Defensie in het digitale domein

'In de loop van 2017 is het Defensie Cyber Commando operationeel', aldus de commandant, brigade-generaal Hans Folmer.[1] 'Rusland vreest cyberaanval vanuit Nederland', kopte het AD een dag later over een echt incident, een criminele actie waarbij in Nederland geplaatste dataservers een rol zouden spelen.[2] Gelukkig staan beide berichten los van elkaar. Het eerste betreft operationele militaire capaciteit van de Commandant der Strijdkrachten. Het tweede gaat over criminele activiteit. Ze hebben slechts gemeen dat ze zich in het digitale domein afspelen. Voor het aanpakken van dit soort bedreigingen kijken maatschappij en samenleving verwachtingsvol naar Defensie. Dit artikel onderzoekt aan de hand van beleidsontwikkeling welke rollen Defensie in dit digitale domein speelt.

*Prof. dr. P.A.L. Ducheine, brigade-generaal van de Militair Juridische Dienst**

Operaties in dit digitale domein of cyberspace staan in Nederland sinds 2009 op de politieke én militaire agenda.[3] Anno 2015 uit zich dat onder meer in beleidsvisies, zoals de eerste Nationale Cybersecurity Strategie (2011), diens opvolger (2013), in de Defensie Cyber Strategie (2012) en diens actualisering (2015). Een aantal organisaties, hoewel jong, is voor de insiders inmiddels bekend: bijvoorbeeld het Nationale Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie, het Defensie Cyber Commando (DCC) en de *Joint Sigint Cyber Unit* van de AIVD en MIVD.

Waar terughoudendheid in defensie-investeringen en inzet in het hoge deel van het geweldsspectrum na 'Afghanistan' de boventoon voerde,[4] is de politieke (en parlementaire) bereidheid te investeren in cybercapaciteiten en daadwerkelijk inzet te overwegen opmerkelijk. Sterker nog: maatschappij en bedrijfsleven kijken vragend naar Defensie voor het aanpakken van bedreigingen in cyberspace.[5] De vraag rijst dan welke rollen Defensie in dit domein speelt.

Ik beoog met dit artikel die vraag te beantwoorden door de beleidsontwikkeling in dit digitale domein te herleiden. De start ligt bij de motie-Knops. Vervolgens wordt de digitale dreiging bezien en het multidisciplinaire antwoord daarop. Dit mondt uit in de eerste Nationale Cyber Security Strategie. De aanloop naar, en

* De auteur dankt drs. Piet Kamphuis, brigade-generaal ir. Hans Folmer en drs. Matthijs Veenendaal voor hun suggesties en commentaar.

1 Interview NOS Journaal vanwege de NAVO-oefening Cyber Coalition, 1-12-2016.

2 AD, 2-12-2016, < http://www.ad.nl/buitenland/rusland-vreest-cyberaanval-vanuit-nederland~ae0f49b8/>.

3 Vijfde dimensie naast land, water, lucht en ruimte ('space'). Zie M.A.D. Tettero & P. de Graaf, 'Het vijfde domein voor de krijgsmacht', in: *Militaire Spectator* 179 (2010) (5) 240-248. Zie voor een oudere agendering: NL ARMS 1999, *Information Operations*, J.M.J. Bosch, H.A.M. Luiijf & A.R. Mollema (red.).

4 Met uitzondering van de luchtmachtbijdrage aan de strijd tegen ISIS.

5 Dennis Broeders, *Investigating the place and role of the armed forces in Dutch cyber security governance*, Department of Sociology, Erasmus University Rotterdam (2014). Zie ook Kamerstukken II 2013–2014, 33 321, nr. 4.

FOTO MCD, P. NIJHUIS

Het Defensie Cyber Commando (DCC) is inmiddels een bekende speler in het digitale domein, samen met het Nationale Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie, en de Joint Sigint Cyber Unit van de AIVD en MIVD

de inhoud van de Defensie Cyber Strategie en de actualisering daarvan komen daarna aan de orde. Een reflectie op vitale belangen en een korte blik in de toekomst sluiten dit artikel af.

Parlementaire pressie

CDA-kamerlid Raymond Knops vroeg (tijdens de behandeling van de defensiebegroting op 3 december 2009) de regering via een motie 'in interdepartementaal verband een *cybersecurity* strategie te ontwikkelen' en 'actief bij te dragen aan de gedachtevorming over cyberwarfare binnen de NAVO'.[6]

Oud-officier Knops had zich laten leiden door de bedreiging die het toenemende aantal 'cyberaanvallen op computersystemen en netwerken' vormde. De verantwoordelijken daarvoor moesten gezocht worden in kringen van georganiseerde criminaliteit, terreurgroepen en krijgsmachten. Bovendien signaleerde hij dat 'diverse NAVO-landen speciale afdelingen opgericht hebben voor digitale oorlogsvoering [...] en daarbij ook offensieve capaciteiten ontwikkelen'. Hij stelde vast dat cyberwarfare in de Defensiebegroting 2010 ontbrak. In het Kamerdebat wees Knops expliciet naar een incident uit 2007, waarbij Estland digitale verstoringen (vanuit 'het assertieve' Rusland) moest incasseren.[7]

6 Motie-Knops, Voordewind, Eijsink: *Kamerstukken* II 2009/10, 32 123 X, nr. 66. Voortgang in 32 123 X, nr. 89; 26 643, nr. 149 en 164.

7 *Handelingen II* 2009-2010, 32-3020 (2 december 2009). Over dit incident: S.W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford: OUP, 2009, 3-6.

FOTO ANP, M. BEEKMAN

De start van de beleidsontwikkeling in het digitale domein ligt bij de motie-Knops. Oud-officier Knops vroeg aandacht voor de gedachtevorming over cyberwarfare binnen de NAVO

Een jaar later, op 14 december 2010, drong PVV-kamerlid en oud-officier Marcial Hernandez, gesteund door Knops, bij de regering aan 'met een visie te komen over de aanpak van cybercrime/cyberwarfare' waarin het ministerie van Defensie leidend zou moeten zijn.[8] Dit zou tot uitdrukking moeten komen in de inmiddels toegezegde beleidsvisie.

Krijgstaal en dreiging

Hernandez en Knops stonden niet alléén in het samenvoegen van de fenomenen cybercrime en cyberwarfare. Nog steeds leeft bij media en samenleving het idee dat deze twee fenomenen in elkaars verlengde liggen. Op zich is dat opmerkelijk: bankovervallen en het gewapende conflict tussen Oekraïne en Rusland in één adem noemen is immers in fysieke zin bepaald niet gebruikelijk. Terwijl in de digitale wereld martiale termen als 'cyberwarfare' en 'cyberattacks' veelvuldig criminele activiteiten, spionage en allerhande beveiligingsincidenten betreffen.

Sterker nog, een ordinaire diefstal van bedrijfsgegevens zou volgens menigeen aanleiding voor het opwerpen van militaire verdedigingslinies en zelfs een reactie met (digitale) middelen tot gevolg moeten hebben.[9] Dit soort uitspraken getuigt van een krijgshaftige inborst, die het milde militaire karakter van de Nederlandse samenleving miskent. Zelfs wetenschappers die waarschuwen voor een 'militarisering van cyberspace en cybersecurity' vertonen deze neiging tot overreactie.[10]

Diverse bedreigingen

Dat de bedreigingen in cyberspace divers zijn, werd duidelijk in november 2010 met het verschijnen van het Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010.[11] Anders dan het populaire taalgebruik suggereert, blijkt dan al dat de omvangrijkste bedreigingen geen relatie hebben met oorlogvoering maar met veiligheidsbewustzijn, criminaliteit en spionage.

Ook latere vervolgrapportages vanuit het Nationale Cyber Security Centrum (NCSC), zoals het Cyber Security Beeld Nederland (CSBN), tonen dit beeld.[12]

Toenemende afhankelijkheid van ICT

Het Trendrapport en de CSBN-rapporten benadrukken de toenemende afhankelijkheid van onze economie, maatschappij, bedrijven en burgers van het digitale domein. Dit domein biedt door de ontwikkelingen in de informatie- en communicatietechnologie (ICT) niet slechts ruimte voor zelfontplooiing en het benutten van grondrechten, voor onderwijs en commercie. Door de kwetsbaarheid en afhankelijkheid van digitale netwerken en systemen bevat het ook bedreigingen.

