Polisiära cyberhot

Tekniska möjligheter

MIKAEL WEDLIN, PETER NILSSON, ARWID KOMULAINEN, FARZAD KAMRANI,
JONATHAN SVENSSON, MIKAEL KRONA, JOHAN BENGTSSON

FOI-R--4739--SE
ISSN 1650-1942 Februari 2019

Mikael Wedlin, Peter Nilsson, Arwid Komulainen, Farzad Kamrani, Jonathan Svensson, Mikael Krona, Johan Bengtsson

Polisiära cyberhot

Tekniska möjligheter

Titel	Polisiära cyberhot
Title	Police Cyber Threats
Rapportnr/Report no	FOI-R--4739--SE
Månad/Month	Februari
Utgivningsår/Year Sidor/	2019
Pages	55 p
Kund/Customer	Polisen
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	A74002
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Bild/Cover: Mikael Wedlin / FOI

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Internets utveckling har skett i en rasande takt och sällan har en teknisk innovation fått så stor spridning på så kort tid. I dag beräknas internet ha mer än 4,3 miljarder användare[1]. Nätet erbjuder unika möjligheter att kommunicera och hantera information, men som alltid finns det grupper som missbrukar möjligheterna för kriminella syften.

I denna studie har vi utgått från de områden som beskrivs i Europols årliga IOCTA-rapport och studerat dem djupare. Vi har även intervjuat personal från Polisen och åklagarmyndigheten för att få deras syn på cyberkriminalitet. Slutligen har vi följt upp ett antal anmälningar av brott med cyberanknytning.

I rapporten ges förslag på hur delar av cyberbrottsligheten kan adresseras samt ett antal förslag till fortsatt forskning.

Nyckelord: Cyberhot, cyberbrott, nätbrott

[1] https://www.internetworldstats.com/stats.htm

Summary

The internet has developed at an explosive rate. The spread of a technical innovation in such a short period of time is almost unprecedented. Currently, it is estimated that the internet has 4.3 billion users. The web offers unique possibilities for communication and information handling, but there are groups that abuse these possibilities for criminal purposes.

This study is based on the areas described in the annual Europol IOCTA report, which were studied more closely. Interviews were also conducted with members of the police force and the Swedish prosecution authority in order to obtain their views on cybercrime. Finally, a number of reported cybercrimes were followed up.

The present report contains suggestions on how to address some areas of cybercrime, as well as ideas for future research.

Keywords: cyber threats, cybercrime, internet crime

Innehåll

1 Inledning 9

1.1 Projektet ... 10

1.2 Rapportens upplägg ... 10

2 Allmänt om kryptovaluta 11

2.1 Bitcoin ... 11

2.2 Anonymitet ... 13

2.3 Olika sätt att reducera anonymitet ... 16

3 IT-relaterade brott 17

3.1 Sexuell exploatering av barn på nätet ... 17

3.1.1 Artificiell intelligens - möjlighet eller hot? ... 17
3.1.2 Bildanalys med hjälp av AI ... 18
3.1.3 Sårbarheten i AI-system ... 18
3.1.4 *Djupförfalskning* ... 18

3.2 Kriminella marknadsplatser på nätet ... 19

3.3 Bedrägeri på nätet ... 20

3.4 Cyberterrorism ... 21

4 Studie av hot via massmail 24

4.1 Metod ... 25

4.2 Kontakt med Polisen ... 26

4.3 Mailets innehåll ... 29

4.4 IT-säkerhetsinformation ... 30

4.5 Bitcoin-mottagare ... 31

4.6 Sammanfattande reflektioner av fallstudien ... 33

5 Intervjuer med polis och åklagare i Malmö 34

5.1 Allmän attityd ... 34

5.2 Förebyggande och upplysande verksamhet ... 34

5.3 Kommunikation med allmänheten ... 34

5.4 Upptäckt av brott ... 35

5.5 Ta upp anmälan ... 35

5.6 Brottsrubricering och klassificering ... 35

5.7 Utreda IT-relaterade brott ... 35

5.8 IT-relaterade brott i domstol ... 36

5.9 Utbildning, kompetens och utveckling ... 36

5.10 Övriga kommentarer ... 37

6 Intervju på NOA SC3 i Stockholm 38

6.1 Allmän attityd ... 38
6.2 Allmänna observationer ... 39
6.3 Kommunikation med allmänheten ... 39
6.4 Säkring av digitala bevis ... 39
6.5 Ta upp anmälan ... 40
6.6 Brottsrubricering och klassificering ... 40
6.7 Utbildning, kompetens och utveckling ... 40
6.8 Övriga kommentarer ... 41

7 Brottsbekämpning på internet 42
7.1 Sexuellt utnyttjande av barn på nätet ... 42
7.2 Infiltration online ... 44
7.3 Kryptovaluta ... 44

8 Rekommendationer 45
8.1 Utbildning ... 45
8.2 Teknikstöd ... 45
8.3 Förändrad metodik ... 46

9 Referenser 47

Bilaga 1 - Intervjumanus 50

Bilaga 2 - Resultatrapport från Xamera 52

Förord

Detta är slutrapporten för det tvåårigа projektet ”Polisiära cyberhot, en förstudie”. Även om flera av projektmedlemmarna tidigare har genomfört projekt åt och med Polismyndigheten och Säkerhetspolisen, så har FOI tidigare haft begränsad kunskap om hur polisarbete går till. Efter det här projektet är FOI betydligt bättre rustat att stödja dessa två myndigheter när det gäller hot och risker som manifesteras via internet.

Jag skulle också vilja ta tillfället i akt att skicka ett tack till alla er som har hjälpt till med framställandet av denna rapport.

Tack till Polismyndigheten och Säkerhetspolisen för er tid och ert engagemang för att hjälpa oss förstå. Ett speciellt tack skulle jag vilja skicka till våra kontaktpersoner Björn Andersson och Göran Garpensved vid SC3.

Tack också till Patrik Lundin, Patrik Bengtsson, Sebastian Nielsen, Joel Brandell och de övriga 18 personerna som ställde upp och polisanmälde de hotfulla breven och delade med er av de erfarenheter det gav.

Mikael Wedlin

Projektledare

1 Inledning

Boktryckarkonsten och informationssamhället, manifesterat i internet, är två stora milstolpar i mänsklighetens historia som helt förändrat samhällsvillkoren. Boktryckarkonstens betydelse är relativt allmän kunskap (Eisenstein 1968), men med internet befinner vi oss mitt i förändringen. Man skulle dock redan nu kunna hävda att informationssamhället är ett ännu större steg än boktryckarkonsten. Det finns idag nästan ingen verksamhet som inte innehåller nätverkskopplade enheter såsom datorer eller telefoner.

Några av de saker informationssamhället har byggt vidare på från boktryckarkonsten är att ha:

1) Gett alla människor i princip omedelbar tillgång till stora mängder information.
2) Gett alla människor möjlighet att obegränsat sprida tankar och åsikter, vilket exempelvis kan ske via sociala medier. I Sverige är det vanligare att använda sociala medier än att inte göra det (Internetstiftelsen 2018). Ett annat exempel är att en medelmåttig mobiltelefon i stort sett är det enda som krävs för att starta egen videoproduktion, likt en tv-station.
3) Skapat en sant global miljö där nationalstatens betydelse kraftigt har minskat, t.ex. gällande handel med varor och tjänster. Det är lika lätt att beställa en elektronikprodukt från ett kinesiskt företag som från ett svenskt. Även grupptillhörigheter har blivit mer globala när möjligheterna att kommunicera inte längre är beroende av fysiskt avstånd.

Gutenbergs tryckpress skapade inte omedelbart dagens dagstidningar utan förändringen i samhället skedde genom en gradvis utveckling under flera sekler. Den gradvisa förändringen över en längre tidsperiod innebar även att olika delar av samhället kunde anpassa sig gradvis. Informationssamhället håller, vid jämförelse med boktryckarkonsten, en extremt hög utvecklingstakt då stora förändringar har skett på enbart ett par decennier.

Den höga utvecklingstakten av informationssamhället innebär även att samhällsapparaten behöver hantera förutsättningar som snabbt förändras. I lagstiftningssammanhang kan dessa snabba förändringar bli problematiska då det krävs god eftertanke för att kunna överblicka möjliga konsekvenser av förändrade lagar. Att å andra sidan inte anpassa lagstiftningen i takt med att samhället förändras kan innebära att lagar som en gång stiftades i en viss samhällskontext kan bli helt verkanslösa, alternativt vara tillämpbara i sammanhang som det inte alls var tänkt då lagen stiftades.

När brottslighet genomförs via internet tydliggörs att rättsskipning, av tradition, är en verksamhet som är hårt knuten till nationalstaten, samtidigt som internet inte känner några geografiska gränser. Den som står bakom ett brott kan således befinna sig i, och utföra brottet från, ett land som har annan lagstiftning än landet där den som utsätts för brottet befinner sig i. Svårigheter kan då uppstå med att lyckas lagföra någon för brottet.

1.1 Projektet

Under en tvåårsperiod har projektet *Polisiära cyberhot, en förstudie* genomförts på FOI i syfte att bygga upp kunskap kring IT-relaterad brottslighet. Bakgrunden till projektet var att det på FOI fanns behov av att få en bättre förståelse för vilka typer av brott som genomförs via internet samt hur dessa brott i dagsläget hanteras av den svenska rättsapparaten. Med en bättre förståelse kring nuläget förbättras förutsättningarna för FOI att kunna stödja relevanta myndigheter i deras arbete med att hantera IT-relaterad brottslighet.

För att få en förståelse för hur de IT-relaterade brotten hanteras genom hela den process som utgör rättsapparaten var det nödvändigt att genomföra studien utifrån flera av de inblandade parternas perspektiv. Det som initierar rättsapparaten är att det upprättas en polisanmälan, troligtvis av den som har utsatts för brottet. Det var därför nödvändigt att även undersöka hur den som anmäler ett IT-relaterat brott bemöts och hur denne upplever hela processen. Avseende rättsapparaten beskrivs IT-relaterade brott både ur polisens och ur åklagarens perspektiv för att få en förståelse för deras arbetssituation och hur de påverkas av informationssamhällets snabba utvecklingstakt.

1.2 Rapportens upplägg

Då kryptovaluta är något som dyker upp i flera olika sammanhang i denna rapport och därmed är nödvändig bakgrundskunskap ges en allmän beskrivning av området i kapitel två. Kapitlet kan förbises av de som redan har kunskap om hur kryptovalutor fungerar.

I kapitel tre ges en sammanställning av olika typer av brott som i dagsläget genomförs via internet. Sammanställningen utgår från Europols årliga studie som beskriver trender i organiserad brottslighet som sker via internet.

I kapitel fyra beskrivs en studie av hur polisanmälning av IT-relaterade brott i praktiken hanteras och hur processen upplevs av de som har utsatts för brott. Fokus för studien var hot som distribuerats via massmail.

I kapitel fem beskrivs IT-relaterade brott ur rättsapparatens perspektiv med fokus på utmaningar och möjligheter som internet innebär. Beskrivningen utgår från intervjuer som genomförts med polis och åklagare i Malmö.

I kapitel sex beskrivs IT-relaterade brott ur ett handläggnings- och utredningsperspektiv. Beskrivningen utgår från en intervju som genomfördes med personal på Swedish Cybercrime Center vid Nationella operativa avdelningen.

I kapitel sju ges en beskrivning av den brottsbekämpning som i dagsläget sker för att hantera och motverka brott som sker på internet.

I kapitel åtta ges avslutningsvis rekommendation baserat på den kunskapsbas som byggts upp under de två år projektet pågått.

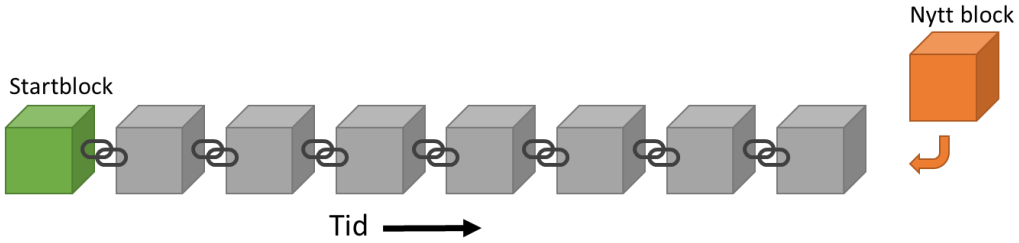
2 Allmänt om kryptovaluta

Kryptovaluta är en digital valuta utan fysisk form, som inte hanteras eller kontrolleras av en centralt reglerande instans (t.ex. stater, företag eller en centralbank som i traditionella banksystem). Dessutom används ett system med kryptografiska metoder för att skydda de transaktioner som genomförs. Kryptovalutor är skapade för att möjliggöra oberoende direkta globala betalningar mellan alla användare av internet utan inblandning från tredje part eller mellanhänder, i syfte att vara skyddad mot t.ex. politisk påverkan eller monopolsystem. Kryptovaluta kan leda till lägre kostnader och högre grad av anonymitet, men riskerna kan vara höga då systemet inte omfattas av lagar och traditionellt konsumentskydd. Det finns flera exempel på fall där stora mängder kryptovaluta försvunnit, antingen genom dataintrång eller helt enkelt genom att förmedlingstjänsterna upphört och de ansvariga försvunnit med pengarna, så kallad *exit-scam*.

2.1 Bitcoin

Det finns över 3000 varianter av kryptovaluta, varav Bitcoin är den äldsta implementationen. Konceptet beskrevs 2008 i en artikel av pseudonymen Satoshi Nakamoto (Nakamoto, 2008). Andra kända större kryptovalutor är t.ex. Ethereum, Bitcoin Cash, Ripple, Dash, Monero, ZCash, IOTA och Litecoin.

Valutan Bitcoin baseras på de tre principerna decentralisering, transparens och irreversibilitet. Systemet som hanterar Bitcoin har ingen central server utan bygger på ett krypterat P2P-nätverk (*peer-to-peer*). Utspritt över de deltagande noderna i nätverket lagras en *blockkedja*, vilket är en gemensam vedertagen databas med historik som loggar samtliga giltiga genomförda transaktioner (Figur 1). Varje block innehåller en logg över en mängd verifierade transaktioner samt deras, enligt systemets algoritmer uträknade, hash-kod. I dagsläget finns ca 550 000 skapade block i kedjan för Bitcoin. Genom att nätverket gemensamt håller reda på och godkänner alla transaktioner med relaterade in- och utadresser kan valuta endast spenderas av dess ägare och bara en gång.



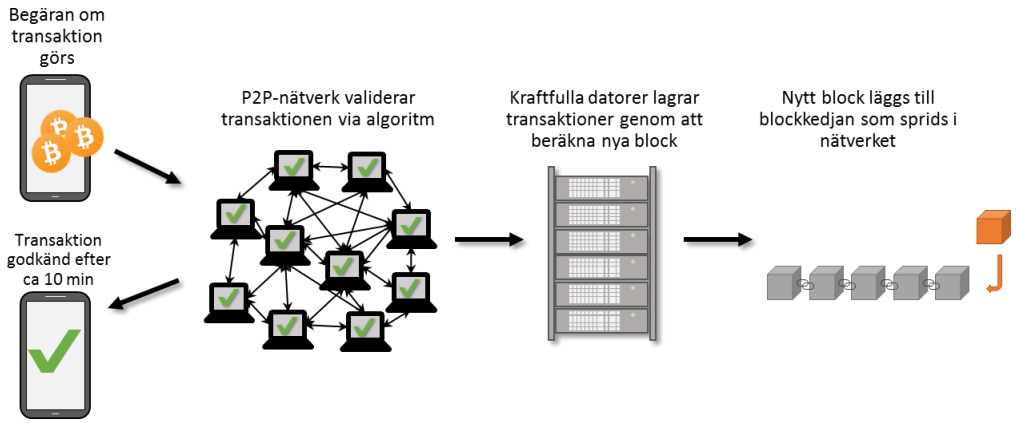
Figur 1. Illustration av blockkedja.

