# De *cyber confidence*-illusie

## Hardnekkige hindernissen op weg naar *cyber confidence-building measures*

**Cyberaanvallen kunnen een bedreiging vormen voor internationale vrede en stabiliteit. Vertrouwenwekkende maatregelen, *confidence-building measures*, voor cyberspace kunnen ongewenste escalatie voorkomen. De internationale gemeenschap heeft ervaring met dit soort maatregelen voor bijvoorbeeld nucleaire wapens. Waarom slagen de belangrijkste spelers er vooralsnog niet in om normen voor het gedrag van staten in cyberspace te ontwikkelen en te implementeren? Dit artikel beschrijft hardnekkige hindernissen die dit belemmeren.**

*Luitenant-kolonel ing. K.L. Arnold EMSD MSc*[*]

In 2015 opende toenmalig minister van Buitenlandse Zaken, Bert Koenders, de Global Conference on CyberSpace in Den Haag. Tijdens zijn openingsspeech uitte hij zijn zorgen over de complexe veiligheidssituatie in de fysieke en de virtuele wereld. Omdat cyberaanvallen een bedreiging kunnen vormen voor internationale vrede en stabiliteit, bepleitte hij een systeem van *confidence-building measures*.[1] Een jaar later concludeerde Koenders teleurgesteld dat verscheidene cyber-uitdagingen niet waren verminderd. Sterker nog, ze waren toegenomen. De minister uitte zijn bezorgdheid over de vele cyberaanvallen die worden uitgevoerd door of namens verscheidene landen om politieke conflicten te beslechten. Hij benadrukte nogmaals de behoefte aan de regulering van normen en gedrag van staten in cyberspace.[2]

Een gemeenschappelijk besef dat schadelijke cyberactiviteiten wereldwijd een bedreiging vormen voor de internationale vrede en veiligheid heeft geresulteerd in de roep om politiekbindende, vertrouwenwekkende maatregelen voor cyberspace.[3] Toch lukt het de internationale gemeenschap niet om kaders voor normen en gedrag van staten in cyberspace vast te leggen en, belangrijker nog, daadwerkelijk te implementeren. Sinds de eerste ontwerpresolutie van Rusland uit 1998 staat het onderwerp op de agenda van de Verenigde Naties. Ongeveer twintig jaar later blijkt consensus binnen het daartoe samengestelde United Nations Group of Governmental Experts (UN GGE), nog altijd ver te zoeken.[4]

De wens is geuit om kaders voor normen en gedrag van staten in cyberspace vast te leggen, maar waarom lukt het dan niet om politiek aanvaardbare maatregelen te ontwikkelen en te implementeren? Dit artikel beschrijft enkele

---

[*] Lt-kol Kraesten Arnold is als (cyber)onderzoeker en docent verbonden aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie in Breda. Dit artikel is een geactualiseerde bewerking van de master thesis 'Cyber Confidence-Building Measures, Ten stumbling blocks which complicate the development and implementation of worldwide politically acceptable cyber confidence-building measures', 25 november 2016. Zie: https://www.csacademy.nl/images/scripties/2017/Arnold-Thesis-final-version-25-nov-2016.pdf.

1 Bert Koenders, *Opening speech*, Global Conference on Cyber Security, Den Haag, 16 april 2015. Zie: https://www.government.nl/documents/speeches/2015/04/16/opening-speech-gccs-bert-koenders.

2 Bert Koenders, *Speech at the Münchner Sicherheitskonferenz*, Den Haag, 12 februari 2016. Zie: https://www.government.nl/documents/speeches/2015/02/09/speech-by-minister-koenders-at-munchner-sicherheitskonferenz.

3 United Nations Office for Disarmament Affairs, *Factsheet: Developments in the field of information and telecommunications in the context of international security*, juli 2019. Zie: https://www.un.org/disarmament/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.

4 United Nations Office for Disarmament Affairs, *Developments in the field of information and telecommunications in the context of international security.* Zie: https://www.un.org/disarmament/ict-security/.


