ARTIKEL

Normen in cyberspace: van belang voor landen én bedrijven

Jochem de Groot

Cyberaanvallen, cyberspionage, digitaal terrorisme: de inzet van digitale middelen voor het bereiken van een maatschappelijk of economisch ontwrichtend effect is een volwassen fenomeen geworden. Digitale dreiging bestaat in allerlei verschijningsvormen en wordt inmiddels veroorzaakt door de meest uiteenlopende actoren. Hoe weren we ons daartegen? In de discussies over cybersecuritybeleid is naast landen een belangrijke rol weggelegd voor het (ICT-)bedrijfsleven. Zo heeft Microsoft normen ontwikkeld voor zowel staten als wereldwijd opererende ICT-bedrijven die een kader bieden voor hun handelingsruimte in cyberspace.

De Amerikaanse presidentsverkiezingen van 2016 zullen om velerlei redenen nog lang in het geheugen liggen. Op het gebied van cybersecurity was met name het aanhoudende nieuws over (mogelijk politiek gemotiveerde) cyberaanvallen uit Rusland in het Amerikaanse democratische proces opvallend. Hoewel berichten over de inmenging van Russische geheime diensten bij de Democratic National Committee, de Democratic Congressional Campaign Committee en de emails van John Podesta – Hillary Clinton's campagnemanager – grotendeels onbevestigd en onbewijsbaar zijn gebleven, hadden ze onmiskenbaar invloed op de dynamiek van de verkiezingsstrijd tussen Trump en Clinton en hun opstelling tegenover Rusland.

Cyberaanvallen, cyberspionage, digitaal terrorisme: de inzet van digitale middelen voor het bereiken van een maatschappelijk of economisch ontwrichtend effect – al dan niet uitgevoerd door staten – is een volwassen fenomeen geworden. Van de regelmatig aangehaalde cyberaanvallen op Estland in 2007 tot de hack van Sony in 2014, mogelijk gemotiveerd om te voorkomen dat een kritische film over Kim-Jong-Il zou worden uitgebracht: digitale dreiging bestaat in allerlei verschijningsvormen. Bovendien wordt die dreiging inmiddels veroorzaakt door de meest uiteenlopende actoren, van staten (door de krijgsmacht, veiligheidsdiensten of politie en justitie) tot (internationale) criminele organisaties, bedrijfsspionnen, individuele hackers of professioneel georganiseerde hackerscollectieven.

Zoals vorig jaar al door Sico van der Meer in de Internationale Spectator uiteengezet,[1] zijn cyberspionage en cybercriminaliteit voor het sterk gedigitaliseerde Nederland grote dreigingen geworden, en moet daarnaast de impact van cyberterrorisme en cyberoorlogsvoering niet worden onderschat. Om Nederland voor al deze dreigingen weerbaarder te maken, maakt Van der Meer onderscheid tussen *passieve* afschrikking, in de vorm van continue evoluerende digitale beveiliging, en *actieve* afschrikking, waarbij mogelijke vergelding van aanvallers in het vooruitzicht wordt gesteld.

Het kabinet Rutte-II heeft de afgelopen jaren laten zien op beide vlakken goed uitgerust te willen zijn. Het in 2014 door minister Hennis van Defensie geopende Cyber Commando belichaamt de ambitie van de Nederlandse regering om in cyberspace steviger te kunnen optreden. Zowel defensief, door het op orde hebben van beveiliging tegen aanvallen en spionage, maar ook offensief, door "digitale systemen van tegenstanders aan [te] vallen, manipuleren of uitschakelen. Tegenstanders [daarbij] kunnen andere landen zijn, maar ook (terroristische) organisaties of hackers."[2]

