Rapport 2016:17

It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem

brå

It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem

Rapport 2016:17

Brå – kunskapscentrum för rättsväsendet

Myndigheten Brå verkar för att brottsligheten minskar och tryggheten ökar i samhället. Det gör vi genom att ta fram fakta och sprida kunskap om brottslighet, brottsbekämpning och brottsförebyggande arbete, till i första hand regeringen och myndigheter inom rättsväsendet.

Publikationen finns som pdf på www.bra.se. På begäran kan Brå ta fram ett alternativt format. Frågor om alternativa format skickas till tillgangligt@bra.se

ISSN 1100-6676
ISBN 978-91-87335-74-7
URN:NBN:SE:BRA-671

© Brottsförebyggande rådet 2016
Författare: Frida Andersson, Kerstin Nelander Hedqvist, Jonas Ring, Alexandra Skarp
Produktion: Ordförrådet AB
Omslag: Maria Westberg
Tryck: Lenanders Grafiska AB

Brottsförebyggande rådet, Box 1386, 111 93 Stockholm
Telefon 08–527 58 400, e-post info@bra.se, www.bra.se

Denna rapport kan beställas hos bokhandeln eller hos Wolters Kluwer, 106 47 Stockholm
Telefon 08–598 191 90, fax 08–598 191 91, e-post kundservice@wolterskluwer.se

Förord

Brottsförebyggande rådet fick 2015 i uppdrag av regeringen att genomföra en studie om it-relaterad brottslighet. Bakgrunden är att det saknas en bild av hur utvecklingen har sett ut, samt vilken kompetens och kapacitet som finns inom rättsväsendet för att hantera brott med it-inslag. I uppdraget ingick även att se över möjligheterna att utforma ett statistiskt system för att framöver kunna följa utvecklingen av it-inslag i de anmälda brotten.

Studien baseras på ett flertal olika datakällor, bland annat en genomgång av polisanmälningar, enkäter till operativa åklagare, polisiära förundersökningsledare och it-undersökare samt intervjuer. Rapporten belyser brister inom de brottsutredande myndigheterna vad gäller förmågan att hantera it-relaterad brottslighet samt lyfter fram ett antal angelägna utvecklingsområden. Rapporten vänder sig i första hand till personer verksamma inom Polismyndigheten och Åklagarmyndigheten, men även till forskare och övriga intresserade inom rättsväsendet.

Rapporten har författats av fil. dr Frida Andersson, utredaren Kerstin Nelander Hedqvist, fil. dr Jonas Ring och projektassistent Alexandra Skarp, samtliga verksamma på Brå. Peter Zvejnieks, Melai Lehkamo och Joanna Carlestål har deltagit i arbetet med kodning respektive transkribering.

Rapporten har vetenskapligt granskats av professor emeritus Sven-Åke Lindgren, Göteborgs universitet. En rad andra sakområdesexperter har också granskat olika delar av rapporten.

Brå vill rikta ett stort tack till de personer inom rättsväsendet som har delat med sig av sina erfarenheter och kunskaper genom intervjuer och genom att delta i Brås enkätundersökning. Brå vill slutligen särskilt tacka Åklagarmyndighetens Utvecklingscentrum och Utbildningscentrum, Nationellt forensiskt centrum (NFC), Nationella operativa avdelningen (Noa) samt Polismyndighetens HR-avdelning för värdefulla synpunkter under projektets gång.

Stockholm i september 2016

Erik Wennerström
Generaldirektör

David Shannon
Tillförordnad enhetschef

Innehåll

Sammanfattning[1]

I takt med den ökade användningen av informationsteknologi (it) i samhället öppnar sig nya arenor för brottsligheten. Brott som per definition är kopplade till it (t.ex. dataintrång) kan förväntas öka, men det innebär också att vissa traditionella brott (t.ex. olaga hot) kan flytta in i it-miljö. Den ökande användningen av informationsteknologi i samhället innebär också att människor lämnar allt fler digitala spår efter sig, vilket kan ha betydelse vid brottsutredningar vid all typ av brottslighet.

I regleringsbrevet för år 2015 fick Brå i uppdrag av regeringen att kartlägga utvecklingen när det gäller förekomsten av it-inslag i de anmälda brotten. Kartläggningen skulle avse utvecklingen sedan år 2006 och innehålla såväl brott mot person som andra relevanta brottstyper. Brå skulle även analysera kompetens och kapacitet vad gäller it-relaterad brottslighet och forensiska it-undersökningar i den brottsutredande verksamheten. I det ingick att belysa brister och utvecklingsmöjligheter. Brå skulle slutligen överväga möjligheterna att utveckla ett system som ger rättsväsendets myndigheter ett statistiskt underlag för att framöver följa utvecklingen av it-inslag i de anmälda brotten, och i så fall föreslå hur systemet borde utformas.

Metod

It-relaterad brottslighet inkluderar, enligt den definition som används i rapporten, all typ av brottslighet där informationsteknologi är närvarande på någon av följande tre nivåer:

1. It är *målet* och en förutsättning för brottets genomförande, till exempel dataintrång.
2. It är *medlet* och har understött brottet, till exempel genom att ett socialt forum används för att hota någon.

[1] En engelsk version av denna sammanfattning finns på Brås webbplats, www.bra.se. Klicka där på fliken *Publikationer*, och skriv sedan in rapportnumret i sökfältet.

It kan, utan att vara mål eller medel, ha *beröring* med brottet. Detta genom att digitala spår[2] har lämnats som kan användas som bevisning vid ett brott som har begåtts utanför it-miljö.

Med it-relaterad brottslighet avses därmed alla brott som på något sätt har koppling till it, det vill säga allt från mängdbrottsärenden utanför it-miljö, men där spår och bevisning kan finnas i it-miljö (t.ex. i mobiltelefoner, på chattforum eller på hårddiskar), till rena it-brott (t.ex. dataintrång).

Brås kartläggning bygger på flera olika datamaterial:

- Den officiella kriminalstatistiken från år 2006 till 2015 avseende de brott där det utifrån brottskod går att utläsa att det anmälda brottet har it-inslag.
- Granskning av ett urval på drygt 4 800 polisanmälningar från år 2006, 2010 och 2014.
- Polismyndighetens registrerade beslag från år 2008, 2010 och 2014.
- Brås frågeundersökning Nationella trygghetsundersökningen (NTU).
- Enkätundersökning bland landets operativa åklagare, polisiära förundersökningsledare samt it-undersökare[3].
- Semistrukturerade intervjuer med företrädare från Polismyndigheten och Åklagarmyndigheten som ansvarar för olika frågor gällande it-relaterad brottslighet samt med operativa åklagare, polisiära förundersökningsledare och it-undersökare från olika delar av landet.
- Skriftliga frågor riktade till personer som är verksamma inom Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten, Domstolsverket, Tullverket, Kustbevakningen, Skatteverket och Säkerhetspolisen (Säpo) gällande behovet av ett statistiskt system för att följa utvecklingen av it-inslagen i de anmälda brotten.

Tydlig ökning av it-inslag i de anmälda brotten sedan 2006

Resultaten från Brås analyser visar att det sedan år 2006 har skett en tydlig ökning av it-inslag i de anmälda brotten. Ökningen kan observeras i samtliga av de datakällor som Brå har använt sig av för att göra kartläggningen. Enligt den officiella kriminalstatistiken

[2] Digitala spår eller digital bevisning är information som antingen är överförd via eller lagrad i binär form (Holt m. fl. 2015). Vi lämnar digitala spår när vi använder vårt busskort, lånar böcker, gör sökningar på internet eller skickar sms till våra vänner.

[3] Med it-undersökare avses, enligt rapportens definition, personer som arbetar med undersökning av it-media, analys av data, internetinhämtning, granskning av barnpornografi samt analys och bearbetning av bild/film/ljud.

har de anmälda brotten, där det utifrån brottskoden går att utläsa att brottet har it-inslag (datorbedrägeri, bedrägeri med hjälp av internet, dataintrång samt internetrelaterade barnpornografibrott), sammantaget ökat med 949 procent mellan år 2006 och 2015. Även den granskning som Brå har gjort av ett urval av polisanmälningar från 2006, 2010 och 2014 visar att it-inslagen har ökat under perioden. Enligt granskningen, som utgör en minimiskattning, har den totala andelen brott med it-inslag mer än fördubblats mellan åren 2006 och 2014. Störst andel brott med it-inslag syns inom brottskategorierna brott mot person och bedrägeri.

Bakom den generella ökning som observeras i urvalet av polisanmälningar bedöms ett antal faktorer spela in. En viktig faktor är att det har skett en ökning av brott som per definition har it-inslag (t.ex. datorbedrägeri, bedrägeri med hjälp av internet och dataintrång). En annan faktor är att utvecklingen av sociala medier avspeglas i ökningar av hot, ofredanden och andra brott som sker via sådana kommunikationsvägar. En tredje faktor är att andelen brott som har filmats av övervakningskameror[4] tycks ha ökat, vilket gäller för flera typer av brott (t.ex. våldsbrott, stöld och skadegörelse). En fjärde faktor som förklarar den ökning av it-inslag som observeras i polisanmälningarna är slutligen att polisens beslag av misstänkta personers mobiltelefoner tycks ha ökat, till exempel vid narkotikabrott.

Ökningen av it-inslag i brottsligheten bekräftas även av Brås analys av antalet registrerade it-beslag under tidsperioden och i den analys som har gjorts av den Nationella trygghetsundersökningen (NTU) avseende internetrelaterade hot och bedrägeribrott.

Bristande kompetens om it-relaterade brott inom den brottsutredande verksamheten

Enligt Åklagarmyndighetens Utbildningscentrum behandlas i dagsläget it-frågor på grundutbildningen både som ett enskilt block och som del i de kursmoment där det bedöms vara relevant. Polisens grundutbildning innehåller däremot ingen särskild kurs om it-relaterad brottslighet. It-aspekten är heller inte tillräckligt integrerad på kurser rörande andra ämnen.

Ett annat sätt att erhålla kunskap på it-området är genom att delta i den vidareutbildning som erbjuds i Åklagarmyndighetens eller Polismyndighetens regi. Resultaten från Brås enkätundersökning visar att över hälften av åklagarna och nio av tio polisiära förundersökningsledare helt saknar vidareutbildning på it-området. Fram till nyligen har det heller inte gjorts några centrala

[4] Bildupptagning från övervakningskameror lagras i dag huvudsakligen i digitalt format, det vill säga lämnar digitala spår (se rapportens definition). Bildundersökningar utgör en del av it-forensiken.

satsningar på vidareutbildning inom it-området för personer som arbetar inom Polismyndighetens kärnverksamhet. It-undersökarna, som utgör Polismyndighetens spetskompetens när det gäller bevissäkring i digital miljö, har generellt sett en hög utbildningsnivå, men 12 procent saknar helt utbildning på it-området.

Att utreda brott med it-inslag skiljer sig från traditionellt polisarbete när det gäller vilka möjliga utredningsåtgärder som förundersökningsledaren har i sin ”verktygslåda”. Resultaten från Brås analys visar att kunskaperna om vilka utredningsåtgärder som är möjliga att genomföra i ärenden med it-inslag ofta brister hos både åklagare och polisiära förundersökningsledare. Exempelvis uppger endast 48 procent av åklagarna och 22 procent av de polisiära förundersökningsledarna att de har goda kunskaper om vilka möjligheter som finns att spåra anonyma gärningspersoner via IP-adress. Kunskapsnivån är lägst när det gäller vilka möjligheter som finns att säkra bevisning som ligger på internet, till exempel på ett e-postkonto, Facebook-konto eller på en annan plats på internet. En förklaring kan vara att sådan bevisning ofta kräver kontakt med externa aktörer utomlands och att regelverket på området upplevs vara komplicerat. En konsekvens av den bristande kompetensen är att brott som sker via internet ofta läggs ner, då de ses som omöjliga att klara upp.

Bristande tekniska kunskaper bland it-undersökare

Brås rapport visar att kunskapsnivån på it-området generellt sett är hög bland Polismyndighetens it-undersökare, men att det finns tydliga kunskapsluckor även i denna grupp. Bland annat uppger över hälften av it-undersökarna som arbetar med internetinhämtning att de har bristfälliga kunskaper om de analysverktyg som används för uppgiften. Närmare 40 procent av it-undersökarna som arbetar med elektronik uppger att de har bristfälliga kunskaper om elektronik, och nästan var fjärde it-undersökare som arbetar med bild, film och ljud uppger att deras tekniska kunskaper på detta område brister. En förklaring till de bristande kunskaperna är att det saknas utbildningskrav för it-undersökare. En annan förklaring kan vara bristen på fortlöpande fort- och vidareutbildning. En tredje förklaring kan vara att många it-undersökare är ”generalister”, det vill säga de har många arbetsområden och har inte möjlighet att fördjupa sig tillräckligt inom något av områdena.

Den it-forensiska processen en flaskhals i utredningarna

För att den it-forensiska verksamheten ska kunna fungera effektivt krävs att ett antal förutsättningar är uppfyllda. En sådan

förutsättning är att det finns en balans mellan antalet it-undersökare och de arbetsuppgifter och beställningar de har att hantera. Brås analys visar att den it-forensiska verksamheten brister i detta avseende. Tre av fyra it-undersökare upplever att en hög arbetsbelastning är ett hinder i deras arbete, och it-undersökare som Brå har intervjuat berättar att de har svårt att hinna med sina arbetsuppgifter inom rimlig tid. En förklaring till den höga arbetsbelastningen är det stora inflödet av beställningar till den it-forensiska verksamheten. Den låga beställarkompetensen bland åklagare, polisiära förundersökningsledare och utredare leder dessutom ofta till att beställningarna blir otydliga och onödigt omfattande.

En annan förklaring till den höga arbetsbelastningen är att it-undersökarna på många håll används ineffektivt, till exempel för att utföra arbetsuppgifter som de är överkvalificerade för. It-undersökare som Brå har intervjuat berättar att de används för att till exempel filma rekonstruktioner av brott eller som en form av allmänt it-stöd i frågor som ligger utanför det it-forensiska arbetet. Det råder även diskussion om huruvida arbetsuppgifter som att fingranska övergreppsbilder mot barn och att skapa presentationer till åklagaren inför en huvudförhandling bör ses som en it-forensisk arbetsuppgift. Drygt var fjärde it-forensiker uppger att de ofta eller mycket ofta fingranskar övergreppsbilder mot barn, och nära var femte att de ofta eller mycket ofta skapar presentationer inför huvudförhandling.

Brist på teknisk utrustning och system

En annan viktig förutsättning för att den brottsutredande verksamheten ska kunna hantera it-relaterad brottslighet på ett effektivt sätt är ett fungerande it-stöd. Brås analys visar att drygt var fjärde åklagare och nära hälften av de polisiära förundersökningsledarna anser att bristande tillgång på teknisk utrustning, programvara och/eller förbrukningsmaterial är ett hinder i deras arbete. Motsvarande siffror för gruppen it-forensiker är 39 procent och gruppen övriga it-undersökare 51 procent. Inom Polismyndigheten nämns till exempel begränsningarna med att polisens plattform Polar inte stöder alla filformat, vilket kan göra det svårt för förundersökningsledare och utredare att ta del av övervakningsfilmer. Inom den it-forensiska verksamheten efterfrågas avancerad it-utrustning som till exempel gör det möjligt att få ut krypterad information, något som bedöms bli allt vanligare.

Låg kännedom om expertfunktionernas roller

Ärenden som har it-inslag kan vara både tekniskt och juridiskt komplicerade. Ett sätt att söka rådgivning i ärenden med it-inslag är via de expertfunktioner som finns vid Åklagarmyndigheten

och Polismyndigheten. Vid Åklagarmyndigheten inrättades år 2015 ett nätverk av kontaktåklagare för it-området, dit enskilda åklagare kan vända sig för att få vägledning när de hanterar brott med it-inslag. Vid Polismyndigheten, vid den Nationella operativa avdelningen (Noa), inrättades samma år ett nationellt it-brottscentrum (SC3), som biträder regionerna med expertkompetens när kunskap eller utrustning saknas, till exempel med bild- och filmarbeten, husrannsakan i komplex it-miljö samt med kvalificerad internetinhämtning. Vid SC3 finns även en deskfunktion som hanterar olika typer av frågor från olika delar av myndigheten relaterat till utredningar med it-inslag. SC3 är dessutom internationell kontaktpunkt för it-relaterade brott och är så kallad Single point of contact (SPOC) mot bland annat Facebook, Google och Apple, vilket innebär att de sköter kontakten med dessa aktörer i samtliga ärenden där information behöver hämtas från dem. Inom Polismyndigheten finns även Nationellt forensiskt centrum (NFC) som bistår regionerna med kompetens i ärenden med tekniskt svåra eller komplexa frågor. Vid NFC finns mer avancerad utrustning som kan användas för att säkra digitala bevis i komplexa ärenden samt en servicetelefon dit utredare och förundersökningsledare kan ringa för att få vägledning.

Brås rapport visar att det råder stor osäkerhet bland åklagare, polisiära förundersökningsledare och it-undersökare om vad olika aktörer inom Polismyndighetens nationella struktur kan bistå med i ärenden med it-inslag. Den låga kännedomen kan troligtvis förklaras av att ansvarsområdena för Noa och NFC inte är tillräckligt tydligt formulerade, att den nya polisorganisationen inte har haft möjlighet att ”sätta sig” ännu och att det har saknats resurser och intern struktur för att föra ut budskapet om vad expertfunktionerna kan bistå med.

Brås bedömning

Stort behov av utbildning inom Åklagarmyndigheten och Polismyndigheten

Brås rapport visar att det sedan år 2006 har skett en tydlig ökning av förekomsten av it-inslag i de anmälda brotten. Rapporten visar samtidigt att kompetensen vad gäller it-relaterad brottslighet brister inom de brottsutredande myndigheterna. Mot bakgrund av detta anser Brå att det finns ett stort behov av utbildningsinsatser om it-relaterade brott inom både Åklagarmyndigheten och Polismyndigheten. Åklagarmyndigheten bör överväga att införa en obligatorisk utbildning gällande brott med it-inslag för operativa åklagare. Det finns även ett behov av fördjupningsutbildning på it-området samt av lättillgänglig information i stunden.

Inom Polismyndigheten finns ett stort behov av fort- och vidareutbildningssatsningar för hela myndighetens kärnverksamhet (till exempel för förundersökningsledare, utredare och polisens anmälningsmottagare). Brå anser därför att det dels bör genomföras en central utbildningssatsning som syftar till att höja grundkompetensen om it-relaterade brott inom kärnverksamheten, dels att det bör skapas flera avancerade utbildningar på specialistnivå. Brå anser även att it-aspekten bättre bör integreras i polisens grundutbildning.

It-undersökarnas spetskompetens behöver säkerställas

Brå anser att Polismyndigheten bör säkerställa att it-undersökarna har den kompetens som är nödvändig för att de ska kunna utföra sitt arbete på ett effektivt och rättssäkert sätt. Dels bör det säkerställas att samtliga it-undersökare har en grundläggande utbildning på it-området som är anpassad efter deras arbetsområde, till exempel att de behärskar de arbetsverktyg som ska användas i arbetet. Dels är det angeläget att it-undersökarna ges kontinuerlig fort- och vidareutbildning, för att säkerställa att kompetensen utvecklas i takt med den tekniska utvecklingen på it-området. Resultatet från Brås undersökning visar även att behovet av utbildning kan se olika ut beroende på om it-undersökaren har en polisiär respektive civil bakgrund, där de polisiära it-undersökarna kan ha ett större behov av att stärka sina kunskaper om teknik och de civila it-undersökarna behöver stärka sina kunskaper om juridik och polisoperativt arbete. Det kan slutligen finnas ett behov av att se över innehållet i de it-forensiska utbildningarna som erbjuds inom Polismyndigheten för att kunna bygga upp expertkompetens inom särskilda it-forensiska områden.

Bättre utredningsstöd och fungerande samarbete

Den snabba tekniska utvecklingen på it-området gör att det inte är möjligt för enskilda åklagare, polisiära förundersökningsledare och it-undersökare att hålla sig helt uppdaterade på området. Utöver behovet av omfattande utbildningsinsatser anser därför Brå att det är viktigt att det inom de brottsutredande myndigheterna finns en möjlighet att söka praktisk hjälp och rådgivning när de egna kunskaperna saknas. Brå anser att det bör skapas en större tydlighet kring vad de olika expertfunktionerna i Åklagarmyndighetens och Polismyndighetens nationella struktur kan bistå med i ärenden med it-inslag. Även den regionala förmågan att hantera it-relaterad brottslighet behöver stärkas; en viktig del i detta arbete bedöms vara inrättande av regionala it-brottscentrum.

Brå bedömer även att myndigheterna på ett bättre sätt behöver ta tillvara den kompetens som finns på it-området. Både åklagare

och polisiära förundersökningsledare efterfrågar strukturerad vägledning på it-området, till exempel sammanställningar över svaren på vanligt förekommande frågor, som hur man säkrar digitala bevis och tar kontakt med externa aktörer utomlands. Kunskapen bör därefter kommuniceras via lämpliga kanaler. En viktig sådan samverkansplattform är Polismyndighetens intranät Intrapolis. Enligt Brås intervjupersoner har dock Intrapolis i dag stora brister. Brå bedömer att arbetet med att utveckla Intrapolis är viktigt för att möjliggöra kunskapsspridning på ett effektivt sätt.

Under hösten 2015 tog Åklagarmyndighetens Utvecklingscentrum fram en webbaserad guide för att ge vägledning på it-området. En utmaning för myndigheten är att sprida information om det utredningsstöd som finns att tillgå samt att säkerställa en fortsatt förvaltning så att utredningsstödet hålls uppdaterat.

Öka bemanningen och reglera inflödet inom den it-forensiska verksamheten

För att uppnå en effektiv it-forensisk verksamhet behöver kapaciteten inom den it-forensiska verksamheten öka. Resurser behöver tillföras till verksamheten för att säkerställa att bemanningen vid de it-forensiska sektionerna motsvarar det inflöde av beställningar som finns. Det är även angeläget att inflödet av beställningar regleras, till exempel genom att det tydliggörs vem som får göra en beställning och att det ställs tydligare krav på att undersökningarna måste ha ett specificerat syfte. Brå anser att det är angeläget att kvaliteten i beställningarna höjs, vilket kan uppnås genom en förbättrad beställarkompetens hos åklagare, polisiära förundersökningsledare och utredare. För att uppnå hög kvalitet i beställningarna till den it-forensiska verksamheten anser majoriteten av Brås intervjupersoner att beställningarna bör ske i dialog mellan beställaren och den it-undersökare som ska genomföra undersökningen.

Renodla it-undersökarens roll och ge fler utbildning och behörighet att utföra it-relaterade arbetsuppgifter

För att den it-forensiska verksamheten ska fungera effektivt är det angeläget att it-undersökaren i första hand används för att utföra kvalificerade it-relaterade arbetsuppgifter. Som ett led i detta bedömer Brå att Polismyndigheten bör se över möjligheterna att i större utsträckning överlåta rutinmässiga och enklare it-undersökningar till andra funktioner än de it-forensiska, vilket skulle kunna motverka flaskhalsar och förkorta handläggningstiderna. Brå betonar att det bör vara reglerat så att handläggaren först efter avslutad utbildning erhåller behörighet för att få genomföra arbetsuppgifterna.

Brås studie visar även att det saknas personal med kompetens att analysera den information som extraherats från olika it-media, till exempel sms och geopositioneringar från mobiltelefoner. Analysfasen riskerar att hamna i gränslandet mellan forensik och utredning. På grund av den höga arbetsbelastningen inom den it-forensiska verksamheten finns det sällan någon möjlighet för it-undersökaren att genomföra en analys av de data som säkrats. Generellt sett förväntas analysen i stället genomföras av utredaren, men eftersom många utredare saknar sådan kompetens finns det en risk att potentiellt bevismaterial inte används till fullo.

Brå bedömer att kapaciteten i analysfasen bör höjas, vilket exempelvis kan ske genom att höja utredarnas analyskompetens. Förutom en ökad kompetens efterfrågar förundersökningsledare och it-undersökare ett användarvänligt verktyg som ska kunna användas för att analysera de data som har extraherats av it-undersökarna.

Behov av ett nationellt uppföljningsverktyg

Inom flera av rättsväsendets myndigheter finns det ett behov av statistik som kan visa utvecklingen av it-inslag i de anmälda brotten. Behovet är tydligast inom Polismyndigheten, där det i första hand finns en efterfrågan på statistikuppgifter som kan beskriva ärendeflödet inom den it-forensiska verksamheten. Statistikuppgifter som efterfrågas är till exempel antalet beställda it-undersökningar, genomströmningstider och grad av komplexitet i de beställda it-undersökningarna. Syftet med sådan statistik är att skapa ett beslutsunderlag vid finansiering och fördelning av resurser inom verksamheten, för att därigenom bättre kunna dimensionera verksamheten efter det inflöde som har registrerats.

Brås förslag är att det ska skapas ett nationellt uppföljningssystem för Polismyndighetens it-forensiska verksamhet. Förutom att kunna producera statistik av hög kvalitet finns det även en efterfrågan på att systemet ska kunna användas som ett stöd i det it-forensiska arbetet, till exempel för att ärendefördela mellan olika it-forensiska sektioner, samt att det ska finnas en koppling mellan systemet och andra ärendehanteringssystem som används inom den brottsutredande verksamheten. Det pågår för närvarande ett omfattande arbete vid Nationellt forensiskt centrum (NFC) för att utveckla den forensiska verksamheten i landet, där en del av arbetet är att utveckla ett gemensamt ärendehanteringssystem. Brå bedömer att NFC och Nationella operativa avdelningen (Noa) bör samarbeta i det fortsatta arbetet med att till exempel klargöra vilket behov av statistikuppgifter som finns när det gäller it-relaterade brott och vilken slags it-undersökningar ett sådant system bör inrymma. En viktig del i detta arbete är att skapa enhetliga definitioner av centrala begrepp.

Rättsväsendet står inför stora framtida utmaningar

Brås rapport visar sammantaget att de satsningar som hittills gjorts på it-området inte motsvarar behovet. Det är ytterst angeläget att Polismyndigheten och Åklagarmyndigheten tillsätter de resurser som krävs för att såväl kompetens- som kapacitetshöjande åtgärder kan genomföras. Det är även viktigt att de åtgärder som genomförs inte blir en engångssatsning, utan att satsningarna på it-området fortlöper och uppdateras i takt med utvecklingen.

Inledning

Utvecklingen och användningen av internet, datorer och mobilteknologi har dramatiskt förändrat vårt moderna samhälle. I dag använder 95 procent av befolkningen i åldern 8–55 år internet, besökarna på sociala medier fortsätter att växa och allt fler använder så kallade smartmobiler[5] (Findahl och Davidsson 2015). Ett alltmer digitaliserat samhälle och utvecklingen av informationsteknologin underlättar på många sätt människors vardag. Våra smartmobiler motsvarar i dag små datorer med oändligt många fler funktioner än tidigare generationer mobiltelefoner. Med hjälp av internet och sociala medier kan vi delta i olika forum som är gratis och öppna för alla, vi kan enkelt hålla kontakt med vänner, delta i debatter, sprida, söka och inhämta information av olika slag, utföra bankärenden, köpa och sälja varor etc.

Men det ökande användandet av informationsteknologi ökar även it-inslagen i brottsligheten, vilket innebär nya utmaningar för rättsväsendet. Det handlar både om organiserade och sofistikerade attacker mot datasystem utförda av ”specialister” och om mer traditionella brott som per automatik får it-inslag i och med det ökade teknologianvändandet i samhället (Wall och Williams 2013). Informationsteknologin innebär även nya möjligheter för rättsväsendet, till exempel avseende att avlyssna, bevaka, inhämta underrättelser samt informera allmänheten om kriminalitet eller annan pågående fara (Bartlett m.fl. 2013). För den utredande verksamheten kan viktig bevisning finnas i sociala medier (Brunty och Helenek 2013).

För att möta utmaningarna och för att ta vara på möjligheterna med de ökade it-inslagen i brottsligheten behöver rättsväsendet möta upp med kompetens och kapacitet som motsvarar utvecklingen. Detta förutsätter bland annat såväl adekvata utbildningsinsatser, internationella samarbeten och ett fullgott lagstöd som investeringar i it-system (se t.ex. Holt m.fl. 2015). Ytterligare en

[5] Smartmobil är en mobiltelefon med avancerade datorfunktioner, internetuppkoppling, kamera och ofta även satellitnavigator och QR-läsare. (http://www.ne.se/uppslagsverk/encyklopedi/lång/smartmobil, hämtad 2016-08-25)

viktig förutsättning för att förstå och hantera it-inslagen i brottsligheten är att få en samlad bild av utveckling och omfattning, något som många gånger är svårt att erhålla eftersom det saknas tillförlitlig data (Williams och Levi 2015). Statistiken över anmälda brott separerar inte brott som skett i it-miljö från dem som skett utanför, detta gäller såväl i det svenska systemet (Brå 2015a) som i andra länders system (se t.ex. McGuire och Dowling 2013).

Brås uppdrag

Brottsförebyggande rådet fick 2015 i uppdrag av regeringen att genomföra en studie om utvecklingen av den it-relaterade brottsligheten och rättsväsendets förmåga att utreda brott med it-inslag. För att på ett effektivt sätt kunna utveckla hanteringen av it-relaterad brottslighet krävs kunskap, såväl om brottslighetens omfattning och karaktär som om rättsväsendets kompetens och kapacitet på området.

Studiens syfte och frågeställningar

Med utgångspunkt i regeringens uppdrag till Brå har föreliggande studie tre huvudsyften:

1. Att kartlägga utvecklingen när det gäller förekomsten av it-inslag i de anmälda brotten. Kartläggningen ska avse utvecklingen sedan 2006 och innehålla såväl brott mot person som andra relevanta brottstyper.
2. Att analysera kompetens och kapacitet vad gäller it-relaterad brottslighet och forensiska it-undersökningar i den brottsutredande verksamheten. I detta ingår att belysa brister och utvecklingsmöjligheter.
3. Att överväga om det är möjligt att skapa ett system som ger rättsväsendets myndigheter ett statistiskt underlag för att framöver följa utvecklingen av it-inslag i de anmälda brotten, och i så fall föreslå hur systemet bör utformas.

Utifrån studiens tre huvudsyften har följande frågeställningar formulerats:

- Hur har utvecklingen av förekomsten av it-inslag i polisanmälningarna sett ut sedan 2006?
- Hur har utvecklingen av förekomsten av it-inslag sett ut enligt den officiella kriminalstatistiken, i registrerade beslag samt i den Nationella trygghetsundersökningen (NTU)?
- Vilken kompetens finns det inom olika grupper av poliser och åklagare för att hantera brott med it-inslag?
- Vilken kapacitet har Polismyndigheten och Åklagarmyndigheten för att hantera brott med it-inslag?

- Vad finns det för särskilda problem som polis och åklagare stöter på i sitt arbete med att utreda och lagföra brott med it-inslag?
- Vilka utvecklingsmöjligheter anser polis och åklagare att rättsväsendet har vad gäller handläggningen av brott med it-inslag?
- Vad finns det för behov inom rättsväsendet gällande statistiskt underlag för brott med it-inslag?
- Är det möjligt att utforma ett system för statistiskt underlag för brott med it-inslag enligt det behov som identifierats? Hur kan i så fall ett sådant system se ut?

Vad är it-relaterad brottslighet?

Inom såväl svensk forskning och verksamhet som inom internationell dito används en rad olika begrepp när man pratar om it-relaterad brottslighet, till exempel ”brott i it-miljö”, ”it-brott[6]” eller ”brott i digital miljö”. Vad man menar med de olika begreppen är dessutom sällan väl definierat, ofta för att det saknas tydliga gränser och för att det pågår en ständig utveckling på området. Tidigare pratade man till exempel vanligen om cybercrime och computer crime som två olika saker. I dag är begreppen i princip synonyma eftersom nästan alla datorer är kopplade till internet (Holt m. fl. 2015). Hur begreppen används skiljer sig även åt internationellt.

Ett vanligt förekommande begrepp är it-relaterad brottslighet (se till exempel Rikspolisstyrelsen 2014, Brå 2000, Savona 1998), och det är också det begrepp som används i föreliggande rapport. It-relaterad brottslighet innebär att brottet har it-inslag genom att informationsteknologi (it) är närvarande på någon av följande tre nivåer:

1. It är *målet* och en förutsättning för brottets genomförande, till exempel dataintrång.
2. It är *medlet* och har understött brottet, till exempel genom att ett socialt forum använts för att hota någon.
3. It kan, utan att vara mål eller medel, ha *beröring* med brottet. Detta genom att digitala spår[7] har lämnats som kan användas som bevisning vid ett brott som begåtts utanför it-miljö.

Med it-relaterad brottslighet avses därmed alla brott som på något sätt har koppling till it, dvs. allt från mängdbrottsärenden

[6] Enligt svensk lagstiftning finns det två rena it-brott, dataintrång (4 kap. 9 c § BrB) och datorbedrägeri (9 kap. 1 § andra stycket BrB).

[7] Digitala spår eller digital bevisning är information som antingen är överförd via eller lagrad i binär form (Holt m. fl. 2015). Vi lämnar digitala spår när vi använder vårt busskort, lånar böcker, gör sökningar på internet eller skickar sms till våra vänner. Dessa spår kan på olika sätt användas som bevisning.

utanför it-miljö, men där spår och bevisning kan finnas i it-miljö (t.ex. i mobiltelefoner, på chattforum eller på hårddiskar), till rena it-brott (t.ex. dataintrång). I rapporten används begreppen brott med it-relevans och brott med it-inslag synonymt med it-relaterade brott.

Avgränsningar

Avseende uppdragets andra syfte gällande kompetens och kapacitet i den brottsutredande verksamheten har Brå av tidsmässiga skäl valt att avgränsa studien till att omfatta Polismyndigheten och Åklagarmyndigheten. Utöver Polismyndigheten och Åklagarmyndigheten bedrivs brottsutredande verksamhet vid Ekobrottsmyndigheten, Skatteverket, Kustbevakningen, Tullverket och Säkerhetspolisen.

Rapportens disposition

Redovisningen av Brås uppdrag börjar i nästa kapitel. Där redogörs för vilka metoder och material som har använts för att besvara frågeställningarna kopplat till uppdragets tre delar.

Rapportens tredje kapitel presenterar resultaten från den första delen av uppdraget, att beskriva utvecklingen av den it-relaterade brottsligheten sedan 2006. Därefter följer två kapitel som är kopplade till uppdragets andra del, där det första beskriver vilken kompetens som finns inom olika grupper av poliser och åklagare för att hantera brott med it-inslag, och det andra vilken kapacitet Polismyndigheten och Åklagarmyndigheten har för att hantera brott med it-inslag.

Det därpå följande kapitlet presenterar resultaten från den tredje delen av uppdraget, det vill säga en beskrivning av de behov som finns inom rättsväsendet gällande ett statistiskt underlag för brott med it-inslag samt huruvida det är möjligt att utforma ett system för statistiskt underlag för brott med it-inslag enligt de behov som identifierats. I rapportens avslutande kapitel beskrivs de angelägna utvecklingsområden som Brå identifierat i sitt arbete, samt en beskrivning av det utvecklingsarbete som pågår inom rättsväsendet i dag.

Metod och material

För att besvara studiens frågeställningar har flera olika datakällor använts:

- Den officiella kriminalstatistiken från 2006 till 2015.
- Polisanmälningar från år 2006, 2010 samt 2014.
- Polismyndighetens registrerade beslag från år 2008, 2010 och 2014.
- Brås frågeundersökning Nationella trygghetsundersökningen (NTU), från 2006–2014.
- Enkätundersökning bland landets operativa åklagare, polisiära förundersökningsledare samt it-undersökare.[8]
- Semistrukturerade intervjuer med företrädare från Polismyndigheten och Åklagarmyndigheten som ansvarar för olika frågor gällande it-relaterad brottslighet, samt med operativa åklagare, polisiära förundersökningsledare och it-undersökare från olika delar av landet.
- Skriftliga frågor riktade till personer verksamma inom Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten, Domstolsverket, Tullverket, Kustbevakningen, Skatteverket och Säkerhetspolisen (Säpo) gällande behovet av ett statistiskt system för att följa utvecklingen av it-inslag i de anmälda brotten.

Uppdraget till Brå har tre delar, och nedan presenteras vilka material som använts för att besvara frågeställningarna kopplat till respektive del.

Del 1 – Utvecklingen av it-inslag i de anmälda brotten

Den första delen av uppdraget är att beskriva förekomsten av it-inslag i de anmälda brotten. Det system som i dag används för att registrera de brott som anmäls till polisen registrerar som regel

[8] Med it-undersökare avses personer som arbetar med undersökning av it-media, analys av data, internetinhämtning, granskning av barnpornografi samt analys och bearbetning av bild/film/ljud.

inte huruvida det anmälda brottet har it-inslag. För att beskriva utvecklingen har Brå därför använt information från fyra olika källor – den officiella kriminalstatistiken (för de brott där brottskoden anvisar att det anmälda brottet är it-relaterat), ett urval av polisanmälningar, statistik över registrerade beslag samt siffror från Brås nationella trygghetsundersökning (NTU). De olika källorna kompletterar varandra och gör det möjligt att skapa en bild av utvecklingen.

Den officiella kriminalstatistiken

Den årliga statistiken över anmälda brott redovisar händelser som anmälts och registrerats som brott under året. I samband med att ett brott registreras kategoriseras det med brottskoder (Brå 2015:16). Den nuvarande statistiken innehåller ett fåtal brottstyper där brottskoden indikerar it-inslag – datorbedrägeri, bedrägeri med hjälp av internet, dataintrång, internetrelaterade barnpornografibrott, datasabotage, brott mot upphovsrätten genom fildelning samt brott mot det industriella rättsskyddet med hjälp av internet. I resultatredovisningen redovisas siffor på hur utvecklingen har sett ut avseende dessa brottskoder.

Urval av polisanmälningar

För de allra flesta brottstyper ger inte brottskoden information om huruvida det anmälda brottet har it-inslag. För att skapa en bild av utvecklingen i den totala anmälda brottsligheten används därför information från fritexten i ingångsanmälan, det vill säga från den text som registreras i samband med att anmälan tas upp.

När statistik över anmälda brott redovisas används vanligen sju olika brottskategorier (se till exempel Brå 2015:16), Brott mot person (BrB kap. 3-7), Bedrägeribrott och annan oredlighet (BrB kap. 9), Brott mot narkotikastrafflagen (1968:64), Tillgreppsbrott (BrB kap. 8), Skadegörelse (BrB kap. 12), Brott mot trafikbrottslagen (1951:649) samt kategorin Övriga brott (brott som inte ingår i någon av de övriga kategorierna). För att kartlägga utvecklingen av it-inslag i polisanmälningarna gjordes ett slumpmässigt urval på 230 anmälningar per brottskategori för åren 2006, 2010 och 2014, det vill säga totalt 4 830 polisanmälningar.

Samtliga fritexter lästes igenom manuellt och eventuella it-inslag kodades enligt den tredelade definitionen som används för rapporten:

1. It är *målet* och en förutsättning för brottets genomförande, till exempel dataintrång.
2. It är *medlet* och har understött brottet, till exempel genom att ett socialt forum används för att hota någon.

3. It påverkar utredningen genom *beröring* på annat sätt. Detta genom att digitala spår har lämnats som kan användas som bevisning vid ett brott som begåtts utanför it-miljö.

Om brottsligheten enligt vad som framgår tillhör någon av de tre kategorierna betecknas det som att det anmälda brottet har it-inslag.[9]

Det ska understrykas att den använda metoden med all sannolikhet innebär en grov underskattning av andelen brott med it-inslag. Underskattningen är sannolikt mindre för kategorierna *it är målet* och *it är medlet*, och störst för kategorin *it har annan beröring*, där underskattningen troligen är betydande. Även om texten i polisanmälan inte innehåller en beskrivning av något it-inslag över huvud taget behöver det inte betyda att så faktiskt var fallet. Det beror på att information om förekomst av sådan bevisning sällan beskrivs i fritexten i polisanmälningarna, utan framkommer först senare när en eventuell förundersökning har inletts. Resultaten är därmed att betrakta som en minimiskattning baserad på vad som framkommer i polisanmälan. Samtidigt som metoden inte ger några absoluta siffor på antalet så ska framhållas att om felkällorna är konstanta över tid kan resultaten ändå ge en bild av utvecklingen.

Det interna bortfallet, det vill säga att fritext saknades i polisanmälan, varierade mellan brottskategorierna (se tabell 1). För brott mot person, bedrägeri, tillgreppsbrott och skadegörelse ligger det totala bortfallet på relativt låga nivåer. För narkotikabrott ligger bortfallet något högre liksom för kategorin övriga brott. För brott mot trafikbrottslagen var bortfallet för åren 2006 och 2010 omfattande. Det beror på att flera av brotten då registrerades i Trafikdiariet från vilket Brå inte kunde göra något fritextuttag. I resultatdelen presenteras därför inga siffror på utvecklingen

Tabell 1. Bortfall totalt samt för respektive år, n = 230 anmälningar per år och brottskategori. Procent.

	2006	2010	2014	Totalt
Brott mot person	1,7	0,9	6,1	2,9
Bedrägeri m.m.	0,0	1,3	0,9	0,7
Narkotikabrott	16,1	25,2	1,7	14,3
Tillgreppsbrott	0,9	2,6	2,2	1,9
Skadegörelse	4,3	0,9	0,0	1,7
Trafikbrott	86,5	82,6	5,2	58,1
Övriga brott	10,0	10,9	5,2	8,7

[9] Skillnader mellan åren i andelen brott med it-inslag har signifikanstestats (Chi-två test) med hjälp av statistikprogrammet SPSS. I de fall antalet observationer och s.k. förväntade värden i vissa celler varit små i analyserna har funktionen ”Exact test” i SPSS använts (Mehta och Patel 2011).

för trafikbrotten. Det totala bortfallet för alla brottstyper sammantagna är 12,6 procent. Om trafikbrott exkluderas (beroende på det stora bortfallet för denna brottstyp) ligger det totala bortfallet på 5,0 procent.

Beslag

Säkringen av digitala spår och bevis börjar ofta med ett beslag. Som en kompletterande datakälla för att belysa utvecklingen av it-inslag i den anmälda brottsligheten använder Brå därför statistik över de beslag som registrerats av polisen.

Brå har begärt in statistik avseende det totala antalet beslag som har registrerats av polismyndigheterna nationellt under åren 2008, 2010 och 2014. Dessutom har Brå begärt in statistik från huvudgruppen *Bokföring/Data/Kontor/Telefoni* samt tillhörande undergrupper *Mobiltelefon, Datautrustning/Tillbehör/Programvara* samt *Dator/PC/ Mac*. Brå har gjort bedömningen att en stor del av de it-relaterade beslagen torde vara registrerade i dessa undergrupper.

