett av skälen till omorganisationen var att anpassa myndigheten till den nya polisorganisation och underlätta samverkan med Polismyndigheten.[78] Alla åklagare ska kunna arbeta med och vara förundersökningsledare för it-relaterade brott. Det finns inga krav på åklagarområdena eller kamrarna att de ska ha åklagare som är specialiserade på it-relaterad brottslighet.[79]

2.6 Politiska initiativ inom området

I detta avsnitt redovisas aktuella initiativ från regeringen och EU inom området it-relaterad brottslighet. För mer information om arbetet inom EU, se bilaga 1.

2.6.1 *Om it-relaterad brottslighet i budgetpropositionerna*

Regeringen har uppmärksammat it-relaterad brottslighet i flera budgetpropositioner, i synnerhet bedrägerier, hot och trakasserier, dataintrång, och sexualbrott.[80] Regeringen betonar att de brottsbekämpande myndigheterna behöver ha tillgång till utredningsverktyg som både är väl anpassade till informationsteknologin och som tar hänsyn till den personliga integriteten.[81] Regeringen understryker även betydelsen av att de brottsutredande myndigheterna anpassar sin verksamhet efter utvecklingen. Myndigheterna behöver ha kapacitet att möta utvecklingen, och regeringen ser behov av både allmänna kunskaps- och kompetenslyft och stärkt expertkunskap på området.[82]

2.6.2 *Utredningar inom området*

Aspekter av den it-relaterade brottsligheten behandlas i flera pågående eller nyligen avslutade utredningar. Områden som behandlas är bland annat förslag kopplade till it-relaterade bedrägerier, sexualbrott som sker via internet samt hot och andra kränkningar som sker online. [83] Regeringen har inom ramen

---

77 De sju geografiska åklagarområdena är Syd, Väst, Öst, Stockholm, Mitt, Bergslagen och Nord.

78 Åklagarmyndigheten (2014), *Ny organisation för Åklagarmyndigheten*, PM 2014-09-10.

79 Intervju med Åklagarmyndigheten 2014-11-14.

80 Prop. 2005/06:1, utgiftsområde 4; prop. 2010/11:1, utgiftsområde 4; prop. 2011/12:1, utgiftsområde 4; prop. 2012/13:1, utgiftsområde 4.

81 Prop. 2005/06:1, utgiftsområde 4; prop. 2010/11:1, utgiftsområde 4; prop. 2011/12:1, utgiftsområde 4; prop. 2015/16:1, utgiftsområde 4.

82 Prop. 2005/06:1, utgiftsområde 4; prop. 2010/11:1, utgiftsområde 4; prop. 2011/12:1, utgiftsområde 4; prop. 2014/15:1, utgiftsområde 4.

83 SOU 2013:85, *Stärkt straffrättsligt skydd för egendom*; dir. 2015:5, *Tilläggsdirektiv till 2014 års sexualbrottskommitté* (Ju 2014:21); Ds. 2015:49, *Översyn av straffbestämmelsen om kontakt med barn i sexuellt syfte;* Dir. 2014:74, *Ett modernt och starkt straffrättsligt skydd för den personliga integriteten.*

för en större utredning om informations- och cybersäkerhet även fått förslag på mål och åtgärder som tar sikte på att stärka arbetet med att förebygga och bekämpa it-relaterad brottslighet. Förslagen innebär att Budapestkonventionen bör ratificeras, att informationsutbyte mellan brottsbekämpande myndigheter och andra myndigheter inom informations- och cybersäkerhetsområdet bör utredas och att det bör genomföras en översyn av hemliga tvångsmedel i den digitala miljön.[84]

Det finns också utredningar som hanterar den personliga integriteten och förutsättningar för det brottsutredande arbetet, såsom användandet av hemliga tvångsmedel och de svenska datalagringsbestämmelserna.[85] Regeringen har även beslutat att ge en särskild utredare i uppdrag att lämna förslag till hur den grundläggande utbildningen till polis kan omformas till en högskoleutbildning. Syftet är att säkerställa att Polismyndigheten har den kompetens som krävs för att utföra sitt uppdrag i ett allt mer komplext samhälle.[86]

2.6.3 Regeringen har gett uppdrag till myndigheterna

Under senare år har regeringen gett ett antal uppdrag till Polisen, Åklagarmyndigheten respektive Brottsförebyggande rådet (Brå) med koppling till it-relaterad brottslighet.

I regleringsbrevet 2014 fick Polisen i uppdrag att redovisa hur den på kort och lång sikt arbetar för att öka effektiviteten och kvaliteten i bedrägeribrott och andra brott som ökar kraftigt med anledning av den snabba teknikutvecklingen. Åklagarmyndigheten fick i regleringsbrevet samma år i uppdrag att säkerställa att de har rätt kompetens vad gäller utredning av it-relaterade brott. Därutöver har myndigheterna fått generella uppdrag kopplade till arbetet med kompetensförsörjning.[87]

Brå fick i regleringsbrevet 2015 i uppdrag att kartlägga utvecklingen av förekomsten av it-relaterade inslag i anmälda brott. Brå ska analysera kompetens och kapacitet vad gäller it-relaterad brottslighet samt it-forensiska undersökningar i den brottsutredande verksamheten. Brå ska även överväga möjligheten att

---

84 SOU 2015:23, *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.*

85 SOU 2015:31, *Datalagring och integritet*; De svenska datalagringsbestämmelserna kommer även att prövas av EU-domstolen då Kammarrätten i Stockholm har begärt ett förhandsavgörande i det så kallade datalagringsmålet mellan Tele2 Sverige AB och Post- och telestyrelsen (PTS), målnummer 7380-14. EU-domstolen ogiltigförklarade EU:s datalagringsdirektiv i april 2014; Se även *Utredningen om tillsynen över den personliga integriteten* (Ju 2015:02) som har i uppdrag att lämna förslag på hur skyddet för den personliga integriteten kan stärkas genom att samla tillsynen över personuppgiftsbehandling hos en myndighet och *Integritetskommittén* (Ju 2014:09).

86 Dir. 2015:29, *En förändrad polisutbildning.*

87 Regleringsbrev för budgetåret 2013 avseende Rikspolisstyrelsen och övriga myndigheter inom polisorganisationen; regleringsbrev för budgetåret 2014 avseende Rikspolisstyrelsen och övriga myndigheter inom polisorganisationen; regleringsbrev för budgetåret 2015 avseende Åklagarmyndigheten.

skapa ett system som gör det möjligt att följa utvecklingen av it-relaterade inslag i anmälda brott. Uppdraget ska redovisas senast i september 2016.

Ett annat regeringsuppdrag till Brå är att kartlägga förändringar i karaktären på anmälda brott, till exempel om it-relaterade inslag i brotten har ökat, och deras påverkan på utvecklingen av personuppklarade brott. Brå ska även studera domstolarnas krav på bevisning och hur de kan ha påverkat utvecklingen av personuppklarade brott. Uppdraget ska redovisas senast i oktober 2016.

2.6.4 Sverige har inte ratificerat Budapestkonventionen

Europarådets it-brottskonvention CETS no. 185 (Budapestkonventionen) syftar huvudsakligen till att harmonisera lagstiftning och förenkla internationellt samarbete. Sverige undertecknade Budapestkonventionen 2001 men har inte ratificerat den. Vissa företrädare för de brottsutredande myndigheterna menar att det skulle underlätta det internationella samarbetet om Sverige ratificerade konventionen.[88] EU-kommissionen uppmanar alla EU:s medlemsstater att ratificera Budapestkonventionen (se bilaga 1). Företrädare för Justitiedepartementet uppger att utredningar om nödvändiga författningsändringar för att kunna tillträda konventionen har genomförts och att ärendet bereds i Regeringskansliet.[89]

2.6.5 Arbetet inom EU

Att bekämpa it-brott är ett av tre fokusområden i den europeiska säkerhetsagendan från april 2015.[90] I strategin lyfter kommissionen särskilt fram EU:s strategi för cybersäkerhet[91] och betydelsen av att medlemsstaterna snabbt antar det aktuella utkastet till direktiv om nät- och informationssäkerhet.[92] Medlemsstaterna behöver även säkerställa ett fullständigt genomförande av befintlig EU-lagstiftning, särskilt direktivet om angrepp mot informationssystem[93] och direktivet om sexuell exploatering av barn för att förebygga sexuella övergrepp mot barn på nätet.[94] Kommissionen

---

88 Intervju med Åklagarmyndigheten 2014-11-14; intervju med Rikspolisstyrelsen 2014-11-17; intervju med Polismyndigheten 2015-03-16.

89 E-post från Justitiedepartementet 2015-04-22.

90 Europeiska kommissionen KOM(2015) 185 slutlig.

91 Europeiska kommissionen och Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik JOIN(2013) 1 slutlig.

92 Europeiska kommissionen KOM(2013) 48 slutlig.

93 Direktiv 2013/40/EU; Sveriges behandling av direktivet, se prop. 2013/14:92 och bet. 2013/14:JuU27.

94 Direktiv 2011/93/EU; Sveriges behandling av direktivet, se prop. 2012/13:194 och bet. 2013/14:JuU8; se även Europeiska kommissionens och USA:s initiativ *Global Alliance against Child Sexual Abuse Online*.

aviserar också en översikt av rambeslutet från 2001[95] om bekämpningen av bedrägeri och förfalskning av andra betalningsmedel än kontanter, då det inte längre är i takt med dagens brottslighet och utmaningar.[96]

Dessutom genomför en arbetsgrupp[97] i Europeiska unionens råd just nu utvärderingar av medlemsstaternas implementering och hantering av EU-direktiv avseende cyberkriminalitet. Utvärderingen av Sverige är planerad att genomföras i mars 2016.[98]

95 Europeiska unionens råd, rådets rambeslut 2001/413/RIF.

96 Europeiska kommissionen KOM(185) slutlig, s. 21–22.

97 Arbetsgruppen för allmänna frågor inklusive utvärdering.

98 Europeiska unionens råd (2014) 7940/14, *Seventh round of mutual evaluations – Order of visits and observers;* Europeiska unionens råd (2014) 5445/1/14 REV 1, *Seventh round of mutual evaluations – Questionnaire.*

3 Hanteringen av it-relaterade brott

I detta kapitel redovisas iakttagelser av hur Polismyndigheten och Åklagarmyndigheten utreder och handlägger it-relaterade brott. Iakttagelserna bygger i huvudsak på Riksrevisionens aktgranskning och intervjuer.

3.1 Från anmälan till beslut om förundersökning

Polismyndigheten ansvarar för att ta emot brottsanmälningar. Allmänheten kan sedan 2006 göra polisanmälningar via internet, men mer än hälften av alla polisanmälningar, cirka 60 procent, som kommer in till Polismyndigheten tas emot av civilanställda operatörer vid Polisens kontaktcenter (PKC). Dessutom kan poliser upprätta anmälningar vid misstanke om brott.[99] Riksrevisionen noterar att det har påbörjats ett arbete med att integrera PKC i den brottsutredande verksamheten för att på så sätt effektivisera utredningsprocessen. De ärenden som inkommer till PKC granskas av en förundersökningsledare vid centret och endast ärenden som bedöms ha förutsättningar att utredas vidare ska gå vidare i utredningsprocessen.[100] Ärendena som överlämnas till polisregionerna fördelas antingen utifrån var brottet har begåtts eller var den misstänkte bor, om en misstänkt person finns med i anmälan. Därefter fördelas ärenden till lämplig utredande enhet i berörd polisregion.[101] De ärenden som överlämnas ska vara bearbetade och hålla en hög kvalitet.[102] Om relevanta uppgifter saknas eller om anmälan innehåller fel krävs kompletteringar som fördröjer arbetet, eller som till och med kan göra vidare utredning omöjlig.[103]

Riksrevisionen har inte granskat kvaliteten i anmälningarna, men aktgranskningen visar att IP-adressen antecknades fel i brottsanmälan i drygt 20 procent av ärendena där en IP-adress var känd. Detta gör att IP-adressen inte går att använda i förundersökningen. Aktgranskningen visar också att annan teknisk information som man borde kunna arbeta vidare med, exempelvis metadata som är information om data, fanns med i anmälan i

99 Telefonintervju med Polismyndigheten 2015-10-05; e-post Polismyndigheten 2015-11-06.

100 Polismyndighetens budgetunderlag 2016-2018, s. 12.

101 Telefonintervju med Polismyndigheten 2015-10-05; e-post Polismyndigheten 2015-11-06.

102 Polismyndighetens budgetunderlag 2016-2018, s. 12.

103 Intervju med Åklagarmyndigheten 2015-03-09.

samma omfattning i avskrivna respektive personuppklarade ärenden. Det var dock vanligare att en misstänkt person fanns angiven redan i anmälan i de ärenden som personuppklarades.