Anders gezegd: de technologische ontwikkeling leidt tot een verandering in menselijk gedrag en verstoringen in technische sfeer raken de mens, maatschappij en bedrijfsleven steeds meer. Niet alleen (individuele en collectieve)

8 Zie ook de motie-Hernandez, *Kamerstukken* II 2010/11, 32 500X, nr. 76.

9 Tijdens het Rondetafelgesprek Digitale oorlogvoering (20 maart 2014) voor de Vaste Kamercommissie van Defensie en Buitenlandse Zaken was dit een van de vragen van Kamerleden. Zie bijvoorbeeld de publieke reactie op de Sony-hack in de VS, 2014.

10 Zie bijvoorbeeld Albert Benschop, *Cyberoorlog: slagveld internet*, Tilburg: De Wereld, 2013.

11 *Kamerstukken* II 2010/11, 28 684, nr. 292: de ministers van Veiligheid & Justitie; Economische Zaken, Landbouw & Innovatie; en Defensie. Het Trendrapport is als bijlage bij dit kamerstuk opgenomen.

12 NCSC (2011) Cybersecurity Beeld Nederland 2011, CSBN-2 (2012), CSBN-3 (2013) en CSBN-4 (2014), via: < https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten>.

wenselijke kansen dienen zich aan, ook ongewenste negatieve kanten komen nadrukkelijk in beeld. De veiligheid in en van het digitale domein komt door malafide activiteiten of neveneffecten onder druk te staan. Digitale veiligheid, veiligheid in het digitale domein of cybersecurity, is in het Trendrapport gedefinieerd als 'een betrouwbare en veilige ICT-omgeving: voorkomen en bestrijden van misbruik en het herstel ervan'.[13]

Wake-up call

Naast de eerder genoemde criminaliteit en spionage leent cyberspace zich (uitstekend) voor subversie, sabotage, activisme en conflictueuze activiteiten die (soms) verband houden met rebellie, opstand, burgeroorlog en interstatelijke gewapende conflicten. Kortom: digitale dreiging in verschillende soorten en maten. Voor Europa en de NAVO dienden de op zichzelf staande digitale verstoringen in Estland (2007) als *wake-up call*.[14] Het Russisch-Georgisch conflict (2008) toont digitale niet-statelijke en patriottische Russische activiteiten die parallel lopen met de militaire fysieke acties.[15]

Digitale onveiligheid is een extreem heterogeen begrip. De omvangrijkste bedreigingen hebben geen relatie hebben met oorlogvoering maar met veiligheidsbewustzijn, criminaliteit en spionage

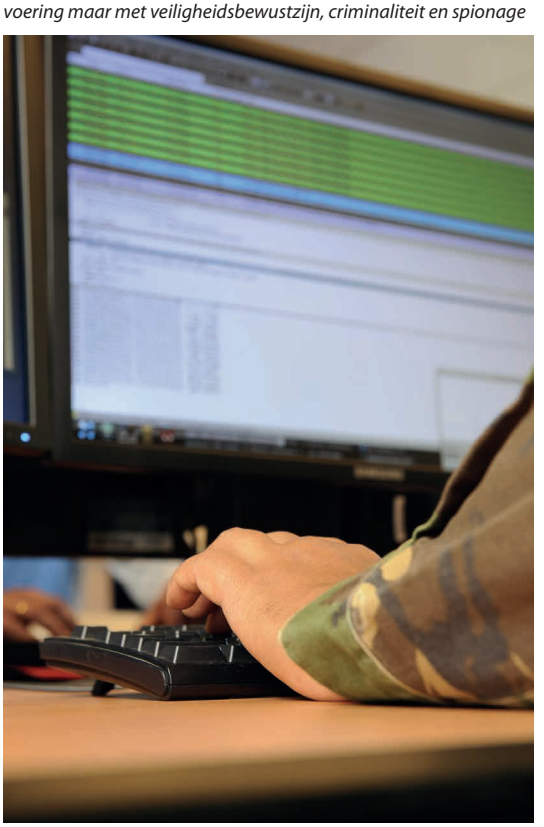


FOTO MCD, H. LEBBE

De ontdekking van Stuxnet trok wereldwijde aandacht als alternatief voor fysieke actie.[16] De uitgekiende *malware*, door de VS en Israël ontwikkeld, beoogde Iraans nucleaire productie te verstoren, het verrijkingsproces te vertragen en een fysieke interventie tegen dat programma uit te stellen, aldus David Sanger.[17]

Multidimensionale dreiging en een multidisciplinaire reactie

Digitale onveiligheid is een extreem heterogeen begrip. Bedreigingen verschillen qua aard en/of intentie. Digitale onveiligheid betreft (een combinatie van) ideologische, criminele, financiële, politieke, economische en militaire inbreuken.[18] Daarachter gaan zowel statelijke als niet-statelijke actoren schuil. Die laatste categorie omvat onder meer (combinaties van) criminelen, activisten, actiegroepen, terroristen, rebellen én commerciële bedrijven.

Een complicerende factor is het feit dat slachtoffers cyberinbreuken niet altijd openlijk delen (voor zover deze überhaupt bekend zijn bij de getroffen organisatie). Geconstateerde inbreuken zijn bovendien niet altijd – technisch of anderszins – te herleiden tot een 'auteur' van die inbreuk.[19]

13 Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010, *Kamerstukken* II 2010/11, 28 684, nr. 292 bijlage, 2.

14 Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: CCDCOE 2010) 15 e.v.

15 Tikk, Kaska & Vihul, 66 e.v..

16 NRC Handelsblad, 16-11-2010, *Kernreactors Iran mogelijk doelwit Stuxnet-worm*, <beta.nrc.nl/nieuws/2010/11/16/kernreactors-iran-doelwit-stuxnet-worm/>, benaderd: 9-12-2010; New York Times, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*: 15 january 2011, <www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>, benaderd: 19-1-2011.

17 David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown 2012) 188 e.v..

18 Tettero & De Graaf, 242.

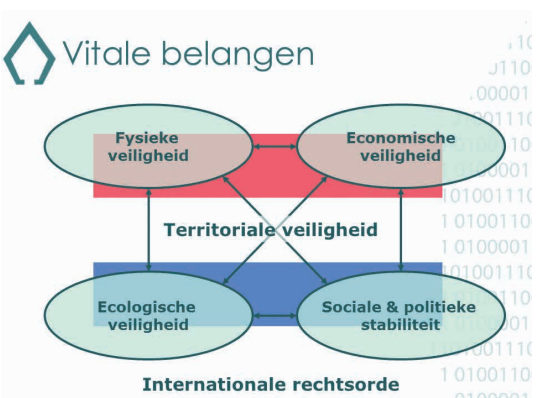
19 Auteur: diegene aan wie de actie wordt toegeschreven of toegedicht. Bijvoorbeeld de dader of de aanvaller.

Vitale belangen

Zo'n veelzijdig en divers dreigingsbeeld vraagt om een multidisciplinaire en getrapte reactie.[20] Uitgangspunt voor veiligheidszorg is de definiëring van 'vitale belangen' zoals dit in de periode 2005-2007 werd gezien:[21]

Vitaal belang: belang dat bepalend is voor de instandhouding van de territoriale, fysieke, economische, ecologische veiligheid en voor de politiek en sociale stabiliteit en maakt dat door het deels of geheel verstoord raken of wegvallen van dat belang het functioneren van de staat en de samenleving in potentie of feitelijk in gevaar komt.[22]

In combinatie met de Internationale Veiligheidsstrategie uit 2013,[23] die naast territoriale en economische veiligheid ook de internationale rechtsorde als een Nederlands vitaal belang aanmerkt, levert dit zes vitale belangen op (zie figuur 1).[24]



Figuur 1 Nationale vitale belangen[25]

De Nederlandse Staat en de Nederlandse overheid staan (uiteindelijk) voor de klassieke taak Nederlands vitale belangen te beschermen en te borgen, ook in het digitale domein. Dat de vitale sectoren doorsneden zijn met digitale systemen, en dat deze zelf veelal ook als vitaal aangemerkt zijn (bijvoorbeeld telecommunicatie), mag helder zijn.

Gelaagde veiligheidsstructuur

De getrapte reactie is bekend van het Stelsel Bewaken en Beveiligen, waarin veiligheidszorg volgens een 'getrapt' systeem is belegd bij
a. private partijen en burgers ('het slot op de deur');
b. decentrale overheden;
c. de rijksoverheid.

Uitgangspunt van het nieuwe stelsel is dat de *verantwoordelijkheid voor de eigen veiligheid primair ligt bij de burger zelf, de organisatie waartoe deze behoort (zoals het bedrijf waar hij werkzaam is) en het decentrale gezag. In aanvulling daarop is er sprake van een bijzondere verantwoordelijkheid van de Rijksoverheid voor een bepaalde groep personen, objecten en diensten.*[26]

Het programma 'bescherming van de vitale infrastructuur' en de Nationale Veiligheidsstrategie (2006-2007) hanteren die gelaagde veiligheidsstructuur eveneens.