Först år 2008 började beslagen registreras digitalt och enhetligt vid samtliga polismyndigheter. Utvecklingen för beslagen presenteras därför för åren 2008, 2010 och 2014. Statistiken över registrerade beslag har hämtats från Tvångsmedelstjänsten som är en del av Polisens ärendehanteringssystem Durtvå. Statistikuttaget har gjorts av Utredningssektionen på Polismyndigheten. Det skall påpekas att den begärda statistiken endast kan ses som en indikation på utvecklingen av it-inslag i den anmälda brottsligheten, och att skälet till att ett föremål tas i beslag inte framgår av begärd data.[10]

Nationella trygghetsundersökningen (NTU)

Brås nationella trygghetsundersökning (NTU) är en årlig frågeundersökning som riktar sig till allmänheten. I NTU tillfrågas ett representativt urval av befolkningen i åldern 16–79 år om sin utsatthet för brott och sina kontakter med rättsväsendet.[11]

I föreliggande rapport presenteras utvecklingen gällande utsatthet för bedrägeri via internet, hot via internet och hot via telefonsamtal/sms. Utsattheten för bedrägeri redovisas för åren 2006–2014. Utsattheten för hot redovisas för åren 2008–2014. Uppgifter finns även för åren 2005–2007 men svarsalternativen

[10] Beslag får till exempel tas om föremålet är ”någon avhänt genom brott”, till exempel om en mobiltelefon som stulits påträffas hos en misstänkt gärningsperson (27 kap. 1 § RB). Ett sådant beslag behöver i regel inte analyseras av en it-undersökare.

[11] För närmare beskrivning av undersökningens genomförande hänvisas till NTU-rapport Brå 2016:1 och därtill hörande teknisk rapport Brå 2016:3.

var då något annorlunda formulerade, vilket gör att de inte är jämförbara med senare år. Svaren utelämnas därför från resultatredovisningen.

Del 2 – Rättsväsendets kompetens och kapacitet gällande it-relaterade brott

För att besvara frågeställningarna som är kopplade till del 2 i uppdraget gällande vilken kompetens och kapacitet som finns inom rättsväsendet för att hantera brott med it-inslag genomfördes en enkätundersökning. Enkätundersökningen följdes även upp med intervjuer.

Enkätundersökning

Under december 2015 skickade Brå ut webbenkäter till tre olika yrkeskategorier inom Åklagarmyndigheten och Polismyndigheten –åklagare, polisiära förundersökningsledare och it-undersökare.

Enkäterna utformades i samråd med representanter från Nationellt forensiskt centrum (NFC), Nationella operativa avdelningen (Noa), Åklagarmyndighetens Utvecklingscentrum Stockholm samt från Åklagarområde Stockholm (där den person med nationellt samordningsansvar för it-relaterad brottslighet arbetar). Enkäterna anpassades efter de tre respondentgrupperna och innehöll huvudsakligen frågor om utbildning, kunskap om olika it-relaterade utredningsåtgärder, kompetensutvecklingsbehov, hinder i det dagliga arbetet, utredningsstöd och samverkansstrukturer.

Målsättningen var att nå samtliga åklagare som vid tiden för undersökningen arbetade operativt som förundersökningsledare samt samtliga polisiära förundersökningsledare. Målsättningen var även att nå samtliga it-forensiker och andra personer inom Polismyndigheten som genomför olika typer av it-undersökningar. Enkäten riktade sig till personer som arbetar med undersökning av it-media, analys av data, internetinhämtning, granskning av barnpornografi samt analys och bearbetning av bild/film/ljud. Dessa personer kan gå under benämningar som till exempel it-tekniker, it-brottsutredare eller it-brottsspecialist. I rapporten används samlingsbegreppet it-undersökare för att beskriva it-forensiker och övriga it-undersökare.

Enkäten riktade sig till förundersökningsledare och it-undersökare placerade på regional nivå, polisområdesnivå eller lokalpolisområdesnivå (det vill säga ej förundersökningsledare och it-undersökare placerade på nationell nivå, t.ex. vid Noa och NFC). Polismyndigheten saknade vid tiden för undersökningen sammanställningar över myndighetens förundersökningsledare och it-undersökare. Urvalsunderlaget sammanställdes i stället

med hjälp av olika representanter ute i regionerna. Kvaliteten på de listor som Brå fick varierade stort mellan regionerna avseende hur uppdaterade och heltäckande listorna var. För samtliga tre respondentgrupper inleddes därför respektive enkät med en filterfråga för att säkerställa att rätt personer besvarade enkäterna.

Svarsfrekvensen i de tre yrkeskategorierna varierade från 54 till 59 procent (tabell 2), se bilaga 2 för mer information om distributionen av enkäten. Totalt besvarade närmare 1 200 personer någon av de tre enkäterna. Brå bedömer att det stora antalet svar ger värdefull information för att belysa de brister och utvecklingsmöjligheter som de tre yrkeskategorierna upplever som kopplade till deras ärenden med it-inslag.

Tabell 2. Distribuerade och besvarade enkäter per respondentgrupp.

	Utskick (antal)	Besvarade (antal)	Svarsfrekvens (%)
Åklagare	719	387	54
Polisiära fu-ledare	1 183	670	57
It-undersökare	224	132	59
Totalt	**2 126**	**1 189**	**56**

Intervjuer

Utöver den enkätundersökning som genomfördes med operativa åklagare, polisiära förundersökningsledare och it-undersökare har Brå även intervjuat 9 personer verksamma inom Åklagarmyndigheten och 24 personer verksamma inom Polismyndigheten, såväl på nationell som på regional nivå.[12] Respondenterna hade varierande erfarenhet och kunskap gällande it-relaterade brott, alltifrån jourhavande förundersökningsledare till personer med specialkunskaper inom it-området.

Syftet med intervjuerna var att utveckla en bättre förståelse för de brister och utvecklingsmöjligheter som framkommer i enkätundersökningen och att därigenom bättre kunna illustrera och tydliggöra dem i rapporten. Intervjuerna var semistrukturerade och följde en intervjuguide. Beroende på respondentens funktion var intervjufrågorna delvis olika vid olika intervjutillfällen. Fokus för intervjuerna har även utvecklats i takt med arbetet. Intervjuerna skedde löpande under uppdragets genomförande.

Del 3 – System för statistiskt underlag

Den tredje delen av uppdraget är att kartlägga vilka behov rättsväsendet har av ett statistiskt underlag för brott med it-inslag

[12] Personer anställda vid Åklagarmyndighetens eller Polismyndighetens område/region Syd, Väst, Stockholm och Nord har intervjuats.

samt vilka möjligheter det finns att utforma ett system enligt de behov som identifierats. För att besvara frågeställningarna kopplade till del 3 skickade Brå ut skriftliga frågor till personer verksamma inom olika delar av rättsväsendet och genomförde intervjuer med företrädare från Polismyndigheten och Åklagarmyndigheten. Därtill analyserades genomförda och planerade förändringar inom Brås officiella kriminalstatistik och i de frågeundersökningar som Brå regelbundet genomför.

Skriftliga frågor och intervjuer

För att analysera vilket behov som finns av ett statistiskt underlag för brott med it-inslag och vilka möjligheter det finns att utforma ett sådant system har Brå skickat ut skriftliga frågor till personer som är verksamma inom Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten, Domstolsverket, Tullverket, Kustbevakningen, Skatteverket och Säkerhetspolisen. Samtliga dessa myndigheter fick frågor om vilket behov myndigheterna har av statistik för att följa utvecklingen av it-inslag i de anmälda brotten, vilket/vilka ärendehanteringssystem som används inom myndigheten i dag och vilka möjligheter det finns att få ut statistik från systemet som kan användas för att följa utvecklingen av it-inslag i den anmälda brottsligheten. Frågorna besvarades skriftligt via mejl. Personerna från de olika myndigheterna rekryterades delvis efter rekommendation från personer som Brå tidigare hade intervjuat, delvis genom att Brå kontaktade myndigheten centralt som därefter delegerade frågorna. I en del fall besvarades frågorna inte av de personer som Brå ursprungligen kontaktade, utan av någon av annan som myndigheten ansåg vara bättre lämpad. I vissa fall besvarades frågorna gemensamt av olika personer på myndigheten. Ofta hade de utvalda personerna något slags ansvar för myndighetens ärendehanteringssystem eller det utvecklingsarbete som bedrivs inom systemet.

För att få en bättre förståelse för hur ett statistiskt system skulle kunna utformas, till exempel vilka nyckeltal som borde registreras, har Brå dessutom genomfört semistrukturerade intervjuer med personer som är verksamma inom olika delar av Polismyndigheten (till exempel Noa, NFC och regionala it-forensiska sektioner).[13] Intervjuerna konkretiserade myndighetens behov av ett statistiskt system som gör det möjligt att kunna följa utvecklingen av it-inslag i de anmälda brotten, vilka nyckeltal en sådan statistik bör innehålla samt hur ett sådant system i så fall bör utformas.

[13] Frågan om vilket behov som finns av ett statistiskt underlag för att kunna följa utvecklingen av it-relaterade brott och hur ett sådant system skulle kunna utformas har ställts i samtliga intervjuer som genomförts inom ramen för uppdraget (se metod för del 2).

Analys av Brås befintliga datakällor

För att besvara frågeställningarna kopplade till del 3 har Brå dessutom sett över möjligheterna att mäta it-inslag i de anmälda brotten genom att använda Brås befintliga datakällor. Bland annat redogörs för möjligheten att föra in nya brottskoder i brottsklassifikationssystemet, vilket ligger grund för den officiella kriminalstatistiken. Dessutom redogörs för genomförda och planerade förändringar i Brås frågeundersökningar Nationella trygghetsundersökningen (NTU) och Skolundersökningen om brott (SUB). I den del av kapitlet där kriminalstatistiken och systemet med brottskoder beskrivs har Enheten för rättsstatistik (ERS) vid Brå medverkat. ERS är den del av myndigheten som ansvarar för uppbyggnaden av statistiken över anmälda brott, användningen av brottskoder i detta system och som representerar Brå i arbetet med Rättsväsendets informationsförsörjning (RIF).

Övriga informationskällor: litteratursökning och referensgrupp

För att få en bild av såväl det nationella som det internationella kunskapsläget har Brå genomfört litteratursökningar i forskningsdatabaser. Brå har även gått igenom myndighetsrapporter och annat bakgrundsmaterial som inte återfinns i databaserna (så kallad grå litteratur). Med hänvisning till att uppdraget tydligt avser svenska förhållanden, vilka påverkas av organisation, regelverk och lagstiftning i Sverige, används huvudsakligen svenska referenser i rapporten. För en kort genomgång av hur andra länder hanterar it-relaterad brottslighet, se Riksrevisionen (2015).

Genom hela projekttiden har Brå haft nära samarbete med Nationella operativa avdelningen (Noa) och Nationellt forensiskt centrum (NFC) vid Polismyndigheten samt med representanter från Åklagarmyndigheten. Personerna har fungerat som referenspersoner och har kontinuerligt bidragit med uppslag. I slutet av projekttiden genomfördes ett seminarium där de preliminära resultaten presenterades för referensgruppen med syfte att få återkoppling från seminariedeltagarna.

Utvecklingen av it-inslag i de anmälda brotten

Den första delen i regeringens uppdrag till Brå handlar om att kartlägga utvecklingen sedan 2006 när det gäller förekomsten av it-inslag i de anmälda brotten. Som beskrevs i det inledande kapitlet saknas det i dag ett system där utvecklingen enkelt går att följa. För att beskriva utvecklingen har Brå därför använt sig av olika källor. I följande kapitel presenteras först siffror från den officiella kriminalstatistiken för de brott där brottskoden anvisar att det anmälda brottet är it-relaterat. Därefter presenteras resultatet från den kartläggning som Brå har gjort utifrån den information som framgår i ett urval omfattande drygt 4800 polisanmälningar. Syftet är att täcka in samtliga brottskategorier och se hur utvecklingen ser ut och vad it-inslagen kan bestå av för de olika kategorierna. I ett tredje steg beskrivs utvecklingen av antalet it-beslag under tidsperioden och i ett fjärde steg siffror över utvecklingen av den självrapporterade utsattheten enligt Brås Nationella trygghetsundersökning (NTU). Förutom ovan nämnda datakällor redogörs i kapitlet även för vad som framkommit i Brås intervjuer med personer verksamma inom Polismyndigheten och Åklagarmyndigheten kring hur ofta det förekommer it-inslag i de polisanmälda brotten samt vad dessa it-inslag utgörs av.

Utvecklingen enligt kriminalstatistiken

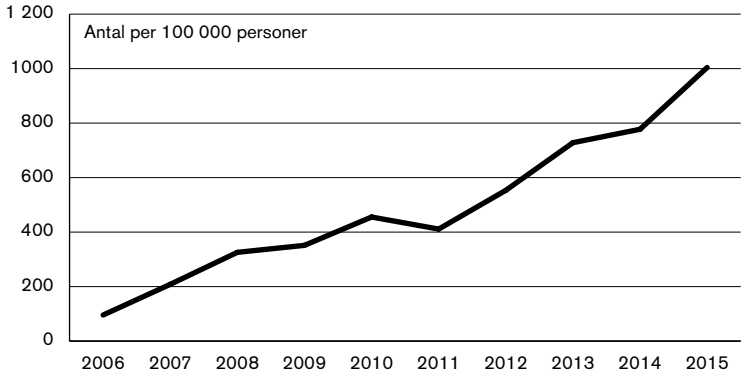
Möjligheten att följa den it-relaterade brottslighetens utveckling med hjälp av kriminalstatistiken är i dag starkt begränsad. Begränsningarna handlar i huvudsak om att det i dagens klassifikationssystem för brott inte finns någon generell it-dimension som visar om brottet har it-inslag eller inte. För ett visst antal brott går det dock att utifrån brottskoden utläsa att brottet har skett i it-miljö. Dessa brottstyper är datorbedrägeri, bedrägeri med hjälp av internet, dataintrång, datasabotage, internetrelaterade barn-

pornografibrott, brott mot upphovsrätten genom fildelning samt brott mot det industriella rättsskyddet med hjälp av internet.[14]

Över 900 procents ökning av antalet anmälda it-relaterade brott enligt brottskod

I figur 1 har de anmälda brott där brottskoden anvisar att brottet skett med hjälp av it slagits samman för att visa hur utvecklingen ser ut för dessa brott under tidsperioden 2006 till 2015, standardiserat för befolkningsutvecklingen.[15] Figuren visar på en kraftig ökning, från 96 per 100 000 invånare år 2006 till 1 004 per 100 000 invånare år 2015. Det innebär en ökning på 949 procent.[16] Detta att jämföra med ökningen för det totala antalet anmälda brott per 100 000 invånare under samma tidsperiod som uppgår till cirka 14 procent. Det går dock inte att med hjälp av diagrammet dra några slutsatser om it-inslagen för brott med övriga brottskoder. Det går inte heller att utifrån siffrorna utläsa om det handlar om nya brott, eller om en förflyttning av brott, det vill säga om traditionella brott har flyttat över till it-miljö.

Figur 1. Totala antalet anmälda it-relaterade brott enligt brottskod (datorbedrägeri, bedrägeri med hjälp av internet, dataintrång, internetrelaterade barnpornografibrott, datasabotage), år 2006–2015 per 100 000 personer i befolkningen.



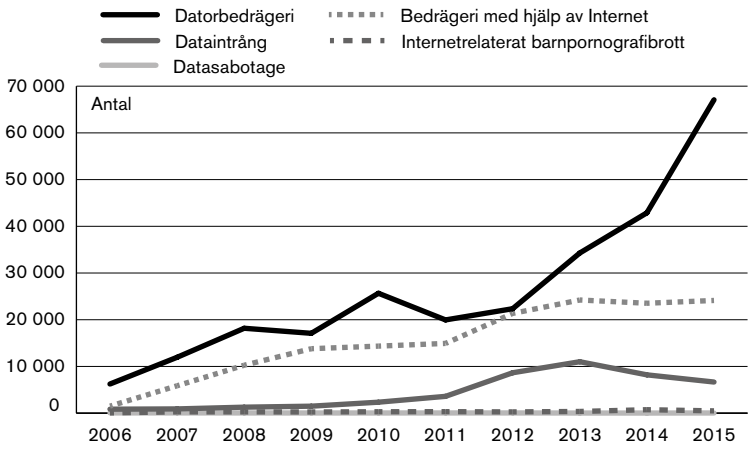
[14] Utöver uppräknade brottskoder finns det ett antal brott som brukar beskrivas som att de i huvudsak begås i it-miljöer, till exempel brott mot personuppgiftslagen, olovlig avlyssning och brott mot telehemlighet.

[15] Den antalsmässigt största brottstypen är datorbedrägeri, följt av bedrägeri med hjälp av internet och därefter dataintrång. Internetrelaterat barnpornografibrott och datasabotage ligger på antalsmässigt betydligt lägre nivåer. Brottskoderna ”Brott mot upphovsrätten genom fildelning” och ”Brott mot det industriella rättsskyddet med hjälp av internet” tillkom först 2010 och redovisas därför ej i figuren.

[16] Riksrevisionen har i en tidigare rapport konstaterat att ökningen av it-relaterade brott fram till år 2014 uppgår till 767 procent (Riksrevisionen 2015). Om denna siffra befolkningsstandardiseras, så att den är jämförbar med Brås beräkningar, är ökningen 712 procent. Brås analyser visar att den snabba ökningstakten har fortsatt sedan 2014.

I absoluta tal är den observerade ökningen störst när det gäller brottstypen datorbedrägeri och därefter bedrägeri med hjälp av internet. Mellan år 2006 och 2015 ökade antalet anmälda datorbedrägerier från cirka 6 200 till 67 100 och bedrägeri med hjälp av internet från 1 500 till 24 100 (figur 2).

Figur 2. Utvecklingen av antalet anmälda it-relaterade brott enligt brottskod år 2006–2015.[17] Absoluta tal. Kriminalstatistik.



Utvecklingen enligt informationen i polisanmälningarna

I denna del redogörs för utvecklingen av it-inslag i polisanmälda brott, både totalt sett och för olika brottskategorier. Resultatet bygger på den granskning av polisanmälningar som Brå har gjort inom ramen för studien. Som redogjorts för i metodavsnittet kodades it-inslagen i tre nivåer (it är *målet*, it är *medlet* eller att det i polisanmälan framkommer att det på något annat sätt finns en *it-beröring*). I den följande resultatredovisningen är de tre kategorierna sammanslagna, vilket fortsättningsvis kallas för att det anmälda brottet har ”it-inslag”. För en mer detaljerad redogörelse över utvecklingen uppdelad på de tre nivåerna, se tabell 1B i bilaga 1.

En begränsning med den kodning av polisanmälningar som har genomförts är att polisanmälningarna sällan innehåller information om ”it-beröring”, det vill säga att det finns digital bevisning

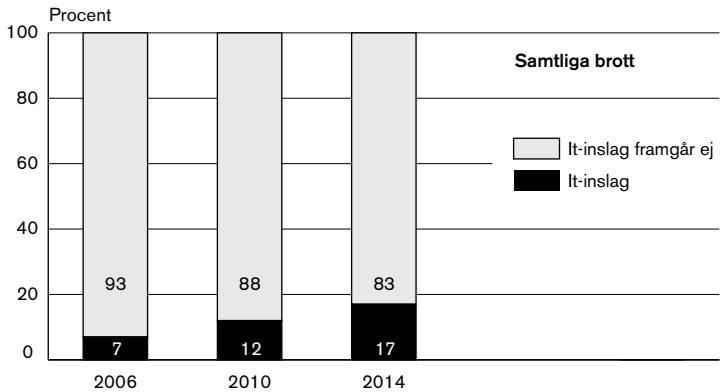
[16] För brottskoderna "Brott mot upphovsrätten genom fildelning" samt "Brott mot det industriella rättsskyddet med hjälp av internet" är antalet anmälningar relativt sett mycket lågt och det finns ingen tydlig trend i utvecklingen. Antalet anmälda brott mot upphovsrätten genom fildelning har varierat mellan 19 och 41 stycken och antalet anmälda brott mot det industriella rättsskyddet har varierat mellan 2 och 14 stycken. Uppgifter finns bara registrerade från 2010 och redovisas därför inte i figuren.

i ärendet. Det beror på att information om förekomst av sådan bevisning sällan beskrivs i fritexten i polisanmälningarna, utan framkommer först senare när en eventuell förundersökning har inletts. Det innebär att andelen anmälningar där det, enligt granskningen, finns en it-beröring med all sannolikhet utgör en grov underskattning av det faktiska antalet ärenden som har en it-beröring. Det påverkar därmed den sammanslagna siffran över andelen ärenden som har it-inslag. På grund av dessa metodproblem går det inte att utifrån dessa siffror uttala sig om de faktiska nivåerna av it-inslag i de anmälda brotten. Eftersom avsaknaden av information rörande it-beröring troligtvis ser likadan ut mellan de olika undersökningsåren går det däremot att tala om den generella utvecklingstrenden när det gäller it-inslag i den anmälda brottsligheten.

Andelen it-inslag har mer än fördubblats sedan 2006

Resultatet från Brås granskning av polisanmälningar visar att it-inslagen i de polisanmälda brotten totalt sett har mer än fördubblats mellan åren 2006 och 2014 (från 7 till 17 procent).[18] Som ovan nämnts bör dock de redovisade nivåerna tolkas med stor försiktighet, då de med all sannolikhet utgör en kraftig underskattning av den totala andelen brott med it-inslag (figur 3).

Figur 3. Skattning av andel av samtliga anmälda brott som har it-inslag år 2006, 2010 och 2014. Procent.



Majoriteten av de polisiära förundersökningsledare och åklagare som Brå har intervjuat inom ramen för studien anser att det i

[18] Skattningen tar hänsyn till det totala antalet anmälda brott som tillhör de separata brottskategorierna (brott mot person, tillgreppsbrott etc.) de olika åren. Brott mot trafikbrottslagen ingår i analysen, men andelen med it-inslag har satts till noll i beräkningarna på grund av det i metodavsnittet nämnda stora interna bortfallet för denna brottstyp, vilket beror på att fritext saknades för många anmälningar, samt att andelen brott med it-inslag var liten bland de anmälningar som hade fritext.

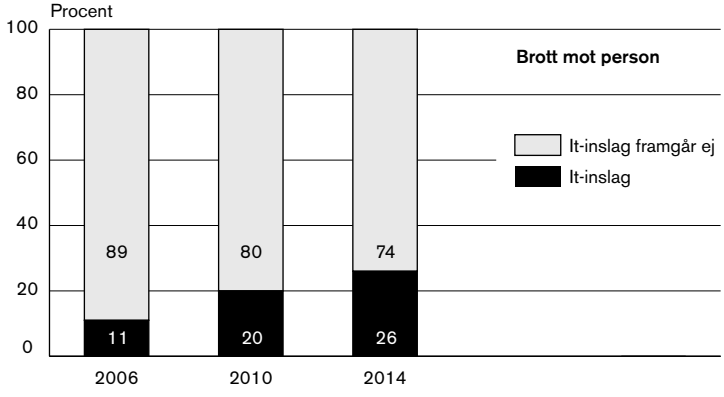
dag snarare är regel än undantag att det finns potentiell digital bevisning i ärendena. Den digitala bevisningen kan till exempel utgöras av beslagtagna mobiltelefoner som innehåller någon slags information som kan styrka brott, våld som har filmats med en mobiltelefon, butiksrån eller snatterier som har filmats med en övervakningskamera[19] eller data från en masttömning. Närmast följer en beskrivning av utvecklingen inom de enskilda brottstyperna i urvalet av polisanmälningar.

Hotfulla och kränkande meddelanden bakom ökning av it-inslag vid brott mot person

Uttrycket brott mot person är en sammanfattande term i kriminalstatistiken som avser brotten i brottsbalkens kapitel 3–7. Det rör sig om olika typer av våldsbrott, olaga hot och ofredande, ärekränkningsbrott (förtal och förolämpning), sexualbrott och brott mot familj. I brott mot person ingår bland annat även brotten dataintrång (BrB kap. 4, 9 c §) och kränkande fotografering (BrB kap. 4, 6 a §).

Andelen brott mot person med it-inslag har ökat från 11 till 26 procent (figur 4) mellan åren 2006 till 2014. Det motsvarar mer än en fördubbling av andelen anmälda brott med it-inslag. Bakom ökningen ligger främst att hotfulla, kränkande eller andra meddelanden via text/ljud/bild på mobiltelefon, via e-post eller socialt forum på internet har ökat. Även it-inslag som består i att målsägarens e-post eller dator har kapats har ökat.

Figur 4. Andel brott inom kategorin brott mot person där det framgår att det finns it-inslag enligt urvalet brottsanmälningar år 2006, 2010 och 2014. Procent.



[19] Bildupptagning från övervakningskameror lagras i dag huvudsakligen i digitalt format, det vill säga lämnar digitala spår (se rapportens definition). Bildundersökningar utgör en del av it-forensiken.

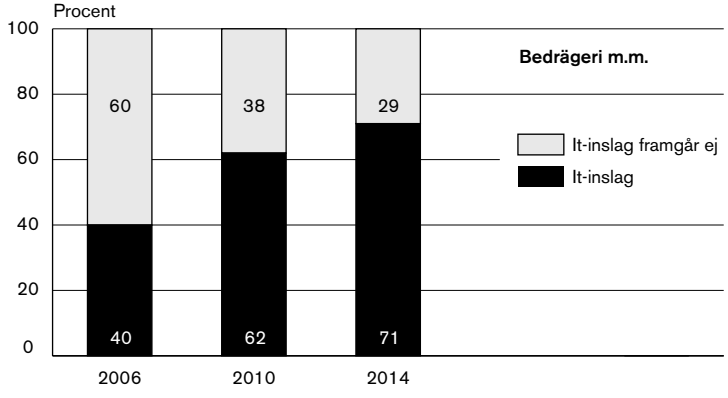
Den observerade ökningen inom kategorin *it har annan beröring* (tabell 1B i bilaga 1) beror främst på en ökad förekomst av övervakningskameror som har, eller kan ha, filmat brottet eller gärningspersonen. Enligt polisiära förundersökningsledare som Brå har intervjuat är det dessutom vanligt att till exempel krogrelaterat våld filmas med mobiltelefoner. Brottet kan både ha filmats av gärningspersonen eller ett vittne till händelsen. Det betonas dock att informationen om sådan bevisning sällan finns i ärendets initialskede.[20]

Störst andel it-inslag bland bedrägeribrotten

Brottsbalkens kapitel ”Bedrägeri och annan oredlighet” (BrB kap. 9) avser bedrägerier samt vissa andra brott, däribland ocker, utpressning och häleri. Antalsmässigt dominerar bedrägeribrotten bland polisanmälningarna om brott mot BrB kap. 9. För bedrägeribrotten återfinns, som tidigare nämnts, två brottskoder som specifikt tar upp brott som per definition har koppling till it: datorbedrägeri och bedrägeri med hjälp av internet. Men it-inslag förekommer också bland bedrägerier som inte registreras under dessa brottskoder (Brå 2016:9).

Totalt sett har det inom kategorin bedrägeri och annan oredlighet skett en ökning av andelen brott som har it-inslag, från 41 till 71 procent (figur 5). Det motsvarar en ökning på 73 procent. Som framgått tidigare har antalet datorbedrägerier och bedrägerier med hjälp av internet ökat kraftigt under perioden, vilket har stor inverkan på resultatet. En vanligt förekommande typ av bedrägeri är kortbedrägerier (Brå 2016:9). De flesta av dessa

Figur 5. Andel brott inom kategorin bedrägeri m.m. där det framgår att det finns it-inslag enligt urvalet brottsanmälningar år 2006, 2010 och 2014. Procent.



[20] För en mer detaljerad redogörelse för hur it-inslag kan se ut vid brott mot person, se bilaga 3.

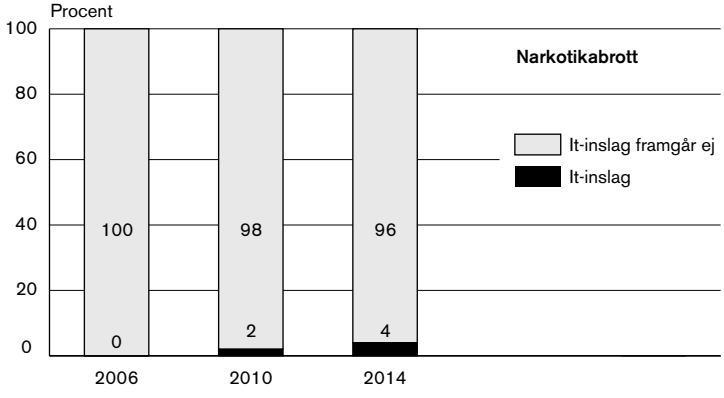
har brottskoden datorbedrägeri enligt anmälningarna, men de återfinns även under brottskoderna för övrigt bedrägeri, kontokortsbedrägeri eller bedrägeri med hjälp av internet.

Det är en stor variation i tillvägagångsättet för anmälda bedrägeribrott med it-inslag. Vanligt vid de polisanmälda kortbedrägerierna i materialet är att målsägaren har sitt kort i behåll men upptäcker att det dragits summor från kontot. Inte sällan gäller det köp eller uttag utomlands i delar av världen som målsägaren inte besökt. En annan relativt vanlig typ av ärenden i materialet gäller försäljning på falska grunder, där bedragarna säljer produkter på försäljningssidor som Blocket eller via andra annonser på internet. Efter betalning levereras aldrig produkterna eller produkten håller inte vad som utlovats.[21]

Fler beslag bakom ökning av it-inslag vid narkotikabrott

Brott mot narkotikastrafflagen (1968:64) tar upp överlåtelse, innehav, eget bruk och framställning av narkotika. De vanligaste anmälda narkotikabrotten gäller innehav och eget bruk. Som framgår av figur 6 visar Brås granskning att det har skett en ökning av it-inslag över tid även vid narkotikabrott, från 0 procent år 2006 till 4 procent år 2014 (figur 6). Samtliga dessa it-inslag utgörs av it-beröring, där det har gjorts ett beslag av de misstänktas mobiltelefoner (tabell 1B i bilaga 1). Dels handlar det om ärenden där personer misstänks för eget bruk eller innehav av narkotika (och i några fall överlåtelse) och där polisen beslagtar

Figur 6. Andel brott inom kategorin narkotikabrott där det framgår att det finns it-inslag enligt urvalet brottsanmälningar år 2006, 2010 och 2014. Procent.



[21] För en mer detaljerad redogörelse för hur it-inslag kan se ut vid bedrägeri och annan oredlighet, se bilaga 3. Se även Brå-rapport 2016:9.

de misstänktas telefoner för att söka efter bevis. Dels handlar det om anmälningar som rör personer som misstänks för andra brott än narkotikabrott, men där en genomgång av meddelanden i deras mobiltelefoner även tyder på befattning med narkotika.

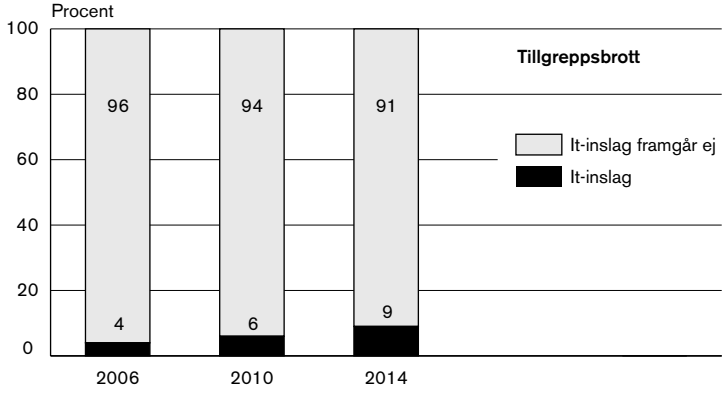
Som tidigare nämnts utgör Brås granskning av andelen it-inslag i de polisanmälda brotten sannolikt en grov underskattning av den faktiska andelen it-inslag i brotten. Det beror på att information om eventuell it-beröring sällan finns tillgänglig eller antecknas i anmälningarnas fritext vid anmälningstillfället. De redovisade nivåerna blir särskilt problematiska för brottstyper där it-inslagen i hög utsträckning består av it-beröring, som vid narkotikabrott.

Enligt Brås intervjuer med personer som är verksamma inom Polismyndigheten är beslag av misstänktas mobiltelefoner vanligt förekommande vid narkotikabrott. Ofta syftar beslaget till att kunna bevisa ett ”köp- och sälj”-förfarande mellan två misstänka personer genom exempelvis sms-korrespondens.

Övervakningskameror bakom ökning av it-relaterade tillgrepps- och skadegörelsebrott

Brottsbalkens kapitel 8 gäller olika tillgreppsbrott, till exempel stöld, inbrott och rån. Här visar Brås genomgång av polisanmälningar en ökande trend över tid av andelen tillgreppsbrott som har it-inslag. Mellan år 2006 och 2014 har denna andel mer än fördubblats från cirka fyra till nio procent (figur 7).[22] Liksom vid narkotikabrott utgörs samtliga it-inslag av någon form av

Figur 7. Andel brott inom kategorin tillgreppsbrott där det framgår att det finns it-inslag enligt urvalet brottsanmälningar år 2006, 2010 och 2014. Procent.



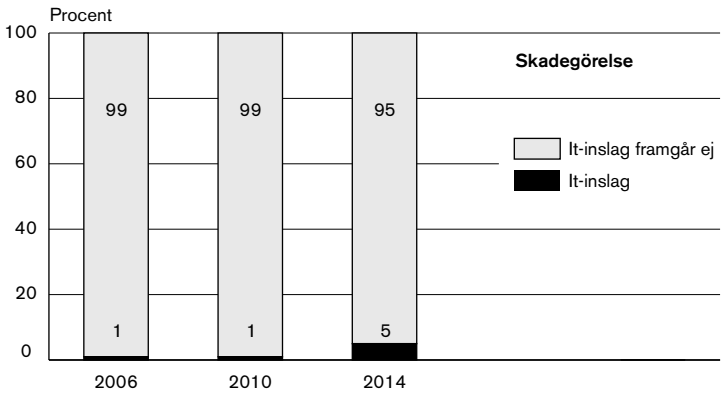
[22] Skillnaderna mellan åren når endast statistisk signifikans på 10-procents nivå (se tabell 1B i bilaga 1). Det ska vidare nämnas att en avgränsning i analysen är att fall som gäller rena stölder av datorer, mobiler och liknande, utan vidare uppgifter i ärendena, inte klassificerats som it-inslag (såtillvida det inte framgått att det finns någon annan slags it-koppling).

it-beröring, vilket innebär att den redovisade nivån för andelen it-inslag bör ses som en grov underskattning (tabell 1B i bilaga 1).

Ökningen av it-inslag vid tillgreppsbrott utgörs i huvudsak av en ökad förekomst av beskrivningar om att det finns övervakningskameror som har, eller kan ha, filmat den brottsliga händelsen eller som bör undersökas. It-inslagen kan även utgöras av beslag av misstänkta personers mobiler. Ett fåtal ärenden gäller stölder som utförts av anställda, där stölderna lämnat spår i arbetsplatsernas datasystem.

Även vid anmälda brott mot brottsbalkens kap. 12 om skadegörelsebrott (t.ex. klotter, skadegörelse på motorfordon och skadegörelse genom brand) kan en ökad förekomst av hänvisningar till övervakningskameror i polisanmälningarna ligga bakom den totala ökningen av it-inslag som observeras inom brottskategorin. Brås granskning visar att andelen it-inslag inom brottskategorin har ökat från 1 procent år 2006 till 5 procent år 2014. Eftersom it-inslagen även vid denna brottstyp enbart utgörs av it-beröring bör de redovisade nivåerna ses som en grov underskattning (figur 8 och tabell 1B i bilaga 1).

Figur 8. Andel brott inom kategorin skadegörelse där det framgår att det finns it-inslag enligt urvalet brottsanmälningar år 2006, 2010 och 2014. Procent.



Förutom hänvisningar till övervakningskameror förekommer beskrivningar om att privatpersoner har filmat händelsen med mobiltelefoner. Det förekommer också att sms-korrespondens mellan misstänkta gärningspersoner har föregått skadegörelsen, vilket därför kan användas som bevismaterial. Enligt Brås intervjuer med polisiära förundersökningsledare finns det en stor potential i de digitala spåren, till exempel vid skadegörelsebrott. Exempelvis kan klottrare som misstänks för ett brott ofta bindas till flera fall av klotter med hjälp av bilder och geopositioneringar i den misstänktes mobiltelefon.

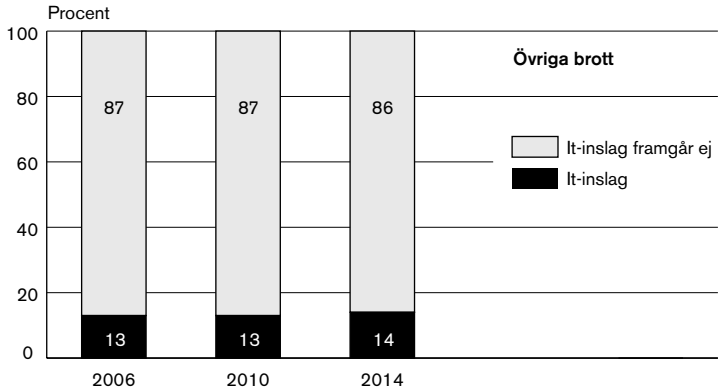
Trafikbrott – svårt att mäta utvecklingen

Brott mot trafikbrottslagen (1951:649) gäller till exempel vårdslöshet i trafik, olovlig körning och rattfylleri.[23] Även brott mot denna lag har ingått i Brås granskning av polisanmälningar. Emellertid visade det sig, som tidigare nämnts, att det interna bortfallet var stort för brottskategorin. Det beror på att en fritext saknades för majoriteten av anmälningarna från åren 2006 och 2010. Det innebär att det inte är meningsfullt med en beskrivning för de olika åren. I det fåtal fall där det framgår någon it-beröring över huvud taget handlar det uteslutande om övervakningskameror.[24]

Övriga brott – ingen ökning av it-inslag

Kategorin ”övriga brott” används ibland i redovisningar av de anmälda brotten i kriminalstatistiken (Brå 2015:16).[25] Den avser brott som inte ingår i de hittills redovisade kategorierna, och täcker ett antal olika brott av varierande slag. Såväl vissa våldseller hotbrott (exempelvis våld mot tjänsteman och övergrepp i rättssak) som andra typer av brott (till exempel överträdelse av kontaktförbud och brott mot skattebrottslagen). Det syns inget klart mönster när det gäller utvecklingen av it-inslag för kategorin övriga brott (figur 9 och tabell 1B i bilaga 1).[26]

Figur 9. Andel brott inom kategorin övriga brott där det framgår att det finns it-inslag enligt urvalet brottsanmälningar år 2006, 2010 och 2014. Procent.



[23] Det är viktigt att notera att fortkörning som gett ordningsbot inte ingår i statistiken över anmälda brott (och därmed inte i urvalet). En annan studie från Brå visar en stor ökning över tid av antalet fortkörningar som upptäcks med hjälp av vägkameror (Brå 2016a).

[24] Sammanlagt 2 procent (sex anmälningar av totalt 289 med fritext).

[25] Kategorin övriga brott utgjorde totalt 11 procent av de anmälda brotten år 2014 (Brå 2015:16).

[26] Skillnaderna mellan åren är inte statistiskt säkerställda.

Det är en relativt stor variation av vilka it-inslag som förekommer i de anmälningar som tillhör denna brottskategori, till exempel överträdelser av kontaktförbud som skett via mobiltelefon, våld mot tjänsteman som filmats av övervakningskamera och brott mot skattebrottslagen, där it-inslagen kan bestå av vilseledande räkenskapsmaterial och bokföring som lagrats digitalt på dataservrar.

Utvecklingen av nya modus och it-inslag

En slutsats utifrån genomgången av urvalet av de polisanmälda brotten är att andelen anmälda brott med it-inslag har mer än fördubblats under den studerade tidsperioden. Andelen brott med it-inslag är störst när det gäller brott mot person och bedrägeribrott, och dessa brottskategorier har därför störst påverkan på resultatet.

Bakom den generella ökning som observeras i polisanmälningarna bedöms ett antal faktorer spela in. En viktig faktor är att det har skett en ökning av brott som per definiton har it-inslag (t.ex. datorbedrägeri, bedrägeri med hjälp av internet, dataintrång). En annan faktor är att utvecklingen av sociala medier avspeglas i ökningar av hot, ofredanden och andra brott som sker via sådana kommunikationsvägar. En tredje faktor är att andelen brott som har filmats av övervakningskameror tycks ha ökat, vilket gäller för flera typer av brott (t.ex. våldsbrott, stöld och skadegörelse). En fjärde faktor som förklarar den ökning av it-inslag som observeras i polisanmälningarna är att polisens beslag av misstänkta personers mobiltelefoner tycks ha ökat, till exempel vid narkotikabrott.

Utvecklingen av antalet it-beslag

Enligt företrädare för NFC är it-spår den typ av spår som växer snabbast inom kriminaltekniken och inom brottsutredningar generellt. För att belysa utvecklingen av it-inslag i de anmälda brotten har Brå, som en kompletterande datakälla, begärt in statistik över beslag som har registrerats i Polisens ärendehanteringssystem DurTvå.[27] Beslagtaget gods registreras i Polisens ärendehanteringssystem i en huvudgrupp och därefter i en undergrupp. I systemet finns huvudgrupper som *Droger/Narkotikaredskap, Fordon/ Fordonstillbehör/Trafik/Flyg* och *Bokföring/Data/Kontor/Telefoni*. Inom huvudgruppen *Bokföring/Data/Kontor/Telefoni* finns bland annat undergrupperna *Mobiltelefon, Datautrustning/Tillbehör/Programvara* samt *Dator/PC/Mac*. Eftersom

[27] Statistiken över registrerade beslag har hämtats från Tvångsmedelstjänsten som är en del av Durtvå. Statistikuttaget har gjorts av Utredningssektionen på Polismyndigheten.

dessa undergrupper rimligtvis kan beskrivas som it-relaterade har Brå valt att studera utvecklingen för dessa undergrupper.

Ett ökat inflöde av registrerade it-beslag kan påverka de brottsutredande myndigheterna i form av ett ökat inflöde till den it-forensiska verksamheten. Det bör dock poängteras att det utifrån statistiken inte går att utläsa om det beslagtagna föremålet har lämnats in för it-undersökning eller inte. Det bör också noteras att skälet till att ett föremål tas i beslag inte framgår av begärd data. Beslag får till exempel tas om föremålet är ”någon avhänt genom brott”, exempelvis om en mobiltelefon som stulits påträffas hos en misstänkt gärningsperson (27 kap. 1 § RB). Ett sådant beslag behöver i regel inte analyseras av en it-undersökare.

De redovisade siffrorna bör därför tolkas med försiktighet. Det ska också betonas att det utifrån materialet inte går att utläsa om det har skett en förändring av komplexiteten av de beslagtagna föremålen som lämnas in för undersökning (t.ex. ökad förekomst av krypterad data) eller av mängden data i den beslagtagna utrustningen. Enligt flera av Brås intervjupersoner har teknikutvecklingen inneburit att till exempel mobiltelefoner har fått en kraftigt ökad lagringskapacitet och även blivit alltmer avancerade under den aktuella tidsperioden. Det gör att det därmed tar längre tid att undersöka varje beslag.

