ARTIKEL

Cyberaanvallen: organisatie, besluitvorming en strategie

Isabelle Duyvesteyn

In een elektronisch steeds verder verknoopte wereld nemen risico's toe. Is Nederland in voldoende mate voorbereid op mogelijke cyberaanvallen? Er zijn in dit verband ten minste drie aspecten die thans zorgen baren: de manier waarop Nederland de organisatie tegen cyberaanvallen heeft ingericht; het besluitvormingsproces voorafgaand aan het extern handelen bij een cyberaanval; en de ratio en manier waarop die handelingen zouden moeten plaatsvinden, de strategie.

De term 'cyber' staat niet gelijk aan alleen het internet, zoals vaak wordt gedacht, maar omschrijft het geheel van de digitale omgeving (zowel fysiek als virtueel) waar electronisch wordt gecreëerd, georganiseerd en opgeslagen. Een cyberaanval is dus niet alleen gericht op een computer, meestal het directe aanvalsobject, maar ook op het netwerk waarmee de computer is verbonden, de informatie die daarbinnen te vinden is en het kritische proces waarmee ze samenhangen.

In een toonaangevende publicatie heeft Thomas Rid beargumenteerd dat cyberaanvallen voornamelijk de vorm hebben van spionage, subversie of sabotage, eerder dan oorlog.[1] De ernstigste vorm van sabotage van recente datum is de cyberaanval op het electriciteitsnet in Oekraïne. Op 23 december 2015 viel gedurende enkele uren de stroom uit, waardoor duizenden Oekraïners zonder elektriciteit zaten. In dit geval wist een cyberaanval fysieke schade toe te brengen, meer dan spionage en subversie tot nu toe hadden bereikt.

© Wikimedia Commons

'Toegenomen interconnectiviteit leidt tot een groter aantal zwakheden'.

Dit voorbeeld is zeker niet de eerste casus van een aanval op belangrijke infrastructuur in de context van een conventioneel interstatelijk conflict, in dit geval tussen Rusland en Oekraïne. Zware fysieke schade aan kritieke infrastructuur vormt thans wel een van de meest angstaanjagende uitingen van de mogelijkheden van cyberaanvallen. Hieronder zullen de drie sets van uitdagingen, zoals in de inleiding aangegeven, in het licht van deze recente praktijk nader worden geduid.

De organisatie

Op twee belangrijke plekken binnen de overheid zijn de Nederlandse componenten te vinden die een rol spelen in geval van een ernstige cyberaanval. Ten *eerste* is er het *Nationaal Cyber Security Centrum* (NCSC), dat als taak heeft de weerbaarheid te vergroten in geval van cyberaanvallen. Dit centrum valt onder de verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), en daarmee onder het Ministerie van Veiligheid en Justitie. Het belangrijkste onderdeel van het NCSC is het Computer Emergency Response Team (CERT), dat gericht is op het voorkomen en bestrijden van inbreuken op cyberveiligheid. Naast het NCSC is er een nationale cybersecurityraad, die onafhankelijk, gevraagd en ongevraagd advies geeft over cyberveiligheidsvraagstukken. In deze raad zitten naast vertegenwoordigers van de overheid, vertegenwoordigers van het bedrijfsleven en een aantal wetenschappers.

Ten *tweede* heeft het Ministerie van Defensie een *Defensie Cyber Commando*, sinds september 2014 operationeel en gericht op de cyber-component bij militaire operaties. Dit commando valt onder de CDS (commandant der strijdkrachten) en handelt op basis van een besluit van de regering; het richt zich expliciet op offensieve cyberoperaties in de context van een gewapend conflict; zo is het in staat de digitale systemen van tegenstanders, zowel staten als niet-statelijke actoren, te ontregelen, te manipuleren of uit te schakelen.

Deze organisatorische inbedding is zeker niet standaard. Andere westerse staten die zich op dit terrein organiseren, waaronder de meeste ons omringende landen, brengen deze capaciteiten veelal onder bij de inlichtingen- en veiligheidsdiensten. In de Verenigde Staten valt het Cyber Command onder de paraplu van de National Security Agency (NSA), de inlichtingendienst die zich richt op het onderscheppen van communicatie.

De eerste uitdaging is het grote contrast dat bestaat tussen deze organisatorische benadering in Nederland en de patronen van cyberaanvallen. Als we inderdaad het meest te vrezen hebben van grootschalige ontwrichting van onze kritieke infrastructuur, dan loont het de moeite naar dié actoren te kijken die over mogelijke capaciteiten beschikken om een dergelijke ontwrichting te veroorzaken. Patronen van cyberaanvallen laten tot nu toe een grote consistentie zien; naast criminele aanvallen is de meerderheid afkomstig van staten, in het bijzonder China, Rusland en Iran.[2] Het Cyber Security-beeld van 2016 signaleert een toegenomen dreiging van offensieve cyberaanvallen.[3] Ook het raffinement van de aanvallen wordt steeds groter.