De vraag is uiteraard hoe de regering deze digitale veiligheid getrapt en multidisciplinair gaat verzorgen.

Nationale Cybersecurity Strategie 1

Die visie op digitale veiligheid, de *Nationale Cybersecurity Strategie* (NCSS-1) werd op 22 februari 2011 aan de Tweede Kamer aangeboden.[27] Het integrale karakter kwam tot uitdrukking in de ondertitel 'Slagkracht door samenwerking' en de gezamenlijke aanbieding door de ministers van Veiligheid & Justitie, Economische Zaken, Landbouw en Innovatie, Defensie en Binnenlandse Zaken en Koninkrijksrelaties. De door Hernandez en Knops voorgestane alomvattende rol van Defensie kwam daarbij overigens niet tot stand: de coördinerende rol bij kwam bij V&J te liggen.

20 P.A.L. Ducheine, 'Legal Framework for Military Cyber Operations', *Militair Rechtelijk Tijdschrift*, 2013, 106 (1), 9-19, 12.
21 *Kamerstukken* II 2004/05, 26 643, nr. 75, 1, Beleidsbrief Bescherming Vitale Infrastructuur.
22 *Kamerstukken* II 2006/07, 30 821, nr. 2, 3.
23 *Kamerstukken* II 2012-13, 33 694, nr. 1, Internationale Veiligheidsstrategie – Veilige wereld, veilig Nederland.
24 Zie HCSS, The Hague Centre for Strategic Studies, *Defensie in het stemhokje*, 1: 'Nederland is een handelsland. Een stabiel internationaal systeem, waarin vrede, veiligheid en vrijhandel prevaleren, is van levensbelang', 2012.
25 Ducheine, P.A.L. *Krijgsmacht, Geweldgebruik & Terreurbestrijding; een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme.* Nijmegen: Wolf Legal Publishers (diss. UvA), 2008, 20.
26 *Kamerstukken* II, 2002/03, 28 974, nr. 2, 1.
27 *Kamerstukken* II, 2010/11, 26 643, nr. 174.

Nederlands ambitie, zo blijkt uit de NCSS-1, is 'uit te groeien tot de "Digital Gateway to Europe".[28] Het doel is 'het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen.'[29]

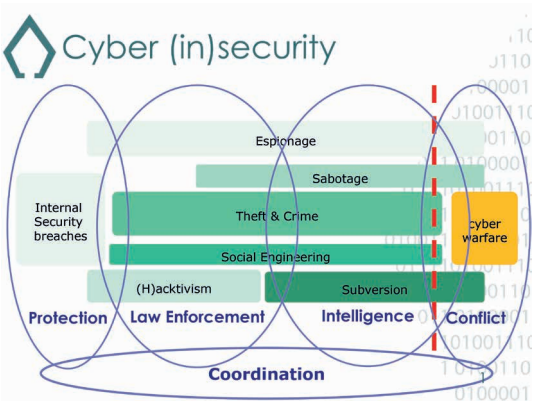
Zes actielijnen moeten dit doel binnen bereik brengen:
- integrale aanpak door publieke en private partijen;
- adequate en actuele dreiging- en risico-analyses;
- weerbaarheid tegen ICT-verstoringen en cyberaanvallen;
- responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren;
- opsporing en vervolging van cybercrime;
- onderzoek en onderwijs.

Uitgangspunten

Bij de uitwerking van doel en ambitie staan zes uitgangspunten centraal: verbinden en versterken van initiatieven; publiek-private samenwerking; eigen verantwoordelijkheid; actieve internationale samenwerking; proportionaliteit van maatregelen; zelfregulering als het kan, wet- en regelgeving als het moet.[30] In deze uitgangspunten klinkt zowel de democratische rechtsstaat, de Nederlandse staatsstructuur, als de technische en maatschappelijke realiteit door: infrastructuur is immers vaak in private handen en departementen delen verantwoordelijkheid in dit multidimensionale domein.

De strategie voorziet in de oprichting van een 'spin in het web': het Nationale Cyber Security Centrum (NCSC). Het NCSC, waarin het bestaande *Governmental Computer Emergency Response Team* (GovCERT) was opgenomen,[31] is ondergebracht bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het NCSC treedt coördinerend op bij cybersecurity-incidenten die tot overheidshandelen nopen.

Een alternatieve oplossing zou een nieuwe organisatie met eigen bevoegdheden zijn geweest, die tegen een breed spectrum – van 'scriptkiddies', hacktivisme, spionage,



Figuur 2 Digitale dreigingen en security paradigma's

subversie, sabotage, criminaliteit tot cyber-aanvallen met fysieke consequenties – aangewend kan worden.

Duidelijk is dat de organisatie van cybersecurity een klassiek bestuurskundig, (bureau)politiek en organisatiekundig probleem oplevert omdat coördinatie tussen de verschillende onderdelen vereist is.[32] Als gevolg daarvan ontstaan uiteraard ook staatsrechtelijke keuzemomenten (of problemen) die (nader) opgelost zullen moeten worden. De vraag is of oplossingen voor fysieke veiligheidsproblemen onverkort zijn toe te passen op en in het digitale domein.[33]

Private partijen

Naast de overheid is er ook een grote rol weggelegd voor particulieren en private partijen.[34] Dat heeft onder meer te maken met

28 NCSS-1, 3.
29 NCSS-1, 7.
30 NCSS-1, 5-6.
31 GovCERT diende ter bescherming van overheidsnetwerken tegen digitale dreigingen.
32 Zie bijvoorbeeld Muller, E.R., Rogier, L.J.J., Kummeling, H.R.B.M., Dammen, R., Bron, R.P., Woltjer, A.J.Th., & Klakhoven, V.C. *Bestuur, recht en veiligheid. Bestuursrechtelijke bevoegdheden voor openbare ordehandhaving en terrorismebestrijding*. Den Haag: Kluwer Juridische uitgevers, 2008; en Brainich von Brainich Felth, E.T. *Het systeem van crisisbeheersing; bevoegdheden en verplichtingen bij de voorbereiding op en het optreden tijdens crises*. Den Haag: Boom, 2004.
33 Zie bijvoorbeeld Ronald Prins (CEO FOX-IT): 'Een veilige cyberwereld vraagt nieuw denken', in: 38 *Justitiële verkenningen*, No. 1, 40-51, 44.
34 Naast de eigen verantwoordelijkheid in beveiliging die eenieder speelt (het slot op de deur). In cyber is eenieder bijvoorbeeld (mede)verantwoordelijk voor spamfilters, firewall, virusscanners, sterke wachtwoorden, et cetera.

de aard van internet, dat niet vanuit staten en overheden wordt 'bestuurd'. Veel van die private partijen zijn internationaal georganiseerd. Bovendien is een groot deel van de (vitale) digitale infrastructuur in private handen. Het is dan ook begrijpelijk dat de overheid publiek-private samenwerking (en partnership) in het digitale domein propageert. De strategie maakt verder duidelijk dat cybercriminaliteit en cyberwarfare (als bedreiging) slechts facetten zijn van het meer omvattende begrip 'cybersecurity'. Cybersecurity is in de NCSS-1 nog gedefinieerd als:

het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.[35]

Deze idealistische en absoluut geformuleerde 'resultaatsverplichting' zal in NCSS-2 worden omgezet in een realistische en relatief verwoorde 'inspanningsverplichting'. Samen met het Trendrapport en het Cybersecuritybeeld Nederland (2011) valt de overheidsinspanning bij cybersecurity in vijf conceptuele raamwerken (of paradigma's) te groeperen.[36] Het betreft bescherming, rechtshandhaving, inlichtingen, conflict en een noodzakelijk en overkoepelend coördinatiemechanisme.

Verschillende departementen

Binnen de overheid zijn meerdere departementen en diensten betrokken bij cybersecurity. Bovenal het ministerie van Veiligheid & Justitie (onder meer NCTV) als coördinator met daarbinnen het Openbaar Ministerie (vervolging en opsporing strafbare feiten), de (Nationale) Politie (opsporing), het ministerie van BZK (de AIVD), het ministerie van Economische Zaken, het ministerie van Infrastructuur en Milieu, en het ministerie van Defensie (waaronder de Commandant der Strijdkrachten, de Marechaussee en de MIVD).

Defensie

Met de NCSS-1 nam de regering alvast een voorschot op het – inmiddels gestarte – strategische besluitvormingsproces binnen Defensie aangezien *'[de] responscapaciteit om ook in het digitale domein effectief te kunnen opereren wordt versterkt, onder andere bij Defensie'*.[37] Dit betreft het vierde paradigma: conflict.