Antalet it-relaterade beslag har ökat

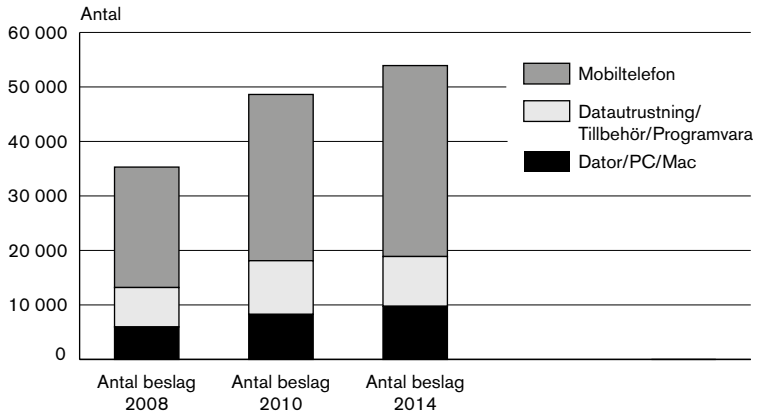
Resultatet visar att det har skett en ökning av antalet it-beslag mellan 2008[28] och 2014 (figur 10). År 2014 registrerades 72 382 beslag i huvudgruppen *Bokföring/Data/Kontor/Telefoni*, vilket kan jämföras med 53 883 beslag år 2008. Det motsvarar en ökning på 34 procent. Ökningen förekommer i samtliga undergrupper av huvudkategorin som Brå har studerat. Den procentuella ökningen är störst inom undergruppen *Dator/PC/Mac* som har ökat med 64 procent. Undergruppen *Mobiltelefon* har ökat med 59 procent och *Datautrustning/Tillbehör/Programvara* har ökat med 26 procent under den aktuella tidsperioden.[29] Den observerade ökningen kan jämföras med den totala ökningen för beslag (för samtliga huvudgrupper) under samma tidsperiod, som är 8 procent.

Även om det utifrån siffrorna inte går att utläsa hur stor andel av det beslagtagna godset som har lämnats in för undersökning till den it-forensiska verksamheten är det sannolikt att ökningen

[28] Beslagsprotokoll har registrerats digitalt och på ett enhetligt sätt från och med år 2008. Brå har därför valt att redovisa statistiken från och med år 2008.

[29] År 2008 registrerades 5 963 beslag i undergruppen Dator/PC/Mac, 22 098 beslag i undergruppen Mobiltelefon och 7 232 i undergruppen Datautrustning/tillbehör/programvara. Motsvarande antal år 2014 var 9 750, 35 036 och 9 135.

Figur 10. Antal beslag i undergrupperna Mobiltelefon, Dator/PC/ Mac och Datautrustning/Tillbehör/Programvara som registrerats i polismyndigheterna under åren 2008, 2010 och 2014.



av antalet it-beslag har inneburit ett större inflöde till Polismyndighetens it-forensiska sektioner. Att det har skett en ökning av antalet it-beslag bekräftas av flera av Brås intervjupersoner, både inom den brottsutredande och inom den it-forensiska verksamheten. Intervjupersonerna är även överens om att bevisen som it-beslagen kan generera många gånger har mycket stor betydelse för utredningen och att det finns en underutnyttjad potential i den information som ligger lagrad i till exempel mobiltelefoner. Flera menar dock att polisen i dag ”tar beslag och tömmer mobiltelefoner i nästan vartenda ärende”, och en del menar att det har skett en ”informationsöverdos” av bevismaterial från mobiltelefoner.

Utveckling av den självrapporterade utsattheten för bedrägeri och hot enligt NTU

Ett annat sätt att studera brottsutvecklingen är att använda sig av frågeundersökningar till representativa urval av befolkningen. I Brås rikstäckande Nationella trygghetsundersökning (NTU) får 12 000 personer mellan 16 och 79 år besvara frågor om utsatthet för brott, trygghet, förtroende för rättsväsendet samt brottsoffers kontakter med rättsväsendet. Respondenter som uppger sig ha utsatts för brott under föregående år ges ett antal följdfrågor om olika omständigheter kring det brott de utsatts för, till exempel var brottet ägde rum.[30] För brottstyperna bedrägeri och hot går det att utifrån undersökningen urskilja hur stor andel av brotten som har skett via internet. En av fördelarna med undersökningen

[29] Respondenter som uppger att de utsatts för hot ges i NTU en följdfråga om på vilket sätt de blev hotade, där telefonsamtal/sms och e-post/chatt/internet är två möjliga svarsalternativ. Respondenter som uppger sig ha utsatts för bedrägeri får svara på frågan om det var via internet som personen "blivit lurad" (Brå 2016:1).

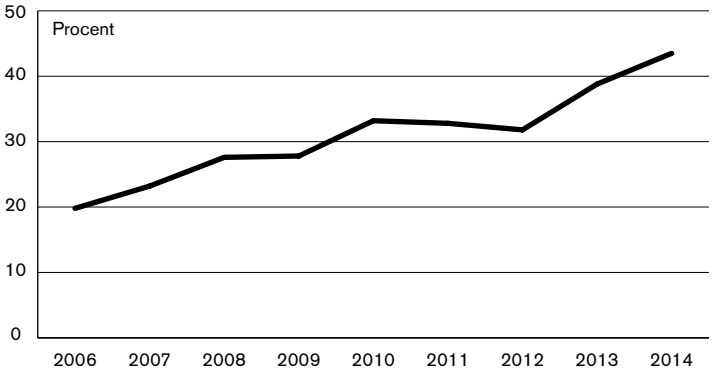
är att det går att studera utvecklingen av brottsligheten utan att vara beroende av att brottet har anmälts till polisen. En annan fördel med att använda NTU, jämfört med kriminalstatistiken, är att det utifrån undersökningen är möjligt att se om brotten ändrar karaktär, till exempel om allt fler brott äger rum i it-miljö.

Ökning av bedrägerier och hot via internet

Enligt NTU har andelen personer som utsatts för bedrägeri under föregående år i genomsnitt legat på cirka 3 procent under hela tidsperioden 2006 till 2014. I förhållande till förändringen av befolkningsmängden har det skett en viss ökning av det skattade antal som uppger sig ha utsatts för bedrägeri.

I 2006 års undersökning uppgick det skattade antalet bedrägerier via internet i befolkningen till 52 178, och i 2014 års undersökning hade detta antal ökat till 139 541. Det motsvarar en ökning på 167 procent avseende bedrägerier via internet. I 2006 års NTU uppgavs närmare 20 procent av bedrägerierna ha ägt rum via internet och i 2014 års undersökning har denna andel ökat till 44 procent (figur 11).[31]

Figur 11. Skattad andel av bedrägerihändelserna i befolkningen (16–79 år) som skett via internet, enligt NTU. Procent.



År 2006 uppgav 4,6 procent av personerna som besvarade NTU att de hade utsatts för hot under det föregående året, oavsett tillvägagångssätt. Sedan dess har nivån legat stabilt kring drygt 4 procent.

I 2008 års undersökning[32] uppgick det skattade antalet hot via ”e-post, chatt eller internet” i befolkningen till 24 534. I 2014 års undersökning hade antalet ökat till 46 836. Det motsvarar en ök-

[31] Kategorierna är inte ömsesidigt uteslutande då de bygger på två separata frågor.

[32] Svarsalternativen för hur respondenterna blivit hotade var annorlunda för 2005-2007, vilket gör att de inte går att jämföra med övriga år.

ning med 91 procent av hot via internet. Resultatet innebär även att en större andel av de hot som allmänheten utsätts för numera äger rum via internet (2,7 procent år 2008, 6,6 procent år 2014).

Resultaten i korthet

- Resultatet från samtliga datakällor som Brå har använt för att kartlägga hur förekomsten av it-inslag i de anmälda brotten har utvecklats visar att det har skett en tydlig ökning av it-relaterade brott under perioden 2006–2014. Ökningen gäller både totalt sett och för flera olika brottstyper.
- Enligt den officiella kriminalstatistiken har de brott som utifrån brottskod anger att brottet har it-inslag (datorbedrägeri, bedrägeri med hjälp av internet, dataintrång samt internetrelaterade barnpornografibrott) ökat med 949 procent.
- I Brås granskning av polisanmälningar framkommer att it-inslagen i de polisanmälda brotten totalt sett har mer än fördubblats mellan åren 2006 och 2014. Andelen brott med it-inslag är störst inom brottstyperna brott mot person och bedrägeri.
- Kartläggningen visar även att antalet registrerade it-beslag har ökat, i synnerhet när det gäller beslagtagna mobiltelefoner och datorer.
- Brås nationella trygghetsundersökning om brott (NTU) visar att både bedrägerier via internet och internetrelaterade hot har ökat under tidsperioden.

Utifrån resultaten går det att konstatera att rättsväsendet står inför stora utmaningar att hantera den ökade andelen brott med it-inslag, vilket ställer stora krav på både kompetens och kapacitet.

Kompetensen gällande brott med it-inslag

En del av regeringens uppdrag till Brå handlar om att analysera vilken kompetens och kapacitet den brottsutredande verksamheten har när det gäller it-relaterad brottslighet och it-forensiska undersökningar. I detta ingår att belysa brister och utvecklingsmöjligheter. Det här kapitlet riktar fokus på kompetens. Frågan om hur kapaciteten ser ut behandlas i nästkommande kapitel. Med kompetens avses i den här rapporten att individen har relevanta kunskaper och färdigheter för att kunna hantera ärenden med it-inslag.

I kapitlet redovisas resultat från Brås enkätundersökning till åklagare, polisiära förundersökningsledare och it-undersökare i landet. I kapitlet redovisas även vad som framkommit i Brås intervjuer med samma yrkesgrupper angående vilken kompetens som är nödvändig för att kunna hantera brott med it-inslag och vilka brister och utvecklingsmöjligheter som finns på området. En mer utförlig beskrivning om de olika datamaterialen ges i rapportens metodavsnitt.

I ett första steg redogörs för hur *utbildningsnivån* ser ut bland åklagare, polisiära förundersökningsledare och it-undersökare avseende brott med it-inslag. I ett andra steg redogörs för hur *kunskaperna* ser ut när det gäller två aspekter av den brottsutredande verksamheten: kunskaper om utredningsåtgärder för att identifiera potentiella gärningspersoner när brottet har begåtts via internet samt kunskaper om utredningsåtgärder för att kunna säkra digitala bevis. Det handlar främst om att respondenterna ska känna till möjligheten att kunna utföra olika utredningsåtgärder, snarare än hur man rent tekniskt går tillväga. I ett tredje steg redogörs för it-undersökarnas *tekniska kunskaper* för att genomföra beställda undersökningar och i ett fjärde steg kunskapen om it-relaterade brott hos polisens utredare och bland poliser i yttre tjänst. Kapitlet avslutas med att belysa åklagarnas och de polisiära förundersökningsledarnas kunskaper om att göra beställningar till it-undersökare, s.k. *beställarkompetens*.

Det interna bortfallet[33] på enkätens frågor är lågt och varierar i de flesta fall mellan 1 och 6 procent. Vid det fåtal frågor där bortfallet överstiger denna nivå redogörs för det i samband med resultatredovisningen. Beskrivningarna över vilka utredningsåtgärder som är möjliga i utredningar med it-inslag har hämtats från olika källor, bland annat den webbaserade guide för it-relaterade brott som Åklagarmyndigheten publicerade år 2015, men även från muntliga och skriftliga kontakter med företrädare från Åklagarmyndigheten, Polismyndigheten, t.ex. Nationella Operativa avdelningen (Noa) och Nationellt forensiskt centrum (NFC), samt relevant litteratur på området.

Utbildningsnivå bland åklagare, polisiära förundersökningsledare och it-undersökare

Den ökade förekomsten av digitala bevis ställer nya krav på rättsväsendet när det gäller utbildning och kunskap om möjliga utredningsåtgärder i digital miljö. Bland annat ställer insamling av digitala bevis stora krav på både teknik och regelverk. Dessa krav ställs inte enbart på dem som genomför åtgärden, utan även på den som beslutar om åtgärden, bedömer den och i olika avseenden värderar resultatet av den (Kronqvist 2013). Ett sätt att erhålla nödvändig kunskap på it-området[34] är genom grundutbildningen för åklagare respektive poliser. Enligt Åklagarmyndighetens Utbildningscentrum behandlas i dagsläget it-frågor på grundutbildningen både som ett enskilt block och som en del i de kursmoment där det bedöms vara relevant. Polisens grundutbildning innehåller däremot ingen särskild kurs om it-relaterad brottslighet. Enligt polisens HR-avdelning är it-aspekten heller inte tillräckligt integrerad på kurser rörande andra ämnen. För en redogörelse över hur it-inslag är integrerade i åklagarnas och polisens grundutbildning, se kapitlet *Angelägna utvecklingsområden och pågående utvecklingsarbete*.

Ett annat sätt att erhålla kunskap på it-området är genom att delta i vidareutbildning som erbjuds i Åklagarmyndighetens eller Polismyndighetens regi. Åklagarna och de polisiära förundersökningsledarna tillfrågades i enkäten om vilken vidareutbildning inom it-området de har gått.[35] It-undersökarna tillfrågades,

[33] Internt bortfall innebär att respondenten inte har besvarat frågan. Till bortfallet hör i det här kapitlet även respondenter som svarat ”vet ej” när ett sådant svarsalternativ har funnits.

[34] Med ”kunskaper på it-området” avses alla typer av kunskaper kopplade till utredningar av brott med it-inslag.

[35] Med vidareutbildning avses här utbildning som ges till personer som efter avslutad grundutbildning får kompetensutveckling inom ett visst område. I enkäten görs ingen åtskillnad mellan begreppen vidareutbildning och fortbildning. Vidareutbildningen kan både bestå av en utbildning med tydliga kursmål som ska bedömas eller som löpande fortbildning inom ett visst område utan krav på examination.

förutom om sin vidareutbildning, även om de hade en akademisk högskole- eller universitetsutbildning på it-området.

Hälften av åklagarna saknar vidareutbildning på it-området

Inom Åklagarmyndigheten ges för närvarande en vidareutbildningskurs i it-brottslighet, vilken har namnet *It-brott och bevissäkring i it-miljö*, även kallad *IT-brottskursen*.[36] Kursen ingår i åklagarnas specialistutbildning och vänder sig till åklagare som har genomgått grundutbildningen och arbetat några år efter det. Kursen omfattar fem dagar, och syftet är att deltagarna ska få grundläggande kunskaper om brott och bevisning i digital miljö. Därutöver berörs it-aspekten översiktligt vid vidareutbildningskurser som handlar om övergrepp mot barn, bedrägeri och ungdomar och brott.

I Brås enkät till åklagare tillfrågades respondenterna om de har gått den aktuella kursen och i så fall vilket år. Åklagarna tillfrågades också om de hade gått någon ”annan vidareutbildning avseende brott med it-relevans” och vilken kurs det i så fall gällde. Resultatet visade sammantaget att 54 procent av åklagarna inte hade fått någon vidareutbildning på it-området. Resultatet är i linje med en tidigare kunskapsinventering som gjorts av Rikspolisstyrelsen (2012), där det framgick att hälften av åklagarna inte hade fått någon it-relaterad utbildning. För en mer detaljerad redogörelse över hur stor andel av åklagarna som har deltagit i någon vidareutbildning på it-området, vilken slags utbildning de i så fall genomgått samt skillnader mellan olika åklagarområden, se avsnittet *Inventering av respondenternas utbildningsnivå* i bilaga 5.

Nio av tio polisiära förundersökningsledare saknar vidareutbildning på it-området

Inom Polismyndigheten ges sedan år 2014 en kurs inom området it-relaterad brottslighet som specifikt riktar sig till förundersökningsledare: *It-forensisk översiktskurs för förundersökningsledare*. Kursen, som ges under fem dagar, innehåller juridik som rör ”brott med it-relation”, internetarkitektur, it-forensik och internationellt samarbete.[37] Därtill erbjuds en liknande kurs som riktar sig till anställda som arbetar som utredare av it-relaterade brott *(It-forensisk översiktskurs för utredare)* samt en kurs som

[36] Kursen har funnits sedan 2002.

[37] Efter godkänd kurs ska kursdeltagaren bland annat kunna göra en prioritering av initiala åtgärder, göra korrekta beställningar till it-forensiker, tolka it-forensiska resultat och redogöra för relevant lagstiftning kopplat till ärenden med ”it-relation” (Kursplan, beslutsdatum 2016-03-03).

riktar sig till personal som arbetar med inhämtningsarbete på internet *(Underrättelse- och inhämtningsarbete på Internet, baskurs)*.[38] För att få en så uttömmande bild som möjligt av de polisiära förundersökningsledarnas utbildningsnivå tillfrågades de därför om de har gått någon av dessa kurser, samt vilket år de i så fall hade gått den aktuella kursen. De tillfrågades även om de hade gått någon ”annan vidareutbildning avseende brott med it-relevans” och i så fall vilken kurs de hade gått.

Sammantaget visar resultatet att 90 procent av de polisiära förundersökningsledarna helt saknar vidareutbildning på it-området.[39] Även det resultatet är i linje med den kunskapsinventering som Rikspolisstyrelsen genomförde år 2012, där det framgick att över 90 procent inte hade någon utbildning som rör bevissäkring av digitala spår (Rikspolisstyrelsen 2012). Även i Riksrevisionens rapport (2015) framgår att utbildningsnivån rörande brott med it-relevans är låg hos polisiära förundersökningsledare. För en mer detaljerad redogörelse över hur stor andel av de polisiära förundersökningsledarna som har gått någon utbildning på it-området, och vilken slags utbildning de i så fall genomgått, se avsnittet *Inventering av respondenternas utbildningsnivå* i bilaga 5.

Drygt var tionde it-undersökare saknar vidareutbildning på it-området

Inom polisen finns det personer som har som främsta arbetsuppgift att arbeta med hanteringen av digitala spår och bevis. Personer med sådana arbetsuppgifter har ingen enhetlig benämning, men kallas vanligtvis för it-forensiker, it-brottsspecialister eller it-undersökare. De har i normalfallet genomgått en viss rekommenderad utbildning som är inriktad på digitala bevis, men också på teknikkompetens (Kronqvist 2013).

I Brås rapport används samlingsbegreppet *it-undersökare* för samtliga personer inom Polismyndigheten som genomför olika typer av it-undersökningar.[40] I vissa analyser delas gruppen it-undersökare in i undergrupperna *it-forensiker* (64 procent) och *övriga it-undersökare* (36 procent). Övriga it-undersökare är

[38] Kursen *Underrättelse- och inhämtningsarbete på internet*, baskurs (tidigare *Grundläggande underrättelsearbete på internet*) ges under 10 dagar. Även denna kurs har funnits sedan år 2014 och innehåller bland annat it-teknik, it-juridik och information om internationella och nationella samarbetsformer. Syftet är att förbättra kvaliteten inom underrättelse- och utredningsarbete på internet (Kursplan beslutsdatum 2014-02-10).

[39] Det är stor variation i de utbildningar som polisiära förundersökningsledare uppger att de har gått, allt från enstaka kurser i Office-paketet till en särskild kurs om it-relaterad brottslighet.

[40] Enkäten riktade sig till personer som arbetar med undersökning av it-media, analys av data, internetinhämtning, granskning av barnpornografi samt analys och bearbetning av bild/film/ljud.

personer som går under någon annan benämning än it-forensiker, till exempel utredare, handläggare, it-tekniker, it-brottsspecialist, it-brottsutredare, analytiker, bildtekniker, mobilforensiker m.m.

Det finns i dagsläget flera olika sätt att utbilda sig till it-undersökare. Av de totalt 132 it-undersökare som besvarade Brås enkät uppgav 30 procent att de var utbildade poliser, medan 70 procent var civilanställda. Civila it-undersökare har i regel någon form av högskole- eller universitetsutbildning på it-området. Ett annat sätt att utbilda sig till it-undersökare är genom att (efter avslutad polisutbildning) genomgå någon av Polismyndighetens två fördjupande vidareutbildningar inom it-forensik: *It-forensiker grundutbildning – Etapp 1* eller *It-forensiker grundutbildning – Etapp 2*.[41] Kursen vänder sig till polisen, men är även öppen för deltagare från bland annat Åklagarmyndigheten, Ekobrottsmyndigheten och Tullverket. Utbildningens andra steg (etapp 2) är en fortsättningskurs och riktar sig till personer som har gått utbildningens första del eller som har motsvarande högskoleutbildning. Därutöver erbjuds ett femtontal kortare kurser som i regel gäller något bestämt digitalt verktyg. Kurserna leds därför ofta av inhyrd personal från något av programvaruföretagen.

I Brås enkät fick it-undersökarna svara på flera frågor rörande deras utbildningsnivå. Frågorna avsåg både kurser och utbildningar som erbjuds vid Polismyndigheten och utbildningar inom it-området som ges vid högskola eller universitet. Resultaten från Brås enkät visar att majoriteten (71 procent) av it-undersökarna har en gedigen utbildning på it-området, det vill säga att de *antingen* har läst någon av de två it-forensiska utbildningar som erbjuds vid Polismyndigheten (etapp 1 eller 2) och/eller att de har en akademisk examen på it-området. Ytterligare 17 procent uppger att de har läst en eller flera kurser på it-området, antingen i Polismyndighetens regi eller vid en högskola/universitet, men att dessa kurser inte har lett fram till en akademisk examen. Dock visar resultaten att 12 procent av it-undersökarna helt och hållet saknar utbildning på it-området.[42]

It-undersökarna är en heterogen grupp, och utbildningsnivån på it-området är generellt sett betydligt högre bland de it-undersökare som kallas för it-forensiker. Av de it-undersökare som går under benämningen it-forensiker har 97 procent en gedigen utbildning, medan enbart 2 procent uppger att de saknar utbildning på it-området. I den övriga gruppen av it-undersökare har enbart 26 procent en gedigen utbildning, och 30 procent saknar

[41] Etapp 1 ges under 58 dagar och Etapp 2 ges under 20 dagar. Båda kurserna upphör i slutet av 2016.

[42] Drygt hälften av dem som saknar utbildning har en polisiär bakgrund och resterande är civilanställda. De vanligaste arbetsområdena för dessa it-undersökare är bild/film och ljud (88 procent) samt mobila enheter (69 procent).

utbildning på it-området. För en mer detaljerad redogörelse över it-undersökarnas utbildningsnivå, se avsnittet *Inventering av respondenternas utbildningsnivå* i bilaga 5.

Kunskaper om möjliga utredningsåtgärder för att spåra gärningspersoner på internet

En förundersökningsledare har det övergripande ansvaret för att leda en förundersökning, vilket kräver tillräckligt god kunskap och förståelse för digitala spår. I en utredning där det förekommer it-inslag är det förundersökningsledarens uppgift att ha kunskap om vilka utredningsåtgärder som är möjliga att genomföra för att utreda brottet. Utredningar av it-relaterade brott skiljer sig från traditionellt polisarbete när det gäller vilka möjliga utredningsåtgärder som förundersökningsledaren har i sin ”verktygslåda” för att till exempel kunna spåra gärningspersoner eller säkra bevis. Enligt den kompetensprofil som Forensiska rådet[43] har tagit fram för förundersökningsledare, när det gäller förmågan att utreda it-relaterade brott, ska dessa bland annat ”ha kunskap om relevant lagstiftning och praxis, ha en övergripande it-kunskap och kunna tillräckligt om it för att i dialog med expertis kunna avgränsa analysarbetet och värdera resultaten” (FOR 2011). I det här avsnittet redogörs för respondenternas kunskaper om att spåra potentiella gärningspersoner i digital miljö. I nästkommande avsnitt redovisas kunskaperna kring att säkra digitala bevis.

För att identifiera personer som begår brott i digital miljö är en central utredningsåtgärd att försöka spåra gärningspersonens IP-adress. IP-adressen är ett unikt nummer som används för att identifiera en abonnent som är uppkopplad mot internet. Adressen tilldelas av en internetleverantör och kan, med stöd av 6 kap. 22 § lagen (2003:389) om elektronisk kommunikation (LEK), begäras ut vid misstanke om brott. Polisen måste först få tag i den aktuella IP-adressen, till exempel genom att kontakta den webbsida/-tjänst som använts vid den brottsliga gärningen. Därefter måste polisen ta reda på vilken operatör som tillhandahållit IP-adressen vid det aktuella tillfället. Slutligen kontaktas den aktuella operatören för att få ut uppgiften om vilket abonnemang som använde IP-adressen vid den aktuella tidpunkten.

Om den brottsliga gärningen har ägt rum på webbsidor eller kommunikationstjänster som har sin server i Sverige är det enligt Brås intervjupersoner sällan något problem med att få ut IP-adressen. I dag sker dock en stor del av kommunikationen på internet via företag som har sin server utomlands. Såväl Micro-

[43] Forensiska rådet bildades år 2009 och har som uppgift att utveckla och samordna kriminaltekniken i Sverige.

soft (som bland annat tillhandahåller webbtjänsterna Outlook och Skype) och Google (som bland annat tillhandahåller Gmail och YouTube) har sina säten i USA.[44] För att få ut dessa uppgifter måste polisen kontakta det aktuella företaget och ansöka om att få ut uppgifterna.[45]

I USA gäller principen att internetleverantören själv får bestämma om den vill lämna ut information från sin internetsida till utländska myndigheter (s.k. ”voluntary disclosure”). Det är dock enbart tillämpligt på abonnentuppgifter och trafikdata såsom IP-adresser (s.k. ”non content information”). Om internetföretaget inte vill lämna ut uppgifterna, eller om de brottsutredande myndigheterna önskar få tillgång till innehållet i ett visst meddelande krävs ofta internationell rättslig hjälp. Det innebär i praktiken att en svensk åklagare måste skriva en begäran om rättslig hjälp som skickas via Justitiedepartementet till dess motsvarighet i USA, som i sin tur efter kontroll vidarebefordrar begäran till rätt myndighet där. Formerna för att ansöka om rättslig hjälp regleras i lagen (2000:562) om internationell rättslig hjälp i brottmål. Det är dock lagstiftningen i det land dit ansökan skickas som avgör om ansökan om rättslig hjälp beviljas eller inte. Enligt Åklagarmyndigheten (2015a) aktualiseras frågor om rättslig hjälp relativt ofta i it-relaterade brottsutredningar, inte enbart vid grova brott.

I Brås enkät tillfrågas respondenterna om sina kunskaper om de ovan beskrivna utredningsåtgärderna för att spåra potentiella gärningspersoner via internet. Respondenterna fick själva bedöma sina kunskaper om respektive utredningsåtgärd som mycket goda, goda, bristfälliga eller mycket bristfälliga.[46] Avsnittet syftar till att identifiera om det finns utredningsåtgärder där kunskapen är särskilt låg och där det finns ett särskilt behov av kompetensutveckling.

Bristande kunskaper om att spåra gärningspersoner på internet

Resultatet från Brås enkät visar att endast hälften av åklagarna och drygt var femte polisiär förundersökningsledare bedömer att deras kunskaper är goda eller mycket goda, när det gäller *möjligheten att spåra potentiella gärningspersoner via IP-adress*. Kun-

[44] Det gäller även företag som Apple och Yahoo samt kommunikationsapplikationer som Facebook, Twitter och Snapchat.

[45] Vid It-brottscentrum (SC3) vid Nationella Operativa Avdelningen (Noa) finns en deskfunktion som är behjälplig när viss information begärs ut från de utländska företagen. Desken har upparbetat ett samarbete, en s.k. SPOC (Single Point of Contact) med en del av företagen, exempelvis Facebook.

[46] Det bör poängteras att resultatet endast baseras på deras egna bedömningar av sin kunskap. Det går inte att säkerställa att respondenterna verkligen har den kunskap som de uppger att de har.

skapsnivån är högst bland it-undersökarna, där drygt 80 procent bedömer sina kunskaper som goda eller mycket goda (tabell 3).

Det är tydligt att kunskaperna är högre bland it-undersökare som går under benämningen it-forensiker, jämfört med gruppen övriga it-undersökare, se tabell 2B i bilaga 1.

Tabell 3. Kunskapen om att spåra potentiella gärningspersoner i digital miljö. Andel i vardera respondentgrupp som uppger att deras kunskapsnivå är god/mycket god respektive bristfällig/mycket bristfällig. Procent.

	Goda/mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Möjligheten att spåra potentiella gärningspersoner via IP-adress		
Åklagare (n = 384)	48	52
Polisiära fu-ledare (n = 655)	22	78
It-undersökare (n = 126)	81	19
Möjligheten att få ut information från externa aktörer utomlands om vem som har registrerat en viss tjänst eller vilka IP-adresser som använt tjänsten den senaste tiden (IP-loggar)		
Åklagare (n = 370)	25	75
Polisiära fu-ledare (n = 635)	13	87
It-undersökare (n = 125)	59	41
Kunskaper om att skriva en rättshjälpsbegäran för att få ut uppgifter från externa aktörer utomlands		
Åklagare (n = 377)	40	60

Eftersom spårning av IP-adresser är en så pass central utredningsåtgärd i utredningar av brott med it-inslag tyder resultaten på att det finns ett behov av kunskapshöjning inom de brottsutredande myndigheterna i detta avseende, i synnerhet bland de polisiära förundersökningsledarna. Även i Riksrevisionens granskning dras slutsatsen att polisen behöver höja sin kunskap om IP-adresser (Riksrevisionen 2015).

I Brås enkät tillfrågades respondenterna även om hur deras kunskaper såg ut när det gäller *vilka möjligheter som finns att få ut information från externa aktörer utomlands kring vem som har registrerat en viss tjänst (t.ex. ett användarkonto) eller vilka IP-adresser som använt tjänsten den senaste tiden (IP-loggar)*. Resultatet visade att kunskapsnivån är låg bland åklagarna och de polisiära förundersökningsledarna även i detta avseende. Endast 25 procent av åklagarna och 13 procent av de polisiära förundersökningsledarna uppger att de har goda eller mycket goda kunskaper om vilka möjligheter som finns att få ut information från externa aktörer utomlands. Bland it-undersökarna är motsvarande andel 59 procent (tabell 3).

Resultatet visar således att det även finns ett stort behov av kompetensutveckling kring vilka möjligheter det finns att få ut information från externa aktörer utomlands, vilket även bekräftas av Brås intervjupersoner. Samtliga yrkesgrupper (även it-undersökare) är eniga om att det behövs en ökad kunskap om det praktiska tillvägagångssättet för att få ut uppgifter från externa aktörer utomlands, till exempel vem man ska vända sig till, men också information kring vad de olika aktörerna lämnar ut för slags information. Det är emellertid svårt att upprätthålla en hög kompetensnivå på detta område eftersom förutsättningarna ständigt förändras.

Brås enkät visar vidare att endast 4 av 10 åklagare[47] bedömer att de har goda eller mycket goda kunskaper om att *skriva en rättshjälpsbegäran för att få ut uppgifter från externa aktörer utomlands*. Åklagare som Brå har intervjuat menar att det är svårt att upprätthålla en god kunskap på området, då man som åklagare så sällan formulerar en rättshjälpsbegäran. Proceduren kring internationell rättslig hjälp upplevs dessutom vara komplicerad och tidskrävande.

Kunskaper om möjliga utredningsåtgärder för att säkra digitala bevis

I utredningar med it-inslag finns som regel digitala bevis som kan behöva säkras. En vanligt förekommande utredningsåtgärd i dessa utredningar är beslag i brottsutredande syfte. En mobiltelefon eller dator kan innehålla värdefull information vid flera typer av brott, även vid brott där it-inslagen inte är lika självklara. Det kan handla om en misshandel som har filmats med hjälp av en mobiltelefon eller sms- eller telefontrafik mellan misstänkta i samband med ett brott. I en polisutredning kan det exempelvis finnas ett intresse av att få tillgång till sms, mms, bilder, datafiler och e-post, som kan innehålla värdefull information för brottsutredningen.

Enligt Åklagarmyndighetens beslagshandbok får ett föremål som tagits i beslag även undersökas, vilket sker genom ett beslut om s.k. tömning (Åklagarmyndigheten 2013). Det finns emellertid lagstiftning som reglerar vilken slags information i en dator eller mobiltelefon som de brottsutredande myndigheterna får ta del av. Dessa regler utgår från var den aktuella informationen finns lagrad. Information kan ligga lagrad lokalt i datorns eller mobiltelefonens lagringsminne, hos en teleoperatör eller på internet (t.ex. på utländska servrar). Inom ramen för ett beslagsbeslut har poli-

[47] Eftersom det endast är åklagare som skriver rättshjälpsansökan ställdes frågan i enkäten enbart till åklagare.

sen endast rätt att undersöka sådan information som finns lagrad lokalt, på till exempel en dators eller mobiltelefons lagringsminne (Kronqvist 2013). Om de brottsutredande myndigheterna däremot vill få tillgång till information som finns lagrad hos en teleoperatör (till exempel meddelanden på en röstbrevlåda, e-post eller telefonlistor) krävs ett beslut om hemliga tvångsmedel, antingen genom hemlig avlyssning av elektronisk kommunikation (HAK) eller hemlig övervakning av elektronisk kommunikation (HÖK), se t.ex. Kronqvist 2013 och Åklagarmyndigheten 2013.[48] För att kunna få ta del av meddelanden (t.ex. röstmeddelanden eller e-post) som finns lagrade hos en operatör krävs ett beslut om HAK. För att kunna ta del av uppgifter som t.ex. visar vilka elektroniska kommunikationsutrustningar som funnits i ett visst geografiskt område, krävs ett beslut om HÖK.[49] En förundersökningsledare bör således känna till vilka delar av en mobiltelefon som går att undersöka och när det krävs ett beslut om hemliga tvångsmedel.

En förundersökningsledare behöver också ha kunskap om möjligheterna att säkra bevismaterial som ligger på internet. I dag ligger en stor del av informationen i mobiler och datorer inte lagrat i själva enheten utan finns i det s.k. ”molnet”. Det innebär att informationen i till exempel en dator lagras hos det företag som anlitas av användaren, och som kan ha sin server i ett annat land. I dag är det också vanligt att många människor kommunicerar med varandra via kommunikationsapplikationer som Facebook, Kik och Snapchat, vilkas servrar ofta ligger utomlands. Om internetföretagets server finns i Sverige gäller svensk lagstiftning. Bevismaterial (t.ex. i form av elektroniska meddelanden) kan då begäras ut efter ett beslut om hemliga tvångsmedel eller husrannsakan, beroende på om informationen finns lagrad hos en operatör eller hos någon annan. Om ett meddelande däremot finns lagrat på en utländsk server krävs i regel ett tillstånd från en domstol/myndighet i det landet, vilket innebär att internationell rättslig hjälp ska sökas.

Bevismaterial som ligger ute på internet är flyktigt och riskerar att snabbt raderas innan polisen har hunnit säkra det. En förundersökningsledare bör därför också ha kunskap om tillvägagångssättet för att begära en så kallad ”frysning”. En frysning innebär att det sparas en ögonblicksbild över det aktuella kontot/hemsidan, så att inte informationen förändras eller raderas. I

[48] Möjligheterna att få ut information från teleoperatörerna styrs även av lagen om elektronisk kommunikation (LEK).

[49] För ett beslut om HAK krävs att flera förutsättningar är uppfyllda, t.ex. att någon är skäligen misstänkt för brottet och att brottet har ett straffminimum om minst två års fängelse eller försök, förberedelse eller stämpling till ett sådant brott (27 kap.18 § RB). En av förutsättningarna för ett beslut om HÖK är att det för brottet inte är föreskrivet lindrigare straff än fängelse i sex månader (27 kap. 19 § RB).

första hand görs detta när polis eller åklagare behöver få ut innehållet från exempelvis en chatt eller hemsida genom rättslig hjälp, vilket riskerar att ta lång tid.

I en brottsutredning kan det vidare finnas ett behov av att kunna ta del av information från olika webbsidor. Det kan handla om allt ifrån svenska och utländska nyhetssidor och bibliotekstjänster till sidor som skyddas av exempelvis ett lösenord. Sådant arbete brukar inom polisen vanligtvis benämnas ”internetspaning” eller ”internetinhämtning”. De brottsutredande myndigheternas möjlighet att ta del av information på internet styrs av hur tillgänglig informationen är för allmänheten. Information som är allmänt tillgänglig på internet får de brottsutredande myndigheterna också ta del av. Det kan till exempel ske genom att ta en skärmdump eller att sidan laddas ner i sin helhet. Om informationen däremot skyddas av ett lösenord, eller om särskilda villkor reglerar åtkomsten till informationen, kan tillträde till den i vissa fall vara olovlig, och polisen riskerar därmed att göra sig skyldig till dataintrång (se t.ex. Kronqvist 2013).

I det här avsnittet redogörs för respondenternas kunskaper om de ovan beskrivna utredningsåtgärderna för att säkra bevis i digital miljö. Liksom i föregående avsnitt har respondenterna fått bedöma sina kunskaper kring respektive utredningsåtgärd som mycket goda, goda, bristfälliga eller mycket bristfälliga.

Kunskapen högst gällande bevisningssäkring i lokala hårddiskar

Majoriteten av respondenterna i Brås enkät uppger att de har goda eller mycket goda kunskaper om de rättsliga möjligheterna *att ta del av elektroniska meddelanden som ligger lagrade på en mobiltelefons eller dators lagringsminne*. Närmare 80 procent av åklagarna och 65 procent av de polisiära förundersökningsledarna uppger att de har goda kunskaper i detta avseende (tabell 4). Andelen som uppger att de har goda kunskaper är högst bland it-undersökarna (88 procent), i synnerhet bland de it-undersökare som går under benämningen it-forensiker (tabell 2B i bilaga 1).

Även om de flesta åklagare och polisiära förundersökningsledare har goda kunskaper om de rättsliga möjligheter som finns att säkra bevisning som ligger lagrad lokalt bör det poängteras att det inte alltid är lätt att veta exakt var en viss information finns lagrad. Exempelvis kan ett sms lagras i mobiltelefonen, men det kan också finnas lagrat på en server utomlands (t.ex. om det har skickats genom kommunikationsapplikationen iMessage).

Majoriteten av åklagarna (75 procent) uppger även att de har goda kunskaper när det gäller de *rättsliga möjligheterna att*

Tabell 4. Kunskapen om möjligheten att säkra lokalt lagrad bevisning samt bevisning som lagras hos teleoperatör. Andel i vardera respondentgrupp som uppger att deras kunskapsnivå är god/mycket god respektive bristfällig/mycket bristfällig. Procent.

	Goda/mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Rättsliga möjligheter att ta del av elektroniska meddelanden som ligger på en mobiltelefons/dators lagringsminne		
Åklagare (n = 381)	78	22
Polisiära fu-ledare (n = 659)	65	35
It-undersökare (n = 129)	88	12
Rättsliga möjligheter att säkra bevisning genom avlyssning eller övervakning av elektronisk kommunikation (HAK eller HÖK)		
Åklagare (n = 381)	75	26
Polisiära fu-ledare (n = 654)	48	52
It-undersökare (n = 125)	25	75

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

säkra bevisning genom avlyssning eller övervakning av elektronisk kommunikation (HAK eller HÖK), vilket ofta behövs då bevismaterialet ligger lagrat hos en teleoperatör (t.ex. röstmeddelanden i en mobiltelefon). Eftersom beslutet om HAK och HÖK fattas av åklagare är det naturligt att kunskapsnivån är högre bland åklagare jämfört med övriga grupper. Även om ett beslut om hemliga tvångsmedel fattas av åklagaren behöver dock polisiära förundersökningsledare och it-undersökare känna till vilken slags information de har rätt att ta del av. Resultatet visar att mindre än hälften av de polisiära förundersökningsledarna och var fjärde it-undersökare uppger att de hade goda eller mycket goda kunskaper om vilka rättsliga möjligheter som finns att säkra bevisning genom att använda HAK eller HÖK.

Kunskapen lägst när bevisningen finns på internet

I Brås enkät ställdes flera frågor om respondenternas kunskaper när det gäller möjligheterna att ta del av elektroniska meddelanden som finns lagrade på en internetserver. Respondenterna fick bland annat värdera sin kunskap om *vilka rättsliga möjligheter det finns att ta del av elektroniska meddelanden som ligger lagrade utanför en mobiltelefons/dators lagringsminne (på t.ex. ett e-postkonto, Facebook eller annan plats på internet)*. Av resultatet framgår att endast var tredje åklagare och var fjärde polisiär förundersökningsledare uppger att deras kunskaper är goda eller mycket goda i detta avseende. När det gäller bevismaterial som finns på internet är kunskapsnivån högst bland it-undersökarna, där 63 procent uppger sig ha goda eller mycket goda kunskaper (tabell 5).

När det gäller bevisning som ligger på internet är kunskapen särskilt låg när det gäller tillvägagångssättet för att begära *en frysning (s.k. preservation request) för att förhindra att digital information från t.ex. ett användarkonto försvinner i väntan på rättslig hjälp*. Endast 4 procent av de polisiära förundersökningsledarna och 14 procent av åklagarna anser att deras kunskaper om frysning är goda eller mycket goda. Bland it-undersökarna uppger 41 procent att de har goda kunskaper i detta avseende (tabell 5).

Tabell 5. Kunskapen om att säkra bevisning på internet. Andel i vardera respondentgrupp som uppger att deras kunskapsnivå är god/mycket god respektive bristfällig/mycket bristfällig. Procent.

	Goda/mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Rättsliga möjligheter att ta del av elektroniska meddelanden som ligger utanför en mobiltelefons/dators lagringsminne (t.ex. på ett e-postkonto, Facebook eller annan plats på internet)		
Åklagare (n = 381)	33	67
Polisiära fu-ledare (n = 651)	24	76
It-undersökare (n = 128)	63	37
Kunskaper om tillvägagångssättet att begära en ”frysning” av uppgifter för att förhindra att digital information försvinner		
Åklagare (n = 373)	14	86
Polisiära fu-ledare (n = 635)	4	96
It-undersökare (n = 124)	41	59
Kunskaper om vilka rättsliga möjligheter det finns att säkra information som ligger öppen på internet		
Åklagare (n = 380)	31	70
Polisiära fu-ledare (n = 652)	17	83
It-undersökare (n = 128)	52	48

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

I Brås enkät tillfrågades respondenterna slutligen även om sina kunskaper om *vilka rättsliga möjligheter som finns för att säkra information som ligger öppen på internet*. Som framgår av tabell 5 visar resultatet att endast 17 procent av de polisiära förundersökningsledarna och 31 procent av åklagarna uppger sig ha goda kunskaper på området. Bland it-undersökarna bedömer hälften sina kunskaper som goda eller mycket goda.

