



Cyber space

Het domein van een nieuw soort totale oorlog

Mr. drs. C. Homan

In *cyber space* krijgt het begrip 'integrale benadering' een nieuwe betekenis. De bestrijding van tegenstanders beperkt zich niet tot de militaire middelen en is evenmin het domein van staten alleen. Ook staat het karakter van 'gevechtshandelingen' niet bijvoorbaat vast: is het oorlog, terrorisme of 'alleen maar' criminaliteit? Hoe het ook zij, onze veiligheid is wel in het geding.

"Iran is het doelwit van een westerse cyberaanval, maar de buitenlandse computerworm heeft alle serieuze doelen gemist" verklaarden Iranse regeringsvertegenwoordigers eind september. Het betrof hier het zogeheten Stuxnetvirus, waarmee meer dan dertigduizend, vooral industriële bronnen in de islamitische republiek zouden zijn besmet. Ook een aantal persoonlijke computers van medewerkers van de kerncentrale in Busher werd getroffen, maar de hoofdsystemen van de kerncentrale zouden niet zijn geïnfecteerd.

Het Stuxnetvirus heeft het gemunt op productieprocessen die draaien op veelgebruikte Siemenssoftware. Het dringt het bedrijfsnetwerk van een elektriciteitscentrale binnen en gaat op zoek naar computers die het productieproces regelen. Vermoed wordt dat Stuxnet speciaal ontwikkeld werd om een Iranse centrale aan te vallen, waarmee het een 'wapen' is geworden, gericht op een specifiek doel. Het wordt ook wel een cyberraket genoemd. Het Amerikaans ministerie van Defensie had in 2008 een andere 'besmettelijke' ervaring, toen zijn militaire computernetwerken gecompromitteerd werden. Het begon met een geïnfecteerde flashdrive ingebracht in een Amerikaanse militaire laptop. De kwaadaardige computercode van deze flashdrive – die het werk was van een buitenlands inlichtingenagentschap – verschaftte zich toegang tot de netwerken van het Amerikaanse Central Command. De code verspreidde zich zowel over geclassificeerde als ongeclassificeerde systemen en vestigde een digitaal bruggenhoofd, van waar data konden worden verzonden naar servers onder buitenlandse controle. Niettemin was tot op heden het meest spraakmakend de grootschalige aanval in 2007 op websites in Estland. Deze Baltische staat had besloten om een oorlogsmonument uit het Sovjettijdperk uit het centrum van de hoofdstad Tallinn te verwijderen. Dat viel bij de Russen in slechte aarde. Uit wraak kregen sites van de Estlandse regering zoveel internetverkeer te verwerken, dat ze crashten. Een sneeuw-



De kerncentrale in Busher

storm van 'buiten dienst' (*Distributed Denial of Service* (DDoS)) -aanslagen trof de websites van de president, het parlement, de ministeries, de politieke partijen, grote nieuwskanalen en de twee grootste banken van Estland. Een DDoS-aanslag, die in Estland was de grootste in de geschiedenis tot nu toe, vuurt namelijk een overweldigende hoeveelheid informatieaanvragen af op een computer of netwerksysteem waardoor deze overbelast raken.