Daarnaast speelt Defensie een rol bij de andere paradigma's: bescherming van het Defensie digitale domein, rechtshandhaving via de Koninklijke Marechaussee en militaire bijstand aan de politie en ten slotte inlichtingen en veiligheidsinformatie via de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en haar samenwerkingsverbanden. Defensie moest dus vier paradigma's in een beleidsvisie en strategie verwerken.

Naar een Defensie cyberstrategie

De ontwikkeling van een beleidsvisie Defensie waarin 'cyberintensiveringen' een plaats hadden, stond niet op zichzelf.[38] Het Eindrapport Verkenningen 2010 bevatte al een beleidsoverweging in die richting:

Om de inzetbaarheid van de krijgsmacht te blijven waarborgen, zal Defensie haar digitale weerbaarheid de komende jaren belangrijk moeten versterken. Uitbreiding van de digitale kennis, vaardigheden en faciliteiten is nodig. Dit impliceert het vergroten van bewustwording van dagelijkse gebruikers en de inzet van specialisten op het gebied van digitale surveillance en emergency response. Uit militair oogpunt bestaat tevens behoefte meer inzicht te krijgen in cyberoperations, zowel [als] onderdeel van offensieve operaties als bij wijze van reactie op een aanval. Nationale en

35 NCSS-1, 4.

36 Zie: Ducheine, P.A.L., Voetelink, J.E.D., Stinissen, J., Gill, T.D. (2012), 'Towards a Legal Framework for Military Cyber Operations', in: Ducheine, P.A.L., Osinga, F., Soeters, J. (eds) (TMC Asser Press, The Hague), 101-128, 110; en Ducheine, P.A.L., 2015'. 'The Notion of Cyber Operations in International Law', in: Tsagourias, N., Buchan, R. (eds) *The Research Handbook on the International Law and Cyberspace*. Cheltenham: Edwar Elgar Publishing, 211-232.

37 *Kamerstukken* II, 2010/11, 26 643, nr. 174.

38 *Kamerstukken* II 2010-11, 26 643, nr. 174.

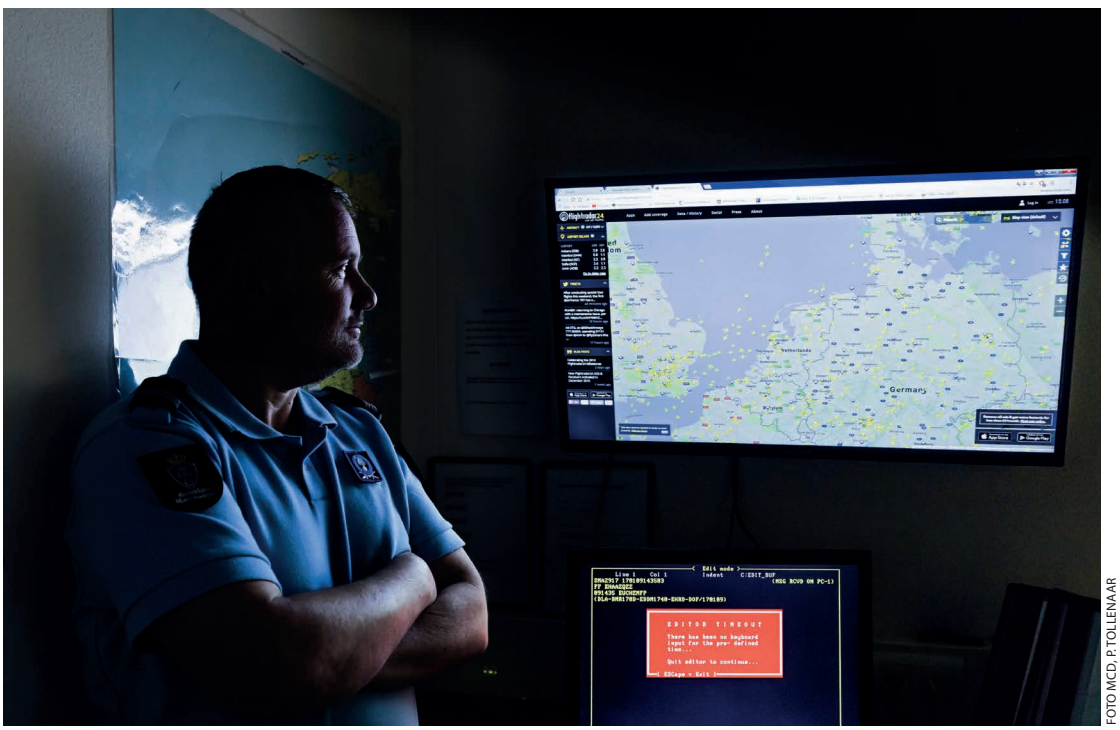


FOTO MCD, P. TOLLENAAR

Binnen de overheid zijn verschillende departementen betrokken bij cybersecurity. De Koninklijke Marechaussee (rechtshandhaving en militaire bijstand aan de politie) is er daar één van

internationale (NAVO en EU) afstemming en juridische inbedding zijn hierbij van wezenlijk belang.[39]

Ook de nota *Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld,* uit 2011, meldde dat '*Defensie haar digitale weerbaarheid de komende jaren [zal] versterken en het vermogen [zal] ontwikkelen tot het uitvoeren van cyber operations*'.[40] Aan dit beleidsvoornemen was een budget gekoppeld. Incidenten in die periode zoals Stuxnet en de Diginotar affaire,[41] brachten de bekendheid van de kwetsbaarheden op een hoger peil en voedden het gevoel van urgentie.

Veronderstellingen

De parlementaire wens om cybercapaciteiten te ontwikkelen houdt niet alleen verband met de bedreigingen tegen vitale belangen, maar mogelijk ook met het niet-kinetische karakter van cyberoperations en cyberwarfare: de gedachte dan wel hoop dat langdurige en omvangrijke inzet (van grondtroepen) daarmee vermeden kan worden, alsmede de perceptie dat cyberaanvallen 'chirurgisch' schoon (lees: met weinig *collateral damage*) en minder politiek gevoelig zijn.

Of dit juiste veronderstellingen en verwachtingen zijn, valt nog te bezien. Feit is dat het advies *Digitale oorlogvoering* dat de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstuk-

39 Ministerie van Defensie, *Eindrapport verkenningen - Houvast voor de krijgsmacht van de toekomst* (2010).

40 Zie de nota *Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld*, 8-4-2011, 22 van 42.

41 Diginotar was een certificeringsinstantie die gecompromitteerd bleek, waardoor Windows de door deze instantie verstrekte certificaten dreigde te blokkeren. Dit zou reguliere communicatie met bijvoorbeeld Word-documenten onmogelijk hebben gemaakt. Zie *Kamerstukken* II 2010–11, 26 643, nr. 188, met bijlage: Fox-IT, Interim report DigiNotar audit, 5 september 2011, <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf>;

ken (AIV & CAVV) in december 2011 uitbrachten,[42] na een schriftelijke ronde in juni 2012,[43] pas in het voorjaar van 2014 werd besproken.[44]

Knelpunten

Een van de grootste knelpunten voor de defensievisie behelsde het ontbreken van een integrale strategische visie: Nederland kent geen (lange) traditie met veiligheidsstrategieën. De Britse denktank Chatham House benadrukte in de studie *On Cyber Warfare* vooral de noodzaak voor een strategisch raamwerk voor cybersecurity en cyberwarfare.[45] De enige strategische documenten die naast de beleidsnota's van Defensie zelf ter beschikking waren, betroffen de Nationale Veiligheidsstrategie (2007) en de NCSS-1.[46] De Nederlandse Internationale Veiligheidsstrategie zag pas in 2013 het levenslicht.[47]

Het advies *Digitale Oorlogvoering* behandelde echter wel cruciale kwesties van politiek-strategische, militair-strategische en internationaalrechtelijke aard.[48] Daarmee beschikten de regering, Defensie en Buitenlandse Zaken in ieder geval over enige strategische fundering. De AIV & CAVV beschreven het digitale domein als: 'het geheel van ICT-middelen en ICT–diensten, [inclusief] alle niet met internet verbonden netwerken of andere digitale apparaten'.[49]

Dit digitale domein is door de mens gemaakt en bestaat uit alle 'entiteiten die digitaal verbonden (kunnen) zijn'.[50] Krijgsmachten hanteren een gelaagd model om werking en toepassing te beschrijven.[51] Het betreft een sociale laag met mensen en hun cyberidentiteiten (e-mailadressen, accounts, et cetera), een logische laag met cyberobjecten (software, applicaties, data) en een fysieke laag met hardware en geografische locaties.[52] Communicatie en informatie tussen de verschillende entiteiten in de lagen staan centraal.[53] De verschillende lagen bieden aanknopingspunten voor beïnvloeding, manipulatie en verstoring waartegen bescherming geboden is. De lagen bieden ook kansen voor het verzamelen en verwerken van informatie, alsmede voor het militair gebruik in operaties.[54]

De tevens door de AIV & CAVV aangedragen operationele drieslag, defensief-inlichtingen-offensief,[55] keerde ook als centraal element terug in de *Defensie Cyber Strategie* die minister Hillen in juni 2012 presenteerde.[56] Die drieslag sluit aan bij drie van de vier voor Defensie relevante paradigma's.[57]

Defensie cyberstrategie

Het doel van de DCS is cyberspace optimaal gebruiken om 'inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te vergroten'.[58] Het startpunt in de DCS is dat 'de drie hoofdtaken van Defensie [..] ook in het digitale domein leidend [zijn] voor de inspan-

42 Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken (AIV & CAVV (2011): *Digitale oorlogvoering*, Den Haag: AIV no. 77; CAVV no. 22, zie <www.aiv-advice.nl>.