3.2 Personuppklarade förundersökningar kom igång snabbare

Med tanke på att digitala bevis är flyktiga är det viktigt att utredningarna kommer igång snabbt för it-relaterade brott. Riksrevisionens aktgranskning visar att beslut om att inleda en förundersökning vanligen sker inom en dag efter att anmälan gjordes. Utredningsåtgärderna kom igång fortare och fler inledande åtgärder vidtogs i de personuppklarade förundersökningarna jämfört med de nedlagda. Det gäller både sådana åtgärder som vidtogs innan beslut om förundersökning och sådana som vidtogs första veckan efter beslutet. I 63 procent av de personuppklarade förundersökningarna vidtogs utredningsåtgärder inom en vecka efter att förundersökningen inleddes, jämfört med 49 procent för de nedlagda förundersökningarna. De vanligaste inledande åtgärderna var att begära information från svenska företag och att hålla förhör med målsäganden.

Tabell 1 De vanligaste inledande åtgärderna i förundersökningarna (FU), procent

	Nedlagda FU			Personuppklarade FU		
Inledande åtgärder	**Före inledd FU**	**Första veckan efter inledd FU**	**Totalt**	**Före inledd FU**	**Första veckan efter inledd FU**	**Totalt**
Begära information från svenska företag	5,6	19	**21,6**	25,7	3,4	**29,1**
Förhöra målsägande	3,7	7,5	**11,2**	8,5	14,8	**23,3**
Säkra kommunikation	2	0	**2**	3	13,7	**16,7**
Begära information från utländska företag	0	2	**2**	9	0	**9**

Källa: Riksrevisionens aktgranskning. Siffrorna anger i hur stor del av ärendena i procent som respektive åtgärd vidtas.

3.3 Fler aktörer och åtgärder i personuppklarade förundersökningar

Aktgranskningen visar att det vidtogs fler olika utredningsåtgärder efter de inledande åtgärderna i de personuppklarade förundersökningarna jämfört med de nedlagda förundersökningarna. Till exempel genomfördes it-forensisk undersökning, husrannsakan och beslag enbart i de personuppklarade förundersökningarna. Det var också vanligare att olika aktörer var delaktiga i de personuppklarade förundersökningarna. Det handlade främst om att uppgifter begärdes in från företag, att it-forensiker var delaktiga samt att målsäganden bidrog med information. Sammantaget vidtogs ytterligare utredningsåtgärder i 91 procent av de personuppklarade förundersökningarna och i 49 procent av de nedlagda. I 44 procent av de nedlagda förundersökningarna vidtogs inte några faktiska utredningsåtgärder.[104] I de nedlagda förundersökningarna var den vanligaste åtgärden att begära information från svenska företag, följt av att hålla förhör med misstänkta och med målsägande. I de personuppklarade förundersökningarna var de vanligaste åtgärderna att förhöra misstänkta och målsägande, följt av att begära information från svenska företag och säkra kommunikation.

Det var vanligare att hålla förhör med målsägande i de personuppklarade förundersökningarna, detta gjordes i 70 procent jämfört med 24 procent för nedlagda förundersökningar. I båda grupperna hölls det oftast ett till två förhör med målsägande. Med den misstänkta och med vittnen hölls det generellt tre till fyra förhör. Förhör med målsägande genomfördes oftast tidigare i förundersökningen än med vittnen eller den misstänkta.

Utredningsåtgärderna vidtogs generellt antingen inom fem veckor efter inledd förundersökning, eller efter mer än sex månader. Företrädare för Polismyndigheten och Åklagarmyndigheten har inte kunnat förklara vad detta beror på. Det finns också flera exempel på ärenden som blev liggande längre perioder utan att utredningsåtgärder vidtogs. Det gick inte alltid att utläsa i akterna hur lång tid olika åtgärder tog att genomföra och det har inte heller gått att identifiera någon särskilt tidskrävande åtgärd. Undantaget är så kallad fingranskning av barnpornografi, som innebär att bilderna klassificeras som barnpornografibrott, grovt barnpornografibrott eller att det inte är ett barnpornografibrott. Fingranskning av barnpornografi tog ett halvt till ett år att genomföra, men eftersom denna brottstyp endast förekom i fyra av akterna går det inte att dra några generella slutsatser.

[104] Direktiv skickades av förundersökningsledaren i 6 stycken av de aktuella ärendena. Några åtgärder vidtogs dock inte utifrån dessa direktiv.

3.4 It-relaterade åtgärder vidtogs sällan i utredningarna

Riksrevisionens aktgranskning visar att Polisen sällan vidtog it-relaterade åtgärder i förundersökningarna. Till exempel var det mindre vanligt att man spårade IP-adresser eller gjorde it-forensiska undersökningar. Fokus var i stället på så kallade traditionella undersökningar, exempelvis kontosökningar för att spåra hur och till vem betalningar har skett. Det är dock inte alltid nödvändigt, eller ens möjligt, att vidta it-relaterade åtgärder i varje enskilt ärende. När det gäller bedrägeri genom annonsering på internet (exempelvis på Blocket eller Tradera) visar aktgranskningen att det ofta var tillräckligt att göra bankkontosökningar och säkra den kommunikation som skett för att åtal skulle kunna väckas. Flera poliser och åklagare framhåller samtidigt i intervjuer att information från it-relaterade utredningsåtgärder kan vara värdefull för att nå framgång i Polismyndighetens underrättelsearbete. Polismyndigheten kan till exempel genom att spåra en IP-adress se om ett visst nätverk på en viss plats regelbundet används för att begå brott.[105] Riksrevisionens uppfattning är att information från it-relaterade åtgärder också skulle kunna vara värdefull för att effektivisera brottsutredningar och se mönster i brottsligheten. Det kan i detta sammanhang också nämnas att Polismyndigheten och Åklagarmyndigheten saknar ett vedertaget metodstöd för vilka it-relaterade åtgärder som kan och bör vidtas i utredningar av it-relaterade brott.

It-forensiska undersökningar genomfördes endast i cirka tre procent av de personuppklarade förundersökningarna och aldrig i de nedlagda. Värdet av att it-forensikerna involveras i utredningsarbetet och deltar i planering av olika åtgärder, till exempel husrannsakan, framhålls av flera företrädare för Polismyndigheten och Åklagarmyndigheten. It-forensikernas medverkan kan säkerställa att bevis tas om hand på rätt sätt och höja effektiviteten i förundersökningsarbetet.[106] Av Riksrevisionens enkät framkommer att det i polisregionerna varierar på vilket sätt it-forensiker är delaktiga under utredningsarbetet. Två ytterligheter är region Syd och region Mitt. I region Syd är it-forensikerna ofta delaktiga i arbetsmöten, vid planering och genomförande av husrannsakan och beslag, samt vid förhör. I region Mitt är it-forensikerna däremot sällan eller aldrig delaktiga vid andra arbetsmoment än vid den it-forensiska undersökningen.

[105] Gruppdiskussion med Riksrevisionens referensgrupp 2015-09-23.

[106] Rikspolisstyrelsen (2014), *Inspektion av polismyndigheternas förmåga att handlägga IT-brott*, s. 1f, 9; intervjuer med Polismyndigheten 2015-03-12 och 2015-03-24; intervju med Åklagarmyndigheten 2015-03-12. Jämför även PNU i avsnitt 1.5.

3.4.1 Det finns utrymme för att vidta fler it-relaterade åtgärder

Riksrevisionens aktgranskning visar att det finns ett utrymme för att vidta fler it-relaterade åtgärder. I 73 av ärendena var till exempel en IP-adress känd antingen i anmälan eller i ett senare skede. Polisen genomförde IP-spårningar i 47 ärenden. Därmed avstod man från att göra IP-spårningar i cirka 35 procent av de fall där man skulle kunna göra det.[107] Utöver detta fanns det också flera ärenden där en IP-adress fanns tillgänglig hos ett privat företag, men där den aldrig inhämtades av Polisen. Det är generellt inte svårt för Polismyndigheten att hämta in en IP-adress och det är också en uppgift som myndigheten får lagra och göra gemensamt tillgänglig inom organisationen.[108]

3.5 Avskrivningsgrunden överensstämde oftast med omständigheterna i fallet

Den genomgång av avskrivna ärenden som Riksrevisionen låtit genomföra visar att 125 av totalt 175 granskade avskrivna ärenden var utan anmärkning, det vill säga avskrivningsgrunden har i dessa ärenden överensstämt med omständigheterna i fallet, se tabell 2. Avskrivningsbesluten motiveras dock i olika omfattning och man hänvisar till olika avskrivningsgrunder trots att omständigheterna i ärendena är likartade. Detta har däremot inte haft någon betydelse för beslutet att skriva av ett ärende. I ett fåtal ärenden har det visat sig finnas materiella brister där ytterligare utredningsåtgärder hade kunnat vidtas. Det är dock inte säkert att utgången i dessa ärenden skulle ha varit annorlunda om ytterligare åtgärder hade vidtagits. När fel avskrivningsgrund används innebär detta att allmänheten, i huvudsak berörda personer i det enskilda ärendet, har fått fel information om varför ärendet skrevs av. En felaktig avskrivningsgrund skulle även kunna leda till problem om man i ett senare skede vill gå tillbaka till en viss typ av ärenden.[109]

---

[107] IP-spårningar får göras vid misstanke om brott. 6 kap 22 § lag (2003:389) om elektronisk kommunikation; prop. 2011/12:55, s. 101.

[108] 3 kap. 2 § första stycket punkterna 1 och 3 polisdatalagen (2010:361).

[109] Riksrevisionen (2015), PM ”Redovisning av granskningsuppdrag”; e-post från Riksrevisionens konsult med åklagarkompetens 2015-09-23.

Tabell 2 Genomgång av beslut om avskrivning av polis och åklagare

Utan anmärkning (dvs. avskrivningsgrunden överensstämmer med omständigheterna i fallet)	125
Motivering för avskrivning saknas	31
FU nedlagd utan att rimliga utredningsåtgärder vidtagits	3
FU inleddes inte men borde ha inletts	1
Felaktig användning av avskrivningsgrund ”brott utomlands”	8
Felaktig användning av andra avskrivningsgrunder	3
Bristfällig anmälan (dvs. det var inget brott)	1
Dubbelanmälda brott	3
Totalt	**175**

Källa: Riksrevisionen (2015), PM ”Redovisning av granskningsuppdrag”.

Not: De dubbelanmälda brotten har inte granskats.

I 31 av ärendena fanns inte någon närmare grund för avskrivningen angiven. Till exempel har avskrivningen i vissa fall motiverats ”går ej att utreda” utan att skälen till detta finns angivna. Av uppgifterna i anmälan har det dock ofta stått klart att det saknats skäl att vidta utredningsåtgärder eller att sådana inte funnits att tillgå. De uppmärksammade bristerna påverkar därför inte möjligheterna att klara upp brottet.

I åtta av ärendena har avskrivningsgrunden ”brott utomlands” angetts trots att uppgifter om brottsforum saknas i anmälan. I dessa fall hade i stället avskrivningsgrunden ”spaningsuppslag saknas” varit mer riktig. Fortsatt utredning hade sannolikt inte heller i dessa fall lett till lagföring. Bristen har därmed inte någon betydelse för möjligheten att klara upp brott.

I tre av ärendena har förundersökningen lagts ned utan att rimliga utredningsåtgärder har vidtagits. I ett av dessa ärenden är det troligt att ärendet hade kunnat gå vidare till lagföring. I de båda andra ärendena går den frågan inte att bedöma.

Bedömningen av om anmälan var bristfällig utgick endast från om det framkom tydligt vilket brott som avsågs. Genomgången visar dock att det varierar vilken information som fanns med i anmälningarna. I de flesta anmälningar framkom tydligt vilket brott som avsågs.

3.6 Gärningstypen hade betydelse för om förundersökning inleddes

De avskrivna ärendena rörde huvudsakligen dataintrång och bedrägerier som skett via internet. Skillnaderna i ärendena kan illustreras i fem så kallade gärningstyper;

- Bedrägeri genom annonsering på internet (exempelvis Blocket och Tradera)
- Bedrägeri genom användning av annans kontokortsuppgifter (exempelvis köp via internet)
- Bedrägeri genom utskick av e-post med betalningsuppmaning
- Dataintrång genom elektronisk tillgång till annans dator
- Dataintrång genom manuell användning av annans dator

Genomgången av avskrivna ärenden visar att gärningstypen hade avgörande betydelse för om förundersökning inleddes och om utredningsåtgärder vidtogs. För gärningstyperna bedrägeri genom annonsering på internet samt bedrägeri genom användning av annans kontokortsuppgifter inleddes i de flesta fall en förundersökning, såvida inte brottet var begånget utomlands. För övriga tre gärningstyper inleddes aldrig en förundersökning, med undantag för ett ärende. Riksrevisionens aktgranskning visar att i en majoritet av de avskrivna ärendena, närmare 70 procent, inleddes aldrig någon förundersökning. I övriga avskrivna ärenden inleddes en förundersökning som senare lades ned.

