Polisiära cyberhot, en förstudie

Mikael Wedlin, Peter Nilsson,
Arwid Komulainen, Farzad Kamrani

FOI-R--4599--SE

Juni 2018

FOI

Mikael Wedlin, Peter Nilsson, Arwid Komulainen, Farzad Kamrani

Polisiära cyberhot, en förstudie

Bild/Cover: Mikael Wedlin

Titel	Polisiära cyberhot, en förstudie
Title	Policing cyber threats, a pilot study
Rapportnr/Report no	FOI-R--4599--SE
Månad/Month	Juni
Utgivningsår/Year	2018
Sidor/Pages	27 p
Kund/Customer	Försvarsdepartementet
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	A74001
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Sammanfattning

Denna rapport redovisar första årets resultat från projektet *Cyberhot, en förstudie*. Projektet syftar till att öka FOIs kunskap om den polisiära verksamheten och i synnerhet arbetet mot IT-relaterad brottslighet, det vill säga de hot mot samhället som främst manifesteras via internet. Projektet syftar även till att i möjligaste mån öka Polisens förmåga att hantera cyberhot. Metodiken har i huvudsak bestått av litteraturstudier och möten med representanter för de olika myndigheterna men även kortare workshops och ett webbinarium.

En stor del av arbetet har gått ut på att karaktärisera vad ett cyberhot egentligen är och vilket ansvar rättsvårdande myndigheterna har i cyberdomänen, samt vilka metoder och redskap som krävs för att möta dessa cyberhot. En fråga som framträtt är huruvida cyberbrott bör betraktas som en egen brottstyp eller om det helt enkelt är gamla brott i ny förpackning. Några av faktorer som gör cyberhot svåra att utreda och förhindra är den utbredda användningen av anonymisering samt att dessa utredningar ofta har internationella dimensioner.

I dagsläget är kompetens inom cyberområdet en knäckfråga för Polisen; en aspekt av detta är att det finns spetskompetens att tillgå inom området men brist på samordning och arbetsfördelning gör att dessa kompetenser inte utnyttjas där de mest behövs. En annan aspekt är att breddkompetens inom cyberområdet saknas i många delar av organisationen.

Nyckelord: Cyberhot, cyberbrott, polisen på nätet

Summary

This report presents the first year's results from the project *Cyberthreat, a prestudy*. The project aims at increasing FOI's knowledge of police cyber activities, and in particular the work against IT related crime, but also to increase Police's ability in the area as much as possible. Methodology has consisted mainly of literature studies and meetings with representatives of the different authorities, but also shorter workshops and a webinar.

A large part of the work has been to characterize what a cyberthreat really is and what responsibility the law enforcement authorities have in the cyber domain, and what methods and tools are required to meet these cyber threats. One issue that has emerged is whether cybercrime should be regarded as its own crime type or if it is simply old crimes in a new package. Some of the factors that make cyber threats difficult to investigate and prevent is the widespread use of anonymization, and that these investigations often have international dimensions.

Currently, competence in the cyber area is a key issue for the Police; One aspect of this is that there is excellence in the field, but lack of coordination and division of labor means that these skills are not utilized where they are most needed. Another aspect is that broadband competence in the cyber area is lacking in many parts of the organization.

Keywords: Cyber threat, cybercrime, police online

Innehållsförteckning

1 Inledning

FOI har av Försvarsdepartementet fått ett anslag med syftet att öka kompetensen om Polisens och Säkerhetspolisens verksamhet för att inom totalförsvarsramen kunna stödja dessa myndigheter med relevant forskning.

Denna rapport redovisar första årets resultat från ett av dessa projekt, *Cyberhot, en förstudie*.

Målet med projektet har dels varit att öka FOIs kunskap om den polisiära verksamheten och i synnerhet arbetet mot IT-relaterad brottslighet men även att i möjligaste mån öka Polisens förmåga inom området. Projektet sträcker sig över två år och denna rapport är en sammanställning av det första årets arbete.

Metodiken har i huvudsak bestått av litteraturstudier och möten med representanter för de olika myndigheterna men även kortare workshops och ett webbinarium.

Även om flera projektmedlemmar har erfarenhet av projekt där polisen varit avnämare på olika sätt så har vi inte sedan tidigare någon djupare erfarenhet av polisiär verksamhet. Polisens verksamhet är dessutom något många påverkas av och därför också har åsikter om. Projektet har därför genomförts med ambitionen att dess projektmedlemmar skulle ha så få förutfattade meningar som möjligt.

1.1 Syfte och mål med projektet

Projektet syftar till att öka FOIs kunskap om den polisiära verksamheten och i synnerhet arbetet mot IT-relaterad brottslighet, det vill säga de hot mot samhället som främst manifesteras via internet. Projektet syftar även till att i möjligaste mån öka Polisens förmåga att hantera cyberhot. Ett led i detta är att förtydliga vad som avses med cyberbrott, vad som förväntas av Polis respektive Säkerhetspolis inom detta område samt att bidra till att formulera en målbild för framtida arbete.

Målet är att FOI efter första året ska ha byggt upp ett kontaktnät samt börjat få en förståelse för problemområdet. År två är målet att vidareutveckla kompetenser mot de identifierade behoven. Målet är också att Polisen och SÄPO efter projektets genomförande har förståelse för utvecklingen inom området och hur kunskapsuppbyggnad på TRL[1] 1-2 kan komma till användning i Polisens och SÄPOs respektive verksamhet.

1.2 Problembeskrivning

Rättsvårdande myndigheter står med i och med att samhället utvidgas till att inkludera cyberdomänen inför omfattande problem och utmaningar. Dessa utmaningar kan delas in i fyra grupper:

- Vad innebär de rättsvårdande myndigheternas ansvar och uppgifter i cyberdomänen?
- Hur ska myndigheterna utöva sina uppgifter i det cyberdomänen?
- Vilka redskap behöver myndigheterna för att kunna utöva sina uppgifter i cyberdomänen?
- Vilka förändringar behövs för att möta de nya utmaningarna?

[1] Technology Readiness Level (TRL) är en skala som används för att beteckna mognadsgraden för en teknologi. Skalan sträcker sig från 1–9 och en TRL-nivå på 1-2 motsvarar grundforskningsnivå och strax däröver.

1.3 Metod

I projektets inledning arrangerades en workshop med syfte att skapa en bild av Polisens organisation och deras arbete med cyberhot. Workshopen skedde tillsammans med kontaktpersoner hos Polisen.

Under projektets gång har litteratur inom området studerats för att dels tydliggöra Polisens behov och problem inom cyberområdet och dels för att identifiera trender inom cyberbrottslighet. Litteraturstudien har inkluderat rapporter från myndigheter och organisationer såväl som vetenskapliga artiklar. Ingen strikt uttömmande studie har genomförts då syftet varit att bygga upp kompetens snarare än att göra en kartläggning av litteraturen.

Under projektets senare del genomfördes ett webbinarium med inbjudna personer från olika delar av Polisens organisation samt åklagarmyndigheten. Webbinariet var uppbyggt kring ett antal verkliga fall som presenterades och diskuterades. Syftet med webbinariet var dels att sprida information om projektet och dels att samla in ytterligare information om Polisens behov och svårigheter samt ge uppslag till fortsatt arbete.

1.4 Avgränsningar

Projektgruppen valde i ett tidigt skede att inte studera sådana aspekter av cyberbrott som Polisen redan hanterar framgångsrikt samt områden där forskning redan bedrivs, så som IT-forensik.

Fokus för projektet fastställdes till att bygga på tre kriterier (Se Figur 1):

a) Sådant som faller under Polisens eller Säkerhetspolisens ansvarsområden.

b) Sådant som på något sätt har beröring med internet.

c) Sådant som är kriminellt, samhällshotande eller samhällsstörande.

