Tegenhouden in cyberspace

Harmen Aalbers
is operationeel specialist bij de Regionale Eenheid Oost-Nederland.

Voor de zoveelste keer in de afgelopen decennia werd dit jaar de noodklok geluid over de oplossingspercentages en kwaliteit van de opsporing. Ook in cyberspace is het geen sinecure om tot succesvolle opsporing en vervolging van de dader(s) te komen. In mijn masterthesis[1] zoek ik naar alternatieven en verken ik de mogelijkheden voor tegenhouden/verstoren door gebruik van handhavingsmiddelen in cyberspace.

Voor het uitoefenen van de politietaak is de Nederlandse politie bevoegd om geweldsmiddelen en vrijheidsbeperkende middelen toe te passen (Politiewet 2012, artikel 7). Er is dan ook een keur aan deze middelen beschikbaar: de handboeien, de wapenstok, de pepperspray, het pistool, de politiehond et cetera. Het lijkt erop dat er voor elke situatie waarin het geweldloze station gepasseerd is wel een geschikt middel voorhanden is. Dit stelt de politie in staat om te voldoen aan de twee belangrijkste eisen bij geweldgebruik: proportionaliteit en subsidiariteit.

Als het gaat om geweldsmiddelen en vrijheidsbeperkende middelen lijkt het er dus op dat er een redelijke balans is gevonden tussen mogelijke situaties en voorhanden middelen. Het heeft echter lang geduurd voordat dit zover was. Tot aan het begin van de 20e eeuw was er bijvoorbeeld nog een grotere rol weggelegd voor het leger als het ging om openbare-ordehandhaving. Twee voorbeelden die dit goed illustreren zijn het Palingoproer en het Aardappeloproer. Het eerste vond plaats in 1886 in de Jordaan, in een tijd van groeiende ontevredenheid over werk- en leefomstandigheden. De rellen begonnen toen het verboden spel palingtrekken werd gespeeld en de politie het wilde beëindigen. Uiteindelijk werden politiemensen met stenen, bloempotten en stukken metaal bekogeld. Zij konden de situatie niet aan en de Mobiele Eenheid bestond destijds nog niet. Daarom werd de hulp van het leger ingeroepen. Cavalerie, infanterie, huzaren en mariniers arriveerden in de smalle straatjes en hebben daar flink huisgehouden, wat resulteerde in 26 doden en vele gewonden (Van der Wal, 2003, pp. 164-172).

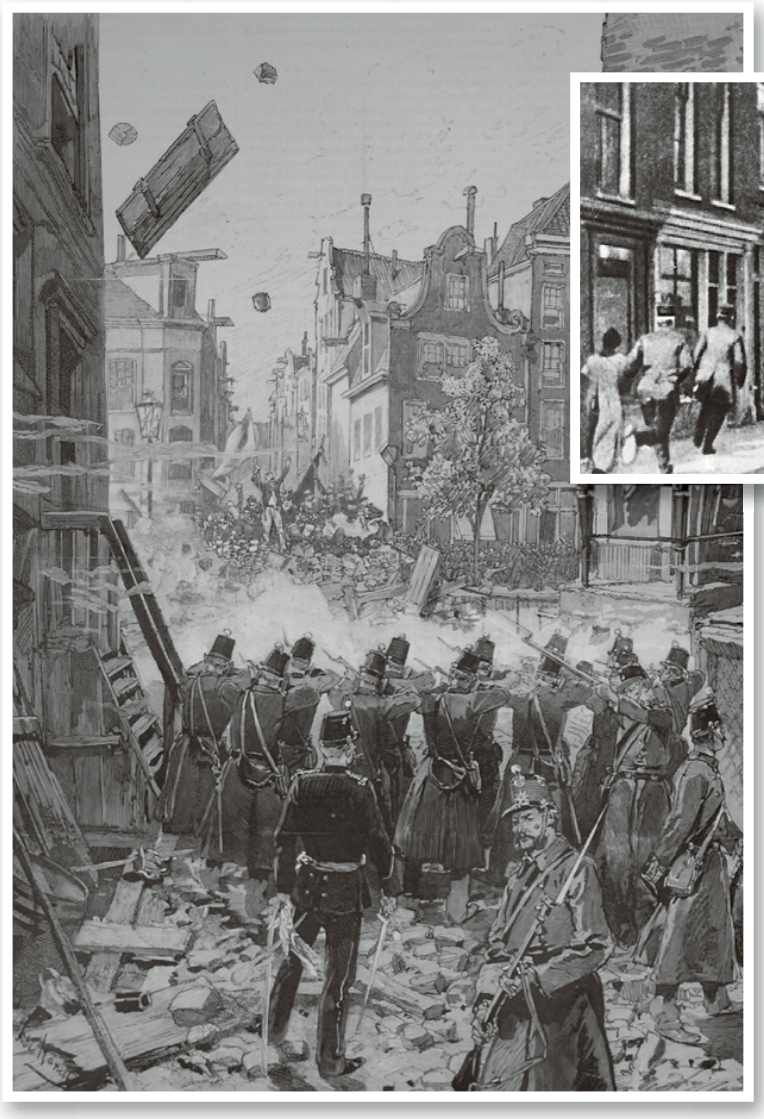
Het Aardappeloproer, dat plaatsvond tijdens een hongersnood in 1917, begon met plundering van voedsel en aardappelopslagplaatsen. De politie vroeg wederom om militaire bijstand. Ook dit incident leidde tot doden en gewonden (Van der Wal, 2003, pp. 274-277). Rond die tijd richtte de politie de voorlopers van de ME op, zoals de karabijnbrigades. Na de watersnoodramp werd de Mobiele Eenheid in het leven geroepen, die verder geprofessionaliseerd is na de heftige krakersrellen in de jaren '70 en '80. De huidige ME stelt de politie in staat om zelf adequaat op te kunnen treden bij openbare ordeverstoring en is niet meer weg te denken uit het gamma van geweldsmiddelen.