*Confidence-building measures voor cyberspace kunnen ongewenste escalatie voorkomen*

FOTO MCD, JOHN VAN HELVERT

initiatieven die zijn ontplooid op dit gebied. Vervolgens komen acht barrières aan de orde die de ontwikkeling en implementatie van die gewenste vertrouwenwekkende maatregelen voor het cyberdomein belemmeren.

## Cyber confidence-building measures

Er bestaat geen vaste definitie voor confidence-building measures (CBM),[5] maar over het algemeen zijn CBM gericht op het vergroten van onderling vertrouwen, voorspelbaarheid en stabiliteit, en omvatten daarom vaak afspraken over transparantie en samenwerking. Het zijn maatregelen die bij spanningen en conflicten de angst voor geweld of een (gewapende) aanval verminderen. Volgens de VN is, behalve politieke toezeggingen en de wil tot samenwerken, ook de mogelijkheid tot voortdurende verificatie essentieel. Een universeel CBM-model is niet realistisch.[6] Uiteindelijke cyber-CBM zouden kunnen leiden tot een mondiale visie op verantwoordelijk gedrag van staten in cyberspace.[7]

### Permanent Monitoring Panel en het eerste cyber-CBM-initiatief

Een van de eerste initiatieven op dit gebied kwam van de World Federation of Scientists. Sinds 2001 streeft haar information security Permanent Monitoring Panel (PMP) naar een mogelijkheid om cyberconflicten te beheersen. Het PMP beveelt een alomvattend juridisch kader aan, alsook richtlijnen voor verantwoordelijk gedrag van staten.[8] Dat vraagt een gezamenlijke inspanning van de gehele internationale gemeenschap, waarbij het PMP een leidende rol voorziet voor de VN bij het beschermen van cyberspace. De VN zou zich moeten inzetten voor een *comprehensive Law of Cyberspace*.[9]

Initieel streefde het PMP naar een universeel verdrag met juridisch bindende afspraken. Het panel realiseerde zich echter dat dit een lang en onhaalbaar traject zou worden. Het PMP besloot om zich te concentreren op CBM en normatieve gedragscodes; geen juridisch bindende afspraken, maar politiek-bindende.[10]

### UN Group of Governmental Experts

In lijn met het PMP-voorstel stelde de VN in 2009 een Group of Governmental Experts samen (UN GGE).[11] De groep kende deskundigen uit, onder meer, Brazilië, China, India, Rusland en de VS en streefde naar haalbare maatregelen om de mondiale cyberveiligheid te vergroten. In 2010 kwam de UN GGE met vijf aanbevelingen voor de ontwikkeling van CBM. De voorgestelde maatregelen gingen onder meer over eenduidige begrippen en definities, normen voor het gedrag van statelijke actoren, vertrouwenwekkende maatregelen en nationale standpunten over het 'gebruik van ICT' in conflictsituaties.[12] Door aanzienlijke meningsverschillen lukte het de GGE niet om in 2010 met een consensusrapport te komen.[13] Sinds 2010 publiceert de UN GGE geregeld haar aanbevelingen.[14]

In 2015 constateerden de experts een significante toename in cyberincidenten als gevolg van schadelijke software door statelijke én niet-statelijke actoren. Als katalysator voor een toenemende dreiging noemden zij de ontwikkeling van cybercapaciteiten voor militaire doeleinden, de vele kwaadwillende niet-statelijke

5 OSCE, *Guide on Non-Military Confidence-Building Measures (CBMs)*, Wenen, 2012, 9. Zie: https://www.osce.org/files/f/documents/6/0/91082.pdf.

6 UN document A/51/182, *Report of the Disarmament Commission, annex F*, paragraaf 2.3.

7 Katharina Ziolkowski, *Confidence Building Measures for Cyberspace*, in: Katharina Ziolkowski (red.), *Peacetime Regime for State Activities in Cyberspace*, (NATO CCD COE Publication, Tallinn, 2013) 533.

8 Henning Wegener, *Information Security Permanent Monitoring Panel World Federation of Scientists*, 457.

9 Henning Wegener et al., *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Report and Recommendations, World Summit on Information Society, Genève 2003 – Tunis 2005, Document WSIS-03/GENEVA/CONTR/6-E 19 November 2003, 14 - 18.

