Københavns Universitet

Sociologisk institut

Policing af kryptomarkeder

Jakob Demant & Rasmus Munksgaard

Det projekt, der beskrives i denne rapport, er støttet økonomisk af Justitsministeriets Forskningspulje. Projektets gennemførelse og resultater er alene forfatternes ansvar. De vurderinger og synspunkter, der fremsættes i rapporten, er forfatternes egne og deles ikke nødvendigvis af Justitsministeriet.

Indhold

Kapitel 1

Indledning

I denne rapport udreder vi, hvorledes interventioner mod online-markeder for stoffer, såkaldte kryptomarkeder, påvirker købere og sælgeres opfattelse af risiko. Med udgangspunkt i *Operation Hyperion* benytter vi en *mixed methods*-tilgang, som kombinerer flere forskellige typer data fra etnografi, interviews og observationer. Tidligere forskning har vist, at kryptomarkederne forandrer risikoaspekterne i visse led af narkotikadistributionen, eksempelvis for grossister og slutbrugere. Denne rapport søger at afdække konsekvenserne og opfattelserne af særligt politiaktionen Operation Hyperion. Operationen blev i særlig grad gennemført i Holland og Sverige, men Danmark deltog ikke. Denne rapport behandler betydningen og effekten af operationen og udreder, hvorvidt en lignende operation med fordel kan gennemføres i Danmark.

Forskningen omhandlende betydningen af forskellige politiaktioner rettet mod traditionelle stofmarkeder har haft den udfordring, at adgangen til pålidelige data er meget vanskelig. Vores adgang til data på kryptomarkederne betyder, at vi har unik mulighed for at afdække konsekvenserne på sikker vis. Tidligere forskning har vist, at politiaktioner mod kryptomarkeder tilsyneladende ikke resulterer i hverken faldende omsætninger, færre sælgere eller højere priser. Ser man på de økonomiske faktorer, er der således ikke sikkerhed for, at interventionerne har målbare effekter. Kvalitative studier viser, at nogle brugere efterfølgende har taget sofistikerede teknologier og praksisser i brug for at sikre egen sikkerhed, hvormed interventioner kan siges at have haft en såkaldt 'target hardening-effekt'. Desuden rapporterer studierne, at interventionerne generelt afstedkom en følelse af usikkerhed på markederne (Bancroft & Reid, 2016a; Barratt, Lenton, Maddox, & Allen, 2016; Soska & Christin, 2015). Disse observationer giver ikke nødvendigvis udslag i økonomiske indikatorer, men kan påvirke markeder over længere sigt.

Kapitel 2

Baggrund - Policing af kryptomarkeder

I dette afsnit introducerer vi først kryptomarkedet som fænomen og opsummerer dernæst den eksisterende relevante forskning på området. En mere udførlig introduktion til kryptomarkeder er tilgængelig i rapporten *Kryptomarkeder i en dansk og skandinavisk kontekst* (Demant & Munksgaard, 2017). Efterfølgende udreder vi de politiindsatser og strategier, der er rettet mod kryptomarkeder. Vi tager udgangspunkt i to begreber, *displacement* og *deterrence*, som er centrale begreber både i forbindelse med indsatser mod kryptomarkeder såvel som for forståelsen af denne undersøgelses fund. Vi gennemgår dernæst en række relevante indsatser og operationer, som har haft til formål at inddæmme aktiviteten på kryptomarkeder. Endeligt skitserer vi nærværende undersøgelses motivation og målsætning.

2.1 Kryptomarkeder

Begrebet *kryptomarked* dækker over en række markeder, som deler karakteristika. Kryptomarkederne omtales også som *darknet markets*, *dark markets* eller *anonymous online markets* (Broséus et al., 2016; Christin, 2013; Europol, 2014; Soska & Christin, 2015). Begrebet *kryptomarked* blev første gang benyttet af Martin (2014a, 2014b) og henviser til *"an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities"*. Herunder hører særligt brugen af virtuelle valuta til transaktioner samt anonymiserings- og krypteringsteknologier, som anvendes for at sikre brugernes sikkerhed og anonymitet. Kryptomarkeder er opbygget og organiseret relativt ens. Administrator(er) tilbyder en platform, hvor sælgere kan sælge varer mod en kommission på typisk 4-8% (Martin, 2014a, 2014b). I den forstand er platformen

decentraliseret på samme vis som eBay og lignende legale online-markeder (Aldridge & Décary-Hétu, 2016; Barratt, 2012). Markederne har fællestræk med markeder for stjålen data. Disse to typer markeder har enslignende modus operandi, men kryptomarkederne adskiller sig ved primært at facilitere handel med illegale stoffer og ved, at de typisk er mere organisatorisk strukturerede, end det er tilfældet med markeder for stjålen data (se eksempelvis Holt, Smirnova, & Chua, 2016; Hutchings & Holt, 2017). Kryptomarkederne er således en af flere måder, hvorpå internettet i stigende grad benyttes til stofdistribution, men kryptomarkederne adskiller sig i kraft af deres decentrale opbygning og sofistikerede brug af teknologi fra både gråzone-apoteker (Hall, Koenraadt, & Antonopoulos, 2017), handel på sociale medier (Stevens, Gilliard-Matthews, Dunaev, Woods, & Brawner, 2016) og salg af *new psychoactive substances* (Brunt et al., 2017).

2.2 Afskrækkelse og forflyttelse

I traditionelle illegale markeder er forflyttelse, *displacement*, en kendt reaktion på policing. Cross (2000) påpeger, at stofsælgere har to strategier, de kan benytte for at minimere risiko. Enten kan de søge at undgå politimyndighederne, eller de kan 'give risikoen videre' til køberne. Dette er en dynamisk proces: når politimyndighederne eller lovgivning gør en indsats mod et marked, flyttes eller dæmpes aktiviteten i den pågældende lokation. Denne proces kaldes *spatial displacement* (Finn & Stalans, 2016, p. 581). Finn & Stalans (2016) påpeger eksempelvis, hvordan regulære indsatser mod sælgere af seksuelle ydelser begrænser aktiviteten på den konkrete lokation, samt hvorledes sælgere og købere herefter finder en ny lokation, hvor transaktionen kan foregå. Eksempelvis er en af de risikominimerende strategier benyttet af amerikanske *"pimps"* at fjerne deres aktivitet fra platforme, som aktivt overvåges af politimyndigheder og i stedet flytte aktiviteten til lukkede platforme, som ikke overvåges (Finn & Stalans, 2016, p. 583). Ligeledes viser Maher & Dixon (1999), hvordan intensiv policing af et åbent stofmarked har som konsekvens, at købere og sælgere skifter lokationer, hvor Cross (2000) peger på displacement som en kritisk del af stofsælgeres repertoire for risikominimering.

Deterrence, *afskrækkelse*, er et kriminologisk begreb, som dækker over en antaget psykologisk proces, hvor *"individer afskrækkes fra at begå illegale handlinger, hvis de opfatter juridiske sanktioner som sikre, hurtige og/eller hårde"*[1] (Williams & Hawkins, 1986, 545). Deterrence kan måles og forstås på forskellige måder: gennem forholdet mellem straf og udøvet kriminalitet eller gennem lovbryderes opfattelser af straf. Der er evidens for, at deterrence har en effekt på individets beslutning om at begå kriminalitet (Nagin,

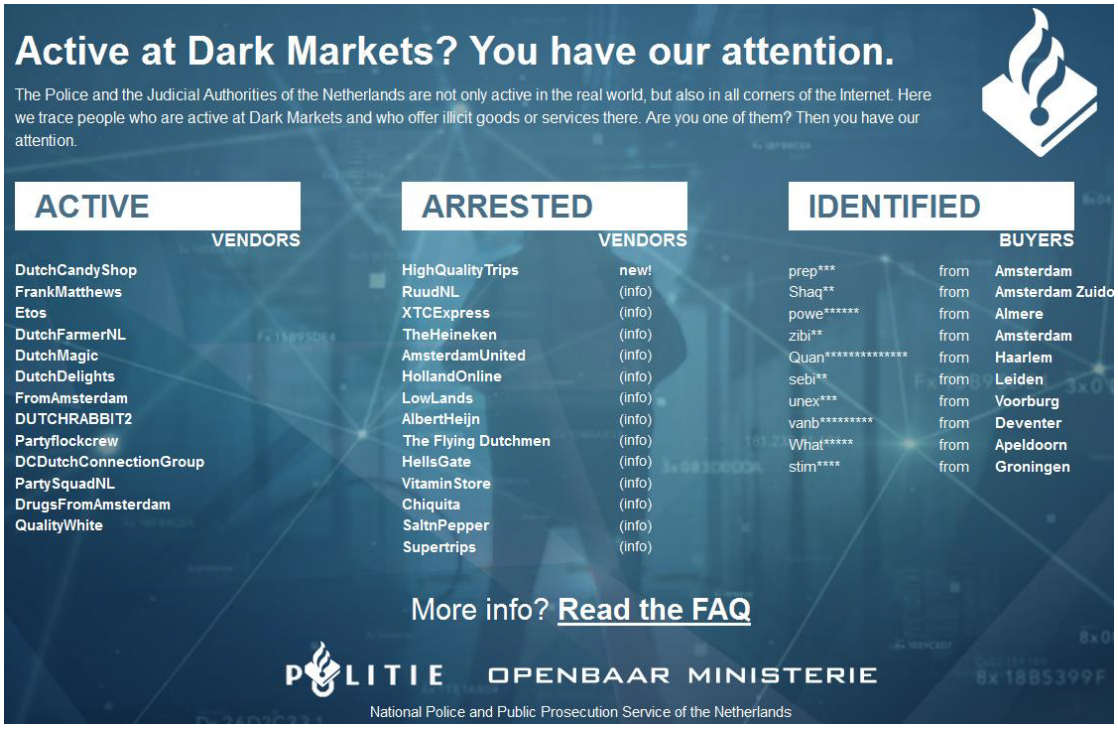
[1] Forfatternes oversættelse af *"Deterrence theory implies a psychological process whereby individuals are deterred from committing criminal acts only if they perceive legal sanctions as certain, swift, and/or severe."*

1998). Effektens form og virkning afhænger af konteksten for det potentielle lovbrud og straffen den potentielle straf for det pågældende lovbrud (Nagin & Pogarsky, 2001). Williams & Hawkins (1986) udvider forståelsen af deterrence med fokus på, hvorledes individet opfatter den potentielle sanktions alvorlighed og sandsynlighed for straf. Flere studier viser, at opfattelser af potentielle sanktioner for lovbrud er en dynamisk størrelse, som ikke er stabil over tid (Williams & Hawkins, 1986, p. 552). For at forstå hvorledes afskrækkelse og de konkrete effekter af politioperationer mod kryptomarkeder påvirker risikoopfattelser, må vi nødvendigvis forstå, hvorledes risikoopfattelser skabes og konstrueres *mellem* lovbrydere. Eksempelvis viser Dickinson & Wright (2015), hvorledes stofsælgere aktivt justerer deres opfattelse af trusler baseret på input såsom andres og egne erfaringer omhandlende risiko for straf. Begrebet *perceptual deterrence*, som betyder opfattet afskrækkelse, referer til den specifikke forståelse af afskrækkelse som en subjektiv og dynamisk frem for objektiv vurdering af omkostningerne ved et lovbrud (Paternoster, 1987; Strelan & Boeckmann, 2006). Således kender en person, som overtræder loven, ikke den faktiske sandsynlighed for anholdelse eller sigtelse (Loughran, Paternoster, Piquero, & Pogarsky, 2011). I stedet må hun fundere sin vurdering på den tilgængelige sparsomme information.

Vi betragter disse to begreber, *deterrence* og *displacement*, som udtryk for processer, der informerer hinanden. Den psykologiske proces, hvor lovbrydere danner sig opfattelse af risikoen ved et lovbrud, kan eksempelvis lede til en rationel beslutning om at forflytte sin aktivitet for at minimere selvsamme risiko. Begge begreber er særligt relevante for vores forståelse af politiindsatser mod kryptomarkeder. Displacement er relevant, fordi købere og sælgere ved lukning af markeder enten må opgive eller forflytte deres aktivitet. Dette foregår på samme vis, som når stofsælgere og stofkøbere i den urban-geografiske virkelighed skifter købs- og salgssted som konsekvens af politiindsatser (Maher & Dixon, 1999). Ligeledes er særligt *perceptual deterrence* relevant, fordi dette begreb har individets kontinuerlige refleksioner over risici for øje. Denne proces kan illustreres ved en køber af narkotika på kryptomarkeder, som ved sine første køb er frygtsom, og som ved efterfølgende køb justerer sin risikoopfattelse på baggrund af de erfaringer, hun gør sig. Hvis et enkelt køb - eller hvis ingen køb - stoppes i toldkontrollen, vil dette antageligvis have indflydelse på købers risikoopfattelse og efterfølgende på hendes beslutning om enten at stoppe eller fortsætte med at købe. Begge begreber er benyttet i studier af, hvorledes policing påvirker kryptomarkeder, som vi gennemgår i det følgende afsnit .

2.3 Operationer mod kryptomarkeder

Det første kryptomarked for narkotika, Silk Road, blev lanceret i 2011 (Barratt, 2012; Christin, 2013), og i 2013 blev siden lukket af FBI i samarbejde med en række andre myndigheder. På kort sigt fjernede dette den største markedsplads for narkotika på mørkenettet, men få uger senere havde købere og sælgere migreret til nye sider (Van Buskirk, Roxburgh, Farrell, & Burns, 2014). I 2014, året efter lukningen af Silk Road, var de største markeder Silk Road 2.0, Agora Marketplace og Evolution Marketplace. I november 2014 blev 417 hidden services lukket og 17 personer anholdt i et internationalt samarbejde kaldet Operation Onymous, som var koordineret af Europols center for cybercrime, EC3 (Europol, 2014). Dog mener kritikere, at antallet af hidden services, som blev lukket i forbindelse med Operation Onymous, var overestimeret, da flere af de sider, der blev lukket i forbindelse med operationen, var phishing-sider, kloner eller decideredе svindelsider(Cubrilovic, 2014). Dog blev kryptomarkederne Silk Road 2.0, Hydra, Could-Nine, Blue Sky og TorBazaar lukket under Operation Onymous, hvoraf Silk Road 2.0 var det største (Soska & Christin, 2015). Senere er to store markeder lukket, men dette skyldes ikke politiindsatser. Evolution lukkede i foråret 2015 som et *marketplace exit scam*[2], mens Agora lukkede i august 2015 og betalte kunderne tilbage (Greenberg, 2015).



[2]Administratorerne af Evolution lukkede siden og forsvandt med alle bitcoins i escrow.

I 2016 præsenterede en række politimyndigheder, herunder det amerikanske DEA, ATF og FBI, det hollandske politi og det svenske politi, resultater fra den fælles *OperationHyperion*, som var rettet mod kryptomarkeder (Cox, 2016). Det svenske politi beskrev, hvorledes de var i besiddelse af 3.000 navne på købere, og FBI mødte personligt op hos 150 mistænkte købere. Mest bemærkelsesværdig var det hollandske politis oprettelse af en *hidden service* på mørkenettet på kryptomarkederne, hvor de publicerede navnene på en række sælgere samt information på købere.

