Samenvatting van de afstudeerscriptie 2016-2017:

BITCOINS EN CRIMINALITEIT, EEN ONVERMIJDELIJK VERBAND? ONDERZOEK NAAR DE UITDAGINGEN BIJ DE AANPAK VAN CRIMINALITEIT GEPLEEGD MET BITCOINS

Auteur: Shana Soetaert, criminologische wetenschappen UGent

Inleiding

De opkomst van het internet heeft de samenleving de laatste decennia grondig veranderd en zette de mogelijkheden en uitdagingen van globalisatie tevens als beleidsthema op de kaart. (Simons, 2002). Zo speelt het internet niet alleen op vlak van communicatie maar ook op economisch vlak een belangrijke rol. Online bankieren is eerder de regel dan de uitzondering en ook het aantal webshops is niet meer bij te houden (Litan & Rivlin, 2010). In een mum van tijd worden grote afstanden overbrugd zonder dat men zich daadwerkelijk hoeft te verplaatsen. Bovendien beperkt het internet zich niet langer tot computers maar zijn ook smartphones, tablets, spelconsoles… uitgerust met deze functie. Op die manier kan men dus waar en wanneer men wil op het internet surfen (Simons, 2002).

Het digitaal tijdperk heeft voor een ommezwaai gezorgd maar gaat bijgevolg ook gepaard met nieuwe problemen en uitdagingen (Federale Overheid, 2016). Zo zijn er sinds de komst van het internet razendsnel nieuwe mogelijkheden ontstaan. Helaas worden vele mogelijkheden die het internet met zich meebrengt steeds vaker misbruikt. De snelheid van het internet en de afwezigheid van grenzen zorgt voor een vergemakkelijking van verschillende criminele daden. Deze opportuniteiten voor criminaliteit zorgen voor nieuwe uitdagingen voor politie en justitie bij opsporing en vervolging van daders. In het Belgisch beleid werden Cybercrime en cybersecurity dan ook opgenomen als beleidsprioriteit in het Nationaal Veiligheidsplan 2016-2019 (Jambon & Geens, 2016).

“Cybercriminaliteit of cybercrime is een misdrijf waarbij automatisering en geautomatiseerde gegevens worden misbruikt als middel, maar waarbij tevens de informaticasystemen of de erin opgeslagen gegevens het doelwit kunnen zijn”(Di Rupo, 2012, p.53.).

In dit veiligheidsplan wordt ook specifiek verwezen naar de opmars van de ransomware (Jambon & Geens, 2016). Dit is een manier om losgeld (ransom) te verkrijgen van slachtoffers door hun computers te blokkeren en in ruil voor een deblokkering gelden te eisen (Verhofstadt, 2014). Niet onbelangrijk hierbij is de aandacht voor de link tussen ransomware en bitcoins. Voor ransomware in het bijzonder en voor criminaliteit in het algemeen wordt namelijk steeds vaker gebruik gemaakt van bitcoins. Dit blijkt mede uit Europol’s Internet Organised Crime Threat Assessment 2

(IOCTA) van 2016 waarin gesteld wordt dat cybercriminelen bitcoins als betaalmiddel blijven gebruiken (Europol, 2016b). Doordat criminelen gebruik blijven maken van deze virtuele, gedecentraliseerde munt worden politiediensten dus frequenter geconfronteerd met bitcoins.

Aangezien bitcoins pas in 2009 werden ontwikkeld en er nog maar weinig wetenschappelijk onderzoek voor handen is, wordt in deze masterproef de gelegenheid aangegrepen deze digitale munt eens van naderbij te bekijken (Nakamoto, 2009).

Probleemstelling

Tijdens de stage die vorig jaar plaatsvond bij de Federale Gerechtelijke Politie West-Vlaanderen kon van dichtbij ervaren worden hoe politiediensten vaak voor een uitdaging worden geplaatst wanneer criminelen gebruik maken van het nieuwe bitcoin-betaalnetwerk. Een concreet voorbeeld: de afwezigheid van een centrale instelling of overheid waarbij ten rade kan worden gegaan om gegevens over gebruikers te bekomen. Het gedecentraliseerd karakter van bitcoins bezorgt de gebruiker dus een grotere anonimiteit doordat er een beroep wordt gedaan op een combinatie van cryptografie(1)1 en een peer-to-peer-netwerk2 (Janssens, Soetaert, & De Vos, 2017). De opsporing van daders die gebruik maken van bitcoins is dus geen sinecure (Sirer, 2016). Daarnaast duiken ook nieuwe criminele fenomenen op waar politiediensten voordien maar weinig mee in aanraking zijn gekomen. Het toenemend belang van het dark web is hier een voorbeeld van (Hendrickson, Hogan, & Luther, 2016).

1 Cryptografie houdt in dat informatie versleuteld en verborgen wordt (Mendez, van Oorschot, & Vanstone, 2014). (2)

Een peer-to-peer-netwerk betekent dat er gegevens worden uitgewisseld zonder daarbij gebruik te maken van één centrale gebruiker of server (Schollmeier, 2001).

Reeds in 2012 trok het Federal Bureau of Investigation (FBI) aan de alarmbel door toen al te voorspellen dat het bitcoin-betaalnetwerk zou worden misbruikt door criminelen (FBI, 2012). Ondertussen, vijf jaar later, blijkt die voorspelling daadwerkelijk te zijn uitgekomen. Toch loopt bitcoinonderzoek anno 2017 nog steeds niet van een leien dakje. Het problematisch karakter van bitcoinonderzoek vormt dan ook de probleemstelling van deze masterproef. Het bitcoin-betaalnetwerk zorgt namelijk voor een lage opsporings- en vervolgingsgraad. Hierdoor kunnen criminelen die gebruik maken van bitcoins meestal ongestraft hun activiteiten verderzetten en de vruchten blijven plukken van hun criminele daden. Daarnaast moeten ook de slachtoffers van dergelijke misdrijven vrede nemen met het feit dat zij nooit zullen worden vergoed voor de schade (3) en het leed dat hen werd berokkend. Doorheen de masterproef zal duidelijk worden waar de knelpunten zich situeren en wat de mogelijke oorzaken hiervan zijn. Deze masterproef poogt dan ook bij te dragen aan de beeldvorming over het fenomeen, zijnde misbruik van bitcoins voor criminele doeleinden, en de kennis over knelpunten en eventuele opportuniteiten in het opsporingsonderzoek samen te brengen.

Onderzoeksvragen

Om de bitcoinproblematiek binnen het politiewezen te duiden en de lezer kennis te laten maken met bitcoins, werden enkele onderzoeksvragen opgesteld die de masterproef vormgeven. Drie hoofdvragen kunnen telkens worden onderverdeeld in twee bijvragen:

- Wat zijn bitcoins?

- Waarom, wanneer en hoe zijn bitcoins ontstaan? (A)

- Op welke manier werkt het bitcoin-betaalnetwerk? (B)

 Waar worden bitcoins voor gebruikt?

- Welke zijn de legale doeleinden van bitcoins? (C)

- Welke zijn de illegale doeleinden van bitcoins? (D)

 Welke problemen en oorzaken van deze problemen kunnen worden geïdentificeerd in de politionele aanpak van criminaliteit gepleegd met bitcoins?

- Welke problemen worden door de bevraagde respondenten aangegeven inzake bitcoinonderzoek? (E)

- Welke suggesties kunnen geformuleerd om tegemoet te komen aan de huidige problematiek? (F)

Aan de hand van wetenschappelijke literatuur wordt eerste het begrippenkader besproken waarin een grondige beschrijving wordt gegeven van bitcoins. Als lezer is het namelijk belangrijk hier een inzicht in te hebben om het verdere verloop van de masterproef te kunnen begrijpen. Aan de hand van het eerste hoofdstuk van dit deel wordt een antwoord gegeven op onderzoeksvraag A. Onderzoeksvraag B en C worden behandeld in het tweede hoofdstuk van het begrippenkader.(4)

Van zodra de lezer vertrouwd is geraakt met de werking en filosofie van bitcoins, komt het empirisch luik aan bod. In hoofdstuk 1 van het empirisch luik wordt de focus verplaatst naar de criminele activiteiten waarmee bitcoins in verband kunnen worden gebracht. In dit deel ligt de aandacht dus op deelvraag D betreffende de illegale doeleinden van bitcoins. Deze illegale activiteiten zorgen ervoor dat politiediensten geconfronteerd worden met bitcoins. Hoofdstuk 2 van het empirisch luik staat vervolgens stil bij de rol van de politie bij de opsporing van deze vormen van criminaliteit. Enerzijds worden de tools besproken die door politie gebruikt worden voor het voeren van bitcoinonderzoek. Anderzijds wordt stilgestaan bij de problemen die men binnen de politie ervaart wanneer onderzoek moet worden gevoerd naar bitcoins om zo een antwoord te kunnen bieden op deelvraag E. Er zal ook getracht worden enkele zaken te concluderen in verband met de pakkans en een criminologische theorie te selecteren die hierbij aansluit.