Flera av gärningstyperna som har ingått i de avskrivna ärendena som granskats är generellt svårutredda och möjligheten att nå framgång i ett enskilt ärende är i det närmaste obefintlig.[110] I några gärningstyper, såsom enskilda bedrägerier som rör mindre belopp, medger till exempel inte lagstiftningen att polis och åklagare vidtar vissa åtgärder eftersom straffskalan är för låg.[111]

[110] Riksrevisionen (2015), PM ”Redovisning av granskningsuppdrag” samt komplettering till denna PM.

[111] För att binda en gärningsman till brottet kan det exempelvis krävas hemliga tvångsmedel i form av hemlig avlyssning eller övervakning av elektronisk kommunikation som bara får användas för brott med en viss straffskala, se 27 kap. 18-19 §§ rättegångsbalken (1942:740). Eftersom åtgärder som kan leda till tillräcklig bevisning för att väcka åtal därmed inte går att vidta är det rätt att skriva av ärendena. Rikspolisstyrelsen föreslog regeringen 2003 att hemliga tvångsmedel även skulle kunna användas vid seriebrottslighet med tillräckligt högt straffvärde. Regeringens bedömning var att tillämpningen då riskerade att bli för vid och därmed integritetskränkande (prop. 2002/03:74, s. 34).

3.7 Sammanfattande iakttagelser

Polis och åklagare kan arbeta effektivare och mer enhetligt

- I de personuppklarade förundersökningarna kom de inledande utredningsåtgärderna igång fortare än i de nedlagda.
- Både inledande och andra åtgärder vidtogs i större utsträckning i de personuppklarade förundersökningarna än i de nedlagda. Dessutom vidtogs fler olika åtgärder i de personuppklarade förundersökningarna. I många nedlagda förundersökningar vidtogs över huvud taget inte några utredningsåtgärder.
- Fler aktörer, såsom it-forensiker och företag, var delaktiga i de personuppklarade förundersökningarna än i de nedlagda.
- IP-adressen antecknades fel i cirka 20 procent av anmälningarna där en IP-adress fanns med. Detta får till följd att uppgiften inte går att använda.

It-relaterade åtgärder vidtogs sällan i utredningarna

- De åtgärder som vidtogs under förundersökningarna var i liten utsträckning it-relaterade. Detta kan bero på att det saknas metodstöd för vilka åtgärder som kan och bör vidtas, samt att det inte alltid är nödvändigt i det enskilda fallet. Samtidigt kan it-relaterade åtgärder ge värdefull information, inte minst för underrättelsearbetet. Det tycks också finnas ett utrymme att genomföra fler it-relaterade åtgärder,
- Det varierar mellan polisregionerna hur delaktiga it-forensikerna är i planering och genomförande av utredningsåtgärder,

Avskrivningar påverkas av gärningstyp och utredningsbarhet

- Gärningstypen hade en avgörande betydelse för om förundersökning inleddes och om utredningsåtgärder vidtogs. Några typer av dataintrång och bedrägerier som sker via internet utreddes i stort sett inte alls.
- Avskrivningarna rörde huvudsakligen gärningstyper som generellt är svårutredda och där möjligheten att nå framgång i ett enskilt ärende är i det närmaste obefintlig. Det finns brottstyper där polis och åklagare i stort sett saknar förutsättningar att vidta utredningsåtgärder i dag.

4 Organiseringen av den utredande verksamheten

I detta kapitel redovisas iakttagelser av hur Polismyndighetens och Åklagarmyndighetens handläggning och utredning av it-relaterad brottslighet är organiserad. Iakttagelserna bygger på Riksrevisionens aktgranskning och enkäter, samt på intervjuer.

4.1 Vedertagna nationella riktlinjer och metodstöd saknas

I Riksrevisionens enkät uppger sex av sju polisregioner att metodstöd för att utreda it-relaterade brott saknas. I region Syd finns ett regionalt framtaget metodstöd. I en förstudie och en tillsynsrapport har Rikspolisstyrelsen tidigare konstaterat att det finns ett behov av nationella riktlinjer för arbetet med it-relaterade brott och hur utredningar ska dokumenteras, men detta har ännu inte tagits fram.[112] I Rikspolisstyrelsens förstudie konstaterade man även att det är otydligt vilka befogenheter enskilda anställda vid Polisen har vid arbete på internet, då det inte finns någon nationell vägledning för detta. Några polismyndigheter i den förra polisorganisationen hade lokala riktlinjer som även användes vid andra polismyndigheter, men dessa var inte bindande.[113] Riksrevisionen noterar att it-aspekten inte heller är en del av Polisens Nationella utredningskoncept (PNU).[114]

Syftet med bildandet av den nya Polismyndigheten var bland annat att arbetet skulle bli mer enhetligt och effektivt. Riksrevisionen noterar att Polismyndigheten har påbörjat ett förändringsarbete med bland annat processöversyner för att åstadkomma detta. Arbetet är dock i ett relativt tidigt skede och det saknas beslut om när processerna för komplex it-brottslighet och barnpornografibrott ska vara klara.[115] Företrädare för Polismyndigheten menar

---

[112] Rikspolisstyrelsen (2014), *Inspektion av polismyndigheternas förmåga att handlägga IT-brott,* tillsynsrapport 2014:2, s. 10, 23; Rikspolisstyrelsen (2013), *Förstudierapport, polisens brottsbekämpande verksamhet, brott med internet-relevans,* dnr PoA480-5583/11, s. 5. Arbetssättet kan komma att ändras och göras mer enhetligt i och med det nationella processansvaret för barnpornografibrott, it-forensik och komplexa it-brott.

[113] Rikspolisstyrelsen (2013), *Förstudierapport, polisens brottsbekämpande verksamhet, brott med internet-relevans,* dnr PoA480-5583/11, s.15; telefonsamtal med Polismyndigheten 2015-08-27.

[114] Intervju med Rikspolisstyrelsen 2014-11-17.

[115] E-post från Polismyndigheten 2015-10-12.

att det även finns planer på att lägga till it-aspekten som en del av PNU, men att detta ännu inte är åtgärdat.[116]

Åklagarmyndigheten genomförde under 2014 en inventering av de utmaningar som finns rörande it-relaterade brottsutredningar. Myndigheten identifierade då att det fanns ett behov av strukturerad information för åklagare om att handlägga it-relaterade brott. Med anledning av detta ska en webbaserad guide med frekvent förekommande frågeställningar bland åklagare tas fram till december 2015.[117] Riksrevisionens enkät visar att fem av sju åklagarområden saknar kunskap om huruvida det finns handböcker för it-relaterade brott. Områdena Stockholm och Bergslagen anger att det finns ett antal promemorior och handböcker där frågor kring vissa it-relaterade brott tas upp.

4.2 Specialiserade enheter kan vara en framgångsfaktor

Riksrevisionens aktgranskning visar att 92 procent av de personuppklarade förundersökningarna utreddes vid en specialiserad enhet, jämfört med 30 procent för de nedlagda förundersökningarna. Till exempel utreddes bedrägeriärendena ofta vid bedrägerisektioner. Specialiserade enheter får i princip alla ärenden som hör till den brottstyp de är specialiserade på. Undantag kan dock förekomma, till exempel om ärendet ska utredas tillsammans med ett annat, redan pågående, ärende.[118]

Enligt Riksrevisionens enkät har tre av sju polisregioner (Öst, Stockholm och Nord) i nuläget särskilda arbetsgrupper för bedrägerier, dataintrång och barnpornografibrott. Region Mitt har endast en arbetsgrupp för bedrägeriärenden, medan övriga regioner inte har några sådana arbetsgrupper eller enheter.

Riksrevisionens referensgrupp menar att specialisering vid utredningsarbetet borde förbättra förutsättningarna för att klara upp brott. Den menar också att det vore bra att i högre utsträckning arbeta i mer eller mindre fasta team där samtliga nödvändiga kompetenser finns samlade.[119]

---

[116] Telefonintervju med Polismyndigheten 2015-10-07.

[117] Åklagarmyndigheten (2014), *Verksamhetsplan 2015,* ÅM-A 2014/1784, s. 13f.

[118] E-post från Polismyndigheten 2015-11-06.

[119] Gruppdiskussion med Riksrevisionens referensgrupp 2015-09-23.

4.3 Den tekniska utrustningen är sällan ett hinder

Riksrevisionens enkät till polisregionerna visar att den tekniska utrustningen sällan är ett hinder för vilka it-forensiska undersökningar de kan göra, men att det finns förbättringspotential. I region Syd menar man att den tekniska utrustningen aldrig utgör ett hinder för it-forensiska undersökningar. Två regioner uppger att den ibland är ett hinder, medan fyra av sju regioner uppger att den mer sällan är ett hinder. Det är främst utrustning för att undersöka mobiltelefoner som saknas i polisregionerna. I intervjuer uppger dock företrädare för Polismyndigheten och Åklagarmyndigheten att den befintliga tekniska utrustningen inte har tillräcklig kapacitet för att hantera den stora mängd undersökningar som behöver göras.[120] Företrädare för Polismyndigheten anser även att den treåriga planeringen inom it-avdelningen försvårar möjligheterna att göra nödvändiga inköp av ny utrustning med kort varsel.[121] Om viss teknisk utrustning saknas i polisregionerna kan de begära biträde från Nationella operativa avdelningen (Noa) eller Nationellt forensiskt center (NFC), men detta görs inte alltid då man vid en andra bedömning ofta kommer fram till att undersökningen inte är nödvändig.[122]

4.4 Sammanfattande iakttagelser

Vedertagna nationella riktlinjer och metodstöd saknas

- Det saknas nationella riktlinjer och metodstöd inom Polismyndigheten för hur it-relaterade brott ska utredas. It-aspekten finns inte heller med i Polisens nationella utredningskoncept (PNU).
- Inom Åklagarmyndigheten finns ett antal vägledningar där frågor avseende vissa it-relaterade brott tas upp, men dessa tycks inte vara kända i hela organisationen.

Specialiserade enheter kan vara en framgångsfaktor

- Specialiserade enheter kan ge bättre förutsättningar för uppklaring, men få polisregioner har i dag specialiserade enheter för bedrägerier, barnpornografibrott eller dataintrång.

---

[120] Intervju med Polismyndigheten 2015-03-24; intervjuer med Åklagarmyndigheten 2014-11-20 och 2015-03-12.

[121] Intervju med Rikspolisstyrelsen 2014-11-17.

[122] Riksrevisionens enkät till polisregionerna. Den operativa brottsutredande verksamheten sker i första hand i polisregionerna. Noa och NFC har dock tillgång till teknisk utrustning och fördjupad specialistkunskap som polisregionerna saknar och kan vid behov vara ett stöd i det brottsutredande arbetet.

Den tekniska utrustningen är sällan ett hinder

- Den tekniska utrustningen är sällan ett hinder för att utreda it-relaterade brott. Det finns dock förbättringspotential, särskilt avseende undersökningar av mobiltelefoner och kapacitet för att hantera antalet undersökningar och stora mängder data.

5 Kompetensförsörjningen inom it-området

I detta kapitel redovisas Riksrevisionens iakttagelser av Polismyndighetens och Åklagarmyndighetens arbete med kompetensförsörjningen avseende handläggning av it-relaterade brott. Iakttagelserna bygger främst på enkäter som besvarats av samtliga polisregioner och åklagarområden, samt på intervjuer och tidigare studier.