Na de Tweede Kamer-verkiezingen in maart 2017 zal moeten blijken in hoeverre een nieuwe regering verder zal willen investeren in dergelijke cybercapaciteit, maar een blik op een aantal verkiezingsprogramma's van politieke partijen maakt duidelijk dat het onderwerp *top-of-mind* is. Zo geeft de VVD aan dat "cybercapaciteiten (zowel offensief al defensief) onmisbaar zijn in de conflicten van vandaag en morgen"[3] en markeert D66 naast de drie klassieke pijlers van defensie – landmacht, marine en luchtmacht – "een nieuw aspect.... digitale oorlogsvoering (cyberwarfare) en.[….].wil dat ons land in staat blijft deel te nemen in het hoogste geweldsspectrum."[4]

Spelregels in cyberspace

De opbouw door Nederland van expertise, mankracht en ervaring voor zowel defensieve als offensieve handelingen in het digitale domein, gaat gepaard met complexe vraagstukken rond wat daarbij toelaatbaar is: niet alleen tegenover andere landen – bondgenoten of derden – maar ook richting bedrijven, organisaties, burgers en andere niet-statelijke actoren. Naast investeringen in de eigen cybercapaciteiten – in Nederland behalve bij Defensie ook bijvoorbeeld in het Nationaal Cybersecurity Centrum en haar strategie – heeft de regering de afgelopen jaren ook laten zien een pro-actieve rol te willen spelen bij het stimuleren van discussies over welke kaders zowel staten als niet-statelijke actoren ter hand kunnen nemen om hun gedrag in het cyberdomein te gidsen.

> De aanjagende rol die het kabinet-Rutte heeft genomen in discussies over cybersecuritybeleid, is prijzenswaardig

Zo zette Nederland als organisator van de *Global Conference on Cyberspace* in april 2015 in Den Haag – waar minsters, beleidsmakers, experts, bedrijven, wetenschappers en NGO's uit tientallen landen bij elkaar kwamen om te praten over de balans tussen veiligheid, vrijheid en economische kansen op internet – het onderwerp van de nut en noodzaak van normen in cyberspace hoog op de agenda.[5] Ook in Europees kader nam Nederland op dit vlak een voortrekkersrol op, door als EU-voorzitter tijdens de eerste helft van 2016 gemeenschappelijk Europees cybersecuritybeleid als een van zijn prioriteiten te bestempelen, waarvoor onder meer een grote cybersecurity-conferentie[6] in Amsterdam werd georganiseerd.

© Flickr / Ministerie van Buitenlandse Zaken

Minister Koenders tijdens de Global Conference on Cyberspace in april 2015.

De aanjagende rol die het kabinet heeft genomen in discussies over cybersecuritybeleid is prijzenswaardig: de geloofwaardigheid van Nederland op dit terrein – met zijn ijzersterke digitale infrastructuur, technologie-gebaseerde groeiambities en ruime academische en beleidsexpertise – is groot, waardoor er internationaal op deze thematiek naar Nederland wordt geluisterd. Als middelgroot land op dit vlak kan Nederland bovendien zowel binnen de EU als daarbuiten een bemiddelende rol spelen om landen met afwijkende visies waar mogelijk wat meer op één lijn te krijgen.

Cybernormen volgens Microsoft

Toch is er niet alleen voor landen een belangrijke rol weggelegd in deze discussies. De ruggengraat van het internet en digitale infrastructuur in bredere zin wordt voor de overgrote meerderheid gevormd door het bedrijfsleven, en vrijwel alle incidenten in cyberspace vinden dan ook plaats op of met technologie in het bezit van marktpartijen. Zelfs als ICT-diensten niet het doel van aanvallen zijn, dan maakt de intrinsieke verbondenheid van het internet het alsnog uitdagend voor aanvallers om gericht of proportioneel te werk te gaan, waardoor de kans op nevenschade groot is.

Bovendien kijken overheden vaak meteen naar technologiebedrijven om na cyberaanvallen een helpende hand te bieden, omdat die bedrijven in veel gevallen als eerste verdediging kunnen bieden en kunnen reageren tijdens een cyberconflict. Voor bedrijven die consumenten, overheden en bedrijven online-diensten aanbieden – en er zijn er steeds minder die dat niet doen – is er dan ook in toenemende mate een belang om stevig te investeren in de beveiliging van die diensten om het vertrouwen van klanten in hun technologie te behouden en vergroten.

