LICHT SCHIJNEN OP HET DARK WEB

Door Anouck Vrouwe Beeld Shutterstock, TNO, Sjoerd van der Hucht

Op het dark web botst de wens van de gebruiker die anoniem wil blijven op die van de politie die toezicht wil houden. De politie pioniert er met online opsporingsmethoden, en dat is weer voer voor onderzoek. Welke strategieën zijn effectief bij het bestrijden van criminaliteit op het dark web?

Buying on the dark web? You are on the menu! Ronkende zinnen te over in het persbericht dat Europol afgelopen maart verspreidde. Bij een internationale actie werden die maand 61 mensen aangehouden. Ook werden 300 kilo drugs, 51 vuurwapens, 4 miljoen euro aan cryptovaluta en 2 miljoen euro aan cash geld in beslag genomen. Het begon allemaal bij de Cyber Patrol Action Week in het Europolhoofdkantoor in Den Haag, ruim een half jaar eerder. Daar stelden internetrechercheurs van over de hele wereld een lijst op met 247 high value targets: mensen die handelden in verboden goederen op het dark web. Lokale politiediensten gingen met die lijst aan de slag. Met goed resultaat, benadrukt het persbericht: 'Deze gecoördineerde actie laat zien dat je, als je illegale activiteiten uitvoert op het dark web, opgespoord kan en zal worden door de autoriteiten. Het dark web is niet zo donker als je denkt.'

Toen Mark van Staalduinen in 2012 voor TNO begon met onderzoek naar het dark web, zeiden collega's hem dat hij naar sprookjes zat te kijken. 'Ik moest dat allemaal niet zo serieus nemen. Dat dark web was fake, een plek voor grapjassen', zo omschrijft hij het sentiment in die tijd. De realiteit bleek anders. Op het dark web vindt serieuze criminaliteit plaats. De Nederlandse politie doet er degelijk onderzoek en doet mee aan grootschalige internationale operaties. Het cybersecurityteam van TNO is inmiddels gegroeid tot 100 mensen, waarvan 10 voor het dark web alleen. Van Staalduinen is er Innovation Manager op het gebied van het dark web, Blockchain en IoT security. Hij werkt grotendeels vanuit Singapore, dat het veiligste land op aarde wil zijn en zwaar inzet op cybersecurity. In 2015 opende INTERPOL er haar internationale innovatiecentrum voor cybercrime.

Anonimiteit

Wouter Stol spreekt liever niet over dark web. De term anonieme communicatienetwerken is neutraler, en daarom beter, vindt hij. Dark web klinkt spectaculair, maar suggereert ook dat dit afgeschermde deel van internet één groot boevenhol is. Dat is het niet, benadrukt Stol. Zijn team onderzoekt hoe de politie opereert op TOR, een van de netwerken die op basis van anonimiteit opereert. Stol is lector Cybersafety bij NHL Stenden Hogeschool en de Politieacademie en bijzonder hoogleraar Politiestudies aan de Open Universiteit. 'TOR is nuttig, en moet blijven bestaan. Dat is ook het beleid van de Nederlandse overheid', benadrukt hij aan het begin van het gesprek. Privacy is een groot goed, je anoniem op internet begeven moet mogelijk zijn. TOR is namelijk ook het netwerk dat journalisten en mensenrechtenactivisten graag gebruiken. Stol: 'Dit is een omgeving waar mensen duidelijk het signaal geven dat ze anoniem willen blijven, om wat voor reden dan ook. Daar moet je respectvol mee omgaan.'

De vraag is vervolgens hoe je de wet handhaaft binnen die anonieme communicatienetwerken. Want een online vrijstaat voor de handel in drugs, wapens en kinderporno is niet acceptabel, benadrukt Stol. 'Gemeenschappen zonder de mogelijkheid van overheidstoezicht kun je je als maatschappij niet veroorloven.' De politie moet dus ook online criminaliteit opsporen. Stol: 'Hoe zet je je opsporingsbevoegdheden goed in? Dat is de vraag die wij in ons onderzoek stellen. Hoe houdt de politie balans tussen toezicht en opsporing enerzijds en rechtswaarborgen anderzijds?' Doordat de communicatie versleuteld is, is die niet goed halverwege af te luisteren, zoals dat bij telefoons wel kan. Om toch te weten wat er gebeurt, moet de politie bij de bron zijn. Stol: 'Ze kan dan bijvoorbeeld inbreken in iemands computer. Dat is niet iets wat de politie al te lichtzinnig doet, want dan weet je ook meteen alles over iemand. Hoe sterk moet je verdenking dan zijn? Hoe balanceer je tussen privacy en toezicht?'

Mark van Staalduinen

'De innovatiekracht van de criminelen vraagt om slimme, creatieve antwoorden'

Stols onderzoeksproject Police Detectives on the TOR-network (PDTOR) is internationaal en multidisciplinair, zoals gebruikelijk is bij onderzoekprojecten naar het dark web. Zweedse techneuten kijken naar het veiligstellen van bewijs: hoe bewaar je online communicatie en handel op zo'n manier dat het later in de rechtszaal als rechtsgeldig materiaal te gebruiken is? Zij oefenen daarvoor in een labversie van TOR. Noorse juristen kijken onder meer naar welke instanties eigenlijk opsporingsbevoegdheid hebben. Stol: 'Online criminaliteit gaat over landsgrenzen heen. Als je in je onderzoek op Franse verdachten stuit, en op servers in Litouwen, wat mag er dan? En omgekeerd, welke ruimte krijgt politie uit andere landen om hier in Nederland mensen op te sporen? Welke informatie deel je?'

