# Digitalisering als tweesnijdend zwaard: gaan we de cybercrimineel ooit kunnen verslaan?

*(door Jessica Kats, senior onderzoeker/adviseur Dialogic, juli 2021)*

**Cybercriminaliteit neemt explosief toe**

Het was een vraag binnen de Nationale WetenschapsAgenda: 'Welke nieuwe vormen van criminaliteit komen op onze samenleving af door de toenemende digitalisering en hoe kan deze criminaliteit worden aangepakt?' Als nieuwe vormen worden o.a. digitale piraterij van 3D-ontwerpen (waaronder van pistolen) en medical cyber crimes (hacking van devices zoals pace makers en e-dossiers) genoemd. Er is zoveel onduidelijkheid over nieuwe vormen van (cyber)criminaliteit en we kunnen het bijna niet bijbenen. Dat is ook niet zo gek, als we bedenken dat de politie nog steeds relatief traditioneel geschoold is en er in bijna alle overheidstakken een tekort is aan ICT-experts. Tegelijkertijd pakt vooral de nieuwe generatie de relatief simpele trucjes op internet snel op. Zo is het extreem gemakkelijk om anoniem te blijven op het dark web waar drugs, wapens, nieuwe identiteiten en cyberaanvallen net zo simpel en snel te bestellen zijn als op bol.com. We beweren absoluut niet dat de opsporings- en veiligheidsdiensten niet de kennis in huis hebben om hiertegen op te treden, maar het is niet te ontkennen dat we altijd achter de feiten aan zullen blijven lopen. De cijfers onderstrepen dat. Medio januari 2021 publiceerde de Nationale Politie de jaarcijfers voor de criminaliteit die zij in 2020 registreerde. Opvallend is de meer dan verdubbelde prevalentie van online criminaliteit[1], een stijging van 127%, terwijl de geregistreerde prevalenties van zakkenrollerij en woninginbraken een sterke afname te zien gaven, respectievelijk bijna 50% en 25% (Politie, z.d.). Betekent dit een verschuiving van traditionele naar cybercriminaliteit? Volgens experts is dat wel degelijk het geval (Van der Vorst, Steur, Jelicic, Van Rees, 2019).

In de meest recente Veiligheidsmonitor gaf 13% van de bevolking van 15 jaar of ouder aan in 2019 slachtoffer te zijn geweest van één of meerdere vormen van cybercriminaliteit (CBS, 2020). Slechts een beperkt deel van de slachtoffers geeft aan daarvan melding of aangifte te doen bij de politie. Voor meldingen is dat 12,8% en voor aangiftes 8,2% (CBS, 2020). Voor

[1] Dit betreft zowel cybercriminaliteit (delicten waarbij ICT zowel het middel als het doel is, zoals DDoS-aanvallen, ramsomware, virussen en malware) als gedigitaliseerde criminaliteit (traditionele delicten waarbij ICT als middel wordt ingezet, zoals internetoplichting, afpersing via e-mail en phishing). In de praktijk lopen deze vormen vaak door elkaar en daarom wordt de term cybercriminaliteit ook als overkoepelende term beschouwd.

traditionele criminaliteit zijn deze percentages aanmerkelijk hoger: in 2019 volgt in 31,9% van de gevallen melding en in 22,9% van de gevallen aangifte. Er vindt dus niet enkel een verschuiving plaats, maar cybercriminaliteit blijft ook nog meer verborgen voor de strafrechtketen dan traditionele criminaliteit.

In 2018 hebben wij onderzoek gedaan naar het infameuze 'dark number in crimes', waarbij cybercriminaliteit één van de focusgebieden was (Smit, Ghauharali, Van der Veen, Willemsen, Steur, et al., 2018). Hieruit bleek dat schattingen over omvang van cybercriminaliteit sterk uiteenlopen. Om de hierboven beschreven redenen ('under-reporting', bijvoorbeeld omdat individuen of bedrijven in veel gevallen niet geneigd zijn een melding te maken van een aanval, omdat ze niet bekend willen maken dat ze slachtoffer zijn geweest of soms niet eens weten dat ze slachtoffer zijn geweest), maar ook omdat algemene schattingen vaak gebaseerd zijn op incomplete data die niet representatief zijn. Zo zijn veel uitspraken gebaseerd op wat virusscanners onderscheppen bij grote bedrijven in bepaalde landen. Wij onderzochtten verschillende nieuwe meetmethoden voor o.a. DDoS, phishing, pharming en ransomware. Iedere interactie die plaatsvindt in een digitaal systeem is in principe immers ergens meetbaar. Dat kan op drie punten zijn: op het computersysteem of netwerk van een slachtoffer, bij de dader of op een tussenliggend platform.[2] Voor de meeste verschijningsvormen komen daarnaast dezelfde interacties terug: acquistie van malware of tools, verspreiding of plaatsing van de aanval, bescherming en beveiligingsacties, betalingen (vaak Bitcoins) en aangiften. Dit zijn allemaal mogelijk meetpunten, maar ook hier geldt de eerdergenoemde beperking: het is incompleet en niet representatief.