Een ander voorbeeld dat de lange geschiedenis en de verandering van geweldgebruik illustreert is het politiekoppel. Een simpel object zou je zeggen, maar de enorme hoeveelheid aan veranderingen die het heeft ondergaan bewijzen het tegendeel. In de depots van het politiemuseum bevinden zich honderden verschillende modellen (Meershoek, 2012, p. 2). Dit herinnert ons eraan dat het aantal en het type geweldsmiddelen waarover de politie beschikt niet iets statisch is: ze komen, ze gaan, en ze veranderen.

> ***» Een goede balans in handhavingsmiddelen op straat was er niet zo snel***

Cyberspace is hier, criminaliteit ook

Cyberspace (waaronder het internet valt) speelt tegenwoordig een centrale rol in ons leven. Dit geldt des te meer voor jongere generaties, die praktisch altijd online zijn. Het cyberdomein wordt in de Nationale Cybersecurity Strategie 2 (2013) omschreven als: *'het conglomeraat van ICT-middelen en -diensten welke alle entiteiten bevat die digitaal verbonden (kunnen) zijn, zowel permanente als tijdelijke of plaatselijke verbindingen, evenals de gegevens (o.a. data, programmacode, informatie) die zich in dit domein bevinden, waarbij geen geografische beperkingen zijn gesteld.'*



Het Palingoproer (1886) en het Aardappeloproer (1917): onmachtige politie riep de hulp in van het leger.

Ook de manier waarop we consumeren en zakendoen verandert hierdoor ingrijpend. Traditionele sectoren worden overbodig gemaakt door online leveranciers van producten en diensten en het aandeel van webwinkels zal nog verder groeien. Daarnaast staan steeds meer van onze spullen in verbinding met het internet, van thermostaten tot deursloten tot zelfrijdende auto's. We gaan richting een kantelpunt waar het aantal en de impact van onze acties in cyberspace even belangrijk worden als onze acties in de fysieke ruimte, of zelfs belangrijker.

De criminaliteit verschuift hierin mee. De schade en het aantal slachtoffers door cybercrime en gedigitaliseerde criminaliteit in Nederland is substantieel en groeiende (Deloitte, 2016; Domenie, Leukfeldt, van Wilsem, Jansen & Stol, 2013). Een van de manieren om iets te doen tegen deze vormen van criminaliteit is opsporing en vervolging op basis van het Wetboek van Strafvordering. Maar dat is lastig in cyberspace.