De masterproef wordt afgesloten met enkele aanbevelingen en besluiten. Er wordt enerzijds stilgestaan bij de initiatieven die reeds werden ondernomen op nationaal en internationaal niveau. Anderzijds worden er een aantal suggesties geformuleerd ter beantwoording van deelvraag F, die bitcoinonderzoek in de toekomst zouden kunnen faciliteren. Deze voorstellen worden geformuleerd aan de hand van de suggesties die de respondenten hebben aangegeven alsook aan de hand van eigen aanbevelingen.

Doelstelling

Uit de opgestelde onderzoeksvragen kan al worden afgeleid dat de doelstelling van deze masterproef meervoudig is. Ten eerste wordt bijgedragen aan de beeldvorming van het

bitcoin fenomeen. Het is de bedoeling de lezer op een globale, duidelijke manier kennis te laten maken met bitcoins en te duiden welke mogelijkheden de bitcoin heeft. Daarnaast dient de lezer ook op de hoogte te worden gebracht over de rol die bitcoins spelen in verschillende criminele feiten om te begrijpen waarom politiediensten geconfronteerd worden met deze virtuele munt. Er zijn natuurlijk nog andere virtuele munten, maar in het tijdsbestek van deze masterproef werd besloten uitsluitend te focussen op bitcoins. Dit omdat bitcoins het vaakst worden gebruikt voor criminele doeleinden en een elaboratie naar andere virtuele munten te complex zou kunnen zijn voor de lezer (Europol, 2016b). Het is dus niet de bedoeling de bitcoin te bestempelen als zijnde een intrinsiek criminele munt aangezien de bitcoin ook heel wat mogelijkheden met zich meebrengt.(5)

Wel is het belangrijk om de lezer te laten inzien dat niet alleen wetsgetrouwe burgers gebruik maken van deze mogelijkheden.

De tweede doelstelling bestaat erin de actuele uitdagingen waarvoor Vlaamse politiediensten staan bij bitcoinonderzoek te inventariseren. Onder Vlaamse politiediensten worden die diensten begrepen die reeds onderzoek hebben gevoerd naar bitcoins. Tot op heden is wetenschappelijk onderzoek specifiek naar de werking van onze opsporingsdiensten inzake bitcoinonderzoek en de hiermee gepaard gaande problemen afwezig waardoor de masterproef tegemoet wil komen aan deze lacune. Het is immers contradictorisch dat cybercrime als een van de prioritaire criminaliteitsfenomenen wordt beschouwd, terwijl er maar beperkte aandacht geschonken wordt aan de bitcoinproblematiek die toch een belangrijke rol speelt in het hele cybercrime-verhaal. De derde doelstelling van deze masterproef is dan ook om aan agenda-setting te doen en de ernst van de bitcoinproblematiek onder de aandacht te brengen. Tot slot zullen ook enkele beleidsaanbevelingen en suggesties ter optimalisatie van bitcoinonderzoek worden geformuleerd op nationaal en internationaal niveau die dit onderzoek in de toekomst kunnen verbeteren.

In het volgende deel zal worden stilgestaan bij de methodologie en theorie die zal worden gehanteerd om de onderzoeksvragen te beantwoorden en om de doelstelling te realiseren.(6)

METHODOLOGIE EN THEORIE

Uit de inleiding kan geconcludeerd worden dat de masterproef vooral de vorm aanneemt van een praktijkgericht onderzoek omdat er vertrokken wordt vanuit een praktijksituatie, namelijk het problematische karakter van bitcoinonderzoek, met de bedoeling deze problematische situatie onder de aandacht te brengen. Er zal met andere woorden een probleemanalytisch onderzoek worden gevoerd waarbij het de bedoeling is de aandacht te vestigen op dit probleem en ervoor te zorgen dat dit zichtbaar en bespreekbaar wordt. Daarnaast zal de masterproef ook de achtergronden van de problemen trachten te achterhalen waardoor er niet uitsluitend sprake is van een probleemanalytisch onderzoek, maar tevens ook van een diagnostisch onderzoek: op die manier kan een richting worden gesuggereerd waarin naar oplossingen gezocht kan worden (Decorte, Tieberghien, & Petintseva, 2016). Om dit te realiseren wordt er in deze masterproef een tweeledige

methode toegepast. Ten eerste is er de literatuurstudie die de bedoeling heeft de lezer meer kennis te verschaffen inzake bitcoins en het bitcoin-betaalnetwerk. Anderzijds is er het empirisch onderzoek waarbij kwalitatieve, semigestructureerde interviews werden afgenomen met respondenten.

Hieronder volgt een overzicht van het onderzoeksmateriaal waarop een beroep werd gedaan om een antwoord te formuleren op de verschillende onderzoeksvragen. Daarna wordt ook beschreven welke materiaal in welk deel aan bod komt. Na het bespreken van het onderzoeksmateriaal wordt stilgestaan bij enkele ethische principes. Tot slot wordt besproken binnen welk criminologisch paradigma deze masterproef gesitueerd kan worden en wordt ook de relevantie van de masterproef toegelicht.

1 Onderzoeksmateriaal

Om de onderzoeksvragen te beantwoorden werd ervoor gekozen om aan bronnentriangulatie te doen. Dit omdat elke bron zijn voor-en nadelen heeft en het dus belangrijk is zo veel mogelijk tegemoet te komen aan de nadelen van bepaalde bronnen door deze te combineren met andere (Decorte et al., 2016).

1.1 Literatuur

Vooreerst is literatuur een belangrijke kennisbron. Er werden reeds verschillende boeken gepubliceerd die bitcoins onder de aandacht brengen, alsook wetenschappelijke artikelen. (7)

Het grootste voordeel van literatuur is dat er inzicht verkregen kan worden in de complexe werking van bitcoins. Daarnaast is het ook een snelle manier om kennis te vergaren aangezien er beroep wordt gedaan op bestaande informatie en inzichten (Williamson & Whittaker, 2017).

Een mogelijk nadeel aan de keuze voor literatuur is het feit dat bitcoins een recent verschijnsel zijn waardoor literatuur niet altijd even uitgebreid aanwezig is. Daarnaast werd tijdens het schrijven van de masterproef vastgesteld dat de wetenschappelijke literatuur het niet altijd eens is over sommige zaken. Dit is dan ook een nadeel van literatuur (Williamson & Whittaker, 2017). Om hieraan tegemoet te komen werd ervoor gekozen bepaalde informatie aan te vullen of na te gaan op validiteit via interviews met respondenten. Zij zijn nauw betrokken bij bitcoinonderzoek waardoor zij eigenlijk als praktijkdeskundigen kunnen worden beschouwd (Decorte et al., 2016).

1.2 Personen

Naast literatuur zijn ook personen onontbeerlijk omdat het grootste deel van de masterproef handelt over de problemen die Vlaamse politiediensten ervaren bij bitcoinonderzoek. Om hierover informatie te bekomen dienen natuurlijk personen binnen het politiewezen geraadpleegd te worden die ervaring hebben met bitcoinonderzoek. Dit blijkt niet evident te zijn: bitcoinonderzoek wordt meestal gecentraliseerd bij het Regional Computer Crime Unit (RCCU) en bij de Federal Computer Crime Unit (FCCU). Het RCCU situeert zich in elk arrondissement binnen de gerechtelijk directie. Hun taak bestaat erin

sporen van internetcriminaliteit te onderzoeken en daders te identificeren. Het FCCU situeert zich daarentegen op nationaal niveau in de directie van de bestrijding van georganiseerde en zware criminaliteit en ondersteunt het RCCU waar nodig (Federale Politie, 2017).