Både European Cybercrime Centre (EC3) och flera länder har konstaterat att den ökande användningen av informationsteknik i brottsligt syfte ställer krav på särskild kompetens inom rättsväsendets myndigheter. De rekommenderar myndigheterna att säkerställa både en grundläggande kompetens inom it-området hos flertalet medarbetare, samt nödvändig specialistkompetens (se bilaga 1). Regeringen bedömer att myndigheterna arbetar aktivt med sin kompetensförsörjning, men framhåller att deras strategiska kompetensförsörjning måste fortsätta att utvecklas för att kunna möta framtida utmaningar.[123]

5.1 Polismyndigheten

I den nya Polismyndigheten är ansvaret för kompetensförsörjningen samlat hos en gemensam HR-avdelning. All utbildning ska ingå i myndighetens kompetensutvecklingsplan med en gemensam budget för utbildningsinsatser inom Polismyndigheten.[124] Den senaste dokumenterade strategin för kompetensförsörjning gäller för perioden 2013–2017.[125] På nationell nivå ansvarar man för att identifiera nationella utvecklingsbehov utifrån förändringar i samhället och regionernas kompetensförsörjningsplaner. Man ansvarar även för att analysera kompetensförsörjningens betydelse för förmågan att förbättra verksamhetens resultat. Varje polisregion ska årligen ta fram en kompetensförsörjningsplan utifrån en analys av verksamhetens och medarbetarnas behov. Två av sju polisregioner har tagit fram kompetensförsörjningsplaner i vilka de redovisar behovet av antal platser per termin och kurstillfälle.

---

[123] Prop. 2015/16:1, utgiftsområde 4, s. 56.

[124] E-post från Polismyndigheten 2015-11-17.

[125] Polismyndighetens strategi för kompetensförsörjning, 2015-01-01, PM 2015:7, Saknr 759. I strategin pekas tre övergripande utvecklingsområden ut; 1) Genomföra uppdraget professionellt och skapa förtroende 2) Synlighet och tillgänglighet 3) En flexibel verksamhet för att lösa uppdraget.

5.1.1 *Bristande it-kompetens inom Polismyndigheten*

Riksrevisionen kan konstatera att det finns ett stort behov av kompetensutveckling för flera personalkategorier inom Polismyndigheten. Rikspolisstyrelsen har både i en förstudierapport från 2013, och under en inspektion samma år, påvisat problem vad gäller Polisens handläggning av brott med it- och internetrelevans. Det konstaterades bland annat att kompetensnivån är alltför låg på samtliga nivåer: hos de som tar emot anmälningar, de som genomför utredningar, förundersökningsledarna, de befattningshavare som genomför aktiviteter på internet samt hos arbetsledarna för inhämtningsverksamheten.[126] Spetskompetensen uppfattas vara mycket god hos it-forensiker och en mindre grupp mer specialiserade medarbetare, men man framhåller att detta inte är tillräckligt. Rikspolisstyrelsen konstaterar både i en förstudierapport och en tillsynsrapport att bristande kompetens riskerar att leda till att ärenden inte tas om hand på ett korrekt sätt, det är onödigt långa utredningar, det tas felaktiga operativa beslut, arbetsledningen är passiv, essentiella bevis säkras inte, metoder som skulle kunna föra utredningen framåt används inte och rättstryggheten minskar. I såväl förstudierapporten som i intervjuer med företrädare för Polismyndigheten lyfter man fram ett behov av en omedelbar kompetenshöjning vad gäller grundläggande kunskaper inom it-området för alla anställda inom myndigheten.[127]

Flera företrädare för Polismyndigheten och Polishögskolan lyfter fram att kompetensen för att utreda it-relaterad brottslighet är otillräcklig eller nästintill obefintlig hos flertalet utredare och förundersökningsledare.[128] I Riksrevisionens enkät uppger samtliga polisregioner att de flesta förundersökningsledare och utredare, som inte är särskilda it-utredare, saknar utbildning inom it-området, alternativt att vissa har gått enstaka kurser eller är självlärda. Inga av dessa har gått någon fördjupad utbildning inom it-området. Inte någon polisregion hävdar att det finns krav på att ha genomgått särskild utbildning inom it-området för förundersökningsledare. Det finns heller inga krav på utredare att ha genomgått särskild utbildning inom it-området för att utreda it-relaterad brottslighet. Undantaget är enligt region Öst utredning av barnpornografibrott som kräver särskild utbildning. Region Mitt framhåller att krav på utbildning inom it-området vore önskvärt och lämpligt. Flera

---

[126] Rikspolisstyrelsen (2014), *Inspektion av polismyndigheternas förmåga att handlägga IT-brott*, tillsynsrapport 2014:2; Rikspolisstyrelsen (2013), *Förstudierapport, polisens brottsbekämpande verksamhet, brott med internet-relevans,* dnr PoA480-5583/11, s. 4, 7–8; Brå (2013), *Bestämmelsen om kontakt med barn i sexuellt syfte,* rapport 2013:14, s. 24, 72.

[127] Rikspolisstyrelsen (2014), *Inspektion av polismyndigheternas förmåga att handlägga IT-brott,* tillsynsrapport 2014:2, s. 1; Rikspolisstyrelsen (2013), *Förstudierapport, polisens brottsbekämpande verksamhet, brott med internet-relevans,* dnr PoA480-5583/11, s. 7-8; intervju med Rikspolisstyrelsen 2014-11-17; intervju med Polishögskolan 2014-11-18.

[128] Intervju med Rikspolisstyrelsen 2014-11-17; intervju med Polishögskolan 2014-11-18; intervju med Polismyndigheten 2015-03-16.

företrädare för Polismyndigheten menar att det i hög grad är det egna intresset som styr medarbetarnas kompetensutveckling, i stället för det faktiska behovet av utbildningsinsatser inom myndigheten.[129]

Det finns ett utbildningsbehov bland it-forensiker

Riksrevisionens enkät visar att it-forensiker finns i alla polisregioner. I region Stockholm finns de både på regionnivå och polisområdesnivå. It-forensiker finns även i det nybildade nationella it-brottscentret. Det ser däremot olika ut i regionerna vilken utbildning dessa personer har. Fem regioner uppger att samtliga eller en majoritet av it-forensikerna har genomgått fördjupad utbildning inom it-forensik eller motsvarande. I region Bergslagen har it-forensikerna endast genomgått enstaka kurser. I region Syd är hälften av it-forensikerna självlärda medan övriga saknar uppdaterad utbildning. Region Syd menar att besparingar under de senaste åren har slagit särskilt hårt mot it-forensiken och att regionen i dag lider svårt av att kompetens saknas på området. Enbart regionerna Väst och Syd menar att det finns krav på utbildning för it-forensiker.

Särskilt utpekade it-utredare saknar utbildning

Riksrevisionen kan konstatera att det finns förhållandevis få särskilt utpekade it-utredare inom Polismyndigheten, det vill säga personer som är särskilt kunniga inom it-relaterad brottslighet och i huvudsak utreder denna typ av brott. Riksrevisionens enkät visar att tre av sju polisregioner har särskilt utpekade it-utredare på regionnivå. I region Stockholm finns totalt fem it-utredare, i region Mitt tre och i region Öst nio. I region Öst uppges samtliga it-utredare vara barnpornografiutredare. I regionerna Bergslagen, Nord och Syd har man inga särskilt utpekade it-utredare. Inte någon av it-utredarna har gått mer än enstaka kurser inom it-området och flera av dem saknar helt utbildning inom området. I region Stockholm och region Mitt har alla särskilt utpekade it-utredare genomgått enstaka kurser inom it-området. I region Öst har en fjärdedel av dem genomgått utbildning inom granskning av barnpornografi. I region Nord har it-brottsutredare sedan tidigare varit personer med så kallade multikompetenser som utreder flera ärendetyper. Region Nord har valt att ha regional samordning men utredarna sitter ute i polisområdena. Kompetensnivån för utredare med multikompetenser uppges se olika ut och region Nord framhåller därför att det finns en tydlig utvecklingspotential inom området, bland annat behöver kompetensen om it-forensiskt material förbättras bland förundersökningsledare. I region Väst har det tidigare inte ansetts tillräckligt angeläget att ha särskilt utpekade it-utredare i konkurrens med andra intressen. Men man menar att det nu finns ett behov av att bättre

[129] Intervju med Rikspolisstyrelsen 2014-11-17.

kunna hantera den ökade mängden it-bedrägerier i regionen.[130] Region Väst uppger också i enkäten att de flesta utredare i regionen har grundläggande kunskaper inom it-området, även om få utredare och förundersökningsledare har genomgått formell utbildning.

5.1.2 *Begränsat utbud av utbildningar på it-området*

Enligt företrädare för Polishögskolan har behovet av utbildning på it-området inom Polismyndigheten ökat kraftigt.[131] Svaren på Riksrevisionens enkät visar också att Polismyndighetens och Polishögskolans utbud av utbildningar inom it-området är otillräckligt för att utreda it-relaterad brottslighet.[132] Det finns en stor efterfrågan både på bredare utbildning för arbete med denna typ av brottslighet och mer specialiserade kurser. Till exempel nämns kurser inom it-spaning/internetinhämtning och fortbildning för it-forensiker. Samtidigt uppger en majoritet av polisregionerna, med undantag för region Mitt, att tidsbrist och kostnader påverkar möjligheterna att gå kurser. I region Väst menar man även att antalet utbildningsplatser i dag är för få.

Flera företrädare för Polismyndigheten menar att den nuvarande grundutbildningen vid Polishögskolan i mycket begränsad omfattning behandlar it-aspekten i brottsligheten.[133] Under 2014 gjordes en genomlysning av Polishögskolans utbud av utbildningar inom it-området eftersom det tidigare har konstaterats brister i Polisens kompetens på området.[134] Därefter föreslogs ett nytt utbildningskoncept på it-området, med en så kallad e-learningutbildning och en specialiserad utbildning med olika inriktningar och nivåer.[135] Det diskuteras även att eventuellt utvidga det nordiska

---

[130] Från och med den 1 januari 2016 kommer region Väst att samla utredning av dataintrång, datasabotage och barnpornografibrott på en ny it-brottssektion under den regionala utredningsenheten. Man kommer då att ha renodlade it-utredare för de angivna brottstyperna. it-bedrägerierna kommer att handläggas under regionala utredningsenhetens bedrägerisektion. Riksrevisionens enkät till polisregionerna samt kompletterande svar från region Väst i e-post 2015-09-04.

[131] Intervju med Polishögskolan 2014-11-18.

[132] Det finns i nuläget en baskurs om internetinhämtning, översiktskurser i it-forensik för förundersökningsledare och utredare, en kurs i utredning av sexuella övergrepp mot barn och en i immaterialrättsliga brott via internet, samt kurser i it-forensik och olika programvaror. E-post från Polishögskolan 2015-11-10.

[133] Gruppdiskussion med Riksrevisionens referensgrupp 2015-09-23; intervju med Polishögskolan 2014-11-18. Polisstuderande i Växjö har möjlighet att välja en viss inriktning och läsa fyra timmar om utredning av it-relaterade brott. I övrigt ingår en föreläsning av it-forensiker, dock inte på utbildningen i Umeå, samt en föreläsning om it-säkerhet och Polisens policy om sociala medier.

[134] Se Rikspolisstyrelsen (2013), *Förstudierapport, polisens brottsbekämpande verksamhet, brott med internet-relevans,* dnr PoA480-5583/11.

[135] Enligt förslaget ska det finnas tre olika inriktningar i tre olika nivåer. Den grundläggande nivån är öppen för samtliga operativa medarbetare inom Polismyndigheten, medan den högsta nivån främst kommer ges till personal på specialisttjänster på regional eller nationell nivå.

utbildningssamarbetet på it-området. Det finns dock ännu inga beslut om huruvida förslagen ska genomföras.[136]

5.2 Åklagarmyndigheten

Åklagarmyndighetens utbildningscentrum har det nationella ansvaret för att ta fram ett lämpligt kursutbud utifrån behov och inventeringar i åklagarområdena. Medarbetare vid Åklagarmyndigheten har ett eget ansvar för att utveckla sin kompetens och cheferna ska se till att de ges möjlighet till detta.[137]

5.2.1 Bristande it-kompetens bland åklagare

Åklagarmyndigheten framhåller i sitt budgetunderlag för 2015–2017 att brott i it-miljö ställer höga krav på åklagarna och att myndigheten måste ha möjlighet att långsiktigt satsa resurser för att kunna hantera den fortsatta utvecklingen. Det ska bland annat ske genom en satsning på att inrätta it-specialiståklagare, något som inte finns i dag. Däremot kan åklagare arbetsledas till att ta ett större ansvar för utredningar av it-relaterade brott. Detta sker inom chefens arbetsledning och kräver inga formella beslut. Riksrevisionen frågade i enkäten till åklagarområdena om det i respektive område finns några särskilt utpekade it-åklagare. Det framkom då att det i nuläget finns sådana i fem av sju åklagarområden. Åklagarområdena Nord och Öst svarade att de inte har några utpekade it-åklagare utan så kallade kontaktåklagare till nätverket för it-kunniga åklagare som bildades i mars 2015. De utpekade it-åklagarna utreder inte enbart it-relaterade ärenden. Det finns heller inga formella krav på särskild utbildning för att bli it-åklagare eller kontaktåklagare i det nyinrättade nätverket. I åklagarområde Syd har hälften av it-åklagarna genomgått fördjupad utbildning inom it-området, medan de i övriga sex åklagarområden har gått enstaka kurser. För andra åklagare som inte har denna inriktning varierar utbildningsnivån inom it-området. En bred majoritet av åklagarna saknar utbildning inom it-området; de är oftast självlärda och endast ett fåtal har fördjupad utbildning.[138] Åklagarmyndigheten framhåller i faktagranskningen att alla kontaktåklagare i nätverket har genomgått vidareutbildning på området.