Figur 1 Projektets fokusområde

1.5 Historisk utveckling av området

Den nuvarande Polislagen (1984:387) skrevs 1984, det vill säga innan både HTML och HTTP hade utvecklats. Lagstiftningen kompletterades 1998 med Lag (1998:112) om ansvar för elektroniska anslagstavlor. Ingen av dessa lagar tog dock höjd för den enormt snabba utveckling som internet och andra elektroniska medier demonstrerat under de senaste 25 åren. Ytterligare en bidragande orsak har varit mobiltelefonins utveckling. I sammanhanget kan nämnas att det första kommersiella SMS-meddelandet var en julhälsning den 3:e december 1992. Tillsammans har mobiltelefonin och internet kommit att fullständigt revolutionera det moderna samhället. I takt med utvecklingen av allt fler

elektroniska tjänster så har också brottslig verksamhet kommit att nyttja elektroniska medier för kriminella ändamål. Rättsvårdande myndigheter har av förklarliga skäl haft svårt att följa med i den snabba utvecklingen, dels på grund av att det faktiskt inte är önskvärt att lagstiftning ändras alltför snabbt men också på grund av elektroniska mediers unika egenskaper som gör det svårt att tillämpa traditionell, beprövad metodik. Situationen är dock inte unik för Sverige utan polismyndigheter över hela världen kämpar för att komma ikapp den digitala utvecklingen och vad den för med sig i form av kriminalitet. De problem och utmaningar som uppstår då en allt större del av samhället flyttar till en digital miljö är inte rent polisiära utan handlar även om vilken slags samhälle vi vill leva i vilket resulterat i en omfattande debatt om brottsbekämpning kontra personlig integritet.

1.6 Cyberspace

Cyberspace är ett begrepp som myntades 1982 av William Gibson i novellen *Burning Chrome*. Gibson har i en senare dokumentär sagt följande om begreppet cyberspace:

"All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page." (Neale 2000)

Begreppet har sedan dess använts flitigt men trots det så saknas det fortfarande en allmänt accepterad definition av begreppet. Mayer med flera (2014) har formulerat en definition som ger en indikering om begreppets ungefärliga innebörd.

"*Cyberspace är en global och dynamisk domän (föremål för konstant förändring) som karaktäriseras av det kombinerade användandet av elektroner och det elektromagnetiska spektret som syftar till att skapa, lagra, modifiera, utbyta, dela och extrahera, använda, eliminera information och påverka fysiska resurser.*

Cyberspace inkluderar:

- *a) Fysisk infrastruktur och telekomutrustning som medger uppkoppling mot kommunikationssystem och tekniska nätverk i sin bredaste mening (SCADA-system, smartphones, surfplattor, datorer, servrar et cetera);*
- *b) Datorsystem (se punkt a) med tillhörande mjukvara (ibland inbäddad) som garanterar domänens basala funktionalitet och anslutningsmöjligheter;*
- *c) Nätverk mellan datorsystem;*
- *d) Nätverk av nätverk som kopplar samman datorsystem (skillnaden mellan nätverk och nätverk av nätverk är huvudsakligen organisatorisk);*
- *e) Ingående data (eller härbärgerad data).*

Ofta i vanligt tal, och ibland i kommersiella sammanhang, benämns nätverk av nätverk som internet (med litet i) och nätverk mellan datorer kan benämnas intranät. Internet (med stort I, populärt kallat nätet) kan betraktas som en del av system a). En distinkt och grundläggande egenskap hos cyberspace är att det inte finns någon central entitet som kontrollerar alla de nätverk som tillsammans utgör denna nya domän."

Speciellt mot slutet kan man ha åsikter om denna definition och ifrågasätta om de verkligen speglar den allmänna användningen när man gör distinktionen mellan att låta Internet vara ett egennamn eller inte på just detta sätt. Svenska språkrådet och datatermgruppen skriver så här om begreppet internet:

"Internet var från början ett namn på ett visst datornät bland andra globala datornät men betraktas numera som ett nät liknande telenätet eller elnätet, och ordet uppfattas därför som ett vanligt substantiv. Dock hanteras det inte riktigt som ett substantiv: det böjs inte i bestämd form. Formen internät med bestämd form internätet förekommer, men än så länge mest i vardagliga sammanhang. I norskan och danskan är sådan böjning etablerad, liksom på svenska för systerordet intranät." (Svenska datatermgruppen, 2016)

Även militärt råder oenighet kring vad som innefattas i begreppet cyberspace, i NATO national cyber security framework manual beskrivs hur olika länder gör olika bedömningar.

”There are differences in how states translate their visions into strategic objectives. A principal explanatory factor behind this may be countries’ diverging understanding of cyberspace. Some countries take a broad view of cyberspace that includes infrastructures (such as control systems in critical infrastructures) and others take a much narrower view of cyberspace, equating it more closely to the internet. To illustrate, the United States is at one end of the spectrum with a broad definition of cyberspace, even implicitly acknowledging the importance of social networks. In the Dutch NCSS, cyberspace is likewise defined broadly, including importance

framför allt på internet som arena och domän när vi säger cyberspace och kommer att

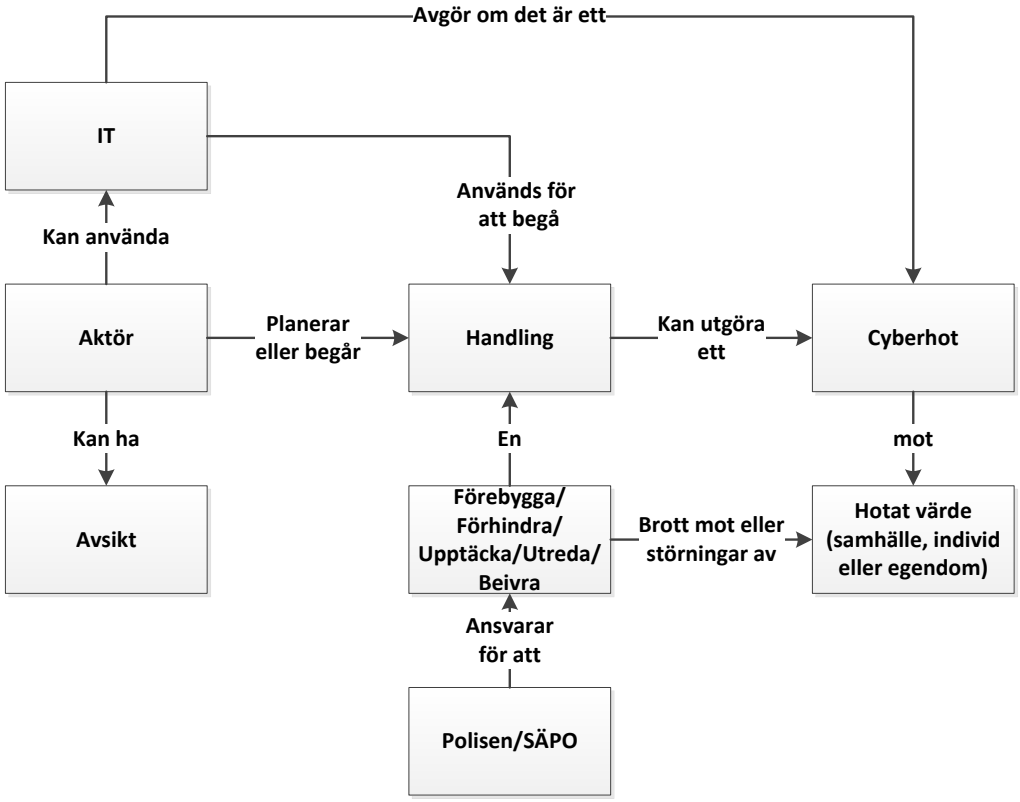
chip cards and in-car systems. On the other side of the spectrum, countries like Australia, Canada, Germany, New Zealand and Spain place an emphasis on the internet and internet connected information technologies (additional details are provided in Section 2.3.1).” (Klimburg 2012, 56)