Moeizame opsporing en vervolging

Het uiteindelijke doel van opsporing en vervolging is het koppelen van een (fysieke) persoon aan een misdrijf om deze voor de rechter te brengen. Uiteindelijk moet er iemand van vlees en bloed in het strafbankje komen te zitten. Maar er zijn legio manieren om de koppeling tussen digitale misdrijven en de fysieke persoon die achter de knoppen zit te belemmeren. Dat zijn bijvoorbeeld The Onion Router (TOR), een techniek die door onder meer encryptie een internetverbinding anonimiseert, en het Virtual Private Network (VPN), een andere techniek om een internetverbinding te anonimiseren, waarbij je als het ware via je VPN-aanbieder het internet op gaat.

Behalve van encryptie (versleuteling van devices en data), kan er gebruik worden gemaakt van IP/DNS-spoofing (het vervalsen van afzenderadressen), bulletproof hosting (webhosting providers die hun uiterste best doen om onder bijvoorbeeld vorderingen en beslaglegging uit te komen) en Tails (een besturingssysteem dat van een USB-stick kan worden gedraaid om geen sporen achter te laten) (Brunner, 2015). En zo zijn er nog meer trucjes die de slimmere criminelen in cyberspace gebruiken om onder de radar te blijven.

Om een beeld van de opsporingspraktijk te krijgen werd een enquête gehouden onder medewerkers van het Team High Tech Crime van de Landelijke Recherche met de vraag wat de grootste uitdagingen zijn bij het opsporen van daders van (D)DoS aanvallen en illegale handel op TOR hidden services. Bij de eerste bleken dat vooral lokalisering van de aanvaller in cyberspace en het ontbreken van sporen en logging (het bewaren van verbindingsgegevens) te zijn. Als het gaat om TOR werd met name de fysieke lokalisering van de hidden service en de identificatie van kopers en verkopers genoemd als voornaamste struikelblok. Iedereen uit de (cyber)opsporingspraktijk kent waarschijnlijk wel voorbeelden van cybercriminelen die (lang) ongestoord hun gang konden gaan.

Andere manieren

Terwijl de politie alleen maar méér met cybercrime te maken krijgt, is opsporing in cyberspace in veel gevallen dus lastig. Maar wanneer het achterhalen van een identiteit ter vervolging niet lukt, kan op andere manieren worden getracht misdaad in cyberspace te bestrijden. Bijvoorbeeld door tegenhouden/verstoren. Die tactiek werd voor het eerst beschreven in de notitie *Tegenhouden Troef*, in opdracht van de toenmalige Raad van Hoofdcommissarissen (Projectgroep Opsporing-2, 2003). De auteurs definiëren tegenhouden als: *'het zodanig beïnvloeden van gedrag en van omstandigheden, dat criminaliteit of andere inbreuken op de veiligheid en de maatschappelijke integriteit worden voorkomen.'*

Het doel is niet iemand voor de rechter te brengen, maar de verstoring van het criminele proces. Niet alleen heimelijk, maar zeker ook openlijk. De politie heeft in cyberspace echter niet de beschikking over de gewelds- en vrijheidsbeperkende middelen zoals die in de inleiding werden beschreven; er is geen digitaal politiekoppel met equivalenten van handboeien, pepperspray en pistool. Om succesvol te kunnen tegenhouden en verstoren zijn die wel vereist. De vraag is: kan dit op basis van bestaande bevoegdheden en met welke middelen?

Handhavingsmiddelen in cyberspace?

Zo formuleerde ik de onderzoeksvraag in mijn thesis: *Hoe kan de bevoegdheid voor het gebruik van geweld van de Nederlandse politie worden vertaald naar cyberspace, wat zijn potentiële handhavingsmiddelen in cyberspace, en welke mogelijkheden en beperkingen brengen deze met zich mee vanuit een juridisch, ethisch en maatschappelijk oogpunt?* Er is hier bewust voor de term 'handhavingsmiddelen' in plaats van 'geweldsmiddelen en vrijheidsbeperkende middelen' gekozen omdat niet alle mogelijke middelen die ter verstoring kunnen worden ingezet per definitie geweld of een beperking van de vrijheid opleveren.

De onderzoeksvraag en deelvragen die eruit voortkwamen zijn beantwoord aan de hand van literatuuronderzoek, een enquête en 14 diepte-interviews (semi-gestructureerd) met toonaangevende experts uit verschillende relevante vakgebieden (technisch, juridisch, ethisch/maatschappelijk) en uit zowel de publieke als private sector.

'Zaken' of niet?