1.2.1 Selectie van de respondenten

Om respondenten te selecteren werd gebruik gemaakt van de sneeuwbalsteekproef. Dit houdt in dat aan de reeds bevraagde respondenten wordt gevraagd of zij andere personen kunnen aanbevelen die mogelijks meer informatie kunnen verschaffen (Bailey, 2008). Er werd voor deze methode gekozen omdat het als buitenstaander niet evident is te weten wie er binnen de politie al dan niet onderzoek voert naar bitcoins. De sneeuwbalsteekproef is dan ook een ideale manier om hieraan tegemoet te komen (Babbie, 2010).(8)

Om van start te gaan moet natuurlijk een eerste respondent geselecteerd worden. Hiervoor werd een beroep gedaan op een persoon met wie een goede band is ontstaan tijdens het uitoefenen van de stage en die bovendien vaak geconfronteerd wordt met bitcoins. De eerste respondent zorgde ervoor dat nog twee andere personen die ook actief bitcoinonderzoek voeren, deelnamen aan het interview. Deze konden opnieuw enkele andere personen aanbevelen. Aangezien er maar een select aantal personen zijn die actief onderzoeken voeren naar bitcoins, werden vaak dezelfde mensen aanbevolen. Naast de eerste respondent die via de stage bewust werd gekozen, konden via de sneeuwbalsteekproef nog vijf andere respondenten worden geïnterviewd. Daarnaast hadden de respondenten het tijdens de interviews soms over bepaalde personen, waardoor ook bij hen ten rade kon worden gegaan of er al dan niet bereidheid was om mee te werken aan de masterproef. Deze werden dus niet expliciet aanbevolen, maar toch gecontacteerd omdat er een vermoeden was dat ook zij interessante zaken konden vertellen. Op deze manier werden nog twee respondenten geselecteerd waardoor er in totaal acht personen konden worden geïnterviewd. Tijdens het selecteren van respondenten was er slechts één persoon die niet wou meewerken. Alle andere respondenten die gecontacteerd werden waren zeer enthousiast en bereid meer informatie te geven over bitcoinonderzoek.

Omdat bitcoinonderzoek vooral geconcentreerd wordt binnen Computer Crime Units3 is het merendeel van de respondenten lid van een RCCU of het FCCU. Er werden RCCU's in drie verschillende provincies in Vlaanderen bezocht alsook het FCCU. Daarnaast werd ook een interview afgenomen met een substituut-Procureur des Konings die nauw samenwerkt met het RCCU en FCCU inzake bitcoinonderzoek. Deze persoon is op provinciaal niveau verantwoordelijk voor dossiers inzake cybercriminaliteit waardoor deze vaak samenzit met RCCU en FCCU en de nodige vorderingen moet uitvaardigen in het kader van bitcoinonderzoeken. Tot slot werd ook een persoon van het team ICT-criminaliteit geraadpleegd omdat deze persoon samenwerkt met het RCCU en tevens vaak onderzoek voert naar bitcoins. In bijlage 1 kan een overzicht teruggevonden worden van de functies van de respondenten.

(-)

1.2.2 Semigestructureerde interviews

Om zo veel mogelijk informatie te bekomen van de respondenten werd gebruik gemaakt van semigestructureerde interviews die mondeling werden afgenomen. De reden waarom voor (9) semigestructureerde interviews werd gekozen is omdat gestructureerde interviews niet voldoende wendbaar zijn aangezien bij dergelijke interviews de vragen op voorhand worden opgesteld en in een vaste volgorde aan bod komen (Willig & Stainton-Rogers, 2008). Op die manier zou mogelijks veel informatie verloren gaan omdat de respondent enkel op de vooraf opgestelde vragen dient te antwoorden. Ook een ongestructureerd interview leek niet geschikt voor deze masterproef omdat er bij dergelijke interviews slechts een algemene vraag wordt gesteld waarover de respondent vrij kan vertellen. Dit zou het risico inhouden dat de interviews te veel zouden afwijken van de kern, zijnde de problemen bij bitcoinonderzoek, en dat enkele cruciale vragen onbeantwoord bleven. Daarom werd besloten gebruik te maken van een mengvorm, zijnde het semigestructureerde interview. Hierbij werd een topiclijst opgesteld met enkele thema's die het interview moesten leiden, maar zeker niet allesbepalend waren. Op die manier had de respondent de mogelijkheid dieper in te gaan op bepaalde zaken die volgens hem of haar belangrijk waren, maar kwamen ook de thema's aan bod die belangrijk waren voor deze masterproef (Decorte & Zaitch, 2010; Willig & Stainton-Rogers, 2008).

De thema's die voornamelijk aan bod kwamen in de topiclijst houden verband met de problemen die politiediensten ervaren bij bitcoinonderzoek, de ervaringen van de respondent met bitcoins, visie over mogelijkheden, de oplossingsgraad van bicoinonderzoek, criminele feiten die gepleegd worden met bitcoins… Deze thema's bleken een goede gids te zijn aangezien de topiclijst gedurende de acht interviews niet werd gewijzigd. Wel werd er voor één interview de wetgeving als extra thema opgenomen in de topiclijst omdat de respondent een juridische achtergrond had en het de bedoeling was tijdens het interview wat meer informatie hieromtrent te bekomen. De topiclijst die werd gebruikt voor de respondenten binnen het politiewezen is terug te vinden in bijlage 2, deze voor de respondent met juridische achtergrond in bijlage 3.

1.2.3 Dataverwerking

Omdat interviews een hoge informatiedichtheid hebben en bovendien de meest belangrijke bron van informatie waren voor bepaalde onderzoeksvragen, werd ervoor gekozen om, mits toestemming van de respondenten via informed consent, geluidsopnames te maken. Op die manier ging er geen tijd verloren aan het nemen van notities en wordt ook het risico uitgesloten dat belangrijke informatie verloren ging (Harinck, 2010). Na het afnemen van de interviews werden de geluidsopnames vervolgens getranscribeerd. Op die manier konden de verschillende (10) transcripten worden vergeleken en geanalyseerd om na te gaan welke de knelpunten zijn die vaak werden aangegeven door de verschillende respondenten (Leavy, 2014). Omdat het voor deze masterproef niet nuttig is de volledige transcripten op te nemen, werden er verschillende citaten geselecteerd om te gebruiken in de masterproef ter illustratie van bepaalde stellingen. Mocht er toch een wens zijn volledige transcripten te bekijken, kunnen deze bij de auteur geraadpleegd worden.

1.2.4 Mogelijke beperkingen

Hoewel het semigestructureerde interview met geluidsopnames een goede methode blijkt te zijn, dient ook stil te worden gestaan bij de mogelijke beperkingen ervan. Omdat gewerkt werd met een topiclijst bestaat er nog steeds een risico dat respondenten te veel gaan afwijken van het onderwerp. Als interviewer is het belangrijk het interview goed bij te sturen om dit te voorkomen. Voor deze masterproef werd beslist zo weinig mogelijk tussen te komen in het interview omdat het de bedoeling was zo veel mogelijk informatie te bekomen over bitcoins in het algemeen en over bitcoinonderzoek in het bijzonder. Door respondenten zo veel mogelijk aan het woord te laten kwamen soms nieuwe zaken aan het licht waardoor ook meer inzicht werd verworven in het thema. Er werd wel gepoogd alle vooraf opgestelde vragen te stellen, maar als respondenten veel te vertellen hadden over een bepaald aspect van bitcoins werd hen ook de mogelijkheid geboden hier verder op in te gaan. Dit is ook de reden waarom sommige interviews meer tijd in beslag namen dan andere (Rowley, 2016). Gemiddeld nam een interview 45 minuten in beslag.

Andere knelpunten houden verband met het feit dat respondenten werkzaam zijn binnen politie en justitie. Daardoor zullen interviews mogelijk soms vertrouwelijke informatie met zich meebrengen. Zo kan een respondent misschien bepaalde zaken uitgebreid toelichten, waardoor gevoelige informatie aan het licht kan komen. In dit opzicht is het belangrijk om als onderzoeker deze vertrouwelijke informatie niet verder te verspreiden.

Het is tot slot ook belangrijk de onpartijdigheid te bewaren (Bogaert et al., 2009). Misschien zullen sommige respondenten negatiever tegenover bitcoins staan dan andere. Misschien is er onenigheid tussen bepaalde diensten en zullen respondenten dit onbewust in hun antwoorden laten doorwegen door bepaalde diensten te viseren. Het zal dus belangrijk zijn de objectieve informatie te gebruiken en de subjectieve zo veel mogelijk weg te filteren. (11)

1.3 Media

Een derde informatiebron in deze masterproef is de media, en in het bijzonder het internet. Er zijn verschillende zoeksystemen voorhanden waardoor op een snelle manier via het internet naar informatie kan worden gezocht. Via het internet kan wetenschappelijke literatuur worden opgezocht maar tevens ook niet-wetenschappelijke bronnen zoals filmpjes, fora, websites… Er is met andere woorden een hoge informatiedichtheid (Decorte et al., 2016).