---

[136] Intervju med Polishögskolan 2014-11-18; telefonsamtal med Polismyndigheten 2015-08-27; e-post från Polismyndigheten 2014-12-08.

[137] Åklagarmyndigheten (2012), *Åklagarmyndighetens riktlinjer. Åklagarmyndighetens plan för utbildning och kompetensutveckling*, ÅMR 2012:2.

[138] Riksrevisionens enkät till åklagarområdena.

5.2.2 *Utbildningarna inom it-området kan utvecklas*

Riksrevisionens enkät visar att fem av sju åklagarområden efterfrågar mer specialistutbildningar inom it-området, fler utbildningstillfällen och en utveckling av de it-relaterade inslagen i grundutbildningen. Åklagarområdena Mitt och Väst anser dock att utbildningsutbudet är tillräckligt. Även i intervjuer menar flera företrädare för Åklagarmyndigheten att mer kontinuerlig fortbildning och fler utbildningsnivåer mellan grundutbildningen och specialistutbildningen behövs.[139] I nuläget finns det inom myndigheten en vidareutbildning på området, ”It-brott och bevissäkring i it-miljö”, som ges två gånger per år. Det finns även andra kurser som berör området utan att handla om det specifikt. Enligt Riksrevisionens enkät anser fem av sju åklagarområden att det finns hinder för att delta i utbildningar inom it-området. Hindren som anges är främst kostnader, platsbrist på utbildningarna och tidsbrist.

5.3 Sammanfattande iakttagelser

- Kompetensen inom it-området är låg inom stora delar av Polismyndigheten och Åklagarmyndigheten, även om spetskompetensen anses vara mycket god hos en mindre grupp medarbetare.
  - Utredare och förundersökningsledare saknar ofta utbildning inom it-området, ingen av dem har gått fördjupad utbildning inom området.
  - Alla polisregioner har it-forensiker och en majoritet av dessa har gått fördjupade kurser inom it-området, men även här uppges det finnas ett behov av kontinuerlig fortbildning.
  - Det finns förhållandevis få särskilt utpekade it-utredare respektive it-åklagare, och deras utbildningsnivå är generellt låg.
- Utbildningsutbudet på it-området anses otillräckligt inom både Polismyndigheten och Åklagarmyndigheten. Polisregionerna och flertalet åklagarområden efterfrågar både mer av grundläggande utbildning för utredning av it-relaterade brott och specialiserade kurser, till exempel inom internetinhämtning och it-forensik.
- Hinder som uppges för att gå de utbildningar som finns är främst tidsbrist, kostnader och att antalet utbildningsplatser är för få.

[139] Intervjuer med Åklagarmyndigheten 2014-11-10 och 2014-11-14.

6 Samarbete och samverkan

I detta kapitel redovisas vilka strukturer det finns för samarbete och samverkan inom området, samt iakttagelser avseende de svårigheter som finns för ett effektivt samarbete och samverkan. Riksrevisionens enkäter till samtliga polisregioner och åklagarområden och intervjuer med företrädare för myndigheterna ligger till grund för dessa iakttagelser.

Samverkan är viktigt i utredningar av it-relaterade brott. Ett behov av stärkt samverkan har identifierats både av European Cybercrime Centre och av flera länder (se bilaga 1). Till exempel behövs samverkan mellan olika polisregioner nationellt då förövare och offer i it-relaterad brottslighet inte nödvändigtvis befinner sig på samma plats geografiskt. Samma förövare begår ofta flera brott som anmäls till olika polisregioner. För att handläggningen ska bli effektiv och dubbelarbete undvikas bör dessa förundersökningar samordnas.[140] Den privata sektorn genomför i allt större utsträckning övervakning på internet och tar emot rapporter om oegentligheter från företag och privatpersoner.[141] Ett brett samarbete med den privata sektorn, både i Sverige och i andra länder, blir därför allt viktigare för att utbyta information om trender inom teknikutvecklingen och för att inhämta nödvändiga bevis, såsom information om användare av olika internetbaserade tjänster och IP-nummer.[142] Brottens internationella karaktär ställer även krav på internationellt samarbete. Regeringen har konstaterat att myndigheterna behöver utveckla sin samverkan med privata aktörer för att kunna bemöta brottslighet på internet.[143]

---

[140] Rikspolisstyrelsen (2013), *Förstudierapport, polisens brottsbekämpande verksamhet, brott med internet-relevans,* dnr PoA480-5583/11, s. 8; intervju med Åklagarmyndigheten 2014-11-14; intervju med Rikspolisstyrelsen 2014-11-17.

[141] Wall, David (2007/11),"Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (Revised Feb. 2011)", *Police Practice & Research: An International Journal,* 8(2): 183 205; Politiet, Politidirektoratet, Norge (2015), Datakrimstrategien, s. 56, 60.

[142] Intervju med Rikspolisstyrelsen 2014-11-17; intervjuer med Polismyndigheten 2015-03-12 och 2015-03-16.

[143] Prop. 2014/15:1 utgiftsområde 4, s. 18.

6.1 Kontaktvägarna inom och mellan myndigheterna kan förbättras

Företrädare för Polismyndigheten framhåller att det ofta är svårt att nå ut i polisorganisationen då det inte är tydligt vem man ska vända sig till. Kontaktvägar bygger ofta på personliga kontakter och nätverk.[144]

Riksrevisionens enkät till polisregionerna visar att regionerna har olika uppfattningar om hur biträde begärs mellan polisregionerna. Några polisregioner uppger att det inte finns några fasta procedurer för hur detta ska göras, medan andra menar att det finns standardiserade nationella procedurer där Nationella operativa avdelningen, Noa, ansvarar för samtliga förfrågningar. Vidare visar enkäten att det är tydligare hur biträde begärs från Noa. Tre av sju polisregioner (regionerna Mitt, Syd och Väst) uppger dock att det är otydligt när Noa ska kopplas in i utredningarna. Polisregionerna uppger att biträde från Noa främst begärs när regionerna saknar nödvändig teknisk utrustning för att göra en viss undersökning, och vid internationella kontakter, till exempel med utländska företag mot vilka Noa är den fasta kontaktpunkten. Region Mitt menar dock att det finns ett motstånd mot att begära biträde från Noa eftersom det är otydligt när Noa ska träda in. Polisen har i egna studier konstaterat att nationell samordning saknas, samt att den regionala samverkan inom Polisen är bristfällig. Detta riskerar att leda till att Polismyndighetens samlade resurser och kompetenser inte används fullt ut.[145] Samverkansstrukturerna kan komma att ändras i och med den nya Polismyndigheten, och det går i dagsläget inte att säga hur samverkan kommer att fungera i praktiken i den nya organisationen.

Åklagarmyndigheten har saknat en fast struktur för utbyte av erfarenheter inom it-området mellan åklagarområdena. För att åtgärda detta inrättades i mars 2015 ett nationellt nätverk med totalt 16 it-kunniga åklagare.[146] Det framkommer samtidigt att det finns svårigheter med att överföra ärenden mellan åklagarområdena, bland annat på grund av hög arbetsbelastning.[147] Företrädare för Åklagarmyndigheten framhåller även att det ibland är svårt att få gehör inom Polismyndigheten för att genomföra de åtgärder som den förundersökningsledande åklagaren begär. En förklaring som ges till detta är att Polismyndigheten i vissa fall prioriterar annorlunda mellan ärendena. Det framkommer även att samarbetet mellan myndigheterna skulle kunna underlättas om man arbetade i team och om det fanns särskilda resurser för vissa ärenden eller brottstyper.[148]

---

[144] Intervju med Rikspolisstyrelsen 2014-11-17; intervju med Polismyndigheten 2015-03-16.

[145] Rikspolisstyrelsen (2013), *Förstudierapport, polisens brottsbekämpande verksamhet, brott med internet-relevans,* dnr PoA480-5583/11, s. 4, 8; Rikspolisstyrelsen (2014), *Inspektion av polismyndigheternas förmåga att handlägga IT-brott,* tillsynsrapport 2014:2, s. 10.

[146] E-post från Åklagarmyndigheten 2015-09-04. Nätverket består av två kontaktåklagare från varje åklagarområde och Nationella avdelningen.

[147] Gruppdiskussion med Riksrevisionens referensgrupp 2015-09-23.

[148] Intervjuer med Åklagarmyndigheten 2014-11-10, 2014-11-20, 2015-03-09 och 2015-03-12.

6.2 Det internationella samarbetet är tidskrävande

Internationellt rättsligt samarbete avser olika former av samarbete i rättsliga frågor mellan stater. Det grundar sig huvudsakligen på internationella konventioner och avtal som förhandlats fram inom Europarådet och FN. Ofta sker det internationella samarbetet genom så kallad internationell rättslig hjälp i brottmål.[149] Flera företrädare för Polismyndigheten och Åklagarmyndigheten lyfter fram att det ofta tar lång tid att få internationell rättslig hjälp. Procedurerna kring den internationella rättsliga hjälpen bedöms vara komplicerade, och vissa länder är ovilliga att samarbeta. Detta är något som kriminella personer utnyttjar genom att exempelvis placera servrar i dessa länder.[150] Eftersom internationell rättslig hjälp aldrig begärdes i de ärenden som ingick i aktgranskningen har Riksrevisionen inte kunnat belägga hur lång tid den tar. Företrädare för Polismyndigheten och Åklagarmyndigheten menar att det är oklart vart man ska vända sig internationellt för att få hjälp från andra länder. Ofta vänder man sig till någon som man känner sedan tidigare. Ett utökat och förenklat internationellt samarbete efterfrågas för att förbättra förutsättningarna att lösa brott.[151]

Ett mer standardiserat internationellt samarbete förekommer inom EU och Europarådet som har underlättat den internationella samverkan (se bilaga 1). Det finns även en svensk desk, det vill säga en hjälpcentral bemannad med svensk personal, på Europol i Haag som svenska myndigheter kan vända sig till med frågor om internationell hjälp eller förmedling av kontakter i andra länder. Det finns ingen förd statistik över frågor som inkommer till den svenska desken, men företrädare för den menar att svensk polis skulle kunna utnyttja deras hjälp i större utsträckning. Det finns en uppfattning att kunskapen om desken generellt är låg inom Polismyndigheten.[152]

Vidare kan reglerna för internationell rättslig hjälp försvåra att information inhämtas från utländska företag. Huruvida man kan kontakta utländska företag direkt eller om frågan måste gå via nationella myndigheter i andra länder

---

[149] Detta innebär att ett lands rättsväsende begär bistånd från ett annat lands rättsväsende med en viss del av en utredning, såsom att ta fram vissa bevis eller att hålla förhör. Möjligheterna till internationell rättslig hjälp regleras genom olika avtal samt de berörda ländernas lagstiftningar. Grundläggande bestämmelser om rättslig hjälp finns i lagen (2000:562) om internationell rättsligt hjälp i brottmål.

[150] Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014*, s. 11; intervju med EC3 2015-06-02, intervju med Polismyndigheten 2015-03-12, intervjuer med Åklagarmyndigheten 2014-11-10, 2015-03-09 och 2015-03-13; Politiet, Politidirektoratet, Norge (2015), *Datakrimstrategien*, s. 142f.

[151] Intervju med Åklagarmyndigheten 2014-11-14; intervju med Polismyndigheten 2015-03-12.

[152] Samtal med företrädare för den svenska desken vid Europol 2015-06-02.

beror på den efterfrågade informationen.[153] Företrädare för Polismyndigheten menar att det kan vara svårt och ta tid att få den hjälp som behövs från företag, särskilt om företagen befinner sig utanför EU och om internationell rättslig hjälp behövs. Polismyndigheten har utvecklat en samsyn för samarbete med vissa utländska företag som levererar internetbaserade tjänster, från vilka det ofta behövs information. Noa fungerar som kontaktpunkt mellan dessa företag och Polismyndigheten. Flera företrädare för myndigheten menar att detta har underlättat kontakterna och möjligheterna att få in svar från företagen.[154]

6.3 Sammanfattande iakttagelser

- Polisregionerna har olika uppfattning om hur samarbete och samverkan mellan regionerna ska bedrivas. Det kan vara svårt att nå ut i polisorganisationen eftersom kontakter ofta bygger på personliga nätverk. Det är också delvis otydligt när Nationella operativa avdelningen ska kopplas in.
- Strukturerna inom Åklagarmyndigheten för utbyte av erfarenheter mellan it-kunniga åklagare har förtydligats något med det nationella nätverket.
- Den internationella rättsliga hjälpen upplevs ta lång tid och vara administrativt komplicerad. Inom EU finns mer utbyggda strukturer för samverkan. Alla möjligheter till internationell hjälp, till exempel den svenska desken vid Europol i Haag, verkar dock inte utnyttjas fullt ut.
- Samsyn mellan Polismyndigheten och utländska privata företag har underlättat arbetet.