En överföring av Bitcoins görs mellan adresser i form av att en transaktion begärs och verifieras av P2P-nätverket (Figur 2). Adresser och transaktioner representeras i form av långa strängar bokstäver och siffror, exempelvis adressen *1JTtwbvmM7ymByxPYCByVYCwasjH49J3Vj* och transaktionen *597f3870dfdadd29ec4c79aa5cf5f4a813e87a9b756ad4447f8f823cc99e34fc*.

Det tar vanligen ca 10 minuter för en transaktion att få en acceptabel nivå av godkännande från nätverket, men den kan ta upp till en timme att verifiera.

En användare hanterar sina Bitcoins via en ”plånbok”, som innehåller en uppsättning av de Bitcoin-adresser användaren har tillgång till. Plånboksmjukvaran kan ligga på en server eller lokalt på en dator. Genom att logga in på plånboken med lösenord kan användaren se sina tillgångar och begära utgående transaktioner eller skapa nya adresser för inkommande transaktioner. Plånboken innehåller inga Bitcoins i sig, utan summerar automatiskt ihop alla transaktioner gjorda till och från ägarens adresser och presenterar det totala värdet av tillgångarna. Bitcoin-adresser representerar den publika nyckeln i ett asymmetriskt nyckelpar, medan den privata nyckeln som behövs för att signera utgående transaktioner lagras i plånboken (motsvarande nyckelring).

Antalet Bitcoins ökar kontinuerligt genom den belöning som ges för ”brytning” (*mining*), vilket är processen att via alltmer krävande datorberäkningar lagra ett antal nya genomförda verifierade transaktioner som nya block i blockkedjan. Just nu finns ca 17 miljoner Bitcoins tillgängliga, dock är ett tak satt på att max 21 miljoner Bitcoin kommer få existera. Hur skapandet av nya block till blockkedjan kommer ske därefter, då ingen belöning i form av nya Bitcoins ges, är oklart.



Figur 2. Schematisk bild av genomförande av en Bitcoin-transaktion.

Användandet och acceptansen av Bitcoin som valuta är alltjämt relativt låg men växande. Det är en laglig valuta i de flesta länder i Europa, Nordamerika och Sydamerika. Det finns ingen central utgivare av Bitcoin och därmed ingen monetär fordran på någon part. Japan accepterade Bitcoin som valuta i april 2017, men Kina verkar inte komma att följa efter utan motarbetar aktivt brytning av Bitcoin. I Sverige är handel med och brytning av Bitcoin inte momsbelagt, men handeln ska beskattas och lyda under Finansinspektionens regler. Dessutom ska tillgångar kapitalvinstbeskattas (Skatterättsnämnden, 2018). Värdet på Bitcoin varierar genom handel, användande och spekulationer, och dess värde har sin grund i en förväntan att valutan kommer att kunna användas i framtiden. Det finns i nuläget en förväntan kring och efterfrågan av Bitcoin, men värdet varierar och kursen har efter en kraftig stigning under 2017 rasat betydligt under senhösten 2018 (Figur 3). En Bitcoin (1 BTC) var 2018-12-14 kl 09:56 värd ca 3 256 USD, eller 29 659 SEK.

Figur 3. Utveckling av värdet på 1 Bitcoin (BTC) i amerikanska dollar (USD) från december 2017 till november 2018.

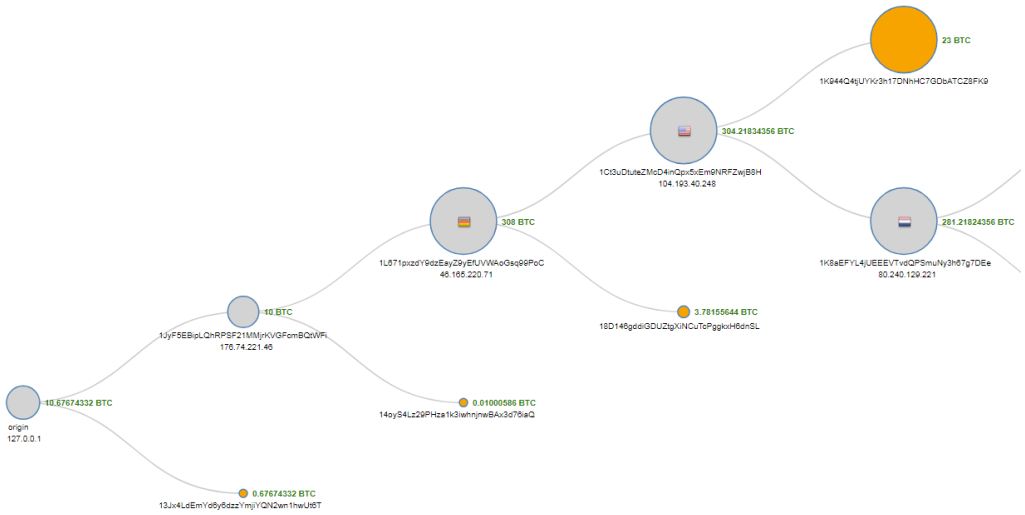
2.2 Anonymitet

Anonymitet i valutasystem kan tjäna både goda och onda syften. När brottslig aktivitet, t.ex. penningtvätt eller köp av illegala varor och tjänster, utförs med stöd av kryptovaluta finns anledning att vilja spåra avsändare och mottagare av medlen.

Bitcoin brukar klassificeras som ett system som är semi-anonymt (*pseudonymous*) på grund av dess mer eller mindre anonyma hantering av transaktioner i P2P-nätverket och att alla händelser i blockkedjan lagras. Trots att Bitcoin-systemet är byggt för att i teorin vara anonymt finns det metoder att i praktiken till en viss nivå koppla identitet till transaktioner och adresser. Med olika former av analys kan relationer synliggöras mellan adresser och transaktioner. Både analys av nätverkstrafik, transaktioner och plånboksmjukvara kan ge ledtrådar till identitet (Andrew och Douglas, 2018).

- Nätverksanalys – följa IP-trafik för att skapa underrättelseinformation.
- Transaktionsanalys – följa överföringar av valuta och associera adresser.
- Plånboksanalys – bearbeta applikationer för hantering av kryptovalutatillgångar och koppla den till specifika överföringar.

En användare kan skaffa flera Bitcoin-adresser som används för transaktioner (något som uppmuntras för ökad integritet) och hantera dessa i virtuella plånböcker på datorn eller via konton hos Bitcoin-tjänsteleverantörer. Det går att finna och visualisera information om Bitcoin-transaktioner via olika webbtjänster, t.ex. blockchain.com (Figur 4) eller walletexplorer.com. Information om adresser och transaktioner kan läcka, göras publika och plockas upp, och genom kombination med öppna källor kan kraftfulla analyser göras. Om en identitet av en adress har röjts, blir alla transaktioner framåt och bakåt förknippade med denna identitet. På sajter som Bitcoinwhoswho.com, hashxp.org eller Bitcoinabuse.com finns det externt inlagd information för ett antal adresser om t.ex. deras förmodade tillhörighet, organisationer de är förknippade med, samt om de förekommit i rapporter om brottslighet eller misstänkt beteende, t.ex. bluffmail.



Figur 4. Exempel på visualisering av en kedja av transaktioner som träddiagram (blockchain.com).

Genom att analysera vilka transaktioner och adresser som hör ihop i blockkedjan kan man skapa grupperingar, kluster, och därigenom sluta sig till att en association av någon sort finns mellan dessa händelser och deras motsvarande fysiska aktörer.

Chang och Svetinovic (2018) beskriver i sin artikel olika transaktionsmönster, två använda heuristiker för klustring av transaktioner[2], samt utvecklar ett angreppssätt som kombinerar gamla och nya metoder för att med större säkerhet kunna hävda att samband finns mellan olika adresser och transaktioner, och vilken nivå av samhörighet olika kluster har. I Remy, Rym och Matthieu (2017) beskrivs vidareutvecklade heuristiker för identifiering av flera adresser som hör till samma användare genom nätverksanalys av typen *community detection.* Harlev m fl (2018) beskriver en ansats att med maskininlärning avanonymisera transaktioner i blockkedjan. Analys av innehåll på Darkweb jämfördes av Jawaheri m.fl. (2018) med öppna källor, och kopplingar mellan Bitcoin-adresser kunde göras.

Även Herrera-Joancomartí (2015) beskriver ett antal tidiga försök till identifiering och gruppering av Bitcoin-användare och liknande arbete har gjorts av Avdoshin och Lazarenko (2018).

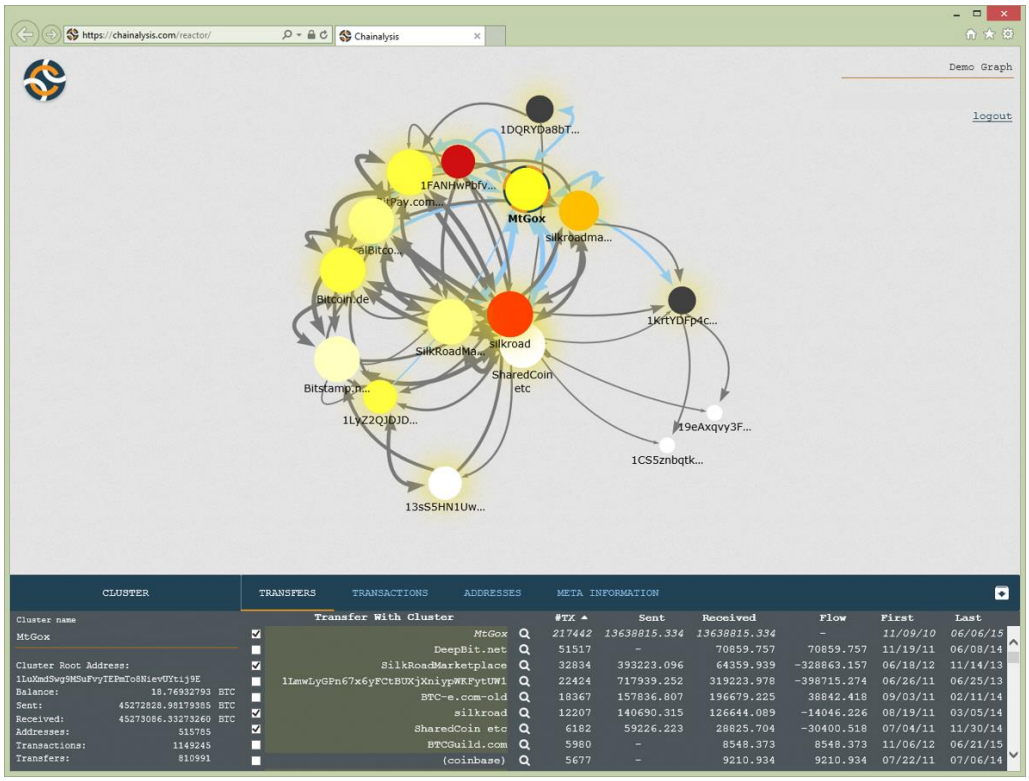
Även om associering mellan plånböcker kan göras är steget till identifiering av ägaren till en plånbok väldigt svårt. Då överföring mellan reguljära valutor och Bitcoin ska göras går användaren vanligen via växlingstjänster, och det finns i USA och Europa krav och reglering rörande identifiering och spårning av pengarnas ursprung. I denna punkt i kedjan är anonymiteten hotad. Transaktioner gjorda till växlingstjänster kan även associeras i storlek och tid till transaktioner gjorda från plånböcker, och på så vis kan identifiering underlättas. När innehavet av valutan ökar sjunker möjligheten att kunna agera obemärkt, och misstag som riskerar att avslöja identiteten kan begås om inte

[2] H1 – alla ingående adresser i en transaktion är associerade med varandra och därmed är framtida adresser som används tillsammans med någon av dessa också associerade; H2 – om en ny adress skapas i en transaktion, vilket sker automatiskt, finns det en mottagare av växelsumman i transaktionen och den hör till avsändaren.

komplexa åtgärder utförs. Sådana åtgärder kan vara invecklade transaktioner som t.ex. reläkonton, distribuering och samling, gemensamma depåtjänster[3], och växling med andra kryptovalutor.

Bedrägerier, *malware*, *ransomware*, *hacking* och *phishing* genom t.ex. *typosquatting* är förekommande, även med inriktning på stöld av cybervaluta. Antalet attacker och kampanjer mot Bitcoin-användare har ökat, särskilt mot användare i länder där det konventionella bankväsendet är dåligt uppbyggt (Holub och O'Connor, 2018). Genom att det inte finns en central garant för tillgångar och det inte går att stoppa eller reversera godkända transaktioner är konsumentskyddet inte lika utbyggt som för konventionell valuta. Om den privata nyckeln för en Bitcoin-plånbok läcker kan vilken användare som helst tömma den på tillgångar.

Företag som exempelvis Chainalysis, Elliptic och Blockseer erbjuder avancerad analys av transaktioner och adresser genom att använda maskininlärning och en kombination av öppna källor och egna databaser över kända adressers innehavare eller associering. Deras tjänster och verktyg används av organisationer och myndigheter globalt för att motverka brottslighet som pengatvätt och illegal handel.



Figur 5. Skärmbild från analysverktyget Chainalysis Reactor.

[3] *mixing*, *shuffling*, *tumbling* – en depå av Bitcoin-resurser som skapar ett mellanled där Bitcoins förs in via en temporär adress, skickas runt i en mängd transaktioner, eventuellt kombineras eller byts ut mot andra orelaterade Bitcoins, och efter en tid levereras ut via en ny temporär adress.

2.3 Olika sätt att reducera anonymitet

Det finns ett antal möjliga vägar att komma åt en användares identitet. Nedanstående lista är några beteenden som ökar sannolikheten för att identiteten kan röjas:

1) En enda Bitcoin-adress används för många transaktioner, vilket gör att olika affärer och användningsområden kan kopplas samman och sannolikheten för röjning ökar.
2) Direkta transaktioner har genomförts, utan depåtjänster som *mixing*/*shuffling*/*tumbling*. Spårning underlättas av att kunna analysera tidsförloppet. Betalningsprocessorer liknande *PayPal* existerar, vilka används som mellanled för betalning till leverantören av en vara eller tjänst.
3) Lösenordet till Bitcoin-plånboken eller dess mjukvara är svagt och plånboken hackas. Volety m.fl. (2018) har funnit att mjukvara för att hantera Bitcoin-plånböcker går att få kontroll över genom brute force-attacker även då datorn inte är ansluten till nätverket.
4) Bitcoin-adress och personlig identitetsinformation har publicerats tillsammans eller läckt ut på nätet, vilket är i princip omöjligt att radera.
5) Växling har skett mot traditionell valuta. Identitet och pengarnas ursprung efterfrågas normalt hos växlingsförmedlaren. Bitcoin kan även köpas genom kontant betalning via t.ex. *LocalBitcoins*.
6) Samma typ av kryptovaluta har använts kontinuerligt utan växling.
7) Produkter som kräver fysisk leveransadress har köpts. Betalning och postadress kan kopplas samman hos butik eller leverantör.
8) Online-plånböcker (*hosted wallet*) har använts, som dels sparar IP-adresser och eventuellt övrig information om identitet, och dels kan röja IP-adresser genom trafiken till dem.
9) Tunna klienter har använts, vilka kan röja IP-adress och Bitcoin-adress vid trafik till SPV-server (*Simplified Payment Verification*), vilket sker vid varje enskild transaktion.
10) Okrypterad internetförbindelse har använts vid trafik som rör transaktioner. Transaktioner skickas normalt via okrypterat protokoll över P2P-nätverket, vilket gör att transaktioner kan identifieras genom analys av trafiken – de transaktioner som först dyker upp via en viss användares IP-adress och inte finns på resterande noder har skapats hos den användaren. Genom att vara delaktig inom P2P-nätverket med flera noder kan man få tillgång till dess trafik och spåra ursprunget.
11) Cookies eller web trackers har tillåtits i webbläsaren, vilka sparar kodsträngar som möjliggör läckage av identitetsinformation och koppling mellan t.ex. ett köp i en webbutik och trafik till en specifik Bitcoin-tjänst.