43 *Kamerstukken* II 2011–12, 33 000 X, nr. 99 (Vragen en antwoorden VCD).

44 *Kamerstukken* II 2013–14, 33 321, nr. 4 (AO Defensie Cyber Strategie), 26 maart 2014. Dit stond los van de parallelle parlementaire sessies inzake het bredere cyber security die in de Vaste Kamercommissie voor V&J plaatsvonden.

45 P. Cornish, D. Livingstone, D. Clemente & C. Yorke, *On Cyber Warfare*, Chatham House, 2010, 21-22.

46 Zie Tettero & de Graaf.

47 *Kamerstukken* II *2012-13*, 33 694, nr. 1, Internationale Veiligheidsstrategie – Veilige wereld, veilig Nederland.

48 AIV & CAVV, 5: '1. Op grond van welke politieke en militaire doelstellingen moeten operationele cybercapaciteiten worden ontwikkeld en kunnen worden ingezet? 2. Wat is de aard en rol van operationele cybercapaciteiten bij militaire operaties? […] 4. Onder welke omstandigheden kan een cyberaanval worden beschouwd als een gewapende aanval waartegen geweld mag worden gebruikt ter zelfverdediging op basis van artikel 51 van het VN Handvest? 5. Wanneer is er sprake van toepasselijkheid van het humanitair oorlogsrecht op gedragingen in het digitale domein?'

49 AIV & CAVV, 7.

50 C.W.M Dessens (2014) *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 - Naar een nieuwe balans tussen bevoegdheden en waarborgen*, in: *Kamerstukken II* 2013–14, 33 820, nr. 1 bijlage, 85.

51 United States Army Training and Doctrine Command (TRADOC 2010), *The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028*, TRADOC Pamphlet 525-7-8, 8. Idem: Wouter Stol (2010), *Cybersafety overwogen - Een introductie in twee lezingen*, Den Haag: Boom Juridische uitgevers.

52 P.A.L. Ducheine & J. van Haaster (2014) 'Fighting Power, Targeting and Cyber Operations', in: Brangetto, P., Maybaum, M., Stinissen, J. (eds) *Proceedings of the 6th International Conference on Cyber Conflict* (2014). CCDCOE, Tallinn, 303-328, 309.

53 Zie de minister van Defensie, in*: Kamerstukken* II 2013–14, 33 321, nr. 3, 2.

54 P.A.L. Ducheine & Jelle van Haaster (2013) 'Cyber-operaties en militair vermogen', *Militaire Spectator* 182 (9) 368-387.

55 Ook reeds in: *Kamerstukken* II 2010-11, 32 733, nr. 1, 19, Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld (8-4-2011).

56 *Kamerstukken* II 2011-12, 33 321, nr. 1 (27-6-2012).

57 De AIV&CAVV waren niet specifiek naar nationale rechtshandhaving gevraagd.

ningen van de krijgsmacht. Zij moet derhalve handelend kunnen optreden tegen een digitale bedreiging van de samenleving of van de internationale rechtsorde'.[59]
Dit sluit aan bij de eerder genoemde vitale belangen (zie figuur 1), bij de grondwettelijke doelomschrijving[60] en bij de hoofdtaken van de krijgsmacht: 'De Nederlandse krijgsmacht trekt hier de noodzakelijke conclusies uit en wil ook in het digitale domein haar rol als 'zwaardmacht' naar behoren vervullen'.[61]

Om dit doel te realiseren, zijn zes 'speerpunten' gedefinieerd, waaronder drie randvoorwaardelijke:
- een integrale aanpak;
- versterking van de kennispositie en het innovatieve vermogen van Defensie in het digitale domein, inclusief werving en het behoud van gekwalificeerd personeel ('adaptief en innovatief');
- intensivering van de samenwerking in nationaal en internationaal verband ('samenwerking').

De kern van de strategie betreft de drieslag:
- versterking van de digitale weerbaarheid van Defensie ('defensief');
- versterking van de inlichtingenpositie in het digitale domein ('inlichtingen');
- ontwikkeling van het militaire vermogen om cyberoperations uit te voeren ('offensief').

De integrale aanpak had al geresulteerd in de instelling van de Task Force Cyber, die de coördinatie over en de uitwerking van de speerpunten ter hand moest nemen. De DCS omvat duidelijk herkenbaar drie paradigma's: bescherming, inlichtingen en conflict. Het rechtshandhavingsparadigma (voor de Koninklijke Marechaussee) ontbreekt vooralsnog, hoewel dit bij een enkeling wel in beeld is.[62]
De – in totaal – vier cyber security paradigma's waaraan defensie bijdraagt, resulteren in vier onderscheidende cyberrollen binnen defensie.[63] De rollen kennen elk hun eigen juridische en bestuurlijke raamwerk, zijn veelal ondergebracht bij verschillende defensieonderdelen, en kennen hun eigen taken, bevoegdheden en verantwoordingslijnen.

Figuur 3 Vier digitale rollen Defensie

Bescherming
De eerste rol betreft *bescherming (of beveiliging)* van de interne bedrijfsvoering in vredestijd alsmede (ondersteuning van de) commandovoering tijdens inzet.[64] De rol omvat taken voor bijvoorbeeld Joint Informatievoorzieningscommando, DefCERT, de afdeling (ICT) Operations van de Defensie Materieel Organisatie, de Beveiligingsautoriteit, maar ook voor de MIVD.

Deze rol treft ook de individuele militair, commandanten en leidinggevenden omdat dit ook de handhaving van interne veiligheidsvoorschriften omvat. Kennisverbetering, scholing, bewustwording en weerbaarheid, maar ook fysieke beveiliging, kwaliteitseisen voor systeemontwerp, hard- en software horen bij deze rol.

58 DCS, 2 en *Kamerstukken* II 2014-15, 33 321, nr. 5, Actualisering Defensie Cyber Strategie, 1.
59 *Kamerstukken* II 2011-12, 33 321, nr. 1, Defensie Cyber Strategie, 2. (hierna DCS).
60 Zie art. 97 Grondwet en P.A.L. Ducheine & K.L. Arnold (2015), 'Besluitvorming bij cyberoperaties', *Militaire Spectator* 184 (2015) (2) 56-70.
61 DCS, 2.
62 Editoriaal 'Marechaussee & cyber', in: *Militaire Spectator* 182 (2013) (6) 278-279.
63 Ducheine (2015 in Tsagourias).
64 Ducheine (2015 in Tsagourias), 221. Zo ook A. Klimburg & P. Mirtl, 'Cyberspace and Governance—A Primer'Austrian Institute for International Affairs . Zie: <http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Cyberspace_and_Governance_-_Working_Paper_65_2.pdf> (benaderd 11 November 2013); en A. Klimburg (ed.) *National Cyber Security Framework Manual* (CCD COE 2012).

Rechtshandhaving
De tweede rol betreft *rechtshandhaving*. De Koninklijke Marechaussee, een militaire politieorganisatie die beheersmatig bij Defensie is ondergebracht maar qua rechtshandhaving onder civiel gezag opereert, speelt voor defensie zelf een rol (op objecten in beheer bij defensie; jegens de strijdkrachten), maar ook op andere terreinen waar zij op grond van art. 4 Politiewet 2012 bevoegd is.

Daarnaast kan de krijgsmacht (inclusief Koninklijke Marechaussee) bijstand leveren aan de civiele politie op grond van art. 57-58 Politiewet 2012. Zij treedt dan op onder civiel gezag (burgemeester c.q. officier van justitie dan wel de minister van Veiligheid en Justitie).