Man kan konstatera att det finns ett stort antal olika divergerande definitioner och tankar om begreppen runt den nya tidens kommunikationsformer. I den här rapporten syftar vi framför allt på internet som arena och domän när vi säger cyberspace och kommer att använda de två termerna omväxlande med varandra, men mena ungefär samma sak. Wedlin (2011)

1.7 Cyberhot

Vad är ett cyberhot? En enkel förklaring är att det är någonting som utgör ett hot mot någonting annat i cyberspace. Ett hot är en relation mellan två entiteter eller fenomen. I detta arbete har vi valt att betrakta den hotande entiteten som en aktör av något slag och det hotade som samhällets kärnvärden, det vill säga rikets säkerhet, allmänhetens säkerhet och ordning och egendomssäkerhet (Se Figur 2).

Med cyberhot avses i denna rapport handlingar som planeras eller genomförs av aktörer med hjälp av IT, utgör ett hot mot samhälle, individ eller egendom och faller inom ramen för Polismyndighetens eller Säkerhetspolisens ansvarsområde.



Figur 2 Begreppsmodell syftande till att beskriva cyberhot.

1.8 Cyberbrott

Det används både inom Sverige och internationellt olika begrepp (t.ex. nätbrottslighet, databrott, IT-brottslighet, cyberbrott etc.) när man diskuterar IT-relaterad brottslighet. Dessa begrepp är oftast inte väldefinierade och gränserna mellan dem är inte helt tydliga. Till exempel, de äldre begreppen *cyberbrott* och *datorbrott* används numera synonymt eftersom nästan alla datorer är kopplade till internet.

Svensk lagstiftning inbegriper inte begreppet IT-relaterad brottslighet och brotten faller oftast under andra brottsrubriceringar oavsett vilken teknik som har använts för att begå dem. I brottsbalken finns endast två brott som är explicit knutna till informationsteknik (IT-brott), nämligen dataintrång (4 kap. 9 c § brottsbalken) och datorbedrägeri (Brottsbalken 9 kap. 1 § andra stycket). Båda dessa brott syftar primärt på register och system för automatisk databehandling.

Förutom dessa två IT-brott finns det en mängd andra brottsliga aktiviteter av olika slag där informationsteknik är mer eller mindre inblandad. För dessa används samlingsbegreppet IT-relaterad brottslighet. Det saknas dock någon enhetlig och vedertagen definition av begreppet.

BRÅ i sin rapport (BRÅ 2017) använder sig av uttrycket IT-relaterad brottslighet för alla brott där informationsteknologi (IT) är närvarande på något sätt. Dessa brott kategoriseras i tre olika kategorier, beroende på vilken grad IT är en del av brottet:

a) IT är en oskiljbar del av brottet och utan IT har brottet inte kunnat begås (det vill säga att IT är målet för brottet), exempelvis dataintrång.

b) IT är inte en oskiljbar del av brottet men har understött brottet (dvs. IT är medlet för brottet), till exempel genom att använda ett socialt forum för att hota någon eller bedriva hets mot folkgrupp.

c) IT är varken mål eller medel för brottet, men har någon typ av beröring med brottet genom att brottet har lämnat digitala spår som kan användas som bevisning vid ett brott som begåtts helt utanför IT-miljön, till exempel den digitala information som finns lagrade på våra busskort, biblioteksкort eller hårddiskar kan användas på olika sätt för bevisföring.

Denna definition är ganska bred och inbegriper alla typer av brott som på något sätt kräver IT-kompetens för att förebygga, förhindra, upptäcka, utreda eller beivra. Till exempel inkluderar den även misshandel om misshandeln har registrerats med övervakningskamera eftersom bildbehandlingen kräver IT-kompetens (IT-forensik).

Riksrevisionen i sin rapport (RIR 2015:21) refererar till (Wall, 2007/11) och delar IT-relaterad brottslighet i tre typer av brott:

a) brott mot en IT-enhet, exempelvis dataintrång och överbelastningsattacker (engelska, computer integrity crimes),

b) brott där en IT-enhet används, exempelvis försäljning av icke-existerande varor på internet och phishing (engelska, computer-related crimes),

c) brott som består i otillåten spridning av digitalt material såsom barnpornografi eller våldspropaganda (engelska, computer content crimes).

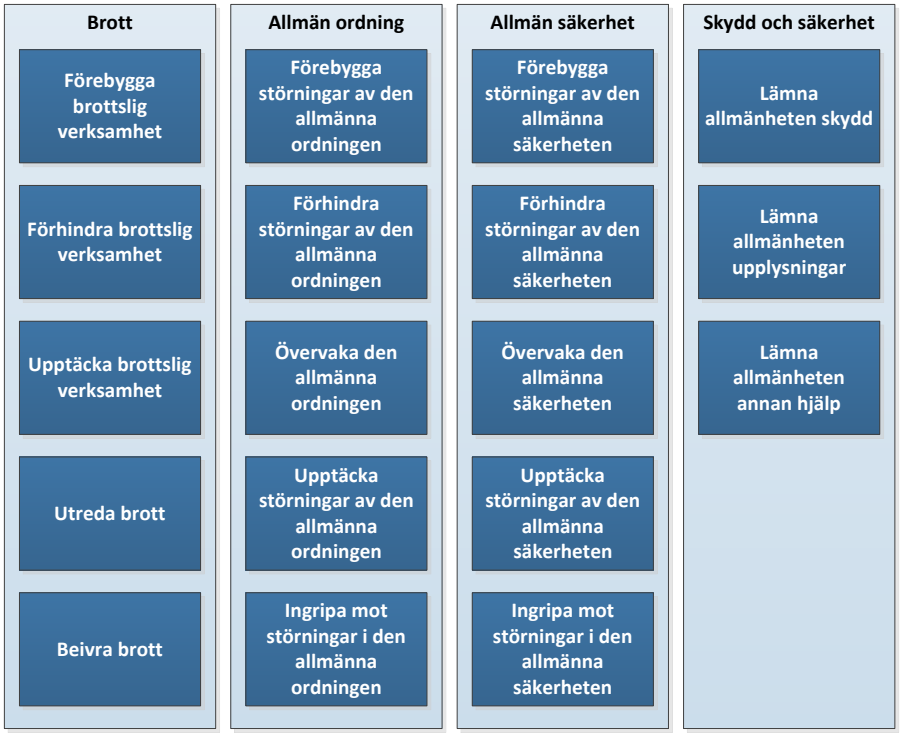
Denna definition innebär att IT-relaterad brottslighet är en brottslig handling där informationsteknik antingen är hjälpmedel, en brottsarena eller ett nödvändigt rekvisit för att begå brottet. Den skiljer sig från BRÅs definition i och med att den inte omfattar brott där gärningsmannen har lämnat digitala spår men inte använt informationsteknik för att begå brottet. Riksrevisionens definition har fördelen att den är i linje med polisens definition av IT-relaterad brottslighet (Polisen, 2017a):

"*IT-relaterad brottslighet innebär att it-teknik används för att genomföra olika brott, medan brotten i sig kan vara av vilken brottstyp som helst. Idag är en stor del av alla brottstyper IT-relaterade*."