Operationen fremstår utraditionel til sammenligning med tidligere operationer. Dette skyldes særligt det hollandske politis offentliggørelse af sælgere under observation samt det målrettede fokus på købere i både Sverige og USA. Operation Hyperion var, ligesom indsatserne mod Silk Road og Operation Onymous, et internationalt samarbejde, men hvor de to førstnævnte fokuserede på administratorer og markeder, fokuserede Operation Hyperion udelukkende på aktive sælgere og købere. Der blev ikke lukket markedspladser i forbindelse med operationen, og både købere og sælgere blev fremhævet som identificerbare og under efterforskning. Der er sparsom information omhandlende operationens planlægningsfase og det internationale samarbejde, men i afsnit 4.1 belyser vi operationen på baggrund af en række interviews med det hollandske politi.

2.4 Effektiviteten af politioperationer

Baseret på deres longitudinelle studie af kryptomarkeder peger Soska & Christin (2015) på, at kryptomarkedernes økosystemer er særdeles *resilient* over for myndigheders indgriben. Den samme konklusion nås i lignende studier, som har undersøgt relationen mellem politiindsatserne og kryptomarkederne (Décary-Hétu & Giommoni, 2016; Ladegaard, 2017; Van Buskirk et al., 2017, 2014). Ad forskellige veje måler disse studier effekten af *displacement*, forflyttelse, eller *deterrence*, afskrækkelse, gennem indikatorer såsom antallet af transaktioner, antallet af sælgere, omsætning og varepriser.

Ladegaard (2017) følger kryptomarkederne Evolution og Agora i perioden november 2014 til marts 2015. I denne periode fandt retssagen mod administratoren af Silk Road sted under stor mediebevågenhed, og Ladegaard finder, at der i perioderne med øget medieeksponering fulgte øget handel på de to kryptomarkeder. Ladegaards (2017) fund peger således på, at politiindsatser og retsforfølgelser ikke har direkte afskrækkende effekt på køberne. Tværtimod tyder det på, at medieopmærksomhed opmuntrer til brug. Décary-Hétu & Giommoni (2016) finder, at der i perioden lige efter Operation Onymous foregik færre transaktioner, og at operationen tilsyneladende havde afskrækkende effekt. Dog varede effekten kun i en til to måneder, hvorefter salget var normalt igen. Omend markeder er særligt modstandsdygtige, og selvom økosystemet hurtigt kommer sig efter

en politioperation som Operation Onymous, finder Décary-Hétu & Giommoni (2016), at mange sælgere bliver inaktive og ikke flytter deres forretning til andre markeder. Det er dog svært at drage sådanne klare konklusioner, da sælgere kan oprette profiler på andre markeder og anvende nye identiteter. Oprettelsen af nye identiteter på andre markeder er således en mulig risikominimeringsstrategi, som sælgerne kan anvende i tilfælde, hvor politiet har beslaglagt servere, som indeholder databaser med deres tidligere aktiviteter. Her er både deterrence og displacement relevante begreber, da nogle sælgere afskrækkes fra at være aktive, mens andre flytter sig til nye lokationer. Van Buskirk et al. (2014) drager her en parallel til det online-marked for NPS, *new psychoactive substances*, hvor kunder skifter sælgere, når en butik lukkes, og når nye produkter introduceres, når de gamle produkter ulovliggøres. Denne form for displacement er desuden velkendt fra studier af internetfora, hvor stjålen data sælges (Soudijn & Zegers, 2012).

Prisen på illegale stoffer er tæt forbundet til risikoen associeret med fremskaffelse, distribution og salg (Caulkins & Reuter, 2010; Desimone, 2006). Risiko fungerer således som en 'skat' på narkotika. Décary-Hétu & Giommoni (2016) studerer priserne efter Operation Onymous og finder overraskende, at priserne på kryptomarkeder ikke steg efter operationen. Dette fund kan tolkes som en indikation på, at sælgerne ikke vurderede deres risiko øget i forbindelse med Operation Onymous (Décary-Hétu & Giommoni, 2016).

Ser vi på de kvantitative indikatorer, finder tidligere studier, at **a)** kryptomarkedernes økosystem er særdeles resilient overfor politiindsatser, **b)** der er begrænset deterrent-effekt i form af sælgere, som stopper og lavere efterspørgsel i en kort periode efter operationer, **c)** der er indikation på, at øget medieopmærksomhed som følge af politioperationer kan lede til øget brug, og **d)** prisen på narkotika påvirkes ikke af politioperationer.

2.4.1 Politimyndigheders redskaber og strategier

Myndigheder har en række midler til rådighed for intervention mod ulovligt online-indhold (Goldsmith, 2000; Hutchings & Holt, 2015). Dette ses eksempelvis i listen over blokerede internetadresser i Danmark, som indeholder sider blokeret grundet børnepornografi, gambling eller lægemiddelsalg (Teleindustrien, 2017). Ligeledes er det muligt at anmode hosting-firmaer om at lukke sider eller anmode ansvarlige om at deregistrere internet-domæner. Disse strategier kan dog kun benyttes på *clear web*, da siderne på mørkenettet er anonymiserede via Tor. Derfor kan de ikke blokeres uden samtidigt at blokere adgangen til Tor, og ligeledes kan serveren ikke lokaliseres, hvilket umuliggør lukning via hosting-firmaer. Dette er dog ikke ensbetydende med at politimyndigheder intet kan stille op. Kruithof et al. (2016) foreslår fire brede strategier, som myndigheder og politi

kan benytte sig af: **1)** traditionelle efterforskningsstrategier, **2)** identifikation og beslaglæggelse i postsystemet, **3)** online-detektion, som eksempelvis kan foretages ved sporing af bitcoin og **4)** lukninger af markedspladser.

I det følgende skitserer vi konkrete eksempler på anvendelse af disse strategier og tilføjer yderligere to strategier: *langsigtet disruption* samt *hacking og lukning af markedspladser*. Den kategorielle opdeling er idealtypisk, fordi strategierne i praksis ofte have overlappende karakteristika.

2.4.1.1 Traditionelle efterforskningsstrategier

Både Kruithof et al. (2016) og Buxton & Bingham (2015) påpeger, at traditionelle efterforskningsstrategier har vist sig at være succesfulde i indsatsen mod kryptomarkeder. Disse kan eksempelvis bestå i såkaldte *controlled buys*, kontrollerede køb, hvor politimyndigheder bestiller et produkt og benytter dette som bevismateriale og i efterforskningen. Et konkret eksempel herpå er identifikationen og anholdelsen af sælgeren *NOD*, som efterfølgende blev rekrutteret som informant (Mullin, 2015). Rekruttering af informanter med privilegeret adgang til markeder er ligeledes benyttet i indsatser mod fora, som faciliterer salg af stjålen data. Eksempelvis infiltrerede FBI administrationen for foraet *DarkMarket*, et forum for handel med stjålen data (Hutchings & Holt, 2017), som efterfølgende gav adgang til kommunikationen på siden. En lignende infiltration blev foretaget af FBI, for hvem det lykkedes at infiltrere administrationen af både Silk Road og Silk Road 2.0 (Jeong, 2015). Endeligt peger Kruithof et al. (2016) på, at eftersom sælgere på kryptomarkeder nødvendigvis må operere offline, eksempelvis gennem indkøb eller dyrkning af produkt, kan efterforskninger med fordel begynde her.

2.4.1.2 Postsystemet

Produkter købt på kryptomarkeder passerer gennem postsystemet. Omend store dele af handlen fungerer inden for landegrænser (Demant & Munksgaard, 2017), må mange pakker formodes at krydse landegrænser. Således kan handlen detekteres, og denne detektion kan give materiale til efterfølgende præventive indsatser eller retsforfølgelser. I 2015 identificerede tysk politi eksempelvis sælgeren *Shiny-flakes* (Locker, 2015). Sagen begyndte med en mistænkelig pakke, som manglede porto, og den efterfølgende efterforskning ledte til anholdelsen af sælgeren, som var i besiddelse af narkotika til en værdi af 4.1 millioner euro. Yderligere betød identifikationen af pakken, at lignende pakker kunne profileres og stoppes. Detektion i posten knytter sig til de ovennævnte traditionelle efterforskningsstrategier, da detektionen således kan påbegynde en efterforskning. Samtidig kan en sådan efterforskning særligt lede til identifikation af købere. Tysk politi

formåede at få adgang til *Shiny-flakes*' krypterede harddisk og fik derigennem adgang til et kunderegister, som indeholdt information på købere.

2.4.1.3 Online-detektion og sporing af bitcoin

Kruithof et al. (2016) placerer to relativt forskellige teknikker under samme strategi. Slobbe (2016) foreslår investeringer i *"big data techniques, in order to link vendor nicknames and internet activity with certain IP addresses"*. Det foreslås dog ikke konkret, hvorledes det i praksis skal foregå. En mulig tolkning kunne være identifikation af sælgere baseret på deres brug af Tor monitoreret gennem internetudbydere. Sådanne metoder ville bevæge sig ind i ophedet politisk territorie, da en sådan identifikation ville nødvendiggøre bred dataindsamling via internetudbydere. Særligt i forbindelse med debatten om overvågning og borgerrettigheder, vil anvendelsen af en sådan metode formentlig være et sensitivt forslag (Barratt, Lenton, & Allen, 2013; Goldsmith, 2000; Watson, Finn, & Barnard-Wills, 2017).

Kryptomarkeder anvender bitcoin til transaktioner. Alle bitcoin-transaktioner er pseudonyme og offentligt tilgængelige i en såkaldt *blockchain*. Implikationen af dette er, at der i en vis grad kan identificeres entiteter, som opererer i bitcoin-økonomien, og aktivitet kan knyttes til disse. Europol har i denne anledning indgået et samarbejde med firmaet Chainalysis, som desuden samarbejder med amerikanske, asiatiske og individuelle europæiske politimyndigheder (Europol, 2016). Yderligere eksisterer et open-source alternativ med lignende funktionalitet, BitCluster, som blev frigivet med henblik på forskningsbrug (Lavoie & Décary-Hétu, 2017). Forfatterne er bekendt med to jyske politisager, hvor bitcoin-transaktioner har fungereret som bevismateriale (Bjørnager & Mortensen, 2017a, 2017b). I disse sager har køberne på kryptomarkedet solgt narkotika offline, og blev identificerede efter pakkerne blev opfanget i toldkontrollen. Herefter har politiet identificeret bitcoin-adresser hos de dømte, som kunne knyttes til flere transaktioner på kryptomarkeder. Vi noterer her, hvorledes pakker identificeret i toldkontrollen begyndte efterforskninger, hvorefter traditionelle efterforskningsstrategier blev taget i brug. Bitcoin fungerer således i denne forbindelse nærmere som yderligere bevismateriale end som grundlag for en efterforskning.

2.4.1.4 Hacking og lukning af markedspladser

Goldsmith (2000) påpeger, at politimyndighederne er i besiddelse af en række redskaber til at kontrollere af illegal aktivitet online. Herunder hører særligt lukning og blokering af sider, som faciliterer illegal aktivitet, og herunder fora for salg og køb af stjålen data. Hutchings & Holt (2017) påpeger herunder særligt kapabiliteten til at de-registrere

internetdomæner, blokere adgang eller konfiskere servere. Disse strategier er enten ikke mulige eller særligt ressourcekrævende for kryptomarkederne (Barratt et al., 2013). I de tilfælde hvor kryptomarkeder er blevet lokaliseret og efterfølgende lukket, som er en strategi i tråd med hvad Hutchings & Holt (2017) foreslår, har dette muligvis involveret hacking. De konkrete detaljer om, hvordan siderne blev lukket i forbindelse med Operation Onymous samt lukningen af Silk Road er dog ukendte (Cox, 2015; Greenberg, 2014). Der er spekulation om, hvorvidt forskere associeret med Carnegie Mellon University udførte et angreb, som deanonymiserede brugere af Tor-netværket, og om de senere leverede oplysninger til FBI, som dannede grundlag for Operation Onymous. Dette er dog ikke bekræftet (Hill, 2014; Tor Project, 2015). En konsekvens af sådanne indsatser er dog, at både udviklere af legal teknologi (eksempelvis Tor) og lovbrydere hurtigt dissekerer og diskuterer efterforskernes metodologi og udvikler modstrategier. Med brug af redskaber såsom hacking eller deanonymisering på mørkenettet følger en række juridiske problemer. Det er uden for rapportens omfang og forfatternes juridiske ekspertise at beskrive disse og de problemer, som er associeret hermed, men vi opridser dem alligevel kortfattet her. Problemerne skyldes blandt andet, at den konkrete myndighed ikke ved, *hvem* den deanonymiserer eller hacker. Særligt er deanonymisering af Tor problematisk, da dette kan lede til identifikation af personer, som har helt legale formål. Der er mange både legale og illegale grunde til at benytte Tor, og deanonymisering risikerer derfor at ramme personer, som ikke foretager sig noget ulovligt. Ydermere er Tor-brugernes nationaliteter ukendte, så både hacking og deanonymisering kan ramme personer, som er bosiddende uden for en myndigheds jurisdiktion. Samtidig kan brugen af hacking lede til problemer i forbindelse med retsforfølgelse. I sagen om børnepornografisiden Playpen betød brugen af NIT, *network investigate technique*, som har funktioner forelige med *hacking*, at mindst en sag om download af børnepornografi måtte frafaldes, da FBI ikke ville uddybe, hvorledes den sigtede var blevet identificeret (Ashok, 2016). Endeligt må der tages hensyn til den politiske kontekst, som debatten om brugen af teknikker såsom hacking og deanonymisering befinder sig i (Gehl, 2014; Goldsmith, 2000; Hutchings & Holt, 2017; Tupman, Zabyelina, & Lavorgna, 2015).

2.4.1.5 Langsigtet disruption

Online-markeder for stjålen data har eksisteret længere end kryptomarkeder, og der eksisterer en række akademiske studier heraf (se eksempelvis Dupont, Côté, Savine, & Décary-Hétu, 2016; Holt, Chua, & Smirnova, 2013; Holt et al., 2016; Hutchings & Holt, 2015, 2017; van Hardeveld, Webber, & O'Hara, 2016; Yip, Webber, & Shadbolt, 2013). Særligt er tillidsrelationen mellem de pseudonyme aktører studeret, og der er konsensus om, at tillid er nøgleelementet i et succesfuldt marked. Ligeledes spiller tillid en

afgørende rolle på kryptomarkeder, hvor gode og dårlige anmeldelser af sælgere spiller en afgørende rolle for deres succes (Hardy & Norgaard, 2015). På markeder for stjålen data er metoder til skabelse af et *lemon market* foreslået (Hutchings & Holt, 2017). Målet med disse strategier er at undergrave den tillid, som aktører på markedet har til hinanden, hvilket gør handel mindre attraktivt. Angreb[3] som søger at skabe et 'lemon market' kan være såkaldte *'fake peach'*-angreb, hvor myndigheder foretager køb på markedet og herefter arbejder sig frem mod identifikation af sælgeren eller såkaldte *'sybil attacks'*, hvor myndighederne udgiver sig for at være troværdige sælgere og derefter svindler kunderne (Hutchings & Holt, 2017, p. 9).

