Uit de schaduw

Perspectieven voor wetenschappelijk onderzoek naar dark markets

Verburgh, Thijmen; Smits, Eefje; van Wegberg, Rolf

DOI
10.5553/JV/016758502018044005006

Publication date
2018

Document Version
Final published version

Published in
Justitiele Verkenningen

Citation (APA)
Verburgh, T., Smits, E., & van Wegberg, R. (2018). Uit de schaduw: Perspectieven voor wetenschappelijk onderzoek naar dark markets. *Justitiele Verkenningen*, *44*(5), 68-82.
https://doi.org/10.5553/JV/016758502018044005006

Uit de schaduw

Perspectieven voor wetenschappelijk onderzoek naar dark markets

Thijmen Verburgh, Eefje Smits en Rolf van Wegberg*

Digitale criminaliteit is een groeiende vorm van criminaliteit en heeft een grote maatschappelijke impact: van onbereikbare bankwebsites die bezwijken onder DDoS-aanvallen tot drugshandel via anonieme markten op het *dark web*. Een vorm van digitale criminaliteit zijn de zogeheten *dark markets*, een plek op het *dark web* waar online en anoniem wordt gehandeld in diverse goederen en diensten. In dit artikel laten we zien zien hoe op *dark markets* het samenspel van technische en sociale aspecten online anonieme handel in wapens, drugs en cybercrimegereedschap, zoals DDoS-aanvallen, mogelijk maakt. Sinds het ontstaan van *dark markets* wordt er onderzoek gedaan naar deze markplaatsen en de onderliggende mechanismen. Vooralsnog blijven veel kansen voor wetenschappers onbenut. Een nog grotendeels onbekend terrein is bijvoorbeeld het onderzoek naar politie-interventies zoals operatie Bayonet, waarbij twee van de grootste dark markets door de FBI en de Nederlandse politie gesloten werden. In deze bijdrage gaat de aandacht vooral uit naar verschillende manieren van onderzoek doen naar *dark markets*. Allereerst kijken we naar de belangrijkste kenmerken van *dark markets*. Daarna staan we stil bij het bestaande onderzoek naar *dark markets* om vervolgens in te gaan op de potentiële kansen voor onderzoek naar politie-interventies op *dark markets*.

* T. Verburgh MSc is als onderzoeker verbonden aan TNO. E. Smits MSc is werkzaam als onderzoeker bij TNO. R. van Wegberg MSc is als onderzoeker verbonden aan TNO en de Technische Universiteit Delft.

doi: 10.5553/JV/016758502018044005006

Figuur 1 **Dark markets en dark web ten opzichte van het internet**

Dark markets: definitie en karakteristieken

Om het concept *dark markets* beter te kunnen duiden, is het van belang om te weten hoe *dark markets* zich verhouden tot het gehele world wide web. Het gehele web is daarbij alle content die beschikbaar is via internetbrowsers. Binnen deze content vallen twee categorieën te onderscheiden: het *surface web* en het *deep web*. Content van sites die beschikbaar is via zoekmachines, zoals Google, vallen onder de categorie *surface web*. Dat wat niet doorzoekbaar is middels zoekmachines, valt onder de categorie *deep web*. Een klein deel van de content op het *deep web* is enkel toegankelijk wanneer gebruik wordt gemaakt van een speciaal anonimiseringsprotocol.[1] Dit gedeelte wordt het *dark web* genoemd (Barratt & Aldridge 2016). Een *dark market* is een ontmoetingsplaats of handelssite op het zogenoemde *dark web* waar gebruikers virtueel bijeenkomen om producten en/of diensten te kopen en/of verkopen.

1 Technologieën die het mogelijk maken om anoniem op het web te surfen en anonieme sites te hosten worden ook wel aangeduid met de term anonimiseringsprotocollen/darknets.