Wat wel in rekening moet worden gebracht, is de mate van validiteit. Zo staat niet met zekerheid vast of bepaalde zaken correct zijn of niet. Om hieraan tegemoet te komen werd steeds geprobeerd wetenschappelijke ondersteuning te vinden voor de informatie die verkregen werd uit niet-wetenschappelijke bronnen (Decorte et al., 2016). Ook waren bepaalde respondenten bereid bijkomende informatie te verschaffen indien bepaalde zaken onduidelijk waren.

1.4 Beantwoorden van de onderzoeksvragen

Het eerste luik van deze masterproef betreft het begrippenkader en is vooral van beschrijvende aard. In dit luik wordt een grondige beschrijving gegeven van bitcoins en het bitcoin-betaalnetwerk. Hierin wordt een antwoord geformuleerd op de vragen A, B en C. Dit

deel kwam dus voornamelijk tot stand via wetenschappelijke bronnen zoals boeken en artikelen. Daarnaast werd ook een beroep gedaan op internetbronnen zoals websites en filmpjes. Dit omdat bitcoins complex in elkaar zitten en het via literatuur niet altijd eenvoudig is te begrijpen hoe bepaalde zaken werken. Deze internetbronnen waren hoofdzakelijk van secundaire aard en werden gebruikt om bepaalde onduidelijkheden in wetenschappelijke literatuur te verhelderen.

Na het begrippenkader volgt het empirisch luik. Hoewel het empirisch luik voornamelijk gebaseerd werd op de afgenomen interviews, komt in dit luik ook ander onderzoeksmateriaal aan bod. Zo was literatuur ook belangrijk voor hoofdstuk 1 van dit luik, waarin dieper wordt gefocust op de criminele activiteiten die gepleegd worden met bitcoins. Om te antwoorden op de vraag met welke criminele activiteiten politiediensten geconfronteerd worden, diende wel vertrokken te worden vanuit interviews. Op basis van die informatie kon in de literatuur aanvullende gegevens worden opgezocht. Dit was belangrijk omdat sommige zaken voor de respondenten erg evident zijn, waardoor ze niet steeds alle termen of wetgeving duidelijk toelichtten, en om bepaalde zaken te staven met wetenschappelijke bronnen.(12)

Hoofdstuk 2 van het empirisch luik dat focust op de rol van de politie bij de opsporing van dergelijke criminaliteit, werd grotendeels gebaseerd op afgenomen interviews wat logisch is aangezien er gepoogd werd een overzicht te geven van de problemen die politiediensten zelf ervaren. Die problemen zijn dus niet zomaar in literatuur terug te vinden. Wel was literatuur een bijkomende bron van informatie om bepaalde aangehaalde problemen verder uit te diepen of bepaalde wetgeving op te zoeken. Daarnaast werd ook literatuur geraadpleegd om passende een criminologische theorie te vinden die mogelijks verklaart waarom criminelen zo graag gebruik blijken te maken van bitcoins.

Bij de aanbevelingen en besluiten ten slotte wordt opnieuw vertrokken vanuit de interviews. Er worden enkele conclusies geformuleerd en op basis van de informatie die de respondenten meedeelden werd gepoogd enkele suggesties te formuleren om bitcoinonderzoek in de toekomst te verbeteren. De masterproef wordt afgesloten met het beantwoorden van de onderzoeksvragen en het formuleren van enkele algemene besluiten. Daarna volgt ook de bibliografie en de bijlagen.

2 Ethische principes: informed consent

Om de respondenten te informeren over de doelstellingen van de thesis en de rol die zij hierin spelen, werd gebruik gemaakt van een informed consent. Op basis hiervan verklaart de respondent dat er vrijwillig wordt deelgenomen aan het interview en dat er toestemming wordt verleend om geluidsopnames te maken. Via de informed consent geeft de respondent ook toestemming om zijn of haar antwoorden op anonieme wijze te bewaren, te verwerken en te rapporteren. Daarnaast wordt de respondent ook op de hoogte gebracht van het feit dat de deelname aan het onderzoek op elk ogenblik stop kan worden gezet zonder dat dit nadelige gevolgen met zich mee zou brengen. Er werd bovendien aan de respondenten meegedeeld dat er kon geweigerd worden bepaalde vragen te beantwoorden. Dit is belangrijk aangezien niemand gedwongen mag worden deel te nemen aan het onderzoek

(Decorte & Zaitch, 2010). In bijlage 4 kan de informed consent brief teruggevonden worden die aan de respondenten werd gegeven. Alle acht de respondenten waren bereid deze te ondertekenen. Hieronder wordt kort stilgestaan bij wat de anonimiteit die de respondenten werd gegarandeerd precies inhoudt. Er dient namelijk met verschillende zaken rekening te worden gehouden. (13)

2.1 Anonimiteit

Bij het verwerken van de interviews werden de respondenten volledig geanonimiseerd door hun naam te veranderen in een willekeurige letter. Hier dient benadrukt te worden dat louter een naamsverandering niet volstaat. Het was noodzakelijk de plaats van tewerkstelling van de respondent niet op te nemen in de masterproef omdat anders mogelijks zou kunnen worden afgeleid welke persoon er achter de respondent schuilgaat. Dit is ook de reden waarom de respondenten eerder vaag worden beschreven in de masterproef.

Een mogelijke bedreiging voor deze anonimiteit kan het feit zijn dat er gewerkt werd met een sneeuwbalsteekproef. Hierdoor zijn de meeste respondenten wel op de hoogte van de identiteit van de anderen aangezien zij deze zelf hebben aanbevolen. Het is dus niet evident een absolute anonimiteit te garanderen. Wel worden er zo veel mogelijk inspanningen geleverd om de identiteit van de respondent voor de lezer verborgen te houden (Leavy, 2014).

Via het ondertekenen van de informed consent gaf de respondent toestemming om geluidsopnames te maken. Op die manier konden de interviews achteraf worden getranscribeerd. De geluidsopnames dienden op een veilige plaats bewaard te worden omdat de anonimiteit van de respondenten anders in het gedrang kon komen (Decorte & Zaitch, 2010). Van zodra deze getranscribeerd waren, werden de geluidsopnames bijgevolg ook vernietigd. Op die manier is er enkel nog een geanonimiseerd transcript voorhanden waardoor aan de respondenten een exemplaar kon worden bezorgd. Hierdoor hadden zij de mogelijkheid om nogmaals te controleren of de zaken die verteld zijn geweest wel degelijk gepubliceerd mogen worden.

3 Situering binnen criminologisch paradigma

Daarnaast is het ook belangrijk aan te halen binnen welk criminologisch paradigma deze masterproef gesitueerd kan worden. Omdat elk paradigma zijn voordelen en beperkingen heeft, balanceert deze masterproef tussen verschillende paradigma's in.

Vooreerst heeft het klassieke paradigma in de criminologie een belangrijk aandeel in deze masterproef. Bij de bespreking van de probleemstelling werd al verwezen naar de momenteel lage opsporings- en vervolgingsgraad bij bitcoinonderzoek. Dit is mogelijks een van de redenen waarom bitcoins zo graag worden gebruikt door criminelen. Het pseudoanonieme karakter zorgt immers voor een lage pakkans waardoor criminelen weinig risico lopen om gevat te worden. Een oplossing (14) voor de heersende knelpunten bij het voeren van bitcoinonderzoek zou dus kunnen leiden tot een hogere opsporings- en vervolgingsgraad wat bijgevolg kan resulteren in meer afschrikking voor criminelen met een

daling van criminaliteit tot gevolg. Deze redenering is ook het uitgangspunt van het rechts realisme dat binnen het klassieke paradigma in de criminologie gesitueerd kan worden. Daarbij wordt uitgegaan van een rationeel mensbeeld waarbij iedereen beschikt over een vrije wil. De straffen moeten met andere woorden voor afschrikking zorgen waarbij snelle en effectieve straffen zullen leiden tot een daling van criminaliteit (Dupont, 2005). Natuurlijk zijn er ook situationele factoren die in rekening moeten worden gebracht. In dit opzicht schiet het rechts realisme dus enigszins tekort. Daarom kan niet alleen een beroep worden gedaan op het rechts realisme.