1.9 Polismyndighetens och Säkerhetspolisens uppgifter och ansvar

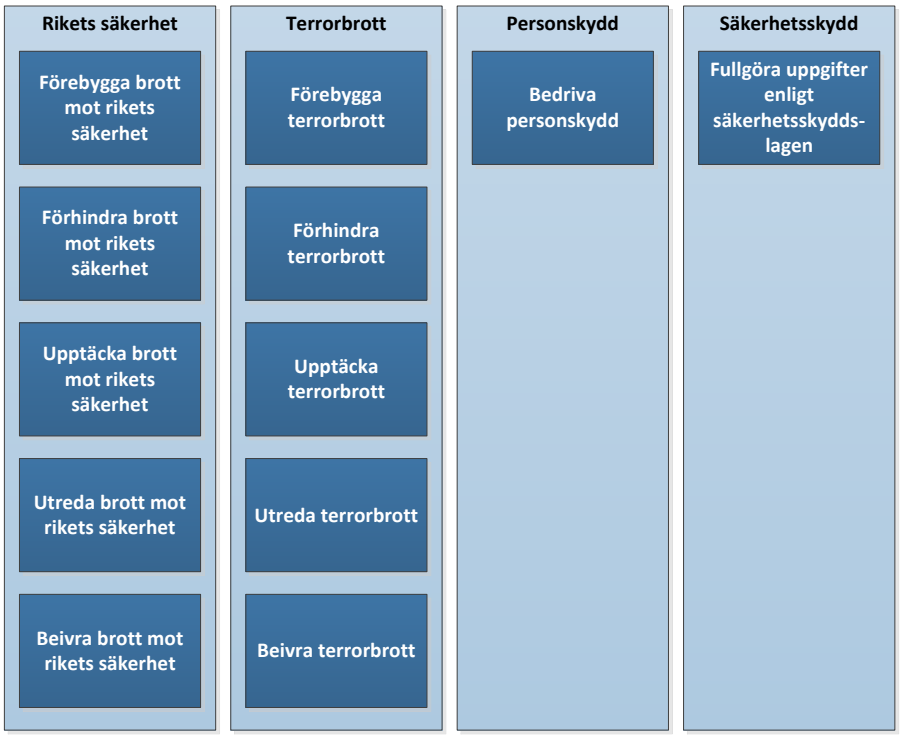
Polisarbete utövas i Sverige av två myndigheter, Polismyndigheten och Säkerhetspolisen. Bägge myndigheternas uppgifter regleras av Polislagen. Även om denna rapport i huvudsak fokuserar på Polismyndighetens verksamhet, den så kallade öppna verksamheten, så utesluter inte det att även Säkerhetspolisens verksamhet omfattas och då det refereras till Polisen så avses bägge myndigheterna.

Polismyndighetens huvudsakliga uppgifter består enligt polislagen i att förebygga, förhindra, upptäcka, utreda och beivra brott samt att förebygga, förhindra, upptäcka och ingripa mot störningar av den allmänna ordningen och säkerheten. Till detta kommer även att övervaka allmän ordning och säkerhet samt att lämna skydd, upplysningar och annan hjälp till allmänheten. (Se Figur 3)



Figur 3 Polismyndighetens primära ansvarsområden och uppgifter

Säkerhetspolisens uppgifter består enligt Polislagen i att förebygga, förhindra, upptäcka, utreda och beivra terrorbrott och brott mot rikets säkerhet samt att skydda statsledningen. Utöver detta så tillkommer även uppgifter som regleras genom annan lagstiftning. (Se Figur 4)



Figur 4 Säkerhetspolisens primära uppgifter (som kan ha bäring på Cyberområdet)

Vad dessa olika uppgifter innebär och hur de löses har mejslats ut under lång tid och hela rättssystemet kännetecknas av en förhållandevis långsam och inkrementell utvecklingsprocess vilket är önskvärt eftersom alltför snabba förändringar skulle skapa bekymmer för såväl privatpersoner som företag och myndigheter. Den snabba tekniska utvecklingen har dock inneburit att rättssystemet inte hunnit med och att avståndet växer sig allt större. Lagen om elektroniska anslagstavlor från 1998 var redan då den kom förhållandevis obsolet eftersom den riktade in sig på BBS:er (Bulletin Board System) där användare kopplade upp sig med modem till en enskild server för att utbyta åsikter och information. Av lagen framgår bland annat att den som tillhandahåller tjänsten ansvarar för att ta bort meddelanden som kan utgöra lagbrott. Vad detta innebär i dagens miljö där miljontals meddelanden hanteras varje minut och tjänster byggs upp av deltjänster som kan vara spridda över flera olika leverantörer och länder är inte helt självklart. Är det den som tillhandahåller mjukvaran, processorkapaciteten eller lagringsutrymmet som ansvarar för tjänsten?

2 Genomförd verksamhet

Fokus för arbetet 2017 var att bygga upp kompetens runt Polismyndighetens och Säkerhetspolisens verksamhet samt att få insikt i vilka utmaningar de står inför vad avser cyberbrott och i förlängningen formulera forskningsfrågor för vidare arbete.

Ursprungligen planerades ett större antal intervjuer med representanter från olika nivåer och avdelningar inom respektive organisation. Efter inledande samtal med representanter från de två organisationerna visade det sig att cyberbrott i dagsläget hanteras centralt och att intervjuer på bredden därför skulle vara av begränsat värde.

2.1 Studerad litteratur

I projektets inledande skede gjordes en översiktlig litteraturstudie i syfte att få överblick över forskningsområdet. Studien resulterade i ett fåtal artiklar med bäring på området samt ett antal rapporter från diverse myndigheter och organisationer (EUROPOL, Brottsförebyggande rådet med flera). Vi gör inte här någon samlad genomgång av de artiklar vi studerat utan dessa refereras till i resten av rapporten på relevanta ställen.

2.2 Möte med Polisen - Nationellt it-brottscentrum (SC3)

Den 16:e juni genomfördes ett inledande möte med Björn Andersson från Nationellt IT-brottscentrum (Swedish Cyber Crime Centre – SC3). Vid mötet redogjorde Björn för Polisens övergripande organisation och ledningsnivåer samt verksamheten vid SC3. Presentationen inkluderade bland annat samarbetet med Europol, Europols publikationer SOCTA (Serious and Organized Crime Threat Assessment) och IOCTA (Internet Organized Crime Threat Assessment) samt de tre projekt (TWINS, CYBORG och TERMINAL) som EUROPOL prioriterar.

Vid mötet framkom även att Regionala IT-brottscentrum är under införande (Regional Cyber Crime Centre – RC3).

Deltagarna i mötet diskuterade även hur FOI skulle kunna stödja Polisen, dock utan att komma fram till några konkreta forskningsfrågor.

Björn har fungerat som kontaktperson vid Polisen under hela projektet och hjälpte bland annat till att organisera webbinariet som hölls i december.

2.3 Möte med Säkerhetspolisen

Den 29:e juni genomfördes ett möte med en representant från Säkerhetspolisen. Vid mötet presenterades mål och syfte för FOI-projektet. Från Säkerhetspolisens sida redogjordes mycket översiktligt för hur internet och social media nyttjas i Säkerhetspolisens arbete. Några tydliga problemområden som skulle kunna adresseras i framtida forskningsprojekt identifierades inte.

2.4 Möte med Marko Forss vid finska polisen

Den 7:e november genomfördes en intervju med Kommissarie Marko Forss vid Helsingforspolisens enhet för grova brott. Marko Forss har tidigare initierat och lett en grupp poliser som verkat på sociala medier genom en form av internetpatrullering (Calcara 2015). Nedan sammanfattas hans tankar och erfarenheter av detta arbete i punktform.