3 IT-relaterade brott

Europol producerar årligen en analys av organiserad brottslighet online kallad *Internet Organised Crime Threat Assessment* (IOCTA), som beskriver trender inom organiserad cyberbrottslighet. Inom ramen för projektet har 2017 och 2018 års utgåvor av IOCTA studerats i syfte att identifiera problemområden och möjliga tekniska lösningar, samt skapa en djupare insikt om de internetrelaterade utmaningar som brottsbekämpande myndigheter ställs inför. Analysarbetet har skett i en serie interna workshoppar med olika teman. Med utgångspunkt i IOCTA-rapporten har flera olika områden studerats djupare.

3.1 Sexuell exploatering av barn på nätet

Sexuell exploatering av barn på internet är, på grund av den allvarliga graden fysisk och psykisk skada som den orsakar mot en av samhällets mest utsatta grupper, en av de mer allvarliga formerna av cyberbrottslighet.

Även om sexuella övergrepp och utnyttjande av barn förekom även innan interneteran, har nätet gjort det möjligt för brottslingar att effektivare interagera med varandra i cyberrymden samt att producera och distribuera barnpornografiskt material i volymer som inte var möjliga för några år sedan.

Då fler och fler barn har tillgång till internet och ett växande antal sociala medier via mobil, har det blivit möjligt för brottslingar att nå ut till barn på sätt som inte var möjligt tidigare. Enligt svensk lagstiftning är kontakt med barn i sexuellt syfte ett sexualbrott. Även om lagstiftningen är teknikneutral är den starkt relaterad till det ökande användandet av internet. Nätgrooming kännetecknas av att förövaren tar kontakt med minderåriga, oftast med ett fingerat konto på sociala media, och bygger upp ett förtroende för att i ett senare skede utnyttja offren. Den ökade användningen av mobila plattformar har ökat risken för nätgrooming ytterligare eftersom antalet olika sätt att komma i kontakt med barn har ökat.

Nätgrooming kan ha olika ändamål. Även om det förekommer att förövaren arrangerar ett fysiskt möte med barnet i syfte att begå sexuellt övergrepp, är det inte så i majoriteten av fallen. Oftast tvingar förövaren barnen att producera sexuellt laddade bilder och filmer. Detta material används sedan många gånger som ett medel för att utpressa offren och tvinga dem att producera mer material med sexuellt laddat innehåll. Via stängda grupper kan förövaren sprida materialet vidare för ekonomisk vinning, i utbyte mot liknande material eller bara för att förstärka sin position i gruppen.

3.1.1 Artificiell intelligens - möjlighet eller hot?

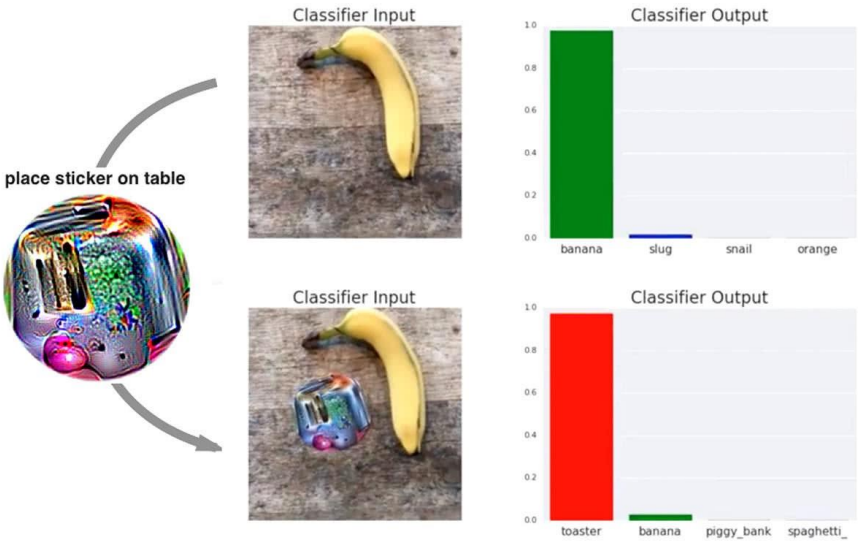
På senare år har utvecklingen av artificiell intelligens (AI) och specifikt djupinlärning ökat markant. Vilka konsekvenser kan detta ha för brottet sexuell exploatering av barn på internet? Vad är möjligheterna och riskerna med de nya tekniker och applikationer som framväxten av AI ger upphov till. Dessa frågor kommer översiktligt att behandlas i det följande avsnittet.

3.1.2 Bildanalys med hjälp av AI

När polisen utreder sexuell exploatering av barn på internet kan de behöva gå igenom miljontals filer, vilket både är tidskrävande och påfrestande för dem som ska utföra uppgiften. Artificiell intelligens kan för närvarande (eller inom en snar framtid) erbjuda effektivare hantering av bild- och videomaterial relaterade till sexuell exploatering av barn. Sortering, klassificering, offerigenkänning och matchning av miljöer där brott har begåtts är olika typer av analyser där djupinlärning under senare år blivit allt mer effektiv och träffsäker. Det finns för närvarande inte några färdiga skräddarsydda produkter att anskaffa på marknaden för att hantera olika uppgifter relaterade till barnpornografibrott, men det skulle vara möjligt att utveckla och träna specifika modeller för ändamålet. Modellerna behöver dock förbättras och utvecklas kontinuerligt, allteftersom nyare teknik och mer data blir tillgängliga.

3.1.3 Sårbarheten i AI-system

Trots att bildanalystekniken har haft stora framgångar tack vare djupinlärning, finns det risker som måste beaktas vid användningen av sådana programvaror. Forskning har visat att djupa neuronnät kan vilseledas oavsett om modellen är känd eller okänd för den som attackerar den (Athalye, 2018)(Figur 1). Tekniskt är det fullt möjligt att maskera bilder så att de blir helt felklassificerade genom att ändra en eller några få pixlar. Detta är neuronnätens akilleshäl som kan utnyttjas om någon vill maskera bilder så att de passerar bildanalysprogrammen obemärkt. Att råda bot på svagheter i modellerna är en het fråga som utgör en av forskningsfronterna inom djupinlärning.

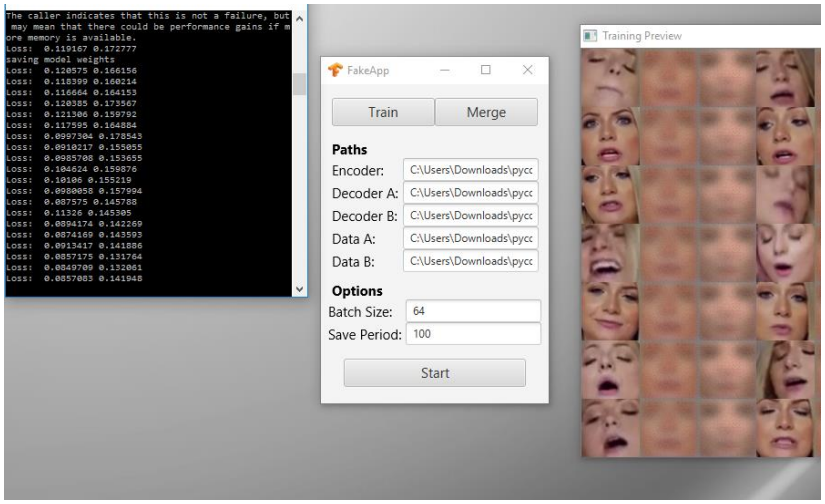


Figur 6. Ett neuralt nät kan luras så att den klassificerar alla bilder som en brödrost med hög konfidensgrad. (Bild: Tom B. Brown/Dandelion Mané)

3.1.4 *Djupförfalskning*

Djupförfalskning (eng. Deepfake) är en teknik som använder sig av djupinlärning och gör det möjligt att med enkla verktyg på en vanlig dator byta

ut en persons ansikte i ett foto eller i en film med mycket hög trovärdighet. Tekniken som är relativt ny finns numera även som en applikation som är tillgänglig för alla. Gränssnittet har blivit mer användarvänligt och man behöver inte längre ha någon maskininlärningskunskap eller kännedom om olika maskininlärningsbibliotek för att hantera verktyget. I princip krävs endast att man har tillräckligt många bilder av den person som man vill föra in i filmen. Tillämpningen har förstås redan testats flitigt inom pornografibranschen för att producera pornografiska filmer av celebriteter med maskininlärningsalgoritmer. Denna teknik kan förstås missbrukas på många olika sätt, men det uppenbara sättet i detta sammanhang är att det blir mycket enkelt att producera nytt barnpornografiskt material i stor skala. Detta kan hända oavsiktligt, vilket lär ha skett i ett fall (Cole, 2018), men dessvärre kommer det att finnas betydligt fler som gör det avsiktligt.



Figur 7. Skärmbild från programmet FakeApp (Bild: Elliot Grove)

3.2 Kriminella marknadsplatser på nätet

Kriminella marknadsplatser på nätet fungerar som en möjliggörare för flera typer av cyberkriminalitet. Möjligheten att med en hög grad av anonymitet kunna handla med illegala varor har lett till ett stort utbud av framför allt droger, stulen data, vapen, förfalskade varor och barnpornografiskt material. Marknadsplatser existerar både på det öppna nätet och som så kallade *hidden services* som enbart är tillgängliga genom användning av TOR[4], vanligtvis benämnt *darknet markets*. Marknadsplatser har gradvis förflyttats från öppna delar av internet till mer svåråtkomliga delar av cyberrymden allt eftersom tillslag har genomförts. Även typen av vara påverkar huruvida denna säljs på öppna internet eller på darknet markets. Förfalskade märkesprodukter säljs exempelvis i huvudsak på den öppna delen medan vapen framför allt säljs på darknet. Droghandel sker både på öppna webben och på darknet. Innan substanserna klassats som illegala säljs de öppet, därefter flyttar försäljningen till darknet. Droger utgör den största produkten på marknader inom darknet.

[4] The Onion Router. Verktyg för att försvåra identifiering internetanvändare genom att trafiken skickas genom ett nätverk av reläpunkter vilket försvårar trafikanalys.

Enligt Europol är det framförallt försäljning till slutanvändare som sker på dessa marknadsplatser (IOCTA 2018). Handel mellan distributörer och producenter sker i huvudsak genom andra krypterade tjänster.

Utöver droger och vapen utgör stulen data, som kreditkorts- och personuppgifter, en stor produktkategori på darknet (IOCTA 2018). Barnpornografi utbyts och säljs online, men detta sker inte på allmänna kriminella marknadsplatser på darknet då det finns ett starkt ogillande mot detta material även på dessa marknadsplatser.

I Europols årliga sammanställning (IOCTA) har den ökade betydelsen av kriminella marknadsplatser som en möjliggörare för cyberbrottslighet förts fram. I den senaste utgåvan (IOCTA 2018) beskrivs dock stora polisiära framsteg som skett under 2017, vilket har lett till att de tre största marknadsplatserna - Alphabay, Hansa och RAMP - kunnat stängas ner. I fallet med Hansa opererades websidan av polis i en månad innan den stängdes ner, i syfte att samla in underrättelser. Utöver dessa tre stora marknader beskrivs hur ytterligare ett antal marknadsplatser stängts ner självmant. I flera av dessa fall har upphovsmännen stulit säljarnas medel (eng. *exit scams*) (IOCTA 2018).

Dessa exempel belyser den osäkerhet som råder på dessa marknadsplatser, i huvudsak till följd av de anonymiseringsverktyg som används. För att användarna ska vara anonyma krävs att rätt verktyg används både av köpare och av säljare. I fallet med Hansa kunde polisen vid infiltrationen ta bort säkerhetsfunktioner på den administrativa sidan och därigenom undergräva anonymiteten hos användarna utan dessas kännedom[5] (IOCTA 2017).

För Polisen bör ett viktigt arbete vara breddutbildning gällande hur kriminella marknader, anonymiseringsverktyg och kryptovalutor fungerar, och vilka deras svagheter är. Egenskaper hos kryptovalutor som Bitcoin kan medföra en väldigt hög spårbarhet då användare inte har använt dessa optimalt ur anonymitetssynpunkt. Genom en större breddkunskap inom organisationen ökar förståelsen för hur dessa typer av brott kan utredas. Spetskunskaperna för att göra detta finns i synnerhet genom internationella samarbeten. Att kunna övervaka och verka mot kriminella cybermarknader bör vara ett prioriterat område för Polisen, då dessa marknader möjliggör många typer av cyberbrottslighet och även utgör ett viktigt verktyg för att omsätta kriminella handlingar till valuta (IOCTA 2018).

3.3 Bedrägeri på nätet

Bedrägeri är beteckningen på en handling då en person avsiktligt vilseleder en annan för egen vinning. Även om den exakta definitionen för bedrägeri varierar mellan olika länder tycks den gemensamma nämnaren vara att endast uppsåtligt vilseledande ska räknas som bedrägeri.

Även om bedrägeri kan förekomma i mycket varierande skepnader, avgränsar IOCTA 2017 och IOCTA 2018 bedrägerier till i stort sett två relativt distinkta brottsområden: betalningsbedrägeri (utan kort), vilket sker huvudsakligen

[5] https://www.wired.com/story/hansa-dutch-police-sting-operation/

online, och kortbedrägerier som typiskt inträffar i butiker och bankomater. Kortbedrägeri sker antingen genom att utnyttja stulen kreditkortsinformation för köp av varor och tjänster eller uttag av pengar från bankomat eller med förfalskade kort. Det senare är ett mer invecklat brott som kan innefatta olika delmoment såsom social manipulation (eng. *social engineering*), sändning av infekterad e-post för att komma åt kontokortdata, skimning via kortterminal eller bankomat och shimming[6].

Förutom förfalskning av kort kan kreditkortsinformationen användas för direkt inköp via e-handel, vilket hamnar under kategorin betalningsbedrägeri (utan kort).

Enligt denna fördelning syftar betalningsbedrägeri till bedräglig användning av kompromettterad kortdata för inköp via e-handel.

I IOCTA-rapporterna har Europol valt att kategorisera andra typer av bedrägeri som har ett starkt inslag av internet som cyberberoende brott. Utpressningsvirus, så kallad ransomware, är enligt IOCTA exempel på ett cyberrelaterat brott. I den här rapporten följs dock den svenska polisens ståndpunkt, vilken räknar alla typer av bedrägeribrott som har en cyberkoppling till denna grupp.

3.4 Cyberterrorism

På åttiotalet myntade Barry Collin begreppet cyberterrorism (Collin 1996), och sedan dess har innebörden diskuterats utan att någon tydlig definition har etablerats. Hotet som man då såg framför sig påminde mycket om filmen War Games, där en tonåring kunde sitta hemma i soffan och förstöra världen. Sedan dess har retoriken skruvats ned och flera forskare ifrågasätter om cyberterrorism någonsin kommer att bli verklighet. (Conway 2014)(Jarvis & Macdonald 2014)

En vid definition av cyberterrorism innebär att det som terrorister gör i cyberdomänen är cyberterrorism. Argumentet mot detta är att man då skulle sätta terror-suffix på vilka ord som helst. Som Gordon och Ford (2002) uttrycker det – vi skulle inte kalla en bombning av en ishackefabrik för ishacketerrorism, inte heller skulle vi kalla terrorism utfört med en ishacka för ishacketerrorism. Man skulle kunna uttrycka det som att terrorism är terrorism, oavsett vilket medel terroristen använder.

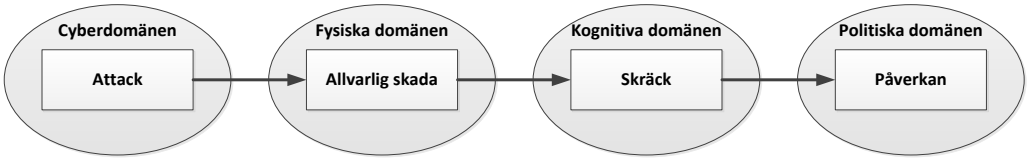
En snävare definition av cyberterrorism bygger på att denna måste innehålla inslag av våld motsvarande konventionell terrorism, samt ha politiska motiv (Denning 2012) (Conway 2014).