[153] Användaruppgifter kan normalt begäras direkt från det enskilda företaget, med undantag från i vissa länder, till exempel Kanada, där det finns nationella beslut om att alla utländska frågor ska behandlas via nationella myndigheter. Annan typ av inhämtning av information kräver ofta rättslig hjälp.

[154] Intervjuer med Polismyndigheten 2015-03-12 och 2015-03-16; intervju med Åklagarmyndigheten 2015-03-13; gruppdiskussion med Riksrevisionens referensgrupp 2015-09-23.

Bilaga 1. Internationell utblick

I denna bilaga redovisas exempel på internationella samarbeten samt iakttagelser och erfarenheter från fem europeiska länders hantering av den it-relaterade brottsligheten.

Väl fungerande internationell och nationell samverkan och ett utvecklat samarbete med relevanta sektorer inom det privata näringslivet är betydelsefulla komponenter i bekämpandet av den it-relaterade brottsligheten.[155] Denna brottstyp är ofta gränsöverskridande och utredningar kan ha betydande internationella inslag. Till exempel kan brottsoffer, kriminella nätverk, servrar och företag som utnyttjas i kriminellt syfte vara spridda över stora delar av världen. Samtidigt är brottsbekämpande verksamhet, jurisdiktion och normering i hög grad nationella angelägenheter. Tydliga internationella regelverk och välfungerande samarbetsformer är därför förutsättningar för att kunna utreda gränsöverskridande it-relaterad brottslighet på ett effektivt sätt.[156]

EU och andra internationella samarbeten

European Cybercrime Centre, Europol

European Cybercrime Centre (EC3) är Europeiska polisbyråns (Europol) avdelning för hantering av it-brott. EC3 är ett samarbetsorgan för EU:s medlemsstater samt ett antal andra länder och organisationer och bildades 2013 i syfte att skydda EU:s medborgare, företag och medlemsstater från brott som begås online.[157]

EC3:s uppdrag är att stödja medlemsstaternas förundersökningar, bland annat genom att koordinera insatser mellan medlemsstaterna och bistå med avdelningens särskilda kompetens, kunskap och förmågor. Europol och EC3 har inte mandat att bedriva egna förundersökningar. Avdelningen är en plattform för internationellt samarbete och ska även kunna fungera som ett nav för medlemsstaternas samlade hantering av it-relaterad brottslighet. Det handlar om att genomföra analyser av stora datamängder, att utveckla expertkompetens och sprida goda exempel samt att koordinera strategiska och operativa samarbeten med icke medlemsstater, företag, organisationer och andra internationella samarbetsorgan.[158]

---

[155] Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014*, s. 9.

[156] Ibid., s. 9, 13–14.

[157] Europeiska kommissionen KOM(2010) 0673 slutlig.

[158] Ibid.

EC3 har både en operativ och en strategisk verksamhet. Det operativa arbetet har tre fokusområden: högteknologiska brott, sexuell exploatering av barn online och betalkortsbedrägerier. De tre fokusområdena är sammankopplade genom ett cyberunderrättelseteam som identifierar hotbilder och mönster utifrån analyser av de stora mängder data som EC3 har tillgång till.[159] En särskild operativ verksamhet är Joint Cybercrime Action Taskforce (J-CAT), vilket är en samarbetsfunktion som hanterar avancerade brott och hot av stor dignitet. J-CAT består i skrivande stund av utredare från EC3 och elva länder i och utanför EU-området. Genom ett tätt samarbete samordnar man insatser och kontakter med andra aktörer samt ser till att ländernas samlade resurser används på ett effektivt sätt.[160]

EC3:s strategiska arbete är indelat i tre delar. Forensisk expertis bedriver både forsknings- och utvecklingsarbete och arbetar operativt med it-forensiska analyser. Det finns också en stödjande verksamhet som arbetar med partnerskapsfrågor och med att förebygga och sprida kunskap om it-relaterad brottslighet. Inom området strategi och utveckling arbetar EC3 med strategiska analyser, utbildningsinsatser, policyutveckling och lagstiftning.[161]

EC3:s rekommendationer till medlemsstaterna

Utifrån omfattande data om begångna brott ger EC3 i sin rapport om hot från organiserad brottslighet på internet[162] ett antal rekommendationer till medlemsstaterna och deras brottsbekämpande myndigheter. Här följer en sammanfattning av ett urval rekommendationer om förebyggande verksamhet, samarbetsformer och utredningsarbete.

I det förebyggande arbetet rekommenderar EC3 medlemsstaterna att höja medvetandegraden hos medborgare och företag, gärna i samarbete med privat sektor. De brottsbekämpande myndigheterna bör dessutom öka sin synlighet och närvaro på internet. För att kunna bemöta brottsligheten rekommenderas de brottsbekämpande myndigheterna säkerställa att de har nödvändig kompetens, expertis och verktyg för att utreda it-relaterad brottslighet. Förutom expertkunskapen bör det även finnas baskunskap brett i organisationen. Det bör också finnas mer specialiserade team som hanterar internationella utredningar – vilka idealiskt sett koordineras och samordnas på EU-nivå.[163]

Vad gäller samarbete framhålls vikten både av samarbete mellan myndigheter och näringslivet och av internationellt samarbete mellan myndigheter. I och med den gränsöverskridande dimensionen ställs nya krav på lagstiftning och policyer, där en harmonisering av lagstiftningen inom EU samt utvidgade internationella samarbeten

---

[159] Europol EC3 (2015), *Organisational chart;* intervju med EC3, Europol 2015-06-02.

[160] Intervju med EC3, Europol 2015-06-02; Europol, Joint Cybercrime Action Taskforce (J-CAT), https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat (hämtad 2015-10-08).

[161] Europol EC3 (2015), *Organisational chart;* intervju med EC3, Europol 2015-06-02.

[162] iOCTA (Internet Organised Crime Threat Assessment). Rapporten är EC3:s huvudsakliga strategiska dokument och är ett resultat av ett omfattande underlag från hela verksamheten.

[163] Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014*, s. 13f, 28, 34, 40, 44.

behövs. Alla relevanta aktörer bör engageras i internationella strategiska och operationella samarbeten och det krävs diversifierade och flexibla angreppssätt. De nationella myndigheterna bör dra nytta av de samarbetsformer som finns, såsom EC3. Samarbetet med länder med en hög frekvens av kriminell aktivitet på området bör enligt EC3 utvecklas. Det krävs även ett säkert sätt att dela information om brottsligheten och erfarenheter internationellt. Utbytet av information bör också utvidgas och det rekommenderas att EC3 används som ett centralt informationsnav. Utöver harmonisering rekommenderar EC3 även att lagstiftare ger rättsväsendet nödvändiga befogenheter för att hindra och utreda brott samt för att få tillgång till information.[164]

I det utredande arbetet rekommenderas de brottsbekämpande myndigheterna att dra nytta av den kunskap och information som finns, bland annat inom EC3, för att kunna prioritera och genomföra proaktiva och underrättelseledda insatser med fokus på särskilt strategiskt viktiga områden. Resurser kan då koordineras och användas på effektivaste sätt. De brottsbekämpande myndigheternas resurser och kompetens bör stärkas i samma takt som den tekniska utvecklingen och ökningen av it-relaterade brott. Myndigheterna måste också få förutsättningar för att bemöta den växande användningen av kryptering och anonymisering.[165]

Andra EU-byråer som hanterar it-relaterad brottslighet

Förutom Europol har EU fler decentraliserade byråer som har verksamhet kopplad till it-relaterad brottslighet.

Eurojust är i hög grad åklagarväsendets motsvarighet till Europol och har behörighet för samma sorters brott. Syftet med Eurojust är att underlätta och förbättra samordning och samarbete mellan medlemsstaterna när det gäller utredning och åtal av grov brottslighet. Eurojust ska underlätta och förbättra samordningen i utredningar som rör två eller fler medlemsstater samt bistå medlemsstaterna i rättsliga samarbeten om till exempel internationell rättslig hjälp och utlämningar.[166] Eurojust samarbetar systematiskt med EC3 och Europol i syfte att hantera it-relaterad brottslighet.[167]

It-relaterad brottslighet av typen attacker mot infrastruktur, dataintrång och cyberspionage hanteras även av aktörer utanför rättsväsendet. Europeiska unionens byrå för nät- och informationssäkerhet (ENISA) arbetar med detta på flera sätt och verkar för att stötta och stärka medlemsstaterna och andra EU-organ i arbetet med bland annat informationssäkerhet och hantering av incidenter.[168] ENISA har även

---

[164] Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014*, s. 13f, 40, 43.

[165] Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA) 2014*, s. 14, 23, 40.

[166] Prop. 2001/02:86; Bet. 2001/02:JuU19; Europeiska unionens råd, rådets beslut 2002/187/RIF, rådets beslut 2009/496/RIF.

[167] Eurojust (2015), *Årlig rapport 2014;* Eurojust (2014), *Report of the Strategic Meeting on Cybercrime. 19–20 November 2014.*

[168] Europaparlamentets och rådets förordning (EU) nr. 526/2013.

ett strategiskt samarbete med Europol och EC3 i syfte att förhindra och bekämpa it-relaterad brottslighet.[169]

Ytterligare ett exempel på samarbete mellan rättsväsenden inom EU är det Europeiska straffrättsliga nätverket (EJN), vilket består av nationella kontaktpunkter som underlättar och samordnar samarbete mellan myndigheter och länder.[170]

Andra EU-initiativ

EU:s strategi för cybersäkerhet från 2013 omfattar insatser från EU-kommissionen inom tre områden. För att främja en stärkt och effektiv lagstiftning ska kommissionen säkerställa att EU:s olika direktiv om cyberbrottslighet införlivas, samt ska kommissionen uppmana medlemsstaterna att ratificera Europarådets Budapestkonvention.[171] Inom området ökad operativ kapacitet har kommissionen finansieringsprogram[172] som syftar till att stödja medlemsstaterna i hanteringen av it-brott. De ska bland annat användas till att stärka kopplingen mellan brottsbekämpande myndigheter, forskningen och den privata sektorn, förbättra samordning av insatser och till att med stöd av EC3 anpassa strategier till bästa praxis. Det tredje området handlar om att samordningen på EU-nivå ska förbättras genom att EC3 används som en central punkt i kampen mot it-brottslighet och genom att kommissionen bygger vidare på ny lagstiftning för att stärka EU:s insatser. Kommissionen ska även göra insatser för att öka domänregistratorers ansvar och säkerställa att information om webbplatsägande är korrekt.[173]

The European Multidisciplinary Platform Against Criminal Threats (EMPACT) är en strukturerad tvärvetenskaplig samarbetsplattform för medlemsstaterna, EU-byråer och -institutioner samt några relevanta icke medlemsstater och organisationer. Plattformen är ett led i en EU-policy mot organiserad brottslighet. It-relaterad brottslighet är ett av de prioriterade områdena för perioden 2014–2017 med fokus på cyberattacker, sexuellt utnyttjande och exploatering av barn online samt betalbedrägerier. I policyn ingår även utbildningsinsatser hos Europeiska polisakademin (Cepol).[174]

---

[169] ENISA, pressmeddelande 2014-06-26, *Fighting cybercrime: Strategic cooperation agreement signed between ENISA and Europol.*

[170] Europeiska unionens råd, rådets beslut 2008/976/RIF.

[171] Europarådet, *The Convention on Cybercrime of the Council of Europe* (CETS 185).

[172] Fonden för inre säkerhet (ISF) genom förordningarna (EU) nr 513/2014 och (EU) nr 515/2014. Fonden är kopplad till EU:s budgetram 2014–2020 och ska användas för att genomföra åtgärder på nationell nivå.

[173] Europeiska kommissionen och Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik JOIN(2013) 1 slutlig, s. 9–11.

[174] Europeiska unionens råd (2014), *EU:s policycykel i kampen mot organiserad och grov internationell brottslighet;* Europeiska unionens råd, dok. 15358/10, dok. 12095/13, dok. 14518/12.