Inlichtingen
Ten derde is er de *inlichtingenrol*. Dit ligt uiteraard bij de MIVD, die naast interne intensivering samen met de AIVD een *Joint Sigint Cyber Unit* (JSCU) oprichtte.[65] Deze eenheid heeft als taken: het verwerven van gegevens uit technische bronnen; het ontsluiten van gegevens uit technische bronnen; ondersteuning bij analyse; het leveren van Signals intelligence en cybercapaciteit. De reguliere taken van de MIVD die verband houden met het digitale domein liggen besloten in de Wet op de inlichtingen- en veiligheidsdiensten 2002.[66]

Conflict
De vierde rol ligt in het domein van de Commandant der Strijdkrachten (en de operationele commando's): de inzet van operationele cybercapaciteiten die *conflict*-gerelateerd zijn.

Een operationele cybercapaciteit omvat alle kennis en middelen die nodig zijn om gedurende operationele inzet langs digitale weg het handelen van tegenstanders te voorspellen, te beïnvloeden of onmogelijk te maken, en zich te verdedigen tegen vergelijkbaar handelen door de tegenstander. Dit gebeurt door infiltratie van computers, computernetwerken, wapen- en sensorsystemen en software om informatie en inlichtingen te vergaren en systemen te beïnvloeden. Een operationele cybercapaciteit omvat dus inzetbare defensieve, inlichtingen- en offensieve elementen.[67]

Deze rol is toebedeeld aan het nieuwe Defensie Cyber Commando (DCC), dat – na reorganisatieperikelen – daadwerkelijk in juni 2015 is opgericht.[68] Het DCC, een krijgsmachtbrede ('joint') eenheid, is administratief ondergebracht bij het Commando Landstrijdkrachten. Het omvat een Defensie Cyber Expertise Centrum (DCEC), een technische poot en een operationele poot. De technische poot ontwikkelt cybercapaciteiten en deelt kennis met specialisten uit de andere drie rollen. De operationele poot vormt de verbinding tussen technische expertise en de eindgebruikers: militaire commandanten.

In de DCS is het DCEC aangewezen als centrale kennisorganisatie voor Defensie en is het verantwoordelijk voor kennisontwikkeling, borging en verspreiding binnen de gehele defensieorganisatie. Het DCEC heeft relaties met externe en interne kennisinstituten, en organisaties als TNO, *NATO's Cooperative Cyber Defence Centre of Excellence* (CCDCOE) in Tallinn en de leerstoel Cyber Operations & Cyber Security van de Nederlandse Defensie Academie. Deze leerstoel en het DCEC geven beide mede invulling aan de speerpunten kennis, innovatie en samenwerking.

De operationele cybercapaciteit varieert van defensief tot offensief, van inlichtingen verzamelen binnen de verantwoordelijkheid van de Commandant der Strijdkrachten (CDS) tot het beïnvloeden van actoren via het digitale domein. Dit kan uiteindelijk uitmonden in disruptieve acties tegen opponenten.[69]

65 *Kamerstukken* II 2013-14, 29 924, nr. 113 (Oprichting en convenant JSCU).
66 Zie de taken in art. 7 Wiv 2002 en de daarbij te hanteren bevoegdheden in artt. 12, 17, 20-30. Voor een evaluatie van de wet, zie Dessens (2014).
67 DCS, 4-5.
68 Aanvankelijk zou het DCC in 2015 worden opgericht. In de nota 'In het belang van Nederland' (Kamerstukken II, 2013-14, 33 763, nr. 1) werd dit versneld beoogd in 2014. Minister Hennis-Plasschaert gaf op 25 september 2014 dan ook het 'virtuele' startschot, maar reorganisatieperikelen vertraagden dit. Zie: <http://www.defensie.nl/actueel/nieuws/2014/09/25/minister-geeft-startschot-voor-defensie-cyber-commando>.
69 Voor een overzicht van de diverse opties: Ducheine & van Haaster (2013). Disruptief heeft hier een brede betekenis (Van Dale: verbrekend, verwoestend) en omvat ook '*destroy, degrade, disrupt, deny*'.

Weinig aandacht voor constructieve capaciteiten

Tot nu toe heeft constructieve toepassing in Nederland weinig aandacht gekregen. Het betreft bijvoorbeeld *information operations* die een positief beeld wegzetten van de eigen inzet via *social media*. Bijvoorbeeld via het plaatsen van beeldmateriaal van een F-16 of Apache dat de zorgvuldige besluitvorming van vliegers bij luchtaanvallen demonstreert.

Buitenlandse initiatieven, zoals de oprichting van 77 (UK) Brigade die de 'focal point for levers of soft power […] or persistent engagement' is, brengen hier mogelijk verandering in. De aandacht voor informatieoperaties waarbij het digitale domein als medium fungeert, waarbij beelden en beeldvorming centraal staat, groeit gestaag. Het is niet vreemd in Nederland als de CDS zijn 'soft' power capaciteiten, anders dan nu, zou (laten) organiseren.[70]

De meeste aandacht van onder andere media en parlement gaat uit naar disruptieve, offensieve capaciteiten. Deze beogen met cyberoperaties schade of verstoring/vertraging te veroorzaken bij anderen (onder wie tegenstanders). Dit betreft cyberwarfare in de definitie van het AIV:

het uitvoeren van militaire operaties die erop zijn gericht om met digitale middelen computersystemen of netwerken van een tegenstander te verstoren, misleiden, veranderen of vernietigen.[71]

Het gaat – in de context van militaire operaties die aan de CDS zijn toevertrouwd – bijvoorbeeld om de inzet van *malware* (zoals bijvoorbeeld Stuxnet), afvangen en manipuleren van communicatie, digitale *social engineering*, et cetera. Minister Hennis wijdde een aparte brief aan deze capaciteit:

Offensieve cybercapaciteiten zijn de digitale middelen die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Deze capaciteiten kunnen in een militaire operatie worden ingezet ter ondersteuning van conventionele militaire capaciteiten.[72]

FOTO MCD, A. SALAMPESSY

Minister Hennis van Defensie wijdde een aparte brief aan de inzet van offensieve cybercapaciteiten

Ten tijde van het uitbrengen van de DCS stelde de regering:

De ontwikkeling van offensieve operationele capaciteiten staat internationaal nog in de kinderschoenen. Er is nog veel onduidelijk over de aard van deze capaciteiten, de mogelijkheden die ze kunnen bieden en de effecten die ermee kunnen worden gesorteerd.[73]

Alsof zij die onduidelijkheid wilde benadrukken, hanteert de regering zelf een eenzijdig beeld van deze offensieve capaciteiten door te stellen dat deze zich *van conventionele militaire capaciteiten [onderscheiden] doordat ze vaak slechts eenmalig inzetbaar zijn en veelal een beperkte levensduur hebben.*[74]

Deze focus op eenmalige, in tijd kritisch inzetbare cybercapaciteiten valt samen met een nadruk op hoogtechnologische capaciteiten, zo blijkt:

Hoogwaardige cybercapaciteiten zijn nauwelijks vergelijkbaar met algemeen bekende, relatief laagdrempelige en wijdverbreide aanvalsmethoden. Het gaat hier om complexe middelen waarvan de ontwikkeling zeer kennisintensief is en daardoor

70 Zie: <https://britisharmedforcesreview.wordpress.com/2015/01/31/the-security-assistance-group-now-the-77th-brigade/>.
71 AIV & CAVV (2011), 8.
72 *Kamerstukken* II 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten, 2.
73 DCS 2012, 7 (Kamerstukken versie).
74 DCS 2012, 7 (Kamerstukken versie).

kostbaar en tijdrovend. Een uitdaging is dat de gewenste effecten moeilijk gegarandeerd kunnen worden doordat de tegenstander op elk moment zijn eigen kwetsbaarheid kan ontdekken en beperken.[75]

Hoe het ook zij, het fameuze Stuxnet is meermaals en gedurende langere tijd ingezet in Iraanse nucleaire faciliteiten.[76] Ook 'algemeen bekende, relatief laagdrempelige en wijdverbreide aanvalsmethoden'[77] zoals DDoS-aanvallen kunnen vaker gebruikt worden tijdens conflictsituaties.[78] En sommige ICT-systemen worden ondanks bekende cyberbedreigen bewust slechts mondjesmaat van softwareaanpassingen voorzien.[79] Daarnaast waant men zich regelmatig veilig vanwege een (van internet) losstaand *Industrial Control System* van internet, en blijft repareren van kwetsbaarheden, *patchen,* (daardoor) soms achterwege.[80] Bovendien zou bijna vergeten worden dat naast deze op cyberobjecten gerichte aanvallen, het ambachtelijke kraken van toegangscodes, het via *social engineering* toegang verkrijgen tot cyberidentiteiten (onder meer administrator accounts), een andere aanvalsmethode is. Ook op deze cybercapaciteit past de hoogtechnologische, vergankelijke en tijd-kritische typering niet.[81]

