Cyber security

Samenwerken voor een veilige en vitale cybersamenleving

De hier weergegeven (en bewerkte) toespraak is door drs. E.S.M. Akerboom uitgesproken in zijn hoedanigheid als Nationaal Coördinator Terrorismebestrijding en Veiligheid op het Defensie Cyber Symposium dat plaatsvond op de Koninklijke Militaire Academie in Breda op 27 juni 2012. Tijdens dit symposium presenteerde toenmalig minister van Defensie drs. J.S.J. Hillen de Defensie Cyber Strategie. Andere sprekers waren: Patrick de Graaf (CapGemini), kolonel Hans Folmer (Task Force Cyber), Ronald Prins (FOX-IT), Henk Jan Vink (TNO) en kolonel Paul Ducheine (NLDA).

*Drs. E.S.M. Akerboom**

Met het opleveren van de Defensie Cyber Strategie heeft Defensie niet alleen een stevig ijkpunt voor zichzelf neergezet, maar ook een belangrijke visie voor haar civiele partners. Overtuigend vind ik de wijze waarop Defensie de grenzeloosheid als uitgangspunt neemt. Op andere, civiele, veiligheidsterreinen domineert het geografisch denken vaak nog sterk. Tevens weerspiegelt de Defensie Cyber Strategie de noodzaak tot een veel intensievere vorm van civiel-militaire samenwerking dan wij tot nu toe gewend zijn. Alle betrokken overheidspartijen worden geconfronteerd met deze noodzaak tot samenwerking. Het is dan ook vanzelfsprekend dat de Defensie Cyber Strategie aansluit bij en voortbouwt op de Nationale Cyber Security Strategie. Dit is voor de Nederlandse overheid het kader van waaruit Nederland zijn cyber security wil verbeteren. De NCTV[1] ziet Defensie als een van zijn vaste partners in het cyberdomein en de Defensie Cyber Strategie zou men dan ook kunnen zien als de militaire pijler van onze Nationale Cyber Security Strategie.

Nieuwe dreiging vraagt om andere aanpak

Zoals de Defensie Cyber Strategie terecht stelt is een klassieke scheiding van domeinen – militair versus civiel, publiek versus privaat en nationaal versus internationaal – in cyberspace minder relevant. Ook digitaal zijn wij in toenemende mate van elkaar afhankelijk. Een grootschalige cyberaanval met als doel de aantasting van de Nederlandse nationale veiligheid kan immers zowel tegen militaire als civiele doelen worden gericht. Of tegen beide tegelijk. Bij een dergelijke aanval zal het bovendien moeilijk zijn te bepalen wie de agressor, de aanvaller is. Dit is het probleem van de attributie van een aanval. In de cyberdimensie is dat buitengewoon complex omdat de aanvaller zich relatief gemakkelijk kan verbergen. Daarnaast vraagt de snelheid waarmee cyberdreigingen zich kunnen manifesteren en ontwikkelen om zeer snel ingrijpen. Het duiden van de dreiging en de intentie van de agressor, het bepalen van het zwaartepunt van de aanval en het coördineren van de respons vragen in het cyberdomein om een snelle en gezamenlijke aanpak. Bij de verdediging tegen dergelijke dreigingen en de voorbereiding daarop is samenwerking hoogst noodzakelijk.

* De auteur is sinds 1 december 2012 secretaris-generaal bij het ministerie van Defensie.

1 Nationaal Coördinator Terrorismebestrijding en Veiligheid, voorheen NCTb (Nationaal Coördinator Terrorismebestrijding).

FOTO ANP, E. OUDENAARDEN

De Maeslantkering in de Nieuwe Waterweg. De beveiliging van procescontrolesystemen, onder meer toegepast in waterbouwkundige werken die de continuïteit an het functioneren van Nederland garanderen, verdient extra aandacht

Zo is het essentieel, wanneer zich een crisis voordoet, dat er een gezamenlijk omgevingsbeeld wordt opgebouwd. Dit vraagt niet alleen om interoperabiliteit, maar ook om een gedeeld referentiekader. Samenwerking in de voorbereiding is dan ook niet alleen wenselijk, maar ook urgent. Hierbij kan men denken aan de onderlinge uitwisseling van capaciteiten en kennis, aan de uitwisseling van informatie om een gezamenlijk omgevingsbeeld op te bouwen, aan de efficiënte inzet van capaciteiten en aan het delen van opleidingsmodules. Defensie heeft daarin reeds de daad bij het woord gevoegd en participeert inmiddels volop in het Nationaal Cyber Security Centrum,[2] samen met vele andere organisaties, waarbij men elkaar bij grote incidenten ondersteunt.