Naar een geïntegreerde benadering

Deze trend staat in schril contrast tot de benadering van cyberveiligheid, dat bezien wordt vanuit bedreiging van de vitale infrastructuur en met name nationaal georganiseerd is. Ook de scheiding tussen de defensieve bescherming tegen bedreigingen van de infrastructuur bij Veiligheid en Justitie en de offensieve capaciteiten bij Defensie bevreemdt. Juist op dit terrein waar de nationale en internationale veiligheid zo dicht bij elkaar zitten, is het veel logischer de

schotten tussen de betrokken Ministeries van Veiligheid en Justitie, van Defensie en het Ministerie van Buitenlandse Zaken op te heffen en naar een werkelijk geïntegreerde benadering toe te werken.

Samenhangend met de vraag naar de positionering binnen de institutionele structuur dient gewezen te worden op de kwestie van competenties. Hoe worden bijvoorbeeld de capaciteiten van het Defensie Cyber Commando ingezet buiten de kaders van een regulier conflict of militaire operatie? Het ligt voor de hand dat, als Nederland besluit tot inzet van de gewapende macht, ook deze mogelijkheden daartoe behoren. Het is echter voorstelbaar, zelfs waarschijnlijk, dat er inbreuken plaatsvinden op onze kritieke infrastructuur wanneer er geen sprake is van een officiële Nederlandse operatie of een besluit tot interventie. Valt dit ook binnen de competenties van dit commando of draagt de NCTV dan primaire verantwoordelijkheid voor een probleem op het terrein van buitenlandse zaken? De organisatorische inbedding heeft dus niet alleen consequenties voor de inzet, maar ook voor de verantwoording.

De besluitvorming

Nederland

Wanneer Nederland in geval van een dreigende ontwrichtende aanval internationaal actief zou willen handelen en offensieve cyberwapens zou willen inzetten, moet de Nederlandse regering volgens de huidige regelgeving de zogenaamde artikel 100-procedure volgen.[4] Gebaseerd op artikel 100 van de Nederlandse grondwet stelt het kabinet de Tweede Kamer op de hoogte van het voornemen tot een bepaalde inzet. Staatsrechtelijk heeft de Tweede Kamer geen instemmingsrecht, maar naar ondertussen goed gebruik met precedent, stelt het kabinet de instemming van een meerderheid in de Tweede Kamer vaak als impliciete voorwaarde. De Kamer debatteert doorgaans op basis van het toetsingskader, een lijst met aandachtspunten die van belang zijn voor de inzet van de krijgsmacht; die aandachtspunten zijn o.a.: een helder mandaat; de juiste middelen; aandacht voor gender en het milieu; en alle andere opties moeten zijn uitgeput.

Dit is gewoonlijk een lang proces, waarin besluitvorming zijn beslag moet krijgen. De infrastructuur van Nederland zal dan naar alle waarschijnlijkheid al zijn platgelegd. Dit is het horror-scenario waar de cyber-pessimisten, zoals Richard Clarke, ons voor waarschuwen.[5] De vraag die dit oproept is in hoeverre onze besluitvormingsprocedures zijn toegeëigend voor de gestelde taken. We kunnen ervan uitgaan dat de snelheid waarmee cyberaanvallen kunnen plaatsvinden extreem hoog is, dat de doelen van deze aanvallen ook zeer secuur uitgezocht zijn en ons in de meest zwakke plekken kunnen en zullen raken. Het lijkt dan ook onverantwoord de besluitvorming op basis van deze processen te laten verlopen. De mogelijkheid tot zelfverdediging staat buiten kijf, maar in aanvalsscenario's waar het om milliseconden gaat, ligt het voor de hand na te denken over andere procedures.

De NAVO

Het internationale kader voor besluitvorming op dit terrein is de NAVO. Tijdens haar topontmoeting in Wales in 2014 heeft het bondgenootschap verklaard dat cyberaanvallen onder de wederzijdse bijstandsclausule vallen; een cyberaanval kan artikel 5 van het Verdrag van Washington activeren, net zoals een kinetische aanval dat kan doen. Deze verklaring versterkt de solidariteit in het bondgenootschap.