Recente Kamerbrieven

Recentere Kamerbrieven bevatten gelukkig een nuancering:

Dit laat onverlet dat in operaties ook kan worden gebruikgemaakt van minder complexe en mogelijk laagdrempelige cybercapaciteiten. Maar ook hiervoor is een goede inlichtingenpositie onontbeerlijk.[82]

De actualisering van de DCS van februari 2015, zet deze draai verder kracht bij:

Offensieve cybermiddelen kunnen variëren van relatief eenvoudig en snel te ontwikkelen middelen met een tactische impact tot aan middelen met een hoge, strategische impact die een lange ontwikkelingstijd vergen.[83]

De actualisering uit 2015 benadrukt daarnaast dat cybercapaciteiten in een breed spectrum van gewenste effecten kunnen worden ingezet: van strategisch tot tactisch. Gecombineerd met een technische variëteit van laagwaardig tot hoogwaardig zijn zo verschillende capaciteiten te duiden: hoogtechnologisch/strategisch, hoogtechnologisch/tactisch, laag-technologisch/strategisch en laag-technologisch/tactisch.

Deze vierdeling kan verder gedifferentieerd worden naar de aard van de gewenste effecten, oftewel het doel van de inzet, en kan variëren van (tijdelijk of permanent) disruptief (inclusief vernieling) tot constructief.[84] Dat laatste gebruik sluit aan bij de eerder genoemde notie van soft power, van beïnvloeding via het informatiedomein, in dit geval cyberspace.[85]

Deze uitbreiding van mogelijkheden sluit aan bij de notie dat de krijgsmacht effecten en beïnvloeding van actoren in militaire operaties centraal stelt.[86] Deze *effect-based* en *manoeuvrist approach* onderstreept dat de doelstelling van

75 DCS 2012, 7 (Kamerstukken versie). Idem: *Kamerstukken* II 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten, 2.

76 Ralph Langner, *To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (November 2013), via < www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>; Sanger, David (2012) *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown. Het moment van lokale ontdekking en publieke bekendheid kunnen verschillen.

77 DCS 2012, 7 (Kamerstukken versie).

78 Waarbij een slachtoffer zich uiteraard kan beschermen. Zie o.a. Carol Matlack, 'Cyberwar in Ukraine Falls Far Short of Russia's Full Powers,' *Bloomberg Business Week*, <businessweek.com/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers> (accessed March 11, 2014).; See also: Reuters, 'Ukrainian Authorities Suffer New Cyber Attacks,'Reuters, <reuters.com/article/2014/03/08/us-ukraine-cricis-cyberattack-idUSBREA270FU20140308> (accessed March 11, 2014).; Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2nd ed. (New York: Syngress, 2014), 139

79 Zoals o.a. bij labiele *legacy* systemen waarbij *patchen* onvermoede complicaties veroorzaakt.

80 Ook losstaande (*air-gapped*) systemen kunnen bijvoorbeeld met akoestische signalen benaderd worden. Zie: Michael Hanspach & Michael Goetz (2013) 'On Covert Acoustical Mesh Networks in Air', in: *Journal of Communications* 8 (11), 758-767.

81 Voor een overzicht van methoden en technieken: Ducheine & Haaster (2014), 317-328.

82 *Kamerstukken* II 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten, 2.

83 *Kamerstukken* II 2014-15, 33 321, nr. 5, 11.

84 Zie hiervoor Ducheine & van Haaster (2013), 386.

85 Zie het gebruik van social media door ISIS: J.M. Berger & Jonathon Morgan (2015). *The ISIS Twitter Census - Defining and describing the po pulation of ISIS supporters on Twitter* Brookings Institute; Christina Schori Liang (2015) *Cyber Jihad: Understanding and Countering Islamic State Propaganda* GCSP Policy Paper 2015/2.

86 Zie Ministerie van Defensie, *Netherlands Defence Doctrine*, 2013. <http://www.defensie.nl/binaries/defensie/documenten/publicaties/2013/11/20/defence-doctrine-en/defensie-doctrine_en.pdf> banderd 16 maart 2014 (p. 111). The Hague; en Koninklijke Landmacht. (2015). Doctrine Publicatie 3.2 Landoperaties (DPLO 3.2).

FOTO MCD, E. KLIJN

Sinds begin 2014 doet de Islamitische Staat in Irak en Syrië meermaals en vaak barbaars van zich spreken. In de coalitie tegen ISIS leek aanvankelijk geen plaats voor Nederland te zijn voorzien

militaire operaties (cyberoperaties incluis) niet alleen het verslaan van opponenten is. Ook andere (zijdelings) betrokken partijen, zoals de bevolking in een missiegebied, bondgenoten, neutrale partijen, afzijdige partijen, kunnen beïnvloed worden.

De actualisering van de DCS

De in het Algemeen Overleg van 26 maart 2014 (waarin het AIV-CAVV-advies 'Digitale oorlogvoering' en de DCS werden besproken) toegezegde actualisering van de DCS is op 23 februari 2015 aan het parlement aangeboden.

De actualisering werd beïnvloed door een aantal – voor Defensie relevante – gebeurtenissen. In chronologische volgorde betreft dit allereerst de onthullingen van Edward Snowden vanaf juni 2013.[87] Kort daarop verscheen de *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 - Naar een nieuwe balans tussen bevoegdheden en waarborgen*, van de Commissie Dessens.[88] De eerder genoemde brief over 'offensieve cybercapaciteiten' van 17 maart 2014 dateerde nog van voor het algemeen overleg.[89]

Op het wereldtoneel culmineert de crisis om de Krim ondertussen in de annexatie van de Krim door Rusland op 18 maart 2014. De vlam slaat sindsdien in de pan in (Oost-) Oekraïne. En sinds het voorjaar van 2014 doet de Islamitische Staat in Irak en Syrië (ISIS of Daesh) meermaals en vaak barbaars van zich spreken.

In juni 2014 bracht het NCSC inmiddels het vierde Cyber Security Beeld Nederland uit. In

87 Zie o.a. Luke Harding (2014) *The Snowden Files: The Inside Story of the World's Most Wanted Man (Pb ed.): Vintage.*

88 C.W.M Dessens (2014) *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 - Naar een nieuwe balans tussen bevoegdheden en waarborgen*, in: *Kamerstukken II* 2013–14, 33 820, nr. 1 bijlage.

89 *Kamerstukken* II 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten.

november 2014 reageerde de regering op de evaluatie van de Commissie Dessens inzake de modernisering van de Wet- op de inlichtingen en veiligheidsdiensten.[90] En na de NAVO-top in Wales is Nederland figuurlijk 'te klein' omdat in de coalitie tegen ISIS aanvankelijk geen plaats voor Nederland lijkt te zijn voorzien. Begin januari schrikt Europa van aanslagen in Parijs, onder andere op de redactie van het tijdschrift Charlie Hebdo, en van een ingreep van justitie en politie in Verviers, België.

Speerpunten

Tegen deze achtergrond, herhaalt de minister van Defensie eerst dat de 'digitale revolutie' kansen biedt om de 'doeltreffendheid en de doelmatigheid van het militaire optreden wezenlijk te bevorderen'.[91] Zij houdt in grote lijnen vast aan de DCS uit 2012, waarbij zij – naast de trits weerbaarheid, inlichtingenvermogen, operationele capaciteit – vier randvoorwaardelijke speerpunten noemt. Het gaat om boeien, binden en ontwikkelen van cyberprofessionals; innoveren; bundelen en samenwerken; en kennis verdiepen.

Vooral op het DCC, de operationele cybercapaciteit, geeft de Kamerbrief verdieping ten opzichte van de DCS:

Om de verantwoorde en doeltreffende inzet van digitale middelen in militaire operaties mogelijk te maken, zal Defensie de komende tijd in het bijzonder aandacht geven aan:

- *de verdere ontwikkeling van een Defensie Cyber Doctrine;*
- *de ontwikkeling van offensieve cybermiddelen en van richtlijnen voor de gereedstelling van flexibel samen te stellen cybereenheden en cybermiddelen;*
- *de inrichting van defensieve digitale middelen bij missies;*
- *de ontwikkeling van cyber(inlichtingen)middelen voor tactische inzet;*
- *de integratie van cyberaspecten in het operationeel besluitvormingsproces, voorafgaand aan en tijdens operaties.*[92]

Onder het speerpunt 'samenwerking' komt na lang touwtrekken uiteindelijk ook de Koninklijke Marechaussee in beeld. Als politieorganisatie werd zij niet expliciet in de NCSS-1 en -2 genoemd. Maar gelet op de algemene en de specifieke taken was al duidelijk dat zij 'geraakt' zou worden door de toename van digitale ontwikkelingen.