De eerste vraag die beantwoord dient te worden betreft de bevoegdheid voor het gebruik van geweldsmiddelen en vrijheidsbeperkende middelen: hoe kunnen deze worden vertaald naar handhavingsmiddelen in cyberspace? De bevoegdheid is vastgelegd in artikel 7 van de Politiewet: *'De ambtenaar van politie (…) is bevoegd in de rechtmatige uitoefening van zijn bediening geweld of vrijheidsbeperkende middelen te gebruiken, wanneer het daarmee beoogde doel dit, mede gelet op de aan het gebruik hiervan verbonden gevaren, rechtvaardigt en dat doel niet op een andere wijze kan worden bereikt.'* Wat onder geweld wordt verstaan wordt gedefinieerd in de Ambtsinstructie, namelijk: *'elke dwangmatige kracht van meer dan geringe betekenis uitgeoefend op personen of zaken'*.

De vraag is nu of de onderdelen waaruit cyberspace bestaat gezien kunnen worden als 'zaken' waarop de politie geweld kan uitoefenen. Daarom werd de volgende nulhypothese geformuleerd: *De gegevens die zich in cyberspace bevinden (o.a. data, programmacode, informatie) kunnen worden gezien als zaken.*

Aangezien dit niet in de bovenstaande wetten wordt beschreven, is gekeken naar uitspraken van de Hoge Raad. In een zaak uit 1996 kwam deze tot het oordeel dat data niet als 'enig goed' gezien kunnen worden. De zaak betrof verduistering van computerschijven/harde schijven met daarop gegevens van de werkgever, die de verdachte zich had toegeëigend. De rechters kwamen destijds tot de conclusie dat de schijf zelf als 'enig goed' gezien kon worden, maar de data op de schijf niet. De motivatie hiervoor: *'van een 'goed' moet als een wezenlijke eigenschap worden beschouwd dat degene die de feitelijke macht daarover heeft deze noodzakelijkerwijze verliest indien een ander zich de feitelijke macht erover verschaft. Computergegevens ontberen deze eigenschap.'* (Hoge Raad, 3 December 1996, NJ 1997/574, p. 3093).

Runescape

Meer dan 15 jaar later, in het 'Runescape-arrest', velde de Hoge Raad een ander oordeel. In deze zaak werd een virtueel computerkarakter (avatar) van het slachtoffer gestolen en werden de daders veroordeeld voor diefstal van enig goed. Ter motivatie gaven de rechters onder andere aan dat gaandeweg in jurisprudentie het economisch waardebegrip steeds verder gerelativeerd en gesubjectiveerd is, waarbij vooral de waarde van het goed voor de bezitter ervan relevant is. Ook stelden zij dat *'als gevolg van de digitalisering van de maatschappij een virtuele realiteit is ontstaan, die niet in alle opzichten kan worden afgedaan als louter illusie, ten aanzien waarvan het plegen van strafbare feiten niet mogelijk*

zou zijn.' (Hoge Raad, 31 January 2012, ECLI: NL: HR: 2012: BQ9251).

De uitspraak is niet onomstreden. Zo plaatst Koops (2014) hier kanttekeningen bij en geeft aan dat deze de deur opent naar een erg casuïstische benadering van de vraag of bepaalde gegevens zich als 'goed' of als 'gegeven' gedragen. Ook in het wetsvoorstel Computercriminaliteit III (2015) wordt ondanks deze uitspraak de keuze gemaakt om gegevens begripsmatig afzonderlijk te behandelen en niet gelijk te stellen aan een 'goed'. In de context van dit onderzoek is het tevens de vraag of de betekenis van de term 'zaken' uit de definitie van geweld in de Ambtsinstructie gelijk te stellen is aan de betekenis van de term 'enig goed' in de zin van artikel 310 Sr, aangezien bovenstaande uitspraken van de Hoge Raad beide in het kader van laatstgenoemde zijn gedaan.

De discussie is onvoltooid. Desalniettemin is de uitspraak in het Runescape-arrest de laatste die een dergelijk orgaan hierover heeft gedaan. Om die reden is de nulhypothese vooralsnog aangenomen en is verdergegaan met deze verkenning.