Det går sammanfattningsvis att konstatera att kunskapsluckorna är störst när det gäller möjligheterna att säkra bevismaterial som ligger på internet. Det är också avseende dessa typer av utredningsåtgärder som flest respondenter (inom samtliga tre yrkesgrupper) anser att de, utifrån sina arbetsuppgifter, har ett stort behov av kompetensutveckling (tabell 3B i bilaga 1). Brås intervjupersoner förklarar vad som gör sådan bevisning särskilt

svår att hantera. En förklaring är att sådan bevisning ofta kräver kontakt med externa aktörer utomlands och att bevismaterialet ibland inte går att få ut då det anmälda brottet inte utgör en brottslig gärning i det land där servern ligger. En annan viktig förklaring är det komplexa regelverket på området, vilket gör att bevis på internet för många upplevs som ”minerad mark”. Brås intervjupersoner anser dock att kunskaperna om möjligheterna att säkra digitala bevis bör höjas inom de brottsutredande myndigheterna. Bland annat bör kunskapen om ”frysning” höjas, i synnerhet bland de poliser som arbetar med utredningar i deras initialskede.

Kunskapsluckor även bland dem som ofta hanterar it-relaterade ärenden

I resultatet från Brås enkätundersökning går det att konstatera att både åklagarnas och de polisiära förundersökningsledarnas kunskaper om utredningsåtgärder i digital miljö ofta ökar ju högre andel av deras ärenden som innehåller it-inslag. Samtidigt bör det poängteras att det finns kunskapsluckor även bland dem som i allra högst utsträckning hanterar sådana ärenden. Totalt 20 procent av åklagarna uppger i enkäten att merparten av deras ärenden (mellan 80 och 100 procent) innehåller it-inslag. Dessa åklagare arbetar ofta med grov brottslighet eller brott mot barn. Trots att it-inslag frekvent förekommer i arbetet saknar 40 procent av dessa åklagare vidareutbildning på it-området, och många saknar kunskaper om möjligheten att genomföra utredningsåtgärder i digital miljö.[50] Bland de polisiära förundersökningsledarna uppger 15 procent att merparten av deras ärenden (mellan 80 och 100 procent) innehåller it-inslag. Dessa förundersökningsledare arbetar ofta med grov brottslighet. Trots den höga förekomsten av it-inslag i ärendena saknar drygt 80 procent av dessa förundersökningsledare utbildning på it-området, samtidigt som kunskaperna om utredningsåtgärder i digital miljö generellt sett är låga.[51]

[50] Exempelvis uppger endast 29 procent att de har goda kunskaper om frysning, 37 procent har goda kunskaper om de rättsliga möjligheterna att ta del av information som ligger öppen på internet, 42 procent uppger att de har goda kunskaper om möjligheten att få ut information från externa aktörer utomlands, och 58 procent har goda kunskaper om möjligheten att spåra potentiella gärningspersoner via IP-adress.

[51] Bland annat uppger endast 14 procent av de polisiära förundersökningsledare som oftast hanterar ärenden med it-inslag att de har goda kunskaper om frysning, 25 procent har goda kunskaper om möjligheten att få ut information från externa aktörer utomlands, 36 procent har goda kunskaper om de rättsliga möjligheterna att ta del av information som ligger öppen på internet, och 45 procent har goda kunskaper om möjligheten att spåra anonyma gärningspersoner via IP-adress.

It-undersökarnas tekniska kunskaper

Medan åklagare och polisiära förundersökningsledare behöver ha kunskaper om vilka tekniska *möjligheter* det finns att säkra digitala bevis behöver it-undersökarna ha de tekniska *färdigheterna* för att genomföra undersökningarna. It-undersökarna utgör spetskompetensen inom de brottsutredande myndigheterna när det gäller ärenden som har it-inslag. Arbetsuppgifterna består huvudsakligen av att säkra bevisning från datorer, mobiltelefoner eller andra lagringsmedier. En it-undersökare kan även närvara vid förhör i ärenden som har it-inslag eller biträda vid husrannsakan. För att utföra sitt arbete tar it-undersökarna hjälp av olika programvaror och analysverktyg.

I Brås enkät tillfrågades it-undersökarna om sina kunskaper när det gäller hantering av mobila enheter, elektronik och bild/film/ljud. De tillfrågades även om sina kunskaper om att hantera olika tekniska svårigheter som lösenord/kryptering och ”live forensics”[52] samt om sina kunskaper om olika analysverktyg. De tillfrågades slutligen även om sina kunskaper i polisoperativt arbete (att biträda vid förhör och vid husrannsakan). Liksom i föregående avsnitt har respondenterna fått bedöma sina kunskaper som mycket goda, goda, bristfälliga eller mycket bristfälliga.

Resultatet visar att it-undersökarnas kunskaper generellt sett är goda inom många teknikområden. Kunskaperna är generellt sett högre bland de it-undersökare som går under benämningen it-forensiker, jämfört med dem som går under andra benämningar. Högst är kunskaperna om mobila enheter (t.ex. mobiltelefoner, läsplattor och GPS), där 87 procent av it-forensikerna respektive 75 procent av de övriga it-undersökarna har goda eller mycket goda kunskaper. Drygt 90 procent av it-forensikerna har goda kunskaper om it-forensiska analysverktyg, något som endast 30 procent av övriga it-undersökare uppger sig ha goda kunskaper om (bilaga 4B i bilaga 1).

Tekniska kunskapsluckor bland it-undersökare

Det är svårt att värdera kunskapsnivåerna utan att beakta vilken typ av arbetsuppgifter it-undersökaren har. Hur många roller en och samma person har varierar över landet, liksom vilken grad av renodling av arbetsuppgifter it-undersökaren har. I mindre regioner har en och samma person oftast fler undersökningsområden, medan man i större regioner har större volymer av ärenden och därmed även en renodling av rollen som it-undersökare. I enkäten tillfrågades it-undersökarna om sitt huvudsakliga arbetsområde. Majoriteten uppger att de i sitt dagliga arbete

[52] ”Live forensics” innebär att den it-forensiska undersökningen sker på plats, i system som är igång.

hanterar mobila enheter (82 procent) och data (77 procent). Vanligt förekommande är även film, bild och ljud (66 procent) och internetinhämtning (40 procent). Vidare uppger 20 procent av it-undersökarna att de arbetar med elektronik[53] och 16 procent med ”annat”.[54] Bland dem som uppger ”annat” är det vanligast att de arbetar med granskning av barnpornografi.

I tabell 6 redovisas de tekniska kunskaperna hos it-undersökarna utifrån det arbetsområde it-undersökaren arbetar inom och de tekniska utredningsåtgärder eller analysverktyg som är relevanta inom respektive område.[55] Även om kunskaperna är goda för flera av de tekniska områden som enkäten frågar om visar resultatet att det finns flera kunskapsluckor även inom gruppen it-undersökare. Som framgår av tabell 6 uppger exempelvis hälften av it-undersökarna som har *data* eller *mobila enheter* som arbetsområde att de har bristfälliga kunskaper om lösenord och kryptering. Över hälften (53 procent) av de it-undersökare som arbetar med *internetinhämtning* uppger att de har bristfälliga kunskaper om de analysverktyg som används vid just internetinhämtning.[56] Närmare 40 procent av de respondenter som arbetar med *elektronik* uppger att de har bristfälliga tekniska kunskaper om elektronik. Resultatet visar vidare att nästan var fjärde it-undersökare (24 procent) som arbetar med *bild, film och ljud* uppger att deras tekniska kunskaper om bild, film och ljud brister.

Bristande tekniska kunskaper hos it-undersökare har enligt Brås intervjupersoner flera olika förklaringar. För det första finns i dagsläget inga utbildningskrav för it-undersökare. Personer som har ett särskilt intresse eller fallenhet inom ett visst område kan få en tjänst som it-undersökare inom det området, utan att personen per automatik ges någon särskild utbildning. En annan förklaring till kunskapsluckorna hos it-undersökarna är bristen på löpande fortbildning. Flera it-undersökare berättar att de inte har fått gå en enda fortbildning sedan de gick ut sin grundutbildning,

---

[53] Med elektronikundersökningar avses t.ex. undersökning av skimmers (för stöld av kontokortsinformation), störsändare, bombutlösare, olika typer av övervakningsutrustning, bilelektronik, larm, m.m.

[54] Eftersom respondenterna tilläts uppge flera svarsalternativ överstiger procentsumman hundra procent.

[55] Bedömningen av vilka tekniska kunskaper som är relevanta för it-undersökare inom olika arbetsområden har gjorts i samråd med NFC och Noa. Det bör betonas att it-undersökare som arbetar inom de olika områdena kan behöva fler kompetenser än de som efterfrågades i Brås enkät, det vill säga de som redovisas i tabellen. Enligt Noas beskrivning behöver till exempel en it-undersökare som arbetar med internetinhämtning även behärska öppen och dold internetinhämtning i underrättelse- och utredningsverksamhet, bevissäkring, analys av nätverkstrafik, analys av betalningsströmmar avseende virtuella valutor m.m.

[56] Enligt Brås intervjupersoner kan det förklaras av att området inte är reglerat och att personer ute i verksamheten kan utses till att vara ”internetinhämtare” utan att varken ha rätt kunskap eller kännedom om de verktyg som ska användas i arbetet.

Tabell 6. It-undersökarnas tekniska kunskaper utifrån vilket arbetsområde de arbetar inom. Andel som uppger att deras kunskapsnivå är god/mycket god respektive bristfällig/mycket bristfällig. Procent.

	Goda/mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Arbetsområde: Data		
Lösenord/kryptering (n = 101)	54	47
Programmering/ programmeringsspråk (n = 101)[56]	28	72
It-forensiska analysverktyg (n = 102)	84	16
Biträda vid förhör (n = 101)	59	41
Biträda vid husrannsakan (n = 102)	83	17
”Live forensics” (n = 98)	60	40
Arbetsområde: Mobila enheter		
Mobila enheter (t.ex. mobiltelefon, läsplatta, GPS) (n = 108)	91	9
Lösenord/kryptering (n = 107)	50	51
It-forensiska analysverktyg (n = 108)	75	25
Biträda vid förhör (n = 106)	53	47
Biträda vid husrannsakan (n = 107)	79	21
”Live forensics” (n = 100)	56	44
Arbetsområde: Bild/film/ljud		
Bild/film/ljud (n = 86)	76	24
It-forensiska analysverktyg (n = 87)	66	35
Biträda vid förhör (n = 87)	53	47
Biträda vid husrannsakan (n = 87)	78	22
Arbetsområde: Elektronik		
Elektronik (n = 26)	62	39
It-forensiska analysverktyg (n = 26)	85	15
Biträda vid förhör (n = 26)	50	50
Biträda vid husrannsakan (n = 26)	73	27
Arbetsområde: Internetinhämtning		
Analysverktyg för internetinhämtning (n = 53)	47	53
Biträda vid förhör (n = 53)	59	42
Biträda vid husrannsakan (n = 53)	75	25

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

vilket oftast var för många år sedan. Detta trots att tekniken på området snabbt går framåt. En it-undersökare uttrycker:

All it-kunskap är färskvara. Den går ut efter ett tag, du kan vara superduktig på Windows XP, men förr eller senare kom-

[57] Det bör noteras att kunskaper om programmering kan behövas för mer avancerade undersökningar inom alla områdena, dock inte för normala undersökningar med köpta analysverktyg. NFC betonar att kunskapen om programmering/ programmeringsspråk heller inte måste finnas hos samtliga it-undersökare som arbetar med data.

mer det vara totalt obsolet. Det måste man börja inse. Alla it-relaterade företag inom det civila exempelvis, de skickar ju folk på utbildningar hela tiden därför att de anställda måste vara i fas med marknaden. Du kan inte jobba med en produkt som du inte känner till, det går ju inte. Det måste man börja inse lite här också, det händer ju grejer hela tiden.

Flera it-undersökare menar att de i dagsläget tvingas kompetensutveckla sig själva på sin fritid, vilket ofta kan vara svårt, då den information som behövs, till exempel om hur man tar sig in i låsta datorer, inte finns tillgänglig på internet. Några it-undersökare berättar att de arbetar i program som de inte har fått någon utbildning i, och eftersom kunskaperna om programmen ofta brister är det svårt att lösa eventuella problem som uppstår och det finns en risk att man ”missar hälften”. De bristande kunskaperna kring en del program skapar också osäkerhet när det ska skrivas protokoll och man ska framträda i rätten. På grund av att it-undersökarna inte alltid är certifierade för de programvaror som har använts i det it-forensiska arbetet kan bristen på utbildning leda till att it-undersökarens kunskaper ifrågasätts av den tilltalades försvarare under rättegången.

En tredje tänkbar förklaring till bristande kunskaper hos it-undersökare kan vara det faktum att många it-undersökare har flera arbetsområden, vilket gör att de inte kan upprätthålla expertkompetens inom något av områdena.[58] It-undersökare som Brå har intervjuat berättar att det både finns för- och nackdelar med att arbeta med flera arbetsområden. Fördelen är att arbetet blir mer givande för den enskilde it-undersökaren, men en nackdel kan vara att det inte går att fördjupa sina kunskaper inom något av områdena.

Kunskapsnivån låg hos poliser i yttre tjänst och hos utredare

Kunskapsinventeringen har tidigare endast berört de tre grupper som omfattas av Brås enkätutskick: åklagare, polisiära förundersökningsledare samt it-undersökare. Dock är det viktigt att grundläggande it-kunskaper finns inom samtliga nivåer och yrkesgrupper inom de brottsutredande myndigheterna. I Brås enkät fick åklagarna och de polisiära förundersökningsledarna bedöma hur den generella kompetensen för brott med it-inslag ser ut hos *polisens utredare* och *förste man på plats*.[59] Med förste man på

[58] Att många it-undersökare har många arbetsområden bekräftas av Brås enkät, där det framgår att 19 procent av it-undersökarna uppger att de endast har ett arbetsområde, 47 procent uppger att de har 2–3 arbetsområden, och 34 procent har 4 arbetsområden eller fler.

[59] Att frågorna inte ställdes till it-undersökarna berodde på att de inte förväntas ha lika stora kunskaper om hur kompetensen ser ut bland poliser i yttre tjänst och utredningspersonal.

plats avses de poliser som arbetar inom den yttre verksamheten (t.ex. inom ordningspolisen eller ingripandeverksamheten) och som oftast är först på en brottsplats.

Förste man på plats viktig roll för säkring av bevis

En viktig uppgift för poliser som är först på en brottsplats är att genomföra initiala utredningsåtgärder på platsen. Enligt uppdragsbeskrivningen för denna roll anges att *förste man på plats ska kunna identifiera och göra inledande säkring av digitala spår. Det innebär att förste man på plats ska veta vad som kan innehålla digitala spår, var dessa föremål kan förväntas finnas samt vad för övrig information som kan vara relevanta att säkra (FOR 2011)*.[60] Brås intervjupersoner bekräftar att poliser som arbetar i yttre tjänst har en viktig roll i utredningar av it-relaterade brott. Förutom att vidta inledande utredningsåtgärder på brottsplatsen förekommer det också att poliser i yttre tjänst formulerar beställningar till it-undersökare, vilket kräver god beställarkompetens.

I Brås enkät tillfrågades åklagarna och de polisiära förundersökningsledarna om hur de bedömer att *kunskaperna om brott med it-inslag generellt sett ser ut hos förste man på plats*. Resultatet visar att såväl åklagare som polisiära förundersökningsledare upplever att kunskaperna om brott med it-inslag är bristfälliga. Endast 11 procent av de polisiära förundersökningsledarna och 17 procent av åklagarna upplever att kunskaperna hos förste man på plats är goda eller mycket goda (tabell 7).

Bilden som framkommer i Brås enkät bekräftas av både myndighetsrapporter (t.ex. Genomförandekommittén för nya Polismyndigheten 2014b) och av de intervjupersoner som Brå har varit i kontakt med. I enkätens fritextsvar uttrycks bland annat följande:

> *Det är ytterst sällan man ser att någon har tänkt tanken att det kan finnas bevisning i it-miljö. Oftast handlar det om att säkra sms i en mobiltelefon, men utöver det ser jag nästan aldrig att man tänkt tanken. /Polisiär förundersökningsledare*

> *Många poliser i ingripandeverksamheten har mycket dåliga kunskaper om hur man säkrar bevisning. Har exempel där de stängt av datorer[61] som står på etc. /Åklagare*

[60] *Förste man på plats* ska ha förmågan att kunna samla uppgifter om ett it-relaterat brott, kunna identifiera och ta it-utrustning i beslag, använda internet för informationssökning m.m. För att klara av sin uppgift behöver de bland annat kunna identifiera bärare av digitala bevis, känna till grundläggande it-begrepp och ha kännedom om relevant lagstiftning och praxis (t.ex. när det gäller inhämtning på internet) (Polishögskolan 2014b, s. 33).

Tabell 7. Generella kunskaper om brott med it-inslag hos förste man på plats och polisens utredare enligt åklagare och polisiära förundersökningsledare. Andelen som uppger att kunskaperna hos de två grupperna är goda/mycket goda respektive bristfälliga/mycket bristfälliga. Procent.[62]

	Goda/mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Generellt sett, hur bedömer du att kunskaperna är hos förste man på plats gällande brott med it-inslag?		
Åklagare (n=305)	17	83
Polisiära fu-ledare (n=606)	11	89
Generellt sett, hur bedömer du att kunskaperna är hos polisens utredare gällande brott med it-inslag?		
Åklagare (n=353)	27	73
Polisiära fu-ledare (n=603)	15	85

Flera åklagare och polisiära förundersökningsledare anser att det finns en tydlig förbättringspotential när det gäller kunskapen om att säkra digitala bevis bland poliser i den yttre verksamheten. Samtidigt är det flera som betonar att kunskaperna är både person- och åldersberoende. De yngre har en större datorvana och har ofta bättre kunskaper om att säkra digitala bevis.

Polisens utredare har viktig roll i utredningarna

Polisens utredare har generellt sett en mycket viktig roll i utredningar av brott. Oavsett om det är en åklagarledd eller polisledd förundersökning är det utredarens roll att genomföra de utredningsåtgärder som förundersökningsledaren ger i sina direktiv. Flera av Brås intervjupersoner betonar vikten av att utredarna har en hög kompetens när det gäller förmågan att hantera digitala spår.[63] I utredningar med it-inslag kan utredaren till exempel ha som uppgift att tömma mobiltelefoner, ta kontakt med externa aktörer utomlands, begära s.k. ”frysningar”, formulera beställningar till it-undersökare rörande undersökning

[61] Eftersom användningen av kryptering blir allt vanligare är det till exempel ofta mycket olägligt att stänga av ett system som sedan inte går att starta utan tillgång till användarens lösenord och nycklar. En polis som saknar kunskap om detta riskerar att vid husrannsakan stänga av igångsatta system, vilket i sin tur kan leda till att det blir svårare att sedan komma åt bevismaterialet (Kronqvist 2013).

[62] Notera att båda frågorna har ett relativt stort bortfall: 21 respektive 9 procent för åklagarna och 10 procent för båda frågorna bland de polisiära förundersökningsledarna. De flesta av dessa respondenter har uppgett svarsalternativet ”vet ej”.

[63] Rollen som *utredare* innebär ett ännu större behov när det gäller kunskaper och färdigheter jämfört med förste man på plats. Utöver den kunskapsnivå som förste man på plats bör ha, bör utredaren dessutom kunna förstå de resultat som erhålls från it-undersökare, kunna skriva beställningar till inhemska och utländska tjänsteleverantörer och kunna företa enklare analyser i de vanligaste analysverktygen (Polishögskolan 2014b, s. 34).

av beslagtaget material m.m. Flera personer som arbetar inom den it-forensiska verksamheten berättar också att utredaren har fått en allt viktigare roll i att analysera det material som säkrats av it-undersökare, eftersom it-undersökarna på grund av hård arbetsbelastning sällan hinner med det momentet.

I Brås enkät tillfrågades åklagarna och de polisiära förundersökningsledarna om *hur de bedömer att kunskaperna om brott med it-inslag generellt sett ser ut hos polisens utredare*. Resultatet visar att majoriteten av åklagarna och de polisiära förundersökningsledarna upplever att kompetensen hos polisens utredare är låg när det gäller brott med it-inslag. Endast 27 procent av åklagarna och 15 procent av de polisiära förundersökningsledarna uppger i enkäten att utredarnas kunskaper är goda eller mycket goda (tabell 7).[64]

Eftersom enkäten varken har besvarats av poliser i yttre tjänst eller polisens utredare bör resultatet om deras kunskapsnivå tolkas med försiktighet. Enligt den enkät som Riksrevisionen har skickat till samtliga polisregioner uppger dock företrädare för samtliga regioner att de flesta utredare, som inte är särskilda it-brottsutredare, saknar utbildning inom it-området, alternativt att vissa har gått enstaka kurser eller är självlärda. Det finns heller inga krav på att utredare ska ha genomgått särskild utbildning inom it-området för att utreda it-relaterad brottslighet (Riksrevisionen 2015).

Beställarkompetens central för en effektiv it-forensisk verksamhet

Den låga utbildnings- och kunskapsnivån bland åklagare och polisiära förundersökningsledare riskerar att påverka deras kunskap om att göra beställningar till it-undersökare. Vid en it-forensisk beställning finns en *beställare* och en *utförare*. Beställaren kan vara en åklagare, en polisiär förundersökningsledare eller en utredare. I en del regioner görs beställningen ofta av poliser i yttre tjänst, till exempel av poliser inom ordningspolisen eller ingripandeverksamheten. Utföraren kan vara en lokal it-tekniker, en analytiker, en it-forensiker eller liknande (en it-undersökare). I beställningen anges vad som ska undersökas, till exempel att i en beslagtagen dator leta efter material som styrker en brottslig gärning. Efter att arbetet är utfört skickas resultatet tillbaka till beställaren.

[64] Även bland utredarna framhålls att kunskaperna till stor del är personberoende och till viss del även åldersberoende. Flera skriver att kunskapen är mycket hög hos de utredare som är särskilt utsedda till att handlägga den här typen av brott, men är lägre hos de ”vanliga” handläggarna.

Enligt Brås intervjupersoner kan en god ”beställarkompetens” kännetecknas av att beställaren har kunskap om vilka utredningsåtgärder som är möjliga att göra i ärenden med it-inslag, förmåga att formulera tydliga och avgränsade beställningar samt tillräcklig kunskap för att förstå resultatet av beställningarna. Majoriteten av Brås intervjupersoner framhåller att en god beställarkompetens är en av de viktigaste faktorerna för att den it-forensiska verksamheten ska fungera på ett effektivt sätt.

Ett sätt att mäta beställarkompetensen är att låta beställarna själva bedöma sina kunskaper om att beställa it-undersökningar. I Brås enkät till åklagare och polisiära förundersökningsledare ställdes därför tre frågor om deras kunskap om att beställa it-undersökningar. Respondenterna fick ta ställning till hur de bedömer sina kunskaper i att

1. På egen hand bedöma vilka utredningsåtgärder som är möjliga att göra i en utredning med it-inslag (t.ex. vilka möjligheter som finns att komma åt raderad information)
2. I dialog med it-undersökare göra bedömningar kring vilka it-relaterade utredningsåtgärder som bör genomföras
3. Förstå resultaten från en it-undersökning

Relativt få åklagare (38 procent) och polisiära förundersökningsledare (29 procent) uppger att de har goda eller mycket goda kunskaper i att på egen hand bedöma vilka utredningsåtgärder som är möjliga att göra i en utredning med it-inslag. Om beställningen däremot sker i samråd med en it-undersökare uppger dock de flesta åklagare (73 procent) och drygt hälften (55 procent) av de polisiära förundersökningsledarna att deras kunskaper är goda eller mycket goda (tabell 8).

Även när det gäller att förstå resultaten från en it-undersökning bedömer många åklagare (drygt 7 av 10) att deras kunskaper är goda eller mycket goda. Bland de polisiära förundersökningsledarna är det endast 39 procent som uppger detsamma (tabell 8).

Det är noterbart att it-undersökarna skattar beställarkompetensen hos åklagare och polisiära förundersökningsledare som betydligt lägre än vad de aktuella grupperna själva gör. I enkäten till it-undersökarna tillfrågades de om *hur den generella beställarkompetensen ser ut hos åklagare, polisiära förundersökningsledare samt hos polisens utredare*. Endast 17 procent av it-undersökarna anser att beställarkompetensen hos åklagare är god eller mycket god. Motsvarande siffror för de polisiära förundersökningsledarna är 11 procent och för polisens utredare 15 procent (tabell 9).

Tabell 8. Åklagarnas och de polisiära förundersökningsledarnas uppfattning om sin egen beställarkompetens. Andelen som uppger att deras kunskaper är goda/mycket goda respektive bristfälliga/mycket bristfälliga. Procent.

	Goda/mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Att på egen hand bedöma vilka utredningsåtgärder som är möjliga att göra i en utredning med it-inslag (t.ex. vilka möjligheter som finns att komma åt raderad information)		
Åklagare (n = 386)	38	62
Polisiära fu-ledare (n = 659)	29	72
Att i dialog med it-undersökare göra bedömningar kring vilka it-relaterade utredningsåtgärder som bör genomföras		
Åklagare (n = 381)	73	27
Polisiära fu-ledare (n = 646)	55	45
Att förstå resultaten från en it-undersökning		
Åklagare (n = 380)	73	27
Polisiära fu-ledare (n = 627)	39	61

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

Tabell 9. It-undersökarnas uppfattning om hur beställarkompetensen ser ut bland åklagare, polisiära förundersökningsledare och polisens utredare. Andelen som uppger att kunskaperna inom respektive yrkesgrupp är goda/mycket goda respektive bristfälliga/mycket bristfälliga. Procent.

	Goda/mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Generellt sett, hur bedömer du att beställarkompetensen är hos nedanstående grupper avseende it-undersökningar?		
Åklagare (n = 126)	17	83
Polisiära fu-ledare (n = 128)	11	89
Polisens utredare (n = 131)	15	86

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

Enligt it-undersökare som Brå har intervjuat måste åklagarnas, de polisiära förundersökningsledarnas och utredarnas kompetens om it-relaterade brott öka för att de ska kunna ge relevanta direktiv om vad som ska undersökas i beställningarna. I dag är flera beställningar alldeles för vaga och omfattande, till exempel att de är formulerade som ”töm datorn”, ”styrk brott” eller ”gör som ni brukar göra”, vilket till stor del kan förklaras av låg beställarkompetens. En beställning om att tömma en dator kan, enligt it-undersökare, liknas vid att tömma ett helt bibliotek i jakt efter några enstaka rader i en viss bok.

De otydliga och omfattande beställningarna till it-undersökarna har en negativ inverkan på rättsväsendets effektivitet, då det lätt bildas en flaskhals inom den it-forensiska verksamheten, vilket resulterar i långa genomströmningstider för ärenden som innehål-

ler digitala bevis. I det kommande kapitlet redogörs närmare för hur rättsväsendets kapacitet ser ut när det gäller förmågan att hantera it-relaterad brottslighet.

Resultaten i korthet

Sammanfattningsvis visar resultaten från Brås analys av rättsväsendets kompetens gällande it-relaterad brottslighet att:

- Utbildningsnivån på it-området är låg hos både åklagare och polisiära förundersökningsledare. Drygt hälften av åklagarna och nio av tio polisiära förundersökningsledare saknar vidareutbildning på it-området.
- Majoriteten av it-undersökarna har en gedigen it-forensisk utbildning, men 12 procent saknar helt utbildning på it-området.
- Kunskaperna om att spåra potentiella gärningspersoner via internet är generellt sett låga. Exempelvis har endast 48 procent av åklagarna och 22 procent av de polisiära förundersökningsledarna goda kunskaper om möjligheten att spåra gärningspersoner via IP-adress.
- Kunskapsnivån är lägst när det gäller möjligheten att säkra bevismaterial som ligger på internet. Sådan bevisning kräver ofta kontakt med externa aktörer utomlands, och regelverket på området upplevs vara komplicerat.
- De tekniska kunskaperna bland it-undersökarna är ofta goda, men det finns områden där kompetensen bör höjas. Några förklaringar till de brister som har identifierats är att det saknas utbildningskrav för it-undersökare, det råder brist på fortbildningsinsatser och att många it-undersökare är ”generalister” och inte har möjlighet att fördjupa sina kunskaper inom ett särskilt arbetsområde.
- Både åklagare och polisära förundersökningsledare anser att poliser i yttre tjänst och utredare har en bristfällig kompetens gällande brott med it-inslag. Det kan till exempel ge negativa konsekvenser för bevissäkringen i utredningarnas initialskede.
- It-undersökare anser att både åklagare, polisära förundersökningsledare och utredare har bristande kunskaper om att göra beställningar till den it-forensiska verksamheten. Det kan leda till att beställningarna blir onödigt omfattande och att det bildas en flaskhals inom den it-forensiska verksamheten.

Rättsväsendets kapacitet gällande brott med it-inslag

En god kapacitet är en förutsättning för ett effektivt och rättssäkert utredningsarbete. I föregående kapitel redogörs för kompetensen inom rättsväsendet för att handlägga och utreda brott med it-inslag, vilket är en viktig del av den totala kapaciteten. I föreliggande kapitel redovisas ytterligare aspekter som är centrala för rättsväsendets kapacitet gällande brott med it-inslag, nämligen kompetenshantering och bemanning, systemstöd och teknisk utrustning, utredningsstöd samt externa samarbeten.

För att kunna bedöma kapaciteten är det viktigt att studera hur väl kompetensen matchar inflödet av ärenden, det vill säga i vilken utsträckning det finns tillräckligt med personal med rätt kompetens för att kunna hantera de olika delarna av utredningsprocessen. Att studera kapaciteten innebär även att redogöra för i vilken utsträckning de personer som är involverade i olika delar av utredningsprocessen har tillgång till de system och den tekniska utrustning som krävs för arbetsuppgiften. Ett effektivt utredningsarbete förutsätter även att det finns expertfunktioner att vända sig till vid behov, liksom ett bra metodstöd. Rättsväsendets förmåga att hantera brott med it-inslag är även i stor utsträckning beroende av ett välfungerande samarbete med externa aktörer. På samma sätt som i föregående kapitel redovisas här resultat från Brås enkätundersökning till åklagare, polisiära förundersökningsledare och it-undersökare, samt resultat från de intervjuer som Brå genomfört. I bilaga 4 redovisas huvuddragen gällande ansvarsfördelning och organisation inom Polismyndigheten respektive Åklagarmyndigheten.

Det interna bortfallet för de enkätfrågor som presenteras i föreliggande kapitel är lågt och varierar mellan 0 och 5 procent.

Kompetenshantering och bemanning

En viktig faktor för att de brottsutredande myndigheterna ska ha tillräcklig kapacitet för att utreda brott med it-inslag är att det finns tillräcklig bemanning för utredningens alla delar. I ärenden med it-inslag har it-undersökaren en central funktion. It-undersökarna är vanligen placerade på regionnivå, men i vissa regioner finns it-undersökare även ute i polisområdena.

It-undersökarna upplever hög arbetsbelastning

Brås enkätundersökning bekräftar tidigare rapporter som visar att det finns en obalans mellan antalet it-undersökare och de arbetsuppgifter och beställningar som de har att hantera. I enkätundersökningen uppger tre av fyra av it-undersökarna att hög arbetsbelastning i hög eller mycket hög utsträckning utgör ett hinder för dem i deras arbete (tabell 10). It-undersökarna beskriver i intervjuer att de skulle kunna mångdubbla personalstyrkan och ändå ha svårt att hinna med alla arbetsuppgifter. It-undersökarna uttrycker även en frustration över att rekryteringsprocessen många gånger är för långsam. Vid de tillfällen en it-undersökare slutar, tar det ofta lång tid innan en ny är på plats och upplärd.

Den höga arbetsbelastningen ger många gånger långa ledtider för it-undersökningar. De långa ledtiderna får konsekvenser för den fortsatta utredningsprocessen. I Brås enkäter tillfrågades åklagarna och de polisiära förundersökningsledarna huruvida långa ledtider gällande svar från it-undersökare utgör ett hinder för dem i deras arbete. Bland åklagarna uppger 74 procent att detta i hög eller mycket hög utsträckning utgör ett hinder för dem i deras arbete. Motsvarande siffra bland de polisiära förundersökningsledarna är 46 procent (Tabell 10).

De förundersökningsledare som Brå intervjuat betonar att ledtiderna varierar stort. Ledtiderna avgörs dels av brottets karaktär, dels av den prioriteringsordning och de förtursregler som finns, men det finns även regionala och lokala skillnader. De långa ledtiderna gör att en beställning riskerar att bli inaktuell innan den kommit fram i kön. Följden kan bli att förundersökningsledare inte begär it-undersökningar i de fall där de bedömer att det kommer att ta för lång tid att få svar. Vidare uppger åklagare att det inte finns några bra rutiner för att återkalla en beställning om den hunnit bli inaktuell. Alltså riskerar it-undersökarna att genomföra undersökningen i onödan, då ärendet redan är nedlagt eller avslutat.

Tabell 10. Andelen som anser att långa ledtider gällande svar från it-undersökare och hög arbetsbelastning utgör ett hinder i arbetet med ärenden med it-inslag. Procent.

	Låg/mkt låg utsträckning	Hög/mkt hög utsträckning	Vet ej
Hög arbetsbelastning			
It-undersökare (n = 132)	24	77	0
It-forensiker (n = 85)	*27*	*73*	*0*
Övriga it-undersökare (n = 47)	*17*	*83*	*0*
Långa ledtider gällande svar från it-undersökare			
Åklagare (n = 378)	16	74	10
Polisiära fu-ledare (n = 665)	29	46	25

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

It-undersökarna används ineffektivt

Tidigare rapporter har beskrivit hur den it-forensiska processen i stor utsträckning blir den trånga sektorn i utredningar som kräver it-undersökningar (se till exempel Genomförandekommittén för nya Polismyndigheten 2014b). I Brås studie framkommer att en förklaring till detta är att inflödet inte är tillräckligt reglerat, bland annat på grund av bristande beställarkompetens.[65] Drygt sex av tio av it-undersökarna som har besvarat Brås enkät uppger att otydliga och onödigt omfattande beställningar blir ett hinder för dem i deras arbete.

En annan förklaring är att it-undersökarna i dag används för arbetsuppgifter som inte kräver den utbildnings- och kompetensnivå som it-undersökaren vanligen besitter. Till exempel används it-undersökarna för att filma rekonstruktioner av brott och för rutinmässiga telefontömningar. It-undersökare används även som en form av it-stöd i frågor som ligger utanför det it-forensiska arbetet, till exempel med frågor om någon funktion i Excel eller vid problem med olika typer av hårdvara.

För två specifika arbetsuppgifter råder det diskussioner om huruvida uppgiften är att betrakta som en uppgift för it-forensiker. Det gäller it-forensikernas delaktighet vid fingranskning av övergreppsbilder mot barn och vid skapandet av presentationer av digitalt material inför huvudförhandlingar. Att fingranska barnpornografiskt material innebär att man går igenom bilder och filmer och bedömer huruvida materialet är att betrakta som barnpornografi. Poliser och it-forensiker som Brå varit i kontakt med menar att detta är en uppgift som inte sällan faller på it-forensikerna och att det tar många resurstimmar eftersom fingranskningen är en tidsödande uppgift. I Polismyndighetens

[65] För en beskrivning av beställarkompetens, se tidigare kapitel.

Förstudierapport för den forensiska processen (2016b) fastställs att uppgiften är icke-forensisk. It-forensikerna ska enbart lösa de tekniska frågorna, medan bedömningar av bildmaterialet ska hanteras i den övriga utredningsverksamheten, enligt rapporten. I Brås enkätundersökning uppger mer än var fjärde it-forensiker att de ofta eller mycket ofta fingranskar övergreppsbilder mot barn (tabell 11).

En annan viktig uppgift i ärenden med it-inslag är att skapa presentationer av den digitala bevisningen inför huvudförhandling. Det saknas i dag nationella riktlinjer kring vem som ansvarar för denna uppgift, och det ser därför olika ut i olika delar av landet. I vissa delar av Polismyndigheten faller uppgiften på it-forensikerna, något som företrädare för Noa och NFC menar är felaktigt. I Brås enkätundersökning framkommer att nära var femte it-forensiker mycket ofta eller ofta skapar presentationer av den digitala bevisningen inför huvudförhandling (tabell 11).

Tabell 11. Andelen som fingranskar övergreppsbilder mot barn, samt skapar presentationer av den digitala bevisningen inför huvudförhandling. Procent.

	Mycket ofta/ ofta	Ibland/Sällan/ Aldrig	Vet ej
Fingranskar övergreppsbilder mot barn			
It-forensiker (n = 84)	27	73	-
Skapar presentationer inför huvudförhandling			
It-forensiker (n = 84)	18	81	1

Förundersökningsledarna upplever svårigheter att ta it-undersökare i anspråk under förundersökningen

Det råder en stor enighet bland såväl polisiära förundersökningsledare och åklagare som bland it-undersökare att kvaliteten på utredningen blir högre om en it-undersökare är med från start till mål. Utöver själva genomförandet av it-undersökningen är det en framgångsfaktor om it-undersökaren är med vid arbetsmöten, vid planering och genomförande av husrannsakan och beslag samt vid förhör. Detta är särskilt viktigt vid större utredningar. Drygt hälften av åklagarna och var tredje polisiär förundersökningsledare menar att svårigheter med att ta en it-undersökare i anspråk under en förundersökning i hög eller mycket hög utsträckning utgör ett hinder för dem i deras arbete (tabell 12). I tabell 6B i bilaga 1 återfinns siffror över hur vanligt det är att it-undersökaren deltar i olika moment av en förundersökning.

Tabell 12. Andelen som uppger att svårigheter att ta it-undersökare i anspråk under förundersökningen utgör ett hinder i arbetet med ärenden med it-inslag. Procent.

	Låg/mkt låg utsträckning	Hög/mkt hög utsträckning	Vet ej
Åklagare (n = 368)	32	53	16
Polisiära fu-ledare (n = 653)	35	33	32

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

Bristande resurser i analysfasen

Enligt Brås intervjupersoner ökar volymen data och spår, vilket leder till en hög arbetsbelastning vid de it-forensiska funktionerna. De data som extraherats och säkrats ska i nästa steg analyseras. I förlängningen påverkar därmed stora datamängder även trycket på bemanning och kompetens i analysfasen. I såväl fritextsvaren från enkätundersökningen som i de intervjuer som Brå har genomfört framförs stora brister kopplade till analysfasen. Det handlar huvudsakligen om att det saknas utredningsresurser för att genomföra analyserna effektivt och rättssäkert.

Analysfasen hamnar i vissa fall i gränslandet mellan forensik och utredning. På grund av den höga arbetsbelastningen inom den it-forensiska verksamheten finns det sällan någon möjlighet för it-undersökaren att genomföra en analys av de data som säkrats. Typfallet är att det i stället är utredaren som ska hantera och analysera resultatet från it-undersökningen. Många av Brås intervjupersoner menar att analyskompetensen bland utredarna generellt är för låg och att risken är överhängande att de datauppgifter som hämtats ut därmed inte används till fullo. Utredarna saknar dessutom ofta analysverktyg för uppgiften, se nästa stycke.

Systemstöd och teknisk utrustning

Ytterligare en förutsättning för rättväsendets förmåga att på ett effektivt och rättssäkert sätt hantera ärenden med it-inslag är ett fungerande it-stöd. Nedan beskrivs de brister som Brå har identifierat kopplat till systemstöd och teknisk utrustning.

Brist på teknisk utrustning och system stort hinder

För att kunna genomföra relevanta undersökningar krävs tillgång till olika typer av teknisk utrustning, programvara och förbrukningsmaterial. Drygt var fjärde åklagare och nära hälften av de polisiära förundersökningsledarna uppger att en bristande tillgång på detta i hög eller mycket hög utsträckning utgör ett hinder för dem i deras arbete. Motsvarande siffror för grupperna

it-forensiker och övriga it-undersökare är 39 respektive 51 procent (tabell 13).

Tabell 13. Andelen som uppger att bristande tillgång till teknisk utrustning, programvara och/eller förbrukningsmaterial utgör ett hinder i arbetet med ärenden med it-inslag. Procent.

	Låg/mkt låg utsträckning	Hög/mkt hög utsträckning	Vet ej
Åklagare (n = 384)	51	28	20
Polisiära fu-ledare (n = 666)	33	48	19
It-undersökare (n = 132)	56	43	1
It-forensiker (n = 85)	*61*	*39*	*0*
Övriga it-undersökare (n = 47)	*47*	*51*	*2*

Not: På grund av avrundningar understiger vissa procentsummor 100 procent.

En del av bristerna härleds till de begränsningar som polisens teknikplattform Polar[66] innebär. Det handlar till exempel om att plattformen inte stöder alla filformat, att all surf via en Polardator innebär att IP-adressen går att härleda till Polismyndigheten vilket blir problematiskt vid internetinhämtning samt att Polar-lösningen saknar för ändamålet adekvata verktyg i form av lämpliga programvaror som gör det möjligt att exempelvis kunna ta del av övervakningsfilmer. För att ligga i framkant inom it-forensik krävs en ständig uppdatering av utrustning och programvara. Det blir till exempel allt vanligare med olika typer av krypteringslösningar. För att kunna få ut krypterad information krävs avancerad utrustning. Samtidigt förändras ständigt tekniken vilket innebär att den kryptering som används i dag, i morgon kommer att ersättas av någon annan, vilket ställer krav på kontinuerlig uppdatering.

Såväl förundersökningsledare som it-undersökare efterfrågar även ett användarvänligt verktyg för analys som är anpassat för utredare och förundersökningsledare. Detta för att göra överlämningen mellan it-undersökarens arbete och fortsatt utredning bättre. Ytterligare behov av it-system som nämns bland Brås intervjupersoner är ett gemensamt ärendehanteringssystem. Frågan om ett gemensamt ärendehanteringssystem hanteras i nästkommande kapitel.

Skillnader i prioriteringar och utrustningsnivå

Vissa regionala skillnader framgår av enkätsvaren, där det är vanligare att polisiära förundersökningsledare från de mindre re-

[66] Under 2014 införde polisen en ny teknisk plattform för en pc-arbetsplats, Polar. Polar möjliggör för polisen att arbeta mobilt och att vara uppkopplade mot polisens system och internet samtidigt.

gionerna uppger att de har brist på teknisk utrustning och att det utgör ett hinder för dem. De regionala eller lokala skillnaderna bekräftas även av intervjumaterialet. Intervjupersonerna beskriver att prioriteringarna ser olika ut; i vissa delar av Polismyndigheten prioriteras utbildning, i andra utrustning.

Enligt intervjupersonerna beror skillnaderna till stor del på att det inte funnits någon styrning gällande prioriteringar. Det finns därför stora variationer på området, även inom regionerna. På de håll där det har varit svårare att få igenom önskemål uttrycks en frustration över att det saknas förståelse för varför inköpen är viktiga. Intervjupersonerna upplever att de ständigt måste motivera att inköpen är avgörande för att komma framåt i en utredning. Företrädare för NFC menar att utrustningen många gånger är mycket kostsam. Om utrustningsnivån är låg så blir det därför dyrt att höja den.

Expertfunktioner och utredningsstöd

Ärenden med it-inslag kan många gånger vara både tekniskt och juridiskt komplicerade. Utvecklingen på it-området innebär dessutom ständiga förändringar avseende möjliga utredningsåtgärder. Ny kunskap genereras kontinuerligt inom rättsväsendet, dels genom strukturerat metod- och utvecklingsarbete, dels genom att nya utredningsåtgärder prövas inom utredningsverksamheten.