doi: 10.5553/JV/016758502018044005006

Het befaamde Silk Road 1.0[2] was niet de allereerste *dark market*[3], maar door de professionaliteit van de site, de positieve feedback van gebruikers en de media-aandacht werd Silk Road 1.0 al snel de grootste *dark market* (Buxton & Bingham 2015). Als gevolg van een grootschalige politieactie werd Silk Road 1.0 na ongeveer twee jaar gesloten. Al spoedig echter ontstonden nieuwe markten. De goederen die op *dark markets* worden aangeboden, zijn meestal illegaal van aard, waarbij drugs het meest worden verhandeld (Soska & Christin 2015). Tegenwoordig is de gemiddelde *dark market* groter dan Silk Road 1.0 was en wordt bij de grootste *dark markets* meer dan $ 200.000 per dag omgezet (Soska & Christin 2015).
Aldridge en Décary-Hétu (2016) stellen dat *dark markets* niet zozeer een nieuwe technologie hebben ontwikkeld, maar dat ze enkele bestaande veiligheidsmaatregelen hebben gecombineerd. Het gaat daarbij om vier onderliggende veiligheidsmaatregelen die *dark markets* mogelijk maken: anonimiseringsprotocollen, cryptocurrencies, *escrow* en *review*systemen, begrippen die hieronder nader worden uitgelegd. Aan deze veiligheidsmaatregelen liggen twee faciliterende principes ten grondslag die de kracht van het businessmodel van *dark markets* bepalen: anonimiteit en vertrouwen (Mounteney e.a. 2016; Cox 2016; Aldrigde & Décary-Hétu 2016; Tzanetakis e.a. 2016). Anonimiteit en vertrouwen zorgen ervoor dat *dark markets* bestaansrecht hebben en bestand zijn tegen externe invloeden van bijvoorbeeld politie, maar ook van overige externe actoren zoals rivaliserende sites die graag de concurrentie dwars zouden willen zitten. In de volgende paragrafen laten we zien op welke wijze anonimiteit en vertrouwen op dark markets worden gefaciliteerd.

Anonimiteit

Aangezien de meeste producten illegaal zijn, is anonimiteit van groot belang op een *dark market*. Hieronder wordt ingegaan op de verschillende technieken en voorzieningen die deze anonimiteit bevorderen: anonimiseringsprotocollen, cryptocurrencies, data-

2 Silk road 1.0 werd in 2011 opgericht en in 2013 gesloten door de FBI. Silk Road 1.0 staat bekend als de eerste moderne dark market, waar o.a. bitcoin gebruikt werd.
3 Andere initiatieven waren The Drugstore, AFOYI, BBS, TLG en OVDB (Buxton & Bingham, 2015).

doi: 10.5553/JV/016758502018044005006

encryptie en het gebruikmaken van post- en pakketdiensten. Met behulp van deze vier maatregelen worden vier belangrijke onderdelen afgedekt: 'ontmoeten', 'betalen', 'communiceren' en 'bezorgen'.

Ontmoeten

Technologieën die het mogelijk maken om anoniem op het web te surfen en anonieme sites te hosten worden ook wel aangeduid met de term anonimiseringsprotocollen/*darknets*. Deze technologie stelt gebruikers in staat om een ontmoetingsplek te creëren waarbij elke partij anoniem is; zowel de koper, verkoper als de eigenaar van de site. Het meest bekende en meest gebruikte anonimiseringsprotocol[4] dateert uit 2002 en wordt The Onion Router (TOR) genoemd. Er zijn echter ook andere protocollen beschikbaar zoals I2P & FREENET. In het geval van TOR wordt een speciale browser gebruikt, die openbaar beschikbaar is.[5]

Betalen

Silk Road 1.0 liet een duidelijke ontwikkeling zien ten opzichte van eerdere online drugsmarkten. Daar waar de voorgaande markten allemaal gebruikmaakten van het anonimiseringsprotocol TOR, was Silk Road 1.0 de eerste site die TOR combineerde met het gebruik van de cryptocurrency bitcoin. Dit maakte het mogelijk om tamelijk anoniem betalingen te verrichten, wat een enorme sprong voorwaarts betekende (Buxton & Bingham 2015). Bitcoin is op dit moment de populairste cryptocurrency voor *dark markets* (Matanovic 2017). Een andere cryptocurrency die ook regelmatig wordt gebruikt is Monero (Matanovic 2017).

Communiceren

Een andere techniek die wordt gebruikt op *dark markets* en die de anonimiteit vergroot, is Pretty Good Privacy (PGP) (Buxton & Bingham 2015). PGP geeft gebruikers de mogelijkheid om bestanden of teksten

4 Het TOR-protocol geleidt het internetverkeer langs meerdere TOR nodes en versleutelt het netwerkverkeer daartussen waardoor het originele IP-adres niet geopenbaard wordt (Dingledine, Mathewson & Syverson, 2004). Hierdoor maakt TOR het mogelijk om te surfen op internet zonder het openbaren van het IP-adres van de gebruikte computer.