Lessen uit recente incidenten

In het recente verleden hebben diverse ernstige incidenten plaatsgevonden, waarbij de kwestie-Diginotar zelfs kan worden betiteld als een echte cybercrisis.[3] Deze incidenten gelden als *blessings in disguise*. Van deze gebeurtenissen is immers erg veel geleerd en ze hebben opnieuw aangetoond dat belangen, dreigingen en de weerbaarheid in samenhang moeten worden bezien. De Cyber Security Raad,[4] ingesteld door de minister van Veiligheid en Justitie om te adviseren over digitale veiligheid, heeft een onderzoek laten uitvoeren naar de lessen die kunnen worden geleerd uit verschillende casus. Drie bevindingen springen er dan uit. Ten eerste wordt de security van organisaties op dit moment vaak te diep in de organisatie bepaald. Kwesties als waar bedrijfsdata worden opgeslagen en welke beveiligingsmaatregelen moeten worden doorgevoerd of geactualiseerd, horen in deze tijd thuis in de *boardroom*. Ten tweede is een paradigmaverandering nodig: we moeten ons meer gaan richten op detectie en respons. Daarmee kunnen we niet garanderen dat incidenten nooit zullen voorkomen, maar we kunnen wel garanderen dat ze adequaat worden aangepakt wanneer ze zich voordoen. Tot slot moeten de leerpunten van cyberincidenten actiever en breder worden verspreid. Op die manier kan de *awareness* van allerlei organi-

2 Het NCSC maakt deel uit van de organisatie van de NCTV. Zie: www.ncsc.nl.

3 Deze kwestie speelde vanaf augustus tot december 2011 en draaide om een digitale inbraak bij een *Certificate Service Provider* (in casu Diginotar). Zie het dossier via: www.govcert.nl/dienstverlening/Kennis+en+publicaties/dossier-diginotar.

4 De Cyber Security Raad is een onafhankelijke adviesraad voor de Nederlandse regering, geïnstalleerd op 30 juni 2011. De raad wordt voorgezeten door de NCTV en drs. Eelco Blok (CEO Koninklijke KPN N.V.).

saties actief worden verbeterd en kunnen ze gaan doen wat nodig is om hun beveiliging op orde te krijgen.

Dreigingen en belangen

We beschermen onze nationale veiligheid onder andere door te kijken of onze vitale belangen worden bedreigd. We brengen dreigingen in kaart en waar mogelijk nemen we ze weg. En wanneer dit niet kan, moet de weerbaarheid tegen deze dreigingen worden vergroot. Dit geldt zeker ook voor het digitale domein. De belangen die voor Nederland op het spel staan zijn omvangrijker dan ooit, want de digitalisering van Nederland is immers ver gevorderd. En daarmee is ook onze afhankelijkheid van ICT zeer groot geworden. Digitale processen zijn instrumenteel geworden voor het functioneren van de overheid, de vitale sectoren en het bedrijfsleven; de organisaties die Nederland draaiende moeten houden. Denk bijvoorbeeld aan procescontrolesystemen, ook wel aangeduid met de Engelse afkortingen ICS of SCADA.[5] Deze systemen worden gebruikt in onder andere industriële processen, waterbouwkundige werken en een groot scala van andere besturingssystemen. Veel van deze systemen zijn van groot belang voor de continuïteit van het functioneren van Nederland. Dit moet allemaal beschermd worden. In het verleden is er echter vooral veel moeite gestoken in het gebruiksgemak en de functionaliteiten van zulke systemen, maar veel minder in de beveiliging ervan. En dat terwijl we in deze tijd geregeld geconfronteerd worden met aanvallen op deze systemen én met volhardende aanvallers.