Enligt lag (2003:148) om straff för terroristbrott är terrorism en gärning som kan skada en stat eller en mellanstatlig organisation om avsikten med gärningen är att:

[6] Shimming är den senaste tekniken för skimning. Den används av kortbedragare för att stjäla kreditkortsinformation, där de i hemlighet sätter in en papperstunn läsare i kortstorlek innehållandes ett inbäddat chipp och lagringsmedia i själva kortläsaren. Läsaren registrerar sedan kredit- eller betalkortets EMV-chipp information.

1. injaga allvarlig fruktan hos en befolkning eller en befolkningsgrupp,
2. otillbörligen tvinga offentliga organ eller en mellanstatlig organisation att vidta eller att avstå från att vidta en åtgärd, eller
3. allvarligt destabilisera eller förstöra grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturer i en stat eller i en mellanstatlig organisation.

Utifrån den svenska definitionen av terrorism så skulle en definition av cyberterrorism kunna vara ”attacker i cyberdomänen som vållar allvarlig skada i den fysiska domänen, vilket ger upphov till skräck i den kognitiva domänen syftande till att påverka den politiska domänen” (Figur 8).



Figur 8. En möjlig domänöverskridande modell av cyberterrorism

Cyberterrorism enligt denna definition är mycket ovanligt. Etablerade terrorgrupper som IS och al-Qaida har ännu inte genomfört några kända attacker i cyberdomänen, möjligen på grund av att cyberattacker är svåra att genomföra och terrorgrupperna saknar den specialistkompetens som behövs (IOCTA, 2018). Flera forskare menar till och med att ingen terroristorganisation någonsin har genomfört en terrorhandling i cyberdomänen (Harrison Dinniss, 2018)(Conway 2014)(Gross m fl 2017).

Det finns flera tänkbara skäl till att terrorattacker i cyberdomänen ännu inte förekommit i någon större omfattning. Conway (2014)menar att faktorer som bidrar till att cyberattacker inte är vanligare är:

- Kostnad – Cyberattacker är betydligt dyrare att genomföra än konventionella attacker med exempelvis hemmagjorda bomber eller lastbilar.
- Komplexitet – En cyberattack kräver inte bara omfattande kunskap om sårbarheter i de IT-system som utgör måltavlor, utan även om de underliggande system som ska påverkas. Ofta anges infrastrukturella anläggningar (kraftverk, vattenrening, etc.) som måltavlor.
- Förstörelse – Att via en cyberattack orsaka förödelse i den fysiska domänen är svårt eftersom anläggningar som skulle kunna skapa stor ödeläggelse ofta har flera inbyggda lager av säkerhetsfunktioner.
- Media – En cyberattack som slår ut delar av infrastrukturen under en begränsad period får inte samma mediala uppmärksamhet som exempelvis en bomb i ett köpcenter och får därför inte samma inverkan på allmänheten.

Ytterligare ett möjligt skäl till att terrororganisationer ännu inte genomfört några allvarliga attacker i cyberdomänen är att det inte injagar samma fruktan.

Ett strömavbrott på några timmar är snarare irriterande än skräckinjagande (Singer 2012).

Oavsett vilken definition man väljer så är terrorism ett allvarligt problem som måste bekämpas inom alla domäner, även cyberdomänen. Om cyberterrorism ännu inte är en realitet så kan möjligheten inte uteslutas i framtiden (Cohen-Almagor 2018)(Singer 2012).

Ett konkret problem är att terrorister använder samma tjänster i cyberdomänen som alla andra, men i terrorsyfte (Singer 2012). Framför allt är det förutsättningsskapande verksamhet som flyttats till cyberdomänen, som kommunikation, finansiering, kunskapsinhämtning, propagandaspridning och rekrytering (Choi m fl, 2018)(Jarvis & Macdonald 2014)(Denning 2010).

4 Studie av hot via massmail

Hotfull elektronisk skräppost, så kallad *sextortion* eller *porrbluff*, har under senare år blivit allt vanligare. Under en månad hösten 2018 kom det in 331 stycken hotfulla meddelanden med just denna typ av innehåll till projektledaren för FOI-projektet.

Förutom de olika varianter av bedrägerier som beskrivits tidigare i rapporten så förekommer även VD-bedrägerier[7], bedrägerier där man lurar någon att använda ett BankID, SMS som ser ut att vara skickade från företag som ICA och så vidare. E-mailbedrägerier har länge varit omfattande men de senaste åren har tonen blivit allt mer aggressiv och hotfull. När det dessutom saknas erforderlig förmåga att utreda dessa bedrägerier, utan de i princip är helt riskfria för förövaren, lär de inte försvinna av sig själva. Redan under skrivandet av denna rapport dök det upp flera nya typer av utpressningsmail, som hot om bombning av byggnader och mordhot av mottagaren av breven.

I det här projektet har hot och utpressning via e-mail studerats djupare. Förutom att det är ett relativt aktuellt ämne så går det också att studera utan att riskera några etiska dilemman. En egenskap som gör dessa e-mail till intressanta studieobjekt är att de var för sig knappt uppfattas som värt besväret att utreda, men den stora mängden e-mail från samma förövare ökar allvaret i brottet. E-mailen vi valde att studera är massmail som påstår att avsändaren har gjort intrång i mottagarens mailkonto och dator samt spelat in när vederbörande har tagit del av pornografiskt material. För att inte publicera dessa filmer kräver förövaren att offret skickar utpressaren ett visst belopp i form av Bitcoin.

Innehållet i de bedrägliga e-mailen har gått från att bara försöka lura mottagaren till rent kriminella hot. Om någon hade fått ett dylikt hot med papperspost hade det sannolikt hanterats med visst allvar, men då hoten kommer via mail tenderar vi att ignorera dem eftersom skräppost är så vanligt. Eftersom bedrägerimail är direktadresserade till mottagaren så kan det vara svårt för den enskilde att avgöra om de är massutskick eller personligt riktade hot vilket gör bedrägerierna tillräckligt framgångsrika.

Mörkertalet är stort eftersom en stor del av skräpposten sorteras bort redan av mailleverantören och lagras i mailboxen för skräppost.

Polisens rekommendation är att inte svara, inte betala och att polisanmäla. Vad kan man då göra?

- Att svara på just de här mailen går i allmänhet inte, då de oftast saknar avsändaradress.
- Som framgår i sammanställningen nedan är det troligtvis inte så många som betalar, men tillräckligt många för att det ska vara lönsamt för dem som skickar ut mailen.
- Att anmäla till polisen är det enda som återstår.

[7] https://www.foretagarna.se/juridisk-faq/bluffakturor-och-bedragerier/vad-ar-vd-bedragerier/

Är det över huvud taget möjligt att utreda hotfulla mail, eller är det bortkastad tid att anmäla dessa brott? En egenskap hos internet är att i princip allt som händer där loggas. Svårigheten är att komma åt loggarna, speciellt från andra länder, vilket ofta tar tid.

I den här studien har ett antal försökspersoner, som fått hotfulla, massutskickade e-mail till sina egna adresser, polisanmält dessa på vanligt sätt och rapporterat till projektgruppen hur det gick. En av våra hypoteser var att man på vissa ställen inom Polismyndigheten skulle uppfatta dessa anmälningar som provocerande, eller i alla fall ett slöseri med resurser. För att spetsa till det skulle det också kunna uppfattas som någon form av omvänd brottsprovokation riktad mot Polisen.

En polisman har skyldighet att utan dröjsmål ta upp anmälan från allmänheten, men sådant som händer på internet tas ofta inte riktigt på allvar och uppfattas inte som värt att upprätta anmälan om. Utan indata, det vill säga bevismaterial, blir dessa brott dock mycket svårare, för att inte säga omöjliga, att utreda. I dagsläget går det inte att elektroniskt anmäla bedrägerier utan man är hänvisad till en manuell rutin som kan uppfattas som lite klumpig i sammanhanget.

4.1 Metod

Företaget Xamera fick i uppdrag att avtala med ett antal personer som fått hotfulla mail att polisanmäla dessa. Respondenterna fick sedan fylla i en enkät om hur de upplevde erfarenheten. Fallstudien avslutades med ett webbinarium där kompletterande frågor ställdes och ytterligare erfarenheter samlades in. För att locka fler deltagare erbjöds dessutom ett presentkort för besväret.

De främsta källorna till respondenter var två Facebook-grupper, Teknikbubblan och Säkerhetsbubblan. Urvalet av respondenter skedde på ett sätt som FOI eller Xamera inte hade kontroll över, och respondenterna var dessutom relativt få. Därför man kan inte förvänta sig någon särskilt hög konfidens i att resultaten skulle gälla befolkningen generellt, men det är åtminstone en indikation.

Deltagarna bestod av sammanlagt 22 respondenter, där 17 personer polisanmälde på en polisstation och 5 personer anmälde via telefon till 114 14.

Två personer lyckades inte på rimlig tid framföra sitt ärende alls på en polisstation utan anmälde via telefon istället (dessa är inkluderade i de tidigare nämnda 5 personerna). Anmälningarna genomfördes under perioden 9-29 november 2018.

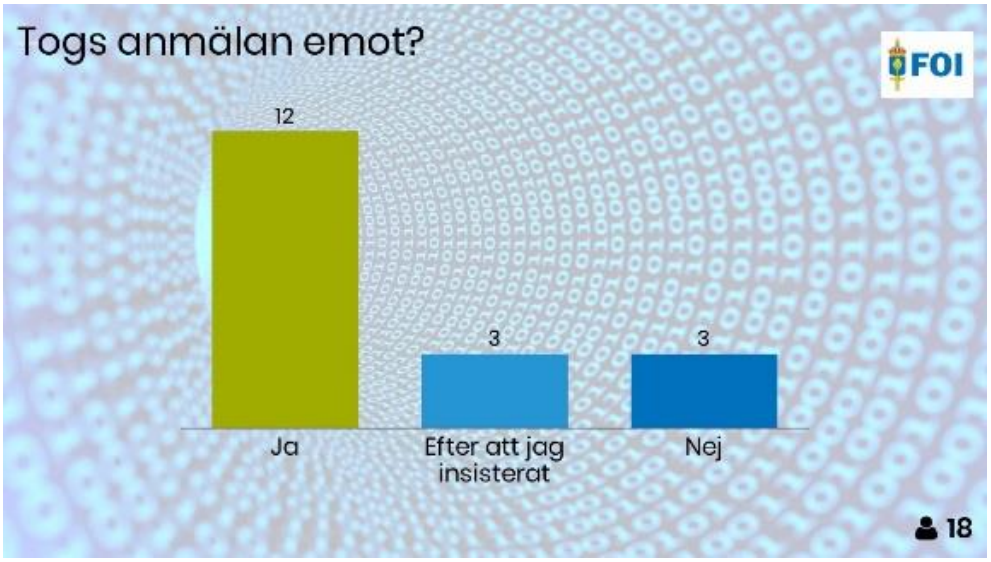
Det avslutande webbinaret genomfördes 18:00-19:00 den 17 december med medverkan av 13 respondenter. Efter webbinaret har ytterligare 5 respondenter fyllt i webbinar-enkäten. Redovisade indata nedan kommer främst från tre källor:

- enkäten som respondenterna fyllde i efter anmälan,
- den live-enkät som gjordes under webbinaret (inklusive de respondenter som fyllde i den i efterhand, totalt 18 respondenter), samt
- data från en skriftlig chat som var aktiv under hela webbinaret.

Observera speciellt att Figur 9 till Figur 19 är från webbinarets respondenter (inklusive de som fyllde i enkäten efteråt), men den beskrivande texten är en sammanvägning av samtliga ovan nämnda datakällor vilket skulle kunna uppfattas som skenbara diskrepanser i datasetet. Det är även värt att notera att mätvärdena i vissa av figurerna hänför sig till att dessa enkätfrågor har besvarats på en skala från 1 till 7 och att den siffran som redovisas helt enkelt är ett medelvärde av svaren.

4.2 Kontakt med Polisen

Av de 22 försöken togs anmälan emot i 17 fall och avvisades i 5. Av de 5 avvisade försöken gjordes 2 per telefon. Merparten av respondenterna fick besked om att utredningen omedelbart skulle komma att läggas ner.



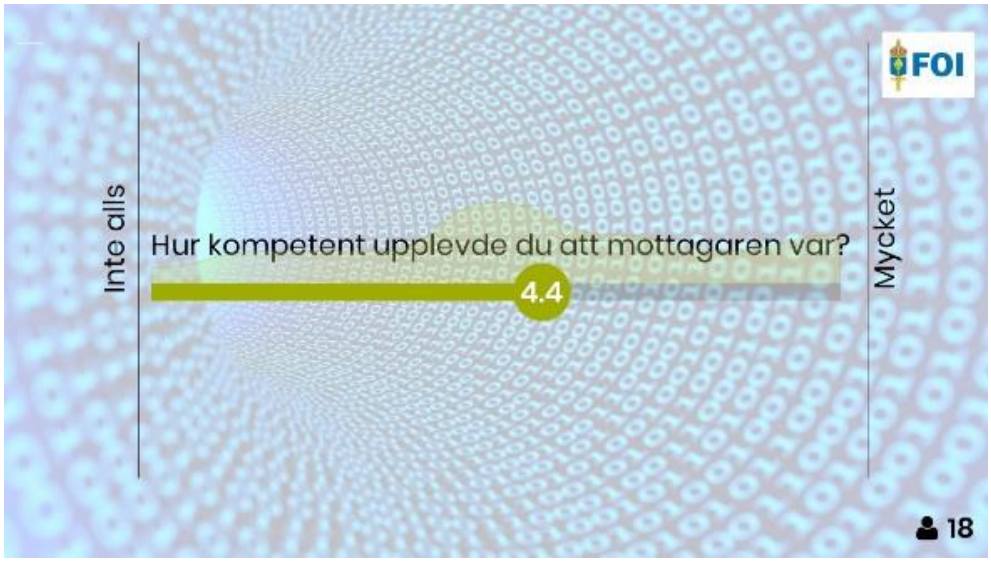
Figur 9. Utfall av polisanmälan av deltagarna i webbinaret

Sammantaget verkar det som att problemet med att anmälningar inte tas emot ändå är mindre än vad som tidigare antogs.

Av respondenterna var det endast två som upplevde att de blev otrevligt bemötta. Övriga upplevde ett korrekt och artigt bemötande, även när anmälan inte togs emot, vilket motsäger vår hypotes att dessa ärenden skulle uppfattas som provocerande.

Figur 10. Upplevt bemötande vid polisanmälan[8]

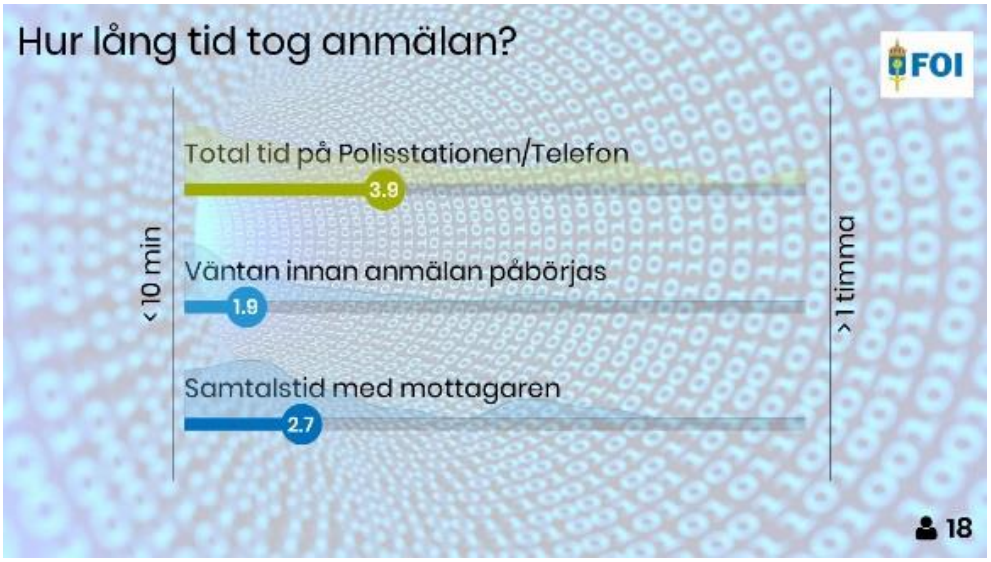
När det gällde kompetensen och allvaret i mottagandet, kan man se att upplevelsen varierade betydligt (Figur 10 och Figur 11). Möjligen kan även kompetensen hos anmälaren påverka resultatet.