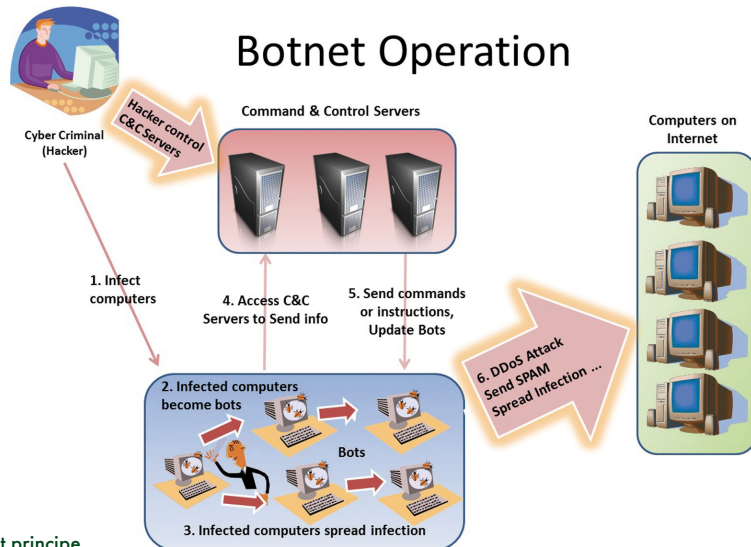
Hoewel de Russen werden dat ze betrokken waren bij de aanslagen in Estland, is het nog steeds niet duidelijk of hier sprake was van een 'cyberoproer van activistische hackers' of dat de aanvallen van hogerhand kwamen. Het grote probleem met cyberaanvallen is namelijk dat de dader(s) moeilijk te achterhalen zijn. Zij maken namelijk gebruik van zogenoemde 'botnets' (*robot networks*): netwerken van computers die op afstand zijn gekraakt en door één persoon kunnen worden beheerd. Sommige botnets bij de aanslagen in Estland bestonden uit 100.000 machines.

Digitale veiligheid

Estland heeft aangetoond dat de kwetsbaarheid van ontwikkelde samenlevingen voor computeraanvallen zeer groot is. Veel

onderdelen van een dergelijke maatschappij zijn immers van computers afhankelijk. Grootschalige uitval van informatiesystemen komt vaak voort uit hun afhankelijkheid van elektriciteit. Maar de razendsnelle, internationale verspreiding van virussen en andere 'malware' is ook een belangrijke oorzaak. Ook al zorgen tegenwoordig geavanceerde detectie- en quarantaine-mechanismen voor vroegtijdig ingrijpen, toch treden wereldwijde besmettingen op met grote verstoringen van IT-systemen. In het buitenland zijn al (petro-)chemische fabrieken en kerncentrales uitgevallen. Ook ging de controle over transportinfrastructuren soms verloren door besmetting van de procescontrolesystemen en -netwerken. Een strategische aanval van een vijandelijke mogendheid of cyberterroristische groep kan dus bijna alles platleggen: kernenergiecentrales of andere elektriciteitscentrales, telecommunicatiesystemen, banken, openbaar vervoer, verkeersleidingcentra, nooddiensten etc. De hierdoor ontstane economische en maatschappelijke ontwrichting kan zeer groot zijn. Ook kunnen gevaarlijke situaties ontstaan.

Digitale veiligheid staat dan ook hoog op de veiligheidsagenda. Deze nieuwe dimensie van veiligheid houdt zich bezig met



Botnet principe

maatregelen die misbruik van computers en netwerken, en de daarin opgeslagen informatie voorkomen of in ieder geval vermijden, eventuele misbruikers opsporen en de schade herstellen.

De cyberdreiging kent drie verschijningsvormen, *cyber crime*, cyberterrorisme en *cyber warfare*. Voorbeelden van *cyber crime* zijn inbreuk op auteursrechten door digitale verspreiding van werken en discriminatie en haat zaaien via internet. Het op het internet publiceren van alle HIV-besmette personen in Nederland is een voorbeeld van cyberterrorisme. De derde vorm van cyberdreiging, *cyber warfare*, ook wel *information war* genoemd, is te definiëren als geplande cyberaanvallen van naties of agenten daarvan, tegen ICT-systemen, software en data van andere naties met als doel vijandelijke verliezen te veroorzaken.