Computercriminaliteit III volstaat niet

Bij de overweging om handhavingsmiddelen in cyberspace te gaan gebruiken komt een veelheid aan verdere juridische vraagstukken kijken. Een eerste voor de hand liggende vraag is: hoe ga je om met andere jurisdicties en mogelijke soevereiniteitsschending? Aangezien een groot deel van de criminaliteit in cyberspace haar oorsprong heeft in het buitenland, is de kans zeer aanwezig dat potentiële doelwitten zich op plekken bevinden waar de Nederlandse politie geen rechtsmacht heeft. Dit vraagstuk is zo veelomvattend dat beantwoording ervan in de thesis er geen recht aan zou doen. Om die reden is het opzij gelegd en heb ik me gericht op de situatie dat handhavingsmiddelen binnen de Nederlandse landsgrenzen worden toegepast.

Daarnaast zijn er toepassingsmogelijkheden denkbaar met betrekking tot TOR hidden services, waarvan het in eerste instantie onduidelijk is waar de rechtsmacht ligt. Zou de huidige wetgeving voldoende juridische basis bieden om dergelijke middelen in cyberspace toe te passen of is er een wetswijziging nodig? Veel respondenten verwezen hierbij naar de voorgestelde Wet Computercriminaliteit III, die de bevoegdheid bevat om op afstand binnen te dringen in een geautomatiseerd werk, ook wel het 'hackvoorstel' genoemd.

Maar interviews met juristen gespecialiseerd op dit terrein wijzen uit dat bevoegdheden uit het Wetboek van Strafvordering, waar de wet toe behoort, enkel toegepast kunnen worden om bewijs te verzamelen in een opsporingsonderzoek ter vervolging van een persoon. Verstoren/tegenhouden kan een tweede doel zijn, maar strafvorderingsbevoegdheden mogen niet alleen daartoe worden ingezet. Dit zou een 'détournement de pouvoir' betekenen, oftewel het gebruiken van bevoegdheden voor andere doeleinden dan waarvoor deze zijn gegeven.

Er zal dus naar een andere juridische basis moeten worden gezocht. Een mogelijke oplossing is het toepassen van handhavingsmiddelen op basis van artikel 3 van de Politiewet, de politietaak. Dit zou echter niet in alle gevallen kunnen. In het Zwolsman-arrest (Hoge Raad 19-12-1995, NJ 1996, 249) heeft de Hoge Raad vastgesteld dat de politietaak enkel bij een 'beperkte' inbreuk op de persoonlijke levenssfeer een toereikende wettelijke grondslag biedt. Er dient dus per handhavingsmiddel te worden bepaald in hoeverre er kan worden gesproken van een 'beperkte' inbreuk om ze te kunnen inzetten op basis van Politiewet artikel 3.

In de gevallen dat de inbreuk groter is, zal aparte wetgeving vereist zijn, conform het legaliteitsprincipe. Uiteindelijk zal dat ook, aldus een aantal respondenten, een betere en nettere oplossing zijn. Er kan dan worden gedacht aan uitbreiding van artikel 7 van de Politiewet en de Ambtsinstructie. Aangezien dergelijke aanpassingen heel wat voeten in de aarde hebben (zie wetsvoorstel Computercriminaliteit III), is het verstandig om hier op tijd over na te denken.

Heimelijk of opvallend

Naast juridische aspecten kleven er ook ethische en maatschappelijke vraagstukken aan dit thema. Er zal moeten worden nagedacht over de impact die dit soort bevoegdheden kunnen hebben op ons dagelijkse leven en op de maatschappij. Het risico bestaat dat mensen bij het horen van de woorden 'handhavingsmiddelen voor de politie in cyberspace' negatief reageren in de trant van: 'moet de politie nu nog meer bevoegdheden krijgen, heeft de sterke arm der wet er nog niet genoeg?'

Er zullen altijd tegenstanders zijn van uitbreiding van politiebevoegdheden. Maar de vraag is allereerst of dit niet meer als een verschuiving dan als een uitbreiding moet worden gezien. Als iedereen, criminelen incluis, zijn of haar digitale identiteit verkent, waarom zou de politie dat dan niet mogen doen?

Daarnaast moet de discussie in zijn bredere context bezien worden: wat zijn de alternatieven en wat is de balans tussen heimelijke opsporing en opvallende handhaving in

» *Voor verdergaande handhaving zal aparte wetgeving zijn vereist*

Foto: Novum RegioFoto

cyberspace? In de fysieke ruimte kennen we enerzijds de opvallende surveillanceauto en geüniformeerde agent, en anderzijds de onopvallende auto en rechercheur in burger. Soms wordt gekozen voor het eerste, in een ander geval voor het tweede.