2.5 Opsummering

Vi har i dette kapitel introduceret to kernebegreber i forbindelse med policing af kryptomarkeder, *deterrence* og *displacement*. Disse udgør den begrebsmæssige ramme for forståelsen af konsekvenserne af de operationer, som politimyndigheder har foretaget på mørkenettet. Der er bred enighed i litteraturen om, at større operationer med lukning af markeder har haft midlertidig, men ikke længerevarende, indflydelse på kryptomarkedernes økonomi (Décary-Hétu & Giommoni, 2016; Soska & Christin, 2015; Van Buskirk et al., 2017). På kort sigt observeres en deterrent-effekt i form af lavere aktivitet og sælgere, som trækker sig tilbage (Décary-Hétu & Giommoni, 2016), men det er uvist, hvorvidt dette skyldes, at sælgerene blot skifter pseudonymer.

Studierne benytter kvantitative indikatorer, og der er følgeligt aspekter af konsekvenserne ved policing, de ikke afdækker. Bancroft & Reid (2016a) beskriver eksempelvis de prakssiser blandt købere på kryptomarkeder, som har til formål at undgå detektion. Ligeledes observerer Barratt et al. (2016), hvordan brugerne efter lukningen af Silk Road fortsatte med at handle, men at de tog yderligere sikkerhedshensyn såsom at benytte offentligt Wi-Fi. Sådanne adfærdsandringer kan obså observeres kvantitativt, hvor Soska & Christin (2015) eksempelvis viser, hvordan sælgere i højere grad tilbød PGP-kryptering efter Operation Onymous. PGP-kryptering er en simpel adfærdsændring, som kan beskytte mod tredjeparters (eks. politimyndigheders) adgang til adresser og lignende, hvis en server identificeres og konfiskeres. Disse adfærdsændringer kan være en forklaring på, hvorfor markeder er så modstandsdygtige: I takt med interventioner og politioperationer ændrer købere og sælgere adfærd på samme vis, som det er tilfældet i traditionelle stofmarkeder (Cross, 2000; Maher & Dixon, 1999). I de følgende kapitler forfølger vi denne problemstilling. Brugere af kryptomarkeder kan ikke fremsætte en objektiv vurdering

[3]Betegnelsen 'Attacks' anvendes af Hutchings & Holt (2017).

af de risici som følger med deres adfærd, hvorfor det nødvendigvis er deres subjektive vurdering heraf, der bliver udslagsgivende.

Kapitel 3

Metode og data

I dette kapitel udreder vi rapportens forskningsmæssige udgangspunkt og præsenterer de forskningsspørgsmål, vi besvarer. Herefter præsenterer vi rapportens empiriske materiale og diskuterer de etiske overvejelser forbundet hermed.

3.1 Forskningsspørgsmål

I forrige kapitel præsenterede vi en gennemgang af litteraturen omhandlende politiaktioner rettet mod kryptomarkeder. Tidligere studier finder overvejende, at der er kortsigtede effekter på kryptomarkedernes økonomi efter politiindsatser, men at disse effekter aftager inden for en periode på 1-2 måneder. På trods af at der heraf kan drages den konklusion, at politiindsatser ingen langsigtede effekter har, finder vi evidens for at, indsatserne påvirker køberens praksisser på kryptomarkederne. Disse fund er ikke modsætninger, men snarere illustrative for, hvorledes særligt stofkøbere og stofsælgere aktivt navigerer i forhold til de gældende risici. I behandlingen af disse problematikker tager vi udgangspunkt i politioperationen *Operation Hyperion*. Vi stiller følgende forskningsspørgsmål:

1. Hvordan ser myndigheder på Operation Hyperion sammenlignet med andre operationer, og hvad er det forventede udbytte?
2. Hvordan forholder købere og sælgere sig til Operation Hyperion?
3. Hvilke risici identificeres af køberne og sælgerne?

3.2 Datakilder

For at bygge en detaljeret og multifacetteret analyse, indsamlede vi data fra fem forskellige kilder. I det følgende afsnit udreder vi kortfattet motivationen bag anvendelsen af de forskellige datakilder, hvilke data vi har indsamlet, og hvad de forskellige datakilder bidrager med til analysen. Analysen er baseret på følgende kilder:

1. Semi-strukturerede kvalitative interviews med købere på kryptomarkeder.
2. Semi-strukturerede kvalitative interviews med sælgere på kryptomarkeder.
3. Ekspertinterviews med politimyndigheder.
4. Etnografiske observationer på kryptomarkedsrelaterede fora.
5. Observationer af sælgeres aktivitet efter Operation Hyperion.

Kombinationen af empiri fra forskellige kilder giver os mulighed for at triangulere datakilder og dermed øge validiteten af vores fund (Golafshani, 2003, 603). Specifikt benytter vi to typer af triangulering, *datatriangulering* og *investigator -triangulering*. Førstnævnte referer til indsamlingen af data fra forskellige kilder, men fordrer desuden dataindsamling fra forskellige steder og tidspunkter (Mathison, 1988). *Investigator-triangulering* refererer til inklusion af flere forskere i dataindsamlingsprocessen, som sideløbende diskuterer og udfordrer de foreløbige fund. Vi inddrog i processen Silje Bakken, norsk forskningsassistent (Universitet i Oslo, Institutt for kriminologi og rettssosiologi) og sociologistuderende Thea Stoustrup (Københavns Universitet, Sociologisk Institut). Førstnævnte har tidligere arbejdet etnografisk på kryptomarkeders debatfora (Bakken, 2015), og sidstnævnte har i nærværende rapport bidraget til indsamling og diskussion af det empiriske materiale.

3.2.1 Interview

Vi foretog 4 interviews med købere på kryptomarkeder og 2 interviews med sælgere. Vi identificerede køberne gennem "snowballing", hvor vi via enkelte interviewpersoner etablerede kontakt med nye interviewpersoner. To købere var norske, hvilket bidrog med et unikt perspektiv på vores indsamlede data, som vi diskuterer senere. Det viste sig at være særdeles svært at komme i kontakt med sælgere på kryptomarkeder, der typisk ikke besvarede vores henvendelser. Baseret på de få afvisninger vi modtog og vores succesfulde interviews, forstår vi denne samplingvanskelighed som forbundet til de sikkerhedsforbehold, som forskningen viser, at kryptomarkedsbrugerne tager (Bancroft

& Reid, 2016a). Ud af 55 fremsendte anmodninger lykkedes det os at afvikle 3 interviews, og på denne rapports udgivelsestidspunkt har vi påbegyndt et yderligere samarbejde med en australsk forskningsgruppe, som interviewer sælgere på kryptomarkeder.

> *"[...] for obvious reasons we try to keep a low profile and do not engage in interviews."* - Sælger.

Endeligt foretog vi to serier af ekspertinterviews med henholdsvis det danske og hollandske politi. Med begge interviews søgte vi at få indsigt i myndighedernes trusselsbillede og efterforskningskapaciteter. Vi valgte at samarbejde med det hollandske politi, fordi Holland er et særdeles aktivt land på kryptomarkeder (Demant & Munksgaard, 2017), fordi hollandsk politi har haft en række højtprofilerede sager, og endeligt fordi hollandsk politi er den første politimyndighed, som har oprettet en hidden service intenderet som "skræmmekampagne".

3.2.2 Etnografi og observationer af sælgeraktivitet

Den lave succesrate i forbindelse med rekruttering af sælgere ledte os til at påbegynde et intenst feltarbejde på debatfora tilknyttet kryptomarkederne. Observationsstudier eller feltarbejde online kaldes *(n)etnografi* og består grundlæggende af "professionel lurking"på internetfora eller andre digitale medier (Kozinets, 2002; Steinmetz, 2012). I en periode på 2 måneder observerede vi disse debatfora og indsamlede gennem målrettede søgninger empiri omhandlende Operation Hyperion samt brug af kryptomarkeder i Danmark og Norge. Hver identificeret debattråd af relevans for Danmark, Norge eller Operation Hyperion blev kopieret, kategoriseret, noteret og gemt med henblik på analyse. Vi indsamlede i alt 194 debattråde fra 8 forskellige fora med tilhørende kommentarer og debatter mellem brugerne. Vi observerede yderligere specifikke sælgere nævnt i Operation Hyperion med henblik på at undersøge eventuelle ændringer i deres praksis som følge af offentliggørelsen af deres navne og den dertilhørende opmærksomhed.

3.3 Etiske overvejelser

Al data indsamlet fra internetfora er åben for offentligheden og kræver ikke login. Det betyder, at en udfordring ved den anvendte datagenereringsmetode knytter sig til spørgsmålet om informeret samtykke. En fortolkning i denne sammenhæng er, at samtykket implicit er afgivet i kraft af brugernes offentlige informationsdeling (Kozinets, 2002, 65). At skelne mellem offentligt og privat indhold er ikke ligetil, og modsatte holdninger

vil ofte være til stede i de forskellige communities Eysenbach & Till (2001) foreslår, at denne graduering kan estimeres ved at overveje, om **1)** informationen kræver en form for registrering for at tilgå siden (eksempelvis i form af oprettelse af en profil eller tilmelding til e-mailliste), **2)** antallet af medlemmer i det pågældende rum og **3)** den pågældende gruppes normer og koder samt publikummet for den delte information. I forbindelse med **1)** og **2)** er det rimeligt at betragte de studerede fora som værende i højere grad offentlige end private. Adgange kræver ingen registrering, og medlemstallet tælles i tusinder. Punkt 3) er dog mere vagt og svært at applicere på de pågældende fora. Aldridge & Décary-Hétu (2014) argumenterer for, at foraenes politiske ophav, krypto-anarkisme og cipherpunk-idealer (Munksgaard, Demant, & Branwen, 2016) er pejlemærker i forhold til, om informationen bør betragtes som offentlig snarere end privat. Omend dette til dels kan retfærdiggøre behandlingen af information som offentlig, er kryptomarkedernes ideologiske ophav særligt centreret om rettigheder, retten til privatliv og anonymitet (Bancroft & Reid, 2016a; Munksgaard et al., 2016). Vi anerkender, at der er diskrepans mellem rummenes ideologiske etos og informationens status som enten offentlig eller privat.

Kozinets (2002) anbefaler, at der indhentes samtykke ved at bekendtgøre etnografens overvågning af det konkrete medie. Dette er dog besværliggjort i forbindelse med studier af ulovlig adfærd, hvor det formodes, at opmærksomhed på etnografens tilstedeværelse kan afstedkomme ændringer i adfærd (Christin, 2013; Martin & Christin, 2016; Steinmetz, 2012) og dermed underminere validiteten af observationerne. Vi forfølger derfor den samme netnografiske tilgang til kryptomarkeder som Martin (2014a, 2014b) og Bancroft & Reid (2016a, 2016b) og informerer ikke medlemmerne af de pågældende fora om, at vi observerer dem. Dette valg er truffet af hensyn til validiteten af vores fund og desuden, fordi det ikke er muligt at indhente informeret samtykke for samtlige deltagere. Kozinets (2002) påpeger, at fejlfortolkninger og misrepræsentationer af det studerede fænomen kan være brud på etiske fordringer, og vi søger derfor at validere vores fortolkninger af foraenes indhold gennem et forskningsdesign, som vægter triangulering. Da den indsamlede data er offentligt tilgængelig på foraene, hvor brugerne er bevidste om, at politimyndigheder er aktivt til stede, tager vi i udgangspunktet ikke særlige sikkerhedshensyn ved behandlingen af denne type data. I forbindelse med vores kvalitative interviews med sælgere og købere indhentede vi aktivt samtykke ved eksplicit at forklare studiet og databehandlingen. Vores primære bekymring omhandler derfor interviewpersonernes personlige sikkerhed. Truslen mod personlig sikkerhed er absolut højest for sælgere, hvorfor vi tager særlige forholdsregler ved disse interview, som alle blev afholdt gennem krypterede og anonymiserede kanaler. Som et yderligere lag af sikkerhed, benyttede vi styresystemet TAILS til afholdelse og anonymisering af interviewene. Denne fremgang er grundlæggende den samme som benyttedes af Barratt et

al. (2016), Maddox, Barratt, Allen, & Lenton (2016) og Van Hout & Bingham (2014) til kvalitative interviews, om end vi i nærværende undersøgelse har tilføjet endnu et lag af sikkerhed i kraft af anvendelsen af TAILS. Sikkerhedstruslen for købere afhænger af deres engagement i kryptomarkederne, og truslen er primært repræsenteret ved politimyndighederne. Som udgangspunkt blev de kvalitative interviews foretaget personligt og optaget via en bærbar computer i operativsystemet TAILS. I et tilfælde benyttede vi af logistiske årsager en diktafon. Vi foretog transskriptionen og anonymiseringen af interviewmaterialet ved brug af TAILS. I forbindelse med begge interviewtyper anonymiserede vi sensitiv information. Vi definerede sensitiv information som information, der indeholdte a) navne, datoer, profilnavne, og b) praksisrelaterede spørgsmål, som kan anvendes til at identificere interviewpersoner.

3.4 Opsummering

Med dette forskningsdesign og dets anvendelse af heterogen data udreder vi, hvorledes købere og sælgere identificerer risici associeret med brug af kryptomarkeder, og hvordan begge brugertyper navigerer i forhold til disse risici. Analysen er centreret om Operation Hyperion, som behandles som udgangspunkt for en dybere indsigt i fænomenet. Vi triangulerer flere forskellige datakilder med henblik på at øge validiteten af vores fund og for at skabe så holdbare tolkninger som muligt. Vores samlede datagrundlag udgøres af 7 semistrukturerede kvalitative interviews med 3 sælgere og 4 købere, 194 debattråde med tilhørende kommentarer indsamlet fra 8 forskellige, observationer af de 13 sælgere udpeget i Operation Hyperion og 2 serier af ekspertinterview.

Kapitel 4

Analyse

I de følgende afsnit præsenterer vi undersøgelsens resultater. Afsnittet er bygget op således, at vi præsenterer en række temaer, som vi dernæst belyser på baggrund af heterogene datakilder. Vi præsenterer indledningsvis Operation Hyperion og skitserer policing af kryptomarkeder set fra politimyndigheders perspektiv. Herefter demonstrerer vi, hvorledes operationen gav udslag på foraene, hvorefter vi tematisk diskuterer risici identificeret af købere og sælgere.

4.1 Operation Hyperion

Operation Hyperion fandt sted fra den 22. til den 28. oktober 2016 (RCMP, 2016) og var et *'brainchild'* under FELEG, som er et netværk af politimyndigheder fra *Five Eyes Law Enforcement Group*, som inkluderer landene USA, Storbritannien, Canada, New Zealand og Australien (FBI, 2016). Ud over disse lande deltog Holland, Sverige, Irland, Finland, Spanien og Frankrig i Operation Hyperion (Polisen, 2016; RCMP, 2016; Vitáris, 2017). Fra den 31. oktober til den 2. november publicerede politimyndigheder i Canada, Sverige, USA, Holland og New Zealand pressemeddelelser, hvor de annoncerede og beskrev indsatsen (FBI, 2016; Landelijk Parket, 2016; New Zealand Police, 2016; Polisen, 2016; RCMP, 2016). I hver af disse pressemeddelelser præsenteredes den samme pointe i varierende form: at købere og sælgere langt fra er anonyme og sikre, blot fordi de handler på kryptomarkeder:

> *"Trots att polisens arbete försvåras av krypteringen, så går ändå säljare och köpare att spåra, det visar inte minst den här insatsen. De kan till och med vara lättare att spåra än de som handlar på gatan, eftersom det ofta finns bevis i både datorer och i hemmet"* - Polisen (2016).