De vraag blijft echter of een cyberaanval ook als zodanig door de bondgenoten herkend en erkend zal worden. De meeste aanvallen die we tot nu toe ervaren hebben en die in de nabije toekomst worden verwacht – uitzonderingen daargelaten – hebben niet de dezelfde mate van geweld als die van conventionele aanvallen. Is de aanval dwingend en hard genoeg om artikel 5 te activeren? Een voorbeeld van het politieke geharrewar was de boodschap aan de Esten bij de aanvallen in 2007 om toch vooral niet artikel 5 aan te roepen. De ruimte voor interpretatie en discussie lijkt toe te nemen.

> De NAVO heeft in 2014 op haar topontmoeting in Wales verklaard dat cyberaanvallen onder de wederzijdse bijstandsclausule vallen

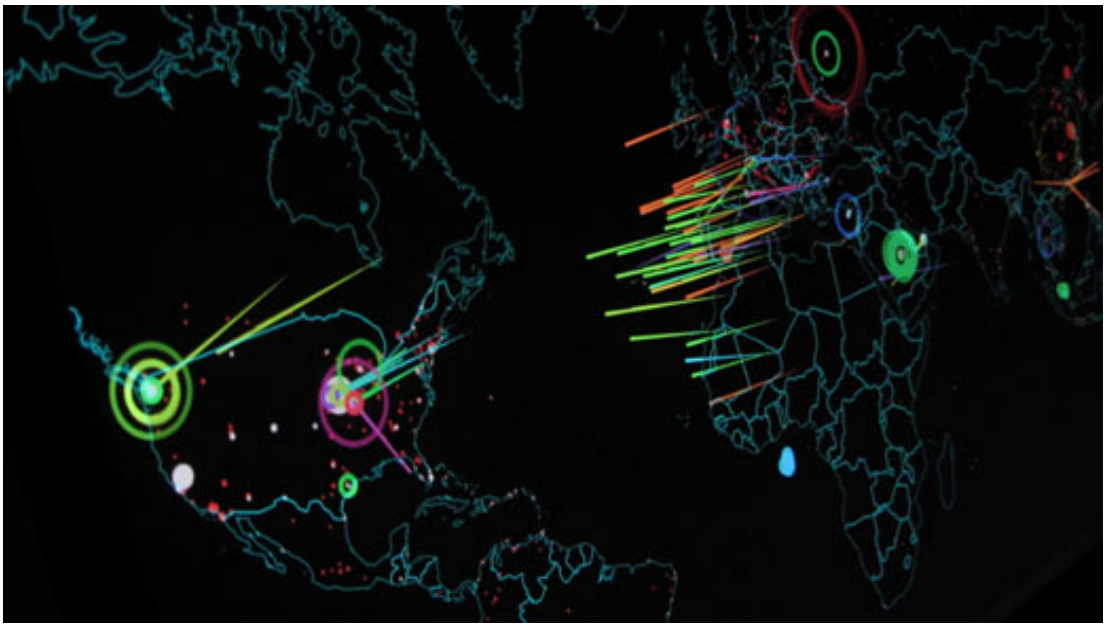
Stel je voor dat een cyberaanval op de Nederlandse vitale infrastrucuur inderdaad wordt aangemerkt als een daad van oorlog en daarmee binnen de NAVO de bijstandsclausule in werking stelt; hoe, wanneer, tot welk doel en onder welke autoriteit gaat Nederland capaciteiten inzetten? We kunnen ons verdedigen, maar dan? Als we eerst de artikel 100-procedure moeten doorlopen en daarna politieke consultaties moeten voeren binnen de NAVO, dan zijn we een hele tijd bezig.

Kortom, de besluitvormingsprocedures zijn thans niet toegesneden op het karakter van de denkbare aanvalsscenario's. Naast de besluitvorming is een gerelateeerde vraag of we ook wel voldoende getraind en voorbereid zijn, mocht zich de noodzaak aandienen voor een daadwerkelijk offensief. Het compromitteren van vijandige wapenssystemen maakt mogelijk deel uit van een reactie, maar is verre van het enige antwoord dat nodig zal zijn.

De strategie

In het regeerakkoord van 2011 is besloten een nationale cyber security-strategie te ontwikkelen; de tweede en meest recente versie daarvan is in 2013 gepubliceerd. De verantwoordelijkheid voor deze strategie is bij het NCSC ondergebracht; er zijn vijf doelstellingen opgenomen, waaronder het vergroten van de weerbaarheid, het investeren in beschermende maatregelen, het bouwen van coalities van belanghebbenden en het investeren in kennisontwikkeling.

Naast deze nationale cyber security-strategie is er in 2012 een Defensie Cyber Strategie gepresenteerd. In deze strategie wordt gesproken van zes 'speerpunten', waaronder het ontwikkelen van zowel defensieve als offensieve cybercapaciteit, het versterken van de digitale inlichtingenpositie en samenwerking met partners in Nederland en daarbuiten.