Europarådet

The Convention on Cybercrime of the Council of Europe (CETS 185), även kallad Budapestkonventionen, är i skrivande stund undertecknad av Sverige men inte ratificerad. Europarådets konvention syftar till att fastlägga riktlinjer för nationell lagstiftning på området samt vara ett ramverk för internationellt samarbete mellan de stater som har ratificerat konventionen. Som komplement till konventionen har Europarådet även uppföljningar och utvärderingar samt kapacitetsbyggande verksamhet och tekniska samarbetsprogram.[175]

Interpol

Internationella polissamarbetsorganisationen (Interpol) har cybercrime som ett särskilt prioriterat brottsområde och fokuserar på att samordna insatser och aktörer, kompetens och kapacitetsbyggande samt operationellt och forensiskt stöd. Interpol har för avsikt att tillhandahålla en global koordineringsfunktion för cybercrime genom Interpol Global Complex for Innovation (IGCI) i Singapore och avdelningen Interpol Digital Crime Centre. Centrets verksamhet omfattar forskning, utbildningar i den senaste tekniken och koordinering av specifika insatser.[176]

Hur andra länder hanterar it-relaterad brottslighet

Riksrevisionen har tittat närmare på hur fem andra länder hanterar it-relaterad brottslighet. Dessa länder är Storbritannien, Nederländerna, Finland, Danmark och Norge. Under projektgruppens besök på EC3 i Haag framhölls att Nederländerna och Storbritannien ligger i framkant när det gäller att bekämpa it-relaterad brottslighet.[177] De tre nordiska länderna valdes ut då de har flera likartade förutsättningar med Sverige. Därtill finns det ett fördjupat polisiärt samarbete mellan de nordiska länderna. EU-området är överlag ett attraktivt mål för it-relaterad brottslighet eftersom många använder internet och betalsystemen i stor utsträckning är digitaliserade.[178] Länderna skiljer sig åt sinsemellan på flera sätt och genomgående används olika motsvarigheter till begreppen it-brott och it-relaterad brottslighet. Detta medför svårigheter med att dra paralleller och göra jämförelser. Underlag från länderna visar ändå flera gemensamma problem och även några liknande tendenser i ländernas angreppssätt för att hantera dessa.

---

[175] Europarådet, Action against cybercrime, http://www.coe.int/en/web/cybercrime/home (hämtad 2015-10-08).

[176] Interpol (2015), *Digital Crime Centre Directorate;* Se även *Interpol's International Child Sexual Exploitation (ICSE) database.*

[177] Intervju med EC3, Europol 2015-06-02.

[178] Europol EC3 (2014), *The internet organised crime threat assessment (iOCTA)* 2014, s. 71.

Kompetensförsörjning och kapacitetslyft

Den centrala betydelsen av särskild kompetensförsörjning och kompetensutveckling lyfts fram av samtliga länder. Den it-relaterade brottsligheten utgör en allt större del av mängdbrotten och den ordinarie polisverksamheten behöver ha förmåga att utreda denna. Därför anses det vara viktigt att säkerställa en viss kompetensbredd inom rättsväsendet. Dessutom behövs spetskompetens för att kunna utreda särskilt komplicerade fall.[179] I Finland, Danmark och Storbritannien finns spetskompetens samlad i särskilda nationella it-brottsenheter. Dessa ska även fungera som nav för internationellt och nationellt samarbete, utvecklings- och policyfrågor m.m.[180] Även Norge står i begrepp att bilda en särskild nationell enhet.[181] I Nederländerna finns det flera specialiserade enheter inom rättsväsendet.[182]

Betydelsen av samarbete

Samtliga länder framhåller genomgående att ett gott internationellt samarbete och samverkan med den privata sektorn och med forskningen är centralt för att effektivt bekämpa den it-relaterade brottsligheten.[183] Vissa typer av it-relaterad brottslighet har tydliga kopplingar till sektorer utanför rättsväsendet. Betydelsen av informationsteknik och informationssystem gör samhällsviktig verksamhet sårbar för it-brott såsom attacker mot infrastruktur och cyberspionage.[184] I sina nationella cyber- och/eller informationssäkerhetsstrategier säkerställer länderna en viss ansvarsfördelning och

---

[179] Politi, Danmark, *Politiets virksomhedsplan 2015,* s. 4–5; Justitsministeriet & Rigspolitiet, Danmark, *Mål- og resultatplan for politiet 2015,* s. 7; e-post från Rigspolitiet, Danmark 2014-04-15; Departementene Norge (2012), *Nasjonal strategi for informasjonssikkerhet*, s. 22–23; Politiet, Politidirektoratet, Norge (2015), *Datakrimstrategien*, s. 147–158; Justis- og beredskapsdepartementet, Norge (2015), *Justis- og bereskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, s. 13–15; E-post från finländska Åklagarväsendet 2015-07-27; e-post från Nederländernas polis 2015-04-20; e-post från National Crime Agency United Kingdom 2015-08-14; Cabinet Office United Kingdom (2014), T*he UK Cyber Security Strategy. Report on Progress and Forward Plans,* s. 2, 10–11.

[180] Politi, Danmark, *Politiets virksomhedsplan 2015,* s. 4–5; Justitsministeriet & Rigspolitiet, Danmark, *Mål- og resultatplan for politiet 2015*, s. 7; Regeringen, Danmark (2014), *National strategi for cyber-og informationssikkerhed – øget professionalisering og mere viden,* s. 30; e-post från Centralkriminalpolisen, Finland 2015-07-09; e-post från National Crime Agency United Kingdom 2015-08-14.

[181] Justis- og beredskapsdepartementet, Norge (2015), *Justis- og bereskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, s. 15.

[182] E-post från Nederländernas polis 2015-04-20.

[183] Justitsministeriet & Rigspolitiet, Danmark, *Mål- og resultatplan for politiet 2015,* s. 7; Departementene Norge (2012), *Nasjonal strategi for informasjonssikkerhet* s. 22–23; Politiet, Politidirektoratet, Norge (2015), *Datakrimstrategien*; Justis- og beredskapsdepartementet, Norge (2015), *Justis- og bereskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, s. 16–17; e-post från finländska Åklagarväsendet 2015-07-27; Försvarsdepartementet, Finland (2013), *Finland's Cyber Security Strategy. Government resolution 24.1.2013,* s. 8; e-post från Nederländernas polis 2015-04-20; The National Coordinator for Security and Counterterrorism the Netherlands, *National Cyber Security Strategy 2. From awareness to capability*, s. 20–21; e-post från National Crime Agency United Kingdom 2015-08-14; Cabinet Office United Kingdom (2014), *The UK Cyber Security Strategy. Report on Progress and Forward Plans,* s. 2, 10–11.

[184] E-post från Rigspolitiet, Danmark 2015-04-15; Nasjonal sikkerhetsmyndighet, Norge, Risiko 2015; Politiet KRIPOS Norge (2014), *Trendrapport 2015. Den organiserte kriminaliteten i Norge,* s. 24–28; Politiet, Politidirektoratet, Norge (2015), *Datakrimstrategien*; e-post från Nederländernas polis 2015-04-20; the National Coordinator for Security and Counterterrorism the Netherlands, *National Cyber Security Strategy 2. From awareness to capability*, s. 20–21; e-post från National Crime Agency United Kingdom 2015-08-14.

samverkansstrukturer mellan myndigheter och andra aktörer inom rättsväsende, infrastruktur, krisberedskap, säkerhetstjänster och totalförsvar.[185] Strategierna innehåller ett antal mål eller dylikt för ländernas arbete med cyber- och/eller informationssäkerhet samt särskilda insatser kopplade till dessa. Samtliga länder har sådana mål med tillhörande insatser som särskilt syftar till att förbättra hanteringen av it-relaterad brottslighet.[186]

Att förstå och följa med i utvecklingen

Sammantaget handlar en stor del av underlagen från länderna om att säkerställa förmågan att följa med i en relativt oförutsägbar och snabb utveckling av den it-relaterade brottsligheten. En ständigt uppdaterad hotbild och god kunskap på området är nödvändigt för att effektivt kunna anpassa sådant som lagstiftning och regelverk, förutsättningar för brottsutredning såsom tillgång till metoder och tekniska verktyg samt översyner av policyer och strategier. Några exempel på insatser som syftar till att förbättra detta är förändrad brottsstatistik, system för brottssamordning, mörkertalsundersökningar, utbyggd forskning, internationellt samarbete och samverkan med den privata sektorn.[187]

---

[185] Regeringen, Danmark (2014), *National strategi for cyber-og informationssikkerhed – øget professionalisering og mere viden*; Departementene Norge (2012), *Nasjonal strategi for informasjonssikkerhet;* Försvarsdepartementet, Finland (2013), *Finland's Cyber Security Strategy. Government resolution 24.1.2013;* the National Coordinator for Security and Counterterrorism the Netherlands, *National Cyber Security Strategy 2. From awareness to capability;* Cabinet Office United Kingdom (2011), *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world;* Cabinet Office United Kingdom (2014), *The UK Cyber Security Strategy. Report on Progress and Forward Plans.*

[186] Regeringen, Danmark (2014), *National strategi for cyber-og informationssikkerhed – øget professionalisering og mere viden,* s. 28–31; Departementene Norge (2012), *Nasjonal strategi for informasjonssikkerhet* s. 22–23; Försvarsdepartementet, Finland (2013), *Finland's Cyber Security Strategy. Government resolution 24.1.2013*, s. 8; The National Coordinator for Security and Counterterrorism the Netherlands, *National Cyber Security Strategy 2. From awareness to capability,* s. 23–25, 30; Cabinet Office United Kingdom (2011), *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world,* s. 8–9, 29–31; Cabinet Office United Kingdom (2014), *The UK Cyber Security Strategy. Report on Progress and Forward Plans,* s. 2, 10–11.

[187] E-post från Rigspolitiet, Danmark 2015-04-15; Politi, Danmark, *Strategisk analyse 2015*; Politiet, Politidirektoratet, Norge (2015), *Datakrimstrategien*, s. 74–158; Justis- og beredskapsdepartementet, Norge (2015), *Justis- og bereskapsdepartementets strategi for å bekjempe IKT-kriminalitet*, s. 6–7, 12–13, 17–18; e-post från National Crime Agency United Kingdom 2015-08-14.

Bilaga 2. Metod

Intervjuer och dokumentstudier

Dokumentstudier och intervjuer har genomförts kontinuerligt under granskningen. Dokumentstudierna har omfattat bland annat regeringens och myndigheternas styrdokument, förstudier, inspektioner och tillsynsrapporter sammanställda av Polismyndigheten och Åklagarmyndigheten, offentliga utredningar inom området, samt akademisk litteratur och internationella rapporter. Den officiella kriminalstatistiken har även analyserats.

Intervjuer har genomförts med företrädare för myndigheterna, både med operativ personal och med olika ansvariga funktioner för styrning och ledning, samt med Justitiedepartementet.

Referensgrupp

En extern referensgrupp bestående av nio poliser, inklusive it-forensiker, och åklagare med kvalificerade kunskaper inom området har bistått Riksrevisionens projektgrupp med sina erfarenheter och kompetens. Referensgruppen har bland annat använts för att identifiera olika moment i förundersökningsarbetet och de särskilda förutsättningar som är utmärkande för den it-relaterade brottsligheten. Referensgruppen har också kunnat verifiera problemindikationer och deltagit i en avslutande diskussion med utgångspunkt i de iakttagelser som gjorts under granskningen.

Aktgranskning

Riksrevisionen har genomfört en aktgranskning som avser anmälda brott. Den har omfattat totalt 350 beslut om avskrivning, åtal, åtalsunderlåtelse eller strafföreläggande fattade under 2013. Syftet med aktgranskningen har varit att identifiera och analysera eventuella brister i arbetet med handläggning och utredning av it-relaterad brottslighet genom att kartlägga vilka aktörer och kompetenser som varit delaktiga under arbetet, samt hur lång tid olika moment har tagit. Riksrevisionen har i aktgranskningen undersökt förundersökningsprotokoll med tillhörande material (så kallad slask), samt åklagarbeslut och direktiv kopplade till de granskade besluten. Undersökningen har utgått från frågor som bygger på de iakttagelser och synpunkter som referensgruppen lämnat. Frågorna återges i bilaga 3 (denna bilaga publiceras bara digitalt och finns att ladda ned på Riksrevisionens webbplats www.riksrevisionen.se).