> *"Illicit DarkNet marketplaces, by their very nature, are difficult to penetrate. But not impossible. The Bureau, with its partners, uses all available investigative techniques to target buyers, sellers, marketplace administrators, and the technical infrastructure of the marketplaces themselves. And we have had success doing it."* - FBI (2016).
>
> *"The clear message for people who think they can use the internet to buy illegal drugs and get away with it is that they can't."* - New Zealand Police (2016).
>
> *"there is a misconception that the Darknet is a place to operate without any risk of police intervention"* - RCMP (2016).

I kombination med den side på mørkenettet, som blev oprettet af det hollandske politi under overskriften ***"Active at Dark Markets? You have our attention"***, synes citaterne fra pressemeddelelserne forskellige aktørers gentagelser af et overordnet budskab. I både vores interview og pressemeddelelserne udsendt i forbindelse med Operation Hyperion observerer vi en afskrækkende frem for intervenerende intention. Denne pointe understøttes desuden af det hollandske politi i et interview foretaget den 2. juni 2017, hvor Operation Hyperion blev beskrevet som en relativt lavprofileret, økonomisk og logistisk let operation sammenlignet med Operations Onymous. Operation Onymous havde konkrete mål bestående i lukning af sider og var logistisk og økonomisk krævende, da servere placeret i en række lande skulle lukkes synkront. Operation Hyperion blev derimod af det hollandske politi snarere beskrevet som en *signalerende* aktion, der skulle formidle en afskrækkende pointe til købere og sælgere. Således viste det sig, at det hollandske politis beslutning om at oprette en hidden service var *improviseret* og havde karakter af en *"gimmick"*. Oprindeligt havde det hollandske politi håbet at intensivere kontrollen med udgående pakker og gøre som FBI og foretage "knock-and-talk-samtaler[1], men af økonomiske og logistiske årsager improviserede de og oprettede siden.

Ideen til Operation Hyperion blev udviklet i FELEG, hvorefter samarbejdslande blev involveret. Siden lukningen af Silk Road og den senere lukning af Operation Onymous havde politimyndighederne fra en række forskellige lande udvekslet databaser fra siderne. Omend siderne opfordrer til det, og selvom der eksisterer sociale og politiske konventioner om brugen af kryptering (Bancroft & Reid, 2016a), er mange privatbeskeder på markederne ukrypterede. Når markedspladsen lukkes og serveren konfiskeres, har politimyndigheder derfor adgang til beskeder, hvor uforsigtige brugere har fremsendt deres adresser. Ifølge vores interviewmateriale indsamlet ved det hollandske politi, er disse adresser i løbet af en længere periode blevet delt mellem landene involveret i Operation Hyperion, og det er i kraft af dette samarbejde, at Operation Hyperion blev iværksat. I

[1] Et personligt besøg foretaget af en politimyndighed. Eksempelvis omhandlende en konfiskeret pakke.

forhold til de interventionsstrategier diskuteret af Kruithof et al. (2016, som er diskuteret og udbygget i afsnit 2.4.1), tilhører dette samarbejde og brugen af data genren *traditionelle efterforskningsstrategier*. Metodologien ligner den, som er benyttet i interventioner mod markeder for stjålen data, hvor en lukning af en side fungerer som udgangspunkt for de efterfølgende sager (Hutchings & Holt, 2017). På kryptomarkeder kan flere typer bevismateriale være tilgængelige i en sådan situation:

1. Ukrypterede beskeder kan ud over adresser indeholde personlige oplysninger og operationelle detaljer såsom detaljer om, hvorfra produktet sendes, eller hvorledes det er pakket ind.

2. En køberprofil på et marked har information tilknyttet, som senere kan benyttes som bevismateriale. Brugerprofilen har en transaktionshistorik knyttet til sig, hvorfra det kan udledes, hvor mange køb personen i kontrol med kontoen har foretaget.

3. Bitcoin sendt til markedet kan udsættes for blockchain-analyse, som det er beskrevet i afsnit 2.4.1.

Både det hollandske og det danske politi gav i interviewene udtryk for, at brugere på kryptomarkeder *ikke* er teknologiske eksperter. Krypterings- og anonymiseringsteknologier bruges rent praktisk til et specifikt formål, men en lille fejltagelse kan efterlade bevismateriale. Sender køberen sin adresse ukrypteret blot én enkelt gang, vil hendes adresse kunne identificeres efter lukningen af et marked. Omend vi ikke kender selektionskriteriet, kan de 150 "knock-and-talk-samtaler, som (FBI, 2016) afholdte under Hyperion, skyldes sådanne uforsigtigheder blandt brugerne. Det påpeges desuden i vores interviewmateriale fra interviewene med det danske og det hollandske politi, at bitcoin er særdeles brugbare i forbindelse med efterforskninger. Selvom brugeren er påpasselig og følger "best practice"ved anvendelse af bitcoin, hvilket inkluderer køb uden om onlinebitcoinvekslerer og brug af bitcoin mixers[2], er der stadig risici, som brugeren må tage højde for (Bancroft & Reid, 2016a). Hvis brugeren blot én gang sender bitcoin til sin konto, som kan spores til en veksler, kan brugerens identitet knyttes til kontoen.

Anvendeligheden af bitcoin som efterforskningsredskab påpeges ligeledes af Kruithof et al. (2016) og er beskrevet detaljeret i det forudgående afsnit 2.4.1. Særligt kritisk er det, at hvis bitcoin købes igennem en veksler, som er *compliant* med love og politimyndigheder, vil denne veksler kunne knytte identiteter til bitcoin-transaktioner.

[2] 'Mixers' eller 'tumblers' er services, som søger at frakoble eventuelle digitale spor mellem eksempelvis en veksler og et kryptomarked.

Både det hollandske og det danske politi gav udtryk for et væsentligt spænd mellem særligt kompetente og mindre kompetente brugere af krypterings- og anonymiseringsteknologier, hvoraf den sidste gruppe udgør majoriteten. I takt med lukninger af markedspladser har politimyndigheder gennem internationalt samarbejde fået adgang til så megen data omhandlende køberne, at det er umuligt at handle på al informationen. Eksempelvis figurerede der på siden oprettet af det hollandske politi en oversigt over censurerede brugernavne og geografiske områder. Oversigten var baseret på data fra lukkede markeder og er præsenteret i afsnit 2.3.

Operation Hyperion lå således i forlængelse af en international deling af data fra lukkede kryptomarkeder, som ledte til fælles erkendelse af, hvor megen inkriminerende information, der var til rådighed for politimyndighederne. Myndighederne blev enige om, at de over en aktionsperiode løbende fra slutningen af oktober til begyndelsen af november 2016 synkront ville handle på denne information. Operationen fik således karakter af afskrækkelse, hvor politimyndighederne i stedet for at foretage anholdelser viste brugerne, hvor megen inkriminerende information, de havde til rådighed.

4.1.1 Operation Hyperion: Et varselsskud

Grundlaget og planlægningen af Operation Hyperion udsprang af et voksende internationalt samarbejde omkring kryptomarkeder, som særligt involverede deling af inkriminerende information fundet på konfiskerede servere. I både pressemeddelelserne og i interviewene med det hollandske politi stod det klart, at intentionen bag operationen var at kommunikere til købere og sælgere, at deres aktiviteter ikke var så sikre, som de potentielt måtte antage, og at politimyndigheder var i besiddelse af mere information, end de kunne handle på. Således kan Operation Hyperion betragtes som et *varselsskud* med det formål at undergrave brugernes sikkerhedsfølelse.

4.2 Hyperion på fora

Som beskrevet i afsnit 3.2.2 foretog vi i løbet af en periode på to måneder observationel etnografi på fora tilknyttet kryptomarkeder, hvilket vi supplerede med en aktiv søgning på forumtråde omhandlende Operation Hyperion. Det mest slående resultat var, hvor *lidt* diskussionen af Operation Hyperion fyldte. En indikator for opmærksomheden på Operation Hyperion er, hvor aktive debattrådene var sammenlignet debattrådene, der

omhandlede Operation Onymous. Et af de mest aktive fora relateret til kryptomarkeder findes på reddit.com[3]. En søgning på ordet "Hyperion"[4] returnerer 7 individuelle debattråde med tilhørende debatindlæg, hvoraf den mest aktive tråd har 18 kommentarer. Til sammenligning returnerer en søgning på ordet "Onymous"49 debattråde, hvoraf den længste har 527 kommentarer. Kryptomarkeders fora fungerer som *virtual offender convergence settings* og kan sammenlignes 'hårde barer'[5] (Soudijn & Zegers, 2012). Her mødes kriminelle, i dette tilfælde administratorer og moderatorer samt købere og sælgere og diskuterer forskellige emner i uformelle omgivelser. Samtalerne vil ofte omhandle praktiske forhold. Denne 'sladder' spiller en afgørende rolle i forbindelse med offline-stofmarkeder, hvor den danner grundlag for adfærd (Dickinson & Wright, 2015). Eksempelvis kan stofsælgere ad denne vej indhente efterretninger om politiets modus operandi. Netop fordi disse fora er centrale for brugerne på kryptomarkederne, er det lave antal aktive tråde, der indeholder diskussioner og efterretninger vedrørende Operation Hyperion slående.

4.3 Et varselsskud høres og diskuteres

Indholdet på de kryptomarkedsrelaterede fora består af en række af forskellige emner, herunder diskussion af stofindtag, anmeldelser af sælgere og diskussioner af operationel sikkerhed. Nyheder af relevans for købere og sælgere deles også, og kryptomarkederne har ligeledes et uofficielt nyhedsorgan i form af bloggen DeepDotWeb.com. Disse fora blev relativt hurtigt informeret om Operation Hyperion efter de førnævnte pressemeddelelser blev publiceret. 1-2 dage efter at FBI (2016) frigav pressemeddelelsen nåede denne forummet r/darknetmarkets. På forummet tilknyttet det svenske marked *Flugsvamp 2.0* blev nyheden delt samme dag, som pressemeddelelsen blev udgivet. Hvorom Operation Hyperion rent kvantitativt ikke fyldte i diskussionerne på daværende tidspunkt, nåede nyheden kryptomarkedernes fora inden for kort tid.

Den komparativt lave aktivitet i trådene på foraene omhandlende Operation Hyperion sammenlignet med trådene omhandlende Operation Onymous kan skyldes, at Operation Onymous resulterede i lukkede markedspladser. Lukningen af markedspladserne i forbindelse med Operation Onymous ledte til *displacement*, hvor brugerne tilgik foraene for at finde ud af, hvad der foregik. Fordi der ikke blev lukket markedspladser i forbindelse med Operation Hyperion og grundet dens lave eksponering på foraene, kunne operationen let overses af de mindre aktive brugere. Dette understøttes af vores interviewmateriale, hvor

[3] reddit.com/r/darknetmarkets
[4] Søgning foretaget den 14/6-2017.
[5] Tough bar.

ingen af de fire købere, som på trods af deres tilstedeværelse på foraene, havde hørt om Operation Hyperion.

Efter en nyhed er blevet delt på disse fora, diskuteres den af brugerne. I vores empiri er denne diskussion er oftest præget af en løs og uformel stemning, hvor hændelsen diskuteres, og hvor tonen i nogle tilfælde tenderer til det paranoide. Her er særligt det svenske kryptomarked *Flugsvamp 2.0* relevant, fordi nyheden om Operation Hyperion nåede forummet på selve dagen, og fordi det svenske politi annoncerede, at de var bekendt med 3.000 købere og 20.000 transaktioner (Polisen, 2016). Komparativt set er dette det højeste tal præsenteret af de lande, som deltog i Operation Hyperion. Fordi pressemeddelelserne indeholdte sparsom information, som kunne diskuteres af køberne og sælgerne, bar trådene præg af spekulation:

> *"Så, vad tror ni? Är detta endast utrikessäljare och brev vi talar om eller bör inrikesköpare vara rädda också?"* - Bruger på Flugsvamp.
>
> *"Slår man ihop svammlet om Erkrans 2000 köpare, Alexandrus 300-400(?) köpare, och säg Nonny med någon hundring så har vi 3000."* - Bruger på Flugsvamp.

Vi ser, at allerede få kommentarer efter pressemeddelelsen og nyhedsartiklerne er delt og spørgsmål er stillet, begynder en bruger at sammensætte en række spor. Han nævner tre tidligere anholdte sælgere, *Alexandrus*, *Erkrans* og *Nonny* og estimerer, at tallene præsenteret i pressemeddelelsen stemmer overens med hans vurdering af, hvor mange adresser disse tre sælgere var i besiddelse af. Denne diskussion af anholdte sælgerkolleger er analog til, hvad Dickinson & Wright (2015) observerer i forbindelse med "sladder"i offline-stofmarkeder, hvor et af de mest diskuterede emner netop er anholdelser. Således præsenterer brugerne selv samme dag, som pressemeddelelsen udgives, en potentiel forklaring på *hvem*, *hvad* og *hvordan*: *De 3.000 personer har købt stoffer hos en af tre anholdte sælgere, og politiet har fået adgang til kunderegistrene.* Tråden fortsætter, og brugere diskuterer særligt, hvor tallet på 3.000 stammer fra. De præsenterer i denne forbindelse en række teorier:

> *"FBI valde att kasta lite loggar till Sverige från Alexandrus istället för papperskorgen om vi nämner SilkRoads nerstängning."* - En bruger foreslår at navnene kunne komme fra Silk Roads database.
>
> *"[...] gjort husis hos säljaren och då denne inte raderat spåren efter sig fått fram kundregister o dyl."* - En bruger forslår at sælgere blev identificeret gennem toldkontrol, og computere ransaget herefter.

Brugeren i det første citat påpeger at navnene vel kunne komme fra lukningen af Silk Road, som på dette tidspunkt blev lukket for tre år siden. Han er ikke alene i den vurdering, som også gentages på engelsksprogede fora:

> *"Where the FBI got their list, who knows? The few posts about people being called by the feds did seem to be about very old purchases, so maybe these are orders from the SR or SR2(more likely) busts."* - Bruger på reddit.com
>
> *"We know for a fact that busts are still being made based on the Silk Road database."* - Bruger på Valhalla.

Omend diskussionen af Operation Hyperion ikke var nær så fyldig (hvis vi ser på aktivitetsniveauerne) på foraene som i forbindelse med Operation Onymous, kan vi se, at køberne og sælgerne på foraene tydeligt modtog den besked, som blev kommunikeret med pressemeddelelsen. Selvom om politimyndighederne ikke angav deres datagrundlag, og hvor eksempelvis informationen om de 3.000 svenske købere stammede fra, præsenterede brugerne i løbet af få dage teorier, som stemmer overnes med de efterforskningsstrategier, som i vores interviewmateriale beskrives af det hollandske politi. Af vores analyse fremgår det altså, at brugerne er bevidste om, at databaserne fra de lukkede markeder deles mellem myndighederne, og at køberregistrene konfiskeres. Med en sådan overensstemmende trusselsvurdering må købere og sælgere vurdere risici i lyset af oplysningerne og handle derpå.