Ook in cyberspace kun je zowel opvallend als onopvallend te werk gaan. Het is de vraag of beide vormen daar in balans zijn. Wanneer oplossingen enkel worden gezocht in het uitbreiden van onopvallende opsporingsbevoegdheden, kan dit eveneens onwenselijke maatschappelijke effecten hebben, bijvoorbeeld op het gebied van privacy. Als we kijken naar het sentiment in de maatschappij en binnen het bedrijfsleven (zie ook de zaak Apple vs. FBI over de te 'kraken' iPhone) hieromtrent, kan het interessant zijn om eens naar opvallend en transparant politieoptreden in cyberspace te kijken.

Een eerste stap

Zoals gezegd bestond een deel van dit onderzoek uit diepte-interviews met experts. Zij zijn ook bevraagd over hun ideeën bij handhavingsmiddelen in cyberspace. Een meerderheid van hen gaf hierbij aan een politiebevoegdheid voor het toepassen van dergelijke middelen in cyberspace een logische volgende stap te vinden. De meningen over hoe deze er uit kunnen zien liepen uiteen, er werden veel verschillende methoden genoemd. Om uiteindelijk een inschatting te kunnen maken van de potentie van genoemde handhavingsmiddelen, is een raamwerk samengesteld met attributen die van belang zijn voor dergelijke middelen. Deze werd afgeleid uit zowel literatuur als interviews. Het gaat om:

Proportionaliteit		**Legaliteit**		**Legitimiteit**	**Praktische bruikbaarheid**	
Nevenschade	Voorspelbaarheid	Inbreuk op privacy	Schending van vrijheid van meningsuiting	Afhankelijkheid van derden	Uitvoerbaarheid	Effectiviteit

Tabel 1.

Slechte scores op bepaalde attributen leidden tot uitsluiting van een middel, zoals een sterke afhankelijkheid van derden. In dit onderzoek is namelijk nadrukkelijk gezocht naar politiële handhavingsmiddelen, voor aan een spreekwoordelijk 'digitaal politiekoppel'. Wanneer een middel alleen door bijvoorbeeld internetproviders kan worden uitgevoerd is daar geen sprake van.

Op een aantal attributen, zoals een zekere inbreuk op privacy of schending van vrijheid van meningsuiting leidden slechte scores niet direct tot uitsluiting. Wel behoeven die middelen extra bedachtzaamheid. Het is juridisch gezien lastiger om bevoegdheid voor deze middelen te krijgen en zij vereisen extra waarborgen. Deze eerste verkenning leidde tot de lijst in tabel 2 van potentiële handhavingsmiddelen in cyberspace. De lijst is niet uitputtend, dit onderzoek is een eerste verkenning. Het laat wel zien in welke richtingen kan worden gedacht.

Verder onderzoek

Een aantal punten vereist nog verdere studie. Het zou allereerst, gezien het internationale karakter van criminaliteit in cyberspace, nuttig zijn om uit te zoeken hoe dit soort handhavingsmiddelen zich verhouden tot landsgrenzen en mogelijke schendingen van soevereiniteit. Waar ligt de rechtsmacht, zijn er überhaupt mogelijkheden om deze middelen in te zetten buiten de Nederlandse grens en welke vraagstukken omtrent internationale politiesamenwerking brengt dit met zich mee?

Ook zou nader onderzoek naar de effectiviteit van de potentiële cyber-handhavingsmiddelen in de praktijk nuttig zijn, met name de verstoring van criminele data(verzameling) en de (D)DoS aanval op hoge netwerklaag, aangezien deze nog relatief onbekend zijn. Ook de potentie van versleuteling om data te 'bevriezen' als politie-handhavingsmiddel zou verder verkend kunnen worden.

Een laatste punt dat aandacht vereist is de cybersecurity van de politie zelf. Voordat er wordt begonnen met de daadwerkelijke inzet van dit soort middelen, is het raadzaam een assessment uit te voeren naar de extra risico's op vergeldingsaanvallen en mogelijke extra eisen aan de beveiliging van de politie-infrastructuur.

