Secondant
THEMA'S:CYBERCRIMESOCIALE MEDIA
RUBRIEK:ONDERZOEK & ANALYSE

WAT KUNNEN POLITIE EN JUSTITIE IN HET DIGITALE DOMEIN?

Foto: Liesbeth Dingemans

3 november 2017
AUTEURS: CARLIJN BROEKMAN , ARNOUT DE VRIES , MARCEL VAN BERLO

Nieuwe communicatiemiddelen zoals sociale media bieden politie en justitie grote kansen. Maar zij zien zich ook voor uitdagingen gesteld. Zo kunnen criminelen via het Dark Web terrorisme financieren en op verzoek misdaden plegen. Hoe gaan veiligheidsinstanties met deze kansen en uitdagingen om?

Rechter geeft stalker 'digitaal straatverbod' kopte de *NRC*. EenVandaag maakte een uitgebreide reportage onder de titel *"Politiewerk onder vergrootglas door social media"*. Burgers kijken steeds meer mee met de politie en nemen bijvoorbeeld opsporingstaken (deels) op zich. Digitale burgeropsporing lijkt onvermijdelijk, maar het resultaat kan 2 kanten op rollen. Denk aan de 'kopschoppers van Eindhoven' voor een ongewenste wending van burgeropsporing waardoor de daders strafvermindering kregen. Bellingcats rapport over de MH17-ramp leverde juist een gewenst

resultaat op, dat het Joint Investigation Team dankbaar in ontvangst nam. Om één ding kunnen we in ieder geval niet heen: sociale media hebben het veiligheidslandschap flink veranderd.

NIEUWE COMMUNICATIEMIDDELEN

Wat doen veiligheidshandhavers in Nederland, maar ook ver daarbuiten nu met deze nieuwe communicatiemiddelen? Wat voor kansen bieden sociale media of het *Dark Web* en worden ze wel voldoende benut? Wat mag nu precies wel en niet? En welke bedreigingen moeten in de gaten gehouden worden? Kortom: wat moeten, mogen en kunnen veiligheidshandhavers, en wat juist níet?

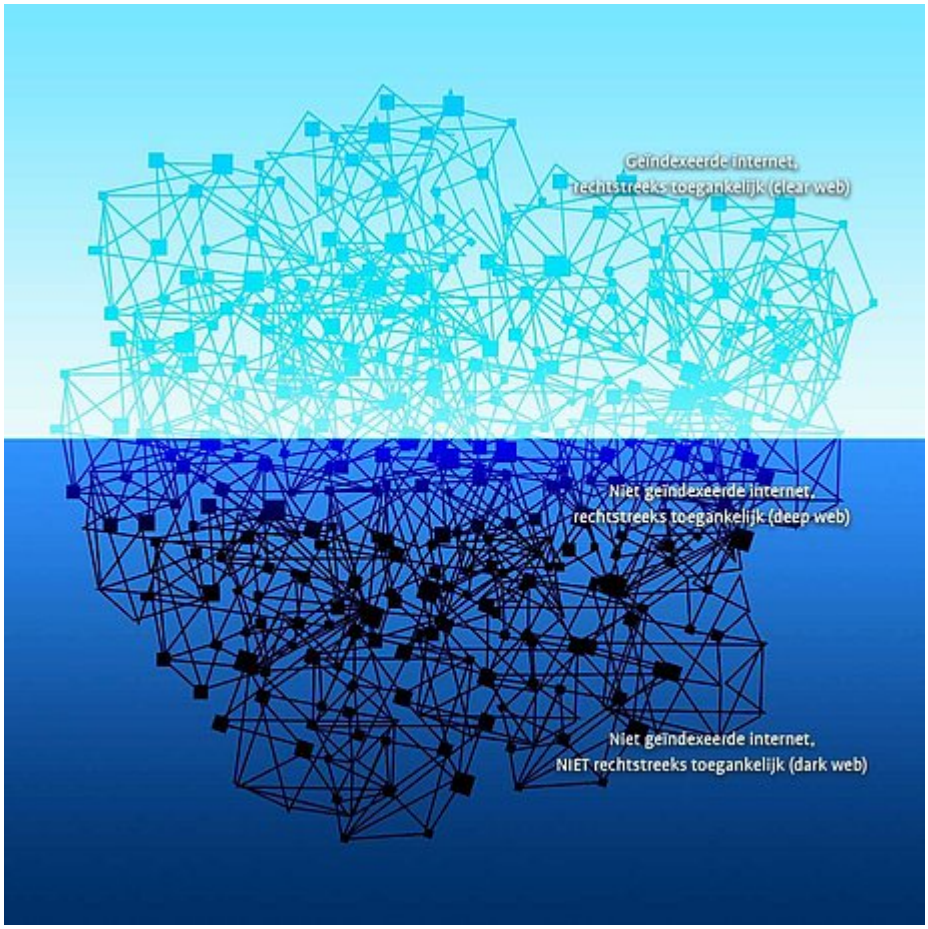
Het Dark Web is voor criminelen interessant, omdat anonimiteit daar de norm is