4.3.1 Hyperion og adfærdsændringer

Diskussioner af Operation Hyperion, såvel som af andre operationer, er gennemgående på de kryptomarkedsrelaterede fora. Udvekslingen af teorier og vurderinger danner grundlag for håndteringen af risici, som købere og sælgere kan handle på øjeblikkeligt (Dickinson & Wright, 2015), og vi observerer en række forskellige adfærdsændringer efter Operation Hyperion. En sælger svarer dagen efter pressemeddelelsen i en debattråd:

> *"Jag tror det gäller inrikes också. Vilket gör att vi på LPHS nu kommer flytta hela verksamheten. Vi hade väldiga problem med paket som försvann förra och förrförra veckan just och ber därför kunder som haft uteblivna ordrar från oss att rensa dator, hem osv."* - Sælger på Flugsvamp 2.0.

Sælgeren refererer her til en diskussion i debattråden, som omhandler, hvorvidt der er tale om udenlandske eller indenlandske pakker, som er en information, der ikke fremgår

af pressemeddelelsen. Han vurderer, at de pakker, som i de foregående uger er forsvundet, muligvis kan skyldes Operation Hyperion og beskriver, hvordan hele hans forretning vil flytte lokation og advarer køberne til at *'gøre rent'*[6] og rense deres computere. Førstnævnte er et typisk råd, som gives, hvis en transaktion vurderes risikabel. En sådan rengøring involverer fjernelse af stoffer fra den pågældendes bopæl samt fjernelse af eventuelle digitale spor.

Sikkerhedsoptimerende adfærdsændringer er ikke forbeholdt sælgere. Vi observerer, at nogle brugere beskriver, at de efter Operation Hyperion har ændret adfærd. I nedenstående citat forklarer en bruger, at han i kølvandet på Operation Hyperion ikke længere vil bestille fra Canada, hvorfor han spørger sine fæller om forslag til gode sælgere. Han efterspørger således aktivt råd om, hvordan han bør tilpasse sin adfærd under en ny trusselsvurdering.

> *"After hearing about ts420 quitting and hyperion I think canada is off the table for now [...] Does anyone have any recent experience with intl orders? preferebly within europe, but if you've had recent success with canada I'd like to hear about it."* - Køber på reddit.
>
> *"I'm just going to consider it a bonus if it arrives I'm done with dnm I think for now."* - Køber på reddit

De to ovenstående citater skal ses i en kontekst, hvor vi observerer en diskussion om ruten mellem Canada og Storbritannien. Denne diskussion er særligt prævalent i et forum, som specifikt omhandler brug af kryptomarkeder i Storbritannien. På forummet melder flere brugere i løbet af oktober måned om forsinkede eller manglende pakker. I det andet citat vurderer en bruger, at det er på tide at tage en pause.

En anden risikominimerende adfærdsændring kan være ændring i brugen af teknologi. Som tidligere beskrevet, vurderer politimyndighederne, at både køberne og sælgerne ofte ikke benytter de redskaber, som sikrer dem den højeste sikkerhed. En svensk køber rådgiver andre købere til at anvende kryptering:

> *"Mitt råd? kryptera, kryptera och åter kryptera, var tyst om allt du gör på forumet, göm sakerna väl, kolla en extra gång i backspelgeln, sväng några gånger extra och kolla om du har någon bakom dig, men viktigast är att att KRYPTERA!!!"* - Køber på Flugsvamp.

[6] På de engelsksprogede fora: 'clean house'.

Dette råd synes på overfladen fornuftigt, men det afhjælper ikke sikkerhedstruslen, hvis sælger opbevarer et kunderegister. Derfor opfordrer en anden bruger kraftigt til, at sælgerne sletter købernes adresser:

> *"SÄLJARE MÅSTE TA MER ANSVAR OCH RADERA ADRESSER DIREKT. ADRESSER SKALL INTE SPARAS PÅ DATORN ÖVHT."* - Køber på Flugsvamp.

Rådet om at slette købernes adresser er et af de mest grundlæggende råd på kryptomarkederne. Der kan dog være rent praktiske grunde til, at sælgerne beholder købernes adresser. I vores interviewmateriale påpegede det hollandske politi, at en sælger potentielt kan anvende sit kunderegister til samarbejde med politiet. Desuden ved vi, at nogle sælgere opbevarer adresser på dårlige kunder.

4.3.1.1 Hyperion og økonomiske tab

Hvis en vare købt på et kryptomarked stoppes i tolden, vil enten køber eller sælgere opleve et økonomisk tab. Tabet deles, og nogle sælgere tilbyder at sende 50% af den købte vare eller delvis refusion af prisen. Således deles det økonomiske tab mellem køber og sælger. Nogle sælgere lider økonomiske tab i de tilfælde, hvor produktet skal refunderes i enten produktform eller økonomisk form og særligt ved gentagne tilfælde. Når en sælger vurderer sin risiko øget, som det eksempelvis kan være tilfældet i forbindelse med Operation Hyperion, kan det motivere eller presse sælgeren til at svindle sine kunder. Eksempelvis kan en sælger under en længere operation, hvor flere pakker konfiskeres, lide svær økonomisk skade og miste produkter og samtidig være nødsaget til at kompensere sine kunder. Dette kan på længere sigt få konsekvenser for sælgerens ry og dermed for dennes økonomiske fremtid. En sælger fortæller i en debattråd, hvordan først Operation Pangea, som var en ikke-kryptomarkedsrelateret operation, ramte ham økonomisk. Senere ramte Operation Hyperion ham økonomisk:

> *"Unfortunately, "TS420"is bankrupted. [...] 2016 has been extremely rough, customs got better and margins fell. There was the HUGE pangea operation bust and then my employee who decided to go rogue and steal everything."* - Sælger på Alphabay.

I den pågældende tråd har sælgeren løbende interageret med sine kunder, og ovenstående citat er taget fra et indlæg, hvor han erklærer, at han stopper med at sælge. Ræsonnementet er klart: Intensiv toldkontrol har afstedkommet økonomiske tab, og problemer

med en ansat har forværret situationen. Som tidligere beskrevet finder vi særlig opmærksomhed på ruten mellem Canada og Storbritannien. Det er købernes og sælgernes indtryk, at denne rute blev heftigt overvåget og kontrolleret i måneden op til Operatioon Hyperion. En bruger konstaterer konsekvenserne:

> *"I believe the same happened to GREENDPOT. Unfortunately one hard months of customs operations is enough to bankrupt 2 established weed vendors."* - Bruger på Alphabay.

Sælgere på kryptomarkeder er særligt sårbare for sådanne konfiskationer på grund af de særlige kvaliteter ved kryptomarkederne. Denne sårbarhed er opmærksomhedsværdig. Hvis en canadisk sælger eksempelvis sælger et ounce cannabis (svarende til 28 gram), som er en typisk mængde til videresalg, som konfiskeres, er produktet tabt. Betalingen for produktet opbevares typisk af markedspladsen som mediator, og hvis produktet ikke når frem, kan køberen klage til markedspladsens moderator. Typisk har sælgerne en refusionspolitik, og de kan derfor være tvunget til at sende produktet igen eller refundere beløbet. Hvis tabet er systematisk over en kort periode, eksempelvis 20 pakker over en to uger lang aktionsperiode, rammes sælgerens forretning hårdt. Konsekvenserne er dog ofte mere omsiggribende, fordi sælgernes ry er afgørende ressourcer på kryptomarkederne (Duxbury & Haynie, 2017; Hardy & Norgaard, 2015; Nurmi, Kaskela, Perälä, & Oksanen, 2017). Under en markedsstruktur som denne kan også de konfiskeringer af produkter, som ikke resulterer i anholdelser, have store konsekvenser.

4.3.1.2 Afhopninger og svindel - En utilsigtet konsekvens af Hyperion

Af de 13 sælgere, som blev nævnt på det hollandske politis hidden service, opererede 10 sælgere stadig i juni 2017. Af de tre, som ikke opererede, identificerede vi to, som havde svindlet kunder ved et såkaldt *'exit scam'*. Dette fund blev diskuteret med det hollandske politi, som ikke havde forudset, at sådanne *'exit scams'* kunne forekomme. På Alphabays forum blev en klage over sælgeren *DrugsFromAmsterdam* indberettet. Kunden havde betalt 20 gram MDMA forud, men sælgerens profil blev senere lukket. En anden bruger svarer således:

> *"Operation Hyperion. Dutch Law enforcement site has him listed as a known vendor but not busted yet (I hope). I am more worried about my information than my money. Google 'operation hyperion'. I wish him well and don't blame him for going off grid."* - Køber på Alphabay.

Denne bruger drager således en direkte forbindelse mellem publiceringen af sælgerens navn på det hollandske politis hidden service og den pågældende sælgers 'exit scam'. Vi finder overraskende, at brugeren ønsker svindleren det bedste, og at han foretrækker et umiddelbart økonomisk tab frem for anholdelse af den pågældende sælger, som muligvis er i besiddelse af køberinformation. I en anden tråd skriver en køber, at den sælger, som har solgt ham et produkt, har fået et 'ban' fra markedspladsen. Vi kender ikke grundlaget herfor, men vi ved, at sælgere typisk udelukkes typisk grundet regelbrud eller svindel (Martin, 2014a, 2014b). En anden køber svarer dog:

> *"Yeah mate, he got banned and I got fully refunded. Been talking to him on Dream and he did actually send out the packs."* - Bruger på reddit.

Om sælgeren taler sandt eller ej, når han fortæller køberen, at han faktisk har sendt sine produkter, kan vi ikke vurdere. Muligvis er hans profil lukket på et marked grundet svindel, mens han stadig opererer på et andet marked, *Dream*, hvor brugerne muligvis endnu ikke er opmærksomme på hans svindel. En alternativ forklaring er, at mange af sælgerens pakker er stoppet i tolden, hvilket har ledt til kundeklager om svindel og det efterfølgende ban. Det er muligt, at Operation Hyperion har spillet en rolle i denne forbindelse og inddrages af brugerne gentagende gange som forklaringsfaktor. Afhopning og svindel i kølvandet på Operation Hyperion må forstås i lyset af både operationens intention såvel som de ovenfor beskrevne umiddelbare økonomiske konsekvenser. En intensiveret kontrolindsats af forsendelser kan ramme sælgerne økonomisk, og de kan blive presset til at svindle for ikke at lide store økonomisk tab. Samtidig kan publiceringen af deres navne have en afskrækkende effekt, og som en bruger foreslår, kan det i den forbindelse være en fornuftig beslutning at hoppe af.

4.3.2 Delkonklusion: Konsekvenserne af Hyperion

Omend Operation Hyperion logistisk og økonomisk var væsentligt mindre end den tidligere Operation Onymous, ser vi en række konsekvenser, og desuden er operationen anvendelig som case til at forstå, hvorledes øget risiko håndteres på kryptomarkederne. Først og fremmest følges sådanne operationer af intensiv vidensdeling og udredning af *hvad*, *hvem* og *hvordan*. Et overraskende fund er, at selvom politimyndighederne i pressemeddelserne ikke beskrev bevismaterialet, præsenterede brugerne i løbet af få dage beskrivelser i overensstemmelse med politimyndighedernes faktiske praksis.

Operation Hyperion bemærkes først af købere og sælgere, som retrospektivt forklarer den forudgående måneds forretningsproblemer. Særligt på ruten fra Canada til Storbritannien var mange pakker stoppet, hvilket særligt havde ramt sælgerne økonomisk.

Gennem vores feltarbejde blev vi opmærksomme på tre sælgere, som havde 'exit scammet' efter Operation Hyperion, hvoraf to var navngivet af det hollandske politi. En anden sælger trak sig tilbage i kølvandet på operationen. Både en intensiveret kontrol og den afskrækkende effekt af publikationen af sælgernes navne lader altså til at have haft reelle konsekvenser. 'Exit scams' er den mest ekstreme form for adfærdsændring, og ud af de 13 sælgere, som blev udpeget af det hollandske politi, havde 2 sælgere begået et 'exit scam'. Vi observerer desuden en række forskellige måder, hvorpå købnre og sælgerne ændrede adfærd. En svensk sælger omorganiserede sin forretning, købere på Canada-Storbritannien-ruten søgte nye sælgere og på foraene opfordrede brugerne hinanden til at kryptere al information og sælgerne til at slette adresser.

4.4 Risiko og handel

Foraenes reaktion på Operation Hyperion fungerer som udgangspunkt for en nærmere undersøgelse af, hvordan købere og sælgere på kryptomarkeder optager og handler på information omhandlende risici. Som tidligere beskrevet fungerer kryptomarkedernes fora som *virtual offencer convergence settings*, analoger til "hårde barer", hvor den udvekslede "sladder"er afgørende for, at brugerne kan udvikle og udveksle strategier til risikominimering (Dickinson & Wright, 2015; Soudijn & Zegers, 2012). Vi behandler her tre generelle temaer. Først behandler vi debatforaenes rolle for brugernes beslutningstagning og fokuserer herunder på foraene som adgangsgivende til lokal viden. Dernæst behandler vi brugen af teknologi som en specifik praksis og undersøger nærmere, hvorledes købere og sælgere anvender teknologien på sikre og usikre måder. Endeligt diskuterer vi en række strategier, som implementeres af købere og sælgere for at mitigere risiko.

4.4.1 Fora som en ressource

De kryptomarkedsrelaterede fora udgør et informationsgrundlag for købernes og sælgernes adfærd. Her ophobes information, hvorfor foraene kan betragtes som en form for 'kollektiv hukommelse'. Her er det muligt for brugerne at finde information, som daterer sig helt tilbage til Silk Road eller Operation Onymous. I vores interviews søgte vi at skabe forbindelse mellem købernes og sælgeres adfærd og deres brug af foraene. Fælles for alle køberne var, at de oftest anvendte foraene til at søge informationer relevante for deres køb frem for at deltage aktivt i debattrådene. De interviewede sælgere var alle etablererede, da de blev interviewet, og de anvendte derfor foraene til at holde sig opdaterede og håndtere kunderelationer. Alle sælgerne havde dog i begyndelsen af deres karriere anvendt foraene og de tilgængelige guides til at optimere deres forretning og til

at kvalificere deres anvendelse af markederne. Der er således tale om to typer af brug af de kryptomarkedsrelaterede fora.

4.4.1.1 Generel viden

Samtlige sælgere og købere i vores interviews havde anvendt foraene i begyndelsen af deres karriere. Handel på kryptomarkeder kræver et grundlæggende kendskab til teknologi og herunder navnligt til Tor, PGP og bitcoin, hvorfor foraene spiller en afgørende rolle i at "uddanne"brugerne. Vi finder, at der går overraskende lang tid fra brugerne første gang besøger et marked, til de beslutter sig for at købe. En køber beskriver i nedenstående, hvor lang tid der gik fra han havde 'window-shoppet', til han begik sit første køb:

> *"I hvert fald et par måneder. Måske, ja, tre-fire måneder tror jeg. Der kiggede jeg på det."* - Dansk køber.