De uitsluitende focus die wordt uitgeoefend op de rol van de overheid is ook een van de kritieken die door het links realisme op het rechts realisme wordt geuit. Het links realisme kan gesitueerd worden binnen het kritisch realisme en argumenteert dat criminaliteit gepleegd wordt in bepaalde situaties waar er sprake is van deprivatie, en dat overheidsoptreden alleen niet voldoende is om hier verandering in te brengen. Dit oogt in eerste instantie minder relevant voor deze masterproef. Wanneer echter wat genuanceerder naar dit paradigma wordt gekeken, kan ook dit paradigma voor een stuk toegepast worden in deze masterproef. Zo is er binnen dit links realisme de ‘square of crime’ die door Young in de jaren 80 werd beschreven (Di Ronco, 2016). Deze stelt dat criminaliteit afhankelijk is van vier factoren: de politie en andere controlerende organen, de samenleving, de dader en het slachtoffer. Volgens Young zal elke verandering in een van deze factoren zorgen voor een verandering in de criminaliteitsfrequentie (Stenson & Cowell, 1991).

Figuur 1: Square of Crime (Carrabine, Iganski & Lee, 2004). (15)

Hoewel de nadruk van deze masterproef vooral zal liggen op de afwezigheid van opsporing en vervolging door politie en dus op het rechts realisme, moet men er zich dus ook bewust van zijn dat ook andere factoren een rol kunnen spelen. Denk maar aan het minder kwetsbaar maken van slachtoffers. Daarom dient ook het links realisme vermeld te worden.

4 Relevantie van de masterproef

Tot slot wordt ook even stilgestaan bij de relevantie van deze masterproef. Aangezien de masterproef een praktijkgericht onderzoek is, brengt dit logischerwijze praktische relevantie met zich mee (Decorte et al., 2016). In deze masterproef bestaat de praktische relevantie er enerzijds in aanbevelingen te doen ter optimalisatie van de huidige situatie. Door de problematiek nader te bestuderen en aanbevelingen te doen wordt gepoogd de huidige situatie te verbeteren en de opsporing en bestrijding van criminaliteit gepleegd met bitcoins te faciliteren. Anderzijds is de thesis vooral relevant om de problematische situatie onder de aandacht te brengen en beleidsmakers er bewust van te maken dat er dringend meer aandacht moet worden geschonken aan dit fenomeen.

Belangrijk om te vermelden is dat, hoewel het om een praktijkgericht onderzoek gaat, de masterproef ook in zekere mate theoretisch relevant is. Bitcoins werden vrij recent in het leven geroepen, namelijk in 2009. Het succes van deze virtuele munt zorgde ervoor dat veel inkt vloeide over de economische voordelen die ze met zich meebracht. Bitcoin werd gepromoot als zijnde een ideale investering. Helaas werd er nog maar weinig wetenschappelijke aandacht besteed aan de criminele mogelijkheden die bitcoins met zich

meebrengen waardoor op dit vlak nog steeds sprake is van een wetenschappelijke lacune. De theoretische relevantie van deze masterproef bestaat er dan ook in tegemoet te komen aan deze lacune

---

BEGRIPPENKADER

Het eerste deel van deze masterproef wordt gewijd aan de beschrijving van bitcoins. Om te begrijpen waarom bitcoins in verband worden gebracht met criminaliteit (hoofdstuk 1 van het empirisch luik) en waarom het voor politiediensten niet evident is hier mee om te gaan (hoofdstuk 2 van het empirisch luik), is het noodzakelijk de lezer wegwijs te maken in het bitcoin-betaalnetwerk. Om dit te realiseren worden dus eerste enkele cruciale begrippen nader toegelicht waarvoor hoofdzakelijk wetenschappelijke literatuur en internetbronnen werden geraadpleegd. De bedoeling is dat de lezer na het lezen van deze begripsbepaling een duidelijk beeld heeft over waarom, wanneer en hoe bitcoins zijn ontstaan, op welke manier het bitcoin-betaalnetwerk in elkaar zit en voor welke doeleinden bitcoins kunnen worden gebruikt. Dit deel is dus onontbeerlijk voor het verdere verloop van het empirisch onderzoek.

Samengevat

Hoewel de bitcoin als anonieme virtuele munt wordt gepromoot, kan uit hoofdstuk 1 geconcludeerd worden dat die anonimiteit toch niet helemaal is wat het lijkt. Satoshi Nakamoto mag de bitcoin dan wel in 2009 ontwikkeld hebben in de vorm van een virtuele, gedecentraliseerde munt als reactie op de bankencrisis, toch is er enigszins sprake van een openbaar karakter (Nakamoto, 2008). Het bitcoin-betaalnetwerk dat in hoofdstuk 2 aan bod kwam doet namelijk een beroep op een combinatie van cryptografie en een peer-to-peer-netwerk waarbij alle transacties in een openbaar logboek worden bijgehouden (Tasca, 2016). De term pseudoanoniem is dus meer van toepassing (Brito & Castillo, 2013).

De waarde van de munt is de laatste jaren enorm toegenomen en ook de betaalmogelijkheden met bitcoins breiden als maar verder uit. In hoofdstuk 2 werd een overzicht gegeven van verschillende mogelijkheden om bitcoins te spenderen. Zo kan er worden gespeculeerd met bitcoins alsook worden betaald met bitcoins via webshops (Illegems, 2014). Ze gebruiken voor de aankoop van een debet kaart of voor de betaling in bepaalde fysieke winkels behoort ook tot de mogelijkheden (Coinmap.org, 2017; de Munck, 2008). De betaalmogelijkheden die in dit deel werden besproken waren tot nog toe allemaal legaal. Helaas wordt vastgesteld dat bitcoins ook voor verschillende criminele doeleinden worden gebruikt (Europol, 2016b) . Hier zal in hoofdstuk 1 van het empirisch luik verder worden op gefocust.

EMPIRISCH LUIK

Nu de lezer via de begripsbepaling een algemeen inzicht heeft verworven in bitcoins en het bitcoin-betaalnetwerk, wordt in het empirisch luik overgegaan tot de verwerking van de interviews. In een eerste hoofdstuk wordt de aandacht gevestigd op de verschillende soorten criminaliteit die volgens de respondenten gepleegd worden met bitcoins. In een

tweede hoofdstuk wordt besproken hoe politiediensten deze criminaliteit momenteel trachten te bestrijden en welke problemen ze hierbij ervaren.

Samengevat

Met de programma's chainalysis en walletexplorer beschikken politiediensten over twee belangrijke tools die bitcoinonderzoek faciliteren. Deze geven een overzicht van de verschillende bitcointransacties die van en naar een bepaald bitcoinadres worden gestuurd. Het recente commerciële programma chainalysis blijkt de voorkeur te genieten omdat het politiediensten toelaat een visuele voorstelling te maken van deze verschillende transacties, iets wat bij het gratis programma walletexplorer niet het geval is.

Ondanks de terbeschikkingstelling van chainalysis zijn er nog heel wat problemen waarmee gekampt wordt bij het voeren van bitcoinonderzoek. Deze zijn volgens de respondenten enerzijds te wijten aan de complexiteit van het bitcoin-betaalnetwerk dat ervoor zorgt dat het niet evident is bitcointransacties op het spoor te komen en personen achter bitcoin wallets te identificeren. Ook daadwerkelijk toegang krijgen tot een bitcoin wallet blijkt geen sinecure. Verder zou de kennis over bitcoins binnen bepaalde units van de federale maar ook binnen de lokale politie te wensen overlaten waardoor CCU's vaak te hulp moeten schieten in diverse andere onderzoeken. CCU's beschikken momenteel over de meeste kennis inzake bitcoinonderzoek door de vele inspanningen die zij geleverd hebben om cybercriminaliteit gepleegd met bitcoins het hoofd te kunnen bieden. Mede door de overbevraging van CCU's maar ook omwille van financiële beperkingen die de toestroom van geschikte kandidaten naar deze Units belemmert, blijkt er vaak sprake te zijn van een onderbemanning. Dit zorgt bijgevolg voor heel wat werkdruk en werkachterstand.

