

Iedereen is kwetsbaar voor ongrijpbare elektronische aanvallers

De digitale revolutie heeft niet alleen de civiele wereld op zijn kop gezet, ook militairen moeten ineens aan compleet nieuwe dreigingen het hoofd bieden. Maar wat is een virtuele dreiging? Hoe verschilt een gevecht nog van spionage en hoe vind je de vijand?

Het onzichtbare

slagveld



Kees Homan

In juni 1982, Op het hoogtepunt van de Koude Oorlog, ontdekte een Amerikaanse waarnemingssatelliet een grote ontploffing in Siberië. Was er een raket gelanceerd? Betrof het een nucleaire test? Het bleek om een zware ontploffing van een gaspijp-leiding te gaan. De oorzaak was een defect in het digitale controlesysteem, dat Sovjetspionnen hadden gestolen van een firma in Canada. Zij wisten niet dat de CIA had geknoeid met de computerchips en programmatuur, waardoor na enige tijd de snelheid van pompen en de instellingen van een belangrijke klep zo veranderden, dat de druk in de buis opliep tot ver boven wat acceptabel is voor verbindingstukken en naden van pijpleidingen. Dit meldt Thomas Reed, een voormalig

Amerikaans minister van de luchtmacht, in zijn memoires. Het resultaat was, aldus Reed, 'de meest monumentale niet-nucleaire explosie en brand die ooit vanuit de ruimte werd gezien'. Het was ook de eerste actie die we als een aanval vanuit cyberspace mogen beschouwen. Inmiddels zijn bedreigingen vanuit cyberspace aan de orde van de dag. Cyberspace bestaat enerzijds uit de denkbeeldige wereld die we digitale informatie noemen, en anderzijds uit fysieke hardware: computers, netwerken, telefoon-, coax-, glasvezelkabels en elektromagnetische straling, alles wat de productie en uitwisseling van digitale informatie mogelijk maakt.

CYBEROPROER

In december 2010 was er in ons land een cyberincident dat ruime aandacht

trok. Dat waren de aanvallen van sympathisanten van WikiLeaks op de websites van MasterCard en Visa, die hierdoor werden platgelegd. Boze hackers reageerden hiermee op het blokkeren door deze creditcardmaatschappijen van donaties aan WikiLeaks. De hackers, die hun aanvallen uitvoerden onder de naam *Operation Payback*, maakten gebruik van een server in Haarlem. Veel grootschaliger was echter de alhier minder bekende aanval die via internet werd uitgevoerd op websites in Estland in 2007. Deze Baltische staat had besloten om een oorlogsmonument uit het Sovjettijdperk uit het centrum van de hoofdstad Tallinn te verwijderen, wat in slechte aarde viel bij de Russen. Uit wraak kregen sites van de Estlandse regering zoveel internetverkeer te verwerken dat ze crashten. Een

sneeuwstorm van 'buiten dienst'-aanvallen trof de websites van de president, het parlement, de ministeries, politieke partijen, grote nieuwskanalen en de twee grootste banken van Estland en legden deze plat. Zo'n aanval, beter bekend als een Distributed Denial of Service Attack, kortweg DDoS, bestaat erin dat zo'n overweldigende hoeveelheid informatieaanvragen wordt afgevuurd op een computer- of netwerksysteem op het internet, dat dat eronder bezwijkt. De DDoS-aanval op Estland was tot nu toe de grootste in de geschiedenis van het internet. Hoewel de Russen betrokkenheid verweten werd is nog steeds niet duidelijk of hier sprake was een cyberoproer van activistische hackers of dat de aanvallen van hogerhand waren georkestreerd. Het grote probleem met cyberaanvallen is namelijk dat daders moei-

lijk te achterhalen zijn omdat ze gebruik maken van zogenoemde bot-nets, een netwerk van 'robots', computers die zonder dat hun eigenaar dat weet op afstand gekraakt zijn, zodat de voor een DDoS-aanval kunnen worden ingezet. Zo'n botnet, groot genoeg om een doelsysteem met een onmogelijk groot aantal aanvragen tegelijkertijd te bombarderen, kan door één persoon worden beheerd. Sommige botnets bij de aanslagen in Estland bestonden uit wel 100.000 machines. Hackers kunnen dus met betrekkelijk weinig middelen veel schade aanrichten. Ze hebben niet veel geld of een leger van mensen nodig en ze kunnen het doen vanuit het comfort van de huiskamer, met een biertje in de hand.

Estland was een teken aan de wand, maar wat het begrip cyberaanval pas echt in de schijnwerpers zette, was het computervirus Stuxnet, dat in september 2010 de kop opstak en waarschijnlijk gericht was tegen het nucleaire programma van Iran. Stuxnet bleek een kwaadaardig computerprogramma te zijn dat zich snel kan verspreiden in specifieke industriële systemen. Duizenden computers in verschillende landen werden erdoor geïnfecteerd, maar vooral computers in nucleaire installaties in Iran.