De aandacht voor cyber security moet daarom structureel worden ingebed in ons veiligheids- en continuïteitsdenken. Het goed functioneren van onze samenleving en de toekomstige economische welvaart en vooruitgang van Nederland zullen namelijk deels afhangen van hoe succesvol wij zijn om cyber security voor Nederland te realiseren. We willen burgers, bedrijven en overheidsorganisaties het vertrouwen kunnen geven dat zij hun activiteiten veilig in cyberspace kunnen ontplooien. Vlak voor de zomer is het tweede Cyber Security Beeld Nederland gepubliceerd.[6] We zien dat de dreigingen die uitgaan van spionage en cybercriminaliteit onverminderd groot blijven. Daarmee laat dit beeld geen grote verschuivingen zien ten opzichte van het eerste beeld dat eind 2011 is gepresenteerd. In het kader van civiel-militaire samenwerking is het echter goed om ons te realiseren dat technieken die gebruikt worden voor digitale spionage en cybercrime, ook gebruikt kunnen en zullen worden voor cyberwarfare en vice versa. Dit besef onderschrijft de noodzaak tot informatie-uitwisseling over dreigingen en het gezamenlijk zoeken naar oplossingen.

Een tweetal bevindingen uit het tweede Cyber Security Beeld Nederland wil ik er uitlichten. Ze dienen ter illustratie voor de uitdaging waarvoor wij staan. Ten eerste zien wij een toenemende *consumerization* van ICT. Dit betekent dat nieuwe ontwikkelingen op het gebied van informatietechnologie steeds vaker ontstaan vanuit de consumentenmarkt. Zo zorgt de continue behoefte aan mobiel internet voor een uitzonderlijke toename van het aantal aangesloten apparaten, vooral vanuit het perspectief van gebruiksgemak voor consumenten. Dit zal resulteren in een grotere maatschappelijke afhankelijkheid, meer kwetsbaarheden en een exponentiële toename in complexiteit. Ten tweede komt daar bij dat kwaadwillenden steeds sneller in staat zullen zijn om zwakheden te misbruiken, ten opzichte van de lange doorlooptijden die organisaties nodig hebben om tegenmaatregelen te implementeren.

Publiek-private samenwerking

Om onze weerbaarheid tegen cyberdreigingen te versterken moeten overheid en private sector nauwer met elkaar gaan samenwerken dan wij tot nu toe gewend zijn. Een groot deel van de ICT-infrastructuur, -kennis en -expertise is in handen van de private sector en wordt ook daar

5 SCADA (Supervisory Control and Data Acquisition) is een vorm van ICS (Industrial Control System).

6 Zie: www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland.html. Zie ook *Kamerstukken II*, 2011-12, 26 643, nr. 245.

ontwikkeld. De publieke en private sectoren zijn van elkaar afhankelijk voor het managen van cyberdreigingen, het uitwisselen van informatie, het verhogen van de weerbaarheid van Nederland en voor het bedenken van innovatieve oplossingen om nieuwe dreigingen aan te grijpen. Alle betrokken partijen zijn afhankelijk van een veilige cyberomgeving. De NCTV wil daarom toewerken naar een sterke publiek-private samenwerking op het terrein van cyber security, waarbij alle partijen hun verantwoordelijkheid nemen. Dit betekent dat de overheid er voor zorgt dat de private sector ook zelf in staat wordt gesteld om de eigen weerbaarheid tegen cyberdreigingen te vergroten, bijvoorbeeld door het verstrekken van kennis en expertise voor het managen van cyberincidenten.

FOTO ASSOCIATED PRESS/REPORTERS, M. DUNHAM

Publiek-private samenwerking op het terrein van cyber security is vereist om dreigingen, zoals van het hackerscollectief Anonymous, in kaart te brengen