De Nederlandse onderzoekers bestuderen de politiepraktijk. 'Verreweg het leukste deel van het onderzoek, vind ik dan', lacht Stol. Zijn mensen reconstrueren afgesloten politiezaken; hoe is de zaak aangepakt, welke beslissingen zijn er genomen, welke strategie heeft de politie gebruikt – of was er geen duidelijke strategie? Stol en zijn team maken zo een analyse van het werk van de politie op TOR. 'Nog niet zo lang geleden was de politie online gewoon afwezig op het TOR-netwerk. Inmiddels hoort digitale opsporing op het dark web bij de kerntaken van de politie. Het is voor politiemensen alleen nog zoeken hoe je dit soort zaken goed aanpakt.'

Nieuwe insteek

Ook Van Staalduinen analyseert politieoptreden op het dark web. Hij vertelt dat politieonderzoek naar het dark web eerst vooral observeren was. 'Hoe werkt het, hoe spoor je mensen op die zich anoniem wanen? Nu staat de vraag centraal hoe de politie cybercriminaliteit kan frustreren en voorkomen. Die insteek is nieuw.' Zijn team bij TNO probeert de effecten te meten van online politieacties. Als voorbeeld noemt hij de cryptomixerdienst Bestmixer.io, die het Nederlandse Openbaar Ministerie en de FIOD in mei offline hebben gehaald. 'De techniek om transacties van cryptovaluta te volgen is de laatste tijd sterk verbeterd, waardoor de politie cryptogeld steeds beter kan volgen', legt hij uit. 'Cryptomixers zijn daar weer het antwoord op, zij verhullen geldstromen.' Nu is het interessant om te kijken hoe effectief het neerhalen van de cryptomixers door FIOD is. Van Staalduinen: 'Dat proberen wij te meten. Houden de criminelen zich een tijdje gedeisd, of verplaatsen ze hun activiteiten gewoon naar een andere mixer? Ontregelt dit zo, dat mensen zich anders gaan gedragen – wat weer kansen biedt voor opsporing?'

Welke ingrepen effectief zijn, is een grote en moeilijke vraag, waarop nog lang geen antwoord te geven is. Zeker is dat het niet enkel draait om technologie, benadrukken beide onderzoekers. Psychologische oorlogsvoering is een essentieel onderdeel van het spel. In de anonieme wereld die het dark web is, draait immers alles om vertrouwen. Wie dat vertrouwen ondermijnt, ondermijnt het systeem. De Nederlandse politie nam in 2017 ongemerkt het beheer van Hansa Market over, een drugsmarktplaats op het dark web. Tienduizenden berichten werden onderschept, vaak bestellingen met

daarin het adres waar de drug geleverd moesten worden. Niet zelden waren dat particulieren die voor eigen gebruik drugs bestelden. De politie ging veel van die adressen langs, wat weer de kranten haalde. Van Staalduinen: 'Zo gaf de politie duidelijk het signaal dat anoniem drugs bestellen en verhandelen via het dark web niet betekent dat je niet kan worden opgespoord.'

Wouter Stol

'Digitale opsporing op het dark web hoort inmiddels bij de kerntaken van de politie'

Het geautomatiseerd filteren van data van het dark web is bij TNO ook een belangrijke onderzoeksrichting. Als je illegale handel op een marktplaats wil volgen, hoe haal je dan de relevante gegevens uit de brij van berichten en transacties? Van Staalduinen: 'Wij verwachten dat technieken uit de artificiële intelligentie kunnen helpen bij het filteren en het herkennen van opmerkelijke en afwijkende activiteiten.'

Dat internetcriminaliteit niet te stoppen is, staat voor Stol en Van Staalduinen als een paal boven water. Stol: 'Ook nieuwe technologie biedt geen definitieve oplossingen.' Van Staalduinen: 'Het criminele circuit beschikt over geweldige cyber-securityexperts. De beveiliging van online criminele marktplaatsen op het dark web is fenomenaal – die mensen moeten niet alleen de politie uit hun nek houden, maar ook de andere criminelen die de marktplaats willen overnemen.' Werk genoeg dus, zegt Staalduinen: 'De innovatiekracht van de criminelen vraagt om slimme, creatieve antwoorden. Dat is waar wij onderzoekers samen met de politie aan werken.'

POLICE CONTROL ON THE DARK WEB

The dark web is no longer an un policed area. However, the police is still figuring out how to operate in this new environment. What is effective, and what do the rules of due process and forensic correctness mean in this digital environment? When do you enter someone's computer, for example? Wouter Stol (NHL Stenden University of Applied Sciences, Police Academy and Open University) studies the online detective work of the Dutch police by looking at closed police cases. Mark van Staalduinen (TNO) is finding new ways to measure the effects of police charges, like shutting down illegal markets or bitcoin mixers.

PDTOR

The study 'Police Detectives on the TOR network' (PDTOR) focuses on police detectives fighting crime on a specific part of the internet: the TOR-network. The study aims at answering the question of how our society can properly deal with the tension between privacy and other fundamental rights of citizens, and the exercise of state power, when this power is exercised for the purpose of preventing and investigating crime.