5 Zie www.torproject.org

doi: 10.5553/JV/016758502018044005006

te versleutelen, zodat deze enkel door de zender en ontvanger kunnen worden gelezen. Door PGP op *dark markets* te gebruiken weten criminelen zeker dat de politie of administrators niet bij de inhoud van hun berichten kunnen, zoals het afleveradres van het pakketje. Omdat de berichten via PGP door slechts één entiteit kunnen worden ontsleuteld, wordt PGP ook gebruikt als een soort identiteitsbewijs. Door te controleren of iemand op verschillende momenten dezelfde PGP-gegevens gebruikt, kan bepaald worden of je contact hebt met dezelfde persoon.

Bezorgen

Gelet op het postgeheim dat in veel landen geldt, kunnen illegale goederen per post anoniem worden verstuurd. Het postsysteem stelt verkopers in staat een grotere klantenkring te bereiken en hun afzetmarkt te vergroten. Ook kunnen verkopers hun producten leveren op lastig te bereiken locaties. Bovendien werkt het postsysteem risicoreducerend aangezien er geen ontmoetingen plaatsvinden tussen koper en verkoper, waardoor geweld vermeden kan worden (Van Hout & Bingham 2013). Postverzending heeft echter ook zwakheden: pakketjes kunnen worden onderschept en autoriteiten controleren bij de landsgrenzen scherp op illegale goederen (Aldridge & Decary-Hetu 2016; Aldridge & Askew 2017).

Vertrouwen

Voor *dark markets* geldt dat iedereen anoniem is. Daarom dienen er veiligheidsmaatregelen te worden ontwikkeld om elkaar desondanks te kunnen vertrouwen. Anonimiteit leidt immers tot een paradijs voor oplichters, die dan ook in significante mate aanwezig zijn op *dark markets*. Voordat criminelen onderling handel drijven moet er enige vorm van vertrouwen bestaan in de markt, andere gebruikers op de markt en de financiële afwikkeling. De onderdelen *escrow, finalize early* en het *review*systeem (zie hieronder) hebben invloed op aspecten als 'bescherming' en 'reputatie', beide van groot belang voor het vertrouwen in de markt.

doi: 10.5553/JV/016758502018044005006

Bescherming

Bij de koop en verkoop van goederen is een systeem nodig om het vertrouwen tussen koper en verkoper te versterken. De verkoper wil erop kunnen vertrouwen dat hij het geld krijgt, de koper wil erop kunnen vertrouwen dat hij het bestelde product krijgt. Er zijn twee soorten bescherming mogelijk die het vertrouwen vergroten, namelijk *escrow* en *finalize early* (*FE*). *Escrow* biedt bescherming voor de koper doordat de betaling van de koper door de marktplaats achtergehouden wordt totdat de goederen in goede orde ontvangen zijn. Wanneer dit het geval is, wordt het bedrag van de koop overgemaakt naar de verkoper. *Finalize early* is een bescherming voor verkopers waarbij de verkoper de garantie krijgt dat hij uitbetaald wordt. Hij krijgt namelijk uitbetaald voordat de koper de producten in ontvangst heeft genomen. Bij beide systemen is de marktplaats de 'objectieve' derde partij die bemiddelt wanneer onenigheid bestaat tussen de koper en verkoper (Aldridge & Askew 2017; Afilipoaie & Shortis 2015). Het geld is in beheer van de marktplaats, wat betekent dat je als koper of verkoper niet meer elke individuele 'zakenrelatie' hoeft te vertrouwen. Je hoeft alleen maar één marktplaats te vertrouwen om garanties te krijgen.

Reputatie

Een andere manier waarop het vertrouwen op *dark markets* wordt vergroot, is door gebruik te maken van een *review*systeem dat vergelijkbaar is met de beoordelingssystemen van legale verkoopwebsites als Ebay en Amazon. Het *review*systeem is opgezet om intrinsieke risico's op oplichting te verminderen (Décary-Hétu & Dupont 2013; Holt e.a. 2015). De basis van het systeem is dat er vertrouwen wordt gecreëerd door informatiedeling. Dit betreft natuurlijk niet data die de anonimiteit in geding brengt, zoals geo-locatie. Het gaat juist om publieke informatiedeling aangezien de community toegang moet hebben tot de informatie voordat het vertrouwen kan worden gecreëerd. Er wordt gebruikgemaakt van een *review*systeem waar zowel de verkopers als de kopers kunnen worden beoordeeld, waardoor het vertrouwen groeit.