För den enskilde medarbetaren kan det vara svårt att själv söka information gällande till exempel nya möjligheter till digital bevisning, nya samarbeten med externa aktörer och lagstiftning. Förundersökningsledare och it-undersökare är därmed i stort behov av stöd i utredningarna. Nedan beskrivs de expertfunktioner som finns inom Polismyndigheten respektive Åklagarmyndigheten, samt hur kunskap sammanställs och kommuniceras i dag.

Polismyndigheten – Noa och NFC

Den Nationella operativa avdelningen (Noa) biträder regionerna med expertkompetens när kunskap eller utrustning saknas, till exempel med bild- och filmarbeten, husrannsakan i komplex it-miljö samt med kvalificerad internetinhämtning. Den 1 oktober 2015 inrättades Nationellt it-brottscentrum (SC3) vid Noa.[67] Vid SC3 finns en deskfunktion som hanterar olika typer av frågor relaterade till utredningar med it-inslag. SC3 är även internationell kontaktpunkt för it-relaterade brott samt så kallad Single point of contact (SPOC) mot bland annat Facebook, Google och Apple, vilket innebär att de sköter kontakten med dessa aktörer i

[67] SC3 är under uppbyggnad och beräknas vara fullt utbyggt den 31 december 2017.

samtliga ärenden där information behöver hämtas från dem. Vid SC3 finns nationell beredskap dygnet runt och mobila it-team som kan biträda i hela landet.

I Brås enkätundersökning uppger tre av tio åklagare (31 procent) och var fjärde polisiär förundersökningsledare (27 procent) att de vid ett eller flera tillfällen vänt sig till Noa för att de har behövt hjälp med någon utredningsåtgärd. Den vanligaste orsaken till att man vänder sig till Noa gäller vilka möjligheter som finns att få ut information från externa aktörer utomlands.

Nationellt forensiskt centrum (NFC) bistår regionerna med kompetens i ärenden med tekniskt svåra eller komplexa frågor. Vid NFC finns även i viss uträckning mer avancerad eller unik utrustning som inte finns ute i regionerna. För att begära en undersökning från NFC används det beställningsformulär som finns på Intrapolis. Vid NFC finns även en servicetelefon dit utredare och förundersökningsledare kan ringa för att få vägledning i olika frågor och ärenden. Bland åklagarna och de polisiära förundersökningsledarna i Brås enkätstudie uppger 9 respektive 12 procent att man vänt sig till NFC vid ett eller flera tillfällen för att man har behövt hjälp med någon utredningsåtgärd.

Låg kännedom om expertfunktionernas roller

Resultatet från Brås enkätundersökning visar att det finns en stor osäkerhet när det gäller vad olika aktörer i polisens nationella struktur kan bistå med vid ärenden med it-inslag (tabell 14). Resultatet bekräftar i stor utsträckning den bild som framkommit i tidigare studier (Rikspolisstyrelsen 2012, Riksrevisionen 2015). Generellt är kännedomen lägst (andel osäkra och nej) bland de polisiära förundersökningsledarna och åklagarna. Bland de polisiära förundersökningsledarna uppger endast var femte att de har kännedom om vad Nationella operativa avdelningen (Noa) kan bistå med, och lika stor andel uppger att de har känndedom om vad Nationellt forensiskt centrum (NFC) kan hjälpa till med. Motsvarande siffror bland åklagarna är något högre.

Företrädare för Noa menar i intervjuer med Brå att den låga kännedomen kan förklaras av tre faktorer. För det första är ansvarsområdena för Noa och NFC inte tillräckligt tydligt formulerade. För det andra har den nya organisationen inte haft möjlighet att ”sätta sig” ännu. För det tredje har det hittills saknats resurser och intern struktur för att till regionerna föra ut budskapet om vad de olika aktörerna kan bistå med.

Tabell 14. Andelen ja, nej respektive osäker gällande kunskapen kring vad de olika aktörerna i Polisens nationella struktur kan bistå med i ärenden med it-inslag. Procent.

	Ja	Nej	Osäker
Nationella operativa avdelningen (Noa)			
Åklagare (n = 380)	29	32	38
Polisiära förundersökningsledare (n = 665)	21	39	39
It-undersökare (n = 131)	54	17	28
It-forensiker (n = 84)	*56*	*17*	*27*
Övriga It-undersökare (n = 47)	*51*	*19*	*30*
Nationellt forensiskt centrum (NFC)			
Åklagare (n = 382)	38	27	35
Polisiära förundersökningsledare (n = 663)	21	34	45
It-undersökare (n = 132)	55	14	31
It-forensiker (n = 85)	*58*	*14*	*28*
Övriga It-undersökare (n = 47)	*49*	*15*	*36*

Not: På grund av avrundningar understiger vissa procentsummor 100 procent.

Åklagarmyndigheten – kontaktåklagare för it-området

År 2014 tilldelades områdeschefen vid Åklagarområde Stockholm ett nationellt samordningsansvar för it-relaterad brottslighet. Inom ramen för samordningsansvaret inrättades under senvintern 2015 ett nätverk av kontaktåklagare för it-området. Nätverket består av två åklagare från Nationella åklagaravdelningen och två åklagare från varje åklagarområde, vilket ger en total på 16 it-kontaktåklagare utspridda över hela landet. Två av dessa åklagare har utsetts som ansvariga för nätverket. Nätverket med it-kontaktåklagare har en samarbetsyta på Åklagarmyndighetens intranät Rånet där man utbyter information och erfarenheter. Tanken är att man som enskild åklagare ska kunna vända sig till sin it-kontaktåklagare med frågor gällande vilka möjligheter som finns i olika ärenden, vart man ska vända sig med vissa frågor osv. Åklagarmyndigheten (2015a) menar att it-kontaktåklagarna är en viktig del i att upprätthålla spetskompetens inom myndigheten.

Ansvariga förklarar att det handlar om att inte behöva uppfinna hjulet igen. Tanken är att åklagare ska kunna kontakta sin it-kontaktåklagare och be om hjälp. Om kontaktåklagaren inte själv har svaret kan hon eller han lägga ut frågan på den gemensamma arbetsytan för nätverket. Via arbetsytan kan tidigare stämningsansökningar, domar eller annat underlag delas. På så vis kan erfarenheter kring vad som fungerar och inte fungerar enkelt och snabbt förmedlas. It-kontaktåklagarna och arbetsytan bidrar till att myndighetens resurser går att nå oavsett placering i landet. Därigenom undviker man risken att resurserna koncentreras till storstäderna.

Hälften (50 procent) av de åklagare som besvarat Brås enkät uppger att de vid ett eller flera tillfällen har vänt sig till en kontaktåklagare för att de har behövt hjälp med olika utredningsåtgärder. Flest uppger att de vänt sig till en kontaktåklagare med frågor om att få ut information från externa aktörer utomlands (29 procent), att begära en frysning (28 procent), att säkra information som ligger öppet på internet (27 procent) eller med frågor om vilka rättsliga möjligheter det finns att ta del av elektroniska meddelanden som ligger lagrade utanför en mobiltelefons/dators lagringsminne (27 procent). Samtidigt framkommer det i intervjuer med åklagare att vissa inte känner till nätverkets existens.

Stor efterfrågan på sammanställningar och vägledning

Både åklagare och polisiära förundersökningsledare efterfrågar sammanställningar över svaren på vanligt förekommande frågeställningar, till exempel gällande vilka åtgärder som går att vidta med olika datamedier, hur man säkrar digitala bevis eller vilka chattsidor det går att få uppgifter från. Ytterligare önskemål är lathundar över lagstiftningen där det framgår vad man får och inte får göra och förutsättningar och straffsatser för hemliga tvångsmedel.

För att möta behovet av snabbare och mer kontinuerlig uppdatering har Åklagarmyndighetens Utvecklingscentrum tagit fram en webbaserad guide för it-området, kallad FAQ.[68] Guiden publicerades under hösten 2015 och är tänkt att fungera som ett metodstöd och en kunskapsbank för åklagare. Den webbaserade guiden återfinns på Åklagarmyndighetens intranät, Rånet.

Intranäten centrala för informationsspridning

Bland såväl poliser, åklagare och it-undersökare som bland andra företrädare för it-området betonas att Åklagarmyndighetens och Polismyndighetens respektive intranät är viktiga plattformar för informationsspridning. Intervjupersoner i Brås undersökning menar att intranäten bör vara den främsta platsen för att komma åt de sammanställningar och kompetensregister som efterfrågas.

Under hösten 2014 bytte Åklagarmyndigheten plattform för intranätet och i och med det lanserades bland annat funktionen med samarbetsytor och projektytor. Efter uppdateringarna har Rånet blivit mer användarvänligt och välfungerande, enligt de åklagare som Brå varit i kontakt med. Kontaktåklagarnätverket för it-området är ett exempel på hur samarbetsytor på Rånet kan

[68] FAQ är en förkortning för Frequently Asked Questions och är en etablerad benämning på en samling frekvent ställda frågor och deras svar och används på många olika fält och webbplatser.

användas. Ytterligare en satsning där intranätet används för informationsspridning inom Åklagarmyndigheten är informationskanalen Kanal Legal. Via Kanal Legal publiceras korta informationsfilmer med nyheter inom olika områden. Syftet är att öka tillgängligheten och göra det enklare att ta del av information.

På Polismyndighetens intranät Intrapolis finns idag ett chattforum kallat It-brottsforum. Efter att ha ansökt om att få behörighet får man tillträde till forumet. Forumet innehåller ett stort antal olika diskussionstrådar där man kan söka information och även ställa egna frågor relaterade till ärenden med it-inslag. Brås intervjupersoner är dock eniga om att Intrapolis i dag har stora brister. Den huvudsakliga kritiken handlar om bristen på information samt att informationen, om den finns, är svår att hitta på grund av dålig struktur och sökfunktion. En företrädare för Noa förklarar att det kan vara svårt att till och med hitta information som man själv har publicerat och ansvarar för och som man vet finns där.

I Polismyndighetens it-strategi för 2015–2017 (Polismyndigheten 2015a) beskrivs Intrapolis som myndighetens viktigaste interna kommunikationskanal för ledning och styrning. Intranätet beskrivs även som ett arbetsverktyg för alla anställda. För att uppnå en effektivare ledning och styrning samt för att främja ett enhetligt arbetssätt i den nya polisorganisationen beskriver it-strategin att det är viktigt att Intrapolis utvecklas avseende mobilitet, redaktörsfunktioner, integration med andra system samt avseende samarbetsfunktioner och samarbetsplattformar.

Externa samarbeten och lagstöd

För de brottsutredande myndigheterna finns ett antal faktorer som påverkar förmågan att utreda brott men som delvis ligger utanför myndigheternas ansvar och den egna kapaciteten. Det handlar om ärenden där rättsväsendet är beroende av välfungerande externa samarbeten samt att det finns lagstöd för de utredningsåtgärder som man önskar vidta.

Stort hinder att internetföretagen inte lämnar ut viktig information

Tidigare i rapporten beskrivs problem kopplade till polisens samarbete med privata aktörer utomlands. Omkring hälften av åklagarna och de polisiära förundersökningsledarna respektive sex av tio it-undersökare uppger att det föreligger svårigheter med att privata aktörer utomlands, såsom Microsoft, Kik och Google, inte lämnar ut viktig information och att detta utgör ett hinder för dem i deras arbete (tabell 15). Brås intervjupersoner

uppger att i de fall aktörerna lämnar ut information är hanteringen i vissa fall långsam. Den brottsutredande verksamheten är beroende av en effektiv hantering för att undvika att uppgifterna, som i nästa steg knyter IP-adressen till användarinformation, inte längre finns sparad, se nästa avsnitt.

Tabell 15. Andelen som anser att det utgör ett hinder i arbetet med ärenden med it-inslag att privata aktörer utomlands (t.ex. Microsoft, Kik och Google) inte lämnar ut viktig information. Procent.

	Låg/mkt låg utsträckning	Hög/mkt hög utsträckning	Vet ej
Åklagare (n = 384)	25	55	21
Polisiära fu (n = 668)	20	47	33
It-undersökare (n = 132)	30	60	10
It-forensiker (n = 85)	*35*	*59*	*6*
Övriga it-undersökare (n = 47)	*21*	*62*	*17*

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

Problem att få ut användarinformation från telekom- och internetoperatörer i Sverige

För att knyta inloggningsuppgifterna till en misstänkt gärningsperson behöver polisen få fram användarinformation från telekom- och internetoperatörer i Sverige. Detta förutsätter att informationen finns sparad hos operatörerna. I vilken utsträckning operatörerna är skyldiga att spara uppgifter regleras i 6 kap. 16 a § LEK.[69] Enligt LEK ska uppgifterna sparas i sex månader.

Rättsläget vad gäller datalagring har dock varit oklart under en period med anledning av EU-domstolens underkännande av det så kallade Datalagringsdirektivet. Trots att den svenska regeringen och Post- och telestyrelsen meddelat att svensk lagstiftning fortfarande gäller sparar vissa operatörer inte den lagstadgade informationen (Åklagarmyndigheten 2015a). Brås intervjupersoner menar dessutom att tidsgränsen på sex månader borde utökas med hänsyn till att det kan ta lång tid att få ut IP-adressen från privata aktörer utomlands.

Att det föreligger svårigheter med att få ut uppgifter på grund av att de inte sparas hos telekom- och internetleverantörer bekräftas av enkätstudien. Bland åklagarna och it-undersökarna uppger drygt hälften att detta i hög eller mycket hög utsträckning utgör ett hinder i deras arbete. Motsvarande siffra för de polisiära förundersökningsledarna är 39 procent (tabell 16).

[69] Lagen (2003:389) om elektronisk kommunikation.

Tabell 16. Andelen som anser att svårigheter med att få ut uppgifter på grund av att de inte sparas hos telekom- och internetleverantörer utgör ett hinder i arbetet med ärenden med it-inslag. Procent.

	Låg/mkt låg utsträckning	Hög/mkt hög utsträckning	Vet ej
Åklagare (n = 380)	29	55	16
Polisiära fu (n = 665)	27	39	35
It-undersökare (n = 131)	37	52	12
It-forensiker (n = 84)	*44*	*50*	*6*
Övriga it-undersökare (n = 47)	*23*	*55*	*21*

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

Utöver de fall där uppgifter inte finns sparade hos operatörerna finns det andra omständigheter som försvårar arbetet med att få ut användarinformation. I enkätsvaren och bland poliser som Brå intervjuat framkommer att internetleverantörer i dag i allt större utsträckning använder sig av Network Adress Translation-teknik (NAT-teknik), även kallat ”operatörsnattning”. NAT är en teknik som möjliggör att många datorer/terminaler ansluter sig till internet med användning av en eller några få gemensamma publika IP-adresser. NAT-tekniken ger därmed en lösning på problemet med det begränsade antalet IP-adresser. För rättsväsendet blir operatörsnattningen dock problematisk då operatörernas lagringsskyldighet inte omfattar de uppgifter som behövs för att knyta trafiken till specifika adresser (SOU 2015:31).

Flera delar av utredningsåtgärdena på it-området är oreglerade

Utöver de begränsningar som Datalagringsdirektivet innebär finns det problem gällande hur reglerna om husrannsakan och beslag ska tillämpas i it-miljö. Som exempel kan nämnas att det inte finns något uttryckligt lagstöd för att genomföra husrannsakan på distans, vilket innebär problem för rättsväsendet när det gäller information som finns lagrad i olika molntjänster. Det råder även en osäkerhet om hur man ska hantera virtuella valutor (Bälter Nordenman 2016). Med anledning av detta tillsattes en utredning i syfte att se över hur reglerna om beslag och husrannsakan kan moderniseras (Dir. 2016:20). En utredning har även tillsatts för att utreda möjligheterna till hemlig dataavläsning, det vill säga rätten att avlyssna internettrafik (Dir. 2016:36).

Slutligen bör nämnas det faktum att Sverige ännu inte ratificerat Europarådets konvention om it-relaterad brottslighet som Sverige undertecknade 2001. Konventionen syftar till att ländernas nationella straffrätt ska närma sig varandra och att säkerställa att det finns nationella processrättsliga bestämmelser som tillgodoser

behoven av att utreda och lagföra de brott som behandlas i konventionen och andra brott som begås med hjälp av datorer samt att kunna ta till vara bevisning i elektronisk form. Konventionen syftar även till att lägga grunden för ett snabbt och effektivt internationellt samarbete vid bekämpningen av it-relaterade brott (SOU 2013:39).

Resultaten i korthet

Sammanfattningsvis visar resultaten från Brås analys av rättsväsendets kapacitet gällande it-relaterad brottslighet att:

- It-undersökarna upplever en hög arbetsbelastning. Detta beror delvis på att inflödet av beställningar till den it-forensiska verksamheten är stort, samtidigt som beställningarna många gånger är otydliga och onödigt omfattande. Den höga arbetsbelastningen beror även på att it-undersökarna många gånger används ineffektivt på så vis att de utför arbetsuppgifter som de är överkvalificerade för.
- En förutsättning för polisens förmåga att på ett effektivt och rättssäkert sätt hantera ärenden med it-inslag är ett fungerande it-stöd. Brist på teknisk utrustning och system beskrivs som ett stort hinder bland it-undersökare, poliser och åklagare.
- För den enskilde medarbetaren är det centralt att det finns ett bra utredningsstöd att tillgå för ärenden med it-inslag. Kännedomen om expertfunktionernas roll är generellt låg. Det finns dessutom en stor efterfrågan på olika typer av sammanställningar och vägledning.
- Rättsväsendets möjligheter att utreda brott med it-inslag är delvis beroende av externa faktorer, såsom fungerande samarbete med externa aktörer och ett fullgott lagstöd.

System för statistiskt underlag

Den tredje delen i regeringens uppdrag till Brå handlar om att överväga möjligheterna att utveckla ett system som ger rättsväsendets myndigheter ett statistiskt underlag för att framöver kunna följa utvecklingen av it-inslag i de anmälda brotten, och i så fall föreslå hur systemet bör utformas.

I kapitlet redogörs först för vilket behov som finns inom rättsväsendets myndigheter när det gäller statistik som visar förekomsten av it-inslag i de anmälda brotten. I ett andra steg beskrivs möjligheterna att utforma ett system som ger rättsväsendets myndigheter ett statistiskt underlag för att framöver följa utvecklingen av it-inslag i de anmälda brotten. Dels redogörs för det arbete som pågår på Brå för att göra det möjligt att på ett bättre sätt kunna följa it-inslag i den anmälda brottsligheten, till exempel genom införandet av nya brottskoder och genom att utveckla de stora frågeundersökningar som myndigheten genomför regelbundet (Nationella trygghetsundersökningen och Skolundersökningen om brott). Dels beskrivs några av de ärendehanteringssystemen som används av rättsväsendets myndigheter och hur it-inslag registreras i dagsläget. Avslutningsvis ger Brå förslag på hur ett statistiskt system skulle kunna utformas för att framöver kunna följa utvecklingen av it-inslag i de anmälda brotten.

För att besvara frågeställningarna kopplade till den tredje delen av regeringsuppdraget har Brå skickat ut skriftliga frågor till personer som är verksamma inom Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten, Domstolsverket, Tullverket, Kustbevakningen, Skatteverket och Säkerhetspolisen.[70] Samtliga av dessa myndigheter fick frågor om vilket behov myndigheterna har av statistik för att följa utvecklingen av it-inslag i de anmälda brotten, vilket/vilka ärendehanteringssystem som används inom myndigheten i dag och vilka möjligheter det finns att från syste-

[70] För en mer detaljerad beskrivning, se metodavsnittet.

met få ut statistik som kan användas för att följa utvecklingen av it-inslag i den anmälda brottsligheten.

Förutom resultaten från de skriftliga frågorna till rättsväsendets myndigheter redogörs även i kapitlet för vad som framkommit i Brås intervjuer med anställda inom Polismyndigheten, den myndighet där behovet av statistik bedöms vara störst. Intervjuerna konkretiserade myndighetens behov av ett statistiskt system som gör det möjligt att kunna följa utvecklingen av it-inslag i de anmälda brotten, vilka nyckeltal en sådan statistik i så fall bör innehålla samt hur ett sådant system i så fall bör utformas. I kapitlet redogörs även för vilka möjligheter det finns att mäta it-inslag i de anmälda brotten genom att använda Brås olika datakällor, samt vilka förändringar som har genomförts (eller planeras) för att i framtiden göra det möjligt att mäta it-inslag i brottsligheten.

Behov av statistik för att kunna följa it-inslagen i de anmälda brotten

Både svaren på de skriftliga frågorna och Brås intervjuer med personer från rättsväsendets myndigheter visar att det finns ett tydligt behov av statistik för att kunna följa it-inslagen i de anmälda brotten, men att olika myndigheter uttrycker ett olika stort behov. Störst behov av statistik uttrycker *Polismyndigheten*, där det både efterfrågas statistik som visar förekomsten av it-inslag i den anmälda brottsligheten rent generellt och en mer verksamhetsnära statistik. Enligt Brås intervjupersoner finns det till exempel en efterfrågan på statistik som visar på inflödet av beställda it-undersökningar till myndighetens it-forensiska sektioner. Statistiken skulle kunna användas för att skapa en bättre grundförståelse för hur utvecklingen ser ut när det gäller förekomsten av it-inslag i den anmälda brottsligheten. Flera intervjupersoner upplever en frustration över att chefer och andra beslutsfattare inte förstår hur vanligt det är med it-inslag i de anmälda brotten, vilket resulterar i att det heller inte sker några större satsningar för att höja kompetensen eller öka kapaciteten när det gäller utredningar av it-relaterade brott.

Brås intervjupersoner är överens om att det behövs statistik som kan användas som ett beslutsunderlag vid finansiering och fördelning av resurser inom verksamheten, för att därigenom kunna dimensionera verksamheten efter det inflöde som har registrerats. En av Brås intervjupersoner beskriver bland annat att en registrerad ökning av en viss typ av it-undersökningar kan innebära att Polismyndigheten behöver öka sin kompetens eller kapacitet för att möta utvecklingen, till exempel genom kompetensutveckling, nyrekrytering eller inköp av teknisk utrustning.

Både *Skatteverket* och *Säkerhetspolisen* uttrycker ett behov av att kunna följa utvecklingen av it-inslag i den anmälda brottsligheten. Skatteverket betonar att it förekommer i merparten av de anmälda ekobrotten, till exempel att elektroniska legitimationer och olika tekniska lösningar används som brottsverktyg. Skatteverket uttrycker ett behov av att kunna identifiera vilka brottsverktyg och modus som används då det är it-inslag i brottsligheten, men även verksamhetsnära statistik som visar hur man har utrett ärendet, vilken bevisning som har krävts, tidsåtgång i ärendena m.m. De uppger att statistiken skulle kunna användas för att öka kunskapen om brotten, för brottsförebyggande åtgärder och för att kunna göra prognoser och planera verksamheten på ett bra sätt. Säkerhetspolisen efterfrågar i första hand statistik om idkapningar, kryptering (omfattning och typ) och anonymiseringstjänster. De uppger att statistiken skulle kunna användas för att inrikta visst utvecklingsarbete på myndigheten.

Även *Domstolsverket* uttrycker ett intresse av att kunna följa utvecklingen av it-inslag i den anmälda brottsligheten, men även i den dömande verksamheten. För att domstolarna ska kunna utveckla hanteringen av brottmål med it-inslag på ett effektivt sätt krävs kunskap om såväl omfattningen av it-inslag i de anmälda brotten, it-inslagens karaktär samt mer verksamhetsnära statistik som rör den dömande verksamheten, till exempel mängden it-bevisning i brottmålen. Domstolsverket ser bland annat att det kan finnas kopplingar mellan it-inslag i den anmälda brottsligheten och storleken på brottmål i domstol. I många stora brottmål finns it-inslag, vilket ofta resulterar i en stor mängd it-bevisning i målet. Ett statistiksystem som bättre kan registrera och följa utvecklingen av it-inslag i den anmälda brottsligheten ger domstolarna ökade möjligheter att göra bättre bedömningar av hur brottmålen ska hanteras och vilka arbetssätt och rutiner som ska tillämpas på domstolen. En sådan statistik kan också skapa ett behov hos domstolarna när det gäller kompetensutveckling på it-området, men även inverka på bemannings- och rekryteringsfrågor vid domstolarna.

De skriftliga svar som inkommit från *Åklagarmyndigheten, Ekobrottsmyndigheten, Tullverket* och *Kustbevakningen* indikerar att behovet av statistik för att följa it-inslag i brottsligheten inte är lika stort hos dessa myndigheter. Som skäl anförs bland annat att it är ett område som genomsyrar hela samhället och att it-inslag förekommer i alla typer av ärenden. Genom att ha en särskild uppföljning av it-inslag i brottsligheten och den brottsutredande verksamheten finns en risk att huvudfokus läggs på it-frågorna i stället för att säkerställa att metodutvecklingen sker utifrån utvecklingen inom olika brottsområden på ett mer generellt och heltäckande plan. Ett annat skäl som anförs är att en uppföljning

av it-inslag är beroende av en tydlig definition, vilket kan vara svårt att fastställa.

Möjligheten att införa en it-dimension i den officiella kriminalstatistiken

Brå är den myndighet som sedan år 1994 ansvarar för den officiella kriminalstatistiken, där statistiken över anmälda brott ingår som en del. Statistiken över anmälda brott bygger på två lika viktiga bitar av information: brottskoden och brottsantalet. Brottskoden ger information om vilken typ av brott som har anmälts, medan brottsantalet ger information om hur många brott som har anmälts. Tillsammans utgör de underlag till statistiken över anmälda brott, handlagda brott och misstänkta personer. I dag finns det drygt 500 olika aktiva brottskoder som var och en motsvarar en brottslig händelse. Beroende på vilken brottskod som väljs avgörs hur den aktuella händelsen kategoriseras i statistiken. Det primära syftet med koderna är att klassificera en potentiellt brottslig gärning enligt gällande lagstiftning. Därutöver beskrivs eventuella omständigheter kring den brottsliga gärningen vilket utgörs av information som är direkt kopplat till den brottsliga händelsen och/eller de berörda personerna (t.ex. kön, ålder och brottsplats). Brottskodssystemet kan således användas för att beskriva både modus och brottsplats. Det kan däremot inte användas för att beskriva olika vidtagna utredningsåtgärder och förekomst av en viss typ av bevisning.

Den officiella kriminalstatistiken kan i dagsläget inte ge något svar på hur stor andel av samtliga anmälda brott som har begåtts i it-miljö. Det beror på att det inte finns någon generell it-dimension i brottskodssystemet som visar om det anmälda brottet begåtts via elektroniska kommunikationsmedel. I samråd med andra myndigheter inom rättsväsendet (Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten, Tullverket och Säkerhetspolisen) bevakar Brå behovet av att göra förändringar av brottskoderna. Nya brottskoder kan införas som en följd av lagändringar, då den juridiska informationen har förändrats, men de kan också införas efter det att statistikanvändare har uttryckt angelägna behov av nya eller förändrade brottskoder. I det senare exemplet rör det sig ofta om information om brottet, det vill säga omständigheter kring brottet som inte framgår av lagrummet (Brå 2015a). Under senare år har Brå noterat en ökad efterfrågan på statistik som belyser internetrelaterad brottslighet.[71] Krimi-

[71] Det har bland annat inkommit önskemål till Brå från rättsväsendets myndigheter om att skapa brottskoder som särskiljer om brottet har begåtts via internet för brottstyperna olaga hot, ärekränkningsbrott, ofredande och sexuellt ofredande.

nalstatistik som belyser internetrelaterad brottslighet är även efterfrågad från internationellt håll (t.ex. från Eurostat och FN).

Ett förslag som har framkommit i Brås intervjuer med personer som är verksamma inom Polismyndigheten är att införa särskilda brottskoder som visar om en anmäld brottshändelse har it-inslag eller inte. Önskemålen avser både statistiska uppgifter om information kring själva brottet (till exempel om informationsteknologi har använts för brottets genomförande) och administrativ information kopplade till brottet, till exempel vidtagna utredningsåtgärder och förekomst av digital bevisning. Ett införande av sådana koder skulle innebära att det ur statistiken går att utläsa hur stor andel av de anmälda brotten som har it-inslag, och det skulle därmed vara möjligt att kunna följa utvecklingen över tid. Det skulle även ge information om utvecklingen av antalet personer som misstänkts för de aktuella brotten samt deras kön och ålder (genom statistiken över misstänkta personer). I statistiken över handlagda brott skulle det finnas information om olika beslut som har fattats för brottsanmälningarna, till exempel hur stor andel som har lett till personuppklaring[72] eller som har lagts ned. Utvecklingsmönstren för ovan nämnda parametrar skulle slutligen kunna analyseras för såväl landet som helhet, som uppdelat på regional nivå. I följande avsnitt redogörs för Brås inställning till att införa en it-dimension i det nuvarande brottskodsystemet.

En it-dimension i brottskodssystemet innebär en kvalitetsförsämring av statistiken

Att föra in en it-dimension i brottskodssystemet skulle, enligt vad som ovan beskrivits, ge nya möjligheter att framöver kunna följa utvecklingen av it-inslag i de anmälda brotten. Samtidigt finns det flera stora problem med att föra in en sådan dimension. Det första problemet är att införandet av nya brottskoder leder till att statistiken blir betydligt mer oöverskådlig och svårare att hantera. Såsom brottskodssystemet är uppbyggt i dag innebär införandet av en ny central dimension, exempelvis ”internetrelaterat”, eller ”it-relaterat”, att en betydande mängd nya brottskoder behöver skapas om den ska ingå genomgående i brottskatalogen. I sammanhanget bör det noteras att det redan i dag finns en mängd olika dimensioner som används i det nuvarande klassifikationssystemet, till exempel kön, ålder, brottsplats och typ av relation. Eftersom systemet är uppbyggt så att varje unik kombination av dimensioner eller egenskaper ges en egen kod, innebär det att uppsättningen koder för en viss brottstyp fördubblas för varje ny dimension som tillförs. För våldsbrotten, där redan många

[72] Personuppklaring innebär ett beslut om åtal, utfärdat strafföreläggande eller åtalsunderlåtelse.

andra egenskaper beskrivs med koderna, blir denna effekt särskilt påtaglig.[73]

Om it-aspekten skulle integreras genomgående i klassifikationssystemet skulle det innebära att brottskoderna skulle bli betydligt svårare att hantera och resultera i en kraftigt ökad uppgiftslämnarbörda för rättsväsendets myndigheter. I förlängningen skulle det leda till att statistikens kvalitet påverkas negativt. Vid en granskning av användningen av brottskoder framkom att brottskategorier med färre mängder brottskoder (t.ex. skadegörelse) höll en betydligt högre kvalitet än de som hade fler (t.ex. stöldbrott) (Brå 2012).

Det finns goda skäl till att vara återhållsam med antalet koder i brottskodssystemet. Dagens system innehåller redan nu ett stort antal brottskoder och det har under tidens gång utökats med många nya koder, sannolikt långt fler än det var tänkt när systemet togs fram på mitten av 1960-talet (Brå 2002). Varje gång det läggs till nya brottskoder riskerar det att försämra kvaliteten, men även försvåra jämförelser över tid.

Svårt att skapa en enhetlig definition

Det andra problemet med att införa en it-dimension i klassifikationssystemet för brott är att en sådan dimension bör vila på en tydlig och enhetlig definition av begreppet (t.ex. ”it-relaterad”). Om begreppet inte avgränsas och tydligt definieras kan det bli mycket svårt att uttolka vad som avses med ”it-relaterad” brottslighet i varje enskilt fall. Även om en tydlig definition av begreppet införs kan det ändå vara svårt för enskilda anmälningsmottagare att bedöma om det anmälda brottet är it-relaterat eller inte. Sammantaget leder definitionsproblematiken till att det blir mycket svårt att avgöra om ett ärende är it-relaterat eller inte, vilket gäller såväl för den som ska registrera ett brott som för den som ska tolka innebörden av en registrerad brottskod.

Brottskoderna kommer på sikt att upphöra

Det tredje problemet när det gäller att föra in nya brottskoder är att det för närvarande pågår ett omfattande utvecklingsarbete inom ramen för Rättsväsendets informationsförsörjning (RIF) med syfte att införa en enhetlig struktur för registreringen av grunduppgifter inom rättsväsendets myndigheter. Det kommer

[73] Enbart för brottet misshandel finns det närmare 70 olika brottskoder. Förutom att särskilja om misshandel är grov eller av normalgraden finns även flera andra dimensioner som styr vilken brottskod som ska registreras (t.ex. om målsäganden är 0-6 år, 7-14 år, 15–17 år eller 18 år eller äldre, om gärningspersonen är obekant eller bekant, om målsäganden och gärningspersonen har/har haft en nära relation samt om misshandeln har ägt rum inomhus eller utomhus).

bland annat att innebära att brottskoderna på sikt upphör och i stället ersätts av ett system som kombinerar juridisk information med information om omständigheterna kring brottet, så kallad brottsinformation (Justitiedepartementet 2014). Tanken är att användaren först ska registrera juridisk information för brottet och därefter kunna välja att ange för brottstypen relevant brottsinformation i syfte att närmare beskriva den aktuella händelsen.

Det nya systemet förväntas kunna erbjuda större möjligheter att föra in olika dimensioner av de anmälda brotten (t.ex. it-inslag) utan att det medför lika stora praktiska problem för uppgiftslämnarna och därmed ge en bättre kvalitet än vad som kan åstadkommas genom brottskodssystemet. När systemet om brottsinformation väl ska utvecklas kommer det, inom ramen för samarbetet mellan rättsväsendets myndigheter, att finnas utrymme att klargöra vilket behov myndigheterna har av att kunna särskilja it-inslagen i de anmälda brotten, vad i så fall dessa it-inslag ska bestå av och hur de ska registreras samt att utreda vinsten respektive kostnaden för att samla in sådan information.

Brottskoderna syftar inte till att ge administrativ information om brottet

Det fjärde problemet med att införa en it-dimension i klassifikationssystemet för brott är att det med hjälp av brottskoderna inte finns någon möjlighet att registrera it-inslag enligt den vida definition av it-inslag som används i den här rapporten, vilket också efterfrågas av Brås intervjupersoner. Enligt denna definition kan informationsteknologi antingen ha använts som mål för brottet, som medel för själva genomförandet eller så kan brottet på annat sätt ha någon form av ”it-beröring”, det vill säga att det finns bevisning i digital miljö. Det primära syftet med brottsklassifikationssystemet är, som ovan nämnts, att klassificera en brottslig gärning enligt gällande lagstiftning. Dessutom beskrivs eventuella omständigheter kring brottet i form av modus och tillvägagångssätt. Brottskoderna kan däremot inte användas till att ge administrativ information kring brottet, som att visa förekomst av en viss typ av bevisning i ärendet eller vidtagna utredningsåtgärder. Vid anmälningstillfället, då brottskoden registreras, finns det sällan sådan information tillgänglig. Om det finns ett behov av att registrera administrativ information kring brottet skulle det behövas ett annat system än brottsklassifikationssystemet.

Brås genomförda och planerade förändringar för att möta efterfrågan av statistik

För att möta efterfrågan av statistik som gör det möjligt att följa utvecklingen av it-inslag i de anmälda brotten har Brå genomfört flera förändringar i de befintliga datakällor som myndigheten ansvarar för. Det gäller både införandet av nya brottskoder och genomförda och planerade förändringar i Brås frågeundersökningar.

Införandet av nya brottskoder för ärekränkning och olaga hot

Det ovan nämnda RIF-arbetet, som innebär att brottskoder kommer att ersättas med brottsinformation, är inte nära förestående i tiden. En rad omständigheter har inneburit att det uppstått förskjutningar i RIF-arbetet och det är i dag ovisst när ett utvecklingsarbete i denna del kan starta. Det innebär att det kommer att ta många år innan ett nytt system för strukturerad brottsinformation kan förväntas vara på plats.[74] Fram till år 2016 har det i brottsklassifikationssystemet funnits ett fåtal koder som visar om ett brott har it-inslag: datorbedrägeri, bedrägeri med hjälp av internet, dataintrång, datasabotage, internetrelaterade barnpornografibrott, brott mot upphovsrätten genom fildelning samt brott mot det industriella rättsskyddet med hjälp av internet.[75] På grund av de förskjutningar som uppstått i RIF-arbetet, och för att det finns en tydlig efterfrågan på brottskoder som visar om brottet har it-inslag, tog Brå i samband med den brottskodsrevidering som infördes i årsskiftet 2015/2016, initiativ till att ändå införa en it-dimension för ett fåtal brottskoder. I förslaget ingick att införa nya brottskoder för olaga hot och ärekränkningsbrott som urskiljer om det anmälda brottet har begåtts via elektroniska kommunikationsmedel (internetrelaterat respektive ej internetrelaterat).[76]

År 2016 införde Brå de nya brottskoderna i brottsklassifikationssystemet: *internetrelaterade olaga hot och internetrelaterade ärekränkningsbrott*.[77] Med internetrelaterad avses ”elektroniskt

[74] För att systemet med brottsinformation ska kunna införas krävs att införandet av juridisk information (JIF) har implementerats av samtliga myndigheter i brottmålsprocessen. Polisen avser att införa JIF tidigast år 2017, och dessförinnan kan inte ett system med brottsinformation tas fram eftersom det bygger på JIF.

[75] Utöver uppräknade brottskoder finns det ett antal som brukar beskrivas som att de i huvudsak begås i it-miljöer, till exempel brott mot personuppgiftslagen, olovlig avlyssning och brott mot telehemlighet.

[76] Båda brottstyperna är sådana till sin karaktär att de i relativt stor utsträckning kan antas ske via internet, till exempel på sociala nätforum eller genom e-post, sms och liknande.

[77] Införandet av it-dimensionen innebär att det numera finns 10 olika brottskoder för brottstypen olaga hot och 8 olika koder för ärekränkning.

överförd information via sociala medier, chattar, sms eller dylikt" (Brå 2015a). De nya brottskoderna kommer att göra det möjligt att på sikt se hur stor andel av de anmälda brotten rörande olaga hot respektive ärekränkningsbrott som är "internetrelaterade". Det kommer även att vara möjligt att se hur stor andel av de anmälda brotten som leder till personuppklaring respektive läggs ned (genom statistiken över handlagda brott) och de misstänkta personernas kön och ålder (enligt statistiken över misstänkta personer). Eftersom brottskoderna för olaga hot och ärekränkningsbrott redan är uppdelade utifrån målsägandens kön och ålder (man eller kvinna, över respektive under 18 år) kommer det i framtiden, utifrån den officiella kriminalstatistiken, även vara möjligt att besvara frågeställningar om det finns någon skillnad mellan män och kvinnor, respektive unga och vuxna, i förekomsten av polisanmälda hot och ärekränkningsbrott som sker via internet.

Under år 2016 planerar Brå dessutom, i samråd med övriga myndigheter som ingår i förvaltningsorganisationen, att påbörja en översyn av brottskoderna som avser bedrägeribrott (9 kap. BrB). I en tidigare kvalitetsgranskning av brottskoderna (Brå 2012) framkom exempelvis att händelser som borde ha kodats som "bedrägeri med hjälp av internet" i många fall kodades som "övrigt bedrägeri". Det innebar, enligt Brås skattning, att cirka 20 procent för få bedrägerier med hjälp av internet redovisades i 2010 års officiella kriminalstatistik. En sådan hög felfrekvens innebär en tydlig risk att omfattningen av ärendeinströmningen av den efterfrågade brottstypen underskattas. Den planerade översynen syftar till att höja kvaliteten i statistikredovisningen, att säkra att bedrägerikoderna uppfyller de behov som finns samt att de används enhetligt och håller en god kvalitet.

Utsatthet för brott via internet införs i den Nationella trygghetsundersökningen (NTU)

Ett sätt att studera brottsutvecklingen är att använda sig av frågeundersökningar till representativa urval av befolkningen. På Brå genomförs varje år den Nationella trygghetsundersökningen (NTU) där drygt 12 000 personer mellan 16 och 79 år får besvara frågor om utsatthet för brott, trygghet, förtroende för rättsväsendet samt brottsoffers kontakter med rättsväsendet. Med hjälp av undersökningen kan man studera brottsutvecklingen utan att vara beroende av att brotten har anmälts till polisen. I NTU ställs frågor om utsatthet för en rad olika typer av brott (till exempel misshandel, bedrägeri, sexualbrott, cykelstöld och bostadsinbrott). Respondenter som uppger sig ha utsatts för brott under föregående år ges ett antal följdfrågor om olika omständigheter kring det brott de utsatts för och om de har polisanmält händelsen.

I dagsläget är it-dimensionen till viss del integrerad i NTU, men enbart för brottstyperna olaga hot respektive bedrägeri. Respondenter som uppger att de utsatts för hot ges en följdfråga om på vilket sätt de blev hotade, där telefonsamtal/sms och e-post/chatt/internet är två möjliga svarsalternativ. Respondenter som uppger sig ha utsatts för bedrägeri får svara på frågan om det var via internet som personen ”blivit lurad” (Brå 2016:1).[78] Inom NTU pågår just nu ett omfattande förändringsarbete, vilket bland annat kommer att innebära att det nuvarande frågeformuläret ses över. En av de åtgärder som planeras är att lägga in en it-dimension i svarsalternativen för fler brottstyper än i dag, till exempel när det gäller frågor om sexualbrott och olaga förföljelse. Brå planerar även att föra in en helt ny fråga som avser att mäta utsatthet för kränkningar av den personliga integriteten via internet, till exempel att någon har spridit känsliga uppgifter, bilder, filmer och/eller kommentarer om personen via sociala medier eller i något annat sammanhang på internet som syftat till att kränka eller skada personen. Förändringarna kommer tidigast att införas i 2018 års trygghetsundersökning.

Om förändringarna genomförs kommer det på sikt att kunna vara möjligt att studera hur utsattheten ser ut för olika typer av brott via internet samt skillnader i utsatthet mellan till exempel kvinnor och män samt unga och vuxna.

Frågor om it-relaterade brott i Skolundersökningen om brott (SUB)

En annan frågeundersökning som genomförs regelbundet på Brå är Skolundersökningen om brott (SUB). Undersökningen utgörs av en enkät om delaktighet i och utsatthet för brott och riktar sig till ett urval av elever i årskurs nio (ungdomar i 15-årsåldern) över hela landet. Undersökningen har genomförts sedan år 1995.

I 2015 års datainsamling gjordes flera stora förändringar av skolundersökningen, bland annat när det gäller urvalsmetod. I samband med det gjordes även en översyn av enkäten. En förändring var att införa flera nya frågor om brott som begås via elektroniska kommunikationsmedel. Elever som uppger att de har utsatts för brott under de senaste 12 månaderna får i enkäten bland annat en följdfråga om var brottet inträffade. För bland annat brottstyperna olaga hot och sexualbrott infördes i 2015 års enkät det nya svarsalternativet ”via internet/sociala medier/mobiltelefon”. I enkäten infördes även frågor om eleverna hade

[78] Även i Brås trygghetsundersökning som riktar sig till politiker och förtroendevalda *(Politikernas trygghetsundersökning, PTU)* finns information om andelen politiker som uppger att de varit utsatta för olika former av hot och trakasserier bland annat via sociala medier.

utsatts för att någon hade skrivit kränkande saker om dem via internet (t.ex. på Facebook, Instagram, en blogg eller liknande) samt om någon hade lagt upp bilder eller filmklipp på dem på internet som de inte ville skulle spridas. I frågorna där eleverna själva får rapportera om sin delaktighet i brott ställs även frågor om de själva har ”skrivit något eller lagt ut bilder/film på internet för att kränka någon” eller om de har laddat ned musik, filmer, spel eller annan programvara genom illegal fildelning.