I perioden mellem det første besøg på et kryptomarked og det første køb eller salg kan brugere lære om kryptering, anskaffelse af bitcoin samt researche, hvilke sælgere eller produkter, de er interesserede i. Efter denne introduktion kan brugerne yderligere anvende foraene til at holde sig opdaterede og informerede. En køber solgte LSD videre i mindre skala og forklarede vigtigheden af at læse de detaljerede brugeranmeldelser, som er tilgængelige på foraene:

> *"Der har været flere gange, hvor at man ligesom ser en sindssygt billig pris på noget, og man er lige ved at købe det, og så tjekker man lige op på det først og finder ud af, at de 150ug i virkeligheden lå på nogle af de 80 [...]"* - Dansk køber.

De kryptomarkedsrelaterede fora leverer således en praktisk introduktion til markederne og særligt til de teknologier, som anvendes. Når købere benytter markederne, anvender de dem ligeledes til at holde sig informeret om, hvilke sælgere der sælger et godt produkt. Det er dog ikke alle købere på markederne, der er så velinformerede. En sælger fortæller:

> *"Not at much as they should. The majority of buyers purchasing for personal are blind. They will click around and click buy with little to no research."* - Europæisk sælger på 'medium-to-large-scale' niveau.

Denne skelnen mellem de velinformerede brugere og de, som med det samme kaster sig ud i køb, er vigtigt. Som det blev påpeget af det hollandske politi, er det særligt "nybegynderne", som ikke har researchet tilstrækkeligt, der ikke anvender kryptering, og som derfor er udsat ved lukning af sider og konfiskering af servere.

Særligt i forhold til hvad både det hollandske og det danske politi påpegede, kan uinformerede 'nybegyndere', som ikke har gjort deres research ordentligt, være blandt dem, som ikke bruger kryptering og derfor udsætter sig selv for øget risiko ved lukninger af sider. Særligt i forhold til hvad både det hollandske og det danske politi påpegede, kan uinformerede 'nybegyndere', som ikke har gjort deres research ordentligt, være blandt dem, som ikke bruger kryptering og derfor udsætter sig selv for øget risiko ved lukninger af sider. Her kan drages en parallel til offline-stofmarkeder, hvor uerfarne bruger oftere udnyttes eller snydes af stofsælgere (Jacques, Allen, & Wright, 2014). Der er ingen tal til rådighed omhandlende, hvor mange brugere, der benytter foraene. Brugerne på foraene vil blive bekendt med en 'best practice' for brug af kryptomarkeder, som inkluderer kryptering af beskeder og lignende. Når politimyndigheder påpeger, at mange brugere ikke krypterer beskeder eller benytter teknologien korrekt, kan dette derfor indikere, at mange brugere enten ikke er bekendt med 'best practice', som den præsenteres på fora, eller simpelthen ikke gider følge den.

4.4.1.2 Lokal viden

Købernes risiko består oftest i identifikation af pakken i tolden og den efterfølgende kontakt med politiet. Når den umiddelbar nært forestående risiko vurderes, vurderes den altså i en lokal kontekst: hvorvidt en pakke risikerer at blive identificeret i posten. På dette punkt er en sammenligning mellem Norge og Danmark særligt interessant, fordi vi her ser, at foraene spiller en afgørende rolle for vurderingen af risici associeret med køb på kryptomarkederne. En bruger forklarer, hvordan research på foraene blev brugt til at vælge afsenderlandet for hans køb:

> *"Jeg tror, jeg brugte en uge på at scrolle igennem alle mulighederne, jeg havde [...] så jeg regnede hurtigt ud, at alt hvad du får - modtager fra Holland - det bliver mere eller mindre opsnappet, så du er en idiot hvis du køber derfra, ikk'?"* - Dansk køber.

Denne køber valgte efter megen research at købe fra et land, han vurderede som ufarligt, og han traf denne beslutning ved at læse andres erfaringer på foraene. For denne køber og for andre danskere er det dog en udfordring, at der er relativt begrænset tilgængelig information. Præcist hvor kritiske fora er, fortæller en anden dansk køber:

> *"Altså, hvis de ikke var der, havde jeg ikke købt, fordi så havde jeg ikke haft nogen at kunne se - men man skal ligesom også se andre gøre det - og det putter mig i en risiko, så det er en måde at finde selvtillid i det, ikk'?"* - Dansk køber.

Udover at være en ressource, som kan hjælpe med at navigere risiko og minimere den, giver foraene således en "selvtillid"omkring købet i form af viden om, at produktet rent faktisk vil blive sendt og modtaget. I vores feltarbejde fik vi kenskab til to norske fora. I det ene forum var der mere end 1.000 debattråde, som alle omhandlende kryptomarkeder fra et norsk perspektiv, som sammenlignet Danmark vidner om, at den danske information er yderst begrænset. I Danmark er informationen spredt ud over et stofforum (Psykedelia.dk) og internationale kryptomarkedsfora. Den risiko, som en dansk køber udsætter sig selv for, er lokal og består af dansk told og dansk politi, og derfor er internationale erfaringer ikke væsentlige i denne sammenhæng. Fraværet af danske fora, hvor risiko og erfaringer kan deles samt den dertilhørende ophobning af information om risiko, betyder, at danske købere træffer sine beslutninger på væsentligt mindre informerede grundlag sammenlignet med norske købere. Denne forskel er tydelig i nedenstående citat fra en moderator på det norske forum, som fremsætter det tætteste, vi kommer på en "officiel position"omhandlende sikre køb:

> *"VI ANBEFALER PÅ DET STERKESTE Å HANDLE INNENLANDS! Vi får mange spørsmål om dette, og konsensusen er at det er en stor risiko, og de fleste pakkene blir tatt i tollen. Hvis du ikke er kjent på darknet bør du ikke begynne med å handle utenlands!"* - Moderator, norsk forum for kryptomarkeder.

Kryptomarkeder er grundlæggende internationale markeder, og det er en væsentlig begrænsning for køberen med hensyn til udvalg og pris at skulle handle indenlands. På trods heraf fremstiller moderatorerne på foraene det officielle råd, at man er mere sikker, hvis man bestiller indenlands. Der er her to vigtige punkter. For det første har de norske brugere et forum, hvor de kan få "officielle"råd, og dernæst vil disse råd angiveligt minimere risiko. De tidligere citerede danske købere som fandt "selvtillid"i at browse fora, som valgte lavrisiko lande på baggrund af fora, har ikke adgang til lignende information. De interviewede købere valgte enten ikke at bestille fra udlandet eller undgik specifikt visse lande, særligt Holland. På foraene har Holland et ry for at være et 'hot country', som er et land, hvorfra post får særlig opmærksomhed. Omend bestillinger fra Holland frarådes på foraene, og selvom de interviewede fravalgte landet ad denne grund, er Holland stadig et af de største eksportlande (Demant & Munksgaard, 2017). Således

er der uoverensstemmelse mellem de råd som gives på foraene, og hvordan brugere reelt opfører sig. Dette giver endnu en indikation på, at der er en stor andel af brugere, som enten ikke læser på foraene eller følger den information, som er tilgængelig.

4.4.2 Krypteringspraksis

Som tidligere beskrevet gjorde både det hollandske og det danske politi opmærksom på, at der var stor forskel på den tekniske formåen blandt både købere og sælgere. Selvom aktivitet på kryptomarkeder involverer brug af en række komplekse teknologier for at sikre anonymitet og sikker kommunikation, er dette ikke ensbetydende med, at disse benyttes korrekt. Vi foreslår at diskutere *krypteringspraksis*, og at der fokuseres på selve brugen af krypterings- og anonymiseringsteknologier frem for alene at fokusere på teknologierne. Købere og sælgere på kryptomarkeder anvender generelt teknologi med det formål at handle stoffer, hvilket kræver særlig viden om teknologien og navnlig viden om, hvordan den anvendes på sikker og praktisk vis. I et interview indså en køber eksempelvis, hvorledes hans sikkerhedspraksis havde fejlet. Han fortæller i nedenstående citat om sine erfaringer med opbevaring af bitcoin:

> *"Jeg havde ligesom haft en USB med en helt masse forskellige nøgler, eller en hel masse forskellige wallets i forvejen, så lagde jeg det hele sammen på min telefon, hvilket jeg lige nu har indset er fucking dumt."* - Dansk køber.

Køberen fortæller i dette tilfælde om "hvide"og "beskidte"bitcoin. Han havde ikke et indgående kendskab til blockchain analyse (en efterforskningsstrategi diskuteret i afsnit 2.4.1.3), men han var akut opmærksom på, at der eksisterede en korrekt og en forkert måde at bruge bitcoin på. Det er vigtigt at understrege, at køberen så visse tekniske risici som værd at løbe, fordi alternativet var tidskrævende eller besværligt. Adspurgt om købsprocessen gjorde han grin med sig selv og sin usikre praksis:

> *"[...] så tager jeg hjem, og så bare bestiller det. I Wifi'et derhjemme, på min Windows computer. Fordi jeg er dum [Griner]. Og jeg ved hver eneste gang jeg skal købe, at jeg burde installere TAILS på min computer, men jeg får det bare aldrig rigtigt gjort."* - Dansk køber.

TAILS er et styresystem som kan opbevares på en USB-stick, og som indeholder diverse softwares af relevans for brug af kryptomarkeder (bl.a. password manager, PGP, Tor samt bitcoin wallets). Brugeren forklarer senere sin usikre praksis som passende for den risiko, han løber ved bestilling af LSD til videresalg på mindre skala, men vi understreger,

at både hans brug af bitcoin og hans aktivitet på kryptomarkederne efterlader en række spor. Det kræver følgeligt sit at praktisere, hvad der på fora kaldes OPSEC, *'operational security'*. Den danske køber har naturligvis ikke selv fået ideen om, at bitcoin kan knyttes til hans identitet eller lært, at han burde bruge TAILS. Dette har han lært på foraene. Adspurgt om hans opstart som sælger, gennemgår en interviewperson, hvordan han brugte måneder på at lære teknologien at kende:

> *"[...] I was just browsing and starting to grasp proper OPSEC and working my head around PGP encryption and buying bitcoin [...] Everything would be completely self-taught, I spent a lot of time on forums reading guides etc. It was no time before I was running better OPSEC than most vendors at the time [...] I would be using WHONIX or TAILS, hard drives would be encrypted [...]"* - Europæisk sælger på 'medium-to-large-scale'-niveau.

Både sælgere og købere indhenter information på foraene omhandlende hvilken teknologi, de bør bruge, og hvordan den bør anvendes. Det er ikke ensbetydende med, at de følger 'best-practice', fordi der nødvendigvis eksisterer et trade-off mellem convenience og sikkerhed. En sælger ønskede at bruge et andet medium for kommunikation end det, vi havde foreslået. Sælgeren forklarer ræsonnementet således:

> *"There's a balance you have to find between safety + security and becoming so cautious and paranoid that it obstructs you in your daily life."* - Europæisk 'mid-level' sælger.

Ligeledes tog de interviewede købere "genveje"med hensyn til sikkerhed såsom opbevaring af sensitiv data på ukrypterede USB-stick, køb med sporbare bitcoin og manglende anvendelse af TAILS. Brugen af krypterings- og anonymiseringsteknologier bør således forstås mere som en praksis end som en kvalitet ved adfærd eller kommunikation. Både købere og sælgere er akut opmærksomme på, at de ikke er sikret per automatik blot fordi de benytter Tor eller bitcoin. Udfordringen består i, *hvordan* teknologien anvendes, og her reflekterer og vurderer købere og sælgere over deres adfærd baseret på faktorer såsom praktikaliteter og behov.

4.4.3 Risiko fra told og politi

Som beskrevet i afsnit 4.4.1.2 er købere på kryptomarkeder særligt opmærksomme på den risiko, de udsætter sig for i forbindelse med brugen af postsystemet og herunder hvilke lande, der er mere eller mindre sikre at bestille fra. I interviewene med køberne

udgjorde dette afgjort den største bekymring, hvor bekymringer om politimyndigheders konfiskering af eksempelvis adresser fyldte forsvindende lidt. Dette er overraskende, fordi vi ved, at køberne er bekendt med blockchain-analyse, og fordi, som både det hollandske og det danske politi gjorde opmærksom på, at mindre fejltagelser i denne sammenhæng har lange holdbarheder. Den umiddelbare frygt, vi identificerer blandt køberne, består altså i produktets identifikation i toldkontrollen, og at køber efterfølgende vil blive kontaktet af politiet. En køber vurderer sikkerheden ved køb på kryptomarkeder således:

> *"[...] de skal jo basically åbne din post for at finde ud af det. [...] Men det kommer også an på, hvor god leverandøen er - altså hvis det er dårlig stealth, hvis det ikke er pakket godt ind [...] så er du måske lidt fucked."* - Dansk køber.

Denne danske køber er altså bekendt med risikoen forbundet med pakker, som krydser grænser, men han påpeger, at særligt inkompetente brugere øger risikoen. Dog vurderede begge vores danskere købere deres køb som relativt sikre, hvilket primært skyldes, at de havde forberedt sig på en eventuel identifikation af pakken. I nedenstående citat fremgår det, at risikoen relativt let kan mitigeres:

> *"Jeg gjorde mig den overvejelse: 'hvad nu hvis du bliver taget?', og så tænkte jeg:'men jeg har betalt anonymt, og jeg kan bare sige, at der her, det er ikke mig', altså; 'der er nogen, der har sendt det her til mig ved en fejl.* - Dansk køber.
>
> *"[...] og så siger man: 'jeg har ikke bestilt noget' [...], og så frafalder sagen i form af manglende bevismateriale [...]"* - Dansk køber.

Igen finder vi, at håndteringen af risikoen refererer til, hvad der diskuteres i foraene. På et forum spørger en bruger eksempelvis, hvordan han skal håndtere en mindre mængde piller identificeret i posten, som politi har kontaktet ham om:

> *"Det betyder, at de ikke ved noget om, hvordan du har bestilt pillerne. De ved intet om sælgeren og intet om hjemmesiden på Darknet. De kan ikke bevise, at du har bestilt pillerne. Efter al sandsynlighed bliver tiltalen frafaldet. Hvis du bliver dømt alene ud fra brevet, så er du den første, jeg har hørt om. [...] Det kommer til at betyde, at vi alle sammen må holde op med at købe stoffer over internettet."* - Bruger på dansk forum.

Vi observerer således, hvordan brugernes vurdering af risiko for straf i forbindelse med bestilling af et produkt trækker på kollektive erfaringer. Dette er særligt interessant, fordi ingen af de interviewede købere havde haft kontakt med politiet eller toldkontrollen i forbindelse med deres bestillinger. Vurderingen af kryptomarkedskøb som risikofri, så længe man var bekendt med, hvordan et identificeret køb skulle håndteres, var altså ikke baseret på egne erfaringer. Når købernes adfærd således ikke afhænger af deres egne erfaringer med køb, men er kvalificeret af informationen tilgængelig på foraene, bliver diskrepansen mellem information tilgængelig for henholdsvis norske og danske brugere af særlig relevans. Som beskrevet i afsnit 4.4.1.2, observerede vi store forskelle i informationsgrundlaget tilgængeligt for norske og danske købere. Selvom vi heraf ikke kan aflede et kausalt forhold, er det værd at overveje, hvorvidt den overvældende mængde information tilgængelig for norske brugere har en afskrækkende effekt, som ansporer til indenlandskøb, som vurderes som mindre risikable.