doi: 10.5553/JV/016758502018044005006

Onderzoek naar dark markets

De grote toegankelijkheid, het mondiale karakter en het solide businessmodel van *dark markets* zorgen ervoor dat interventies van opsporingsinstanties niet eenvoudig uit te voeren zijn. Het achterhalen van de locatie van een server of de identiteit van een crimineel is een grote uitdaging. Wetenschappelijk onderzoekers ondervinden minder hinder van deze barrières, omdat het voor onderzoekers niet gaat om het achterhalen van een specifieke identiteit of locatie. Voor onderzoekers gaat het om trends en ontwikkelingen, waarbij het gebruik van afgeleiden voldoende is. De omvang van een marktplaats wordt bijvoorbeeld geschat op basis van het aantal *listings* (advertenties) dat een *dark market* heeft. Daarnaast kunnen onderzoekers in verschillende gevallen juist profiteren van het feit dat *dark markets* een businessmodel hebben waarbij anonimiteit en vertrouwen centraal staan. Omdat niemand elkaar kent, noch weet waar iemand zich bevindt, vindt veel van de communicatie, en dus informatie-uitwisseling, plaats op de platformen zelf. Alle interactie met de site of elkaar zijn mogelijke datapunten die gebruikt kunnen worden voor onderzoek. Hierbij moet men zich wel realiseren dat criminelen buiten de platformen om contact kunnen hebben of elkaar fysiek kunnen ontmoeten, waardoor er ook een *dark number*[6] is.
Middels het bestuderen van *dark market*s kunnen zowel criminele fenomenen alsook interventies worden onderzocht. Bij fenomeenonderzoek kan bijvoorbeeld inzicht worden verschaft in de criminele werkwijze en trends die zichtbaar zijn op een *dark market*. Bij onderzoek naar interventies kijkt men juist naar de impact van een interventie op het ecosysteem van de *dark market*. Voor beide typen research geldt dat dit zowel kwalitatief als kwantitatief onderzoek kan betreffen.

Fenomeenonderzoek dark markets

Fenomeenonderzoek is gericht op een misdaadveld of criminele markt, waarbij wordt gekeken naar aard, omvang, trends en ontwikkelingen. Onderzoeksgegevens kunnen worden vergaard door middel van observatie, participatie of via interventies. Bij data uit observatie worden onderzoeksgegevens vaak met behulp van *scraping*

6 Aantal criminelen dat buiten de steekproef valt en daardoor de conclusies van het onderzoek kan beïnvloeden.

doi: 10.5553/JV/016758502018044005006

en *crawling* vergaard. *Scraping* en *crawling* zijn technieken waarmee het mogelijk is op een geautomatiseerde wijze de content van webpagina's op te slaan (Christin 2013b; Spitters e.a. 2015; Van Remunt & Van Wilsem 2016). Hierbij wordt van elke pagina van de site een soort *snapshot* gemaakt. Dit leidt ertoe dat kwantitatief onderzoek vaak gemakkelijk uit te voeren is, omdat er vaak grotere datasets beschikbaar zijn. Bij het observeren van *dark markets* probeert men periodiek zo veel mogelijk data van de grootste marktplaatsen te verzamelen. Anders zouden namelijk alle data verloren gaan als een marktplaats plotseling wordt opgeheven.

Bij participatie wordt deelgenomen aan de criminele activiteiten op *dark markets*. Van Wegberg e.a. (2018b) pasten deze methode toe op bitcoinmixers.[7] Het onderzoek was niet alleen gericht op het bestuderen van witwassen (door verschillende bitcoinmixers te gebruiken), maar ook op het *review*systeem van mixerdiensten. Het interveniëren op een *dark market* door politieacties levert in sommige gevallen ook toegang op tot data die beschikbaar zijn op de server. Hierdoor wordt het mogelijk inzicht te krijgen in de omvang van de daadwerkelijke handel en de achterliggende transacties. Deze schat aan data kan niet alleen tot nieuwe inzichten leiden, maar ook bestaande onderzoeken met data uit observaties valideren. Het onderzoeken van een marktplaats middels observatie maakt veelal gebruik van afgeleiden. Dit lijkt een valide methodologie, maar vraagt wel om toetsing. Om bijvoorbeeld het aantal *reviews* als afgeleide te gebruiken voor een inschatting van de totale transacties kan deze naast het daadwerkelijke aantal transacties gelegd worden. De daadwerkelijke transacties kunnen bijvoorbeeld worden onderzocht met behulp van de *back-end* van een site. In de *back-end*, ofwel de server waarop de website draait, staat de database die onder andere transactie- en registratiedata bevat.