> De ruggengraat van het internet en de digitale infrastructuur in bredere zin wordt voor de overgrote meerderheid gevormd door het bedrijfsleven

Een wereldwijd opererend technologiebedrijf als Microsoft heeft naast het doen van continue miljardeninvesteringen in beveiligingsmaatregelen ook besloten actief deel te nemen aan internationale discussies over gedragingen van zowel overheden als bedrijven in cyberspace. Omdat dagelijks bijvoorbeeld wereldwijd duizenden cyberaanvallen op Microsoft-technologie gericht zijn of via Microsoft-technologie verlopen, zijn we door onze decennialange ervaringen wijzer geworden over wat wel werkt en wat niet, en over welke lessen daaruit te trekken zijn.

Die lessen zijn omgezet in advies aan overheden en andere bedrijven over welke uitgangpunten zij wat ons betreft moeten nemen om cyberconflicten wereldwijd zoveel als mogelijk in de hand te houden, of in ieder geval de impact daarvan zo veel mogelijk te beperken. Voor zowel staten als wereldwijd opererende ICT-bedrijven heeft Microsoft zes normen geïdentificeerd die een kader bieden voor hun handelingsruimte in cyberspace en uitgangspunten voor hun gedrag op het gebied van zowel defensieve als offensieve acties:

Cybersecurity-normen voor staten[7]

- Staten moeten ICT-bedrijven niet misbruiken om kwetsbaarheden (zogenoemde *backdoors*) uit te buiten of anderzijds actie ondernemen die het publieke vertrouwen in producten en diensten van die bedrijven ondermijnt.
- Staten moeten een duidelijk beleid voeren – gebaseerd op heldere uitgangspunten – voor het omgaan met kwetsbaarheden in producten en diensten, die ze direct aan ICT-bedrijven zullen doorgeven en niet zullen verzamelen, kopen, verkopen of uitbuiten.
- Staten moeten zich terughoudend opstellen bij de ontwikkeling van cyberwapens en erop toezien dat wapens die wel worden ontwikkeld beperkt, precies en eenmalig zijn.
- Staten moeten zich committeren aan nonproliferatie ten aanzien van cyberwapens.
- Staten moeten zich beperken bij de inzet van offensieve cyberoperaties om massa-incidenten zoveel als mogelijk te voorkomen.
- Staten moeten de inzet van de private sector om incidenten in cyberspace te ontdekken, in te perken en daarvan te herstellen, zoveel als mogelijk steunen.

Cybersecurity-normen voor wereldwijd opererende ICT-bedrijven[8]

Wereldwijd opererende ICT-bedrijven:

- moeten staten de veiligheid van commerciële, breed uitgerolde ICT-producten en diensten niet laten beïnvloeden.
- moeten zich strikt houden aan gecoordineerde onthulling (*disclosure*) van kwetsbaarheden in producten en diensten.
- moeten goed samenwerken om zich pro-actief te verdedigen tegen aanvallen door staten en de impact van eventuele aanvallen zo goed als mogelijk op te vangen.
- moeten niet handelen in cyberkwetsbaarheden voor offensieve doeleinden, noch moeten ze bedrijfsmodellen omarmen waarbij de proliferatie van cyberkwetsbaarheden voor offensieve doeleinden noodzakelijk is.

- moeten partijen in de publieke sector zoveel als mogelijk helpen om cyberincidenten te identificeren, voorkomen, erop te reageren en ervan te herstellen.
- moeten kwetsbaarheden zo snel als mogelijk repareren om ICT-gebruikers te beschermen, los van de oorzaak van de kwetsbaarheid of zijn motieven.

Beide sets normen zijn in aparte papers verder uitgewerkt, waarbij per norm is toegelicht op basis waarvan Microsoft tot de norm is gekomen en wat de praktische uitwerking daarvan zou kunnen zijn.