10 Wegener, *Information Security Permanent Monitoring Panel World Federation of Scientists*, 458-459.

11 Voluit: *The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.*

12 UN document A/65/201, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 30 juli 2010, 6-8.

13 Eneken Tikk-Ringas, 'Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012', *Ict4Peace Cyber Policy Process Brief*, (ICT4Peace Publishing, Genève, 2012) 7. Zie: https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf.

14 Sinds 2004 hebben UN GGE-bijeenkomsten plaatsgevonden en er zijn rapporten gepubliceerd in de jaren 2004/2005, 2009/2010, 2012/2013, 2014/2015, 2016/2017 en 2019/2020. Zie: https://dig.watch/processes/un-gge#view-7541-3.


*Politiemotorrijders begeleiden voertuigen met deelnemers aan de Global Conference on CyberSpace in Den Haag (2015)* FOTO RIJKSOVERHEID, PETER MONTENY

actoren en het attributieprobleem (de toewijzing van activiteiten aan een dader).[15] De UN GGE stelde voor om niet-bindende normen voor overheden op te stellen, die weergeven wat een land wel, of juist niet zou mogen doen in cyberspace. Die normen moeten ook beschrijven welke activiteiten van niet-statelijke actoren ongewenst zijn en niet mogen worden gedoogd. Landen moeten afzien van cyberaanvallen op de vitale infrastructuur van anderen en hun eigen vitale infrastructuur daartegen beschermen.[16] Opmerkelijk is dat zowel Rusland als China instemde met de, initieel door de VS voorgestelde, vrijwillige normen. Frappant, aangezien Rusland en China de vrijwillige normen zagen als opmaat naar (ongewenste) wettelijk bindende normen.[17]

De meest recente bijeenkomsten van de UN GGE, in 2016 en 2017, leidden niet tot consensus over het eindrapport. Sterker, de fundamentele verschillen in inzicht tussen de VS en gelijkgestemde partners, en Rusland en China met hun gelijkgezinde bondgenoten, resulteerden in een scheiding der wegen. In 2018 besloot de VN derhalve om niet alleen (weer) een nieuwe (westers georiënteerde) expertgroep samen te stellen (met 25 lidstaten), maar daarnaast ook een (bredere) Open-Ended Working Group (OEWG) te vormen, toegankelijk voor alle VN-lidstaten.

**OVSE**

De Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) wordt vaak beschouwd als ideaal platform om internationale samen-

15 UN document A/70/174, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 juli 2015, 6.

16 UN document A/70/174, 8.

17 Henry Rõigas en Tomáš Minárik, '2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law', in: *Incyder News*, augustus 2015. Zie: https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

De U.S. International Security Advisory Board adviseerde dat de VS zich beter kon richten op de confrontatie met Rusland

werking en stabiliteit te bespreken en te bevorderen.[18] In 2013 nam de OVSE een pakket van elf cyber-CBM aan. Het voorstel bestond voornamelijk uit vrijwillige, praktische en risicoverlagende maatregelen. De focus lag op samenwerken, informatie-uitwisseling en transparantie, en op het voorkomen van misverstanden en escalatie.[19] In ruil voor zijn steun aan het OVSE-voorstel dwong Rusland een bijlage bij het document af. Daarin bedongen de Russen dat het beginsel van soevereiniteit, territoriale integriteit en politieke onafhankelijkheid voor alle landen, ook van toepassing is in cyberspace.[20]

In maart 2016 nam de OVSE aanvullende maatregelen aan, onder meer gericht op de beveiliging van vitale infrastructuur en daaraan gerelateerde grensoverschrijdende ICT-netwerken. Ook adviseerde de OVSE om ook de particuliere sector, universiteiten, expertisecentra en de burgermaatschappij te betrekken bij de uitwerking van de maatregelen.[21] Ondanks de succesvolle start kwam het proces later in 2016 vrijwel tot stilstand. Tot op heden is daarin geen verandering gekomen. Door onenigheid en beschuldigingen van (staatsgesteunde) hackactiviteiten loopt de implementatie van eerder afgesproken maatregelen vertraging op.