DIGITALE VEILIGHEID

Estland heeft aangetoond dat de kwetsbaarheid van ontwikkelde samenlevingen voor computeraanvallen zeer groot is. Aangezien veel sectoren van de maatschappij van computers afhankelijk zijn, kan de maatschappelijke en economische ontwrichting door een cyberaanval ingrijpend zijn. Een strategische aanval van een vijandelijke mogendheid of cyberterroristische groep kan bijna alles platleggen: elektriciteits- en kernenergiecentrales, telecommunicatiesystemen, banken, openbaar vervoer, verkeersleidingscentra, nooddiensten en ga zo maar door. Digitale veiligheid staat dan ook

hoog op de veiligheidsagenda. Deze nieuwe veiligheidsdimensie houdt zich bezig met maatregelen die misbruik van computers en netwerken en de daarin opgeslagen informatie dienen te voorkómen of in ieder geval vermijden, moeten helpen om eventuele misbruikers op te sporen en schade te herstellen.

In de praktijk worden termen voor kwaadaardig gedrag in cyberspace als cyberterrorisme, hacktivisme, cyberdefence en cyberwarfare nogal eens door elkaar heen gebruikt, met wisselende definities. Maar in wezen gaat het om drie verschijningsvormen van cyberdreiging: cybercrime, cyberterrorisme en cyberwarfare. Voorbeelden van cybercrime zijn inbreuk op auteursrechten door digitale verspreiding van werken en discriminatie en haatzaaien via internet. Het op het internet publiceren van persoonsgegevens van alle HIV besmette personen in Nederland is een voorbeeld van cyberterrorisme. Tenslotte is cyberwarfare – ook wel information warfare genoemd – te definiëren als geplande cyberaanvallen van naties of agenten daarvan tegen informatie- en communicatietechnologie (ICT), software en data van andere naties met als doel vijandelijke verliezen te veroorzaken. Sommige deskundigen onderscheiden daarnaast cyberspionage als een vierde vorm van cyberdreiging.

CYBER WARFARE

ICT is ook van vitaal belang voor de inzet van krijgsmachten. Zonder ICT geen communicatiesatellieten, maar ook geen moderne logistieke steun, geen bevelvoering en geen vergaring van actuele inlichtingen. Zo is de Amerikaanse krijgsmacht bijvoorbeeld afhankelijk van 15.000 netwerken en zeven miljoen computers die verspreid zijn over honderden installaties in tientallen landen. De grootscheepse informatisering van strijdkrachten dan ook reeds geleid tot een nieuwe vorm van

Waarschijnlijk zal oorlogvoering via internet zich voordoen naast, maar ook in samenhang met de meer traditionele vormen van oorlogvoering

oorlogvoering, de eerdergenoemde cyberwarfare. Naast ruimte-, land-, lucht- en watergebonden optreden wordt dit ook wel de 'vijfde dimensie' van oorlogvoering genoemd. Het gaat om handelingen die vijandige besluitvormers moeten misleiden door hun informatie en/of hun informatiesystemen te manipuleren. Tegelijkertijd wordt de eigen informatie optimaal gebruikt en beschermd tegen soortgelijke activiteiten van anderen. Aangezien steeds meer defensiesystemen van elektronische componenten met software zijn voorzien, zal cyberwarfare een steeds belangrijker rol spelen op het slagveld. Waarschijnlijk zal oorlogvoering via internet zich voordoen naast, maar ook in samenhang met de meer traditionele vormen van oorlogvoering. Een voorbeeld is de Georgisch-Russische oorlog in 2008, toen tegelijk met de oorlog op de grond computeraanvallen op Georgië plaatsvonden.

ASYMMETRISCHE OORLOGVOERING

Cyberdreigingen zijn als vorm van asymmetrische oorlogvoering ook een middel voor potentiële tegenstanders van de Verenigde Staten om de overweldigende Amerikaanse overmacht op conventioneel militair terrein te overwinnen. Cyberdreigingen openbaren zich geheel onverwachts en zijn buitengewoon moeilijk tot hun oorsprong te herleiden. Het traditionele afschrikingsmodel van massale vergelding is omdat het zo moeilijk is de uitvoerder van een aanval te identificeren niet toepasbaar. 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 aanvaller te achterhalen kan maanden in beslag nemen, als het al lukt. Zelfs is het moeilijk om vast te stellen in hoeverre een incident een echte aanval betreft. Veelal gaat het eerder om spionage dan om een oorlogsdaad.