Dit is een eerste artikel van een reeks waarin we antwoorden op deze vragen zoeken, als onderdeel van het Europese onderzoeksproject MEDI@4SEC. Dat buigt zich over de kansen en bedreigingen die sociale media bieden voor veiligheidsinstanties.

CRIMINELE HANDELINGEN OP HET CLEAR WEB

Nieuwe communicatietechnieken zoals sociale media worden voor steeds meer criminele – en ongewenste – handelingen gebruikt. Denk bij ongewenste handelingen bijvoorbeeld aan cyberpesten, stalken, of het versturen van (doods)bedreigingen. In het 3-jarige onderzoeksproject wordt niet alleen gekeken naar wat er op het *Clear Web* gebeurt. Dat is het normale web, dat met een normale webbrowser toegankelijk is en via gebruikelijke zoekmachines als Google kan worden doorzocht.

Figuur 1> Metafoor voor het Clear Web versus het Deep web. Slechts een deel van de content op internet wordt geïndexeerd en getoond na een zoekopdracht



Illustratie: het CCV

ANONIMITEIT VAN HET DARK WEB

Juist het Dark Web (onderdeel van het Deep Web) is voor criminelen interessant, omdat anonimiteit daar de norm is. Voor dit deel van het web heb je een speciale TOR-browser nodig en de webpagina's worden niet door Google doorzoekbaar gemaakt (figuur 1). Criminelen maken handig gebruik (of eigenlijk misbruik) van deze nieuwe technologische mogelijkheden. Voorbeelden van nieuwe criminele toepassingen zijn:

- IS-strijders werven, door middel van versleutelde berichten;
- terrorisme financieren, door anonieme crowdfunding (concept waarbij vele mensen bijdragen aan de financiering. Betaling met Bitcoins waarborgt een bepaalde anonimiteit);
- criminele cyberaanvallen aanbieden, zoals een DDoS (al vanaf 10 euro per uur);
- misdaden op verzoek plegen, via *crimesourcing*, of *crime as a service*;
- beeldmateriaal anoniem delen, door en voor pedofiel-netwerken.

Maar wat zijn nu eigenlijk de taken van de politie en het OM in deze digitale domeinen? Waar kan of moet het bedrijfsleven de handschoen oppakken? Wat kan, moet en mag men online doen om veiligheid te handhaven?

Internettrollen plaatsten een gerucht dat er haaien in de straten van Manhattan zwommen

Hebben politie en justitie eigenlijk wel voldoende middelen, kennis en mogelijkheden om de verwachtingen in de digitale samenleving waar te maken? Of is er behoefte aan meer (nieuwe) middelen, zoals technische tools of kennis gericht op gedragsbeïnvloeding?

KANSEN VOOR VEILIGHEIDSINSTANTIES

Sociale media bieden voor verschillende operationele processen kansen voor de veiligheidsinstanties, waaronder de politie. Maar deze gaan vaak ook gepaard met uitdagingen en/of bedreigingen. Een aantal van deze kansen beschrijven we hierna.

CRISISMANAGEMENT EN ALARMERING

Sociale media worden hierbij bijvoorbeeld ingezet om snel een indruk te krijgen van de situatie (*situational awareness*), om hulpvragen te signaleren en eventueel uit te zetten. Toepassingen zoals Twitter of NL Alert worden hierbij gebruikt om mensen te informeren. De grote hoeveelheden berichten die moeten worden geanalyseerd en de interpretatie hiervan, vormen hierbij grote uitdagingen. Opruiende nepberichten die veel paniek kunnen veroorzaken zijn zelfs een bedreiging. Deze worden ook wel hoaxes genoemd. Een voorbeeld van een hoax is het bericht tijdens Project X Haren. Daarin werd met een foto als ‘bewijs’ aangekondigd dat er Hell’s Angels onderweg waren die ‘wel even zouden komen helpen’. Een ander voorbeeld zijn internettrollen die een gerucht plaatsten dat er haaien in de straten van Manhattan zwommen, terwijl de orkanen Irene en Sandy over New York raasden.