Vooral de inzet van technieken als *scraping* en *crawling* levert potentieel grote datasets op met de mogelijkheid om een volledige historie in te zien. Dit maakt het mogelijk om het fenomeen *dark market* over een langere periode beter in kaart te brengen. Zo bestudeerde Christin (2013) binnen een tijdsperiode van drie maanden de producten die verhandeld werden op Silk Road 1.0. Hij onderzocht wat de omzet was van de verkopers en de omvang van de totale commissie die de administrators ontvingen. Andere onderzoeken brachten meerdere markt-

7 Mixerservices zorgen dat de traceerbaarheid van bitcoins wordt bemoeilijkt (Van Wegberg e.a. 2018).

doi: 10.5553/JV/016758502018044005006

plaatsen in kaart (Soska & Christin 2015; Kruithof e.a. 2016; Van Wegberg e.a. 2018). Aldrigde en Décary-Hétu (2014) onderzochten welk type koper actief was op Silk Road 1.0. Daarbij keken ze naar omvang en prijs van de transacties en de handel met behulp van *review*data. Zij concludeerden dat er niet enkel sprake was van *business-to-consumer* handel, maar dat er ook sprake was van *business-to-business* handel waarbij (offline) kopers drugs online kopen om hun eigen voorraad aan te leggen.

Onderzoek naar interventies op dark markets

Interventies op *dark markets* kunnen worden uitgevoerd door drie partijen, namelijk de marktplaats zelf, een private partij of een overheidsinstantie zoals de politie (zie volgende paragraaf). Hoewel het onlogisch klinkt dat een marktplaats zelf een interventie uitvoert, zijn er voorbeelden die dit illustreren. Zo zijn er voorbeelden van marktplaatseigenaren die ervandoor gaan met alle bitcoins die zij op dat moment in beheer hebben, ook wel een *exit scam* genoemd. Interventies gepleegd door een private partij zijn directe of indirecte acties uitgevoerd door derde partijen die de modus operandi van digitale criminaliteit veranderen. Zo kan een private partij stoppen met het aanbieden van haar diensten in het algemeen of voor specifieke locaties. Karami e.a. (2015) bestudeerden bijvoorbeeld de effecten van de interventie gepleegd door PayPal waarbij accounts gerelateerd aan een aantal specifieke booter-sites[8] werden bevroren.

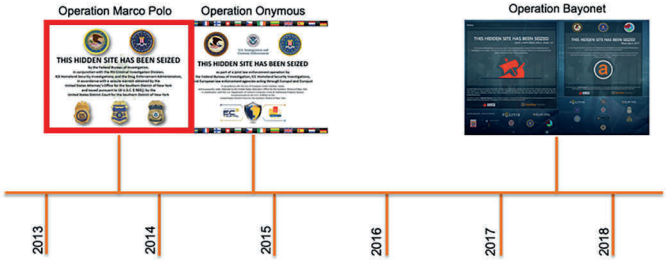
Onderzoek naar politie-interventies

De allereerste grote mondiale politieoperatie betreft Operatie Marco Polo, die in 2013 leidde tot sluiting van het befaamde Silk Road 1.0 en arrestatie van de administrator Ross Ulbricht. Operatie Onymous was de tweede mondiale operatie, deze leidde in 2014 tot de sluiting van meerdere sites op het *dark web*. Silk Road 2.0 was één van deze sites. De meest recente en laatste mondiale operatie betreft die van Operatie Bayonet in 2017. Deze operatie leidde tot de sluiting van de twee grootste markplaatsen van dat moment, namelijk Alphabay en Hansa