Hoewel voor opsporing in het algemeen geldt dat we per definitie achter de feiten aanlopen en altijd maar een deel van de incidenten kunnen meten, is dit probleem groter in een zeer dynamisch domein als cybercriminaliteit. Talloze ontwikkelingen (die ironisch genoeg vaak voortkomen uit de tendens om privacy te verbeteren) leiden tot nieuwe uitdagingen voor de opsporingsdiensten. In 2019 verkende wij bijvoorbeeld de technische opsporingsmogelijkheden bij toenemend hergebruik van IP-adressen (Van der Vorst, Steur, Jelicic & Van Rees, 2019). Dat bleek een interessante kwestie, want hoewel een IP-adres als een soort 'kenteken' op internet de dader vindbaar kan maken, zijn deze IP(v4)-adressen schaars. Om die reden worden IP-adressen in toenemende mate hergebruikt, waardoor criminelen nog moeilijker zijn op te sporen. Daarnaast wordt er steeds meer data versleuteld en opgeslagen 'in de cloud', neemt de complexiteit van software toe en worden aanvalstechnieken steeds geavanceerder.

Het is een enorme uitdaging, maar de achterstand ten opzichte van cybercriminelen kan weldegelijk beperkt worden gehouden of verder worden verkleind. De afgelopen jaren is de bestrijding van cybercriminaliteit ver geprofessionaliseerd en beter georganiseerd. Het onderwerp staat hoog op de agenda, ook in Den Haag. Denk aan de Nederlandse Cyber

[2] Deze definities zijn analoog aan de categorieën user centric, network centric en site centric die worden gehanteerd bij het meten van statistieken op basis van het internet (Munnichs, Kouw & Kool, 2017).

Security Agenda en alle initiatieven die daaruit zijn voortgekomen (waaronder een gedegen evaluatiemethodiek, Brennenraedts, Hanswijk, Jansen, Kats, Sahebali & Hermanussen, 2020). En opsporingsdiensten gaan zelf ook steeds meer innovatieve technieken inzetten. De hoeveelheid beschikbare data wordt langzaamaan een voordeel. Een specifiek voorbeeld is de opkomende trend van geplande vechtafspraken tussen supporters van betaald voetbalclubs. De daders posten foto's en filmpjes online, waarop ze geïdentificeerd kunnen worden. Waar voorheen die data door politiemedewerkers werd bekeken, wordt steeds meer geëxperimenteerd met het inzetten van automatische gezichtsherkenning en voorspellende modellen (Ferwerda, Wolsink, Steur, Jelicic, 2020).

**Het dark web wordt steeds een beetje lichter**

De belangrijkste reden waarom cybercriminelen zo moeilijk te pakken zijn, ligt in de anonimiteit die zij vinden op het internet. Dat kan bijvoorbeeld via een VPN-verbinding. Bij verbinding met een VPN verloopt het internetverkeer via een beveiligde verbinding en wordt het IP-adres verborgen. Anoniem internetten kan ook met een proxyserver. De gebruiker vraagt dan internetgegevens op bij de proxyserver en vanuit daar wordt de aanvraag doorgestuurd naar de desbetreffende website. Ook hier is het IP-adres van alleen de proxyserver te zien (maar mist de encryptie van data en is het dataverkeer en IP-adres van de gebruiker toch te achterhalen). Next level anoniem browsen is mogelijk met een Tor-browser. Tor (een acroniem voor The Onion Router) is een onlinenetwerk voor versleutelde en anonieme communicatie. Het netwerk bestaat uit vele duizenden servers wereldwijd en het dataverkeer wordt gefragmenteerd en versleuteld door meerdere servers gestuurd voordat het bij de ontvanger aankomt. Data kan dus niet herleid worden tot één computer of gebruiker. Tor geeft gebruikers toegang tot het dark web en daar wordt het pas echt interessant. Dit is het deel van het internet dat niet gereguleerd wordt en het is de basis voor veel illegale activiteiten.[3]

We kennen allemaal de verhalen van de bizarre en afschuwelijke diensten en goederen die worden aangeboden op het dark web. Denk aan drugs, wapens, persoonlijke gegevens, nieuwe identiteiten, gerichte wire of apparaatfraude, kinderporno, gewelddadige video's, snuff-films en zelfs huurmoordenaarservices (hoewel dit grotendeels oplichterij is; wel betalen, niet uitvoeren). De bekendste 'marktplaats' op het dark web was Silk Road. Silk Road zou gedurende zijn bestaan de verkoop van verdovende middelen mogelijk hebben gemaakt voor een bedrag van 1,2 miljard dollar. Het platform is opgedoekt, maar er zijn inmiddels weer voldoende vergelijkbare sites aanwezig.

De Nederlandse politie is dan ook meer en meer aanwezig op het dark web, mede door de politieke druk vanuit de VS en Australië vanwege de hoeveelheid verscheepte (hoofdzakelijk synthetische) drugs vanuit Nederland (Hietkamp, 2021). En we doen dat goed. Zo heeft de

[3] Overigens is het dark web ook een veilige plek voor journalisten, klokkenluiders en burgers die onder dictatoriale regimes leven, en dus niet per definitie 'slecht'.