© Flickr / Christiaan Colen

'Patronen van cyberaanvallen laten tot nu toe een grote consistentie zien'.

Deze beide beschrijvingen zijn echter meer opsommingen van beleidsvoornemens dan een formulering van een strategie. Er wordt in deze documenten met geen woord gerept over de middelen, methoden of werkwijzen die zijn vereist om deze nationale doelstellingen in het digitale domein te verwezenlijken. Zo wordt eraan voorbijgegaan dat een belangrijke functie van een strategie haar afschikkende werking is. Het is niet nodig om zó ver te gaan als de Amerikaanse cyberstrategie, die zich het recht voorbehoudt een extreem ontwrichtende aanval met nucleaire wapens te beantwoorden. Dit is wel een voorbeeld van afschrikking waarbij de potentiële aanvaller weet dat het ultieme wapen ter vergelding kan worden ingezet.

Ook binnen de NAVO bestaat er geen cyberwar strategie. Terwijl het bondgenootschap op velerlei terreinen aan standaarden werkt en congruentie probeert te ontwikkelen – denk aan vredesoperaties en civiel-militaire relaties – geldt bij het onderwerp cyber een zekere subsidiariteit. Dat verbaast, zoals de *New York Times* deze zomer schreef: "the Western alliance has yet to develop a strategy to counter Russia's increasingly aggressive action in cyberspace …." Voorts, "there are no serious military plans, apart from locking down the alliance's own networks".[6]

> Nederland is een van de weinige landen ter wereld die publiekelijk bekend heeft gemaakt offensieve cyberwapens te ontwikkelen

Zoals elders betoogd, bestaat er een groot gevaar voor de samenleving als er niet goed wordt doordacht wat het politieke kader is waarbinnen deze activiteiten zich moeten ontplooien.[7] Bij het ontbreken hiervan zal de technologisch oplossing de boventoon voeren ten koste van politieke manouvreerruimte en dat is onwenselijk. Cyberwapens behoren tot het instrumentarium waarmee buitenlandse politiek bedreven kan worden; het creëren van een

duidelijk denkkader waarin zij onderworpen worden aan het primaat van de politiek is dringend gewenst, evenals het doordenken van een doctrine op basis waarvan zij optimale bruikbaarheid voor Nederland zouden kunnen hebben.

Toegenomen interconnectiviteit leidt tot een groter aantal zwakheden, die allemaal door politieke tegenstanders kunnen en zullen worden uitgebuit. En Nederland behoort tot de landen met de grootste mate van interconnectiviteit. Dit biedt vele voordelen, maar zorgt daarnaast ook voor uitdagingen, zo niet voor risico's. Nederland is een van de weinige landen ter wereld die publiekelijk bekend heeft gemaakt offensieve cyberwapens te ontwikkelen. Hoe we de organisatie, het besluitvormingsproces en de strategie vormgeven, heeft vérgaande consequenties voor hoe we een mogelijke cyberconfrontatie kunnen aangaan. Het verdient aanbeveling deze drie aspecten nog eens goed tegen het licht te houden.

Noten

[1]
Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies* , jrg. 35 (2012), nr. 1, pp. 5-32; voor een weerwoord, zie: John Stone, 'Cyber War Will Take Place!', *Journal of Strategic Studies* , jrg. 36 (2013), nr. 1, pp. 101-108.

[2]
Ministerie van Veiligheid en Justitie, *Cybersecuritybeeld CSBN-2016*, Den Haag 2016, 27.

[3]
Ministerie van Veiligheid en Justitie, *Cybersecuritybeeld CSBN-2016*, 12.

[4]
Paul Ducheine & Kraesten Arnold, 'Besluitvorming bij Cyberoperaties', *Militaire Spectator* 184/2, 2015, pp. 56-70.

[5]
Richard Clarke & Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: HarperCollins, 2010.

[6]
David E. Sanger, 'As Russian Hackers Probe; NATO Has No Clear Cyberwar Strategy', *New York Times*, 17 juni 2016.

[7]
Isabelle Duyvesteyn, 'Tijd voor een Handbook Cyberoorlog' ("Time for a Handbook on Cyber War"), *Socialisme en Democratie*, jrg. 71, nr. 5 (oktober 2014), pp. 32-37.

Auteurs

Isabelle Duyvesteyn
Hoogleraar 'Global History' aan het Instituut voor Geschiedenis van de Universiteit Leiden ▸
(https://www.universiteitleiden.nl/medewerkers/isabelle-duijvesteijn)