Ook wanneer op grotere schaal gekeken wordt, kunnen er binnen het politie- en justitielandschap enkele gebeurtenissen geïdentificeerd worden die volgens de respondenten een weerslag hebben gehad op bitcoinonderzoek. Zo blijkt dat ondanks het arrest van het Hof van Cassatie dat Belgische justitie toelaat artikel 46bis van het wetboek van Strafvordering te gebruiken om rechtstreeks de medewerking te vorderen van internetondernemingen die communicatiediensten aanbieden en actief zijn op het Belgisch grondgebied, de internationale samenwerking nog steeds stroef verloopt. Dit komt volgens enkele respondenten mede doordat er op Europees niveau een gebrek is aan (68) definiëring wanneer het gaat over bitcoins en diensten die bitcoins aanbieden. Ook in België is er na vele inspanningen nog steeds geen duidelijke richtlijn omtrent de inbeslagname van bitcoins, wat erg vervelend is volgens de respondenten. Daarnaast heeft de vernietiging van de dataretentiewet van 30 juni 2013 ervoor gezorgd dat de termijn voor het bijhouden van data werd teruggeschroefd van twaalf naar zes maanden, wat natuurlijk gevolgen heeft voor bitcoinonderzoek waarbij data onontbeerlijk is om personen te identificeren. In het volgende hoofdstuk zal verder ingegaan worden op de mogelijkheden die er zijn om aan deze knelpunten tegemoet te komen.(69)

AANBEVELINGEN EN BESLUIT

Na de verschillende problemen te hebben besproken waarmee politiediensten kampen bij het voeren van bitcoinonderzoek, wordt in dit deel stilgestaan bij mogelijke handvaten zowel op nationaal als internationaal vlak voor de optimalisatie van bitcoinonderzoek. Omdat er reeds enkele initiatieven werden genomen, zullen deze eerst onder de aandacht worden gebracht. Daarna zullen aan de hand van de verklaringen van de respondenten alsook aan de hand van eigen bedenkingen enkele suggesties worden geformuleerd. Tot slot wordt teruggekoppeld naar de onderzoeksvragen die in de inleiding werden vermeld waarna enkele algemene besluiten aan bod komen.

HOOFDSTUK 1: LOPENDE INITIATIEVEN

Doorheen het afnemen van de interviews werd opgemerkt dat er momenteel enkele initiatieven genomen worden om de huidige situatie in verband met bitcoins en met cybercriminaliteit te verbeteren. Dit toont aan dat er binnen het politie- en justitielandschap stilaan meer aandacht wordt geschonken aan het bitcoin-betaalnetwerk en dat men er zich van bewust wordt dat er enkele zaken moeten worden ondernomen.

1 Initiatieven op Belgische bodem

Het samenwerkingsverband tussen het private programma chainalysis en de Belgische politie werd reeds besproken. Daarnaast zijn er nog enkele andere lopende initiatieven die de ambitie hebben de huidige problematiek het hoofd te bieden.

1.1 Werkgroep inbeslagname van bitcoins

Een eerste initiatief waar moet worden bij stilgestaan is de oprichting van een nationale werkgroep die zich specifiek toelegt op bitcoins en zich buigt over een procedure voor de inbeslagname en tegeldemaking ervan. Deze werkgroep bestaat uit leden van het Centraal Orgaan voor de Inbeslagneming en Verbeurdverklaring (COIV), het FCCU, het cybercrimenetwerk van het College van procureurs-generaal en tot slot de federale overheidsdienst Financiën (Kurstjens, 2017). Deze werkgroep heeft tot doel de problemen die momenteel heersen inzake de inbeslagname van bitcoins structureel aan te pakken.

Respondent X: […] “En dan een werkgroep politie en magistratuur erbij om vooral die procedure voor die inbeslagname.”(70)

1.2 Werkgroep ransomware

Naast de werkgroep inbeslagname van bitcoins, is er ook een werkgroep die zich focust op ransomware. Deze werkgroep is momenteel bezig met het opstellen van een standaard Proces Verbaal voor ransomware om de registratie door politiediensten te optimaliseren(17). De bedoeling van deze werkgroep is een nationale afstemming te creëren in de aanpak van ransomware (metrotime, 2017).

Respondent B: “Nu is er ook een vergadering, werkgroep met justitie om specifieke richtlijnen uit te schrijven over ransomeware he.”

1.3 Centrum voor Cybersecurity België

Voor een derde initiatief moet verwezen worden naar het Koninklijk Besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België. Hierin werd beslist een Centrum voor Cybersecurity op te richten onder gezag van de Eerste minister dat verantwoordelijk is voor het opstellen van het nationaal Cyber Security beleid (Centrum voor Cybersecurity, 2016b). Eind april 2017 werd er een actieplan tegen ransomware ontwikkeld maar gezien de recente verschijningsdatum is het plan nog niet publiekelijk te raadplegen.

1.4 Vrijwillige initiatieven

Tot slot werd ook vastgesteld dat er binnen het politiewezen een grote bereidheid is om vrijwillig enkele zaken te ondernemen met het oog op een optimalisatie. Zo verklaarde een respondent dat de dienst waar hij deel van uitmaakt voorziet in een kleine opleiding om mensen van de lokale en federale politie vertrouwd te maken met het bitcoin fenomeen. De opleiding bestaat uit een PowerPointpresentatie die op provinciaal niveau word gepresenteerd met de bedoeling onderzoekers toe te lichten wat bitcoins precies zijn en hoe hiermee moet worden omgegaan. Ook het gebruik van het programma chainalysis wordt erin besproken. De opleiding zorgt dus voor een basiskennis die ervoor zorgt dat de awareness omtrent het fenomeen binnen politie toeneemt en dat men ook weet welke stappen ondernomen moeten worden als men in aanraking komt met bitcoins(18). Ook een andere respondent verklaarde dat er binnen zijn dienst een soort van opleiding17 (-) werd gegeven aan RCCU's over het dark net en cryptocurrencies. Deze opleiding werd door de respondent ook verschillende keren aan Europese politiediensten gegeven(19).

Respondent D: "We zijn gestart met een project, een opleiding in mekaar gestoken over dark net en over currencies. Die hebben wij al een keer of drie gaan geven in buitenland, voor Europese politiediensten. En nu gaan we dat uiteindelijk hier in België ook doen. We hebben dat al gedaan vorig jaar voor de RCCU's, maar nu gaan we dat verderzetten in een soort trainer-trainer optiek."

"Respondent G: Wij hebben een paar weken geleden een opleiding voorzien voor de mensen van de federale en lokale politie. Een basisopleiding waarin elke onderzoeker een beetje uitgelegd wordt wat dat bitcoins zijn en hoe dat het werkt."

2 Internationale initiatieven

Net zoals er in België een samenwerkingsverband is met het programma chainalysis, is dit ook op Europees niveau het geval. Er werd al stilgestaan bij het gebruik van chainalysis door Europol's Europees Cybercrime Center. Daarnaast zijn er nog andere belangrijke initiatieven op internationaal niveau, namelijk Cyber Europe en "nomoreransom".

2.1 Cyber Europe 2016

Een initiatief op Europees niveau is Cyber Europe 2016 waarbij de mogelijkheid wordt geboden aan cybersecurity centra en aan operationele cyberdiensten van de Europese lidstaten om te oefenen hoe met crisissituaties moet worden omgegaan en hoe er moet worden samengewerkt. Men is zich dus bewust dat samenwerking en informatie-uitwisseling erg belangrijk is en probeert aan de hand van dit initiatief de samenwerking te bevorderen. Ook het Centrum voor Cybersecurity België neemt hieraan deel. Dit initiatief is

dus niet specifiek gericht op de bitcoinproblematiek, maar kan er wel mede toe bijdragen dat informatie-uitwisseling in de toekomst vlotter verloopt (Centrum voor Cybersecurity, 2016a).

2.2 “Nomoreransom”

Ook op het gebied van ransomware kwam er een internationaal initiatief tot stand dat nomoreransom (no-more-ransom) heet. Dit initiatief ontstond omdat men besefte dat er steeds meer (-)mensen slachtoffer worden van ransomware en heeft zich dan ook toegelegd op deze problematiek. Het is een samenwerkingsverband tussen de National High Tech Crime Unit van Nederland, Europol’s Cybercrime Centre en twee cyber security bedrijven (Kaspersky Lab en Intel Security). Het is dus een publieke en private samenwerking. Dit is noodzakelijk omdat politie alleen momenteel niet in staat is dit fenomeen aan te pakken (nomoreransom.org, 2017).

Via de website www.nomoreransom.org wordt gepoogd zo veel mogelijk informatie en kennis te verspreiden betreffende ransomware en mensen te leren hoe ze kunnen voorkomen zelf het slachtoffer te worden. De website stelt verschillende tools ter beschikking die kunnen gebruikt worden door slachtoffers om mogelijks hun computerbestanden te recupereren. Deze tools werken natuurlijk niet altijd en niet voor elke vorm van ransomware, maar kunnen een redmiddel zijn voor bepaalde slachtoffers. Op die manier zullen de criminelen ook minder bitcoins verwerven via de ransomware (nomoreransom.org, 2017).