Nederlandse politie een paar grote successen geboekt. In 2017 heeft de Nederlandse politie samen met de FBI handelaren opgepakt door een maand lang een illegale handelsplaats in de lucht te houden: Hansa. Toen Alphabay (een markt die naar schatting tien keer groter was dan Silk Road) uit de lucht werd gehaald, vluchtten veel gebruikers naar Hansa, precies zoals de politie had gepland. Door de encryptie uit te zetten, kon de politie meelezen met alles wat er via de site werd verstuurd. En opeens is het dark web dan niet meer zo dark.

Toch blijft het in de meeste gevallen bij reactieve en opportunistische acties, zo blijkt uit het onderzoek van onze stagiair Lennart Hietkamp (2021). Monitoren, meelezen en hopen dat iemand iets prijsgeeft, bijvoorbeeld over verpakkingsmethoden of locaties. Communicatie is één van de belangrijkste puzzelstukjes voor online opsporing. Handel op het dark web draait om vertrouwen. Daarvoor zijn reviews en reputatie essentieel. Het helpt daarbij om te zeggen dat de drugs uit Nederland komen of te hinten naar een Nederlandse herkomst door namen met een Nederlands tintje, want Nederlandse drugs staan goed aangeschreven. Deze 'Dutch branding' wordt overigens ook toegepast door verkopers die niet uit Nederland komen. De politie vertrouwt daarom vooral op Nederlandse communicatie, al is het maar een begrip of bepaalde zinsopbouw in het Engels. Om de opgebouwde reputatie en identiteit mee te kunnen nemen naar verschillende platformen wordt vaak pgp (pretty good privacy; een manier waarop men berichten en bestanden onderling kan uitwisselen met versleuteling) gebruikt.

Die zorgvuldig opgebouwde vertrouwensstructuur probeert de politie dan ook onderuit te halen door zelf zichtbaar te zijn op het dark web (Hietkamp, 2021). Door kenbaar te maken wie ze de laatste tijd hebben opgepakt of op het spoor zijn, communiceert de politie bewust dat het dark web niet zo anoniem is als gedacht. Door het gevoel van de pakkans te vergroten worden vooral de kleinere kopers afgeschrikt.

Hoewel er de laatste tijd al de nodige successen zijn geboekt, kan er wat ons betreft nog heel wat gewonnen worden op het terrein van opsporing op het dark web. De bekende marktplaatsen zijn letterlijk een verzamelplaats van illegale activiteiten, beschikbaar voor de politie om criminelen uit te vissen. Dat kan proactiever benaderd worden. Tal van aanknopingspunten zijn nog niet uitgeput, zoals het opsporen van financiële transacties (cryptosporen).

**Wedloop die we kunnen winnen?**

Ja, dat kunnen we. De huidige ontwikkelingen en toenemende digitalisering maken het de cybercrimineel weliswaar steeds makkelijker, maar diezelfde kansen zijn er voor de opsporingsdiensten. Als we maar genoeg innovatieve methoden blijven inzetten, proactief optreden, (internationale) afspraken blijven maken en vooral veel onderzoek blijven doen.

**Literatuurlijst**


- Brennenraedts, R., Hanswijk, M., Jansen, R., Kats, J., Sahebali, W. & Hermanussen, L. (2020). *Planevaluatie Nederlandse Cyber Security Agenda.* Den Haag: WODC Publications.
- CBS (2020). *Veiligheidsmonitor 2019*. Den Haag: CBS.
- Ferwerda, H., Wolsink, J., Steur, J., Jelicic, N. (2020) Vechtafspraken: daders herkennen en afspraken voorspellen met kunstmatige intelligentie. In opdracht van: Politie & Wetenschap.
- Hietkamp, L. (2021). Het vertrouwen op het *Dark Web*: De communicatie van de Nederlandse drugsverkoper. Masterscriptie Criminologie, Faculteit der Rechtsgeleerheid, Universiteit Leiden.
- Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid.* Den Haag: Rathenau Instituut. Met bijdragen van Dialogic.
- Smit, P., Ghauharali, R., Veen, H.C.J. van der, Willemsen, F., Steur, J., Velde, R.A. te, Vorst, T. van der, & Bongers, F. (2018a). *Tasten in het duister: Een verkenning naar bronnen en methoden om de aard en omvang van criminaliteit te meten. Deel 1: Hoofdrapport.* Den Haag: WODC. Cahier 2018-21a.
- Smit, P., Ghauharali, R., Veen, H.C.J. van der, Willemsen, F., Steur, J., Velde, R.A. te, Vorst, T. van der, & Bongers, F. (2018a). *Tasten in het duister: Een verkenning naar bronnen en methoden om de aard en omvang van criminaliteit te meten. Deel 1: Technisch rapport.* Den Haag: WODC. Cahier 2018-21b.
- Van der Vorst, T., Steur, J., Jelicic, N., Van Rees, J. (2019). *Mogelijkheden voor identificatie op internet op basis van IP-adres.* Den Haag: WODC Publications.

Websites

- www.politie.nl/nieuws/2021/januari/15/00-criminaliteit-2020-minder-inbraak-meer-cybercrime.html