Kapitel 5

Diskussion

Der er inden for den kryptomarkedsrelaterede litteratur bred enighed om, at lukninger af markederne har midlertidige effekter i form af lavere aktivitet (Décary-Hétu & Giommoni, 2016; Ladegaard, 2017; Soska & Christin, 2015; Van Buskirk et al., 2017). Kriminologisk litteratur foreslår, at sådanne aktioner har en afskrækkende eller forflyttende effekter, men foreslår ligeledes, at praksisser og adfærd vil tilpasse sig risikobilledet(Dickinson & Wright, 2015; Finn & Stalans, 2016; Maher & Dixon, 1999). Vi finder, at selvom Operation Hyperion logistisk og økonomisk var væsentligt mindre end tidligere operationer, særligt Operation Onymous, havde den stadig konsekvenser for købere og sælgeres adfærd på markederne.

Særligt overraskende var, at to sælgere efter at være blevet nævnt af hollandsk politi forsvandt fra markederne. Vores datamateriale antyder, at der eksisterer et potentielt kausalt forhold mellem Operation Hyperion og de efterfølgende afhopninger. Andetsteds i vores empiri finder vi, at sælgere og købere indirekte rammes af en sådan aktion, når de lider økonomiske tab. Dette kan opmuntre til afhopning, men vi finder desuden en sælger, som offentligt fortæller, at han har ændret adfærd. Dette er et ubelyst aspekt af sådanne operationer, som det hollandske politi ikke gør opmærksom på i vores interviewmateriale: Kortvarige operationer, som ikke involverer anholdelser, kan stadig gøre stor skade på sælgernes forretninger. Sælgerene vil typisk refundere forsvundne eller konfiskerede pakker, hvormed de lider økonomisk tab. Det er således ikke svært at forestille sig, at en midlertidig operation, som går disproportionelt ud over nogle sælgere, kan gøre disse sælgers forretninger urentable og lede til afhopninger.

Blandt både sælgere og købere fandt vi, at foraene spillede en vigtig rolle for brugen af kryptomarkederne. En informant forklarer, at de gav ham *'selvtillid'* i, at et køb kunne foretages sikkert, mens sælgere beskrev, hvordan de i begyndelsen af deres karrierer havde brugt måneder på research. Foraene benyttes altså til række forskellige formål,

og vi vurderer, at den parallel, som Soudijn & Zegers (2012) drager mellem sådanne fora og 'hårde barer' samt 'hangouts' for kriminelle, også er passende i denne sammenhæng. Der er dog nogle særlige karakteristika ved kryptomarkedernes fora, hvilket eksempelvis består i den konstante ophobning af information. Hvor guides og introduktioner til teknologier kan bruges og læses af alle, har køberne brug for lokalt forankret information. I deres indledende research udsøger køberne særligt information omhandlende risici associeret med postforsendelser, hvor særligt afsenderlandet var af interesse. I denne kontekst er det nødvendigt med lokalt forankret information såsom information om, fra hvilke lande posten profileres i Danmark. I forbindelse med vores netnografiske arbejde fandt vi en stor mængde information tilgængelig for norske købere, men meget lidt information tilgængelig for danske købere. Navnligt havde førstnævnte gruppe dedikerede fora og lukkede kanaler, hvor information til danske købere var spredt. *Hvorfor* det norske community er så aktivt er uvist. Det kan skyldes en mere intens toldkontrol, fordi Norge ikke er et EU-land, men det kan også skyldes en stærkere tilstedeværelse af nordmænd på kryptomarkedernes fora (Bakken, 2015). Disse implikationer bør overvejes, og hvis et dansk forum for kryptomarkeder oprettes i fremtiden, bør dets rolle for beslutningstagning og risikominimerende adfærd blandt brugerne studeres.

Vores fund viser, hvor afgørende foraene er for kryptomarkedernes sælgere og købere. Fordi både køberne og sælgerne oftest ikke har erfaringer med de risici, som er associeret med køb og salg på kryptomarkeder, er de nødt til at læne sig op ad andre brugeres erfaringer og meninger. Objektiviteten af dette erfaringsgrundlag er ikke garanteret, men det er den eneste tilgængelige information for brugerne. Den risiko, som købere og sælgere oplever, *skabes* således aktivt på foraene. Troværdigheden af denne information er til diskussion, og vi noterer, at misinformation kan spredes med efterfølgende virkninger for købernes og sælgernes adfærd. En sådan spredning af misinformation kan udføres af politimyndighederne såvel som af andre forumbrugere og kan placeres i genren af langsigtede disruptioner foreslået af Hutchings & Holt (2017). Konkret kunne det norske råd om kun at handle indenlands i udgangspunktet være propageret af de sælgere, som selv deltager aktivt i foraene (Bakken, 2015).

Kryptomarkederne er svære at afskære fra den bredere samfundsmæssig diskussion om, hvorvidt politimyndigheder er ved at *gå sort* som en konsekvens af udbredelsen af krypterings- og anonymiseringsteknologier (Comey, 2014; Schulze, 2017). På overfladen synes brugen af sofistikerede teknologier uoverkommelig for politimyndighederne. En sådan tolkning stemmer dog ikke overens med, hvad vi erfarede i forbindelse med vores interviews med de danske og hollandske politimyndighede, som udviste stor opmærksomhed på, hvor mange steder det kan gå galt. Ligeledes fandt vi, at de interviewede købere og sælgere aktivt vurderede de risici, de udsatte sig for, og at de ikke nødvendigvis traf paranoide valg. De interviewede købere var primært bekymrede for

selve forsendelsesprocessen, men tænkte tilsyneladende ikke udpræget over, hvorvidt deres køb på et senere tidspunkt ville kunne identificeres af politiet. En køber kaldte sig 'dum' for ikke at udøve tilpas forsigtighed og var utvivlsomt bekendt med at have truffet risikoøgende valg. Desuden påtalte køberen, at han burde anvende det sikre styresystem TAILS for at øge sin sikkerhed. Dette ville dog betyde, at han ville være nødsaget til at anvende mere tid til at gennemføre købene, huske flere kodeord og lære at anvende ny software. Den høje sikkerhed har desuden en høj pris for sælgerne. I forbindelse med vores feltarbejde identificerede vi en sælger, som i sin profil gjorde opmærksom på, at han opbevarede kundenavne for at forhindre gentagen svindel. Skulle sælgeren følge den bedste sikkerhedspraksis i forhold til at beskytte sig mod politimyndighederne, skulle han slette kundernes navne og oplysninger straks efter gennemført transaktion, hvilket samtidig ville betyde øget risiko for svindel.

Købernes fokus på nuet og den forventede pakke med stoffer er særligt relevant i lyset af politimyndigheders udsagn. Det er overraskende, at vi i i interviewene ikke identificerede bekymringer omhandlende blockchain-analyser, sælgernes opbevaring af adresser og køb af stoffer på sider, som var blevet lukket af politiet. Kriminologisk teori og forskning foreslår, at en afskrækkende effekt vil have mindre virkning, hvis der går lang tid mellem lovbrud og straf (Nagin & Pogarsky, 2001). Dette kan muligvis forklare, hvorfor køberne bekymrer sig om den mest umiddelbare risiko, forsendelsen, frem for det inkriminerende materiale, de efterlader. Hvis det forholder sig således, at købernes bekymringer kun relaterer sig til nuet, forsendelsen i posten, er Operation Hyperions målsætning om at sende besked til købenre formentlig ineffektiv, fordi køberne simpelthen ikke bekymrer sig om fremtiden. Med hensyn til effektiviteten af politioperationer, er det således værd at vurdere, om der er grundlag for at tro at brugere vil vurdere dem relevante.

5.1 Begrænsninger og fremtidig forskning

Vi ser en række spørgsmål, som kan forfølges i fremtidig forskning, som vi kortfattet opsummer i det følgende. Vores empiriske materiale er begrænset, men i forbindelse med projektet er vi påbegyndt en længerevarende indsamling af kvalitative data, som vi forventer vil medvirke til at besvare nogle af disse spørgsmål.

Aldridge & Askew (2017) observerer, at transaktioner via kryptomarkeder er trukket ud i tid i den forstand, at der kan gå dage eller uger mellem begyndelse på og afslutning af en transaktion. Vi foreslår, at fremtidig forskning forsøger at inkludere tid som dimension i både det kvalitative og kvantitativte arbejde. Informationsgrundlaget ophobes over tid, hvilket må formodes at påvirke brugernes adfærd. Ligeledes er tid en relevant faktor i

forbindelse med afskrækkelse, fordi den tidslige perioden mellem den ulovlige handling og den tilhørende straf er vigtig for effekten af afskrækkelsen (Nagin & Pogarsky, 2001).

Selvom alle vores informanter benyttede foraene, vurderer vi, at en del af brugerne på kryptomarkederne ikke anvender dem. Det kan således være en prioritet at specifikt søge inklusion af købere, som ikke anvender foraene, fordi vi på heraf kan udlede, om der eksisterer en relation mellem informationsgrundlaget og brugernes reelle adfærd. Særligt relevante spørgsmål er, hvorledes købere, som ikke anvender foraene, vurderer, hvilke lande de kan bestille fra, og hvorvidt deres brug af kryptering adskiller sig fra de brugere, som anvender foraene.

Vi fandt indikationer på, at Operation Hyperion havde ansporet sælgerne til at begå 'exit scams'. Dette er et underbelyst aspekt i forskningen. Det er i høj grad muligt, at selvom aktioner rettet mod postsystemet ikke resulterer i anholdelser, kan de gøre kriminalitet uøkonomisk for en periode. Særligt grundet sælgernes refusionspolitikker, afstedkommer sådanne indsatser en "dobbelt"straf, hvis sælger først mister produktet og derefter må kompensere kunden økonomisk. Sådanne ikke-intenderede konsekvenser af politioperationer kan med fordel studeres nærmere. Blandt andet er det værd at studere, hvorvidt politioperationer leder til øget risiko for 'exit scamming'.

Endeligt er kryptomarkeder illustrative for, hvordan brug af krypterings- og anonymiseringsteknologier indgår i sociale kontekster og udføres af personer med forskellige trusselsmodeller og mål. Vi foreslog derfor at diskutere *krypteringspraksis* frem for blot tilstedeværelsen og brugen af teknologi. Som det hollandske politi påpegede, kan sælgerne kryptere deres harddiske med kundeinformation med nok så sofistikerede midler, men hvis de skriver kodeordet ned på en post-it, er deres sikkerhedsforanstaltninger ligegyldige. Det er således vigtigere at tale om brugen af teknologien, samt hvordan denne indgår i sociale kontekster frem for teknologiens objektive kvaliteter. Fremtidig forskning kunne med fordel beskæftige sig medkrypteringspraksisse og studere nærmere, hvilke overvejelser brugerne gør sig, og hvordan de reelt anvender teknologien. I denne forbindelse kan det desuden studeres, hvorvidt operationer som Operation Hyperion og Operation Onymous har langtsigtede effekter i form af øget eller bedre brug af krypterings- og anonymiseringsteknologier.

Kapitel 6

Konklusion

I denne rapport har vi præsenteret Operation Hyperion detaljeret og vist, hvorledes operationen tog sit udgangspunkt i et øget internationalt samarbejde. Målet med operationen var at kommunikere et alternativ til, hvad politimyndighederne vurderede som en misforståelse af sikkerheden ved brug af kryptomarkeder. Denne indsigt søgtes kommunikeret gennem en række pressemeddelelser og operationer, som havde til formål at vise, at politimyndighederne i mange tilfælde havde mere inkriminerede information, end de kunne handle på. Operation Hyperion kunne derfor anskues som et "varselsskud".

Kort tid efter annonceringen af den nu afsluttede operation nåede informationen de kryptomarkedsrelaterede fora, hvor den blev diskuteret og analyseret af sælgerne og køberne. Operationen fik væsentligt mindre opmærksomhed end Operation Onymous, hvilket vi formoder skyldes, at Operation Onymous lukkede markedspladser, hvilket havde mærkbare *displacement*-effekter. I diskussionerne af operationen på foraene fandt vi, at brugeres vurdering af den i høj grad stemte overens med, hvad politimyndigheder søgte at kommunikere. Operationen ledte ligeledes til adfærdsændringer blandt nogle af brugerne, og vi observerede opfordringer til bedre sikkerhedspraksisser samt operationelle tiltag hos sælgerne. Yderligere fandt vi, at nogle sælgere stoppede deres handel, hvilket flere brugere tilskrev den øgede opmærksomhed som følge af Operation Hyperion. Endeligt observerede vi, at operationen havde en effekt på de individuelle sælgeres økonomiske situation.

Med udgangspunkt i disse fund åbnede vi for en bredere analyse af, hvorledes brugere på kryptomarkeder navigerer risici. Vi fandt i vores interviewmateriale, at både sælgerne og køberne i høj grad anvendte foraene til at tilpasse sig trusselsbilledet, hvilket særligt omfattede kvalificering af korrekt brug af teknologier. I forlængelse heraf fandt vi desuden, at købere var særligt interesserede i den risiko, som er associeret med forsendelsen af stoffer. Af denne grund efterspurgte vores interviewpersoner viden om, hvilke

faktorer, navnligt oprindelseslandet, som udsatte dem for øget risiko. Vi identificerede et aktivt norsk community med etablerede råd i forbindelse med bestillinger, hvor intet lignende eksisterer i en dansk kontekst. Dette peger således på, at de danske købere har et ringere informationsgrundlag for deres adfærd grundet mindre tilgængelig viden om de risici, som er associeret med kryptomarkederne. Både det hollandske og det danske politi påpegede, at omend kryptomarkederne i udgangspunkt kræver brugen af sofistikeret teknologi, er det ikke ensbetydende med, at handlen foregår risikofrit. Vi finder, at købere er akut opmærksomme på diverse risici, men at de samtidig vurderer, hvilke forbehold de bør tage. På baggrund af dette foreslår vi, at en diskussion, som tager højde for de konkrete *krypteringspraksisser* bedre kan begribe den forståelse sikkerhed, som brugerene opnår gennem kryptomarkederne.

Det er svært at identificere kortsigtede effekter af Operation Hyperion, men baseret på vores materiale ser vi to effekter. For det første observerer vi, at to sælgere nævnt af det hollandske politi er afhoppet, og for det andet finder vi, at flere brugere revurderer importen af cannabis fra Canada til Storbritannien. Effekter af sådanne operationer er dog komplekse, og de kan få betydning på længere sigt. Vi observerer opfordringer til øget og korrekt brug af krypteringsteknologi, hvilket kan være en potentiel langsigtet konsekvens af operationen. Ligeledes har vi grund til at tro, at Operaton Hyperion vil indgå i det informationsgrundlag, som brugerne trækker på, når de læser informationen på foraene, og det er forventeligt, at dette vil afstedkomme adfærdsændringer blandt både sælgere og købere.