Ook het voorziene wetsvoorstel Computercriminaliteit III raakt de Marechaussee door de voorgestelde introductie van nieuwe strafbaarstellingen en opsporingsbevoegdheden. Bovendien leidt inzet van het Defensie Cyber Commando tot een extra rol in de *ex post* beoordeling van militaire operaties, zoals dat bij fysieke operaties (regulier of speciaal) al het geval is.

Nuancering van cybercapaciteiten

Een ander markant punt in de actualisering is de nuancering van cybercapaciteiten. Waar deze voorheen vrij eenzijdig als strategisch, hoogtechnologisch, vluchtig en tijd-kritisch werden aangemerkt, herkent de minister nu ook tactische, eenvoudigere, meermalig en niet-tijdgebonden inzetbare capaciteiten. Of zij daarmee ook (al) oog heeft voor 'soft' cybercapaciteiten voor constructieve effecten of dat het digitale domein slechts dient als medium voor het overbrengen van effecten, bijvoorbeeld ter beïnvloeding, is zeer de vraag.

De Oekraïne-crisis en de strijd tegen ISIS bevestigen dat niet slechts fysieke actie maar vooral informatie en communicatie als boodschap en 'wapen' wordt aangewend.[93]

Cybersecurity: vitaal belang?

Niet-statelijke actoren, zoals ISIS, terroristische en criminele netwerken, maar ook multinationals, internationale organisaties, gelegenheidscoalities van burgers (bijvoorbeeld tijdens de Arabische Lente) of belangengroepen (bijvoor-

90 *Kamerstukken* II 2014–15, 33 820, nr. 4.

91 *Kamerstukken* II 2014-15, 33 321, nr. 5, 1.

92 *Kamerstukken* II 2014-15, 33 321, nr. 5, 11.

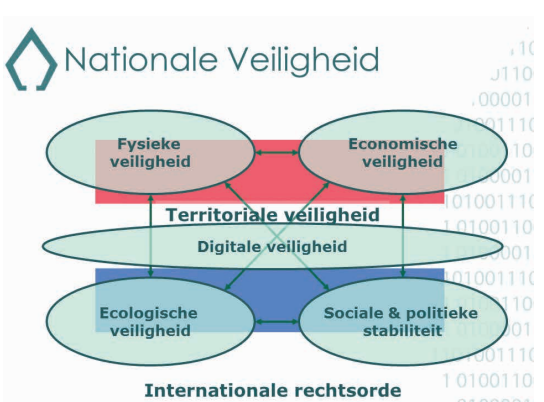
93 Zie ISIS' *Al-Hayat Media Centre* <http://jihadology.net/category/al-%E1%B8%A5ayat-media-center/> en het tijdschrift *Dabiq*, <www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq>, evenals Al Qaida's *Al-Shahab*, in: Carloen Roelants 'Terrorisme bestaat niet zonder communicatie - De mediastrategie van IS', *NRC Handelsblad* (16-9-2014).

FOTO ANP, F. VAN DEN BERGH

Ook niet-statelijke actoren, waaronder gelegenheidscoalities van burgers of belangengroepen zoals GeenPeil, manifesteren zich steeds vaker als machtsspeler

beeld GeenPeil 2.0) manifesteren zich – in toenemende mate – ook als machtsspeler. Informatie als machtsbron is in het huidige digitale tijdperk toe aan een herwaardering.[94]

Via directe dwang (dreigen met onthulling), door institutionele (sleutelposities binnen ICANN)[95] of structurele macht (Microsoft, met het besturingssysteem Windows) is dit bekend terrein. Maar vooral als productieve machtsfactor komt informatie toenemend tot wasdom.



Figuur 4 Nationale veiligheid met zeven vitale belangen

Dat wil zeggen dat actoren met informatie agenda's kunnen vormen en een debat kunnen starten, versterken en beïnvloeden.[96] Dit geheel faciliteert nieuwe 'elites' en actoren.

De proliferatie van ICT en de brede maatschappelijke afhankelijkheid van ICT brengt onze (interdependente) vitale economische, bestuurlijke, politieke en sociale processen binnen het bereik van deze actoren. Een geavanceerde digitale samenleving en economie is dus niet slechts een zegen én een machtsfactor, maar ook een kwetsbare en alle vitale belangen doorsnijdende factor.[97] In dat opzicht zou ons begrip van nationale veiligheid ondertussen best een zevende vitale belang kunnen bevatten: digitale veiligheid (zie figuur 4).[98]

94 Zie o.a. Jelle van Haaster, Assessing Cyber Power, in: N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.), *8th International Conference on Cyber Conflict: Cyber Power*, Tallinn: CCDCOE, 2016, via: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2001%20Assessing%20Cyber%20Power.pdf>

95 ICANN verzorgt onder meer domeinnamen en IP-nummers.

96 David Betz & Tim Stevens, Power and cyberspace, *Adelphi Series*, 2011.

97 McKinsey Global Institute, *Digital globalization: The new era of global flows*, March 2016, via: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>.

FOTO MCD, G.VAN ES

Cybersymposium op de NLDA: een geavanceerde digitale samenleving is ook kwetsbaar

Tot slot

Inmiddels liggen twee genoemde wetsvoorstellen, *Wet Computercriminaliteit III* en *Wet op de inlichtingen en veiligheidsdiensten 20..* [sic], in de Eerste Kamer. Het parlement is dus aan zet.[99] Die voorstellen en de parlementaire reactie zijn bepalend voor de uiteindelijke bevoegdheden en taakvervulling van respectievelijk de Marechaussee en de MIVD. Met het feit dat het DCC in de loop van 2017 operationeel wordt en de voortdurende inspanningen om de defensie-ICT beveiliging te verbeteren, zijn er voldoende impulsen voor verdere ontwikkelingen.

Het idee dat informatie, communicatie en de informatieomgeving, waarvan cyberspace deel uitmaakt, de volgende *high grounds* voor toekomstige inzet worden, heeft inmiddels stevig postgevat.[100] Dit uit zich in een toename aan beschouwingen, analyses en studies naar (para)militaire activiteiten in het digitale domein.[101] De aandacht voor hybride dreigingen helpt daarbij. De notie dat complexe veiligheidsproblemen niet zonder multidisciplinaire benadering zijn aan te pakken, krijgt gelukkig steeds meer steun.[102]

Hoe dit uitpakt voor het monopolie van het DCC, cyberwarfare, laat zich raden nu de Verenigde Staten en het Verenigd Koninkrijk hun eerste digitale wapenfeiten in de strijd tegen ISIS publiekelijk hebben gemaakt. Het feit dat ook de NAVO (eindelijk) de notie van cyberspace als een operationeel domein onderzoekt, spreekt overigens boekdelen. Cyberwarfare is realiteit geworden.[103] ■

98 In die zin moet ook het pleidooi voor een minister-zonder-portefeuille voor ICT worden verstaan, in: *Het Financieele Dagblad*, 'Kabinet heeft minister van ICT nodig' (10 januari 2016), via: <https://fd.nl/economie-politiek/1134298/kabinet-heeft-minister-van-ict-nodig>. Hoewel de petitie daarvoor heden (21-9-2016) slechts 316 ondertekeningen kent, zie: < http://ministervanict.nl/>.

99 Zie P. A.L. Ducheine, 'Mythen over digitale oorlogvoering en recht', *Militaire Spectator* 185 (2016) (3) 131.

100 Zie bijvoorbeeld de oprichting van de 77 (UK) Brigade, <https://britisharmedforces-review.wordpress.com/2015/01/31/the-security-assistance-group-now-the-77th-brigade/> en A. Schnitger, 'De luchtmacht in het security ecosysteem', *Militaire Spectator* 185 (2016) (7/8) 301.

101 Zie onder meer de publicaties van NATO's STRATCOM Centre of Excellence, <http://www.stratcomcoe.org/publications>.

102 Zie onder meer de afzonderlijke bijdragen van Frans Osinga, Rob de Wijk en Paul Ducheine in het themanummer van het Magazine Nationale Veiligheid <https://www.nctv.nl/onderwerpen_a_z/mnvc/index.aspx>.

103 Zie P. A.L. Ducheine, 'Cyber warfare is taking place', *Internationale Spectator* 70 (2016) (6) <https://www.internationalespectator.nl/pub/2016/6/>.