2.4.1 Bakgrund

- Projektet startade 2008 med en profil i ungdomssiten IRC-Galleria (motsvarande enligt Forss ungefär Lunarstorm[2] i Sverige), men hade relativt svagt stöd från sin ledning.
- Fokus för projektet var att lösa brott snarare än marknadsföring och kommunikation med allmänheten. Grundtanken var att använda metodiken från lokal patrullering och applicera den på sociala media.
- Poliserna i projektet använde sina riktiga namn och bilder, dock med en textram runt bilden som tydligt signalerade att de var poliser. Ursprungligen på förslag från de sociala medier man medverkade i, ”Polisen bör också följa mediets regler”. Det visade sig dock vara bra att använda sin egen identitet.
- Poliserna fick en hel del hot via sociala media men de var noggranna med att svara på alla hot och de flesta visade sig vara tomma. Hotnivån upplevdes dock aldrig som svår att hantera. Jämförde med Costa Rica som han nyss besökt. ”En polis som gick ut öppet med sitt namn där hade blivit avrättad inom 24 timmar.”
- Typer av fall som de jobbade med var barnmisshandel, övergrepp på barn, grooming, mobbing och narkotika.
- De vanligaste brotten de kom i kontakt med var mobbing, bedrägerier, förtal och olika former av sexualbrott.
- Nätmobbing är vanligare bland vuxna än bland ungdomar (från en studie den finska polisen gjorde 2011).
- 2011 anmäldes 15% av barnmisshandelsfallen genom sociala media.
- Veckan efter att en artikel om polisens projekt på sociala medier publicerats i en dagstidning (Helsingin Sanomat) så hade polisens profil 35.000 besökare.
- I dagsläget finns ingen organiserad polisverksamhet i Finland på sociala media.

2.4.2 Erfarenheter

- Barns vardagsmiljö kan grovt delas upp i skola, fritid och hemmet. Tidigare kunde barn som på olika sätt for illa i en miljö oftast ta sin tillflykt till en annan av dessa miljöer men sociala media har medfört att gränserna suddas ut.
- Det är enklare att chatta med en polis än att anmäla på en polisstation eller annan traditionell väg. Enligt Forss får man mer information den här vägen, även om gamla fall.
- De viktigaste framgångsfaktorerna var att poliserna som arbetade på sociala media hade gedigen erfarenhet av traditionellt polisarbete och att de använde riktiga identiteter.
- Några konkreta effekter av polisnärvaro på sociala medier är svåra att identifiera men närvaron bedömdes ha en brottsförebyggande effekt.
- Initialt sågs inte polisnärvaro på sociala medier som riktigt polisarbete men efterhand så har det allt mer accepterats.
- Det är svårt, näst intill omöjligt, att tala vuxna människor tillrätta vid olämpligt beteende på sociala media. Att tillrättavisa barn och ungdomar är betydligt enklare.

[2] Webbcommunity som var populärt i Sverige, i huvudsak bland yngre, under 00-talet.

- Kommunikation via sociala media kan vara användbart för att etablera kontakt med personer som har perifer koppling till brottslig verksamhet (exempelvis personer som rör sig i brottsliga kretsar eller vänner och släktingar) men oftast krävs någon form av infiltration för att komma åt organiserad brottslighet.
- Att kombinera sociala media och traditionell patrullering skapade förtroende och stärkte relationerna till allmänheten. Det gjorde det möjligt för framför allt ungdomar att först etablera kontakt med en patrullerande polis och sedan fördjupa kontakten via sociala media och då kommunicera sådant man inte ville eller vågade prata öppet om.
- Den finska polisen utvecklade en säker chat-funktion men den lades ned på grund av låg användningsgrad. Vanliga privata meddelanden via messenger bedömdes av alla inblandade som tillräckligt säkert.
- Provokation med undercover-konton som låtsas vara barn vore en god ide. Är inte tillåtet idag. Forss framhöll Sweetie[3] som ett gott initiativ.
- Den finska polisen fick väldigt många frågor av allmän karaktär via sina konton på sociala media och startade därför en blogg där de vanligaste frågorna diskuterades. Forss hade ett antal standardsvar till vanligt återkommande frågor av typen ”Jag jobbar inte med det och kan inte svara på den typen av frågor”.

2.4.3 Utmaningar

- Det var svårt att komma igång eftersom det saknades stöd från polisledningen. Arbetet på nätet fick drivas som ett sidoprojekt parallellt med ordinarie arbete.
- Resursbrist – I den finska polisen arbetade som mest tre personer med sociala media och Marko Forss kunde få upp till 800 privata meddelande på en vecka.
- Det är för svårt för den finska polisen att få fram IP-adresser. För en husrannsakan krävs misstanke om brott som ger minst 6 månaders fängelse men för att få ut en IP-adress krävs en straffskala med minimum 2 års fängelse.
- Det blir allt svårare att som polis få tillträde till privata grupper i olika sociala media. Forss har dock konstaterat att en enkel förfrågan om medlemskap i slutna grupper förvånansvärt ofta ger positivt resultat.

2.4.4 Tankar och slutsatser

- Polisen kan inte undvika närvaro på sociala media. Redan i dag finns personer som väljer att tillbringa huvuddelen av sina liv i den virtuella miljön snarare än den traditionella.
- För att kunna utforma arbetsmetoderna krävs att man analyserar vilken målgrupp man vill nå, vilka typer av brott man vill komma åt och vilka sajter man vill närvara på.
- Vid polisarbete på sociala media bör arbetet fokusera på barn och ungdomar eftersom det får större förebyggande effekt.
- Det behövs en gemensam plattform för att se vad andra poliser arbetar med, en gemensam operativ lägesbild. Inte sällan visade det sig att information som polisen fick in via sociala media hade bäring på fall som utreddes inom andra delar av poliskåren.

[3] Sweetie är ett projekt som syftar till att med hjälp av en virtuell flicka, identifiera personer som är involverade i barnporr. Projektet organiseras av Terres des Hommes. http://www.terredeshommes.org/

- Vid intervjun med Forss uppfattade vi att det finska polisarbetet på sociala media i hög utsträckning kretsade kring några få personer med hög grad av personligt engagemang. Detta resulterade i att det blev svårt att upprätthålla funktionen då en av de centrala personerna (Forss) gick vidare till andra uppgifter. För att initiativ som initieras underifrån i en organisation ska bli livskraftig och hållbar över tiden är det vår erfarenhet att det krävs att den integreras i ordinarie verksamhet och processer med tydlig förankring i ledningen.

2.5 Deltagande i Polisens seminarium ”Cyberkriminalitet”

Den 8:e november deltog representanter ur projektgruppen i ett polisinternt arbetsmöte som organiserades av Polisens utvecklingschef Anders Hall. Arbetsmötet genomfördes i polishuset på Kungsholmen och ingick i projektet ”Polisen 2024”. Syftet med arbetsmötet var att diskutera vilka utmaningar svensk polis ställs inför på grund av utvecklingen hos cyberbrott samt att ta fram förslag på vad som kan göras för att möta utmaningarna. På agendan stod bland annat att identifiera resursbehov under den kommande sjuårsperioden, att identifiera kompetensbehov inom området samt de viktigaste åtgärderna för att stärka Polisens förmåga inom området.

FOI-projektet har ännu inte kompetens nog att ge några viktigare bidrag i ett arbete av detta slag, men av reaktionerna vi fick efteråt så upplevde mötesdeltagare det som positivt att vi såg verksamheten utifrån och kunde komma med nya idéer och föra in erfarenhet från andra områden.

2.6 Orienterande event för Polisen 19/12

Den 19:e december 2017 anordnades ett webbinarium kallat ”Polis i cyberspace” av FOI och SC3. Webbinariet var uppbyggt kring ett antal exempel på olika typer av IT-relaterade brott och diskussioner kring dessa exempel. De större teman som diskuterades var Polisens ansvar i cyberrymden, Polisens arbete med IT-relaterad brottslighet i dagsläget samt utmaningar med IT-relaterad brottslighet.