8 Platformen waar DDoS-aanvallen te koop zijn (Karami e.a 2015).

doi: 10.5553/JV/016758502018044005006

Figuur 2 Politie-interventies Marco Polo, Onymous en Bayonet



market. Alphabay werd hierbij als eerste door de FBI uit de lucht gehaald. Vervolgens werd Hansa market door de Nederlandse politie overgenomen en voor een maand draaiende gehouden. Dit heeft ertoe geleid dat veel data konden worden verzameld. Na een maand is ook Hansa market door de Nederlandse politie uit de lucht gehaald.
Onderzoek naar politie-interventies kan voor opsporingsdiensten potentieel van groot belang zijn. Met opgedane inzichten over de impact van operaties kunnen er immers verbeteringen worden gerealiseerd. Er zijn slechts enkele wetenschappelijke studies waarin onderzoek is gedaan naar of inzicht wordt verschaft in de effecten van politie-interventies.
Soska en Christin (2015) maken duidelijk dat *dark markets* in zekere mate bestand zijn tegen de tot nu toe ingezette interventies. Deze auteurs hebben over een langere periode onderzoek verricht naar de dagelijkse omzet binnen een aantal prominente marktplaatsen. Hoewel het onderzoek primair niet als doel had om interventies en de effectiviteit ervan te meten, konden zij daar uiteindelijk wel het een en ander over zeggen, omdat in de onderzoeksperiode zowel operatie Marco Polo als operatie Onymous plaatsvond. Uit dit onderzoek blijkt dat interventies slechts tijdelijk invloed hadden op de totale dagelijkse omzet van alle markten. De destijds overgebleven *dark markets* vulden namelijk het gat van de gesloten marktplaatsen snel op en maakten zelfs een significante groei door. Ook Décary-Hétu & Giommoni (2017) zagen slechts een gelimiteerd effect van operatie Onymous. Zo werd de prijs van de producten op de *dark markets* niet beïnvloed. Op de marktplaatsen in hun steekproef zagen ze daarnaast dat er voor een periode van een maand een daling te zien was van het totale aantal

doi: 10.5553/JV/016758502018044005006

verkopers en *listings*[9] in de steekproef (waaronder de sites die door operatie Onymous gesloten waren), maar dat deze aantallen na een maand weer aantrokken.

Van Wegberg en Verburgh (2018) deden onderzoek naar operatie Bayonet. Ze onderzochten daarbij specifiek de migratiepatronen vanaf de door de politie gesloten *dark market*s Alphabay en Hansa Market naar Dream Market. Dream Market werd na operatie Bayonet de grootste *dark market*. Om de instroom van criminelen naar Dream market te bepalen, werd met behulp van *scraping* en *crawling* data vergaard van de nieuwe registraties op het forum.[10] De registraties op de marktplaats zijn niet publiekelijk zichtbaar. Nieuwe kopers en verkopers zijn hierdoor niet goed te onderscheiden van de al aanwezige kopers en verkopers. Dit is omdat je alleen hun eerste publieke activiteit kunt meten, bijvoorbeeld een verkoper die zijn eerste advertentie plaatst. Een koper is niet verplicht een review achter te laten. Kopers en verkopers kunnen dus al langer actief zijn op de marktplaats, maar nog nooit eerder zichtbare datapunten hebben achtergelaten. Hoewel een eerste reviewscore of eerste advertentie mogelijke afgeleiden zijn voor nieuwe instroom, zijn deze variabelen – voorzover de onderzoekers kunnen nagaan – nog niet getest op validiteit. Door te kijken naar de registratie op het forum weten we zeker dat dit nieuwe kopers en verkopers zijn. Als onderzoeker mis je dan echter de groep die zich niet registreert op het forum. Het selecteren van de juiste variabelen is vaak een grote uitdaging en vergt een creatieve kijk op data. Onze ervaring is dat het combineren van technische en sociale invalshoeken het beste werkt om achterliggende concepten zoals identiteit en in- en uitstroompatronen het best te kunnen meten.

Uit de resultaten van de nieuwe forumregistraties bleek dat er een aanzienlijk grotere instroom was na operatie Bayonet dan daarvoor (Van Wegberg & Verburgh 2018). De traceerbaarheid werd onder andere bepaald door de geregistreerde PGP-gegevens en door de username van de verkoper in een *dark web*-database[11] op te zoeken.

9 Advertenties op een dark market.

10 De gemiddelde marktplaats bestaat uit een forum en een marktplaats. Voor het forum moet je je apart registreren. Hierbij zijn de exacte datum en het exacte tijdstip zichtbaar als deze wordt gescraped en crawled.