SURVEILLANCE

Analyse van berichten op sociale media kan de effectiviteit en efficiëntie van surveillance vergroten. Capaciteit kan op basis van verkregen inzichten worden ingepland en opgeschaald bij potentiële incidenten en vermoedens van criminele activiteiten. Men experimenteert door soms vroegtijdig reacties op berichten te plaatsen met als doel gedragsbeïnvloeding. Tijdens grote evenementen gebeurt dit al. Bijvoorbeeld tijdens de Olympische spelen van 2012 in Londen of tijdens diverse evenementen in Nederland.

Voorkomen moet worden dat burgers voor eigen rechter gaan spelen

Er is grote behoefte aan het monitoren van online berichtenverkeer, maar partijen als Twitter en Facebook willen surveillancetoepassingen momenteel juist weer blokkeren om de privacy van hun klanten te beschermen. Wetgeving loopt achter op deze ontwikkelingen, maar er zijn ook kansen voor samenwerking doordat bedrijven, burgers en politie andere wettelijke kaders hebben.

OPSPORING NA EEN DELICT

Het rapport van Bellingcat over de MH17-ramp is misschien wel het beste recente voorbeeld van hoe sociale media het mogelijk maken om bij te dragen in een belangrijk politieonderzoek. Met meerdere gemotiveerde speurneuzen zijn vele beelden en inzichten samengebracht tot een serieus onderzoeksrapport met waardevolle informatie. Onderzoek van Julian Foster liet zien dat 54 procent van de bevraagde politieorganisaties waardevolle informatie ontvangen via sociale media. In het Verenigd Koninkrijk is zelfs het aantal zaken dat opgelost kon worden door Facebook te gebruiken, met 540 procent gestegen. Achterblijvende wet- en regelgeving over wat wel en niet mag, ook in de samenwerking met burgers die digitaal sporen veilig proberen te stellen, vormt hierbij nog wel een uitdaging.

COMMUNITY POLICING

Sociale media faciliteren en stimuleren een Community Policing-strategie waarin iedereen mee kan werken aan veiligheid. Bekende voorbeelden in Nederland zijn de WhatsApp-buurtgroepen. Een van de uitdagingen bij deze moderne vorm van Community Policing is om de groepsdynamiek en samenwerking in goede banen te leiden. Voorkomen moet worden dat burgers voor eigen rechter gaan spelen. Juridisch ligt het lastig om als wijkagent onderdeel te worden van een WhatsApp-buurtgroep, terwijl men wel op nieuwe manieren met elkaar in contact wil staan.

INTELLIGENCE

Sociale media en Dark Web vormen rijke bronnen van informatie die met behulp van (complexe) analyses tot politionele intelligence kunnen worden veredeld. Sociale media bieden bovendien toegang tot een ‘wisdom of the crowd’. Zo beschikt de Nederlandse politie over nieuwe organisatieonderdelen zoals Real-Time Intelligence Centers (RTIC), die collega’s van relevante informatie ten tijde van incidenten kunnen voorzien. Ook wordt er geëxperimenteerd met nieuwe technologie zoals Predictive

Policing. De politie van de Australische staat Victoria gebruikt sociale media intelligence zelfs om te kijken naar de prestaties van hun eigen medewerkers. De politie moet leren omgaan met blijvende uitdagingen, zoals de overmaat aan berichten die uit verschillende sociale media en fora op het Dark Web moeten worden gedestilleerd en geanalyseerd. Dat geldt ook voor de interpretatie van deze berichten in combinatie met de relatieve anonimiteit van de afzenders. <<

Europees project
Het onderzoeksproject MEDI@4SEC brengt de kansen en bedreigingen in kaart die nieuwe communicatietechnologieën teweegbrengen voor de veiligheid en veiligheidsinstanties. Dit artikel ging in op algemene kansen en bedreigingen voor veiligheidsinstanties, en in het bijzonder een aantal operationele taakstellingen van de politie. In volgende artikelen zullen 6 specifieke thema's centraal staan: 1) *Do It Yourself (DIY) Policing*; 2) Rellen en massabijeenkomsten; 3) Dagelijks politiewerk; 4) Dark Web; 5) *Trolling* en; 6) Innovatieve marktoplossingen.
Meer informatie over MEDI@4SEC is te vinden op de **projectwebsite**. Hier zijn ook de volledige onderzoeksrapporten te downloaden zodra deze openbaar zijn.

Carlijn Broekman, Arnout de Vries en Marcel van Berlo zijn werkzaam bij TNO. Zij zijn bereikbaar voor vragen en discussie via e-mail: carlijn.broekman(at)tno.nl, arnout.devries(at)tno.nl en marcel.vanberlo(at)tno.nl.