Litteratur

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*. doi: 10.1016/j.drugpo.2016.10.010

Aldridge, J., & Décary-Hétu, D. (2014). Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *Available at SSRN 2436643*. doi: 10.2139/ssrn.2436643

Aldridge, J., & Décary-Hétu, D. (2016). Hidden Wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, *35*, 7–15. doi: 10.1016/j.drugpo.2016.04.020

Ashok, I. (2016, 5). *FBI hacking evidence in Playpen case thrown out after agency declines to provide code.* Tilgængelig på `http://www.ibtimes.co.uk/fbi-hacking-evidence-playpen-case-thrown-out-after-agency-declines-provide-code-1562103`

Bakken, S. (2015). *Silk Road 2.0-A Study of Cryptomarkets in a Deleuze-Guattarian Perspective* (Doctoral dissertation, University of Oslo). Tilgængelig på `https://www.duo.uio.no/handle/10852/44788`

Bancroft, A., & Reid, P. (2016a). Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society*, *20*(4), 497–512. doi: 10.1080/1369118X.2016.1187643

Bancroft, A., & Reid, P. S. (2016b). Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy*, *35*, 42–49.

Barratt, M. J. (2012). Silk Road: eBay for drugs. *Addiction*, *107*(3), 683.

Barratt, M. J., Lenton, S., & Allen, M. (2013). Internet content regulation, public drug websites and the growth in hidden Internet services. *Drugs: Education, Prevention & Policy*, *20*(3), 195–202. doi: 10.3109/09687637.2012.745828

Barratt, M. J., Lenton, S., Maddox, A., & Allen, M. (2016). 'What if you live on top of a bakery and you like cakes?'—Drug use and harm trajectories before, during and after the emergence of Silk Road. *International Journal of Drug Policy*, *35*, 50–57. doi: http://dx.doi.org/10.1016/j.drugpo.2016.04.006

Bjørnager, J. A., & Mortensen, M. W. (2017a, 2). *Dom: Tegnebog med bitcoins gav 23-årig otte år i fængsel.* Tilgængelig på `https://www.b.dk/nationalt/dom-tegnebog-med-bitcoins-gav-23-aarig-otte-aar-i-faengsel`

Bjørnager, J. A., & Mortensen, M. W. (2017b, 2). *Dom: Word-dokument og bitcoins fælder narkohandler.* Tilgængelig på `https://www.b.dk/nationalt/dom-word-dokument-og-bitcoins-faelder-narkohandler`

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets: structure and organisation from a Canadian perspective. *Forensic science international*, *264*, 7–14.

Brunt, T. M., Atkinson, A. M., Nefau, T., Martinez, M., Lahaie, E., Malzcewski, A., ... Brandt, S. D. (2017). Online test purchased new psychoactive substances in 5 different European countries: A snapshot study of chemical composition and price. *International Journal of Drug Policy*, *44*, 105–114. doi: 10.1016/j.drugpo.2017.03.006

Buxton, J., & Bingham, T. (2015). The rise and challenge of dark net drug markets. *Policy Brief*, *7*.

Caulkins, J. P., & Reuter, P. H. (2010). How Drug Enforcement Affects Drug Prices. *Crime and Justice*, *39*(1), 213–271. doi: 10.1086/652386

Christin, N. (2013). Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. *Proceedings of the 22nd international conference on World Wide Web*, 213–224. doi: 10.1145/2488388.2488408

Comey, J. B. (2014). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Tilgængelig på `https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course`

Cox, J. (2015, 11). *Court Docs Show a University Helped FBI Bust Silk Road 2, Child Porn Suspects.* Tilgængelig på `https://motherboard.vice.com/en_us/article/court-docs-show-a-university-helped-fbi-bust-silk-road-2-child-porn-suspects`

Cox, J. (2016, 11). *'Operation Hyperion' Targets Suspected Dark Web Users Around the World — Motherboard.* Tilgængelig på `http://motherboard.vice.com/read/operation-hyperion-targets-suspected-dark-web-users-around-the-world`

Cross, J. C. (2000). Passing the buck: Risk avoidance and risk management in the illegal/informal drug trade. *The International Journal of Sociology and Social Policy Social Science*, *20*(910), 68–94.

Cubrilovic, N. (2014). *Large Number of Tor Hidden Sites Seized by the FBI in Operation Onymous were Clone or Scam Sites.* Tilgængelig på `https://www.nikcub.com/`

posts/onymous-part1/

Décary-Hétu, D., & Giommoni, L. (2016, 10). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, 1–21. doi: 10.1007/s10611-016-9644-4

Demant, J., & Munksgaard, R. (2017). *Kryptomarkeder i en dansk og skandinavisk kontekst*. Copenhagen: Justitsministeriet.

Desimone, J. (2006). The relationship between illegal drug prices at the retail user and seller levels. *Contemporary Economic Policy*, *24*(1), 64–73. doi: 10.1093/cep/byj004

Dickinson, T., & Wright, R. (2015, 11). Gossip, Decision-making and Deterrence in Drug Markets. *British Journal of Criminology*, *55*(6), 1263–1281. doi: 10.1093/bjc/azv010

Dupont, B., Côté, A.-M., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime*, *17*(2), 1–23.

Duxbury, S. W., & Haynie, D. L. (2017). The Network Structure of Opioid Distribution on a Darknet Cryptomarket. *Journal of Quantitative Criminology*, *In print*. doi: 10.1007/s10940-017-9359-4

Europol. (2014). *Global Action Against Dark Market on Tor Network.* Tilgængelig på https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network

Europol. (2016). *IOCTA 2016 - Internet Organized Crime Threat Assesment*. Hague: Europol.

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *BMJ*, *323*(7321).

FBI. (2016). *A Primer on DarkNet Marketplaces.* Tilgængelig på https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces

Finn, M. A., & Stalans, L. J. (2016). How Targeted Enforcement Shapes Marketing Decisions of Pimps: Evidence of Displacement and Innovation. *Victims & Offenders*, 1–22.

Gehl, R. W. (2014). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, *18*(7), 1219–1235. doi: 10.1177/1461444814554900

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597–606.

Goldsmith, J. (2000). Unilateral regulation of the Internet: A modest defence. *European Journal of International Law*, *11*(1), 135–148.

Greenberg, A. (2014, 9). *FBI's Story of Finding Silk Road's Server Sounds a Lot Like Hacking.* Tilgængelig på https://www.wired.com/2014/09/fbi-silk-road-hacking-question/

Greenberg, A. (2015, 8). *Agora, the Dark Web's Biggest Drug Market, Is Going Offline.* Tilgængelig på `https://www.wired.com/2015/08/agora-dark-webs-biggest-drug-market-going-offline/`

Hall, A., Koenraadt, R., & Antonopoulos, G. A. (2017, 3). Illicit pharmaceutical networks in Europe: organising the illicit medicine market in the United Kingdom and the Netherlands. *Trends in Organized Crime*, 1–20. doi: 10.1007/s12117-017-9304-9

Hardy, R. A., & Norgaard, J. R. (2015, 9). Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics*, *12*(June), 1–25. doi: 10.1017/S1744137415000454

Hill, K. (2014, 11). *How did law enforcement break Tor?* Tilgængelig på `http://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break-tor/#4f21ca891b38`

Holt, T. J., Chua, Y.-T., & Smirnova, O. (2013). An exploration of the factors affecting the advertised price for stolen data. In *ecrime researchers summit (ecrs), 2013* (pp. 1–10).

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016, 4). Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets. *Deviant Behavior*, *37*(4), 353–367. doi: 10.1080/01639625.2015.1026766

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596–614. doi: 10.1093/bjc/azu106

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11–30. doi: 10.1080/17440572.2016.1197123

Jacques, S., Allen, A., & Wright, R. (2014). Drug dealers' rational choices on which customers to rip-off. *International Journal of Drug Policy*, *25*, 251–256. doi: 10.1016/j.drugpo.2013.11.010

Jeong, S. (2015, 1). *The DHS Agent Who Infiltrated Silk Road to Take Down Its Kingpin.* Tilgængelig på `http://www.forbes.com/sites/sarahjeong/2015/01/14/the-dhs-agent-who-infiltrated-silk-road-to-take-down-its-kingpin/#5612174969dd`

Kozinets, R. V. (2002). The Field behind the Screen: Using Netnography for Marketing Research in Online Communities. *Journal of Marketing Research*, *39*(1), 61–72.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*. Santa Monica, CA: RAND Corporation. Tilgængelig på `http://www.rand.org/pubs/research_reports/RR1607.html`

Ladegaard, I. (2017, 4). We Know Where You Are, What You Are Doing and We Will Catch You. *The British Journal of Criminology*, *4*, 175–92. doi: 10.1093/bjc/azx021

Landelijk Parket. (2016). *Dutch National Prosecution Service and police launch Hidden Service in global Darknet enforcement operation.* Tilgængelig på `https://www.om.nl/actueel/nieuwsberichten/@96509/dutch-national/`

Lavoie, M., & Décary-Hétu, D. (2017). *Bitcluster.* Tilgængelig på `https://github.com/mathieulavoie/Bitcluster`

Locker, T. (2015, 3). *The Rise and Fall of Shiny Flakes, Germany's Online Drug Market.* Tilgængelig på `https://motherboard.vice.com/en_us/article/the-rise-and-fall-of-shiny-flakes-germanys-online-drug-market`

Loughran, T. A., Paternoster, R., Piquero, A. R., & Pogarsky, G. (2011, 11). ON AMBIGUITY IN PERCEPTIONS OF RISK:IMPLICATIONS FOR CRIMINAL DECISION MAKING AND DETERRENCE*. *Criminology*, *49*(4), 1029–1061. doi: 10.1111/j.1745-9125.2011.00251.x

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society*, *19*(1), 111–126. doi: 10.1080/1369118X.2015.1093531

Maher, L., & Dixon, D. (1999). Policing and public health: Law enforcement and harm minimization in a street-level drug market. *British journal of criminology*, *39*(4), 488–512.

Martin, J. (2014a). *Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs [Kindle edition].* Palgrave Macmillan.

Martin, J. (2014b). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice*, *14*(3), 351–367. doi: 10.1177/1748895813505234

Martin, J., & Christin, N. (2016). Ethics in Cryptomarket Research. *International Journal of Drug Policy*. doi: 10.1016/j.drugpo.2016.05.006

Mathison, S. (1988). Why triangulate? *Educational researcher*, *17*(2).

Mullin, J. (2015, 3). *Silk Road drug dealer who cooperated, then fled, sentenced to five years.* Tilgængelig på `http://arstechnica.com/tech-policy/2015/03/silk-road-drug-dealer-who-cooperated-then-fled-sentenced-to-five-years/`

Munksgaard, R., Demant, J., & Branwen, G. (2016). A replication and methodological critique of the study 'Evaluating drug trafficking on the Tor Network'. *International Journal of Drug Policy*, *35*. doi: 10.1016/j.drugpo.2016.02.027

Nagin, D. S. (1998, 1). Criminal Deterrence Research at the Outset of the Twenty-First Century. *Crime and Justice*, *23*, 1–42. Tilgængelig på `http://www.journals.uchicago.edu/doi/10.1086/449268` doi: 10.1086/449268

Nagin, D. S., & Pogarsky, G. (2001). Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence. *Criminology*, *39*.

New Zealand Police. (2016). *Kiwi darknet illegal drug buyers identified during worldwide operation.* Tilgængelig på `http://www.police.govt.nz/news/release/kiwi-darknet-illegal-drug-buyers-identified-during-worldwide-operation?nondesktop`

Nurmi, J., Kaskela, T., Perälä, J., & Oksanen, A. (2017). Seller's reputation and capacity on the illicit drug markets: 11-month study on the Finnish version of the Silk Road. *Drug and Alcohol Dependence*, *178*, 201–207. doi: 10.1016/j.drugalcdep.2017.05.018

Paternoster, R. (1987). The Deterrent Effect of the Perceived Certainty and Severity of Punishment: A Review of the Evidence and Issues. *Justice Quarterly*, *4*.

Polisen. (2016). *Tusentals köpare av droger på nätet identifierade.* Tilgængelig på `https://polisen.se/Stockholms_lan/Aktuellt/Nyheter/2016/Oktober/Tusentals-kopare-av-droger-pa-natet-identifierade/`

RCMP. (2016). *The RCMP and law enforcement agencies around the world collaborate on international Darknet marketplace enforcement.* Tilgængelig på `http://www.rcmp-grc.gc.ca/en/news/2016/1/the-rcmp-and-law-enforcement-agencies-the-world-collaborate-international-darknet`

Schulze, M. (2017). Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. *Media and Communication*, *5*(1), 54. doi: 10.17645/mac.v5i1.805

Slobbe, J. v. (2016). The drug trade on the deep web: a law enforcement perspective. In *The internet and drug markets* (pp. 77–83). Luxembourg: Publications Office of the European Union. Tilgængelig på `www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf`

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *24th USENIX Security Symposium (USENIX Security 15)*, 33–48.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in organized crime*, *15*(2-3), 111–129. doi: 10.1007/s12117-012-9159-z

Steinmetz, K. F. (2012, 2). Message Received: Virtual Ethnography in Online Message Boards. *International Journal of Qualitative Methods*, *11*(1), 26–39. doi: 10.1177/160940691201100103

Stevens, R., Gilliard-Matthews, S., Dunaev, J., Woods, M. K., & Brawner, B. M. (2016). The digital hood: Social media use among youth in disadvantaged neighborhoods. *New Media & Society*, 1461444815625941.

Strelan, P., & Boeckmann, R. J. (2006, 12). Why Drug Testing in Elite Sport Does Not Work: Perceptual Deterrence Theory and the Role of Personal Moral Beliefs. *Journal of Applied Social Psychology*, *36*(12), 2909–2934. doi: 10.1111/j.0021-9029

.2006.00135.x

Teleindustrien. (2017). *Blokeringer på nettet.* Tilgængelig på `http://www.teleindu.dk/brancheholdninger/blokeringer-pa-nettet/`

Tor Project. (2015). *Did the FBI pay university to hack Tor users?* Tilgængelig på `https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users`

Tupman, B., Zabyelina, Y., & Lavorgna, A. (2015). Organised crime goes online: realities and challenges. *Journal of Money Laundering Control*, *18*(2), 153–168.

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., & Roxburgh, A. (2017). The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence*. doi: 10.1016/j.drugalcdep.2017.01.004

Van Buskirk, J., Roxburgh, A., Farrell, M., & Burns, L. (2014, 4). The closure of the Silk Road: what has this meant for online drug trading? *Addiction*, *109*(4), 517–518. doi: 10.1111/add.12422

van Hardeveld, G. J., Webber, C., & O'Hara, K. (2016). Discovering credit card fraud methods in online tutorials. In *Proceedings of the 1st international workshop on online safety, trust and fraud prevention* (p. 1).

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, *25*(2), 183–189.

Vitáris, B. (2017, 1). *176 Investigations Started In Sweden, Operation Hyperion - Deep Dot Web.* Tilgængelig på `https://www.deepdotweb.com/2017/01/06/176-investigations-started-norway-operation-hyperion/`

Watson, H., Finn, R. L., & Barnard-Wills, D. (2017). A gap in the market: the conceptualisation of surveillance, security, privacy and trust in public opinion surveys. *Surveillance & Society*, *15*(2), 269–285.

Williams, K. R., & Hawkins, R. (1986). Perceptual Research on General Deterrence: A Critical Review. *Law & Society Review*, *20*(4), 545. doi: 10.2307/3053466

Yip, M., Webber, C., & Shadbolt, N. (2013, 12). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing & Society*, *23*(4), 516–539. doi: 10.1080/10439463.2013.780227