Opbouwen van een gezamenlijk omgevingsbeeld

Eén van de zaken die we prioriteit geven is het organiseren van inzicht in de dreigingen tegen en de weerbaarheid van onze ICT-systemen. Dit is op dit moment nog te beperkt. De beveiliging moet worden verbeterd, evenals de mogelijkheden om aanvallen te onderkennen en te duiden door monitoring en analyse. Wij willen immers een beter beeld hebben van wat er in cyberspace gebeurt en manieren vinden om daders te identificeren. Alleen dan kunnen we effectief ingrijpen. Dit vraagt wederom om nauwe samenwerking en informatie-uitwisseling. Het gaat dan om afspraken maken met het bedrijfsleven en wetenschap om over en weer van elkaars kennis en ervaring te kunnen profiteren, bijvoorbeeld bij het tegengaan van (bedrijfs)spionage via internet. De overheid wil de kennis die zij opdoet bij het monitoren van de eigen netwerken beschikbaar stellen aan bedrijven en vitale sectoren. Dit kan hen helpen zich afdoende te beveiligen tegen digitale aanvallen. Daarnaast wordt er, op verzoek van de Tweede Kamer, gewerkt aan een *security breach notification*,[7] oftewel meldplicht en aan aanvullende interventiemogelijkheden om in te grijpen bij een cybercrisis. Daarmee krijgt de overheid meer en beter zicht op dreigingen

7 Zie *Kamerstukken II*, 2011-12, 26 643, nr. 247.

en de beschikking over een uitgebreid palet van interventiemogelijkheden voor een (dreigende) cybercrisis.

De race om kennis en innovatie

Bij cyber security worden wij geconfronteerd met een permanente wapenwedloop van kennisontwikkeling en innovatie, waarin wij het ons niet kunnen veroorloven achterop te raken. Eén van de belangrijkste dingen die wij nodig hebben is kennis, kunde en expertise op het gebied van cyber security en goed opgeleide cyber security experts. In publiek-privaat en civiel-militair verband moeten wij werken aan het opbouwen en versterken hiervan. Ik denk dan aan onder andere het samenwerken waar het gaat om opleiden en trainen, het over en weer bieden van loopbaanperspectief en het gezamenlijk investeren in onderzoek en innovatie.

Eendracht maakt macht

De discussie in Nederland gaat vaak over de rol van Defensie in de ondersteuning van civiele autoriteiten. De discussie die in het kader van cyber security echter even goed gevoerd kan worden, is die van de rol van de civiele autoriteiten in de ondersteuning van Defensie. Samenwerking op het cyberdomein is geen eenrichtingsverkeer. Het kernbegrip hier is *unity of effort* of, om een oud-Nederlandse term te gebruiken, eendracht maakt macht. Daarbij waken we ervoor alle cyberinspanningen in Nederland op één hoop te vegen. Dat zou contraproductief zijn, omdat unieke capaciteiten mogelijk verwateren of verloren gaan. Niet alles hoeft onder één dak samen te worden gebracht. Geen *Homeland Cyber Security* naar Amerikaans model voor Nederland dus. Waar het om gaat is dat partijen elkaar snel weten te vinden, elkaar kennen, goed kunnen samenwerken en in dat kader vanuit de eigen (unieke) kennis en expertise bijdragen aan het bestrijden van incidenten.
Defensie en civiele autoriteiten hebben hun eigen specifieke kaders waarbinnen zij hun kerntaken uitvoeren. Het is van belang dat rollen, taken en verantwoordelijkheden helder

Rond cyber security heerst een permanente wapenwedloop van kennisontwikkeling en innovatie; de vele aspecten van het cyberdomein vragen om goed opgeleide experts

zijn en ieder de klus kan oppakken waarvoor hij aan de lat staat. De capaciteiten die Nederland opbouwt zijn niet concurrerend, maar zullen in de praktijk complementair blijken. Dit vraagt om samenwerking, zowel tijdens crises als in de voorbereiding daarop. Vooral in het digitale domein zal deze samenwerking structureel en intensief moeten zijn. Functionarissen moeten elkaar snel kunnen vinden en elkaars taal kunnen spreken. Om dit te bereiken kan gedacht worden aan het opbouwen van een gezamenlijk omgevingsbeeld in cyberspace, het uitwisselen van informatie, kennis en kunde, het gezamenlijk investeren in onderzoek en innovatie en het gezamenlijk oefenen en opleiden. Samenwerking op het gebied van cyber security is geen optie, maar een noodzaak. De Defensie Cyber Strategie ademt ambitie. Ambitie en samenwerking zijn nodig om in deze tijd iets te bereiken en met Defensie als partner wil de NCTV deze uitdaging graag aangaan. ■