De nya frågorna i skolundersökningen gör det möjligt att till exempel studera hur stor andel av de olaga hot som de unga utsatts för som har skett via internet, sociala medier eller via en mobiltelefon. Det kommer även att vara möjligt att analysera utsattheten kopplat till flera bakgrundsfaktorer, såsom kön, familjesituation och egen delaktighet i brott. De nya frågorna kommer även att möjliggöra analyser av hur stor andel av niondeklassarna som uppger att de själva har kränkt någon annan på internet, respektive laddat ned filer illegalt.

Befintliga ärendehanteringssystem och statistik över it-inslag

Ett annat sätt för rättsväsendets myndigheter att följa utvecklingen av it-inslag i den anmälda brottsligheten är att de själva utvecklar indikatorer utifrån de data som de har tillgång till inom ramen för sina egna ärendehanteringssystem. I följande avsnitt beskrivs några av de befintliga ärendehanteringssystemen som i dag används av rättsväsendets myndigheter samt hur it-inslag i brottsanmälningar/brottmål registreras i dagsläget. Även här bygger resultatet på svaren från de skriftliga förfrågningar som Brå skickade ut till personer verksamma inom rättsväsendets myndigheter samt på de intervjuer som Brå har gjort med personer verksamma inom Polismyndigheten och Åklagarmyndigheten.

Rättsväsendets myndigheter använder sig av olika ärendehanteringssystem som kan vara av intresse när det gäller möjligheter att ta fram statistik över förekomsten av it-inslag i de anmälda brotten. Inom Polismyndigheten använder man sig av flera separata ärendehanteringssystem för olika delar av den brottsutredande processen. Ett av systemen är *Rationell anmälningsrutin (RAR)*, som är det system där brottsanmälningar registreras och diarieförs.[79] RAR används i dagsläget av Polismyndigheten och Ekobrottsmyndigheten, men det pågår ett arbete för att även Kustbevakningen ska få tillgång till systemet. I dagsläget registreras inte it-inslag i de anmälda brotten på något annat sätt än genom

[79] Enligt Polisens it-strategi för 2015-2017 ska funktionen för anmälningsupptagning som finns i RAR utvecklas i Durtvå så att RAR kan avvecklas (Polismyndigheten 2015a).

brottskod. Som ovan nämnts finns det endast ett fåtal brottskoder som visar om det anmälda brottet har skett i it-miljö eller inte.

Inom polisen används även ärendehanteringssystemet *Datoriserad utredningsrutin tvångsmedel* (DurTvå), där information som hör till själva utredningsprocessen dokumenteras, till exempel olika typer av beslut, direktiv, förhör, beslagsprotokoll och andra utredningsåtgärder. Durtvå används inom Polismyndigheten och Ekobrottsmyndigheten, men även här pågår ett arbete för att även Kustbevakningen och Tullverket ska få tillgång till systemet. Durtvå är sammankopplat med åklagarväsendets system Cåbra (se nedan), vilket gör det möjligt att skicka direktiv, beslut samt material mellan systemen. Från DurTvå finns det en möjlighet att få fram statistik om olika typer av it-relaterade beslag, såsom mobiltelefoner och datorer. Sådan statistik skulle kunna användas som en indikator för att kunna följa utvecklingen av it-inslag i de anmälda brotten.

Utöver dessa system finns inom Polismyndigheten systemet *Tekniskt protokoll* (Tekpro) som används vid kriminaltekniska undersökningar och delar av den it-forensiska verksamheten samt systemet *Forensiska uppdrags- och materialhanteringssystemet* (Forum), som är ett ärendehanteringssystem för laborativ verksamhet som i dagsläget används av Nationellt forensiskt centrum (NFC). I båda systemen registreras information om till exempel antalet beställda it-undersökningar inom olika kategorier.

Inom Åklagarmyndighetens ärendehanteringssystem *Centralt system för åklagarväsendets brottmålshantering* (Cåbra), Sveriges Domstolars system för målhantering (Vera), Skatteverkets system *Brottsanmälan* och *Brottsutredningsstöd* samt Tullverkets ärendehanteringssystem *BOW* och *Tullmålsjournalen* (TMJ) registreras inte någon information om it-inslag i samband med brott.[80]

Sammantaget går det att konstatera att inget av de ärendehanteringssystem som används av rättsväsendets myndigheter i dagsläget kan ge ett statistiskt underlag över utvecklingen av it-inslag i de anmälda brotten totalt sett. Däremot kan några av systemen användas för att få fram olika indikatorer över utvecklingen, till exempel genom antalet it-beslag (DurTvå) eller antalet beställda it-undersökningar (TekPro eller Forum). För att på sikt kunna producera en nationell statistik med hög kvalitet behöver dock systemen utvecklas ytterligare. I nästkommande avsnitt ges Brås förslag på hur ett statistiskt system skulle kunna utformas för att framöver kunna följa utvecklingen av it-inslag i de anmälda brotten.

[80] Kustbevakningen använder sig i dagsläget av ett pappersbaserat system för dokumentation av förundersökningsprocessen, där it-inslag inte registreras. Säkerhetspolisen har inte besvarat Brås frågor rörande vilket ärendehanteringssystem som används.

Möjligheten att utveckla ett statistiskt system för att mäta it-inslag i de anmälda brotten

I den första delen av det här kapitlet beskrivs att det inom flera av rättsväsendets myndigheter finns ett tydligt behov av statistik som kan visa utvecklingen av it-inslag i de anmälda brotten. Enligt personer som Brå har intervjuat och som är verksamma inom Polismyndigheten finns det dels ett behov av ett statistiskt underlag för att kunna påvisa att det sker en ökning av it-inslag i ärendena, dels ett behov av en mer verksamhetsnära statistik som till exempel visar utvecklingen av antalet beställda it-undersökningar. Syftet med sådan statistik är att skapa ett beslutsunderlag för finansiering och fördelning av resurser inom myndigheten. Även om flera av företrädarna från rättsväsendets myndigheter uttrycker ett önskemål om statistik som gör det möjligt att kunna följa it-inslagen i samtliga av de anmälda brotten anser de flesta att sådana siffror troligtvis är mycket svåra att få fram. Det beror på att en stor andel ärenden i dag innehåller någon typ av it-inslag. Eftersom det dessutom saknas en enhetlig definition av begreppet skulle en sådan dimension vara svår att registrera.

Brås sammantagna bedömning är att det inte är möjligt att införa en generell it-dimension för samtliga brottstyper i dagens klassifikationssystem för brott, eftersom det skulle leda till en alltför stor börda för uppgiftslämnarna samt att kvaliteten inte kan förväntas hålla en tillräckligt hög nivå, vilket skulle hota systemets grundläggande funktion. Syftet med brottsklassifikationssystemet är heller inte att ge administrativ information kring brottet, till exempel vidtagna utredningsåtgärder eller förekomst av viss typ av bevisning. Det finns dock en möjlighet att föra in en it-dimension för enskilda brott, där det finns en särskild efterfrågan för att kunna urskilja hur stor andel av brotten som har begåtts i it-miljö. År 2016 infördes, som ovan nämnts, en it-dimension för brottstyperna olaga hot och ärekränkningsbrott, där det numera görs en åtskillnad om brottet är ”internetrelaterat” eller inte. Innan det eventuellt införs fler koder som gör det möjligt att urskilja om brottet är ”internetrelaterat” bör de nyligen införda brottskoderna kvalitetsgranskas. Brås bedömning är att det i dagsläget inte är aktuellt att genomföra några genomgripande förändringar i det nuvarande brottskodssystemet. Om det finns ett önskemål hos rättsväsendets myndigheter om särskild statistik för att mäta it-inslag i de anmälda brotten kommer det däremot att finnas möjlighet att föra in den aspekten inom ramen för Rättsväsendets informationsförsörjning (RIF).

Brå har även fört in en it-dimension i myndighetens två stora frågeundersökningar om brott: Nationella trygghetsundersökningen om brott (NTU) och Skolundersökningen om brott (SUB).

Det bör dock poängteras att varken de nya brottskoderna eller de genomförda eller planerade förändringarna i NTU och SUB kommer att kunna ge något svar på hur stor andel av brotten som har it-inslag, enligt den vida definition som används i den här rapporten. Förändringarna syftar enbart till att mäta om elektroniska kommunikationsmedel har använts för att begå själva brottet.

Skapa en verksamhetsnära statistik

Det huvudsakliga syftet med att få fram ett statistiskt underlag över it-inslag i de anmälda brotten är, enligt Brås intervjupersoner, att det ska finnas ett beslutsunderlag för verksamhetens satsningar på exempelvis kompetens och kapacitet. Brås bedömning är att sådan statistik enklast tas fram genom en verksamhetsnära statistik, som bygger på uppgifter som registreras i myndigheternas egna ärendehanteringssystem. En sådan statistik skulle med en större tydlighet kunna kopplas till verksamhetens behov av kompetens och resurser och därmed kunna användas som ett beslutsunderlag för dimensionering av verksamheten.

I Brås intervjuer med personer verksamma inom Polismyndigheten finns det i första hand en efterfrågan på statistikuppgifter som kan beskriva ärendeflödet inom den it-forensiska verksamheten. Flera är överens om att den it-forensiska processen i dag är en flaskhals i många utredningar, vilket till stor del beror på att it-forensikerna är för få. En statistik som på ett bättre sätt kan visa hur inflödet ser ut skulle kunna identifiera de ”svaga länkarna” i den it-forensiska processen och kunna ligga till grund för ett förbättringsarbete. Flera menar även att en sådan statistik skulle kunna användas som underlag för att påvisa behov av ökade resurser, till exempel att det inom en viss region behövs anställas fler it-undersökare som har en viss typ av kompetens.

Det finns en relativt stor enighet bland Brås intervjupersoner inom Polismyndigheten om vilken typ av statistikuppgifter (s.k. nyckeltal) som efterfrågas. Dessa är exempelvis:

- antal beställda it-undersökningar
- typ av it-undersökningar som beställs (t.ex. vilken slags enhet som ska undersökas och datamängd[81])
- grad av komplexitet i beställningen[82]
- antal genomförda/makulerade it-undersökningar

[81] En intervjuperson beskriver att en registrerad undersökning av en dator inte ger särskilt mycket information, eftersom dess innehåll kan variera i såväl datamängd, grad av komplexitet (t.ex. krypteringar) och hur omfattande beställningen är. Tidsåtgången för en beställning kan variera från någon enstaka timme till ett års arbete (t.ex. vid barnpornografibrott).

[82] Som ovan nämnts efterfrågar t.ex. Säkerhetspolisen omfattningen av och typ av krypteringar och anonymiseringstjänster.

- antal it-undersökningar i balans (väntande på kö)
- antal dagar från beställning till slutredovisad undersökning
- antal dagar/timmar en it-undersökare lägger på en viss it-undersökning (tidsredovisning)

Inom Domstolsverket finns det önskemål om att kunna få statistik som visar hur många mål som innehåller it-inslag samt vilken typ av it-inslag det är fråga om. Det finns även ett intresse av att få statistik som beskriver genomströmningstider för mål med it-inslag (från att ett mål inkommer till domstolen till att det avgörs), omfattningen och karaktären på dessa mål och i vilken typ av brottslighet it-inslag är vanligast förekommande. Som ovan nämnts uttrycker Skatteverket ett behov av verksamhetsnära statistik som till exempel visar hur man har utrett ärendet och tidsåtgång.

Ett nationellt uppföljningsverktyg

Brås förslag är att skapa ett nationellt uppföljningssystem för Polismyndighetens it-forensiska verksamhet.[83] Ett nationellt uppföljningssystem för den it-forensiska verksamheten skulle, förutom att skapa ett statistiskt underlag för planering och styrning av verksamheten, även kunna användas som stöd i det it-forensiska arbetet. Flera av Brås intervjupersoner uttrycker ett önskemål om att systemet till exempel ska kunna användas för att ärendefördela mellan olika it-forensiska sektioner för att jämna ut arbetsbelastningen, att det ska finnas information om var beslagtaget gods finns och att det ska finnas en koppling mellan systemet och andra ärendehanteringssystem.[84]

I och med omorganisationen av Polismyndigheten pågår ett omfattande arbete med att utveckla den it-forensiska verksamheten inom myndigheten. Nationellt forensiskt centrum (NFC) har fått processansvar för den it-forensiska verksamheten och bedriver för närvarande ett stort arbete (det s.k. harmoniseringsprojektet) för att skapa en större enhetlighet inom den forensiska verksamheten (där den it-forensiska verksamheten ingår). En del av det arbetet är att utveckla ett gemensamt ärendehanteringssys-

[83] Även när det gäller Säkerhetspolisens, Skatteverkets och Domstolsverkets behov av att följa utvecklingen av it-inslag i de anmälda brotten/brottmålen är Brås bedömning att de behov som efterfrågas lämpligast tas fram genom uppgifter som registreras i myndigheternas egna ärendehanteringsystem. Att utveckla ett sådant system kräver tydliga definitioner av det som avses mätas och ett enhetligt sätt att registrera uppgifterna på.

[84] Idag registreras exempelvis beslag i ärendehanteringssystemet DurTvå. Det finns dock inga kopplingar mellan DurTvå och TekPro (som i dag ofta används inom den it-forensiska verksamheten), vilket innebär att beslag som ska undersökas måste registreras på nytt. Flera it-forensiker som Brå har intervjuat anser att det vore önskvärt att beslagen kunde överföras automatiskt mellan de olika systemen.

tem. Enligt företrädare från NFC har det ännu inte fattats något beslut om vilket ärendehanteringssystem som ska användas för den it-forensiska verksamheten. Förutom att systemet ska kunna användas som ett laborativt stöd ska det kunna leverera en statistik som håller hög kvalitet. Ett av de system som har diskuterats som framtida lösning är det kriminaltekniska verktyget TekPro, ett annat är det laborativa stödverktyget Forum (se beskrivning ovan). I Brås intervjuer med företrädare från Noa har det även lyfts fram ett förslag om att utveckla ärendehanteringssystemet DurTvå, vilket har fördelen att statistikuppgifter från både utredningsprocessen och den it-forensiska processen samlas i ett och samma system.

Brås bedömning är att Polismyndighetens arbete med att fastställa vilket ärendehanteringssystem som är bäst lämpat att använda i den it-forensiska verksamheten är viktigt och att NFC och Noa samarbetar i frågan med att klargöra vilket behov av statistikuppgifter som finns, vilka slags it-undersökningar ett sådant system bör inrymma och hur de olika begreppen ska definieras, till exempel begreppet it-forensik. *För det första* bör det övervägas vilka kostnads- och kvalitetsmässiga för- och nackdelar det finns med att ha ett stort system som täcker hela utredningsprocessen (inklusive den it-forensiska processen) gentemot att ha ett separat system för den it-forensiska processen när det gäller förmågan att producera verksamhetsnära statistik. *För det andra* bör det diskuteras vilka slags funktioner systemet bör innehålla, till exempel vilka uppgifter som ska registreras, hur kopplingen ska se ut mellan systemet och övriga ärendehanteringssystem inom Polismyndigheten och vem som ska använda systemet. Företrädare från Noa poängterar att det är viktigt att definitionen av vad som är en it-forensisk åtgärd[85] (och vem som är en it-forensiker) förtydligas innan ett gemensamt uppföljningssystem tas fram, eftersom det både styr vem som ska använda sig av systemet och vilka slags undersökningar som ska registreras i det.

Brå vill även understryka vikten av att det i arbetet tas fram tydliga riktlinjer för hur uppgifter ska registreras. För att uppnå en statistikproduktion som håller en hög kvalitet är det nödvändigt att statistikuppgifter registreras enhetligt av samtliga användare och enligt en förutbestämd struktur.

[85] Enligt Brås intervjupersoner bygger exempelvis de nuvarande systemen TekPro och Forum på undersökning av beslagtaget gods, medan en stor del av it-forensikers arbete i dag handlar om it-undersökningar av annan karaktär, till exempel internetinhämtning, arbete med skadlig kod etc.

Resultaten i korthet

- Inom flera av rättsväsendets myndigheter finns det ett behov av statistik för att följa it-inslagen i de anmälda brotten. Behovet gäller både statistik som visar förekomsten av it-inslag i den anmälda brottsligheten generellt och mer verksamhetsnära statistik.
- Brås sammantagna bedömning är att det inte är möjligt att föra in en it-dimension i det brottskodssystem som ligger till grund för den officiella kriminalstatistiken. En sådan förändring skulle bland annat resultera i en kraftigt ökad uppgiftslämnarbörda för rättsväsendets myndigheter och försämra statistikens kvalitet, vilket skulle hota systemets grundläggande funktion.
- För att möta det behov som finns av ett statistiskt underlag avseende it-relaterade brott införde Brå år 2016 två nya brottskoder i brottskodssystemet: internetrelaterade olaga hot och internetrelaterade ärekränkningsbrott. Brå har även fört in en it-dimension i myndighetens frågeundersökning Skolundersökningen om brott (SUB) och planerar även att göra liknande förändringar i Nationella trygghetsundersökningen (NTU).
- Brå bedömer att det behov av statistik som myndigheterna uttrycker lämpligast tas fram genom verksamhetsnära statistik, som bygger på uppgifter som registreras i myndigheternas egna ärendehanteringssystem. Nyckeltal som efterfrågas är bland annat antal beställda it-undersökningar och tidsåtgång för genomförda it-undersökningar.
- Brås förslag är att skapa ett nationellt uppföljningssystem för Polismyndighetens it-forensiska verksamhet. Arbetet som pågår med att ta fram ett sådant system bedrivs för närvarande vid Nationellt forensiskt centrum (NFC). NFC och Nationella operativa avdelningen (Noa) bör samarbeta i frågan kring hur det framtida systemet bör utformas, vad systemet ska innehålla och hur centrala begrepp ska definieras (t.ex. begreppet it-forensik).

Angelägna utvecklingsområden och pågående utvecklingsarbete

Resultatet från Brås studie visar att förekomsten av it-inslag i de anmälda brotten har ökat kontinuerligt sedan år 2006. Det visar såväl den officiella kriminalstatistiken avseende de brott där det utifrån brottskod går att urskilja om ett ärende har it-inslag som den granskning av polisanmälningar som Brå har genomfört inom ramen för studien. Genomgången av polisanmälningarna, tillsammans med underlag från enkäter och intervjuer, visar sammantaget på en stor variation i de ärenden som rättsväsendet har att hantera. It-inslag kan finnas i alla typer av ärenden, och även vid brott som till synes inte har någon som helst it-koppling kan viktig bevisning finnas i digitala miljöer.

Den ökade förekomsten av it-relaterade brott ställer stora krav på rättsväsendets myndigheter när det gäller förmågan att hantera brott med it-inslag. Brås studie visar att det sammantaget finns ett stort behov av såväl kompetens- som kapacitetshöjande åtgärder för att bygga upp en tillräcklig förmåga för att säkerställa en effektiv och rättssäker hantering.

Flera av Brås intervjupersoner berättar till exempel att brott som sker via internet i dagsläget ofta läggs ner, då de ses som omöjliga att klara upp. Det kan dels bero på en bristande kompetens kring vad som går att göra, dels på dåliga erfarenheter, där det tidigare till exempel har varit svårt att få ut bevisning från utländska företag. Flera intervjupersoner betonar dock att rättsväsendets möjligheter att utreda brott som sker via internet ständigt förändras, men att denna information sällan når fram till de förundersökningsledare som fattar besluten. Det riskerar att leda till att ärenden läggs ner i onödan.[86] Förutom att få ärenden klaras upp

[86] I rapporten *Polisanmälda hot och kränkningar mot enskilda personer via internet* (Brå 2015:6) har Brå tidigare fastslagit att en bristande it-kompetens hos förundersökningsledare kan leda till att ärenden som har en utredningspotential ändå läggs ner eftersom förundersökningsledaren inte har tillräckligt god kunskap om vilka utredningsåtgärder som är möjliga.

riskerar de identifierade bristerna att leda till långa handläggningstider för ärenden med it-inslag och en skiftande kvalitet i de it-forensiska undersökningarna.

I följande avsnitt ges en beskrivning av de satsningar som har påbörjats inom Åklagarmyndigheten och Polismyndigheten för att möta utvecklingen av fler it-inslag i de anmälda brotten. I avsnittet ger även Brå förslag på hur de brottsutredande myndigheterna kan gå tillväga för att höja it-kompetensen och öka kapaciteten inom den it-forensiska verksamheten.

Tydligare ansvarsfördelning och begreppsdefinitioner

Det övergripande syftet med ombildningen av polisorganisationen var att ge bättre förutsättningar för att hela myndigheten ska arbeta effektivt, rättssäkert och enhetligt (Genomförandekommittén för nya Polismyndigheten 2014a). Sammanslagningen har skapat nya förutsättningar för att genomföra kompetens- och kapacitetshöjande satsningar för att öka rättsväsendets förmåga att hantera brott med it-inslag. En viktig förändring är att olika aktörer har fått ett uttalat ansvar för olika områden.

Noa har i den nya polisorganisationen processansvar[87] för komplex it-brottslighet, internetrelaterade sexualbrott mot barn och it-relaterade brott (Polismyndigheten 2016a och Polismyndigheten 2016c). Enligt *Beslutsprotokoll avseende inrättandet av ett nationellt it-brottscentrum* (Polismyndigheten 2015c) har Noa även ansvar för att se till att polisen har förmåga att på såväl nationell nivå, som på regionnivå, polisområdesnivå och lokalpolisområdesnivå hantera it-relaterade brott. Inom ramen för detta ansvar har Noa tagit fram direktiv för nationell hantering av komplex it-brottslighet respektive för nationell hantering av internetrelaterade sexualbrott mot barn. I förlängningen kommer det även att arbetas fram nationella direktiv för nationell hantering av övriga it-relaterade brott.

NFC har i den nya polisorganisationen processansvar för den it-forensiska verksamheten (Polismyndigheten 2016a). Inom ramen för NFC:s processansvar för den it-forensiska processen har ett omfattande arbete påbörjats som syftar till att det it-forensiska arbetet ska uppnå större enhetlighet och högre kvalitet samt genomföras med högre effektivitet än tidigare. Projektet *Har-*

[87] De organisatoriska enheternas ansvarsområden beskrivs i Arbetsordningen för Polismyndigheten (Polismyndigheten 2016a) utifrån funktionsansvar och processansvar. Med funktionsansvar avses ansvar för att styra, utveckla och följa upp en viss *verksamhet* och att säkerställa en enhetlighet. Funktionsansvaret omfattar ett personalansvar. Med processansvar avses att styra, utveckla och följa upp en viss *process* och att säkerställa enhetlighet.

monisering av it-forensik innebär att NFC bland annat ska ta fram verifierade arbetsmetoder och ett ackrediterat arbetssätt för it-forensiken för att säkerställa att en och samma it-undersökning genomförs på samma sätt oavsett vem som genomför den eller i vilken del av myndigheten den genomförs (Polismyndigheten 2015d).[88]

I Brås intervjuer påtalar företrädare för Noa och NFC att det finns en viss överlappning mellan de två aktörernas ansvarsområden. Företrädarna menar att det i stor utsträckning beror på avsaknad av definitioner, till exempel skillnader mellan ”laborativ” och ”operativ verksamhet”, vad som räknas som ”it-forensik” och vem som kan kallas för ”it-forensiker”. Enligt Brås intervjupersoner är det i den nya polisorganisationen heller inte helt tydliga gränsdragningar mellan det arbete som ingår i Noas processansvar och det ansvar som ligger på utvecklingsavdelningarna. Även inom Åklagarmyndigheten råder en viss överlappning mellan ansvarsområdena. Enligt en rapport från Åklagarmyndigheten (2015a) rörande internetrelaterade brott kan samverkan mellan olika delar inom myndigheten förbättras.

En risk med den otydlighet som råder i dagsläget är att olika delar av Polismyndigheten arbetar med liknande saker. För att kunna få ett samlat grepp om området it-relaterad brottslighet och kunna genomföra de satsningar som krävs för att stärka rättsväsendets förmåga, anser Brå att ansvarsfördelningen mellan olika aktörer bör förtydligas och att det bör skapas en större enhetlighet och samsyn kring de begreppsdefinitioner som används i arbetet.

Behov av utbildningsinsatser för åklagare

Brås rapport visar att operativa åklagare har behov av kompetensutveckling inom it-området. Resultatet från Brås enkät visar att 88 procent av åklagarna även själva bedömer att de, utifrån sina arbetsuppgifter, har ett stort eller mycket stort behov av kompetensutveckling kring minst en av de utredningsåtgärder som Brå frågar om i enkäten. Behovet av kompetensutveckling är störst för de utredningsåtgärder där kunskapsluckorna är störst, nämligen kring bevismaterial som ligger på internet.[89] Åklagare önskar bland annat bättre kunskap om hur man ska gå tillväga för att få ut information från externa aktörer utomlands; det vill säga vilka regler som gäller, vart man ska vända sig och vad de olika aktörerna lämnar ut för slags information.

[88] Projektet är en del av NFC:s övergripande arbete med att harmonisera all forensisk verksamhet i programmet *Harmonisering av ämnesområden*.

[89] Det vill säga möjligheter att få ut information från externa aktörer utomlands, möjligheten att ta del av elektroniska meddelanden som ligger utanför en mobiltelefons/dators lagringsminne, tillvägagångssättet att begära frysning samt vilka rättsliga möjligheter som finns att säkra information som ligger öppen på internet.

Att it-kompetensen bör höjas bland landets åklagare framkommer även i Åklagarmyndighetens egna rapporter (t.ex. Åklagarmyndigheten 2015a). Dels behöver den lägsta kunskapsnivån höjas hos myndighetens åklagare, dels är det angeläget att upprätthålla spetskompetens på it-området. Enligt Åklagarmyndighetens budgetunderlag för 2015–2017 ska myndigheten långsiktigt satsa särskilda resurser för att kunna hantera den fortsatta utvecklingen av brott i it-miljö, däribland genom utbildningsinsatser (Åklagarmyndigheten 2014). I myndighetens verksamhetsplan för 2016 anges att det kommer att ske flera satsningar på att utveckla förmågan att hantera it-relaterad brottslighet (Åklagarmyndigheten 2015b).

Inom Åklagarmyndigheten är det myndighetens Utbildningscentrum som har det nationella ansvaret för myndighetens kompetensutveckling och för att få fram ett lämpligt kursutbud för åklagarna. Enligt Utbildningscentrum bestäms utbudet av kurser i en dialog med utbildningsrådet i samband med den årliga verksamhetsplaneringen. Beslutet om vilka vidareutbildningskurser som ska erbjudas inom myndigheten är efterfrågestyrt och utgår från vilka identifierade behov och prioriteringar som finns. Förutom det nationella ansvaret för utbildning som finns hos Utbildningscentrum har cheferna för respektive åklagarkammare ansvar för att åklagarna på kammaren har rätt kompetens.

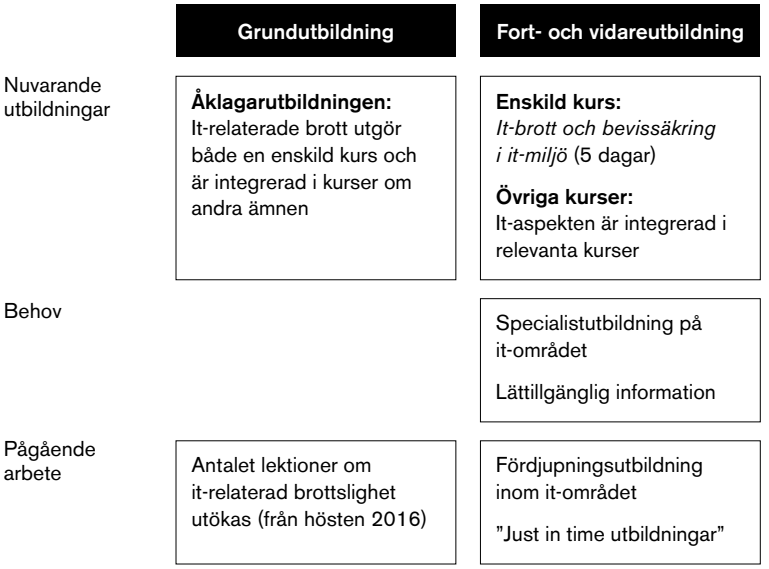
Överväg en obligatorisk it-utbildning för åklagare

För att åklagarna ska hålla en hög kunskapsnivå på it-området är det viktigt att det erbjuds kurser om it-relaterade brott på åklagarnas grundutbildning. Med grundutbildning avses den teoretiska grundutbildning på femton veckor som är obligatorisk för att bli åklagare.[90] Enligt Åklagarmyndighetens Utbildningscentrum behandlas i dagsläget it-frågor på grundutbildningen både som ett enskilt block och som del i de kursmoment där det bedöms vara relevant (figur 12). Från och med hösten 2016 kommer antalet lektioner om it-relaterade brott utökas och lärandemålen har setts över.

Efter grundutbildningen erbjuder Åklagarmyndigheten vidareutbildningskurser på it-området, däribland den s.k. ”It-brottskusen”, men även kurser om andra ämnen där it-aspekten är integrerad.

[90] Åklagarnas grundutbildning genomförs under två perioder. Den första utbildningsperioden, ”aspiranttiden”, är en provanställning och pågår i minst nio månader, tills åklagaraspiranten blivit assistentåklagare. Den andra utbildningsperioden utgörs av tiden mellan förordnandet som assistentåklagare fram till dess att grundutbildningen slutförts. Under denna period genomförs en femton veckor lång teoretisk grundutbildning i internatform (www.aklagare.se).

Figur 12. Nuvarande utbildningar på it-området för åklagare på grund-, fort- och vidareutbildningsnivå, identifierade behov av kompetenshöjande åtgärder samt pågående arbete.[91]



Enligt Åklagarmyndigheten finns behov av utbildningar på specialistnivå. En av de utbildningssatsningar som lyfts fram i Åklagarmyndighetens verksamhetsplan för år 2016 är därför att det under året ska tas fram en *fördjupningsutbildning* avseende it-brott för åklagare, som syftar till att ge en djupare kunskap om utredningar av komplicerade it-brott (Åklagarmyndigheten 2015b). Enligt Utbildningscentrum är kursen främst tänkt att rikta sig till de erfarna kontaktåklagarna som förväntas kunna sprida kunskapen vidare på sina kammare och kunna fungera som bollplank vid svårare it-frågor. Ett antal platser på kursen kommer även att erbjudas till poliser.

Brå anser att det är positivt att it-frågan är ett av myndighetens prioriterade områden och att satsningar görs för att höja kunskaperna om brott med it-inslag bland landets åklagare. Det är positivt att det inom myndigheten erbjuds kurser på it-området på både grund- och vidareutbildningsnivå. Ett utvecklingsområde för Åklagarmyndigheten är att lyfta frågan om hur kunskapen om it-relaterade brott ska kunna nå samtliga åklagare i landet. I

[91] Med *vidareutbildning* avses utbildning med syfte att utveckla högre kompetens inom ett område där deltagaren redan har grundläggande kompetens. För att en utbildning ska ses som en vidareutbildning ska en kursplan finnas och mål ska bedömas efter avslutad kurs. Med *fortbildning* avses uppdatering av kunskaper och färdigheter inom ett område där den enskilde redan har utbildning eller arbetar inom. Deltagarbevis utfärdas som garant för att deltagaren har varit närvarande (Polishögskolan 2014a).

dagsläget är det åklagaren själv som ansöker om att få gå vidareutbildningskursen om it-relaterade brott (”It-brottskursen”), vilket också måste godkännas av kammarchefen. Ett sådant upplägg riskerar att leda till att endast de åklagare som har ett särskilt intresse av dessa frågor söker sig till kursen och att kunskapen därför inte når fram till alla. Åklagarmyndigheten bör överväga möjligheterna att införa ett obligatoriskt baspaket för samtliga åklagare när det gäller brott med it-inslag (se t.ex. den e-learningutbildning som planeras inom Polismyndigheten), alternativt att se över möjligheterna att göra den nuvarande ”It-brottskursen” obligatorisk för att höja grundkompetensen.

Just in time-utbildningar

Ett annat behov som uttrycks i Brås intervjuer med åklagare och i enkäternas fritextsvar är behovet av lättillgänglig information i stunden, det vill säga att det ska finnas en möjlighet att få svar på sina frågor om it-relaterade brott direkt. Flera åklagare menar att deras arbetsbelastning är mycket hög och att det i dag finns ett ”informationsöverflöd” av dokument som de förväntas läsa.

På Åklagarmyndighetens Utbildningscentrum pågår ett arbete för att möjliggöra den egna kunskapsinhämtningen genom s.k. *Just in time-utbildningar*. Enligt Åklagarmyndighetens Utbildningscentrum handlar projektet om att komprimera befintlig kunskap och göra den mer lättillgänglig för åklagarna, t.ex. genom korta filmsekvenser där viktig information sammanfattas. Inom myndigheten finns numera en ny informationskanal *(”Kanal Legal”)*, där det publiceras korta informationsfilmer (t.ex. beslut från JO). Syftet är att öka tillgängligheten och göra det enklare att ta del av information. Brå anser att Just in time-utbildningar troligtvis kan sprida kunskapen om it-relaterad brottslighet på ett effektivt sätt, men vill betona att det bör ses som ett komplement till övrig utbildning. Se även avsnittet om kunskaps- och kompetensspridning längre fram.

Behov av utbildningsinsatser inom polisens kärnverksamhet

Brå bedömer att det finns ett stort behov av kompetensutveckling inom Polismyndighetens kärnverksamhet.[92] Kompetensen om it-relaterade brott är låg hos såväl polisiära förundersökningsledare och utredare som hos förste man på plats. Enkätresultatet visar att 87 procent av de polisiära förundersökningsledarna även själva bedömer att de, utifrån sina arbetsuppgifter, har ett stort eller mycket stort behov av kompetensutveckling kring minst en av de utredningsåtgärder som Brå frågar om i enkäten. Liksom bland åklagare är behovet av kompetensutveckling störst kring säkring av bevismaterial som ligger på internet, i synnerhet då informationen ligger på en utländsk server och kontakt behöver tas med externa aktörer utomlands.

Flera av Polismyndighetens rapporter visar att kompetensen brister när det gäller it-relaterade brott (t.ex. Rikspolisstyrelsen 2013, Rikspolisstyrelsen 2014). Trots att det i flera rapporter har identifierats kunskapsbrister på it-området, verkar det inte ha skett några större satsningar på it-relaterad brottslighet under de senaste åren för att höja kompetensen inom myndigheten. Enligt en rapport från Polishögskolan (2014b) kan det konstateras att utvecklingen på it-området har gått fortare än förändrings- och förnyelsearbetet inom polisen. I Polismyndighetens budgetunderlag för perioden 2017–2019 framhålls dock att den omfattande ökningen av it-relaterade brott ställer betydande krav på polisen, bland annat gällande kompetens och resurser. I budgetunderlaget framhålls att polisen behöver öka sin kompetens, för att både förebygga och utreda it-relaterad brottslighet. En förutsättning för detta är att it-brottsperspektivet beaktas i alla delar av den brottsbekämpande verksamheten (Polismyndigheten 2015e).

I den nya Polismyndigheten är ansvaret för kompetensförsörjning inklusive myndighetens kompetensutveckling samlat hos en gemensam HR-avdelning. Ansvaret för kompetensutveckling har

[92] En myndighets verksamhet brukar delas upp i kärnverksamhet och stödverksamhet. Det finns dock inte någon enhetlig definition av de två begreppen. I rapporten använder sig Brå därför av den definition som användes i Genomförandekommitténs rapport *Beslut om huvuddragen i den nya polismyndighetens detaljorganisation* (2014a) som lyder: ”Med kärnverksamhet inom Polismyndigheten avses det som anges i 2 § polislagen (1984:387) enligt regeringens förslag till ändring i polislagen (prop. 2013/14:110). I paragrafen anges att till polisens uppgifter hör att: 1. förebygga förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten, 2. övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat, 3. utreda och beivra brott som hör under allmänt åtal, 4. lämna allmänheten skydd, upplysningar och annan hjälp, när sådant bistånd lämpligen kan ges av polisen. 5. fullgöra den verksamhet som ankommer på Polismyndigheten enligt särskilda bestämmelser.” Med Polisens kärnverksamhet avses i Brås rapport därmed funktioner som exempelvis förundersökningsledare, utredare och anmälningsmottagare.

samordnats till en enhet som har fyra regionalt placerade kompetenscentrum. Polisens kompetensutveckling ska utgå från verksamhetens behov, förutsättningar och ekonomi. Enligt polisens HR-avdelning görs varje år en inventering av vilket behov det finns av kompetensutveckling inom myndigheten. Utöver det ska det finnas en flexibilitet för tillkommande utbildningsbehov som uppstår under året mot bakgrund av samhällsförändringar eller hastigt uppkomna situationer och fenomen. Kompetensplanering och åtgärder för att säkra kompetens är ett ansvar som ligger på samtliga chefer utifrån respektive ansvarsområde. Liksom hos Åklagarmyndigheten har även chefer på olika nivåer ett ansvar för att medarbetarna har den kompetens som krävs för att utföra sitt arbete.

Öka it-inslagen i grundutbildningen till polis

En viktig åtgärd för att sprida kunskapen om it-relaterade brott är att integrera it-aspekten i grundutbildningen till polis. Med grundutbildningen till polis avses Polisprogrammet, som i dagsläget bedrivs som uppdragsuppbildning vid tre olika lärosäten (Södertörns högskola, Umeå universitet och Linnéuniversitetet i Växjö).[93] Polismyndigheten är beställare och kravställare för utbildningen och ansvarar för att samordna verksamheten vid de tre lärosätena. Programmet består av studier under fyra terminer, varefter studenterna (vid godkänt resultat) erhåller polisexamen och blir behöriga att påbörja sin aspirantutbildning vid Polismyndigheten. Enligt polisens HR-avdelning ingår i dagsläget it-relaterad brottslighet inte som en särskild kurs i Polisprogrammet. Inte heller är it-aspekten tillräckligt integrerad i kurser i andra ämnen på polisens grundutbildning (figur 13).

År 2006 beslutade regeringen att tillsätta en särskild utredare med uppdrag att lämna förslag på hur den dåvarande polisutbildningen borde reformeras. Utredningens uppdrag var att kartlägga hur kraven på polisverksamheten kunde komma att förändras i framtiden. I delbetänkandet *Framtidens polis* (SOU 2007:39) konstaterades att samhällsutvecklingen kommer att ställa ökade krav på polisen under de kommande åren (fram till år 2020). Det konstaterades att en allt större del av brottsligheten på ett eller annat sätt skulle relateras till internet och andra elektroniska kommunikationssystem och att ny teknik kommer att ställa ökade krav på kompetens inom polisorganisationen i framtiden. I mars 2015 tillsatte regeringen en utredning som hade som uppdrag att föreslå hur polisutbildningen kan omformas till

[93] Utbildningen har i många år genomförts i Polismyndighetens (tidigare Rikspolisstyrelsens) regi på Polishögskolan i Sörentorp i Solna. Utbildningen har under de senaste åren fasats ut och de sista studenterna tar sin examen höstterminen 2016 (SOU 2016:39).

Figur 13. Nuvarande utbildningar på it-området för funktioner inom Polismyndighetens kärnverksamhet på grund-, fort- och vidareutbildningsnivå, identifierade behov av kompetenshöjande åtgärder samt pågående arbete.

	Grundutbildning	Fort- och vidareutbildning
Nuvarande utbildningar	**Polisprogrammet:** Ingen enskild kurs om it-relaterade brott. It-aspekten är heller inte tillräckligt integrerad i övriga kurser på grundnivå	**Enskild kurs:** *It-forensisk översiktskurs för förundersöknings-ledare/utredare* (5 dagar) **Övriga kurser:** It-aspekten är inte tillräckligt integrerad i övrig vidareutbildning (t.ex. i den nationella förundersökningsledarutbildningen)
Behov	It-relaterade brott bör integreras bättre i Polisprogrammet	Vidareutbildningssatsningar på it-området för funktioner inom kärnverksamheten (både grundkompetens, fördjupad kompetens och specialistkompetens) It-aspekten bör integreras i relevanta vidareutbildningar/kurser
Pågående arbete	Det pågår en översyn där it-relaterade inslag på Polisprogrammet ses över	Planerad ny utbildningsform (e-learning) på grund-, fortsättnings- och specialistnivå

en ändamålsenlig högskoleutbildning. Syftet med reformen är att säkerställa att Polismyndigheten har den kompetens som krävs för att utföra sitt uppdrag i ett alltmer komplext samhälle. Utredningen *Polis i framtiden – polisutbildningen som högskoleutbildning* (SOU 2016:39) redovisades i maj 2016. Ett av utredningens förslag är att den nuvarande grundutbildningen till polisman ska omformas till en högskoleutbildning, motsvarande tre års heltidsstudier (180 högskolepoäng) som ska leda till en yrkesexamen som ska benämnas polisexamen.

I det förändringsarbete som pågår för närvarande avseende polisens grundutbildning anser Brå att it-aspekten bör lyftas fram som en central del. It-relaterad brottslighet bör utgöra en fristående kurs på polisens grundutbildning, men också integreras i kurser som rör andra ämnen på grundnivå. Att it-aspekten på ett bättre sätt integreras i grundutbildningen innebär att kunskapen når fram till samtliga poliser, oavsett vilken typ av tjänst de senare får. Att bättre integrera it-aspekten i polisens grundutbild-

ning har också lyfts fram som ett viktigt utvecklingsområde i Brås intervjuer med polisiära förundersökningsledare, i enkätens fritextsvar samt i Polismyndighetens egna rapporter på området (se t.ex. Polishögskolan 2014b).