Figur 11. Upplevd kompetens hos mottagare av anmälan

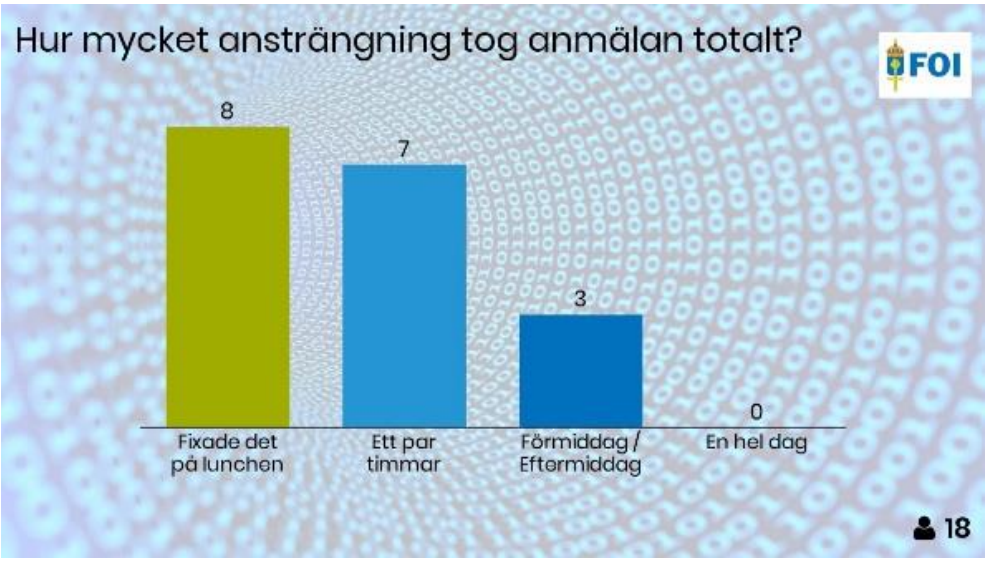
I det övriga materialet framgår det att reaktionerna varierade från att slänga på telefonluren i örat på respondenten till att dela med sig av lite enklare IT-säkerhetstips och att uttrycka att dessa anmälningar är viktiga.

[8] Notera den halvtransparenta gröna kurvan som beskriver fördelningen av svar.



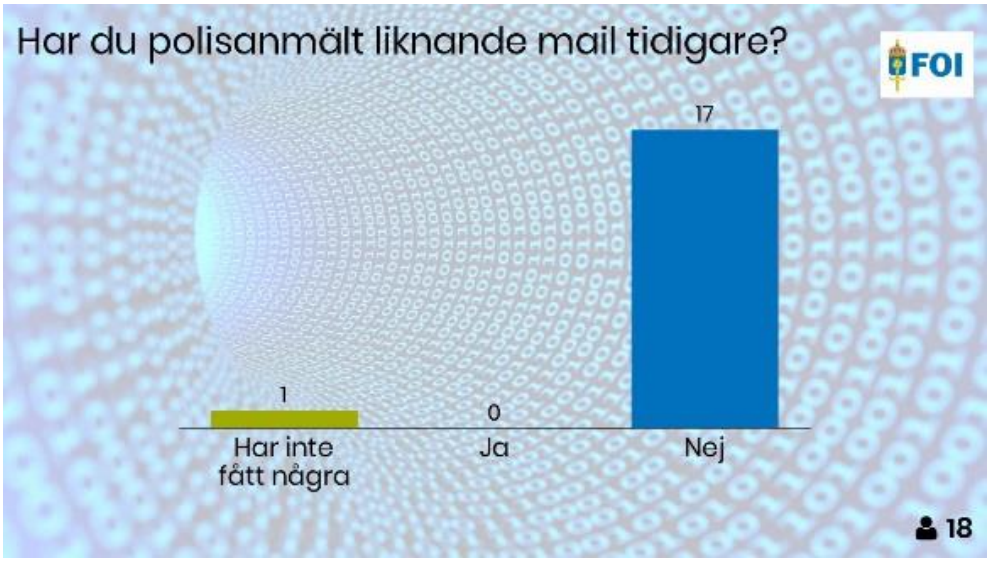
Figur 12. Upplevd tidsåtgång för anmälan

Det verkar som att respondenterna inte tyckte att det var speciellt tidsödande eller besvärligt av andra anledningar att genomföra själva anmälan. Hur man skulle känna om det blev en rutin som genomfördes flera gånger i veckan frågade vi inte, men det kan antas att det upplevda besväret skulle öka.



Figur 13. Bedömd total ansträngning för anmälan

Ingen av respondenterna hade polisanmält liknande e-mail tidigare (Figur 14).



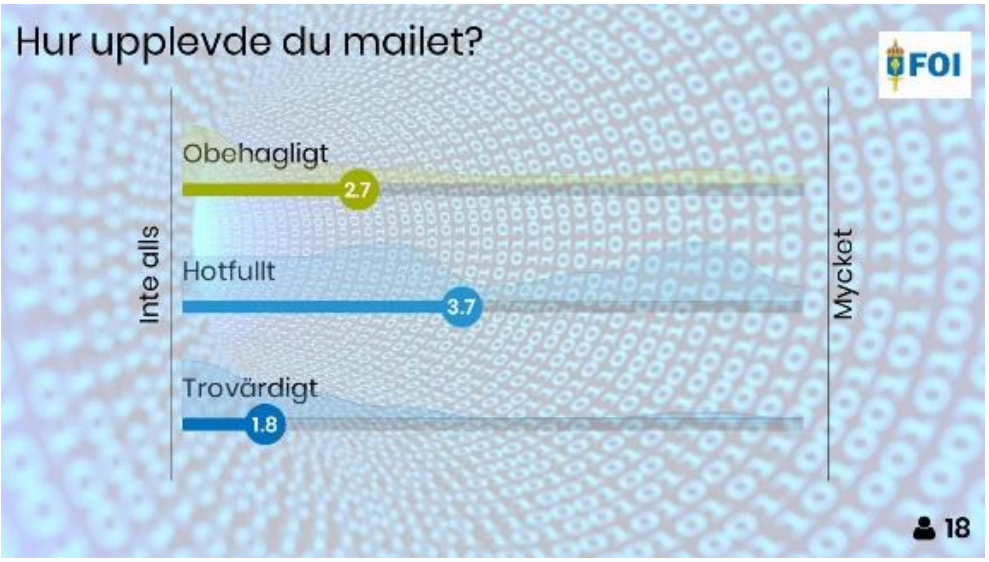
Figur 14. Tidigare erfarenheter av att anmäla denna typ av brott

När det kom till skälen att man inte anmält tidigare är det tydligt att dessa mail behandlas som skräppost och därför inte värda att rapportera. När det gäller besväret att anmäla mailen syns en stor spridning i uppfattningarna (Figur 15).

Figur 15. Skäl för att inte anmäla tidigare

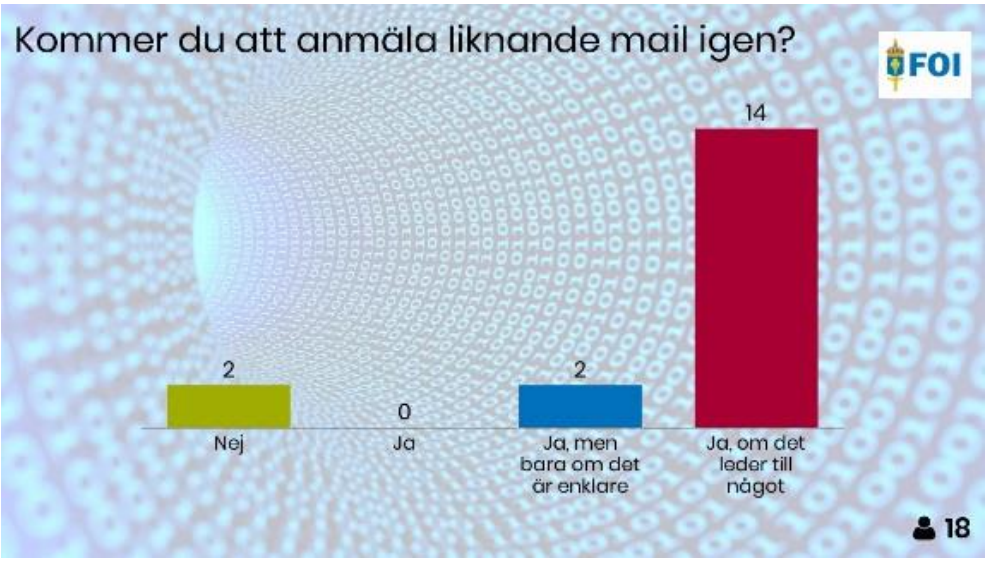
4.3 Mailets innehåll

Det är stor spridning i hur hotfullt respondenterna tyckte mailet var, men det uppfattades i mindre grad som obehagligt eller trovärdigt. Här kan dock gruppens förhållandevis datorvana personer sänka värdena. Speciellt trovärdighetssiffran borde rimligen vara lägre hos datorvana personer än hos befolkningen i allmänhet.



Figur 16. Upplevelse av mail

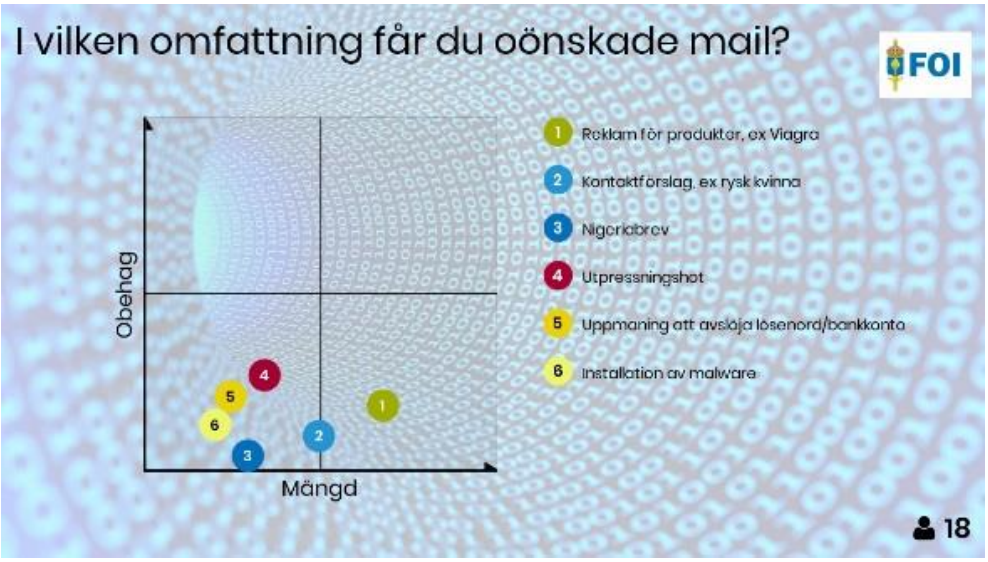
Tydligt är dock att den viktigaste faktorn för att anmäla liknande mail i framtiden är att det kommuniceras ett resultat i form av uppklarade brott.



Figur 17. Bedömt framtida agerande

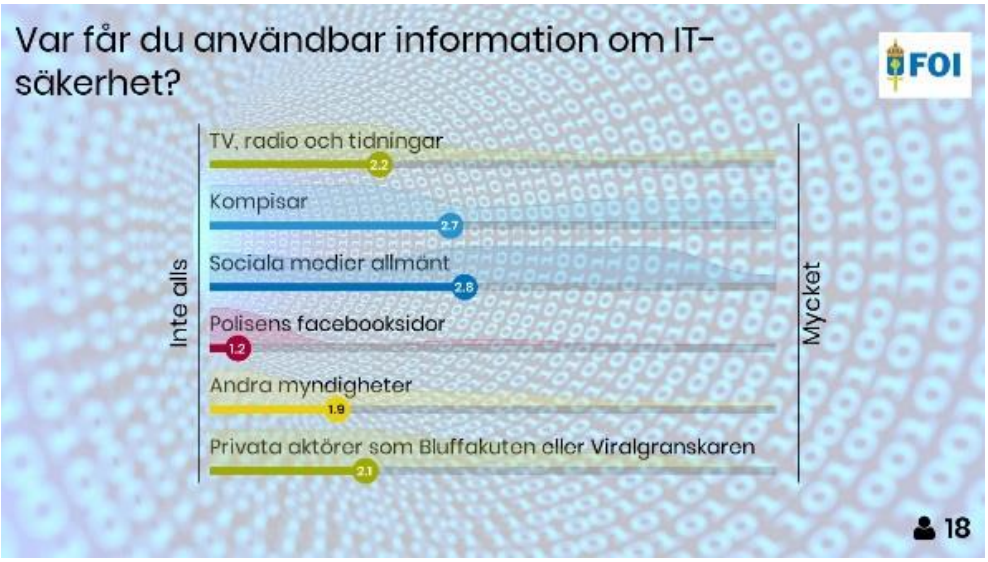
4.4 IT-säkerhetsinformation

Det kan konstateras att av de hot vi ser idag så är det utpressningshot via mail som ligger högst upp på obehagsskalan, men att mängden tycks vara hanterbar (Figur 18). Om man tränger djupare in i svaren finns en tydlig tendens att vi är på väg att trubbas av och accepterar mer och mer. Underlaget är dock för litet för att säkert kunna fastställa detta.



Figur 18. Uppfattad omfattning av oönskade mail. Skalorna går från liten till stor mängd och litet till stort obehag.

Det är stor spridning på var information om IT-säkerhet inhämtas, men en sak är tydlig; Polisens Facebook-sidor är inte den främsta källan till information (Figur 19). Kommentarerna på den här frågan visade på ytterligare källor för information, som ”Säkerhetssidor/IT-sidor på nätet” och ”övriga webbsidor”. Samtidigt konstaterades det att Polisens information är för ytlig och grund. Ett annat förslag på plats för information som inkom via chatten var att köpa annonsplats i närhet till söksträngen ”köpa Bitcoin” för att informera om internetbedrägerier i syfte att få fler att anmäla dessa.



Figur 19. Källor till information om IT-säkerhet

4.5 Bitcoin-mottagare

En enklare analys av de 331 mottagna mailen har utförts av FOI. Mailen innehöll några olika varianter av hotfulla texter på automatöversatt svenska,

men bara 11 olika Bitcoin-adresser fanns med (Tabell 1). Alla dessa adresser har under sin existens mottagit 3-56 Bitcoin-transaktioner, som totalt under perioden motsvarande ca 305 000 SEK till en enskild plånbok. Till dessa konton har totalt motsvarande dåvarande värde, ca 1140 000 SEK överförts. Ingen djupare analys av ursprunget av dessa transaktioner har utförts, men plånböckerna var aktiva endast en kortare period under hösten 2018 och har därefter tömts på alla tillgångar. Det finns därför skäl att misstänka att merparten av pengarna kommit från mottagare av de hotfulla mailen.

Tabell 1. Bitcoin-adresser i skräpmail med antal transaktioner och total summa av mottagna Bitcoin, samt motsvarande värde i SEK den 10 oktober 2018.

Bitcoin-adress	Mail	Trans-aktioner	Tot. mott. BTC	Tot. mott. SEK
1BSAHXc58m2DQGuzVaKXD15xeDrE4xYZna	90	12	0,54699096	32 852,28
1Mkgo9ACuciLhpinUPhTmRDfswL1aFChir	76	3	0,22349653	13 423,20
1Pau7aAFNZ5rvogxMnfP37zDAzoeipCqPP	68	27	1,71950922	103 273,72
19i2Zn4QMg5y9gDTRfLyPXaw2zY3ikPzqg	35	18	1,21250887	72 823,28
1Aq77aob4mxfgfuD7Cs12GN2gv82kBJmYW	30	6	0,30144088	18 104,54
144CDUeBhcwoEUmA2B1cL5p5PqZrhJWCCt	15	32	2,24736076	134 976,49
13H6Nszz1xP6Xn5tDKAUVWpm97vLfcNMVi	12	8	0,4040819	24 269,16
1JTtwbvmM7ymByxPYCByVYCwasjH49J3Vj	2	56	5,07673184	304 908,51
1MZHWpgmUyjmExofPDCmYuVz9kmnTpu6m	1	18	0,67098768	40 299,52
1HQ7wGdA5G9qUtM8jyDt5obDv1x3vEvjCy	1	42	3,58995649	215 612,79
15ZHnf1MPn6ybb8yUeAoCQ1AJtiKhg3NrP	1	24	2,98619488	179 350,86
SUMMA	**331**	**246**	**18,97926001**	**1 139 894,36**

Via ett enkelt online-verktyg (Figur 20) kan det konstateras att alla dessa 11 adresser har en koppling till varandra, antingen genom direkta överföringar mellan två adresser eller via ett till två mellanled. Således är de antagligen kopplade till samma grupp av användare.