En gemensam uppfattning finns om att den generella utbildningsnivån gällande cyber-relaterad brottslighet är alldeles för låg och att cyber ses som ett eget område snarare än en förlängning av samhället. Utbildning behövs över hela organisationen och det anses särskilt viktigt att höja den allmänna kunskapsnivån och se till att det finns en förståelse för cyberaspekterna redan hos den polis som först tar emot anmälan. Ett led i detta arbete är införandet av de regionala IT-brottscentren RC3.

Utredningsmässigt upplever Polisen att dataloggning är av yttersta vikt för att utreda begångna brott. I Sverige upplevs integritetdebatten livligare än i många andra EU-länder och operatörerna upplevs mindre villiga att logga data. En fråga som FOI skulle kunna undersöka är huruvida andra redskap än dataloggar från operatörer kan vara till nytta i utredningsarbetet.

Från Polisens sida efterfrågas bättre verktyg, för exempelvis omvärldsbevakning och spårning av kryptovalutor. De verktyg Polisen har tillgång till nu är kommersiella och släpar ofta efter i utvecklingen. Utveckling av polisiärt inriktade verktyg är ett möjligt område för FOI att bidra inom. På åklagarmyndigheten har man med gott resultat infört en FAQ för cyberfrågor och en liknande funktion efterlyses inom Polisen.

Mängden IT-relaterade bedrägeribrott har växt explosionsartat de senaste åren och det råder en stor obalans mellan brottsvolymen och utredningsinsatserna. Dessa brott sker automatiserat mot ett stort antal brottsoffer. Verktyg för att utföra dessa brott finns att tillgå på kriminella marknadsplatser för brottslingar och verktygen kräver ofta ingen större IT-kompetens. Utredningen av dessa typer av brott anses däremot komplicerad då de ofta

innefattar spårning av kryptovalutor och omfattande internationella kopplingar. Det finns flera faktorer som försvårar utredningsarbetet, såväl resursbrist som juridiska, tekniska och kunskapsmässiga hinder. Följden av detta är att dessa anmälningar ofta läggs ner utan att utredas.

Anonymiteten på internet anses vara ett stort problem, det räcker oftast inte med att ha en IP-adress för att komma i mål med utredningarna. Man måste även kunna knyta en individ till kommunikationen. Både verktyg för anonymisering och spridning av skadlig kod säljs idag som tjänster på internet. Från Polisens sida bör man rikta in sig på de som underlättar dessa brott snarare än att reagera på effekterna av dem.

3 Resultat

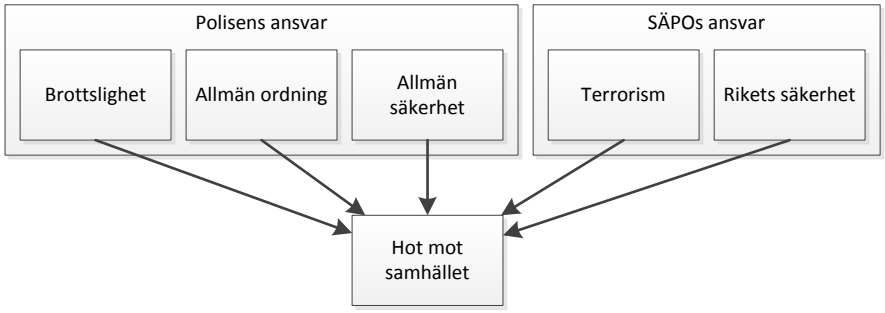
I detta avsnitt redogörs för de kunskaper, hypoteser och slutsatser som byggts upp och identifierats under projektets gång. Kunskapen bygger både på granskad litteratur och diskussioner inom projektgruppen.

3.1 Polisiära utmaningar i det elektroniska samhället

Den fulla vidden av det uppkopplade samhället och dess påverkan på Polisens verksamhet är svår att överblicka och förutsäga men det går att formulera generella frågeställningar. Grundfrågan är vad Polisens uppgifter och ansvar faktiskt består i och denna fråga kan sedan brytas ned i hur uppgifterna ska lösas och vilka verktyg som behövs (se Figur 5).

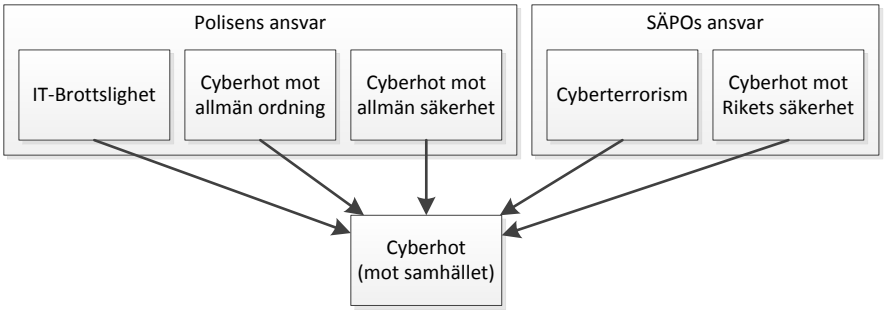
Figur 5 Tre centrala frågeställningar och deras inbördes beroenden

Polisen och säkerhetspolisen har till uppgift att förebygga, förhindra, upptäcka, utreda och beivra olika slags aktiviteter som kan utgöra någon form av hot mot samhället (se Figur 6).



Figur 6 Polismyndighetens och Säkerhetspolisens primära ansvarsområden

Om man mot bakgrund av detta applicerar ett slags ”cyber-filter” så kan uppgifterna omformuleras så att de får en tydligare cyber-koppling (se Figur 7).



Figur 7 Polismyndighetens och Säkerhetspolisens primära ansvarsområden ur ett cyberperspektiv

3.2 Identifierade utmaningar för polisarbete i cyberspace

3.2.1 Automatisering

Många typer av cyberbrott, tydligast bedrägeribrott, sker som automatiserade angrepp mot ett stort antal brottsoffer. Arbetsinsatsen som krävs för att genomföra varje enskilt brott i en sådan attack är således liten. Om dessa brott anmäls till Polisen krävs då stora resurser för att utreda alla dessa brott eftersom det arbetet inte kan automatiseras på samma sätt. Automatisering lämpar sig väl för många aktiviteter i cyberrymden och en utmaning för Polisen är att reda ut hur och när man bör använda sig automatisering för att minska resursövertaget för de som begår cyberbrott. Detta är ett relevant område att undersöka för såväl förebyggande arbete, spaning som utredning.

3.2.2 Beroende av kommersiella verktyg

Polisen använder eller är på väg att införa ett antal verktyg för bland annat informationsinhämtning, och spårning av bitcoin. Dessa verktyg utvecklas av kommersiella aktörer och en åsikt som lyftes fram under det orienterande evenemanget för Polisen 19/12-2017 var att verktygen hinner bli omoderna innan de är klara att föras in i organisationen. Idag sker en mycket snabb utveckling av bland annat skadlig kod, anonymiseringstjänster och svårspårade kryptovalutor och Polisen behöver spanings- och utredningsverktyg som följer den utvecklingen. Man behöver både en egen utveckling och ett snabbare införande av tillfälliga verktyg för enskilda fall.

3.2.3 Anonymiseringsverktyg

Anonymisering online upplevs från Polisens sida som ett stort och växande problem som i hög grad försvårar utredning av cyber-relaterad brottslighet. En uppfattning som råder är det är mycket lättare att förbli anonym online jämfört med i den fysiska verkligheten. Å andra sidan lämnar en person som är aktiv online mycket spår efter sig. Det är möjligt att problemen med anonymisering upplevs som stora för att man saknar kunskap och/eller verktyg för att avanonymisera alias och ekonomiska transaktioner online.