11 De *dark web*-zoekmachine Grams had een database waarbij de PGP-gegevens, username(s) en beoordelingen van verkopers van verschillende marktplaatse bijgehouden werden. Hierdoor konden kopers buiten de marktplaatsen op eenvoudige wijze controleren hoe betrouwbaar een verkoper was. Grams is in 2017 gestopt en is niet meer beschikbaar.

doi: 10.5553/JV/016758502018044005006

Zo kon worden achterhaald of de nieuwe verkoper eerder actief was op Alphabay, Hansa Market of beide marktplaatsen. Het bleek dat verkopers minder migreerden, of in ieder geval minder traceerbaar waren, vanaf Hansa Market dan vanaf Alphabay. Ervan uitgaande dat verkopers in een anonieme setting juist traceerbaar willen blijven, zodat ze vindbaar blijven voor hun cliënten, indiceren deze uitkomsten dat de verkopers op Hansa market zich meer terugtrokken uit de markt, of in ieder geval de traceerbaarheid verminderden, dan op Alphabay. De verkopers vertoonden dus een heftiger reactie op de interventie op Hansa Market.

Het voornaamste verschil tussen deze twee interventies is dat bij Alphabay de stekker eruit werd getrokken en dat Hansa nog een maand werd gerund door de Nederlandse politie alvorens de politie deze marktplaats opdoekte. De criminele gemeenschap op *dark markets* was bekend met het risico van een 'gewone' sluiting van een marktplaats zoals Silk Road 1.0 en Silk Road 2.0. De criminelen waren echter onbekend met het risico van een overname en wisten niet welke gegevens de politie van hen had weten te bemachtigen. De Hansa-overname heeft daarmee het vertrouwen van de gemeenschap in de onderliggende faciliterende principes van *dark markets* meer geschaad dan andere interventies. Dit was ook het doel van de overname. Een interessante vraag is of het effect bij een volgende overname net zo groot zal zijn of dat de impact hiervan afneemt.

Dit onderzoek is de eerste stap richting nieuwe onderzoeksaanpakken die zich richten op de gedragseffecten na politieacties. Bij deze methode geldt het voorbehoud dat er enkel uitspraken gedaan kunnen worden over de instroom en niet over de groep verkopers die zich voorafgaand aan de politieactie al hadden verplaatst over meerdere marktplaatsen. Sommige verkopers verspreiden zich proactief over meerdere marktplaatsen als strategie om businesscontinuïteit te behouden (Soska & Christin, 2015). Daarnaast zorgt men er op deze wijze voor dat de eigen username niet door anderen gebruikt kan worden op andere platformen. Hiermee dammen verkopers niet alleen potentiële reputatieschade in, maar is het voor verkopers ook gemakkelijker om te migreren naar een andere marktplaats als de huidige verdwijnt.

doi: 10.5553/JV/016758502018044005006

Tot slot

In dit artikel hebben we aangegeven welke mogelijkheden er zijn voor onderzoek naar *dark markets*. Soms moeten onderzoekers creatief zijn bij het vergaren van data en bij het meten van constructen, waarbij sociale en technische invalshoeken worden gecombineerd. Om zeker te weten dat er gemeten wordt wat men wil weten, is het essentieel dat er goed begrip is van de werkzame mechanismen op een *dark market*. Of de omvang van een marktplaats kan worden bepaald aan de hand van het totale aantal advertenties, moet nog worden getoetst. De data die voorkomen uit operatie Bayonet zijn van grote waarde hiervoor en vormen een goudmijn voor (Nederlandse) wetenschappers die *dark markets* onderzoeken. Met deze data kunnen afgeleide variabelen getoetst worden door ze af te zetten tegen de werkelijke waarden. Door in onderzoeken aandacht te besteden aan interventies op *dark markets* kan allereerst de effectiviteit van interventies worden beoordeeld. Bij een volgende operatie kan worden geprofiteerd van inzicht in de succesvolle en minder succesvolle elementen van eerdere politieacties. Met het schetsen van de context rondom de impactstudie van operatie Bayonet (Van Wegberg & Verburgh 2018) is getracht een nieuwe invalshoek weer te geven. Deze invalshoek richt zich op het bestuderen van de gedragseffecten van interventies. Onderzoek naar *dark market*-interventies staat echter nog in de kinderschoenen en initiatieven om creatief te interveniëren en dit te onderzoeken moedigen wij ten zeerste aan.

Literatuur

Afilipoaie & Shortis 2015
A. Afilipoaie & P. Shortis, *From Dealer to Doorstep – how Drugs are sold on the dark net. GDPO Situation Analysis*. Swansea: Swansea University, 2015.

Aldrigde & Décary-Hétu 2016
J. Aldridge & D. Décary-Hétu, 'Cryptomarkets and the future of illicit drug markets', in: EMCDDA *The Internet and Drug Markets*, 2016, p. 23-32.

doi: 10.5553/JV/016758502018044005006

Aldrigde & Askew 2017
J. Aldridge & R. Askew, 'How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement', *International Journal of Drug Policy* 2017, afl. 41, p. 101-109.