Urval och felmarginaler

Besluten som har granskats i aktgranskningen har valts ut genom ett stratifierat slumpmässigt urval inom de tre granskade brottskategorierna – it-bedrägerier, internetrelaterat barnpornografibrott och attacker mot infrastruktur. Målpopulationen delades in i två delpopulationer utifrån hur ärendet har avslutats - om åklagare har väckt åtal, utfärdat åtalsunderlåtelse eller strafföreläggande, eller om ärendet har skrivits av. Totalt 175 beslut togs fram genom ett obundet slumpmässigt urval (OSU) i respektive delpopulation. Urvalsstorleken har beslutats i samråd med en extern statistikkonsult som även har beräknat felmarginaler. Brottsförebyggande rådet har tagit fram populationsstorlekarna och även gjort urvalet utifrån grunddata från de brottsutredande myndigheterna.

Bilagetabell 1 Populationsstorlekar

Delpopulation 1, personuppklarade ärenden				Delpopulation 2, avskrivna ärenden				Totalt
Bedrägeri	Attacker mot infrastruktur	Barnpornografi	Summa delpopulation 1	Bedrägeri	Attacker mot infrastruktur	Barnpornografi	Summa delpopulation 2	Summa delpopulation 1 + 2
5 332	1 011	138	**6 481**	54 696	10 753	180	**65 629**	**72 110**

Bilagetabell 2 Urvalsstorlekar

Delpopulation 1, personuppklarade ärenden				Delpopulation 2, avskrivna ärenden				Totalt
Bedrägeri	Attacker mot infrastruktur	Barnpornografi	Summa delpopulation 1	Bedrägeri	Attacker mot infrastruktur	Barnpornografi	Summa delpopulation 2	Summa delpopulation 1 + 2
149	23	3	**175**	142	32	1	**175**	**350**

För att uppskatta viktning mellan delpopulationerna har följande formel använts.

$$\hat{p} = \frac{N_1 \times \hat{p}_1 + N_2 \times \hat{p}_2}{N_1 + N_2}$$

där

N_1 är antal beslut i delpopulation 1

N_2 är antal beslut i delpopulation 2

$\hat{p}_1$ är skattat procenttal i delpopulation 1

$\hat{p}_2$ är skattat procenttal i delpopulation 2

Bilagetabell 3 Approximativa felmarginaler för skattning av procenttal

Andel svar på ett visst sätt i en viss fråga	Felmarginal skattning i delpopulation 1 (± procent)	Felmarginal skattning i delpopulation 2 (± procent)	Felmarginal totalskattning (± procent)
10%	4,5	4,5	4,2
20%	6	6,1	5,5
30%	6,9	6,9	6,3
40%	7,3	7,4	6,8
50%	7,5	7,6	6,9
60%	7,3	7,4	6,8
70%	6,9	6,9	6,3
80%	6	6,1	5,5
90%	4,5	4,5	4,2

Anm. Felmarginalerna är beräknade med 95 procent av konfidensgrad.

Genomgång av avskrivna ärenden

För att bedöma om avskrivningsgrunderna använts enhetligt och ändamålsenligt har en konsult med åklagarkompetens på uppdrag av Riksrevisionen gjort en genomgång av de avskrivna ärendena som ingått i urvalet för aktgranskningen. Konsulten har även bedömt om mer hade kunnat göras för att nå lagföring i de avskrivna ärendena.[188] De avskrivna åklagarledda förundersökningarna har bedömts av en överåklagare vid Åklagarmyndigheten, som arbetar vid Utvecklingscentrum Stockholm. De åklagarledda

[188] Konsulten med åklagarkompetens har varit projektanställd vid Riksrevisionen under genomförandet.

ärendena har hanterats som så kallade tillsynsärenden inom Åklagarmyndigheten, i enlighet med den rättshierarki som finns.

I genomgången av de polisledda avskrivna ärendena har konsulten med åklagarkompetens utgått från följande frågor –

Fråga 1 Synes avskrivningsgrunden (-erna) stämma med omständigheterna i fallet? (Om svaret är Ja behöver inget mer fyllas i).

☐	Ja.
☐	Nej, ange vilken avskrivningsgrund som har använts och vilken som borde ha använts.
☐	Går ej att bedöma, ange varför inte.

Fråga 2 Varför borde ärendet inte ha skrivits av? Saknas det åtgärder som uppenbart och rimligen i förhållande till brottets dignitet kunde ha vidtagits? Om svaret är Ja, vilka åtgärder kunde ha vidtagits?

Fråga 3 Hade detta ärende, enligt bedömning, kunnat gå till lagföring?

☐	Ja, sannolikt.
☐	Ja, med viss sannolikhet.
☐	Nej, sannolikt inte.
☐	Det går inte att bedöma.

Fråga 4 Särskilda noteringar.

Här finns utrymme att notera uppgifter i ärendet.

Enkät till polisregioner och åklagarområden

Vi har sammanställt och analyserat en digital enkät som samtliga polisregioner och åklagarområden har besvarat. Syftet med enkäten har varit att göra en nulägesanalys över hur Polismyndigheten och Åklagarmyndigheten handlägger och utreder it-relaterade brott. Frågorna avsåg exempelvis organisation, arbetsmetoder, samverkan, samt utbildningsnivå för olika personalkategorier. Frågorna återges i bilaga 4 (denna bilaga publiceras bara digitalt och finns att ladda ned på Riksrevisionens webbplats www.riksrevisionen.se).

Övrigt

Riksrevisionen har även besökt European Cybercrime Center (EC3) i Haag i juni 2015. Syftet var att få mer kunskap om hur centret arbetar, ta del av goda exempel samt att få veta mer om förutsättningarna för internationell samverkan vid utredning av it-relaterad brottslighet. Material har även sammanställts för att se hur Storbritannien och Nederländerna, som har lyfts fram av European Cybercrime Center som mer framstående inom området, hanterar denna typ av brottslighet. Eftersom förutsättningarna är relativt lika i Norden har även Danmark, Norge och Finland studerats närmare. Detta presenteras i bilaga 1.

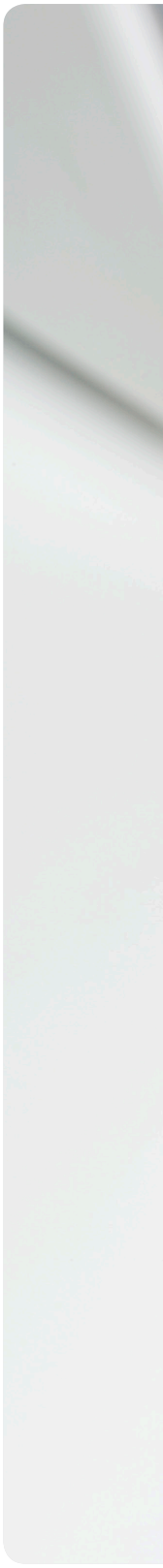
Tidigare utgivna rapporter från Riksrevisionen

Alla Riksrevisionens tidigare utgivna rapporter finns tillgängliga på www.riksrevisionen.se

2014	2014:1	Statens insatser för riskkapitalförsörjning – i senaste laget
	2014:2	Bostäder för äldre i avfolkningsorter
	2014:3	Staten och det civila samhället i integrationsarbetet
	2014:4	Försvarets omställning
	2014:5	Effekter av förändrade regler för deltidsarbetslösa
	2014:6	Att överklaga till förvaltningsrätten – Handläggningstider och information till enskilda
	2014:7	Ekonomiska förutsättningar för en fortsatt omställning av försvaret
	2014:8	Försvaret – en utmaning för staten. Granskningar inom försvarsområdet 2010–2014
	2014:9	Stödet till anhöriga omsorgsgivare
	2014:10	Förvaltningen av regionala projektmedel – delat ansvar, minskad tydlighet?
	2014:11	Att tillvarata och utveckla nyanländas kompetens – rätt insats i rätt tid?
	2014:12	Livsmedelskontrollen – tar staten sitt ansvar?
	2014:13	Att gå i pension – varför så krångligt?
	2014:14	Etableringslotsar – fungerar länken mellan individen och arbetsmarknaden?
	2014:15	Nyanländ i Sverige – effektiva insatser för ett snabbt mottagande?
	2014:16	Swedfund International AB – Är finansieringen av bolaget effektiv för staten?
	2014:17	Det allmänna pensionssystemet – en granskning av granskningen
	2014:18	Statens dimensionering av lärarutbildningen – utbildas rätt antal lärare?
	2014:19	Valuta för biståndspengarna? – valutahantering i det internationella utvecklingssamarbetet
	2014:20	Överenskommelser mellan regeringen och SKL inom hälso- och sjukvården – frivilligt att delta men svårt att tacka nej
	2014:21	Exportkreditnämnden – effektivitet i exportgarantisystemet?
	2014:22	Primärvårdens styrning – efter behov eller efterfrågan?
	2014:23	Informationssäkerheten i den civila statsförvaltningen

	2014:24	Bistånd genom internationella organisationer – UD:s hantering av det multilaterala utvecklingssamarbetet
	2014:25	Specialdestinerade statsbidrag – Ett sätt att styra mot en mer likvärdig skola?
	2014:26	Näringspolitikens effekter – Brister i informationen om statliga satsningar
	2014:27	Arbetsförmedlingens arbete vid varsel – Ett bidrag till effektiva omställningsinsatser?
2015	2015:1	Omskolad till arbete? – Utbildningsstödet till varslade vid Volvo Cars
	2015:2	Kontrollen av försvarsunderrättelseverksamheten
	2015:3	Den officiella statistiken – en rättvisande bild av samhällsutvecklingen?
	2015:4	Återfall i brott – hur kan samhällets samlade resurser användas bättre?
	2015:5	Digitalradio – varför och för vem?
	2015:6	Vattenfall – konkurrenskraftigt och ledande i energiomställningen?
	2015:7	Aktivitetsersättning – en ersättning utan aktivitet?
	2015:8	Arktiska rådet – vad Sverige kan göra för att möta rådets utmaningar
	2015:9	Granskning av Årsredovisning för staten 2014
	2015:10	Transporter av farligt avfall – fungerar tillsynen?
	2015:11	Regeringens styrning av SOS Alarm – viktigt för människors trygghet
	2015:12	Patientsäkerhet – har staten gett tillräckliga förutsättningar för en hög patientsäkerhet?
	2015:13	Regeringens jämställdhetssatsning – tillfälligheter eller långsiktiga förbättringar?
	2015:14	Överskuldsättning – hur fungerar samhällets stöd och insatser?
	2015:15	Regeringens hantering av risker i statliga bolag
	2015:16	Statens finansiella tillgångar – något att räkna med?
	2015:17	Nyanländas etablering – är statens insatser effektiva?
	2015:18	Länsstyrelsernas krisberedskapsarbete – Skydd mot olyckor, krisberedskap och civilt försvar
	2015:19	Rehabiliteringsgarantin fungerar inte – tänk om eller lägg ner
	2015:20	Gruvavfall – Ekonomiska risker för staten

Beställning: publikationsservice@riksrevisionen.se



It-relaterad brottslighet är ett växande problem och flera typer av it-relaterade brott klaras upp i mindre omfattning än andra brott. Det är viktigt att Polismyndigheten och andra delar av rättsväsendet håller jämna steg med utvecklingen för att det brottsutredande arbetet inte ska försämras. Riksrevisionen har granskat om Polismyndigheten och Åklagarmyndigheten har beredskap för att ändamålsenligt och effektivt handlägga och utreda it-relaterade brott.

Bristen på vedertagna metodstöd, utvecklade arbetssätt, tillräcklig kompetens och specialisering inom området gör att polis och åklagare inte har beredskap och förmåga att utreda och handlägga it-relaterade brott effektivt och ändamålsenligt. Bristerna riskerar också att leda till att it-relaterade brott inte hanteras likvärdigt och enhetligt, och att det i högre grad blir personberoende hur ett ärende utreds. Några typer av dataintrång och bedrägerier som sker via internet utreds i stort sett inte alls. Dessa ärenden är en del av en brottslighet där möjligheten att nå framgång i ett enskilt ärende är i det närmaste obefintlig i dag. När människor drabbas av brott och ärenden skrivs av i stället för att utredas, finns det en risk att förtroendet för rättsväsendet påverkas negativt. Myndigheterna har relativt sent börjat vidta flera åtgärder inom området. Riksrevisionens uppfattning är dock att det kommer att krävas ett långsiktigt och uthålligt arbete för att nå resultat.

ISSN 1652-6597
ISBN 978-91-7086-390-5
Beställning:
www.riksrevisionen.se
publikationsservice@riksrevisionen.se
Riksrevisionens publikationsservice
114 90 Stockholm

RIKSREVISIONEN

NYBROGATAN 55, 114 90 STOCKHOLM
08-5171 40 00
WWW.RIKSREVISIONEN.SE