3.2.4 Behov av utbildning

Polisens utbildning fokuserar framför allt på juridik, trafik och förmågan att hantera människor vilket förbereder dem för traditionellt polisarbete som patrullering och utryckning på olika slags larm. Polisens organisation är stor och den allmänna IT-kompetensen är mycket blandad. Flera av de poliser projektet varit i kontakt med pekar på behovet av breddutbildning för att möta den förskjutning mot cyberbrott som håller på att

ske. Det behövs en grundläggande kunskap om cyberbrott för att kunna ta emot och utreda anmälningar om cyberbrott.

3.3 Internationella trender och identifierade behov

Europol producerar rapporter årligen som bedömer utvecklingen av organiserad brottslighet på internet ”Internet organised crime threat assessment (IOCTA)”. Syftet med dessa rapporter är att kartlägga trender inom organiserad brottslighet med koppling till internet och föreslå prioriterade områden och åtgärder. I den senaste utgåvan (IOCTA 2017) delar man in den cyber-relaterade organiserade brottsligheten i fyra prioriterade områden. Förutom dessa specifika typer av cyberbrott beskrivs även en rad möjliggörande faktorer (eng. *Cross-cutting crime factors*) som kraftigt påverkar utvecklingen av cyberhot och möjliggör organiserad cyberbrottslighet.

3.3.1 Möjliggörare

Ett antal, i huvudsak tekniska, faktorer har en stor påverkan på utvecklingen av cyberhot. Dessa faktorer behöver dock i sig inte vara kriminella. Cyberkriminella använder sig i ökande grad av anonymiseringsverktyg och kryptering för att dölja sina förehavanden. De vanligaste verktygen för anonymisering är enkla proxy-lösningar[4], följt av TOR[5] och virtuella privata nätverk[6] (VPN). Alla dessa verktyg är i grunden utvecklade för att öka säkerheten och skydda integriteten hos användaren, exempelvis för personer som lever under förtryck och censur.

Kryptering i olika former är å ena sidan ett oumbärligt verktyg för att garantera säkerheten på internet, å andra sidan döljer sig kriminella i ökande omfattning bakom kryptering. Allt fler kommersiella kommunikationstjänster implementerar end-to-end kryptering för att öka integriteten för dess användare och därmed ökar även användningen bland kriminella av denna typ av tjänster. Kommunikationstjänster med end-to-end kryptering är en klart försvårande omständighet i utredningsarbetet. Rekommendationerna från Europols sida är att polismyndigheter följer trender kring vilka kommunikationsplattformar som används och tar hjälp av industri och högskolor/universitet för att bredda kompetensen kring vilka utredningsåtgärder som är möjliga för dessa plattformar.

En annan faktor som möjliggör många typer av cyberbrottslighet är användandet av kryptovalutor, i huvudsak bitcoin (IOCTA 2017, 60). Penningtvätt, betalningar brottslingar emellan, lösensummor för ransomware och handel med droger online sker i hög grad med denna typ av valutor. Vikten av att sprida kunskap kring hur bitcoin kan spåras lyfts fram. Även om bitcoin är den klart mest använda kryptovalutan för tillfället utvecklas alternativa valutor som har ytterligare mekanismer som gör transaktioner svåra att spåra.

Något som beskrivs som relativt unikt för cyberbrottslighet är att verktyg för cyberbrottslighet i stor grad erbjuds som tjänster som kan köpas (eng. *Crime-as-a-Service)* (IOCTA 2017, 58). Den tekniska kompetens som krävs för att genomföra överbelastningsattacker, bygga upp och kontrollera bot-nät eller utveckla skadlig kod behöver därmed bara byggas upp hos ett fåtal individer. Därmed menar författarna att avståndet minskar mellan erfarna brottslingar och de som är i början av sin brottsliga bana.

[4] En proxy-lösning innebär att kommunikation sker via en mellanliggande server i syfte att dölja den faktiska avsändaren.

[5] The Onion Router (TOR) är ett verktyg som leder internettrafik genom nätverk av noder vilket försvårar spårning av sändare och mottagare.

[6] Virtuella privata nätverk är en teknik för att realisera privata nätverk över ett publikt nätverk, med hjälp av exempelvis kryptering.

Dessa tjänster erbjuds i huvudsak på kriminella forum på *darknet-marknader*[7], som är en illegal marknad enbart åtkomlig via TOR.

3.3.2 Cyber-dependent crimes (Cyberberoende brott)

Detta prioriterade område inkluderar brott som inte existerar alls utanför cyberdomänen. Till denna typ av brott räknar Europol spridning av skadlig kod, cyberattacker mot kritisk infrastruktur, nätverksattacker, Distributed Denial of Service (DDoS) samt nätverksintrång. Förekomsten av ransomware-attacker har ökat de senaste åren och utgjorde 2017 den mest spridda formen av skadlig kod sett till omfattning och skada. Ransomware uppvisar i stort sett alla aspekter av komplex cyberbrottslighet; elakartad användning av kryptering, betalning av lösensummor med hjälp av bitcoin, stora inkomster genereras från ett stort antal mindre transaktioner och själva attackerna erbjuds i ökande grad som tjänster på darknet. Störst uppmärksamhet fick *WannaCry* som under Maj 2017 beräknas ha drabbat 300 000 offer i 150 länder (IOCTA 2017, 19) och drabbat allt ifrån privatpersoner till sjukhus, telekommunikationsföretag och järnvägsbolag (IOCTA 2017, 26).

Överbelastningsattacker fortsätter att utgöra ett hot. Trenden med uppkopplade smarta prylar (Internet of Things) leder till en hög tillgänglighet av uppkopplade prylar med i bästa fall bristfälliga säkerhetslösningar. Den största attacken av denna typ, *Mirai,* utnyttjade bland annat gamla routrar (IOCTA 2017, 26). Källkoden för Mirai publicerades öppet och fler attacker som direkt använder eller bygger vidare på källkoden är att vänta.

3.3.3 Child sexual exploitation online (Sexuellt utnyttjande av barn online)

Peer-2-peer-nätverk är den huvudsakliga kanalen för spridning av material, dock sker även delning av material i ökande grad på kommersiella tjänster för mediadelning. En anledning är att allt fler av dessa tjänster erbjuder end-to-end kryptering[8]. Även slutna grupper på darknet för delning av material och metoder för anonymisering blir allt vanligare. Generellt är användandet av kryptering och anonymiseringstjänster mycket utbrett inom detta område (IOCTA 2017, 39).

Mängden material ökar snabbt, en enskild utredning kan inkludera flera terabyte med bilder och videomaterial som behöver analyseras. Det är inte möjligt att manuellt granska sådana stora mängder material utan här behöver polismyndigheter använda sig av utvecklingen inom automatisk bildanalys och klassificering.

3.3.4 Payment fraud (Kortbedrägerier)

Kortbedrägerier fortsätter vara ett omfattande cyberhot, bara i november 2017 anmäldes över 20 000 fall (Polisen 2017b). Kortbedrägerier delas typiskt upp i två typer beroende på om bedrägeriet kräver fysisk tillgång till kortet eller ej. Bedrägerier som kräver fysisk tillgång till betalkort, exempelvis skimming, är på nedgång. Övergången till att använda chip i betalkorten och geografisk blockering gör denna typ av bedrägerier svårare att genomföra.