Figur 20. Illustration av närmaste koppling mellan två Bitcoin-adresser via verktyget på learnmeaBitcoin.com/tools/path.

4.6 Sammanfattande reflektioner av fallstudien

Polisen har ett stort tillitskapital som är viktigt att vårda. Från allmänheten har det bara framkommit positiva reaktioner på att försöka minska ett problem som av många upplevs som ökande. Dagens anmälningsprocess verkar inte vara särskilt avskräckande, även om den inte är anpassad för volymer om hundratusentals anmälningar i veckan. Det som avhåller från anmälan verkar mer vara att det inte upplevs vara meningsfullt eller ge resultat. Att hot och andra bedrägeriförsök ignoreras för att de kommit via internet är en oroande tendens om människor blir avtrubbade och accepterar eller ignorerar även tämligen grovt innehåll bara för att omfattningen är stor och att det varit en smygande utveckling från oskyldigt till grovt innehåll.

5 Intervjuer med polis och åklagare i Malmö

En begränsad intervjuserie genomfördes med polis och åklagare i Malmö. Syftet med intervjuerna var att få en uppfattning om hur representanter ur den operativa verksamheten ser på internet och internetrelaterade brott, samt vilka utmaningar och möjligheter internet innebär. Totalt genomfördes tre intervjuer med en gruppchef vid Lokalpolisområde Malmö Öst, Inre befäl för Polisområde Malmö samt en åklagare med särskild IT-kompetens.

Intervjuerna genomfördes som semistrukturerade, det vill säga utifrån ett manus (Bilaga1), men anpassades efter situationen.

5.1 Allmän attityd

På frågan om hur de intervjuade själva skulle agera om de utsattes för brott på nätet gavs en blandad bild. En respondent uppgav att anmälan skulle göras omgående, medan en annan ignorerade och skrattade bort även allvarliga brott som mordhot. Den allmänna uppfattningen var dock att även om det formellt sett inte är någon skillnad på internetrelaterade brott och ”vanliga” brott, så är de internetrelaterade inte lika allvarliga. En respondent menade även att internetrelaterade hot och kränkningar är så vanliga att de blivit normaliserade och accepterade som en del av vardagen.

5.2 Förebyggande och upplysande verksamhet

Samtliga respondenter får regelbundet förfrågningar från allmänheten om vad man kan göra åt förtal och bedrägerier på nätet, men samtidigt menar de att det är väldigt få som faktiskt anmäler denna typ av brott. Organiserad upplysning sker i begränsad form. I LPO Malmö Öst har man fått en enda förfrågan om att föreläsa om brott på sociala medier under de senaste fyra åren.

På lokal polisområdesnivå har det observerats att ungdomsgäng som tidigare uppehöll sig på allmänna platser har minskat, men gissningsvis har gängen har flyttat till andra miljöer, som exempelvis sociala medier.

5.3 Kommunikation med allmänheten

Samtliga intervjuade ansåg att Polisen borde visa en mer omfattande närvaro på internet och nämnde exempel från bland annat Holland och Danmark. Där använder Polisen olika kommunikationskanaler, både för att få information från allmänheten och för att orientera allmänheten om risker och händelser inom olika områden. En respondent nämnde även att det kan vara svårt för allmänheten att få kontakt med rätt person eller funktion inom Polisen, eftersom det är en stor och komplex organisation och det kan ta timmar att hitta rätt.

Kommunikation med allmänheten är viktigt eftersom Polisen ofta får in tips och ledtrådar den vägen. Det finns till och med självutnämnda internetväktare som letar vad som i deras ögon är olämpligheter och tipsar Polisen.

5.4 Upptäckt av brott

Samtliga respondenter uppgav att de vid flera tillfällen upptäckt brott på internet, och en respondent angav även att han aktivt sökte efter brottslig aktivitet i mån av tid. På frågan om Polisen skulle kunna patrullera på internet trodde samtliga respondenter att det säkert skulle vara möjligt, men att det skulle krävas särskilda sökverktyg för att gå igenom de stora mängderna data som finns tillgängligt.

5.5 Ta upp anmälan

En respondent menade att sättet att upprätta anmälningar på inte är anpassat till modern media och att arbetsmetodiken inte är anpassad till dagens verksamhet. Samma respondent uppgav även att det saknas nationella IT-relaterade direktiv för polisverksamheten.

5.6 Brottsrubricering och klassificering

Flera av respondenterna framförde kritik mot Brottsförebyggande Rådets (Brottsförebyggande Rådet, 2018) anvisningar och regler för klassificering av brott, och menar att det saknas klassificering av IT-inslag. Vid en granskning av BRÅ:s instruktion visade det sig dock att det finns koder för koppling till internet vad gäller olaga hot, ärekränkning, bedrägeri, barnpornografibrott samt brott mot immaterialrätten. Totalt finns tolv brottskoder för internetrelaterade brott. Utöver detta tillkommer klassificeringarna datorbedrägeri, dataintrång och fildelning. Den allmänna uppfattningen om klassificeringssystemet var dock att det fungerar ganska bra när man lärt sig hur det ska tillämpas.

5.7 Utreda IT-relaterade brott

Samtliga respondenter uppgav att det ofta är svårt att utreda internetrelaterade brott, och att det finns flera skäl till detta. Några orsaker som uppgavs var:

- Allmän okunskap om hur internetrelaterade brott utreds, framför allt längst ut i organisationen.
- Osäkerhet om hur bevis kan och bör säkras.
- Snabba förlopp, i en del sociala medier har informationen begränsad livslängd och kan snabbt försvinna.
- Internetoperatörerna är ovilliga att hjälpa till och det kan bli långa responstider.
- Svårigheter att knyta individer till konton. Ofta används falska konton som är svåra att knyta till faktiska individer. Det kan även vara svårt att knyta enskilda individer till en dator vid en viss tidpunkt.
- Kryptering och anonymisering. En respondent uppgav att det nästan verkar som att produkter utvecklas specifikt för att försvåra polisens arbete, som telefoner med fingeravtrycksidentifiering, krypterade tjänster och fjärradering.
- IT-industrin vill inte offentliggöra tekniska brister som skulle kunna hjälpa polisen.

- Ofta finns kopplingar till andra länder, vilket fördröjer och försvårar utredning.
- Det är inte ovanligt med fabricerade IT-bevis, exempelvis vid konflikter inom familjen.
- Den tekniska utvecklingen går fort men lagstiftningen släpar efter. Ett exempel som nämndes är spårningsutrustning för sin bil eller cykel. Dessa utrustningar kan enkelt appliceras på andras fordon, eller till och med polisfordon, vilket i dagsläget inte är olagligt.

Internet medför också fördelar. Flera respondenter uppgav att de använder bland annat Facebook för att identifiera misstänkta individer samt för att kartlägga misstänkta personers kontaktnät.

Internet blir också en allt viktigare beviskälla och inom polisen har spaningsgrupper upprättats som aktivt söker bevis. Ett exempel som nämndes var en våldtäkt som polisen visste hade filmats och där man väntade på att den skulle publiceras.

Den intervjuade åklagaren framförde vikten av att IT-forensiker är med från början i en utredning och att de måste vara med långt in i utredningen.

5.8 IT-relaterade brott i domstol

Bevisföringen i internetrelaterade brott är ofta både omfattande, abstrakt och komplex, vilket enligt en respondent ofta gör det svårt att förklara i rätten så att alla förstår. Detta kan i viss mån hanteras genom åklagare och domare med specialistkompetens, men samtidigt blir IT-bevis allt vanligare. Enligt den intervjuade åklagaren förekommer IT-inslag i så gott som samtliga narkotikautredningar för att ta ett exempel.

5.9 Utbildning, kompetens och utveckling

På frågor om vilken specialistkompetens avseende IT som finns inom Polisen och vilket stöd som går att få varierade svaren. På lokal nivå rådde en stor osäkerhet men på regional nivå fanns en större kunskap om både regionala och nationella stödresurser. Samtliga respondenter uppgav dock att det behövs en bredare allmänkunskap om IT-relaterade brott och en utveckling av metodiken, så att man på alla nivåer blir bättre på att samla och säkra bevis.

Problem och frågeställningar som behöver behandlas var bland annat:

- Hur kan och bör kryptovaluta beslagtas?
- Räcker det med att maila eller vidarebefordra bevis från den anmälandes elektroniska utrustning?
- Vilket bevismaterial är tidskritiskt? Hur säkerställer man exempelvis att ett trådlöst nätverk var lösenordsskyddat vid en given tidpunkt?

Den allmänna uppfattningen var att det finns specialistkompetens inom Polisen, framför allt på nationell nivå (NOA), men att det råder en viss

osäkerhet var i organisationen denna kompetens finns och vilket stöd som går att få.

Bland respondenterna rådde även osäkerhet om vilken del av Polisens utvecklingsorganisation som utvecklar metodiken kring IT-relaterade brott.

5.10 Övriga kommentarer

Samtliga respondenter bedömde att internetrelaterade brott hela tiden ökar och att Polisen borde vara mer aktiv inom detta område, men att det råder resursbrist och därför prioriteras den fysiska miljön. Internetrelaterade bedrägerier har blivit vanligt och det finns en omfattande flora av säkra kommunikationslösningar som avsevärt försvårar polisens möjligheter att avlyssna kommunikationen mellan kriminella element.

En respondent menade att provokativa åtgärder och infiltration kommer att bli viktigare inom IT-domänen eftersom passiv spaning blivit svårare med alla de skyddade kommunikationer som finns tillgängliga.

6 Intervju på NOA SC3 i Stockholm

Inom ramen för projektet genomfördes en intervju med en polis som arbetar som handläggare/utredare vid NOA SC3 (Nationella operativa avdelningen, Swedish Cybercrime Center). Syftet med denna intervju var att få ökad kunskap om hur SC3 bedriver sin verksamhet, med de utmaningar och möjligheter som de möter i sitt vardagliga arbete, samt ge möjlighet att utifrån ett centralt perspektiv jämföra med det lokala och regionala perspektivet. Ytterligare ett syfte var att få djupare insikt i hur samarbetet fungerar med aktörer inom sociala medier och bredbandsleverantörer, samt hur svensk polis samverkar och förhåller sig till andra länder.

SC3 utreder komplexa cyberbrott, primärt på nationell nivå snarare än regionala eller lokala brott. Anledningen till detta är dels den geografiska omfattningen av brottet och dels att det fordras djupare specialkompetens och större tillgång till resurser i form av personal med tillgång till olika underlättande och till viss del även nödvändiga specialverktyg.

SC3 är processägare till hur svensk polis ska arbeta med cyberbrott. I det ansvaret ligger också att skriva riktlinjer om hur det arbetet ska gå till. SC3 kan också fungera som rådgivande och stödjande resurs till resten av landet. De är också kontaktyta, eller *single point of contact*, för leverantörer av internetrelaterade tjänster. De samverkar också centralt med olika myndigheter såsom Brottsförebyggande rådet (BRÅ).

Intervjun genomfördes på samma sätt som med Polis och åklagare i Malmö.

6.1 Allmän attityd

Den intervjuades vardag består i mångt och mycket av att utreda brott som hot, förtal, bedrägerier, pornografi, utpressning, men också mer komplexa ärenden som involverar flera länder, kontakt med flera myndigheter, banker eller med polis i andra länder. På frågan om hur den intervjuade själv skulle agera om vederbörande utsattes för brott, berodde agerandet på flera faktorer; om respondenten upplevde att brottet var verkligt, att respondenten verkligen kände sig rädd eller att respondenten uppfattade att det verkligen förelåg ett brott.

För att kunna avgöra om brott föreligger används lagstiftning, förarbeten, praxis, erfarenheter och kontinuerlig dialog med förundersökningsledare och åklagare.

Sammanfattningsvis skulle respondenten absolut göra en polisanmälan vid brott, men menade också att vardagen bidrar till att en normalisering sker. Det vill säga, med tanke på personens arbetsuppgifter är det lätt att bli luttrad, och de ”vanliga” brott som gemene man utsätts för kanske inte skulle rendera i en anmälan – acceptansen är kanske högre för de hot eller försök till brott som man utsätts för.

6.2 Allmänna observationer

I och med det höga antalet ärenden och frågor ökar också kunskapen och erfarenheten om vad som fungerar och vad som inte fungerar. Detta gäller exempelvis kontakt med andra länders polis och rättsväsende, hur och på vilket sätt begäran om rättshjälp fungerar, kontakter med operatörer och andra informationsbärare, samt om uppgifterna är sparade och hur länge.

Ett exempel är att ofta när SC3 skickar ut en begäran om frysning[9] räcker dagens lagstiftning inte till. Bakgrunden eller anledningen till det är sannolikt att Sverige idag inte har ratificerat Europarådets konvention om IT-relaterad brottslighet (Budapestkonventionen). Uppfattningen är att det försvårar det dagliga arbetet i kontakt med andra länder eftersom andra länder menar att Sverige inte ingår och därför lämnar de inte ut uppgifter. Nuvarande arbetssätt, där Sverige nästan får vädja till andra länder att respondera, är inte i längden hållbart. Detta eftersom framgångsfaktorn är just samverkan och samarbete länder emellan gällande informationsutbyte.

Sammanfattningsvis så fungerar verksamheten tämligen bra, men utrymme för förbättringar finns alltid. Exempelvis så behövs fler verktyg, fler medarbetare, större delaktighet, bättre anpassad lagstiftning, snabbare processer, bättre rutiner och ökad kunskap. Alla nivåer, både nationellt, inom och utanför polisen, måste arbeta tillsammans för att kunna hantera den ökade volymen av IT-relaterade brott, komplexiteten och utmaningarna i det alltmer digitaliserade samhället som lämnar stora möjligheter för att begå brott.

SC3 har för avsikt att bli mer publika och delta i flera sammanhang för att kunna bygga relationer, visa på kunskap och insikt men även för att inhämta kunskap. Det genomförs nu en större satsning inom svensk polis genom att bygga upp ett regionalt cybercrime center (RC3) i varje region.

6.3 Kommunikation med allmänheten

SC3 kontakt med allmänheten är mycket begränsad med anledning av hur polisens struktur är uppbyggd och tänkt att fungera. Kontakten med allmänheten sker nästan uteslutande på regional nivå. SC3 fungerar då mer som ett backoffice med råd, stöd och hjälp.

6.4 Säkring av digitala bevis

Den intervjuade uppger att nästan alla brottsutredningar i dagens samhälle är internetrelaterade eller har anknytning till någon digital produkt. Nästan alla brottsutredningar innefattar moment som tömning av mobiltelefon som kan ge bevisning gällande kommunikation runt brottet. Det är idag mycket vanligare med större informationsmängder och mängden data ökar hela tiden. Detta ställer krav på att varje utredare eller polis som arbetar på fältet har rätt kunskap och verktyg för att kunna utföra sina arbetsuppgifter. Det saknas idag nationella rutiner, verktyg och kunskap för hur tömningar av mobiltelefoner

[9] Frysning innebär att man låser information som annars skulle ha raderats en viss tid efter att informationen samlats in så att polisen i ett senare skede kan begära ut uppgifterna.

och annan elektronisk utrustning ska ske men även hur och var informationen ska lagras, sorteras och presenteras.