Respondent B: “En alle slachtoffers kunnen dan ook een decryptie vinden op de website nomorerandsomeware.org.”(73)

HOOFDSTUK 2: SUGGESTIES

Hoewel verschillende problemen werden aangekaart door de respondenten, blijken huidige initiatieven aan enkele van deze problemen tegemoet te komen. Zo kunnen de opleidingen en presentaties die vrijwillig door enkele respondenten worden gegeven ervoor zorgen dat de kennis inzake bitcoins binnen het politiewezen toeneemt. De werkgroep ransomware kan er daarnaast voor zorgen dat er meer eenduidigheid is betreffende de registratie van feiten waarbij bitcoins betrokken zijn. Ook de inbeslagname wordt momenteel nader bekeken door de werkgroep inbeslagname van bitcoins. Er is met andere woorden al het een en ander in beweging. Toch blijken sommige problemen nog onvoldoende aandacht te krijgen. Hieronder worden dan ook enkele handvaten aangereikt ter optimalisatie van bitcoinonderzoek.

1 Internationale veranderingen?

Gezien het internationaal karakter van de bitcoinproblematiek zou in eerste instantie op internationaal niveau enkele veranderingen moeten worden doorgevoerd. Een aanpak op nationaal niveau is onvoldoende om de criminaliteit met bitcoins te kunnen indijken. Dit wegens het gedecentraliseerde karakter van bitcoins en de grenzeloosheid van het internet (De belgische Senaat, 2013). Op internationaal niveau blijkt er voornamelijk nood te zijn aan wettelijke bepalingen en regelgeving.

1.1 Duidelijke wetsbepalingen ontwikkelen

Zoals respondent X tijdens het interview aanhaalde zou het een goede zaak zijn om bijvoorbeeld op Europees niveau eens te gaan bepalen hoe overheden bitcoins en bitcoin exchangers moeten benaderen en welke wetgeving al dan niet van toepassing is. Door deze een duidelijke definiëring te geven zou er geen discussie meer mogelijk zijn over welke wetgeving al dan niet van toepassing is. In het arrest van het Europees Hof van Justitie van 22 oktober 2015 oordeelde het Hof van Justitie dat bitcoin exchangers vrijgesteld zijn aan de btw-richtlijnen omdat deze door partijen als officieel betaalmiddel worden gebruikt. Door gebrek aan definiëring van bitcoins en bitcoin exchangers wordt dit arrest op verschillende manieren geïnterpreteerd waardoor sommigen van oordeel zijn dat het Hof bitcoins als officieel betaalmiddel erkend heeft.

Wanneer dit arrest kritisch wordt bekeken kan hier van een gemiste kans gesproken worden die het Hof de mogelijkheid bood om duidelijkheid te scheppen omtrent bitcoins en de status ervan. In het (74) arrest werd geoordeeld dat de bitcoin exchangers vrijgesteld worden van de btw-richtlijnen omdat de wetgeving hieromtrent anders zou worden uitgehold. Het hof nam echter geen expliciet standpunt in over het al dan niet officiële karakter van bitcoins. Het stelde alleen dat er partijen zijn die het als officieel betaalmiddel gebruiken. Op Europees niveau zou er dus veel meer duidelijkheid moeten komen om te voorkomen dat deze rechtspraak op verschillende manieren wordt geïnterpreteerd.

1.2 Know your customer principe doorvoeren

Hoewel er geen centrale bank of autoriteit is die instaat voor het beheer van bitcoins, zijn er toch enkele mogelijkheden om gebruikers van bitcoins zo veel mogelijk te kunnen identificeren. Zo zou het een goede zaak zijn mocht er op internationaal niveau de verplichting worden opgelegd aan bitcoin exchangers om gedetailleerde informatie bij te houden over de gebruikers die bitcoins komen omzetten in andere valuta, of omgekeerd. Dit werd ook al aangekaart door de Europese Commissie (Europees Parlement en de Raad, 2005). Een mogelijkheid zou kunnen zijn een foto van de identiteitskaart te vragen en deze vervolgens te controleren op geldigheid. Op die manier zouden politiediensten eenvoudiger de identiteit van criminelen kunnen gaan bepalen doordat systematisch bij bitcoin exchangers ten rade kan worden gegaan.

Gezien het internationaal karakter van bitcoins is dit natuurlijk niet evident. Om daadwerkelijk efficiënt te zijn zou elk land zijn exchangers moeten verplichten de gegevens van gebruikers te registreren en bij te houden. Deze maatregel uitsluitend op Europees niveau doorvoeren volstaat dus niet omdat anders het risico bestaat dat criminelen gewoon die landen opzoeken waarin exchangers niet aan strikte regels onderworpen worden en alsnog pseudoanoniem door het leven kunnen gaan. In de criminologie wordt dit ook wel het “waterbedeffect” genoemd. Dit wil zeggen dat druk op een bepaalde plaats inderdaad zal leiden tot een daling van criminaliteit op die plaats, maar zal stijgen op die plaatsen waar geen druk wordt uitgeoefend. Hier dient dus zeker rekening mee te worden gehouden (Bruinsma, Bernasco & Elffers, 2010).

Daarnaast zal er ook controle moeten worden uitgeoefend op de exchangers om na te gaan of ze zich aan de regels houden. Frequente controles en hoge sancties zouden een mogelijke manier kunnen zijn om ervoor te zorgen dat exchangers de regelgeving zullen respecteren en toepassen. Bij gebrek aan controles en sancties kan het daarentegen aanlokkelijk zijn voor exchangers om de regels te overtreden omdat deze bijvoorbeeld de administratieve last niet kunnen opvangen en (75)

daardoor opportuniteiten voor crimineel misbruik niet kunnen uitsluiten. Het spreekt dus voor zich dat het niet eenvoudig is om elk land hiertoe aan te zetten, maar hoe meer landen hiertoe bereid zijn, des te minder gelegenheden criminelen hebben om hun identiteit te maskeren.

Een ander obstakel zou het feit kunnen zijn dat niet elke crimineel een exchanger raadpleegt waardoor er alsnog pseudoanoniem kan worden gehandeld. Toch zou een dergelijke wetgeving een stap in de goede richting zijn om zo veel mogelijk te voorkomen dat bitcoin exchangers de drijvende kracht zijn achter criminelen.

2 Nationale veranderingen?

Naast het internationale aspect werd door de respondenten ook vaak verwezen naar enkele problemen die op nationaal niveau kunnen gesitueerd worden. Zo blijken het gebrek aan kennis binnen verschillende diensten van de federale en lokale politie, en de onderbemanning van CCU's belangrijke knelpunt te zijn. Voor deze problemen kunnen onderstaande suggesties geformuleerd worden.

2.1 Gebrek aan kennis binnen politiediensten met verschillende gevolgen

Doorheen het schrijven van deze masterproef werd duidelijk dat bitcoins erg complex zijn en dat het geen sinecure is alle aspecten en werkingsmechanismen van het hele systeem te begrijpen. Een eerste probleem is dan ook het feit dat er erg weinig personen zijn binnen het politiewezen, zowel op lokaal als federaal niveau, die grondige kennis hebben over de wijze waarop bitcoinonderzoek succesvol kan worden afgerond. Op lokaal niveau vormt dit vooral een probleem betreffende de inbeslagname van bitcoins, omdat inspecteurs van de lokale politie bitcoin wallets over het hoofd kunnen zien bij huiszoekingen. Op federaal niveau zorgt het gebrek aan kennis vooral voor een overbevraging van de CCU's die momenteel onderhevig zijn aan capaciteitsproblemen wat uiteraard een negatief effect heeft op de werkachterstand. Dit leidt als het ware tot een soort domino-effect waardoor de noodzaak voor optimalisatie toeneemt. Alternatieven voor het systematisch belasten van de CCU's met bitcoinonderzoek worden hieronder besproken. Elk van deze drie afzonderlijk zou mogelijks al grote veranderingen met zich meebrengen, maar een combinatie ervan zou natuurlijk het meest effectief zijn.(76)

2.1.1 Specialisatie binnen elke sectie als optie?

Een eerste mogelijkheid om tegemoet te komen aan dit probleem zou erin kunnen bestaan binnen elke sectie van de federale politie voldoende kennis te genereren over de wijze waarop bitcoinonderzoek moet worden gevoerd zodat er niet meer systematisch een beroep moet worden gedaan op CCU's. Deze Units hebben inspanningen geleverd om dit

probleem te kunnen beheersen waardoor de vraag gesteld kan worden of dergelijke inspanningen niet gelijkmatig zouden verdeeld moeten worden. De reden waarom vooral op federaal niveau specialisatie nodig is, is omdat criminaliteit gepleegd met bitcoins vaak een internationaal, georganiseerd karakter heeft wat onder de bevoegdheid van de federale politie valt (Van den Wyngaert, 2014).