Militaire cyber warfare

Informatie- en communicatietechnologie (ICT) is uiteraard ook van vitaal belang voor de inzet van krijgsmachten. Zo is de Amerikaanse krijgsmacht afhankelijk van 15.000 netwerken en zeven miljoen computers die verspreid zijn over honderden installaties en tientallen landen. Op militair gebied heeft de grootscheepse informatisering van strijdkrachten dan ook geleid tot een nieuwe vorm van oorlogvoering, de eerder genoemde *cyber warfare*. Naast ruimte-, land-, lucht- en watergebonden optreden wordt dit ook wel de 'vijfde dimensie' genoemd. Het gaat hier om handelingen die vijandige besluitvormers moeten misleiden door het manipuleren van hun informatie en/of informatiesystemen. Tegelijkertijd wordt de eigen informatie optimaal gebruikt en beschermd. Aangezien steeds meer defensiesystemen van elektronische componenten met software zijn voorzien, zal *cyber warfare* een steeds belangrijker rol spelen op het slagveld. Cyberdreigingen kunnen bijvoorbeeld een middel zijn voor potentiële tegenstanders

van de Verenigde Staten, om de overweldigende Amerikaanse overmacht op conventioneel militair terrein te overwinnen. Ze kunnen heel onverwacht plaatsvinden zijn buitengewoon moeilijk te herleiden tot een bron.

Het traditionele afschrikingsmodel van (massale) vergelding is dan ook niet toepasbaar op cyberdreigingen. Terwijl een raket is voorzien van een 'afzenderadres', is dat bij een computervirus over het algemeen niet het geval. Het forensische werk dat noodzakelijk is om een aanval te achterhalen, voor zover dat al mogelijk zou zijn, kan maanden in beslag nemen. Ook is het moeilijk vast te stellen in hoeverre het om een aanval gaat en bijvoorbeeld niet alleen om spionage, iets dat vaak eerder voor de hand ligt.

De Amerikaanse minister van Defensie gaf vorig jaar juni de opdracht tot oprichting van het Amerikaanse *Cyber Command*. Dat werd in mei jl. operationeel en staat onder leiding van generaal Keith Alexander. Die verklaarde onlangs in het Congres dat de computers van het Pentagon 250.000 maal per uur belaagd worden, tot zes miljoen

maal per dag. Het betreft hier volgens de generaal onder meer 140 buitenlandse spionageorganisaties die proberen de Amerikaanse netwerken te infiltreren. Het Cyber Command geeft leiding aan de dagelijkse bescherming van alle defensienetwerken en ondersteunt militaire en contraterrorisme missies met 'cyberoperaties'. Daarnaast coördineert het de verspreiding van *cyber warfare* middelen over de krijgsmacht. Ten slotte werkt het commando samen met veel verschillende partners zowel binnen als buiten de overheid zoals het departement van Homeland Security en de particuliere sector.

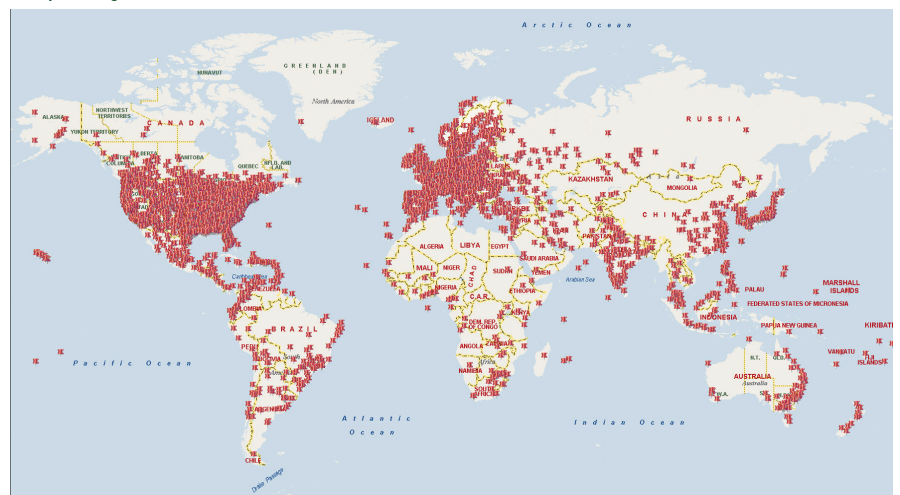
NAVO

Ook de NAVO onderkent de cyberdreigingen en neemt die even serieus als het risico van een raketaanval. Ze beschouwt cyberaanvallen echter (nog) niet als een militaire actie, waarop artikel V van het NAVO-verdrag van toepassing is. Het rapport 'NATO 2020', een door de NAVO ingestelde commissie onder voorzitterschap van een voormalige Amerikaanse minister van Buitenlandse Zaken, Madeleine Albright, bepleit wel om cyberverdediging op te nemen in het nieuwe NAVO Strategisch Concept.