De Amerikaanse Minister van Defensie gaf in juni 2009 de opdracht tot oprichting van Cyber Command, dat vorig jaar mei operationeel werd en onder leiding staat van generaal Keith Alexander. Hij verklaarde 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 Alexander onder meer 140 buitenlandse spionageorganisaties die gedurig proberen de Amerikaanse netwerken te infiltreren. Het Cyber Command geeft onder meer leiding aan de dagelijkse bescherming van alle defensie netwerken en ondersteunt militaire en antiterroristische missies met operaties in cyberspace.

NAVO

Internationale organisaties als de NAVO en de EU onderkennen uiteraard ook de gevaren die vanuit cyberspace dreigen. De NAVO heeft sinds 2008 beleid voor Cyber Defence, dat bedoeld 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 opgericht en in dat land gedetacheerd. Dit Centre of Excellence adviseert en ondersteunt NAVO-partnerlanden bij het opzetten van hun digitale beveiliging. In tegenstelling tot de Verenigde

De juridische wereld loopt echter als altijd achter bij nieuwe technologische ontwikkelingen. Wat is bijvoorbeeld juridisch gezien een cyberaanval?

Staten wil de NAVO voorlopig geen offensieve cyberwarfare capaciteiten ontwikkelen omdat zij de relatie tussen de internationale wetgeving voor gewapend conflict en die voor informatie-operaties, waar cyberwarfare deel van uitmaakt, nog niet duidelijk vindt. De Europese Unie heeft ook beleid en regelgeving ontwikkeld, ingegeven door het belang van de informatie-infrastructuur voor Europa en het grensoverschrijdend karakter van cyberaanvallen. Voor een hoogwaardige en effectieve beveiliging van netwerken en informatie in de EU werd reeds in 2005 het European Network and Information Security Agency opgericht. Daarnaast nam de EU-top in Tallinn in april 2009 een cyber-actieplan van de Europese Commissie over.

NEDERLAND

In Nederland heeft de overheid in 2002 een Computer Emergency Response Team opgezet, onder de naam Govcert.nl. De hoofdtaken zijn het voorkomen en in tweede instantie zoveel mogelijk beperken van 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 en het bestrijden van cybercriminaliteit. Defensie besloot, 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 computer-

netwerken 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 Govcert.nl en internationaal met het in Estland gevestigde Cooperative Cyber Defence Centre of Excellence van de NAVO. 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.

REGULERING

Inmiddels wordt een dringende behoefte gesignaleerd aan internationale regelgeving op het gebied van cyberspace. 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? Is een grootschalige cyberaanval op een lidstaat van de NAVO een oorlogsverklaring waarop artikel 5 van het NAVO-verdrag van toepassing is, het artikel van de collectieve verdediging? Als er burgerslachtoffers vallen, worden dan de Conventies van Genève geschonden? Wat is de juridische status van een burger die een militair doel, bijvoorbeeld het netwerk van een commandocentrale, platlegt? Dat zijn nog maar een paar van heel veel vooralsnog onbeantwoorde vragen.

Daar komt nog bij dat cyberspace regelgeving vereist die afwijkt van de wetgeving die van toepassing is op fysieke, geografisch gedefinieerde territoria. Het recht was altijd gebaseerd op territoriale grenzen, maar in cyberspace kan het werkingsgebied niet meer zo gemakkelijk in territoriale entiteiten verdeeld worden. Hier is vooral een belangrijke rol weggelegd voor het internationaal recht, dat het tot nu toe grotendeels laat afweten. In navolging van wapenbeheersingsverdragen op het gebied van strategische wapens stellen Richard A. Clarke en Robert K. Knake in hun spraakmakende boek *Cyber War* een Cyber War Limitation Treaty voor. Zo'n verdrag zou onder meer een Cyber Risk Reduction Center moeten omvatten voor het uitwisselen van informatie en het verlenen van assistentie aan landen. Voorts een verbod op first-use

van cyberaanvallen tegen civiele infrastructuur en een verbod op het veranderen van gegevens of het beschadigen van netwerken van financiële instanties. Clarke en Knake beogen met hun boek cyberwarfare tot onderwerp van publiek debat te maken. Een debat dat verdient serieus te worden genomen! De Verenigde Staten hebben zich tot op heden tegen wapenverdragen voor cyberspace verklaard. Het land vreest dat dit zou kunnen leiden tot een rigide mondiale regulering van het internet die de dominantie van Amerikaanse internetfirma's zou ondermijnen, innovatie zou belemmeren en ook nog de openheid zou beperken die het internet veel van zijn aantrekkingskracht geeft. Vooralsnog kunnen hackers dan ook met muis en toetsenbord in een juridisch niemandsland blijven opereren, al dan niet met een biertje in de hand. ■