Enligt polisens HR-avdelning har lärosätena som bedriver Polisprogrammet gjort vissa förändringar, men utvecklingsarbetet måste fortsätta, inte minst kopplat till den examensbeskrivning som nu tas fram inom polisutbildningsutredningen.[94]

Behov av utbildningssatsningar för personer inom polisens kärnverksamhet

En annan viktig åtgärd för att höja kompetensen om it-relaterade brott är kompetenssatsningar som riktar sig till poliser som redan arbetar inom myndigheten. Fram till nyligen har det dock inte erbjudits några centrala utbildningssatsningar på it-området för personer som arbetar inom polisens kärnverksamhet. Sedan år 2014 erbjuds kursen ”It-forensisk översiktskurs för förundersökningsledare” och en liknande kurs för utredare (6 respektive 1 procent av förundersökningsledarna som besvarat Brås enkät uppger sig ha gått någon av dessa kurser).[95] Det saknas dock fortfarande vidareutbildningskurser som specifikt berör it-relaterade brott för övriga funktioner inom polisens kärnverksamhet, till exempel poliser i yttre tjänst och polisens anmälningsmottagare. It-aspekten är heller inte särskilt integrerad i de vidareutbildningskurser som ges i andra ämnen, mer än något enstaka moment i vissa kurser, till exempel i basutbildningen till utredare av bedrägeribrott samt i utbildningen till ungdomsbrottsutredare. Flera av Brås intervjupersoner anser att it-relaterade brott får alldeles för lite utrymme vid den nationella utbildningen till förundersökningsledare och att it-relaterade brott borde utgöra en egen kurs.[96]

Brå anser att det finns ett stort behov av utbildningssatsningar för all personal inom Polismyndighetens kärnverksamhet (t.ex. förundersökningsledare, utredare och anmälningsmottagare). När det gäller redan befintliga vidareutbildningar som ges i Polismyndighetens regi bör dessa ses över, för att se hur it-relaterade brott

---

[94] Vid Södertörns högskola har det i kursplanen för hösten 2017 införts en kurs, där ett av momenten avhandlar olika varianter av it-relaterad brottslighet, särskilda problem under brottsutredningen, vanligt förekommande sociala medier, initiala och brottsutredande åtgärder för dessa brottstyper m.m.

[95] Dessutom erbjuds en kurs som riktar sig till personal som arbetar med inhämtningsarbete på internet *(”Underrättelse- och inhämtningsarbete på Internet, baskurs”)* som 1 procent av de förundersökningsledare som besvarade Brås enkät har gått (se bilaga 5).

[96] Enligt Polismyndighetens kursbeskrivning avseende nationell förundersökningsledarutbildning så utgör it-relaterade brott inte någon egen kurs i dagsläget men ämnet ”Utredning och bevissäkring i digital miljö” återfinns under utbildningens block 2.

kan integreras på ett lämpligt sätt. Det bör till exempel övervägas att utöka antalet utbildningstimmar kopplade till utredningsåtgärder i digital miljö i utbildningen till förundersökningsledare.

När det gäller nya utbildningar och kurser anser Brå att man bör genomföra en central satsning på utbildning som syftar till att höja grundkompetensen om it-relaterade brott för poliser inom kärnverksamheten. Det behöver även tas fram mer avancerade utbildningar för personer som utifrån sina arbetsuppgifter har ett mer uttalat behov av it-kompetens, till exempel it-brottsutredare, personer som arbetar inom underrättelseverksamheten, internetspanare (det vill säga en utbildning på ”specialistnivå”).

Den Nationella operativa avdelningen (Noa) har i den nya polisorganisationen fått ett processansvar för utredningsprocessen rörande komplex it-brottslighet, internetrelaterade sexuella övergrepp mot barn och it-relaterad brottslighet. Inom ramen för detta processansvar pågår ett omfattade arbete för att höja kompetensen om it-relaterade brott inom myndigheten, bland annat genom att ta fram ett omfattande utbildningspaket, vilket beskrivs närmare nedan.

Omfattande utbildningspaket för polisens kärnverksamhet

Under 2016 har Noa tillsammans med polisens HR-avdelning och it-avdelning påbörjat ett arbete med att ta fram en omfattande utbildningssatsning, i form av ett baspaket för personer som är verksamma inom Polismyndighetens kärnverksamhet. Utbildningen avser att vara webbaserad (s.k. e-learningutbildning) och ges via polisens intranät Intrapolis.[97] Utbildningen förväntas leda till att samtliga poliser ska få en bättre förståelse för brott med it-inslag och vilka utredningsåtgärder som är möjliga i dessa ärenden. Enligt företrädare från Noa bör samtliga poliser exempelvis känna till vad en IP-adress är och hur den kan användas i en brottsutredning samt känna till viktiga begrepp som ”nickname”, ”avatar” och ”molntjänst”. Baspaketet kommer även att innehålla information om hur man går tillväga för att säkra bevis i ärenden med it-inslag, till exempel vikten av att informera målsäganden om att ta en skärmdump, hur kontakt tas med externa aktörer utomlands, hur man går tillväga för att begära en frysning av information på internet etc. Kursen kommer även att innehålla information om de rättsliga möjligheterna att säkra olika typer av digitala spår.

[97] Förslaget om att ta fram en interaktiv e-learningutbildning lyftes redan i Polisens årsredovisning för 2014 (Polismyndigheten 2015b), men det har ännu inte genomförts.

Enligt företrädare från Noa och Polisens HR-avdelning föreslås att utbildningen ska vara obligatorisk för personer som är verksamma inom Polismyndighetens kärnverksamhet (t.ex. förundersökningsledare, utredare, poliser i yttre tjänst och receptionspersonal). Den grundläggande basutbildningen förväntas leda till att kunskaperna om it-relaterade brott höjs avsevärt inom myndigheten.

Den planerade utbildningssatsningen kommer även att ge möjligheter till mer fördjupade kunskaper på it-området. E-learningutbildningen ska enligt planerna vara uppbyggd i olika steg som man successivt bygger på.[98] Enligt företrädare från Noa kommer det att krävas att personen är godkänd på föregående nivå för att kunna ta sig vidare till nästa nivå. De menar att det i framtiden kommer att krävas olika slags kompetensnivåer för olika tjänster inom polisen. En polis som söker en ny tjänst inom myndigheten kan automatiskt komma att behöva genomgå en viss utbildning för att över huvud taget kunna få påbörja sina nya arbetsuppgifter. Enligt Noa är den planerade utbildningsmodellen effektiv, då den kan genomföras i egen takt, och it-kunniga personer kommer att ges en möjlighet att ”tenta av” kurser i snabb takt, medan andra kommer att behöva längre tid för att bli godkända. Dessutom är den behovsanpassad och utgår från personens arbetsuppgifter och de kompetenskrav som kommer att ställas för de just de uppgifterna.

Brå anser att det är positivt att Polismyndigheten planerar för en omfattande satsning för att höja baskunskapen om it-relaterade brott bland myndighetens anställda. Fördelen med en sådan satsning är att utbildningen når fram till samtliga poliser, oavsett vilken tjänst de har. Det är angeläget att tid och resurser avsätts så att utbildningen kan tas fram och att den kan påbörjas inom en snar framtid.[99] Brå vill dock poängtera att den planerade utbildningsinsatsen per automatik kräver en viss förkunskap hos de poliser som ska genomföra utbildningen, då den är webbaserad. Inom regionerna bör det säkerställas att samtliga poliser kommer att ges tid och möjlighet att genomföra kursen. Brå anser att det också bör tillförsäkras att stöd erbjuds för de individer där it-kunskapen är allra lägst.

Behov av utbildningsinsatser för it-undersökare

Brå bedömer att det även finns ett behov av kompetensutveckling bland Polismyndighetens it-undersökare, det vill säga de personer

[98] De fördjupade utbildningarna kommer troligtvis att ske genom föreläsningstillfällen, och de mest specialiserade utbildningarna kan eventuellt komma att ske i samarbete med t.ex. CPOL på Europol eller Interpol.

[99] Det bör noteras att samtliga tre kurser som startade år 2014 om it-relaterade brott inte finns med i 2017 års utbildningskatalog för polisanställda, på grund av den planerade e-learningutbildningen.

som ska utgöra myndighetens spetskompetens på it-området. Resultatet från Brås enkät visar att nästan samtliga (97 procent) av it-undersökarna även själva bedömer att de, utifrån sina arbetsuppgifter, har ett stort eller mycket stort behov av kompetensutveckling kring minst en av de utredningsåtgärder som Brå frågar om i enkäten. Behovet av kompetensutveckling rör både tekniska, juridiska och polisoperativa delar av arbetet.

Nationellt forensiskt centrums (NFC) processansvar för den it-forensiska verksamheten i Sverige innebär att NFC har getts i uppdrag att utforma den forensiska processen, där behovet av kompetensutveckling är en del. På NFC pågår just nu ett omfattande arbete som handlar om att säkerställa att it-undersökarna har tillräckligt god kompetens för att kunna utföra sina arbetsuppgifter på ett effektivt och rättssäkert sätt. Även på Noa pågår ett omfattande arbete för att höja it-kompetensen inom myndigheten, inom ramen för deras processansvar för komplex it-brottslighet och internetrelaterade sexualbrott mot barn. År 2016 påbörjades exempelvis en kunskapsinventering för att se vilken förmåga landets regioner har när det gäller utredningar av de brott som ryms inom processansvaret. Kunskapsinventeringen syftar till att undersöka vilken kompetens som finns i regionerna och om det finns behov av kompetenshöjande åtgärder eller nyrekryteringar.

Säkerställ att samtliga it-undersökare har en grundläggande utbildning på it-området

För att säkerställa att it-undersökarna har en god kompetens på it-området är det nödvändigt att de har en adekvat grundutbildning. Som nämnts tidigare i rapporten finns det flera sätt att utbilda sig till it-undersökare. Majoriteten av it-undersökarna inom polisen är civilanställda, och deras grundutbildning utgörs i regel av en högskole- eller universitetsexamen på it-området. Resterande it-undersökare har en polisiär bakgrund, vilket innebär att deras grundutbildning utgörs av Polisprogrammet. Efter sin examen till polis genomgår de någon av polisens vidareutbildningar inom it-forensik (Etapp 1 eller 2). Resultatet från Brås enkät visar att de flesta av it-undersökarna har en gedigen utbildning på it-området, det vill säga att de antingen har erhållit en akademisk examen på it-området och/eller att de har genomgått någon av Polismyndighetens vidareutbildningar inom it-forensik.

Samtidigt visar resultatet att 12 procent av it-undersökarna varken har gått någon universitets- eller högskolekurs eller någon av de fördjupade utbildningar inom it-forensik som ges i polisens regi. De har heller inte gått någon ”annan relevant vidareutbildning” i polisens regi. Dessa it-undersökare arbetar i första hand

med mobila enheter eller bild, film och ljud. Enligt Brås intervjupersoner ställs i dagsläget inga utbildningskrav på de personer som arbetar som it-undersökare. Flera menar att det är angeläget att krav på utbildning införs, inte minst ur ett rättssäkerhetsperspektiv.

Figur 14. Nuvarande utbildningar på it-området för it-undersökare på grund-, fort- och vidareutbildningsnivå, identifierade behov av kompetenshöjande åtgärder samt pågående arbete.

	Grundutbildning	Fort- och vidareutbildning
Nuvarande utbildningar	**Polisprogrammet:** Ingen enskild kurs om it-relaterade brott **Övriga utbildningar:** Högskole- eller universitetsutbildning på it-området	**Kurser:** *It-forensiker grundutbildning etapp 1 och 2* (58 dagar/20 dagar) *Underrättelse- och inhämtningsarbete på internet* (10 dagar) Cirka 15 kurser om olika digitala verktyg
Behov	Samtliga it-undersökare bör ha en adekvat utbildning Polisens it-forensiska utbildningar behöver moderniseras	Fort- och vidareutbildningsinsatser för it-undersökare utifrån deras arbetsområde och utbildningsbakgrund Löpande fortbildning om olika digitala verktyg, programvaror etc.
Pågående arbete	NFC har ett pågående arbete med att modernisera utbildningarna	NFC har ett pågående arbete med att se över fort- och vidareutbildningsutbudet för it-undersökare Noa genomför en kunskapsinventering

Enligt en rapport från Polishögskolan (2014b) finns det ett relativt stort antal personer inom myndigheten som uteslutande arbetar med undersökning och bevissäkring från mobila enheter (företrädesvis mobiltelefoner). Eftersom den lokala arbetsledningen många gånger inte anser att dessa personer är sysselsatta med någon egentlig it-forensisk undersökning anser man heller inte att personen behöver genomgå någon it-forensisk utbildning. Enligt rapporten medför det att dessa personer genomför undersökning och bevissäkring med system vilkas egentliga funktioner man inte själv behärskar. Till viss del finns samma förhållande beträffande it-undersökare som arbetar med bevissäkring från övervakningskameror och annan digital media som ljud och bild. De nuvaran-

de förhållandena anses vara rättsosäkra, och det framkommer att det finns ett behov av utbildningar som är nischade mot mobila enheter och bild/film och ljud.

Brå anser det är angeläget att Polismyndigheten säkerställer att it-undersökarna har en grundläggande utbildningsnivå som är anpassad efter deras arbetsområde, till exempel att personerna behärskar de arbetsverktyg som ska användas i arbetet. Det är vidare positivt att både Noa och NFC har ett pågående arbete för att säkerställa att it-undersökarna har den grundläggande utbildning som krävs för deras arbete.

En modern och flexibel utbildning för it-undersökare

Förutom att det bör säkerställas att samtliga it-undersökare har en grundläggande utbildning på it-området kan det även finnas behov att modernisera den it-forensiska vidareutbildning som ges i Polismyndighetens regi. I Polishögskolans genomlysning av polisens utbildningar (2014b) framkom att båda de it-forensiska vidareutbildningarna (Etapp 1 och Etapp 2) har ett behov av att nutidsanpassas efter de förändringar som har skett inom it-forensiken under de senaste åren. Allt fler it-undersökare arbetar i dag huvudsakligen inom ett eller några få ämnesområden, jämfört med tidigare då fler var ”generalister”. Den it-forensiska grundutbildningen bör därför vara flexibel och anpassas när det gäller innehåll. Det finns bland annat ett behov av att göra kurserna ”smalare” men ”djupare” inom respektive tekniskt delområde.

Inom NFC pågår för närvarande ett arbete med att modernisera de aktuella utbildningarna. Enligt NFC kommer båda utbildningarna på sikt att ersättas med nya utbildningar.[100] Bland annat finns det ett behov av att bygga upp expertkompetens inom särskilda it-forensiska arbetsområden. Brå ställer sig positivt till det arbete som pågår med att modernisera grundutbildningen till it-undersökare.

Kontinuerlig fort- och vidareutbildning för it-undersökarna

Polismyndighetens it-undersökare förväntas utgöra myndighetens spetskompetens på it-området. Såväl i intervjuer med åklagare och polisiära förundersökningsledare som i enkätens fritextsvar, framkommer att det finns höga förväntningar på it-undersökarnas kompetens och vad de ska kunna bistå med i utredningarna. I intervjuer med it-undersökare framkommer dock att många inte har fått någon fort- och vidareutbildning alls under den tid de

[100] År 2016 ersattes, enligt NFC, Polismyndighetens it-forensiska kurs ”Etapp 1” med en ny kurs, och det har även skett förändringar i ”Etapp 2”. Den senare kommer troligtvis att delas upp framöver för att ge mer utbildning inom respektive delområde.

har varit anställda inom Polismyndigheten. Flera upplever en stor frustration över att det saknas möjlighet till fort- och vidareutbildning och att de i dagsläget tvingas kompetensutveckla sig på sin fritid.

Om it-undersökarna ska bibehålla sin spetskompetens på it-området anser Brå det angeläget att de får kontinuerlig fort- och vidareutbildning för att deras kunskapsnivå ska kunna utvecklas i takt med den tekniska utvecklingen. Utbildningarna bör vara behovsanpassade utifrån it-undersökarnas arbetsområde och kunna innehålla såväl tekniska aspekter av arbetet som kunskaper om polisoperativt polisarbete och de lagar och regelverk som it-undersökare arbetar inom.

Enligt Nationellt forensiskt centrum (NFC) har det nationella kursutbudet för it-undersökare inom polisen varit ytterst begränsat under flera års tid. Vissa polismyndigheter har själva kompenserat för det, medan andra inte har gjort det. År 2016 har kursutbudet ökat och år 2017 kommer det att justeras ytterligare.

Behov av förstärkta juridiska och polisoperativa kunskaper hos civila it-undersökare

Förutom att fort- och vidareutbildningskurserna bör vara individanpassade utifrån it-undersökarens arbetsområde bör de anpassas efter it-undersökarens utbildningsbakgrund. It-undersökare som har en *civil bakgrund* bedömer sina tekniska kunskaper som högre än it-undersökare som har en polisiär bakgrund.[101] De civila it-undersökarna har emellertid lägre kunskaper än de polisiära it-undersökarna när det gäller polisoperativt arbete, som att biträda vid förhör och husrannsakan. Kunskapen bland de civila it-undersökarna är också lägre om en del rättsliga aspekter av arbetet.[102] Att it-undersökarna med civil bakgrund kan behöva förstärka sina juridiska kunskaper bekräftas av att var fjärde (26 procent) civil it-undersökare upplever att ”bristande kunskaper kring lagar och regelverk” är ett hinder för deras arbete. Motsvarande andel bland de polisiära it-undersökarna är endast 8 procent. It-undersökarna med en *polisiär bakgrund* bedömer i sin tur oftare att deras tekniska kunskaper är bristfälliga, jämfört med de civila it-undersökarna. Det bekräftas av att drygt var fjärde (26 procent) it-undersökare med en polisiär bakgrund upplever att en ”teknisk kunskapsbrist” är ett hinder för deras arbete (jämfört med 15 procent av de civila it-undersökarna). Resulta-

[101] Kunskapsnivån tycks till exempel vara högre när det gäller lösenord/kryptering, mobila enheter, programmering, it-forensiska analysverktyg, analysverktyg för internetinhämtning och ”live forensics”.

[102] Det gäller vilka rättsliga möjligheter det finns att säkra information som ligger öppen på internet och de rättsliga möjligheterna att säkra bevisning genom att använda hemliga tvångsmedel.

tet från Brås enkät visar att det således kan finnas ett behov av att förstärka de polisiära it-undersökarnas tekniska kompetens, medan de civila it-undersökarna kan ha ett större behov av att förstärka sina kunskaper om juridik och polisoperativt arbete, vilket även bekräftas av polisens egna rapporter (se t.ex. Polishögskolan 2014b).

Att de civila it-undersökarnas ”starka ben” är deras tekniska kompetens, medan deras ”svagare ben” är juridik och polisoperativt arbete lyfts även fram i Brås intervjuer med personer inom den it-forensiska verksamheten. Samtidigt betonas att it-undersökare ”behöver de båda benen för att stå stadigt i organisationen”. Enligt intervjuade it-forensiker bör Polismyndigheten därför ha en tydligare plan för att ta emot de civila medarbetarna på ett bra sätt och ge dem bättre förutsättningar för att integreras i den polisiära verksamheten, som många gånger är komplex och vitt skild från verksamhet på den civila marknaden.

Förbättra kunskaps- och kompetensspridningen

Utöver behovet av omfattande utbildningsinsatser ställer den ständiga förändringen avseende möjliga utredningsåtgärder och tekniska möjligheter på it-området krav på löpande kunskapsinhämtning. För den enskilde förundersökningsledaren och it-undersökaren saknas ofta tiden, och ibland även kunskapen, att själv söka efter ny information. Brås studie visar sammantaget att såväl åklagare och polisiära förundersökningsledare som it-undersökare i stor utsträckning efterfrågar en tydlighet kring vart man kan vända sig för att få stöd och hjälp. I dag sker mycket av arbetet mer eller mindre ostrukturerat, där den huvudsakliga strategin är att ”ringa runt”. Vanligt är att man använder sig av egna nätverk och kanaler, något som är helt avgörande för att få bra stöd, enligt flera respondenter.

Ett mer resurseffektivt sätt är att den kunskap som genereras inom rättsväsendet sammanställs centralt och kommuniceras via lämpliga kanaler. Inom rättsväsendet finns dessutom expertfunktioner dit man kan vända sig med olika it-relaterade frågor. De förväntade effekterna av ett förbättrat utredningsstöd och en tydlig samverkansstruktur är bättre förutsättningar för förundersökningsledaren att fatta rätt beslut och att de utredningsåtgärder som är möjliga vidtas. För it-undersökarna är de förväntade effekterna bättre förutsättningar att genomföra relevanta it-undersökningar. Nedan ges ett antal förslag på utvecklingsarbete som syftar till att förbättra kunskaps- och kompetensspridningen inom Åklagarmyndigheten och Polismyndigheten.

Ökat arbete med att tydliggöra och kommunicera vad den nationella strukturen kan bistå med

Det arbete som bedrivs vid Nationella operativa avdelningen (Noa) och vid Nationellt forensiskt centrum (NFC) är centrala för utredningsprocessen vid ärenden med it-inslag. Det gäller både det långsiktiga utvecklingsarbetet kring metodstöd, forskning och internationella samarbeten och det löpande stödet till utredningsprocessen.

Av Brås studie framgår att bland dem som vänt sig till Noa eller NFC är erfarenheterna från kontakterna goda. Poliser och åklagare upplever att de fått ett kompetent och bra bemötande. Dock finns det generellt en utbredd osäkerhet om vad den nationella strukturen kan bistå med i ärenden med it-inslag. Brås bedömning är att en viktig del i ombildningen av den nya Polismyndigheten och arbetet med den it-relaterade brottsligheten är att internt kommunicera var kompetensen finns inom myndigheten och i vilka ärenden man kan vända sig till de olika funktionerna.

Stärk och samla förmågan på regional nivå

I takt med det ökade behovet av it-forensiskt stöd i utredningsprocessen accentueras behovet av stärkt förmåga på regional nivå. Ett led i detta är det arbete som pågår avseende att inrätta regionala it-brottscentrum. Tanken med detta är att samla all regional it-forensisk kompetens under ett tak och därmed kunna ge samma stöd till hela regionen, oavsett organisatorisk tillhörighet. Att organisera det it-forensiska arbetet inom regionen på detta sätt menar företrädare skulle medföra ökad flexibilitet, samordningsvinster och en mer slagkraftig organisation. Brås intervjupersoner poängterar dock att olika regioner har olika förutsättningar och behov, till exempel varierar ärendeinflöde och geografiska avstånd mellan regionerna, och att man måste ta hänsyn till detta och ge utrymme för regionala lösningar.

Att vid respektive regionalt centrum inrätta en regional deskfunktion dit personal i regionen kan vända sig om de behöver vägledning i utredningsarbetet skulle möta det behov av stöd som respondenterna i Brås studie uttrycker. Inrättandet av regionala centrum skulle dessutom innebära att centrumen blir den naturliga kontaktytan mot nationellt it-brottscentrum som i sin tur är kontaktytan mot European Crime Center (EC3). På så vis skulle det finnas en tydlig kontaktyta för samverkan och informations- och kunskapsutbyte såväl nationellt som internationellt.

Driv på utvecklingsarbetet avseende Intrapolis

En viktig samverkansplattform för att samla kunskap på it-området är Intrapolis. I Brås arbete framkommer dock stark kritik mot Intrapolis. I huvudsak avser kritiken dålig struktur och navigering samt brist på innehåll. Polisens kommunikationsavdelning känner igen kritiken. Att Intrapolis bara funnits i sin nuvarande form i knappt två år och att det tar tid att lära sig ett nytt intranät beskrivs som en förklaring till kritiken. Det behövs därför göras satsningar på mer information och utbildning till användarna, menar man. Att det har saknats innehåll på intranätet förklaras delvis av att det i den organisationsförändring som polisen genomgår har varit svårt att hitta innehållsansvariga för olika områden. I och med det nya intranätet har man gått från en publiceringsorganisation där webbredaktörer publicerat det mesta av innehållet till en decentraliserad publiceringsorganisation där i stället chefer och sakkunniga i stor utsträckning ansvarar för innehållet.

Kommunikationsavdelningen uppger att man arbetar systematiskt och löpande med att förbättra struktur, navigering och innehåll. Brå ser det som helt centralt att Polismyndigheten även fortsatt avsätter resurser för att driva på utvecklingsarbetet. Ett fungerande intranät är inte bara en viktig fråga för kunskaps- och kompetensspridningen på it-området, utan för alla delar av Polismyndighetens arbete.

Ökad informationsspridning och fortsatt utvecklingsarbete inom Åklagarmyndigheten

Det utvecklingsarbete som pågår inom Åklagarmyndigheten och som syftar till att förbättra kunskaps- och kompetensspridningen bedöms vara en utveckling i rätt riktning och i enlighet med de önskemål som framkommit i Brås undersökning. Åklagarmyndighetens intranät Rånet beskrivs som lättnavigerat, och via Rånet kommer åklagarna åt den webbaserade guide, kallad FAQ, som sammanställts för att ge vägledning på it-området. Utmaningen för Åklagarmyndigheten är att sprida informationen om det utredningsstöd som finns att tillgå, samt att säkerställa en fortsatt förvaltning så att utredningsstödet hålls uppdaterat. Konkret handlar det om att tillförsäkra att det finns en utpekad resurs med tydligt ansvar för att kontinuerligt uppdatera Åklagarmyndighetens webbaserade guide. Det är också centralt att den som är ansvarig följer upp hur guiden används för att få svar på om den fyller sitt syfte. I nuläget finns möjlighet för användarna att kommentera guiden med hjälp av en kommentarsknapp. Åklagarmyndigheten har även tillgång till statistik över hur många som besökt de olika sidorna som guiden består av. Brå bedömer dock att en mer strukturerad uppföljning skulle ge bättre förut-

sättningar att höja kvaliteten på innehållet ytterligare och även ge underlag för att säkrare veta vem som använder sig av guiden i dag och därmed få reda på var informationsinsatser bör göras för att öka kännedomen om guidens existens.

Även avseende nätverket för it-kontaktåklagare betonar Brå vikten av att Åklagarmyndigheten säkerställer att det även fortsatt finns en resurs säkrad med ansvar för nätverkets fortlevnad, samt att informationsinsatser vidtas för att öka kännedomen om nätverkets existens. I Åklagarmyndighetens verksamhetsplan för 2016 (Åklagarmyndigheten 2015b) nämns en fortsatt utveckling av samverkan inom nätverket för it-åklagare som en del i arbetet med att utveckla förmågan att hantera it-relaterad brottslighet.

Effektivisera och tillför utredningsresurser

Den höga arbetsbelastningen som it-undersökarna i Brås studie ger uttryck för beror på en rad faktorer. Det handlar dels om otillräcklig bemanning i förhållande till inflöde, dels om att it-undersökarna på många sätt används ineffektivt. Att it-undersökarna är för få och att de delvis används felaktigt har konstaterats vid ett flertal tillfällen tidigare (se till exempel Genomförandekommittén för nya Polismyndigheten 2014b, Brå 2013:14, Brå 2015:6, Brå 2016:9, Åklagarmyndigheten 2015a, Rikspolisstyrelsen 2014). Nedan presenteras ett antal förslag på åtgärder för ett mer effektivt nyttjande av de it-forensiska resurserna.

Reglera inflödet och höj kvaliteten i beställningarna

En förklaring till den höga arbetsbelastningen är att inflödet av beställningar av it-undersökningar i stor utsträckning är oreglerat, både avseende antal och form. Med en hög kvalitet i beställningarna ökar kvaliteten i utredningar samtidigt som resurser frigörs från it-undersökarna. För att höja kvaliteten i beställningarna finns ett antal framgångsfaktorer och förslag på åtgärder.

Rutinerna för beslagshantering ser i dag olika ut i olika delar av Polismyndigheten. På vissa håll skickas till exempel beslagtagna mobiltelefoner för telefontömning i samma stund som beslaget görs av poliser i yttre tjänst. Brås bedömning är att det bör regleras vem som får göra en beställning. För att undvika det som beskrivs som slentrianmässiga beslag och beställningar av it-undersökningar, bör det ställas tydligare krav på att undersökningarna måste ha ett specificerat syfte.

För de personer som är behöriga att beställa en it-undersökning krävs en god beställarkompetens. God beställarkompetens utgår från en grundkompetens om vad som går att göra med olika enheter. Beställaren måste även ha förmågan att bedöma värdet

av it-undersökningen i relation till övriga utredningsåtgärder. Åklagare, polisiära förundersökningsledare och it-undersökare som Brå intervjuat betonar att beställningarnas kvalitet ökar i de fall som beställningen görs i dialog med it-undersökaren, något som även bekräftas av resultatet från enkäterna.

Vidare bör beställaren vara noga med att dra tillbaka sin beställning i de fall en undersökning av någon anledning inte längre är aktuell, och det måste finnas rutiner kring hur detta görs. För att öka kvaliteten i beställningarna finns det även åtgärder som it-undersökaren kan vidta. För att undvika att it-undersökningar genomförs i onödan kan it-undersökaren före påbörjad undersökning, i den utsträckning det är möjligt, kontakta beställaren för att säkerställa att undersökningen fortfarande är aktuell. It-undersökaren kan då även vid behov ställa följdfrågor i syfte att ytterligare precisera beställningen. I vissa större ärenden kan det även finnas anledning att löpande stämma av gentemot förundersökningen eftersom värdet av och syftet med undersökningen kan förändras under utredningens gång.

Renodla it-undersökarens roll

En konsekvens av eftersläpningar på utbildnings- och kompetensområdet för bland annat utredare och förundersökningsledare är att it-undersökarna många gånger används för arbetsuppgifter som de är överkvalificerade för. It-undersökarna utför i varierande utsträckning arbetsuppgifter som bör kunna hanteras av andra personer inom myndigheten, till exempel utredaren. För att effektivisera handläggningen av ärenden med it-inslag är Brås bedömning att det krävs att it-undersökarnas roll renodlas och tydliggörs i förhållande till övriga utredningsresurser (se till exempel Rikspolisstyrelsen 2014).

En arbetsuppgift som i varierande utsträckning faller på it-forensikerna är fingranskning av barnpornografiskt material. Då ärenden med barnpornografiskt material många gånger innebär stora mängder gods och data och därmed blir tidskrävande bedömer Brå att Polismyndigheten bör se över de förslag på åtgärder som beskrivs i Polisens *Förstudierapport för den forensiska verksamheten* (Polismyndigheten 2016b). Kortfattat handlar förslagen om att det bör finnas särskild personal med rätt egenskaper och utbildning för ändamålet, ett förslag som styrks i de intervjuer som Brå genomfört. Att skapa presentationer av den digitala bevisningen inför huvudförhandling är en annan arbetsuppgift som bör lyftas från it-forensikerna. Flera poliser och åklagare som Brå varit i kontakt med menar att ansvaret för uppgiften bör falla på Åklagarmyndigheten. Åklagarmyndigheten (2015a) signalerar att en förskjutning från polisen till Åklagarmyndigheten redan skett

och att personer med kompetens att göra presentationer i utredningar därmed behöver rekryteras.

Ge fler utbildning och behörighet att genomföra it-relaterade arbetsuppgifter

För att möta det ökade inflödet av beställningar och trycket på den it-forensiska processen behövs mer utredningsresurser. Brå bedömer att Polismyndigheten som ett led i detta även bör se över möjligheterna att i större utsträckning överlåta rutinmässiga och enklare it-undersökningar till andra funktioner än de it-forensiska. Varianter av detta tillämpas på olika håll redan i dag, bland annat genom framtagna produkter för mobiltömningar, så kallade kiosklösningar. Enligt intervjupersoner kan en sådan lösning motverka flaskhalsar och förkorta handläggningstiderna. För att försäkra att kvaliteten i undersökningarna bibehålls är det viktigt att handläggarna får den utbildning som krävs. Brå betonar att det bör vara reglerat så att de som ska utföra uppgiften först efter avslutad utbildning erhåller behörighet att genomföra arbetsuppgifterna.

Brås studie visar även att det saknas personal med kompetens att analysera den information som extraherats från olika it-media. It-undersökarna uttrycker en önskan om att kunna lämna ett mer färdigt material till utredaren, men att de på grund av tidsbrist ofta är hindrade från detta. Det säkrade materialet riskerar därmed att bli oanalyserat. De analysfunktioner som finns inom Polismyndigheten arbetar huvudsakligen enbart med grov brottslighet. Brås bedömning är att analysfasen måste tillföras resurser, till exempel genom att utredarens analyskompetens höjs och genom ett förbättrat it-stöd, se nedan.

It-undersökarens delaktighet i utredningen beskrivs som en framgångsfaktor

I linje med vad som presenterats i andra studier (se till exempel Brå 2015:6, Åklagarmyndigheten 2015a) framhåller flertalet poliser, åklagare och it-undersökare i Brås studie att en kontinuerlig dialog mellan den it-forensiska processen och utredningsprocessen är en framgångsfaktor för utredning av brott med it-inslag. Att it-undersökaren är delaktig i ett ärende innebär att hon eller han därmed har större möjligheter att avgöra vad som är relevant för utredningen. Detta leder i förlängningen till en mer effektiv it-forensisk process.

Det pågår en diskussion om hur nära en it-undersökare får vara utredningen, utan att dennes objektivitet påverkas (se till exempel Genomförandekommittén för den nya Polismyndigheten 2014b).

I prop. 2014/15:94 anges att ”i kravet på oberoende ligger att forensiska undersökningar, analyser och jämförelser hanteras helt separat från annat utredningsarbete under en förundersökning”. Brå anser att det behövs ett klargörande av hur texten ska tolkas och på vilket sätt en it-undersökare får bistå brottsutredningen.

Effektivitet förutsätter ett modernt it-stöd

Ett modernt it-stöd är en förutsättning för ett effektivt och rättssäkert utredningsarbete. I Brås studie framkommer att brist på teknisk utrustning och system utgör ett stort hinder för många åklagare, polisiära förundersökningsledare och it-undersökare. För att nå framgång i utvecklingsarbetet för att höja rättsväsendets förmåga att handlägga it-relaterade brott behövs stora it-satsningar.

It-satsningar är viktiga för att kunna genomföra olika kompetenshöjande åtgärder, till exempel för att kunna genomföra den planerade e-learningutbildningen för samtliga polisanställda och för att möjliggöra en bättre spridning av de erfarenheter och kunskaper som kontinuerligt genereras på it-området inom respektive myndighet.

It-satsningar behövs även för att säkerställa att det finns teknisk utrustning och programvara för att genomföra nödvändiga utredningsåtgärder och it-undersökningar. Som exempel kan nämnas att förslaget om att effektivisera den it-forensiska processen genom att vissa moment utförs av annan personal än it-undersökare inte bara förutsätter att den som ska genomföra de olika momenten har rätt utbildning och behörighet. Det är även helt centralt att personen har ett bra it-stöd i form av analysverktyg och programvaror.

Ett nationellt uppföljningsverktyg

Den tredje delen i regeringens uppdrag till Brå handlar om att överväga möjligheterna att utveckla ett system som ger rättsväsendets myndigheter ett statistiskt underlag för att framöver kunna följa utvecklingen av it-inslag i de anmälda brotten och i så fall föreslå hur systemet bör utformas. Resultatet från Brås analys presenteras i föregående kapitel.

Som beskrivs i kapitlet är Brås bedömning att Polismyndigheten bör skapa ett nationellt uppföljningssystem för den it-forensiska verksamheten. Systemet ska användas för att kunna ta fram ett statistiskt underlag för planering och styrning av verksamheten. Systemet ska även kunna användas som stöd i det it-forensiska arbetet, till exempel för att kunna ärendefördela mellan olika it-forensiska sektioner. Systemet ska även ha en koppling till andra

ärendehanteringssystem. Ansvaret för att utveckla systemet ligger inom ramen för NFC:s processansvar. NFC har i nuläget inte fattat något beslut om vilket ärendehanteringssystem som ska användas. I utvecklingsarbetet bedömer Brå att det är viktigt att det sker i dialog med Noa för att klargöra exakt hur behovet av statistikuppgifter ser ut och för att definiera centrala begrepp.

Rättsväsendet står inför stora utmaningar

Den it-relaterade brottsligheten ökar kontinuerligt, och enligt Brås intervjupersoner finns det it-inslag i de flesta typer av brott (”från klotter till mord”). Den snabba tekniska utvecklingen och det ökade internetanvändandet har haft stor inverkan på de brottsutredande myndigheternas arbete, och det ställs numera helt nya krav på kompetens och kapacitet för att kunna möta utvecklingen. Under de kommande åren förväntas efterfrågan på it-forensiskt stöd i förundersökningarna dessutom fortsätta att öka. Den snabba tekniska utvecklingen, där till exempel komplexa krypteringslösningar har börjat sprida sig till massmarknaden, kommer att ställa stora krav på kompetens, it-stöd och utrustning inom den it-forensiska verksamheten (Genomförandekommittén för nya Polismyndigheten 2014b).[103]

Enligt Brås intervjupersoner har den ökade förekomsten av it-relaterade brott och den bristande förmågan att utreda dessa brott varit allmänt kända inom rättsväsendet under många års tid. Flera upplever en stor frustration kring att det inte har skett några större satsningar för att öka rättsväsendets förmåga att hantera it-relaterad brottslighet. En viktig förklaring kan vara att den traditionella synen på ”it-brott” lever kvar hos många chefer och beslutsfattare och att brott med it-inslag fortfarande ses som något särskilt, som bör hanteras på särskilda enheter och av personer som har en särskild it-kompetens.

Brås bedömning är att de satsningar som hittills gjorts på it-området inte motsvarar behovet. Det utvecklingsarbete som pågår avseende såväl kompetens- som kapacitetshöjande åtgärder är ytterst angelägna för att tillförsäkra effektivitet och rättssäkerhet. Polismyndigheten och Åklagarmyndigheten måste tillsätta de resurser som krävs för att de planerade åtgärderna ska kunna genomföras. Det är även viktigt att de åtgärder som görs inte blir en engångssatsning, utan att satsningarna på it-området fortlöper och uppdateras i takt med utvecklingen.

---

[103] Enligt NFC väntas merparten av all data på smarta telefoner, surfplattor och datorer vara krypterad inom några år. För att kunna hantera avancerat it-stöd kommer det bland annat behöva anställas fler it-specialister med rätt kompetens, vilka måste rekryteras i konkurrens med andra myndigheter och näringsliv som ofta erbjuder avsevärt högre lön än polisen (Genomförandekommittén för nya Polismyndigheten 2014b).

Referenser

Bartlett, J., Crump, J., Middleton, L. och Miller, C. (2013). *Policing in an information age*. London: Demos.

Brottsförebyggande rådet, Brå (2000). *It-relaterad brottslighet*. Rapport 2000:2. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2002). *Strukturerad information om brott. STUK. Ett nytt sätt att koda brott*. Slutrapport. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2012). *Användningen av brottskoder. En kvalitetsstudie inom kriminalstatistiken. Kvalitetsstudie 1*. Stockholm: Brottsförbyggande rådet.

Brottsförebyggande rådet, Brå (2013). *Bestämmelsen om kontakt med barn i sexuellt syfte*. Rapport 2013:14. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2015). *Polisanmälda hot och kränkningar mot enskilda personer via internet*. Rapport 2015:6. Stockholm: Brottsförbyggande rådet.

Brottsförebyggande rådet, Brå (2015). *Kriminalstatistik 2014*. Rapport 2015:16. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2015a). *Klassificering av brott. Anvisningar och regler.* Version 4.1. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2016). *Nationella trygghets-undersökningen 2015. Om utsatthet, otrygghet och förtroende*. Rapport 2016:1. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2016). *Nationella trygghets-undersökningen 2015 - Teknisk rapport. Rapport* 2016:3. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2016). *Bedrägeribrottsligheten i Sverige. Kartläggning och åtgärdsförslag*. Rapport 2016:9. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2016a). *Analys av böter*. Kortanalys. Under produktion. Stockholm: Brottsförebyggande rådet.

Brunty, J. och Helenek, K. (2013). *Social Media Investigation for Law Enforcement*. New York: Routledge, Taylor & Francis.

Bälter Nordenman, T. (2016). *Nätbrottsligheten kräver nya verktyg*. Karnov group. http://www.karnovgroup.se/om-oss/kunskap-och-reflektioner/natbrottsligheten-kraver-nya-verktyg. (Hämtad 2016-08-23).

Dir. 2016:20. *Moderna regler om beslag och husrannsakan*. Stockholm: Justitiedepartementet.

Dir. 2016:36. *Hemlig dataavläsning*. Stockholm: Justitiedepartementet.

Findahl, O. och Davidsson, P. (2015). *Svenskarna och internet 2015*. Stockholm: Stiftelsen för Internetinfrastruktur.

Forensiska rådet, FOR (2011). *Kompetensprofiler för olika IT-forensiska roller i brottsutredningar*. Samordningsgruppen Digitala medier.

Genomförandekommittén för nya Polismyndigheten (2014a). *Beslut om huvuddragen i den nya Polismyndighetens detaljorganisation*. Datum 2014-05-14. Stockholm: Statens offentliga utredningar.

Genomförandekommittén för nya Polismyndigheten (2014b). *OP-16 It-forensik*. Slutrapport. Datum 2014-12-18. Stockholm: Statens offentliga utredningar.

Holt, T.J., Bossler, A.M. och Seigfried-Spellar, K.C. (2015). *Cybercrime and digital forensics. An introduction*. New York: Routledge.

Justitiedepartementet (2014). *En digitalt sammanlänkad rättskedja*. Stockholm: Justitiedepartementet, Regeringskansliet.

Kronqvist, S. (2013). *Brott och digitala bevis: En handledning*. Stockholm: Norstedts Juridik.

McGuire, M. och Dowling, S. (2013). *Cyber crime: A review of the evidence*. Home Office Research Report 75. Home Office.

Mehta, C.R. och Patel, N.R. (2011). *IBM SPSS Exact Tests*. IBM Corp.

Nationalencyklopedin, smartmobil. http://www.ne.se/uppslagsverk/encyklopedi/lång/smartmobil (hämtad 2016-08-25)

Polishögskolan (2014a). *Delrapport. Struktur för Polisens vidareutbildningar*. Dnr A413.136/2014. Datum 2014-10-07.

Polishögskolan (2014b). *Översyn av Polisens utbildningar i syfte att i högre grad beakta it-brottsperspektivet*. Version 01.00. Datum 2014-11-10.

Polismyndigheten (2015a). *Polismyndighetens it-strategi 2015-2017*. PM 2015:212, Saknummer 170. Datum 2015-01-01. Polismyndigheten.

Polismyndigheten (2015b). *Polisens Årsredovisning 2014*. Dnr: A001.274/2014, saknummer 902. Datum 2015-02-20. Stockholm: Polismyndigheten.

Polismyndigheten (2015c). *Beslut avseende inrättande av ett nationellt IT-brottscentrum*. Dnr: A134.986/2015, Noa 39/15, saknummer 121. Datum 2015-04-21. Polismyndigheten.

Polismyndigheten (2015d). *Projektdirektiv för harmonisering av it-forensik*. Projektdirektiv Datum 2015-11-04. Polismyndigheten.

Polismyndigheten (2015e). *Polismyndighetens budgetunderlag 2017–2019*. Dnr A383.968/2015, saknummer 979. Stockholm: Ekonomiavdelningen, Polismyndigheten.

Polismyndigheten (2016a). *Arbetsordningen för Polismyndigheten*. PM 2016:01, A145.527/2015, saknummer 127. Datum 2016-02-02. Polismyndigheten.

Polismyndigheten (2016b). *Förstudierapport för den forensiska processen*. Dnr. A354.673/2015, saknummer 169. Datum 2016-05-18. Polismyndigheten.

Polismyndigheten (2016c) *Nationella operativa avdelningens handläggningsordning*. Noa 2016:148 Saknummer 127. Datum 2016-06-30. Polismyndigheten.

Prop. 2014/15:94. *Den nya polisorganisationen – några frågor om personuppgiftsbehandling m.m*. Stockholm: Justitiedepartementet.

Rikspolisstyrelsen (2012). *Modell för kompetensutveckling och förvaltning för olika IT-forensiska roller i brottsutredningar*. Slutrapport. Arbetsgruppen Kompetensutveckling för Digitala medier. Version 01.00, Datum: 2012-03-22.