Het bondgenootschap heeft overigens al sinds 2008 beleid voor *Cyber Defence*. Het doel hiervan is om de communicatie- en informatiesystemen (CIS) van de NAVO te beschermen. Naar aanleiding van de cyberaanvallen op Estland heeft de NAVO tevens een *Cooperative Cyber Defence Centre of Excellence* (CCC COE) opgericht en in dit land gedetacheerd. Dit Centre of Excellence adviseert en ondersteunt NAVO-partners in het opzetten van hun *cyber security*. In deze denktank houden dertig medewerkers uit verschillende NAVO-landen, van hackers tot wetenschappers, zich bezig met elektronische oorlogvoering.

In het NAVO *Cyber Defence* beleid staat dat de lidstaten verantwoordelijk zijn voor de bescherming van hun eigen (niet-NAVO)

Verspreiding Waledac botnet





Crisis Management Center in Doha, Qatar.
Bron USCENTCOM

communicatie- en informatiesystemen. De NAVO heeft ervoor gekozen om voorlopig geen offensieve *cyber warfare* capaciteiten te ontwikkelen omdat de relatie tussen de internationale wetgeving over gewapende conflicten en informatieoperaties, waar *cyber warfare* onderdeel van uitmaakt, (nog) niet duidelijk is.

Nederland

Hoe is de situatie in Nederland op dit gebied? De overheid heeft in 2002 een *Computer Emergency Response Team* opgezet, onder de naam 'Govcert.nl'. Deze organisatie valt onder verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties. De hoofdtaken zijn het voorkomen en zoveel mogelijk beperken van de schade die voortvloeit uit digitale veiligheidsincidenten. Govcert.nl maakt deel uit van een internationaal netwerk van vergelijkbare *response teams* die nauw samenwerken. De aandacht gaat daarbij uit naar het neutraliseren van computervirussen of het bestrijden van cybercriminaliteit. Belangrijke trends die Govcert.nl signaleert zijn onder meer eindgebruikers die – zowel thuis als op het werk – een zwakke schakel blijven in internetveiligheid. Zo maken internetcriminelen misbruik van lekken in software en ontbreken soms basisbeveiligingsmaatregelen zoals anti-virussoftware en het tijdig updaten van software. Ook wordt ingespeeld op angst: aanbiedingen van nep-antivirusproducten waardoor mensen geld kwijtraken en ook hun computers nog worden besmet om deel uit te maken van een botnet. De overheid heeft onder het programma Nationale Veiligheid in het Project ICT-verstoringen een tweetal toekomst scenario's ontwikkeld om de risico's van ICT-verstoringen op de nationale veiligheid in Ne-

derland te beoordelen. In deze scenario's voeren activistische groeperingen cyberaanvallen uit op de vitale infrastructuur van de energiesector en de telecommunicatiesector en veroorzaken daarmee gedurende enkele dagen ernstige maatschappelijke ontwrichting, met honderden gewonden, tientallen dodelijke slachtoffers en honderden miljoenen euro's schade. Hoewel er geen concrete aanwijzingen zijn dat Nederland op korte termijn zal worden getroffen, vinden de experts van de werkgroep dat de scenario's voorstelbaar en technologisch haalbaar zijn.