Informationen som skulle kunna användas som bevis vid brottsutredningar ”lever” inte så länge vilket ger vid handen att rätt person med rätt kunskap och verktyg måste vara närvarande för att ”säkra” de digitala spår eller information som finns. Detta kan i vissa fall vara helt avgörande för utgången av utredningen.

6.5 Ta upp anmälan

Polisen har förändrat sitt sätt att ta upp anmälan, det går idag fortare och systemet är mer anpassat till dagens moderna IT-miljö men det är fortfarande många steg kvar innan systemet kan beskrivas som effektivt, anpassat och modernt.

6.6 Brottsrubricering och klassificering

SC3 är nationell kontaktpunkt mot BRÅ och det sker en löpande samverkan. Det pågår en översyn av brottskoderna för dataintrång. Dialogen mellan BRÅ och polisen är god. Förändring, utveckling och uppdatering av polisens brottskodssystem hanteras av BRÅ men används praktiskt av polisen i samband med anmälningsupptagning.

6.7 Utbildning, kompetens och utveckling

När diskussionen handlar om hur den intervjuade ser på framtiden kan det sammanfattas i nedanstående punkter.

- Skapa nationella utbildningsprogram med flera olika nivåer för att säkerhetsställa en lägsta nivå men även en löpande kompetensutveckling. Innehållet i en sådan utbildning skulle kunna innehålla bevishantering i den digitala miljön, hur datorer kommunicerar, telefoner, hur IP-adresser fungerar, domäner, vilken väg som ska användas i kontakt med leverantörer av digital media, hur kontakter ska ske med andra länder, hur virtuell valuta fungerar.
- Nationella riktlinjer och verktyg för hur olika arbetsmoment i en utredning ska gå till. Från polis på fältet där mobiltelefoner, datorer med mera påträffas till samarbete med åklagarmyndigheten och till hur datainformation ska lämnas ut till och inhämtas från andra länder.
- Nationella riktlinjer för hur plötsligt uppkomna brottsvågor som t.ex. ransomware och utpressningsmail ska koordineras och tas om hand för att öka tryggheten i samhället och minska brottsligheten.
- Svensk polis bör vara mer närvarande och mer synlig i det offentliga rummet, dels för att informera samhället men även för att fortsätta bygga goda relationer med andra länder och privata aktörer.

6.8 Övriga kommentarer

Respondenten ansåg att Polisen både måste vara mer aktiv och mer proaktiv t.ex. genom provokativa åtgärder. Det är svårt att utreda brott som redan har hänt i komplexa digitala miljöer. Europol har ett projekt som kallas ”cyber-patrolling week” och innebär att ett visst antal timmar läggs på att vara aktiv och synlig på nätet. Verktyg och kunskap finns det gäller bara att använda dessa.

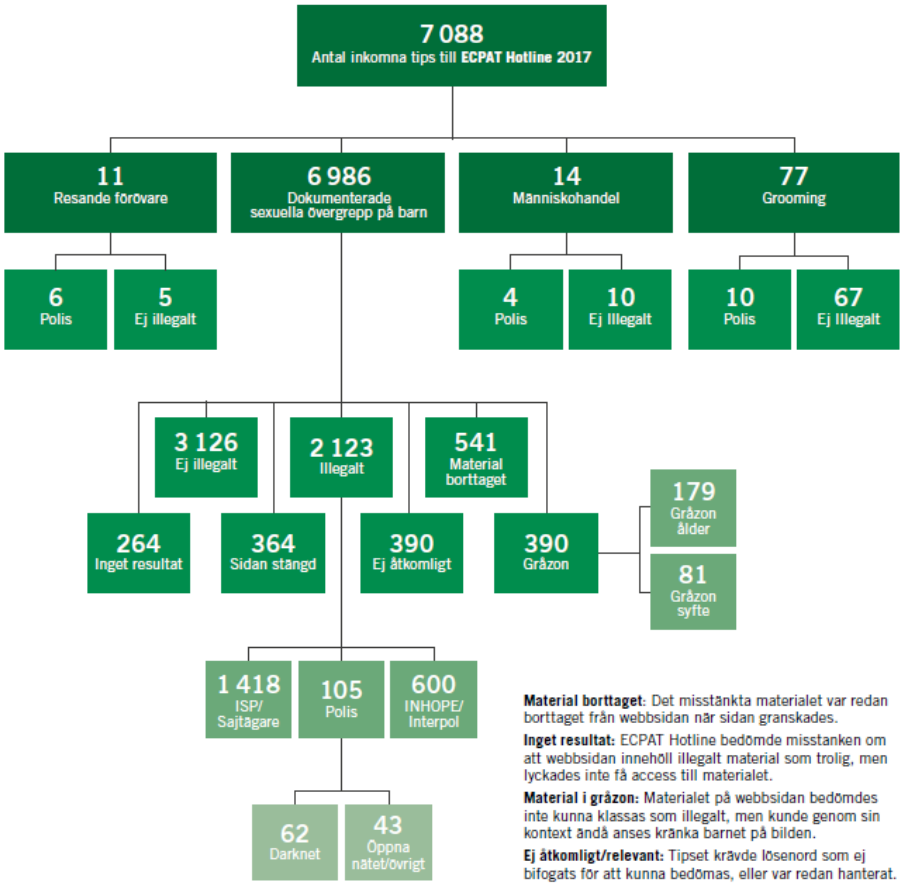
7 Brottsbekämpning på internet

I detta avsnitt ges övergripande beskrivningar av aktiviteter som genomförs i syfte att bekämpa olika typer av IT-relaterad brottslighet.

7.1 Sexuellt utnyttjande av barn på nätet

Anmälda brott relaterade till sexuellt utnyttjande av barn på nätet kan för det mesta delas i två huvudkategorier: dokumenterade sexuella övergrep på barn (så kallade barnpornografibrott) och nätgrooming (vuxnas kontakter med barn på nätet i sexuella syften). Även om det finns starka kopplingar mellan dessa två typer av brott och förövaren i vissa fall kan dokumentera begångna övergrepp vare sig det sker online eller i det verkliga livet och sprida dokumentationen vidare i ekonomiskt syfte eller för att få högre status i slutna grupper som delar material relaterade till sexuellt övergrepp på barn, bör man skilja mellan dessa två kategorier eftersom de kan prioriteras och bekämpas på olika sätt. Dessutom är barnpornografibrott mycket vanligare. Till exempel, av totalt 7088 inkomna tips till ECPAT[10] under 2017 var 6986 misstänkta fall av barnpornografi medan 77 fall var relaterad till misstanke om nätgrooming (se Figur 21).

[10] ECPAT (End Child Prostitution, Child Pornography, and Trafficking of Children for Sexual Purposes) är en ideell organisation som arbetar mot alla former av kommersiell sexuell exploatering av barn, även kallad barnsexhandel. Detta inkluderar barnpornografi, barnsexturism och trafficking, dvs. människohandel med barn i sexuella syften.



Figur 21. Sammanfattning av statistik från ECPAT Hotline för 2017

Medan tekniker såsom mönsterigenkänning, bildanalys, textanalys, författarprofilering, författaridentifiering och spårningscookies är mest relevanta i samband med barnpornografibrott, så kräver effektiv bekämpning av nätgrooming mer proaktiva metoder såsom infiltration.

Ett exempel på en proaktiv kampanj mot sexualbrott mot barn var projektet Sweetie[11]. Projektet startades 2013 av den ideella organisationen *Terre des Hommes*[12] som är inriktad på barns rättigheter och gick ut på att ett datoranimerat barn (se Figur 22) som presenterade sig som ett tioårig filippinsk flicka i ett chattrum fungerade som ett lockbete för att samla information såsom Skypeadress från de som var villiga att betala för att hon klär av sig inför webkameran. Inom loppet av 10 veckor kontaktade runt 20000 personer henne och närmare 1000 av dessa var villiga att betala. All insamlad information om förövarna lämnades till brottsbekämpande myndigheter i respektive land.

[11] https://www.bbc.com/news/uk-24818769
[12] http://www.terredeshommes.org/

Figur 22. Datoranimerade barnet Sweetie skapat för att samla information om förövarna. (https://www.terredeshommes.org)

7.2 Infiltration online

Lyckade operationer mot kriminella handelsplatser som Alphabay och Hansa (se avsnitt 3.2) illustrerar potentialen i att genomföra infiltration i kriminella miljöer online. Infiltration online medför en klart mindre risk för operatören, jämfört med klassiskt infiltration, då även operatören har skydd av anonymiseringstjänster och konsekvenserna vid eventuell röjning är klart lindrigare.

7.3 Kryptovaluta

Associering mellan olika Bitcoin-plånböcker är möjlig, och deras relationer via transaktioner kan analyseras med webbresurser och proprietär programvara. Att ta steget vidare till identifiering av en viss användare är svårt, men inte omöjligt. Genom att skapa databaser där misstänkt verksamhet kan märkas upp och dela denna information över gränserna kan skillnader i resurser mellan länder och myndigheter kringgås. Transaktioner med Bitcoin sker transparent och lagras, vilket är en stor fördel i juridiska sammanhang.

EU satsar ca 5 miljoner euro i projektet TITANIUM för att under 2017-2020 arbeta med forskning och utveckling inom teknik och lösningar som ska stödja polis och rättsväsende i utredning av kriminellas och terroristers aktiviteter rörande kryptovaluta och underjordiska marknader på Darknet (Titanium, 2018). Inga resultat har ännu publicerats på projektets hemsida.

Amerikanska myndigheter överväger att skapa en svartlistning av kryptovalutaadresser som är associerade med kriminella grupperingar såsom terrorister, droghandlare, etc. (Heaven, 2018).

8 Rekommendationer

Under de två år som projektet har löpt har det byggts upp en betydande kunskapsbas att använda till framtida projekt som exempelvis syftar till att stödja Polismyndigheten i deras arbete. Projektarbetet har även resulterat i ett antal konkreta förslag till åtgärder och till fortsatt forskningsverksamhet.

8.1 Utbildning

Ett genomgående tema under hela projektets gång och i alla sammanhang är att Polismyndigheten saknar kunskap och erfarenhet på bredden om cyberdomänen. Exempelvis finns inte några kursmoment alls om brott på internet på polisutbildningen. Ett uttryck som vi stötte på redan på webbinaret 2017 var att ”utbilda löven”, och det måste vara en av de viktigaste åtgärderna för att förbättra läget inför framtiden. Detta kan ske genom att införa relevanta moment i utbildningar, självstudiekurser och nätbaserade studiecirklar, kortare informationsvideor, samt anställning av fler experter som kan ge stöd.

Även när det gäller information till allmänheten finns det förbättringspotential. Polismyndigheten är rikt representerad med olika bloggar, Facebook- och Twitterkonton. Trots denna flora av olika informationskanaler kunde vi i fallstudien konstatera att i alla fall de deltagare vi hade där i liten omfattning använde information från polisens kanaler på sociala medier för sina säkerhetsbeslut. Vad detta beror på har vi inte hittat något entydigt svar på i den här studien, men det vore nog inte orimligt att tänka över placering och innehåll i de kanaler man redan har.

Ett tydligt önskemål från deltagarna i fallstudien var också att det är viktigt att man visar på resultat. Som ett försök att hitta effektivare kanaler skulle vi därför vilja föreslå att man startar en live-kanal av nyhetskaraktär på t.ex. YouTube, där man redovisar lösta cyberärenden, aktuella trender och först i tredje hand allmän IT-säkerhetskunskap.

Det kan vara värt att utreda det förslag som framkom under webbswinaret om att Polismyndigheten skulle kunna köpa annonsplats i samband med sökningar av exempelvis ”Köpa Bitcoin”. Att lägga annonspengar på riktade annonser skulle kunna styra in personer som riskerar att utsättas för brott till Polisens informationskällor. En förutsättning är dock att denna metod motiverar kostnaden jämfört med traditionell marknadsföring.

8.2 Teknikstöd

En stor del av brottsligheten på internet använder tekniska verktyg som ger möjlighet för ett litet antal brottslingar att genomföra en stor mängd brott. För att möta detta behöver det införas tekniskt stöd för att automatisera delar av polisarbetet, till exempel i form av automatiserade, enklare spaningsregister till AI-system för avspaning av sociala medier.

Som ett första steg föreslås en utredning och testimplementation av en förenklad insamlingsfunktion för att samla in bedrägeriförsök via mail, behandla dessa automatiskt och bygga en spaningsdatabas över malware och

annan information som kan underlätta både spaningsarbete och bevisföring. Många människor blir oroade av dessa mail men genom att på ett enkelt sätt skicka dessa till polisen kan de få ett lugnande automatiskt svar för alla mail som redan är kända.

Brottslig verksamhet drivs mestadels av ekonomisk vinning, ofta genom att använda olika former av kryptovaluta för att dölja transaktioner. Projektgruppen rekommenderar därför ett antal steg för att arbeta för en bättre möjlighet att identifiera brottslingars agerande inom kryptovalutahandel:

- Bygg upp kunskap om teknik och problem kring kryptovaluta.
- Skapa eller delta i gemensamma forensiska projekt kring kryptovaluta.
- Använd verktyg för analys – både fritt tillgängliga eller via tjänster som erbjuds av företag.
- Kartlägg och bygg upp databaser med Bitcoin-adresser som kan knytas till kriminell verksamhet.

8.3 Förändrad metodik

Internet är ett relativt nytt fält att verka på, där de två viktigaste skillnaderna är att miljön är sant global utan några som helst gränser, samt att den intensiva integritetsdebatten har gjort att krypterande och integritetshöjande lösningar har blivit mycket vanligare. Dessa två skillnader gör att man måste arbeta betydligt intensivare med infiltration än vad man gjort tidigare. Den positiva sidan av myntet är att infiltration på internet är betydligt mindre riskabelt, både säkerhetsmässigt och juridiskt, än infiltration i den ”riktiga” världen.

En ytterligare förändring som skulle behövas är en förstärkning av det internationella samarbetet, med effektivare samarbetsformer där man breddar formerna till att avtalsvägen kunna ta hjälp av andra länders förmåga till tvångsåtgärder på samma sätt som om brottet skett lokalt.

9 Referenser

Andrew, L.R., Douglas A.O. (2018) Bitcoin Investigations: Evolving Methodologies and Case Studies. *Journal of Forensic Research*, 9:420.

Athalye, A., Engstrom, L., Ilyas, A., Kwok, K. (2018). Synthesizing Robust Adversarial Examples. *Proceedings of the 35th International Conference on Machine Learning*, in PMLR 80:284-293

Avdoshin S.M., Lazarenko A.V. (2018) Bitcoin Users Deanonimization Methods. *Trudy ISP RAN/Proc. ISP RAS*, vol. 30, issue 1, 2018. Sid. 89-102.

Brottsförebyggande Rådet (2018) *Klassificering av brott – Anvisningar och regler*, Version 6.1, Juni 2018

Chang T-H., Svetinovic D. (2018). Improving Bitcoin Ownership Identification Using Transaction Patterns Analysis. September 2018. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. Sid. 1-12.

Choi, K. m fl (2018) Spreading Propaganda in Cyberspace: Comparing Cuber-Resource usage of Al Qaeda and ISIS. *International Journal of Cybersecurity Intelligence and Cybercrime*, Vol. 1, Issue 1

Cohen-Almagor, R. (2018) Cyberterrorism. In Barney Warf (ed.), SAGE *Encyclopedia of the Internet* (Thousand Oakes, CA.: SAGE Publications Inc.), Sid. 169-171

Cole, S. (2018) *Fake Porn Makers Are Worried About Accidentally Making Child Porn* [On-line], Tillgänglig på nätet: https://motherboard.vice.com/en_us/article/evmkxa/ai-fake-porn-deepfakes-child-pornography-emma-watson-elle-fanning

Collin, B. (1996) The Future of CyberTerrorism. Proceedings of the 11th Annual International Symposium on Criminal Justice issues, The University of Illinois at Chicago

Conway, M. (2014) Reality Check: Assessing the (Un)Likelihood of Cyberterrorism. In Chen, T., Jarvis, L. & Macdonald, S. (Eds.), *Cyberterrorism – Understanding, Assessment, and Response*. Springer, New York, NY

Denning, D. (2007) A View of Cyberterrorism Five Years Later. In Himma, K, (Ed) *Internet Security: Hacking , Counterhacking, and Society*. Sudbury, MA: Jones and Bartlett Publishers.