Barratt & Aldrigde 2016
M. Barratt & J. Aldridge, 'Everything you always wanted to know about drug cryptomarkets (but were afraid to ask)', *International Journal of Drug Policy* 2016, afl. 35, 1-6.

Buxton & Bingham 2015
J. Buxton & T. Bingham, *The rise and challenge of dark net drug markets,* Policy Brief, Swansea: Swansea University 2015.

Christin 2013
N. Christin, 'Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace', *World Wide Web* 2013, Conference Proceedings, p. 213–224.

Cox 2016
J. Cox, 'Staying in the shadows: the use of bitcoin and encryption in cryptomarkets', in: *EMCDDA, The Internet and Drug Markets*, 2016, p. 41-47.

Décary-Hétu & Dupont 2013
D. Décary-Hétu & B. Dupont, 'Reputation in a dark network of online criminals', *Global Crime* (14) 2013, afl. 2/3, p. 175–196.

Décary-Hétu & Giommoni 2017
D. Décary-Hétu & L. Giommoni, 'Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous', *Crime, Law and Social Change* 2017 afl. 67, p. 55–75.

Van Hout & Bingham 2013
M.C. van Hout &T. Bingham, "'Surfing the Silk Road': A study of users' experiences', *International Journal of Drug Policy* (24) 2013, afl. 6, p. 524-529.

Holt e.a. 2015
T.J. Holt, O. Smirnova, Y.T. Chua & H. Copes, 'Examining the risk reduction strategies of actors in online criminal markets', *Global Crime*, (16) 2015, afl. 2, p. 81–103.

Karami e.a. 2015
M. Karami, Y. Park & D. McCoy, 'Stress testing the Booters: Understanding and undermining the business of DDoS services', *Arxiv* 2015, p. 1033–1043.

Kruithof e.a. 2016
K. Kruithof, J. Aldrigde, D. Décary-Hétu, M. Sim e.a., *Internet-facilitated drugs trade. An Analysis of the size, scope and the role of the Netherlands*, Santa Monica: RAND Europe 2016

doi: 10.5553/JV/016758502018044005006

Matanovic 2017
A. Matanovic, Blockchain/cryptocurrencies and cybersecurity. Threats and opportunities' *The 9 th International Conference on Business Information Security (BISEC-2017)* 2017, conference proceedings, p. 11-15.

Mounteney e.a.
J. Mounteney, A. Oteo & P. Griffiths, 'The internet and drug markets: shining a light on these complex and dynamic systems', in: *EMCDDA, The Internet and Drug Markets* 2016, p. 13-17.

Van Remunt & Van Wilsem 2016
T. van Remunt, & J. van Wilsem, 'Wat wordt er nu eigenlijk gezegd? Een verkennend onderzoek naar communicatiepatronen op het Darkweb', *PROCES* (95) 2016, afl. 1, p. 24–39.

Soska & Christin 2015
K. Soska, & N. Christin, 'Measuring the longitudinal evolution of the online anonymous marketplace ecosystem', *24th USENIX Security Symposium (USENIX Security 15)* 2015, conference proceedings, p. 33–48.

Spitters e.a. 2015
M. Spitters, F. Klaver, G. Koot & M. van Staalduinen, 'Authorship analysis on dark marketplace forums', *Intelligence and Security Informatics Conference (EISIC)* 2015, conference proceedings, p. 1–8.

Tzanetakis e.a. 2016
M. Tzanetakis, G. Kamphausen, B. Werse & R. von Laufenberg, 'The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets', *The International Journal on Drug Policy* (35) 2016, afl. 1, p. 58-68.

Van Wegberg e.a. 2018a
R.S. van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi e.a.'Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets', *27th USENIX Security Symposium (USENIX Security 18)* 2018, conference proceedings, p. 1009–1026.

Van Wegberg e.a. 2018b
R.S. van Wegberg, J. Oerlemans & M.O. Deventer, 'Bitcoin money laundering: mixed results?', *Journal of financial crime* (2) 2018, afl. 2, p. 419-435.

Van Wegberg & Verburgh 2018
R.S. Van Wegberg & T. Verburgh, 'Lost in the fream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market', *Websci* 2018, conference paper.

doi: 10.5553/JV/016758502018044005006