Krijgsmacht

Ook bij de krijgsmacht is digitale veiligheid een onderwerp van zorg. Zo heeft Defensie besloten, gelet op het specifieke karakter van militaire informatiesystemen, een eigen *Computer Emergency Response Team* (DefCERT) op te richten. DefCERT heeft tot doel de digitale beveiligingen van alle bij Defensie in gebruik zijnde geclassificeerde en ongeclassificeerde computernetwerken en informatiesystemen in één organisatie te bundelen. Naast de bescherming van gegevens en systemen tegen virussen zal de krijgsmacht in de toekomst ook rekening houden met grootschalige cyberaanvallen die gericht zijn op de ontwrichting van operationele informatiesystemen. DefCERT zal nationaal nauw samenwerken met het Govcert.nl en internationaal met het in Estland gevestigde NATO-CCC COE. Bundeling van civiele en militaire kennis en capaciteiten is een belangrijke stap voorwaarts. Tegen deze achtergrond zou de wenselijkheid van een civiel-militair agentschap kunnen worden bezien.

Het belang van digitale veiligheid voor de krijgsmacht wordt ook nog eens onderstreven in het dit voorjaar verschenen 'Eindrapport Verkenningen – Houvast voor de krijgsmacht van de toekomst'. Voor alle vier beleidsopties (Veilig blijven, Kort en krachtig, Veiligheid brengen en Veelzijdig inzetbaar) en hun varianten beveelt het rapport aan de aandacht voor *cyber defence* uit te breiden.



Zetel NATO Cooperative Cyber Defence Centre of Excellence in Estland

Regelgeving gewenst

Inmiddels wordt alom een dringende behoefte signaleerd aan internationale regelgeving op het gebied van *cyber warfare*. De juridische wereld loopt echter als altijd achter bij nieuwe technologische ontwikkelingen. Wat is bijvoorbeeld juridisch gezien een cyberaanval? Wat zijn de juridische gevolgen van een aanval op een defensienetwerk dat ook een ziekenhuis bedient? Worden, als er burger slachtoffers vallen, de Conventies van Genève geschonden? Wat is de juridische status van een burger die een militair doel aanvalt, bijvoorbeeld het netwerk van een commandocentrale? Het zijn slechts enkele van de vele vragen die beantwoord moeten worden. Het recht was altijd gebaseerd op territoriale grenzen maar *cyber space* vraagt om regelgeving die vaak zal afwijken van de wetten die fysieke, geografisch gedefinieerde territoria reguleren. *Cyber space* kan immers niet meer zo gemakkelijk aan territorium worden gekoppeld. Hier is dus een belangrijke rol weggelegd voor het internationaal recht. Dat laat het echter tot nu toe grotendeels afweten. De Russische hackers, of wie het ook waren bij de cyberaanvallen op Estland, kunnen dus voorslagnog in een juridisch niemandsland opereren. Een van de weinige, internationaal werkende wettelijke instrumenten op het gebied van digitale veiligheid is het Cybercrime Verdrag van de Raad van Europa. Het verdrag eist dat leden nationale wetgeving invoeren die onder meer ongeautoriseerde toegang en het kraken van netwerken, naast het witwassen van geld en kinderpornografie strafbaar stellen. De Verenigde Staten is als een van de weinige niet-lidstaten van de Raad van Europa ook partij bij deze conventie.

Richard A. Clarke en Robert K. Knake stellen in hun recente, spraakmakende boek 'Cyber War', in navolging van wapenbeheersingsverdragen op het gebied van strategische wapens, een *Cyber War Limitation Treaty* voor. Dit verdrag zou onder meer moeten omvatten: een *Cyber Risk Reduction Center* voor het uitwisselen van informatie en het verlenen van assistentie aan landen, een verbod op een *first use* van cyberaanvallen tegen civiele infrastructuur en het verbieden om netwerken van financiële instanties te beschadigen en data te veranderen of te beschadigen.

Clarke en Knake beogen met hun boek *cyber warfare* tot onderwerp van publiek debat te maken. Een debat dat verdient serieus te worden genomen!◀

Robert K. Knake (li) en Richard A. Clarke