Natuurlijk kan men zich in dit opzicht afvragen of er van elke functie op federaal niveau binnen de politieorganisatie verwacht kan worden op de hoogte te zijn van alle nieuwe ontwikkelingen? Deze masterproef handelde over bitcoins, maar er zijn ongetwijfeld talrijke nieuwe ontwikkelingen op allerlei gebieden wat zeker in het achterhoofd moet worden gehouden. Daarnaast zal er moeten geïnvesteerd worden in tijd en middelen om er voor te zorgen dat deze mensen in staat zijn degelijk bitcoinonderzoek te voeren omdat de materie erg complex is.

Toch zou dergelijke specialisatie een goede zaak zijn omdat niet alleen het gebruik van bitcoins toeneemt, maar ook het gebruik van de blockchain technologie. De blockchain blijkt zich niet uitsluitend voor het bitcoin-betaalnetwerk te lenen maar ook voor diverse andere doeleinden (Canada NewsWire, 2016). Zo blijkt deze ook stilaan zijn intrede te doen in de financiële sector (MENA Report, 2016). Het zal dus waarschijnlijk een kwestie van tijd zijn vooraleer de blockchain technologie op grotere schaal wordt gebruikt, wat opnieuw gevolgen kan hebben voor het politiewezen.

2.1.2 Gespecialiseerde dienst binnen het politiewezen?

Een andere mogelijkheid zou kunnen zijn om net zoals in Nederland binnen de federale politie een gespecialiseerde dienst op te richten die zich uitsluitend kan focussen op dergelijke bitcoinonderzoeken. Zo verklaarde respondent X dat er in Nederland drie teams werden opgericht die zich uitsluitend focussen op ransomware.(77)

Respondent X over High Tech Crime Unit (Nederland): “Die mannen hebben daar drie teams van 90 man om daar op te werken, op ransomware weliswaar en dan bitcoin erbij. Hallucinant!”

Dergelijke initiatieven zouden ook op Belgische bodem kunnen worden genomen. Om dit te realiseren zullen natuurlijk personen met het geschikte profiel moeten worden aangeworven. Aangezien zowel respondent X alsook Catherine De Bolle verklaarden dat het loon bij politie beperkt is, kan dit een van de redenen zijn waarom er tot op heden beperkte specialisatie is binnen de politie. Om een gespecialiseerde dienst op te richten en om personen warm te maken om zich hiervoor te engageren zou er dus vooreerst moeten worden overwogen de lonen voor dergelijke personen te verhogen om te vermijden dat zij een job in de private sector verkiezen boven een job bij de politie.

Dit blijkt natuurlijk makkelijker gezegd dan gedaan aangezien er op tal van vlakken besparingen zijn. Een gespecialiseerde dienst oprichten zou dus een grote hap uit het budget van politie zijn. Anderzijds kan geargumenteerd worden dat de politie door middel van deze dienst waarschijnlijk meer in staat zal zijn bitcoinonderzoek tot een goed eind te brengen

wat zich vertaalt in meer gelegenheden tot inbeslagname en verbeurdverklaring van bitcoins en zo dus opnieuw inkomsten voor de Belgische Staat betekent.

2.1.3 Samenwerking met private actoren als extra piste?

Er mag dan wel sprake zijn van criminaliteit, waarom wordt er niet veel vaker een beroep gedaan op private ondernemingen? Steven Wilson, hoofd van Europol's Europees Cybercrime Center benadrukte reeds dat samenwerking met andere actoren cruciaal is om cybercriminaliteit te bestrijden:

"Close working co-operation between law enforcement and industry is the only way to successfully tackle the significant threat from cybercrime (Europol, 2016a)."

De samenwerking met chainalysis en nomoreransom kunnen beschouwd worden als een good practices. Het zou een goede zaak zijn mochten dergelijke samenwerkingsverbanden in de toekomst toenemen. Zo verklaarde onderzoeksrechter Philippe van Linthout bijvoorbeeld dat de verschillende universiteiten in België alsook de ingenieurs en mensen die gespecialiseerd zijn in (78) encryptie erg veel potentieel in zich hebben. Als het van hem afhangt zou hier een beroep worden op gedaan voor het ontwikkelen van tools in de strijd tegen cybercriminaliteit (Leestmans, 2015).

2.2 Uitbreiden van Computer Crime Units

Er kan daarnaast geopperd worden dat de CCU's dringend zouden moeten worden uitgebreid. Zelfs als bitcoinonderzoek in de toekomst niet meer systematisch voortvloeit naar dergelijke Units, dan nog blijken deze onderbemand te zijn. De argumenten die hier aangehaald kunnen worden zijn dezelfde als deze voor de oprichting van een gespecialiseerde dienst. Zo zal er inderdaad geïnvesteerd moeten worden om deze Units uit te breiden, maar dit kan er bijgevolg voor zorgen dat er meer dossiers tot een goed einde worden gebracht. Via inbeslagnames en verbeurdverklaringen kan dit dan weer leiden tot opbrengsten voor de Belgische Staat.

Er dient natuurlijk niet uitsluitend in termen van winstbejag te worden gedacht. Door meer capaciteit in te zetten op dergelijke vormen van criminaliteit zal de pakkans stijgen wat voor een afschrikkend effect kan zorgen voor criminelen.

2.3 Awareness creëren bij de burger

Tot slot is het volgens respondent D ook belangrijk de burger op de hoogte te brengen van de risico's die bitcoins met zich mee kunnen brengen om ervoor te zorgen dat ze zich bijvoorbeeld niet laten innemen door bepaalde e-mails die het ransomware virus verspreiden.

Respondent D: "ze moeten een beetje awareness geven aan de mensen die er werken dat ze niet op alles gaan klikken en dergelijke"

Daarnaast moeten mensen gestimuleerd worden om zo veel mogelijk een back-up te maken van hun gegevens. Indien er dan toch iets mis dreigt te lopen en de computer besmet wordt, kan hierop worden teruggevallen en wordt voorkomen dat criminelen hun buit binnenhalen.

Belangrijk is ook om mensen te aan te sporen om zo veel mogelijk melding te maken aan de politie om het dark number zo laag mogelijk te houden.

3 Samengevat

De suggesties die hierboven werden opgesomd zijn zeer divers, wat noodzakelijk is om criminaliteit te bestrijden. Zo zijn er ten eerste aanbevelingen die inwerken op de redenen waarom (79) daders gebruik maken van bitcoins, namelijk de pseudoanonimiteit. Door verschillende landen aan te moedigen de bitcoinexchangers op hun grondgebied te verplichten gegevens bij te houden van hun gebruikers, kunnen daders mogelijks afzien van de keuze om beroep te doen op bitcoins voor hun criminele daden. Ten tweede werden ook suggesties gedaan die ervoor moeten zorgen dat personen minder kwetsbaar zijn om slachtoffer te worden, namelijk door het creëren van awareness. Hier is het aandeel van het links realisme en de square of crime terug te vinden, die werden besproken bij methodologie en theorie bij aanvang van deze masterproef.

Tot slot werden ook heel wat aanbevelingen gedaan die ervoor zorgen dat politie en justitie veel meer controle kunnen uitoefenen. Dit toont dan weer de dominantie aan van het rechts realisme. De uitbreiding van CCU's, specialisatie binnen elke sectie van politie, de oprichting van een gespecialiseerde dienst, samenwerking met private organisaties en het opstellen van duidelijke wetsbepalingen kunnen in deze categorie worden ondergebracht.

Met andere woorden, door de vooropgestelde aanbevelingen door te voeren zou de overheid veel meer mogelijkheden hebben om daders te vervolgen. Dit in combinatie met het verlies van pseudoanonimiteit zou afschrikkend kunnen werken voor daders om criminaliteit te plegen met bitcoins. Tot slot zouden er ook veel minder kwetsbare doelwitten aanwezig. Een combinatie van al deze factoren zou ervoor kunnen zorgen dat criminaliteit gepleegd met bitcoins afneemt.

Inhoudstafel