Handhavingsmiddel:	**Beschrijving:**	**Geschatte schending van grondrechten:**
Verstoring van criminele data(verzameling)	Het criminele proces verstoren door loze gegevens te versturen of te plaatsen waardoor het niet meer duidelijk is wat echt is en wat niet. Voorbeeld: extreem veel reacties op phishingmails versturen waardoor het proces voor de phisher onwerkbaar wordt.	Laag
(D)DoS aanval op hoge netwerklaag	Een techniek die processen in een hogere netwerklaag overbelast waarmee getracht wordt een website of webservice onbruikbaar te maken zonder daarbij veel nevenschade te veroorzaken. Voorbeeld: het zodanig vaak gebruiken van een inlogprocedure dat deze het begeeft.	
Hack i.c.m. uitschakelen/versleutelen/vernietigen (niet te verwarren met 'hackvoorstel' in computercriminaliteit III t.b.v. opsporing)	Het binnentreden van een computersysteem zonder fysieke toegang ertoe en zonder toestemming van de eigenaar om vervolgens criminele processen of data uit te schakelen, te versleutelen of te vernietigen. Voorbeeld: het hacken van een criminele website en vernietigen van content, en plaatsen van politielogo's waar voorheen foto's stonden.	
WiFi/UMTS-internetuitschakeling	Het verstoren (jammen) van de frequentie van het WiFi-of UMTS-signaal om in een bepaalde locatie gebruik van internet onmogelijk te maken. Voorbeeld: het jammen van internet tijdens een gijzeling, zodat gijzelnemers niet alles via internet kunnen volgen.	Hoog

Tabel 2. Potentiële handhavingsmiddelen in cyberspace.

De tijd is rijp

Zullen we in de toekomst ook in cyberspace situaties gaan zien waarvoor de politie niet voldoende toegerust is? De tijd zal het leren. Het zou in ieder geval verstandig zijn om de discussie over handhavingsmiddelen in cyberspace zo snel mogelijk te starten. Dat geldt voor partijen binnen het veiligheidsdomein, maar zeker ook voor het parlement, want de ontwikkelingen in cyberspace gaan snel en aanpassing van wetgeving zelden. De politie is overigens maar een van de vele spelers in het veilig houden van cyberspace. Ook andere publieke én private partijen moeten betrokken worden bij deze discussie.

Dus zien we cyberspace vooral als een bak met informatie waar we in kunnen graaien om strafbare feiten op te sporen, of zien we het als een verlengstuk van de fysieke ruimte, waar daadwerkelijke handhaving van de rechtsorde vereist is en hulp dient te worden verleend aan hen die deze behoeven? Na het schrijven van deze masterthesis pleit ik voor het laatste. «

Literatuur

Brunner, G. (2015). *The ultimate guide to staying anonymous and protecting your privacy online.*

Deloitte (2016). *Cyber Value at Risk in the Netherlands. 10 billion value lost through cyber risk in The Netherlands.*

Domenie, M.M.L., Leukfeldt, E.R., van Wilsem, J.A., Jansen, J. & Stol, W. Ph. (2013). *Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit*. Den Haag: Boom Lemma.

Koops, E. J. (2014). Cybercriminaliteit. In S. van der Hof, A. R. Lodder, & G. J. Zwenne (Eds.), *Recht en computer,* zesde druk. (pp. 213-241). Deventer: Kluwer

Meershoek, A.J.J. (2012). De politiekoppel: vormgever van het geweldsmonopolie. In: P.W. Tops (Ed.), *Inleiding politiekunde (pp. 71-80)*. Apeldoorn: Politieacademie.

Naeyé, J. (2005). *Niet zonder slag of stoot. De geweldsbevoegdheid en doorzettingskracht van de Nederlandse politie*. Zeist: Kerkebosch.

Projectgroep Opsporing-2, Raad van Hoofdcommissarissen (2003). *Tegenhouden troef. Een nadere verkenning van Tegenhouden als alternatieve strategie van misdaadbestrijding.*

Rijksoverheid (2013). *Nationale Cybersecurity Strategie 2. Van bewust naar bekwaam.*

Rijksoverheid (2015). *Wetsvoorstel Computercriminaliteit 3. Memorie van Toelichting.*

Wal, R. van der (2003). *Of geweld zal worden gebruikt! Militaire bijstand bij de handhaving en het herstel van de openbare orde 1840-1920.* Hilversum: Verloren.

Noot

Master of Science in Policing. *Enforcing the Law in Cyberspace. Exploring Cyber Enforcement Capabilities for the Police in the Netherlands*.