Denning, D. E. (2010) Terror's Web: How the Internet is Transforming Terrorism. In *Handbook on Internet Crime* (Y. Jewkes and M. Yar, eds.), Willan Publishing, 2010.

Denning, D. (2012) Stuxnet: What has changed?. *Future Internet*, 4, Sid. 672-687. MDPI, St. Alban-Anlage 66, 4052 Basel, SwitzerlandEuropol (2017)

Eisenstein, E (1968) Some Conjectures about the Impact of Printing on Western Society and Thought: A preliminary Report, The Journal of Modern History, Vol 40, No. 1 (Mar., 1968), 1-56 HTTP://links.jstor.org/sici?sici=0022-2801%28196803%2940%3A1%3C1%3ASCATIO%3E2.0.CO%3B2-7

Internetstiftelsen. (2018) *Svenskarna och internet – 2018*. [Online] Tillgänglig på nätet: https://internetstiftelsen.se/docs/Svenskarna_och_internet_2018.pdf

I*OCTA2017: Internet Organised Crime Threat Assessment*, The Hague: European Police Office, DOI 10.2813/55735

Europol (2018) *IOCTA2018*: *Internet Organised Crime Threat Assessment*, The Hague: European Police Office, DOI 10.2813/858843

Gordon, S., Ford, R. (2002) Cyberterrorism, *Computers and Security,* Vol 21, no 7: Sid. 636-647

Gross, M. L., Canetti, D., Vashdi, D. R. (2017) The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*. Vol 72. Issue 5. Taylor Francis Online.
[Online] Tillgänglig på nätet:
https://www.tandfonline.com/doi/full/10.1080/00963402.2016.1216502

Harlev, M.A., Sun Yin, H., Langenheldt, K.C., Mukkamala R., Vatrapu, R. (2018) Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

Harrison Dinniss, H. A. (2018) The Threat of Cyber Terrorism and What International Law Should (Try To) Do about It. *Georgetown Journal of International Affairs*. Georgetown University Press. Volume 19, Fall 2018

Heaven, Douglas (2018). Can You Spot The Crypto-Crime In This Picture? *MIT's Technology Review*. 31 maj 2018.

Herrera-Joancomartí, J. (2015) Research and challenges on Bitcoin anonymity. I Joaquin Garcia-Alfaro, Jordi Herrera-Joancomartí, Emil Lupu, Joachim Posegga, Alessandro Aldini, Fabio Martinelli,and Neeraj Suri (eds): *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. Sid 3–16. Cham, 2015. Springer International Publishing.

Holub, A., O'Connor, J. (2018) COINHOARDER: Tracking a Ukrainian Bitcoin phishing ring DNS style. *Proceedings of the APWG Symp. Electron. Crime Res. (eCrime)*. Maj 2018. Sid. 1–5.

Jarvis, L., Macdonald, S. (2014) What is Cyberterrorism? Findings from a Survey of Researchers. *Terrorism and Political Violence*. 0:1-22

Jawaheri, H.A., Sabah, M.A., Boshmaf, Y., & Erbad, A. (2018). *When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis*. *CoRR*, abs/1801.07501.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. [On-line], Tillgänglig på nätet: https://Bitcoin.org/Bitcoin.pdf

Remy, C., Rym, B., Matthieu, L. (2017). Tracking Bitcoin users activity using community detection on a network of weak signals. *The 6th International Conference on Complex Networks and Their Applications*, Nov 2017, Lyon, Frankrike. Sid. 166–177. Springer.

Singer, P. W. (2012) *The Cyber Terror Bogeyman*. The Brookings Institution. Washington, DC. [Online] Tillgänglig på nätet: https://www.brookings.edu/articles/the-cyber-terror-bogeyman/

Skatterättsnämnden. (2018-04-18). Avyttring av Bitcoin. Avyttring av Bitcoin ska beskattas enligt bestämmelserna om andra tillgångar i 52 kap. 3 § inkomstskattelagen (1999:1229). [Online] Tillgänglig på nätet: https://www.skatterattsnamnden.se/publiceradeforhandsbesked/2018/avyttringavBitcoin.5.14dfc9b0163796ee3e77480d.html

Sveriges Riksdag (2018) Lag (2003:148) om straff för terroristbrott. Uppdaterad t.o.m. SFS 2018:1312

Titanium (2018) *Tools for the investigation of transactions in underground markets*. EU. [Online] Tillgänglig på nätet: https://www.titanium-project.eu/

Traynor, I. (2007) Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. 2007-05-17

Volety T., Saini S., McGhin T., Zhechao Liu C., Choo K.K.R. (2018) Cracking Bitcoing Wallets: I want what you have in the wallets. *Future Generation Computer Systems*. Volume 91, publiceras februari 2019, onlineversion tillgänglig 31 augusti 2018. Sid. 136-143.

Bilaga 1 - Intervjumanus

Inledning

Projekt Cyberhot är ett kunskapsuppbyggande projekt som är finansierat av Försvarsdepartementet och sträcker sig över två år och avslutas vid årsskiftet. Syftet med projektet är primärt att FOI ska bygga upp kunskap om Polisen och de utmaningar som Polisen står inför avseende IT-brott.

Om vi kan kommer vi även att ge förslag på lösningar eller fortsatt forskning som kan bidra till att lösa problem.

Intervjusvaren kommer att hanteras konfidentiellt, men om någon begär ut underlagen från myndigheten så har vi inte laglig grund att vägra.

Vill du vara anonym eller får vi referera?

Den Intervjuades namn, befattning, datum (alternativt löpnummer)

(Genom att slå radmatning efter en fråga så skapas automatiskt en bullet-list med svar.)

Kan du förklara lite om dina arbetsuppgifter?

Hur länge har du jobbat som polis?

Vad är din uppfattning om brott på nätet?

Vilka är de primära utmaningarna?

Vad är din uppfattning gällande hur stort inflödet gällande internet relaterad brottslighet är?

I vilken utsträckning kommer du i kontakt med sociala medier?

På vilket sätt (inifrån och ut eller utifrån och in)

Hur mycket frågor får du om sociala medier?

Har du någon polis-profil på nätet?

Arbetar du med sociala medier?

Vad gör du på sociala medier?

Hur arbetar du med ungdomar?

Går det arbetet att applicera på internet?

Har du upptäckt något brott på internet?

I vilket sammanhang?

Ledde det till något?

Tror du att polisen skulle kunna ”patrullera” på nätet

- Patrullerar du på nätet?
- Hur skulle det gå till?
- Vad skulle det kunna leda till?

Hur agerar du när du utsätts för hot och bedrägeriförsök på nätet?

Om du tar upp en anmälan gällande brott på nätet, vad händer med den sedan?

Hur vet du hur du ska brottsrubricera?

- Vilken hjälp har du för att avgöra vilken brottsrubricering som ska användas?
- Finns det underkategorier gällande denna typ av brottslighet t ex medelst… för att samla statistik?

Vilket stöd/hjälp kan du få lokalt, regionalt, central?

När, om och hur vänder du dig till central nivå för råd/stöd?

Vilka förstahandsåtgärder görs vanligtvis? (Vid en anmälan?)

Vad och när skickas ärendet vidare internt för att utreda vidare?

Hur arbetar ni regionalt med brottslighet på nätet?

- Vilka direktiv går ut centralt?
- Vilken utbildning får de enskilda poliserna gällande detta?

Vilken utbildning skulle vara önskvärd?

Vilka verktyg skulle du behöva för att hantera IT-relaterade brott?

Hur tycker du att Polisens hantering av IT-relaterade borde utvecklas?

Finns det något ytterligare som du tycker vi borde ha kännedom om?

Bilaga 2 - Resultatrapport från Xamera

I studien har 22 personer medverkat och bidragit till dess resultat genom att polisanmäla hotfulla spam-mail som skickats till deras mailadress och dela med sig av sin upplevelse. Nedan presenteras resultatet av studien.

Deltagare och anmälningssätt

Studien har haft 22 deltagare. Fem av dessa har polisanmält via telefon och resterande 17 personerna har anmält fysiskt på 15 olika polisstationer. Två av de som har anmält via telefon har försökt anmäla på polisstationen men har fått vänta väldigt länge så anmälning fick ske via telefon istället.

Anmälningar

Utav de 22 deltagarna har 17 personer lyckats anmäla medan fem personer inte har fått anmäla. Av dessa fem personer försökte två anmäla via telefon och övriga tre personer försökte anmäla fysiskt på olika polisstationer.

De som lyckats anmäla

Bemötande

Tolv deltagare ansåg att de hade blivit mycket bra och trevligt bemötta. De har uttryckt ord som proffsigt, hjälpsam, pedagogiskt, snabbt och förstående. Tre personer upplevde bemötandet som trevligt men med en underton av att ärendet inte skulle leda någon vart och att det skulle läggas ner omedelbart. En deltagare upplevde ett gott bemötande över telefon även om de sa att det var onödigt för hen att anmäla fick hen tillslut anmäla ändå. Samma person fick däremot inte ett bra intryck på polisstation där hen försökte anmäla innan. På polisstationen verkade kösystemet inte vara igång eftersom hen var näst på tur i 50 min. Det fanns inte någon som kunde svara på hur lång tid det skulle ta heller. Ytterligare en deltagare fick ge upp att anmäla på en polisstation då hen fick vänta väldigt länge. Över telefon upplevde hen att bemötandet var trevligt men något uppgivet. Deltagaren fick anmäla tillslut efter att ha stått på sig.

Brottsrubricering

Två personer fick inte svar på frågan om vad det skulle bli för brottsrubricering. Den vanligaste brottsrubriceringen var utpressning som uppgavs av sex deltagare. Två deltagare fick rubriceringen försök till utpressning och dataintrång. Tre stycken fick svaret att det skulle bli försök till bedrägeri eller bedrägeri. Sedan var det även enstaka brottsrubriceringar:

- Utpressning men även förtal och dataintrång om uppgifterna visade sig stämma
- Försök till bedrägeri och dataintrång
- Hot och utpressning/mängdbrott
- Olaga hot

Kopia på anmälan

Endast två personer fick en kopia på sin anmälan. Tre personer uppgav att de kunde få en kopia men att de i så fall behövde vänta 20–40 minuter för att få den godkänd av utredare, en svarade att de inte visste hur lång tid det skulle ta.

Övriga tolv deltagare har inte fått en kopia på plats varav två har fått förklaringen att det inte är möjligt att få en kopia på anmälningen vid anmälningstillfället. Fem har endast uppgett att de inte fått en kopia. Sju deltagare har fått svaret att den kommer skickas via post inom en vecka.

De som inte lyckats anmäla

Anledningar

Anledningarna till att de inte har fått anmäla har varit olika. En fick förklaringen att hade tillräckligt med underlag för dessa sorters bedrägeriförsök. Samma gällde för en annan av polisstationerna men där förklarade de att det hade kommit in för många anmälningar så de hade fått direktiv om att inte ta emot anmälningar från privatpersoner. De förklarade att de arbetar med att ta reda på var mailen kommer ifrån och hur de ska kunna stoppas. En fick svaret att de tyckte att det var fjantigt och slöseri med polisens resurser samt att de inte kunde att det skulle leda till något. En av deltagarna som anmälde via telefon fick svaret att de inte tog emot anmälningar om spam. När personen förklarade att det var innehållet i mailet hen ville anmäla fick personen fortfarande inte anmäla. Sista personen fick förklarat att de hade fått tusentals anmälningar men de kunde konstatera att det inte rörde sig om något brott. Polisen hade då uttryckt att amerikanarna bryr sig inte om något annat än terror så det är ingen idé.

Bemötande

Två av deltagarna hade fått ett trevligt bemötande och polisen hade varit hjälpsamma. En tredje deltagare hade blivit artigt bemött men upplevt polisen som ointresserad. De två sista deltagarna som inte fick anmäla hade fått väldigt otrevligt bemötande av polisen. Polisen lade till och med på luren mitt i samtalet för en av deltagarna som försökte anmäla via telefon.

Övrig återkoppling från deltagarna

- En deltagare upplever att polisen verkligen behöver mer kunskap kring IT för att kunna se helheten.
- Flera av deltagarna uppger att handläggarna kände igen denna typ av mail och att de hade fått in anmälningar förut. Flera har även fått veta att det inte kommer leda någon vart och en fick höra att det inte går att spåra mailen så långt för att kunna gripa en gärningsman.
- I ett av fallen erbjöd sig receptionisten att ta emot en direktanmälan men deltagaren uppgav att hen ville prata med polis istället vilket hen fick.
- En deltagare hade med sig mail som stod att det var från den egna mailadressen men även andra adresser. De mailen med andra adresser än ens egna var tydligen nytt för polisen.
- En deltagare fick det förklarat att det finns en utredningsgrupp inom mängdbrott som arbetar med att reda ut just denna typ av scam.
- En fick förklarat att polisen har gått ut och varnat för att denna typ av meddelande har spridits i stor omfattning, att de är väl kända för polisen men de har uppmanat om att inte bry sig om dem.

- En polis hade uttryckt tacksamhet för anmälan då det kunde ge mer synlighet i hur stort problem det är och genom det kan det kanske tillsättas resurser i framtiden även om ärendet troligtvis skulle läggas ner omgående.
- En person fick lite kort information om säkerhet och förklarade att hen skulle se över hur ofta hen bytte lösenord och vilka lösenord hen hade. Samma polis berättade även att man arbetar med ärendet och har kommit fram till att mailen skickas från två servrar, en i Mexiko och en i Thailand. Tydligen har beloppet höjts från $600 till (i deltagarens fall) $967. Ytterligare en deltagare hade uppmanats att byta lösenord.

Övriga reflektioner från mig inför webbinaret

Jag tror att det skulle vara bra att fråga igen hur många som upplevde att polisen gladeligen/motvilligt tog upp anmälan, då det verkar ha varit väldigt skiftande.

Övrig info angående de som inte valt att delta i undersökningen

Jag har även pratat med några via telefon eller som jag har träffat som inte har velat delta. Jag har ingen bra statistik över detta men de har i så fall inte orkat eller inte haft tid, skulle gissa att dessa personer kanske rör sig om runt fem personer. Men via facebook har jag haft kontakt med flera potentiella deltagare, med kontakt menas att de har svarat på mitt första PM minst en gång.

- Två bor utomlands men tyckte det var bra initiativ och önskade att de kunde vara med.
- Tre personer kunde tänka sig att vara med men när hen fick reda på att det rörde sig om polisanmälan tyckte hen att det var slöseri med polisens resurser och att de inte kommer kunna spåra vem som skickat det ändå.
- En person trodde inte att en anmälan skulle göra någon skillnad eftersom hen tror att polisen inte har tillräckligt med resurser att hantera dessa volymer ändå.
- En person har övervägt att anmäla men upplever att dessa typer av brott inte prioriteras ändå. Hen menar att anmälan borde gå att göras elektroniskt och tror att anmälningsbenägenheten hade definitivt förändrat anmälningsstatistiken.
- Två personer orkade inte anmäla. En av dem menade att det fanns väldigt lite att göra åt detta och att det finns scamförsök som är värre.
- En person ansåg att studien var intressant och ville gärna ta del av resultatet. Dock var hen inte intresserad av att delta själv då hen har haft konkret erfarenhet av polisen och dess hantering av bedrägerier som initialt börjar på nätet. Efter det var förtroende förstört och hen ville undvika kontakt med polisen om hen inte var tvungen.

- Tre personer kunde inte delta på grund av tidsbrist. En av dessa var dock intresserad av resultatet då hen hade negativa erfarenheter av polisens hantering av identitetskapningar via nätet.
- En slutade svara efter att ha hört syftet utan vidare förklaring, två till valde att avstå utan vidare förklaring när de hört syftet.
- En person ville inte delta eftersom hen ansåg att det endast var spam.
- Två slutade svara efter att ha visat intresse för att delta utan vidare förklaring.
- Två kunde inte delta på grund av sjukdom.
- Fyra personer som var bestämt att de skulle delta i studien polisanmälde aldrig. Två av dessa meddelade att de inte hann och två av dem slutade svara.

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

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

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

www.foi.se