Bedrägerier utan fysik tillgång till betalkortet (eng. *Card-not-present fraud*) utgör majoriteten av anmälda bedrägerier i Sverige (Polisen 2017b). Kriminella organisationer använder sig i stor utsträckning av stulna kort för att köpa flygbiljetter. Detta agerar som en möjliggörare för människo- och drogsmuggling (IOCTA 2017, 43).

[7] Darknet-marknader är en typ av marknadsplatser för illegala varor som existerar utanför det öppna internet (surface web) och åtkomst kräver speciell programvara, exempelvis TOR (IOCTA 2017, s. 49)

[8] End-to-end-kryptering innebär att ett meddelande krypteras hos sändaren och förblir krypterat hela vägen till mottagaren.

Till skillnad från annan cyberbrottslighet noteras bland kortbedrägerier en tillbakagång till mer lågteknologiska attackvektorer, så som social manipulering och infekterade bilagor i e-post.

3.3.5 Online criminal markets (Kriminell näthandel)

Handel med illegala varor, i huvudsak droger, på marknader på darknet fortsätter att öka. Försäljning av narkotiska preparat som ännu inte drogklassats sker i huvudsak på det öppna nätet. När preparaten klassats som droger migrerar försäljningen av dessa preparat till kriminella marknader på darknet. Drogförsäljning på internet är en förutsättning för organiserade brottslingar att bekosta andra kriminella aktiviteter.

4 Diskussion

I det här kapitlet diskuteras de aspekter av cyberbrott som framträtt tydligast under det första årets arbete.

4.1 Cyberbrott – nya typer av brott eller gamla brott i ny förpackning?

Vad är egentligen cyberbrott? Är det en helt ny kategori av brott eller är det helt enkelt traditionella brott som begås med nya medel? Ska man betrakta cyberbrott som ett unikt polisiärt område eller är det snarare ett perspektiv på brottslighet som återfinns inom de traditionella områdena? Hur bör rättsvårdande organisationer organisera sig för att på bästa sätt bekämpa cyberbrott? Ibland beskrivs cyberdomänen som ett eget polisområde och polisarbete i cyberdomänen jämförs med lokalpolisens patrullering i ett distrikt men kanske är detta mest ett tecken på att området fortfarande är omoget. Inom exempelvis ekonomisk brottslighet har elektroniska överföringar länge varit vanligt och det förekommer inga diskussioner om att pappersbaserad och elektronisk brottslighet skulle vara olika.

4.2 Möjligheter att förebygga och förhindra cyberbrott

En unik egenskap i cyberdomänen är att i princip all information finns tillgänglig under alla faser i ett brott. Ofta finns information om såväl förberedelser som genomförande och kvarvarande spår. Rent hypotetiskt innebär detta att möjligheterna att upptäcka brottsförberedelser och förhindra att brott begås aldrig varit så stora som i dag. Dessutom skulle kostnaderna för att sammanställa och analysera stora mängder information som skulle kunna innehålla brottsförberedelser bara vara en bråkdel av kostnaderna för traditionell informationsinhämtning. Dock skulle en sådan övervakning kunna innebära stora inskränkningar av den personliga integriteten vilket är en känslig fråga. Utvecklingen av metoder och verktyg för att upptäcka och förhindra brott i cyberdomänen går därför långsamt.

4.3 Nya metoder och verktyg

Även om cyberbrott till stor del handlar om traditionella brott så innebär inte det att traditionella polisiära metoder och verktyg alltid kan tillämpas i brottsbekämpningen. Eftersom cyberbrott i grunden bygger på de möjligheter som IT erbjuder så behöver även brottsbekämpningen anpassas till IT-domänen. I dagsläget finns en rad begränsningar i hur polismyndigheterna får agera i IT-domänen men dessa begränsningar bygger till stor del på den traditionellt analoga världen och tar därför inte hänsyn till de tekniska möjligheter som finns att tillgå. Ett exempel på detta är en teknik där man tidigt anonymiserar data och först efter konstaterat brott och särskilt beslut får tillgång till information som kan identifiera en förövare. I stället för att kartlägga individers rörelser och beteende så skulle det gå att först identifiera en brottslig händelse och därefter identifiera förövaren, ungefär som vid en hastighetskontroll.

5 Förslag till fortsatt arbete

År 2 genomförs fortsatt arbete enligt kring de frågor och aspekter som framträtt under arbetes gång med särskilt fokus på utveckling av robust kompetens inom området. Verksamhet som planeras är:

a) Utbildningsinsats i form av 2-4 webbinarier.

b) En artikel i Polistidningen för att orientera om projektet.

c) En studie som syftar till att sammanställa aktuella cyberhot och cyberbrott samt en analys av tekniska möjligheter att möta dessa.

d) Fortsatta litteraturstudier och kartläggning av forskningsområdet.

5.1 Frågor som bör undersökas

a) Vilka cyberbrottsproblem bör FOI satsa på att forska inom? Vad är det som definierar cyberbrott som forskningsområde?

b) Hur förhåller sig Polisens cyberansvar till andra myndigheter? Hur ser gränsdragningen ut?

c) Vilka tekniska möjligheter finns att förhindra och bekämpa cyberhot och cyberbrott?

d) Vilka kompetenser och verktyg behöver utvecklas, och i vilken omfattning, för att möta dessa cyberhot och cyberbrott?

Referenser

Bossler, A. M. & Holt, T. J. (2013) Assessing officer perceptions and support for online community policing, *Security Journal*, Vol. 26, s. 349-366, Macmillan Publishers Ltd.

Brå, (2017), *IT-inslag i brottsligheten och rättsväsendets förmåga att hantera dem*, s. 19–20.

Calcara, G., et al (2015) The Finnish Internet Police (Nettipoliise): towards the development of a real cyber police, *European Journal of Law and Technology*, Vol 6, No 2, Belfast

Europol (2016) *IOCTA2016: Internet Organised Crime Threat Assessment*, The Hague : European Police Office, DOI 10.2813/275589

Europol (2017) *IOCTA2017: Internet Organised Crime Threat Assessment*, The Hague : European Police Office, DOI 10.2813/55735

Jardine, E. (2015) *The Dark Web Dilemma: Tor, Anonymity and online Policing (Global Commission on Internet Governance Paper Series: No21)*. Centre for International Governance Innovation and The Royal Institute for International Affairs.

Klimburg, A. (Ed.), (2012) *National Cyber Security Framework Manual*, NATO CCD COE Publication

Mayer, M., Martino, L., Mazurier, P., Tzvetkova, G. (2014) How would you define Cyberspace?, First Draft Pisa, [Senast besökt 2018-01-16]

Neale, M. (Director) (2000) *No Maps for These Territories* [Film].

Polisen, (2017), https://polisen.se/Om-polisen/Olika-typer-av-brott/IT-brott/ [senast besökt 2017-11-27]

Polisen (2017) *Intressant just nu om bedrägerier*, Nationellt bedrägericenter, Dnr: A116.272/2015

RIR 2015:21, *It-relaterad brottslighet - polis och åklagare kan bli effektivare*, s. 17–18

Stakston, B. (2013) *Utvärdering Polisens närvaro i sociala medier*, Rikspolisstyrelsen, Dnr: A033.554/2013

Svenska datatermgruppen, (2016), http://www.datatermgruppen.se/ordlista.html [senast besökt 2018-03-06]

Wall, D.S. (2005/15) The Internet as a Conduit for Criminals, s.77–98 in Pattavina, A. (ed) *Information and Technology and the Criminal Justice System*, Thousand Oaks, CA: Sage (Chapter revised August 2015 – see Postscripts)

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

Wedlin, M. (2011), *Informationsarenan och Cyberspace som begrepp*, FOI-R--3157--SE, Totalförsvarets Forskningsinstitut

ISSN 1650-1942

www.foi.se