Kompas voor beleid

Microsoft heeft niet tot doel met deze normen een specifieke *niche* in internationale betrekkingen aan te jagen. Als bedrijf beseft Microsoft dat het veel tijd en energie zal kosten om van politieke normen richting juridisch bindende normen te bewegen, en dat sommige beleidsmakers onze voorstellen vooral meer als inspiratie zullen zien dan als daadwerkelijk realistisch. Toch vindt Microsoft het belangrijk om in deze fase een bijdrage aan het debat te leveren: historisch gezien zijn internationale normen vaak pas tot stand gekomen na zeer ingrijpende gebeurtenissen, waarna de internationale gemeenschap ging beseffen dat een bepaald soort activiteit – of dat nu het gebruik van chemische wapens of landmijnen betrof – niet langer acceptabel was.

© Flickr / Fabien Lavocat

'Overheden kijken vaak meteen naar technologiebedrijven om na cyberaanvallen een helpende hand te bieden'.

De doelstelling van Microsoft is daarom – hoe ambitieus ook – om op de lange termijn te voorkomen dat cyberconflicten het vertrouwen in technologie zullen gaan ondermijnen. Een alternatief is dat we ons ooit te laat zullen realiseren, zwaar getroffen door de fysieke impact van een cyberconflict, dat we te laat tot regels zijn gekomen. Cybersecurity-normen zullen leiden tot meer voorspelbaarheid, stabiliteit en veiligheid in de internationale gemeenschap,

en dus op minder kans op conflict. De bovengenoemde normen kunnen bovendien als kompas dienen voor zowel overheden als ICT-bedrijven in hun inventarisatie van mogelijke wet- en regelgeving of intern beleid over hun eigen gedrag in cyberspace.

Hoewel een gedegen, secuur proces tot het afspreken van normen een flinke uitdaging zal worden – zeker omdat demografische, politieke en economische veranderingen de houdbaarheid van ouderwetse samenwerkingsmodellen zullen verkorten – is Microsoft hoopvol gestemd dat door dialoog en lessen uit de dagelijkse praktijk sommige cybersecurity-normen op de lange termijn in internationale wetgeving kunnen worden vastgelegd en opgenomen in de bedrijfsvoering van ICT bedrijven. De afgelopen jaren zijn er meer dan genoeg voorbeelden geweest van cyberincidenten die hebben aangetoond dat een gebrek aan actie op dit vlak simpelweg niet langer acceptabel is.

Noten

[1]
Sico van der Meer, 'Digitale dreiging. Is afschrikking van cyberaanvallen mogelijk?', (2015) *Internationale Spectator* (https://www.internationalespectator.nl/pub/2015/4/digitale_dreiging_is_afschrikking_van_cyberaanvallen_mogelijk/).

[2]
Ministerie van Defensie, 'Cybercommando' (https://www.defensie.nl/onderwerpen/cyber-security/inhoud/cyber-commando).

[3]
VVD, 'Zeker Nederland. Concept-verkiezingsprogramma (https://secure.cdn.vellance.com/usmedia/vvd/uploaded/attachment-files/348.pdf) 2017-2021'.

[4]
D66, 'Concept-verkiezingsprogramma (https://verkiezingsprogramma.d66.nl/). Samen sterker – kansen voor iedereen'.

[5]
Global Conference on Cyberspace 2015 (http://www.gccs2015.com/gccs/all-about-gccs2015)

[6]
High Level Meeting Cyber Security (https://english.eu2016.nl/events/2016/05/12/high-level-meeting-on-cyber-security)

[7]
Jochem de Groot, 'Six Proposed Norms to Reduce Conflict in Cyberspace (https://blogs.microsoft.com/microsoftsecure/2015/01/20/six-proposed-norms/)'.

[8]

Microsoft, ‘From Articulation to Implementation: Enabling progress on cybersecurity norms (https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf)’.

Auteurs

Jochem de Groot
Director Corporate Affairs van Microsoft in de Benelux ▸
(https://blogs.microsoft.nl/author/jochemdegroot)