Rikspolisstyrelsen (2013). *Förstudierapport, polisens brottsbekämpande verksamhet, brott med it-relevans*. Diarienummer PoA480-5583/11. Datum: 2013-02-04.

Rikspolisstyrelsen (2014). *Tillsynsrapport 2014:2. Inspektion av polismyndigheternas förmåga att handlägga IT-brott*. Stockholm: Rikspolisstyrelsen.

Riksrevisionen (2015). *It-relaterad brottslighet – polis och åklagare kan bli effektivare*. RiR 2015:21. Stockholm: Riksrevisionen.

Savona, E. U. (1998). *The organisational framework of european crime in the globalisation process*. Transcrime working paper.

SOU (2007). *Framtidens polis*. Delbetänkande av Utredningen om den framtida polisutbildningen. SOU 2007:39. Stockholm: Statens offentliga utredningar.

SOU (2013). *Europarådets konvention om it-relaterad brottslighet*. Betänkande av Utredningen om it-brottskonventionen. 2013:39. Stockholm: Statens offentliga utredningar.

SOU (2015). *Datalagring och integritet*. Betänkande av Datalagringsutredningen. SOU 2015:31. Stockholm: Statens offentliga utredningar.

SOU (2016). *Polis i framtiden – polisutbildningen som högskoleutbildning*. Betänkande av Polisutbildningsutredningen. SOU 2016:39. Stockholm: Statens offentliga utredningar.

Wall, D.S. och Williams, M.L. (2013). *Policing cybercrime: networked and social media technologies and the challenges for policing. Policing and Society* 23 (4), s. 409–412.

Williams, M. och Levi, M. (2015). *Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors*. Security Journal 28 (3), s.252–271.

Åklagarmyndigheten (2013). *Beslag – en handbok*. Utvecklingscentrum Malmö.

Åklagarmyndigheten (2014). *Budgetunderlag 2015–2017*. Dnr ÅM-A 2014/0271 Stockholm: Åklagarmyndigheten.

Åklagarmyndigheten (2015a). *Trygghet på internet. En inventering av it-rättsliga frågor där internet är brottsplats eller brottsverktyg*. Stockholm: Utvecklingscentrum.

Åklagarmyndigheten (2015b). *Verksamhetsplan 2016*. Dnr ÅM-A 2015/1756. Stockholm: Ekonomiavdelningen, Åklagarmyndigheten.

Bilagor

Bilaga 1. Tabeller

Tabell 1B. Andel brott inom olika brottstyper där det framgår it-inslag enligt urvalet av brottsanmälningar år 2006, 2010 och 2014. Procent.

		2006	2010	2014	Sig.
Brott mot person		(n = 226)	(n = 228)	(n = 216)	
	It är målet	0	2,2	4,6	
	It är medlet	8,8	12,3	15,7	
	It har annan beröring	1,8	5,3	5,6	***
	Totalt: Mål/medel/beröring	10,6	19,7	25,9	***
Bedrägeri m.m.		(n = 230)	(n = 227)	(n = 228)	
	It är målet	0	0,9	4,4	
	It är medlet	37	49,8	56,1	
	It har annan beröring	3,5	11,0	10,1	***
	Totalt: Mål/medel/beröring	40,4	61,7	70,6	***
Narkotikabrott		(n = 193)	(n = 172)	(n = 226)	
	It är målet	0	0	0	
	It är medlet	0	0	0	
	It har annan beröring	0	1,7	4,0	*
	Totalt: Mål/medel/beröring	0	1,7	4,0	*
Tillgreppsbrott		(n = 228)	(n = 224)	(n = 225)	
	It är målet	0	0	0	
	It är medlet	0	0	0	
	It har annan beröring	3,9	5,8	8,9	(*)
	Totalt: Mål/medel/beröring	3,9	5,8	8,9	(*)
Skadegörelse		(n = 220)	(n = 228)	(n = 230)	
	It är målet	0	0	0	
	It är medlet	0	0	0	
	It har annan beröring	0,9	0,9	4,8	**
	Totalt: Mål/medel/beröring	0,9	0,9	4,8	**
Övriga brott (exklusive trafikbrott)		(n = 207)	(n = 205)	(n = 218)	
	It är målet	0,5	0,5	0,5	
	It är medlet	7,7	5,4	3,2	
	It har annan beröring	4,3	7,3	10,1	
	Totalt: Mål/medel/beröring	12,6	13,2	13,8	

*** $p < 0{,}001$ ** $p < 0{,}01$ * $p < 0{,}05$ (*) $p < 0{,}10$, tvåsidigt Chi-två test (Exact test).

Tabell 2B. Kunskapen om möjligheten att genomföra olika utredningsåtgärder i digital miljö. Andelen it-forensiker respektive övriga it-undersökare som uppger att deras kunskapsnivå är god/mycket god respektive bristfällig/mycket bristfällig. Procent.

	Goda/mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Möjligheten att spåra potentiella gärningspersoner via IP-adress		
It-forensiker (n = 83)	90	10
Övriga it-undersökare (n = 43)	63	37
Möjligheten att få ut information från externa aktörer utomlands om vem som har registrerat en viss tjänst eller vilka IP-adresser som har använt tjänsten den senaste tiden (IP-loggar)		
It-forensiker (n = 83)	68	33
Övriga it-undersökare (n = 42)	43	57
Rättsliga möjligheter att ta del av elektroniska meddelanden som ligger på en mobiltelefons/dators lagringsminne		
It-forensiker (n = 85)	95	5
Övriga it-undersökare (n = 44)	75	25
Rättsliga möjligheter att säkra bevisning genom avlyssning eller övervakning av elektronisk kommunikation (HAK eller HÖK)		
It-forensiker (n = 81)	22	78
Övriga it-undersökare (n = 44)	30	71
Rättsliga möjligheter att ta del av elektroniska meddelanden som ligger utanför en dators eller mobiltelefons lagringsminne (t.ex. på ett e-postkonto, Facebook eller annan plats på internet)		
It-forensiker (n = 85)	68	32
Övriga it-undersökare (n = 43)	54	47
Kunskaper om tillvägagångssättet att begära en ”frysning” för att förhindra att digital information försvinner		
It-forensiker (n = 81)	47	53
Övriga it-undersökare (n = 43)	30	70
Kunskaper om vilka rättsliga möjligheter det finns att säkra information som ligger öppen på internet		
It-forensiker (n = 85)	55	45
Övriga it-undersökare (n = 43)	47	54

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

Tabell 3B. Respondenternas behov av kompetensutveckling kring möjliga utredningsåtgärder i digital miljö. Andel personer inom respektive yrkesgrupp som uppger att de, utifrån sina arbetsuppgifter, har ett *stort eller mycket stort behov* av kompetensutveckling avseende olika utredningsåtgärder i digital miljö. Procent.

	Åklagare (n = 364-382)	Polisiära förundersökningsledare (n = 644-658)	It-undersökare (n = 122-127)
Spårning av gärningspersoner i digital miljö			
Möjligheten att spåra potentiella gärningspersoner via IP-adress	58	63	32
Möjligheten att få ut information från externa aktörer utomlands om vem som har registrerat en viss tjänst eller vilka IP-adresser som använt tjänsten den senaste tiden (IP-loggar)	67	62	41
Kunskaper om att skriva en rättshjälpsbegäran för att få ut uppgifter från externa aktörer utomlands	61	-	-
Möjligheter att säkra digitala bevis			
Möjligheter att ta del av elektroniska meddelanden som ligger på en mobiltelefons/dators lagringsminne	35	50	28
Möjligheter att säkra bevisning genom avlyssning och övervakning av elektronisk kommunikation (HAK eller HÖK)	39	47	46
Möjligheter att ta del av elektroniska meddelanden som ligger utanför en mobiltelefons/dators lagringsminne (t.ex. på ett e-postkonto, Facebook eller annan plats på internet).	68	66	50
Kunskaper om tillvägagångssättet för att begära en ”frysning” av uppgifter för att förhindra att digital information försvinner	67	67	45
Kunskaper om vilka rättsliga möjligheter det finns att säkra information som ligger öppen på internet	66	68	49

Tabell 4B. It-undersökarnas tekniska kunskaper. Andelen it-forensiker respektive övriga it-undersökare som uppger att deras kunskapsnivå är god/mycket god respektive bristfällig/mycket bristfällig. Procent.

	Goda/ mkt goda kunskaper	Bristfälliga/mkt bristfälliga kunskaper
Lösenord/kryptering		
It-forensiker (n = 84)	55	45
Övriga it-undersökare (n = 46)	37	63
Mobila enheter (t.ex. mobiltelefon, läsplatta, GPS)		
It-forensiker (n = 85)	87	13
Övriga it-undersökare (n = 47)	75	26
Bild/film/ljud		
It-forensiker (n = 84)	68	32
Övriga it-undersökare (n = 46)	67	33
Elektronik		
It-forensiker (n = 84)	31	69
Övriga it-undersökare (n = 47)	45	55
Programmering/programmeringsspråk		
It-forensiker (n = 84)	27	73
Övriga it-undersökare (n = 47)	19	81
It-forensiska analysverktyg		
It-forensiker (n = 85)	91	9
Övriga it-undersökare (n = 47)	30	70
Analysverktyg, internetinhämtning		
It-forensiker (n = 83)	41	59
Övriga it-undersökare (n = 43)	26	74
Biträda vid förhör		
It-forensiker (n = 83)	57	43
Övriga it-undersökare (n = 46)	57	44
Biträda vid husrannsakan		
It-forensiker (n = 85)	86	14
Övriga it-undersökare (n = 46)	70	30
”Live forensics”		
It-forensiker (n = 84)	68	32
Övriga it-undersökare (n = 35)	14	86

Not: På grund av avrundningar överstiger vissa procentsummor 100 procent.

Tabell 5B. It-undersökarnas behov av kompetensutveckling kring tekniska aspekter av arbetet. Andel it-undersökare som uppger att de, utifrån sina arbetsuppgifter, har ett *stort eller mycket stort* behov av kompetensutveckling. Procent.

	Mycket stort/ stort behov
Lösenord/kryptering	
It-forensiker (n = 84)	73
Övriga it-undersökare (n = 45)	53
Mobila enheter (t.ex. mobiltelefon, läsplatta, GPS)	
It-forensiker (n = 84)	57
Övriga it-undersökare (n = 45)	53
Bild/film/ljud	
It-forensiker (n = 85)	45
Övriga it-undersökare (n = 45)	71
Elektronik	
It-forensiker (n = 84)	46
Övriga it-undersökare (n = 45)	51
Programmering/programmeringsspråk	
It-forensiker (n = 84)	55
Övriga it-undersökare (n = 44)	43
It-forensiska analysverktyg	
It-forensiker (n = 85)	64
Övriga it-undersökare (n = 45)	53
Analysverktyg, internetinhämtning	
It-forensiker (n = 85)	52
Övriga it-undersökare (n = 42)	55
Biträda vid förhör	
It-forensiker (n = 84)	46
Övriga it-undersökare (n = 43)	23
Biträda vid husrannsakan	
It-forensiker (n = 84)	32
Övriga it-undersökare (n = 44)	32
”Live forensics”	
It-forensiker (n = 82)	68
Övriga it-undersökare (n = 36)	53

Tabell 6B. Andelen som mycket ofta/ofta respektive ibland/sällan/aldrig uppger att en it-undersökare är delaktig vid olika moment i en förundersökning gällande brott med it-relevans. Procent.

	Mycket ofta/ofta	Sällan, aldrig/ mycket sällan	Vet ej
Arbetsmöten under förundersökning			
Åklagare (n = 383)	19	68	13
Polisiära förundersökningsledare (n = 667)	13	62	26
Planering av husrannsakan/beslag			
Åklagare (n = 379)	24	62	14
Polisiära förundersökningsledare (n = 662)	18	60	22
Genomförande av husrannsakan/beslag			
Åklagare (n = 380)	26	59	15
Polisiära förundersökningsledare (n = 663)	18	62	20
Vid förhör			
Åklagare (n = 379)	5	84	12
Polisiära förundersökningsledare (n = 667)	2	73	24

Not: På grund av avrundningar understiger/överstiger vissa procentsummor 100 procent.

Bilaga 2. Metod

Distribution av Brås enkät

Målsättningen med Brås enkätundersökning var att nå samtliga åklagare som vid tiden för undersökningen arbetade operativt som förundersökningsledare samt samtliga polisiära förundersökningsledare och it-undersökare på regional nivå, polisområdesnivå eller lokalpolisområdesnivå (det vill säga ej förundersökningsledare och it-undersökare placerade på nationell nivå, t.ex. Noa och NFC). I rapporten beskrivs brister med urvalsunderlaget, samt den filterfråga som används för att säkerställa att rätt personer besvarade respektive enkät. I rapporten återfinns en tabell över distribuerade och besvarade enkäter samt svarsfrekvensen. Nedan redogörs för fler detaljer kring distribution och utskickssiffror.

Sammanställningen av de olika underlagen från regionerna gav totalt 1 941 namn på förmodade förundersökningsledare. Enkäten skickades ut till samtliga 1 941. Vid utskicket fastnade 383 enkäter i Polismyndighetens brandvägg, antingen för att adressen var ogiltig (24 stycken), eller för att personen inte ansökt om att få ta emot extern epost (363 stycken). Eftersom Brå inte hade möjlighet att nå dessa 383 individer justerades utskickssiffran initialt från 1 941 till 1 558.

Bland dem som öppnade enkäten uppgav 24 procent att de inte arbetade operativt som förundersökningsledare vid tidpunkten, det vill säga att de felaktigt ingick i underlaget. För dem som aldrig öppnade enkäten har Brå ingen information om huruvida personerna är förundersökningsledare eller inte. Brå gjorde därför ett antagande om att 24 procent (det vill säga andelen felaktigt utskick enligt filterfrågan) av dem som inte besvarat enkäten inte tillhörde målgruppen, och alltså felaktigt fanns med i det underlag som Brå tillhandahållit. Slutlig utskickssiffra för de polisiära förundersökningsledarna blev därmed 1 183. Svarsfrekvensen baseras därmed på denna justerade siffra. Andelen som inte är förundersökningsledare bland dem som inte öppnade enkäten är förmodligen högre eftersom enkätens missivbrev angav att enkäten riktade sig till förundersökningsledare och man kan därmed anta att icke förundersökningsledare i större utsträckning valde att inte öppna och besvara enkäten.

Bland åklagarna som öppnade enkäten sållades 10 procent bort i filterfrågan, det vill säga de arbetade inte operativt som förundersökningsledare vid tidpunkten. Utskickssiffran för åklagare justerades, i enlighet med resonemanget ovan, utifrån ett antagande om att även 10 procent bland dem som inte öppnade enkäten inte tillhörde målgruppen. Slutlig utskickssiffra för åklagarna

blev därmed 719. Bland it-undersökarna som öppnade enkäten sållades 9 procent bort i filterfrågan, det vill säga de arbetade inte som it-undersökare vid tidpunkten. Utskickssiffran justerades därefter. Slutlig utskickssiffra för it-undersökarna blev därmed 224.

Bilaga 3. Exempel på it-inslag

Nedan följer beskrivande exempel på ärenden i urvalet av polisanmälningar av brott mot person (Brb kap. 3–7) respektive bedrägeri och annan oredlighet (Brb kap. 9), de två brottskategorier där it-inslag är vanligast förekommande enligt anmälningarna.

Exempel på it-inslag bland brott mot person

I den första kategorin (tabell 1B i bilaga 1) återfinns de fall som klassificerats som *it är målet*. Nästan alla av dessa brott hade brottskoden dataintrång vid polisanmälan. En relativt stor andel rör ärenden där den drabbades e-post eller sociala medier-konto på okänt sätt uppges ha kapats av någon okänd. I flera av dessa fall har falska meddelanden gått ut till den drabbades kontakter som ombeds föra över pengar eller lämna ut känsliga uppgifter. I andra ärenden har ett meddelande kommit upp på dataskärmen där det står att den drabbade måste betala för att datorn ska låsas upp (s.k. ”ransomware”). En annan typ av fall gäller att någon person på okänt sätt gjort intrång i den drabbade personens dator och kommit över privata bilder med sexuellt innehåll. Ytterligare ett exempel är att gärningspersonen genom att installera ett program i målsägarens bärbara dator kunnat filma den drabbade genom den inbyggda kameran. En annan typ av kapningar av e-post eller sociala medier-konton gäller dataintrång där det är en bekant person, ofta partner i en relation eller expartner, som uppges vara gärningspersonen. Han eller hon har obehörigen loggat in på den andras konto och sedan låst det och i vissa fall skrivit meddelanden eller gjort andra ändringar. Intrången kan vara del i en rad övergrepp inom relationen. En tredje typ av dataintrång gäller vårdpersonal som obehörigen loggat in i datasystemen på sin arbetsplats och läst patientjournaler, vilket upptäckts genom dataloggar.

Det dominerade inslaget inom kategorin *it är medlet* gäller text/ljud/bild-meddelanden på mobiltelefon eller på sociala medier. Ofta gäller brottsligheten olaga hot, ofredande och i en del fall sexuellt ofredande.

I kategorin *it har annan beröring* ingår några fall där målsägaren eller ett vittne filmat hot eller ofredanden genom mobilkamera. Antalsmässigt klart dominerande bland dessa händelser är emellertid att brottet har spelats in med övervakningskamera eller att det uttryckligen noterats i anmälan att det bör undersökas om händelsen spelats in eftersom det finns övervakningskamera på platsen. Bland dessa fall ingår även att gärningspersonen kan ha filmats i nära anslutningen till brottet. Händelserna gäller en rad olika typer av brott, varav misshandel är vanligast.

Exempel på it-inslag bland bedrägeri och annan oredlighet

Bland de fall som är klassificerade som att *it är målet* finns det ett antal sinsemellan olika typer. I några ärenden har den drabbades dator blivit låst och det har kommit upp meddelanden på skärmen att man måste betala för att den ska låsas upp. En annan typ av ärende gäller att någon kapat målsägarens e-post och skickat ut meddelanden till dennes kontakter som ombeds sätta in pengar. Flera andra ärenden gäller att målsägarna blivit uppringda på telefon av någon person som uppger sig vara från Microsoft. Personen påstår att det är problem med den drabbades dator och erbjuder hjälp. Användaren uppmanas att slå på fjärrstyrningsfunktionen i Windows så att bedragaren kan fjärrstyra datorn. Sammantaget sett tycks de nämnda typerna av bedrägerier ha ökat.

När det gäller kategorin *it är medlet* förekommer varierande typer av ärenden. Den vanligast förekommande typen, som också har ökat under perioden, är kort-/kontobedrägerier (se även Brå 2016:9). Vanligt är att målsägaren har sitt kort i behåll men upptäcker att det dragits summor från kontot. Inte sällan gäller det köp eller uttag utomlands i delar av världen som målsägaren inte besökt. I en del fall är det banken som meddelar målsägaren att man spärrat kortet eller kontot på grund av man misstänker bedrägeri. Ibland anges i anmälan att man misstänker eller antar att kortet har blivit skimmat, medan det i andra fall är mer oklart i anmälan hur bedragarna kommit över uppgifterna. Enligt en intervju med utredare på Nationellt bedrägericentrum (NBC) går det för bedragare att köpa nödvändiga uppgifter, vilka i sig härrör från stora dataintrång, på svarta marknader på internet.

En annan relativt vanlig typ av ärenden gäller försäljning på falska grunder. Bedragarna säljer produkter på försäljningssidor som Blocket eller via andra annonser på internet. Efter betalning levereras aldrig produkterna eller de håller inte vad som utlovats. Målsägarna försöker förgäves få kontakt med säljarna. En annan typ gäller köp eller lån i annans namn. Bedragarna har genom att utnyttja personuppgifter för målsägarna beställt varor på internet eller ansökt om lån/krediter som de använder för eget bruk.

Tillsammans utgör de hittills nämnda typerna av bedrägerier en klar majoritet (cirka 90 procent) av fallen i kategorin *it är medlet*. De resterande fallen är utspridda över olika typer av ärenden. Några gäller fakturabedrägerier där målsägaren får en faktura via e-post för tjänster denne inte beställt. Andra gäller utpressning via mobil eller e-post. Något enstaka fall gäller köp av en stulen vara via en annons på Blocket, och några fall är svåra att klassificera eller innehåller många olika typer av it-inslag.

Kategorin *it har annan beröring* består till stor av ärenden med koppling till abonnemang på mobiltelefoni, som att någon i en telefonbutik öppnat abonnemang i annans namn. Den andra typen som är vanligt förekommande i kategorin gäller olika typer av brott där det uppges att en övervakningskamera har eller kan ha filmat gärningspersonen.

Bilaga 4. Organisation och ansvarsfördelning

Olika delar av Polismyndigheten respektive Åklagarmyndigheten är involverade vid såväl handläggning och utredning, som styrning och utveckling gällande brott med it-inslag. Nedan beskrivs huvuddragen avseende ansvarsfördelning och organisation inom respektive myndighet.

Organisation och ansvarsfördelning inom Polismyndigheten

Polismyndighetens sju polisregioner (Bergslagen, Mitt, Nord, Stockholm, Syd, Väst och Öst) har helhetsansvar för polisverksamheten i respektive region. Inom varje polisregion finns ett antal polisområden som i sin tur är indelade i ett antal lokalpolisområden. I Arbetsordningen för polismyndigheten (Polismyndigheten 2016a) framgår att det vid polisområdenas samt vid polisregionernas utredningsenheter ska finnas forensisk kunskap och verksamhet.[104]

Inom Polismyndigheten finns även ett antal nationella avdelningar, däribland Nationella operativa avdelningen (Noa) och Nationellt forensiskt centrum (NFC[105]). Den Nationella operativa avdelningen (Noa) har processansvaret för bland annat komplex it-brottslighet, internetrelaterade sexuella övergrepp mot barn och it-relaterad brottslighet. Nationellt forensiskt centrum (NFC) har processansvar för all forensisk verksamhet, inklusive it-forensisk verksamhet som utförs utanför avdelningen. Vid Noa finns även sju geografiskt regionalt placerade utvecklingscentrum. Varje utvecklingscentrum har tilldelats nationellt utvecklingsansvar för olika typer av brott.

Polismyndighetens kärnverksamhet ska utföras nära medborgarna. Målet ska vara att mer än hälften av regionernas verksamhet ska bedrivas i lokalpolisområdet, där även en stor del av ärendena ska utredas (Genomförandekommittén för nya Polismyndigheten 2014a).

Organisation och ansvarsfördelning inom Åklagarmyndigheten

Åklagarmyndighetens operativa verksamhet utövas i sju åklagarområden samt vid en nationell avdelning. Åklagarområdena

[104] Polisregionerna och avdelningarna får, inom arbetsordningens och andra överordnade bestämmelsers ramar, besluta mer i detalj hur organisation och arbetsfördelning ska se ut inom polisregionen eller avdelningen. Sådana beslut ska dokumenteras i respektive handläggningsordning (1 kap. 4 §, Arbetsordning för Polismyndigheten).

[105] Tidigare Statens kriminaltekniska laboratorium (SKL).

följer samma geografiska indelning som polisregionerna. Varje åklagarområde består av ett antal allmänna kammare. Nationella åklagaravdelningen består av tre riksenheter (Riksenheten mot korruption, Riksenheten för miljö- och arbetsmiljömål samt Riksenheten för säkerhets- och terroristmål), samt av Internationella åklagarkammaren i Stockholm. Det finns ytterligare två internationella åklagarkammare, Göteborg och Malmö, som är placerade under område Väst respektive område Syd. Slutligen finns Särskilda åklagarkammaren som är placerad direkt under Riksåklagaren.

Vid Åklagarmyndighetens tre utvecklingscentrum bedrivs metod- och rättsutveckling inom olika brottsområden. Utvecklingscentrum i Stockholm ansvarar för metod- och rättsutvecklingsfrågor avseende it-relaterad brottslighet. Områdeschefen vid Åklagarområde Stockholm har nationellt samordningsansvar för it-området.

Bilaga 5. Inventering av respondenternas utbildningsnivå

I följande avsnitt ges en mer detaljerad redogörelse för respondenternas utbildningsnivå på it-området. När det gäller åklagare och polisiära förundersökningsledare rör inventeringen endast kurser och utbildningar på vidareutbildningsnivå,[106] medan it-undersökarna även tillfrågades om sin grundutbildning på it-området.[107] Syftet är att ge en bättre bild av vilka utbildningar som finns på it-området samt hur stor andel av respondenterna som har gått respektive kurs eller utbildning.

Drygt 4 av 10 åklagare har gått ”It-brottskursen”

Inom Åklagarmyndigheten ges för närvarande en vidareutbildningskurs i it-brottslighet, vilken har namnet ”It-brott och bevissäkring i it-miljö”, även kallad ”IT-brottskursen”. Kursen ingår i åklagarnas specialistutbildning och vänder sig till åklagare som har genomgått grundutbildningen och arbetat några år efter det. Kursen omfattar fem dagar och syftet är att deltagarna ska få grundläggande kunskaper om brott och bevisning i digital miljö. Målet med kursen är att deltagarna bland annat ska få kunskaper i hur en IP-spårning går till, få en fördjupad kunskap om tvångsmedelsanvändning och bevissäkring i it-miljö och kunskaper i att hantera barnpornografiärenden.[108] Därutöver berörs it-aspekten översiktligt vid vidareutbildningskurser som handlar om övergrepp mot barn, bedrägeri och ungdomar och brott.

I Brås enkät fick åklagarna uppge om de hade gått ”It-brottskursen” samt i så fall vilket år de gick den. Åklagarna tillfrågades också om de hade gått någon ”annan vidareutbildning avseende brott med it-relevans” och vilken kurs de i så fall hade gått. Av de åklagare som besvarade Brås enkät uppgav drygt 4 av 10 att de hade gått ”It-brottskursen”. Det bör noteras att det i materialet inte framgår hur länge personerna har tjänstgjort som åklagare, och det kan därmed finnas åklagare som inte har haft möjlighet att gå den aktuella kursen.

---

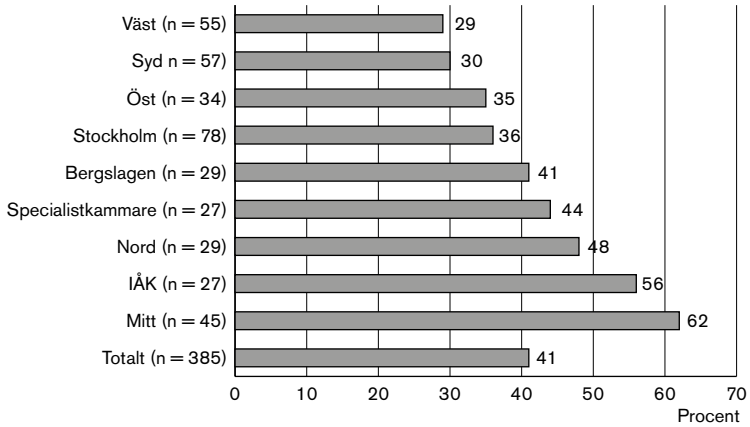
[106] Med vidareutbildning avses i den här rapporten utbildning som ges till personer som efter avslutad grundutbildning får kompetensutveckling inom ett visst område. I enkäten görs ingen åtskillnad mellan begreppen vidareutbildning och fortbildning. Vidareutbildningen kan både bestå av en utbildning med tydliga kursmål som ska bedömas eller som löpande fortbildning inom ett visst område utan krav på examination.

[107] I åklagarnas grundutbildning ingår en kurs om it-relaterade brott. I polisens grundutbildning saknas däremot en sådan kurs. För en redogörelse över hur it-inslag är integrerat i åklagarnas och polisens grundutbildning, se kapitlet *”Angelägna utvecklingsområden och pågående utvecklingsarbete”.*

[108] Kursplan, IT-brottskursen (gäller från 2015-06-01).

Andelen som uppger att de har gått ”It-brottskursen” varierar stort mellan olika åklagarområden. Som framgår av figur 1B har exempelvis 29 procent av åklagarna tillhörande område Väst gått den aktuella kursen, jämfört med 62 procent av åklagarna från område Mitt.

Figur 1B. Andelen åklagare som uppger att de har gått vidareutbildningskursen ”It-brott och bevissäkring i it-miljö” som ges i Åklagarmyndighetens regi. Totalt samt uppdelat på åklagarområde.[109]



Resultatet visar att över hälften av åklagarna hade gått kursen någon gång under de senaste tre åren (mellan 2013 och 2016). Drygt var femte åklagare (22 procent) uppgav dock att de gått kursen för över tio år sedan (tabell 7B).[110]

Tabell 7B. Andelen åklagare som uppger att de har gått vidareutbildningskursen ”It-brott och bevissäkring i it-miljö” uppdelat på senaste kurstillfälle. Antal och procent (n = 131).

	Antal	Procent
Fram till 2006	29	22
2007–2008	5	4
2009–2010	10	8
2011–2012	17	13
2013–2014	48	37
2015–2016	22	17
Totalt	**131**	**100**

[109] I kategorin ”specialistkammare” ingår Riksenheten mot korruption, Riksenheten för miljö- och arbetsmiljömål, Riksenheten för säkerhetsmål samt Särskilda åklagarkammaren. Med IÅK avses någon av de tre internationella åklagarkamrarna i Stockholm, Göteborg eller Malmö.

[110] Totalt 131 åklagare som hade gått ”It-brottskursen” kunde även specificera vilket år de gått den. Frågan var öppen och har därefter kategoriserats i årsintervall. Individer som var osäkra, men som ändå har uppgett ett år de tror att de gick kursen, har medräknats i analysen. Om individen har uppgett flera årtal har det senaste använts.

Närmare 13 procent av åklagarna uppgav att de har gått ”någon annan vidareutbildning avseende brott med it-relevans”. Ofta utgjordes det av kurser om andra ämnen där informationsteknologi hade berörts, till exempel kurser om bedrägeri, unga lagöverträdare, brott begångna mot barn, narkotikabrott etc.

Svaren på båda utbildningsfrågorna sammanfördes därefter till en dikotom utbildningsvariabel. Åklagare som uppgav att de antingen hade gått ”It-brottskursen” eller ”någon annan vidareutbildning avseende brott med it-relevans” kategoriserades som att de har en utbildning på it-området. Resultatet visade sammantaget att 46 procent av åklagarna har någon form av utbildning på it-området, medan 54 procent saknade en sådan utbildning.

Få polisiära förundersökningsledare har fått någon vidareutbildning på it-området

Inom Polismyndigheten ges sedan år 2014 en kurs inom området it-brottslighet som specifikt riktar sig till förundersökningsledare; ”It-forensisk översiktskurs för förundersökningsledare”. Kursen omfattar fem dagar, varav en dag är självstudier. Kursen innehåller juridik som rör brott med it-relation, internetarkitektur, it-forensik och internationellt samarbete.[111] Därtill erbjuds en liknande kurs som riktar sig till anställda som arbetar som utredare av it-relaterade brott (”It-forensisk översiktskurs för utredare”) samt en kurs som riktar sig till personal som arbetar med inhämtningsarbete på internet (”Underrättelse- och inhämtningsarbete på Internet, baskurs”).[112] I Brås enkät fick förundersökningsledarna uppge om de hade gått någon av de aktuella kurserna samt i så fall vilket år de gick kursen. De tillfrågades även om de hade gått någon ”annan vidareutbildning avseende brott med it-relevans” och i så fall vilken kurs de hade gått.

Endast ett fåtal av de 670 polisiära förundersökningsledare som besvarade Brås enkät uppgav att de hade gått någon av de tre kurserna på it-området som erbjuds i Polismyndighetens regi. Knappt 6 procent uppger att de har gått kursen ”It-forensisk översiktskurs för förundersökningsledare” och 1 procent att de har gått kursen ”It-forensisk översiktskurs för utredare” eller ”Underrättelse- och inhämtningsarbete på Internet, baskurs”

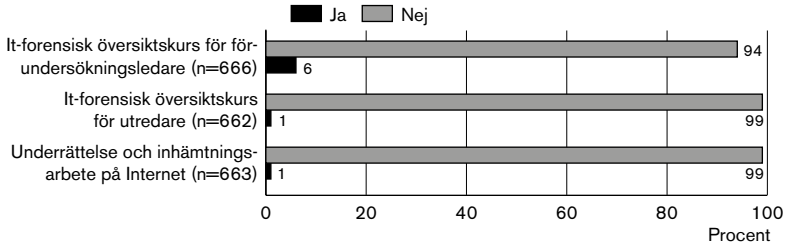
[111] Efter godkänd kurs ska kursdeltagaren bland annat kunna göra en prioritering av initiala åtgärder, göra korrekta beställningar till it-forensiker, tolka it-forensiska resultat och redogöra för relevant lagstiftning kopplat till ärenden med it-relation (Kursplan, beslutsdatum 2016-03-03).

[112] Kursen *Underrättelse- och inhämtningsarbete på Internet*, baskurs (tidigare *Grundläggande underrättelsearbete på internet*) ges under tio dagar, varav två dagar är självstudier. Även denna kurs har funnits sedan år 2014 och innehåller bland annat it-teknik, it-juridik och information om internationella och nationella samarbetsformer. Syftet är att förbättra kvaliteten inom underrättelse- och utredningsarbete på internet (Kursplan beslutsdatum 2014-02-10).

(figur 2B). På grund av att så få förundersökningsledare har gått de aktuella kurserna görs inga regionala jämförelser. Inte heller redogörs för det år då respondenterna gick kurserna. I sammanhanget bör det nämnas att samtliga dessa tre kurser endast har genomförts sedan år 2014.

Totalt 4 procent av de polisiära förundersökningsledarna uppger att de har gått ”annan relevant utbildning på it-området”. Några exempel på utbildningar de uppger sig ha gått är olika typer av högskole- eller universitetsutbildningar i exempelvis datateknik eller dataprogrammering eller interna kurser i telefontömning, granskning av barnpornografi eller kurser i Excel. Det bör dock nämnas att det finns enstaka poliser i materialet som uppger att de har en gedigen utbildning på it-området, till exempel en längre it-forensisk utbildning.

Figur 2B. Andelen polisiära förundersökningsledare som uppger att de har gått någon av de tre vidareutbildningskurserna på it-området som erbjuds i Polismyndighetens regi. Procent.



Svaren på samtliga utbildningsfrågor sammanfördes till en dikotom utbildningsvariabel. Polisiära förundersökningsledare som uppgav att de antingen hade gått kursen ”It-forensisk översiktskurs för förundersökningsledare”, kursen ”It-forensisk översiktskurs för utredare”, ”Underrättelse- och inhämtningsarbete på internet” eller ”någon annan vidareutbildning avseende brott med it-relevans” kategoriserades som att de har en utbildning på it-området. Resultatet visar att sammantaget 10 procent av förundersökningsledarna har någon form av utbildning på it-området, medan 90 procent saknar en sådan utbildning.[113]

Majoriteten av it-undersökarna har en gedigen utbildning på it-området

Det finns i dagsläget flera olika sätt att utbilda sig till it-undersökare. Ett sätt är att genomgå en högskole- eller universitetsut-

[113] Det är stor variation i de utbildningar som polisiära förundersökningsledare uppger att de har gått, allt från enstaka kurser i Office-paketet till en särskild kurs om it-relaterad brottslighet.

bildning på it-området. Drygt hälften av it-undersökarna som har besvarat Brås enkät har någon form av högskole- eller universitetsutbildning, där ungefär var tredje (30 procent) uppger att de har en kandidat- eller högskoleingenjörsexamen, 7 procent att de hade en magister-, master- eller civilingenjörsexamen och 17 procent har gått en eller flera andra högskole- eller universitetskurser på it-området, men som inte har lett fram till en examen (tabell 8B). Några exempel på utbildningar som nämns är data- och systemvetenskap och datanätteknik eller fristående kurser i programmering, it-juridik eller it-säkerhet.

Som förväntat är andelen it-undersökare med en akademisk utbildning på it-området betydligt högre bland civilanställda än hos it-undersökare med en polisiär bakgrund. Resultatet visar att drygt 70 procent av de civilanställda it-undersökarna har någon form av högskole- eller universitetsutbildning på it-området. Motsvarande andel bland polisiära it-undersökare är drygt 18 procent. Oftast har den civila it-undersökaren en kandidat- eller högskoleingenjörsexamen på it-området (41 procent). Ett fåtal (9 procent) har en magister-, master- eller civilingenjörsexamen på it-området och 20 procent har läst en eller flera kurser eller högskole- eller universitetsutbildningar på it-området som inte lett fram till en examen.

Ett annat sätt att utbilda sig till it-undersökare är att efter avklarad grundutbildning till polis (Polisprogrammet) genomgå någon av de fördjupade vidareutbildningar inom it-forensik som erbjuds inom Polismyndigheten; ”It-forensiker grundutbildning – Etapp 1” eller ”It-forensiker grundutbildning – Etapp 2”.[114] Kursen vänder sig till polisen, men är även öppen för deltagare från bland annat Åklagarmyndigheten, Ekobrottsmyndigheten och Tullverket (Polishögskolan 2014). Utbildningens andra steg (etapp 2) är en fortsättningskurs och riktar sig till personer som har gått utbildningens första del eller som har motsvarande högskoleutbildning. I tabell 8B redovisas andelen it-undersökare som har gått någon av de fördjupade utbildningar inom it-forensik som erbjuds inom Polismyndigheten. Av de 132 it-undersökare som besvarade Brås enkät uppgav 36 procent att de hade genomgått fördjupningsutbildningen ”It-forensiker grundutbildning – Etapp 1” och 59 procent uppgav att de hade gått fortsättningskursen ”It-forensiker grundutbildning – Etapp 2”.

Förutom de längre utbildningar inom it-forensik som erbjuds vid Polismyndigheten finns för närvarande även ett femtontal kortare kurser som specifikt riktar sig till it-undersökare. Kurserna gäller i regel något bestämt digitalt verktyg och leds därför ofta av

[114] Etapp 1 ges under 58 dagar, varav 17 dagars närstudier och 41 dagars självstudier. Etapp 2 utgörs av 20 dagars närstudier. Båda kurserna upphör i slutet av 2016.

inhyrd personal från något av programvaruföretagen. Det finns också, som ovan nämnts, kursen ”Underrättelse- och inhämtningsarbete på internet, baskurs” och de två översiktskurser som riktar sig till förundersökningsledare och utredare (”It-forensisk översiktskurs för förundersökningsledare” och ”It-forensisk översiktskurs för utredare”). För att få en sådan uttömmande bild som möjligt av it-undersökarnas utbildningsnivå tillfrågas de därför om de har gått någon av dessa tre kurser. De tillfrågas dessutom om de har gått ”någon annan vidareutbildning i Polisens regi”.

Resultatet visar att över hälften av it-undersökarna uppger att de har genomgått någon ”annan vidareutbildning i Polisens regi”, till exempel en eller flera kurser om de programvaror (t.ex. Encase eller Forensic Tool Kit, FTK) som används av it-undersökare vid analys av datorer och annan lagringsmedia, t.ex. USB-minnen och externa hårddiskar.[115] Några andra exempel på utbildningar som it-undersökarna nämner är kurser i fingranskning av barnpornografiskt material, internethämtning, telefontömning eller ”live forensics”.[116] Totalt 15 procent uppger att de gått kursen ”Underrättelse- och inhämtningsarbete på internet, baskurs”, medan ytterst få uppger sig ha gått någon av de it-forensiska översiktskurser som erbjuds till förundersökningsledare eller utredare (tabell 8B).

Tabell 8B. Utbildningsnivå bland it-undersökarna. Procent.

	Procent
Akademisk grundutbildning	
Kandidat- eller högskoleingenjörsexamen på it-området (n = 132)	30
Magister-, master-, eller civilingenjörsexamen på it-området (n = 130)	7
Annan relevant högskole- eller universitetsutbildning (n = 132)	17
Vidareutbildning i Polismyndighetens regi	
It-forensiker grundutbildning etapp 1 (n = 132)	36
It-forensiker grundutbildning etapp 2 (n = 132)	59
It-forensisk översiktskurs för förundersökningsledare (n = 132)	3
It-forensisk översiktskurs för utredare (n = 132)	2
Underrättelse- och inhämtningsarbete på internet, baskurs (n = 131)	15
Annan relevant utbildning på it-området i Polisens regi (n = 132)	55
Summerad utbildning	
Kategori 1: Gedigen utbildning (n = 94)	71
Kategori 2: Enstaka kurser (n = 22)	17
Kategori 3: Ingen utbildning (n = 16)	12

[115] Med hjälp av programvarorna kan man bl.a. ta fram raderat material och kategorisera bevisning.

[116] Live forensics innebär it-forensiska åtgärder, spegling eller säkrande av digital bevisning som utförs på plats i ett igångsatt system (Kronqvist 2013, s. 51).

I analysen av it-undersökarnas utbildningsnivå skapades en kategoriserad utbildningsvariabel där svaren från samtliga utbildningsfrågor sammanfördes. It-undersökare som hade läst någon av de fördjupade utbildningarna om it-forensik som erbjuds inom Polismyndigheten eller hade en akademisk examen på it-området kategoriserades som en ”gedigen utbildning”, it-undersökare som hade läst någon annan kurs eller utbildning i Polisens regi eller på högskola/universitet (utan examen) kategoriserades som ”enstaka kurser” och de som svaret nej på samtliga utbildningsfrågor kategoriserades som ”saknar utbildning”.

Resultatet från Brås enkät visade att majoriteten (71 procent) av it-undersökarna har en gedigen utbildning på it-området, det vill säga att de antingen har läst någon av de två it-forensiska utbildningar som erbjuds vid Polishögskolan (etapp 1 eller 2) och/eller att de har en akademisk examen på it-området. Ytterligare 17 procent uppger att de har läst en eller flera kurser på it-området, antingen i Polismyndighetens regi eller vid en högskola/universitet, men som inte lett fram till en examen. Dock visar resultaten att 12 procent av it- undersökarna helt och hållet saknar utbildning på it-området.[117]

[117] Drygt hälften av dem som saknar utbildning har en polisiär bakgrund och resterande är civilanställda. De vanligaste arbetsområdena för dessa it-undersökare är bild/film och ljud (88 procent) samt mobila enheter (69 procent).

Dagens samhälle genomsyras alltmer av informationsteknologi (it), och detsamma gäller brottsligheten.

Denna rapport beskriver de senaste tio årens utveckling av den it-relaterade brottsligheten, liksom rättsväsendets kompetens och kapacitet att hantera den. Rapporten belyser också brister och angelägna utvecklingsområden för att höja rättsväsendets förmåga att hantera brott med it-inslag.

Rapporten vänder sig i första hand till personer som är verksamma inom Polismyndigheten och Åklagarmyndigheten, men även till forskare och övriga intresserade inom rättsväsendet.

ISBN 978-91-87335-74-7 • URN:NBN:SE:BRA-671 • ISSN 1100-6676

brå

Brottsförebyggande rådet/National Council for Crime Prevention
BOX 1386/TEGNÉRGATAN 23, SE-111 93 STOCKHOLM, SWEDEN
TELEFON +46 (0)8 527 58 400 • FAX +46 (0)8 411 90 75 • E-POST INFO@BRA.SE • WWW.BRA.SE