**Shanghai Cooperation Organisation**

Reeds in 2001 diende de Russisch-Chinees geleide Shanghai Cooperation Organisation (SCO)[22] een voorstel in bij de VN voor een cybergedragscode. De gedragscode behelsde onder meer soevereiniteit, territoriale integriteit en politieke onafhankelijkheid voor alle landen, maar ook het voorstel om geen ICT te gebruiken voor vijandige activiteiten of bedreigingen van de internationale vrede en stabiliteit. De gedragscode beoogde daarnaast de oprichting van een multilateraal, internationaal internet-managementsysteem, en bepleitte de rol van de VN om internationale gedragsnormen op te stellen. Naleving van de code had een vrijwillig karakter.[23]

Veel westerse landen waren, om uiteenlopende redenen, tegen de voorgestelde gedragscode. De code zou de vrije informatiestroom bedreigen. Bovendien werd het voorstel gezien als opmaat naar een juridisch bindend verdrag om het gedrag van overheden te reguleren. Ironisch genoeg vreesden westerse landen de juridisch bindende gevolgen van de (Chinees-Russische) SCO-gedragscode, terwijl Rusland en China juist de juridisch bindende consequenties van het UN GGE 2015 rapport vreesden. Een andere reden voor de westerse weerstand tegen de gedragscode was de voorgestelde wijziging in het (tot dan toe Amerikaans-gedomineerde) internetbeheer. Door de meningsverschillen werd het voorstel niet in stemming gebracht.[24]

**Bilaterale initiatieven**

Naast voornoemde initiatieven van VN, OVSE en de SCO hebben ook de Association of Southeast Asian nations (ASEAN)[25] en de Organisation of American States (OAS)[26] vergelijkbare, maar

18 Vooral door de ervaringen die de OVSE opdeed met vertrouwenwekkende maatregelen tussen de partijen uit de Koude Oorlog.

19 OSCE, *Decision No 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1106 (Organization for Security and Co-operation in Europe, Permanent Council, 975th Plenary Meeting, 3 December 2013) 1.

20 OSCE, *Decision No 1106, Interpretative Statement Under paragraph IV.1(A)6 of the rules of procedure of the Organization for Security and Co-operation in Europe*, Attachment, 4.

21 OSCE, *Decision No 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1202 (Organization for Security and Co-operation in Europe, Permanent Council, 1092nd Plenary Meeting, 10 March 2016) 3-5.

22 De Shanghai Cooperation Organisation is een Euraziatische politieke, economische, en militaire organisatie, opgericht in 2001 in Shanghai door de leiders van China, Kazachstan, Kirgizië, de Russische Federatie, Tajikistan en Oezbekistan. Zie: 'What is SCO', http://infoshos.ru/en/?id=51.

23 UN document A/66/359, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, 14 september 2011, 4-5.

24 Anna-Maria Osula en Henry Rõigas (red.), *International Cyber Norms, Legal, Policy & Industry Perspectives* (NATO CCD COE, Tallinn, 2016), 17-18.

25 Het ASEAN Regional Forum (ARF) brengt niet alleen de tien ASEAN-lidstaten bij elkaar, maar ook zeven andere landen uit de regio, alsook tien gesprekspartners, waaronder de VS, Rusland, China en de EU.

26 De organisatie van Amerikaanse staten kent 35 onafhankelijke lidstaten. Zie: http://www.oas.org/en/about/who_we_are.asp.

eveneens schijnbaar vruchteloze, pogingen gedaan om tot vertrouwenwekkende cybermaatregelen of normen te komen. Amerika, Rusland en China hebben ook bilaterale afspraken gemaakt.

In 2013 kondigden de VS en Rusland een bilaterale cyber-samenwerkingsovereenkomst aan om onnodige escalatie van cyberincidenten te voorkomen. Speciale aandacht ging uit naar cyberdreigingen vanaf elkaars grondgebied.[27] De overeenkomst leek veelbelovend en er werd concrete vooruitgang geboekt, maar de Oekraïne-crisis (2014) en de Russische annexatie van de Krim verstoorden deze ontwikkeling. Sterker nog, de US International Security Advisory Board adviseerde dat de VS zich beter kon richten op de confrontatie met Rusland, dan te zoeken naar manieren om de betrekkingen te verbeteren.[28]

In 2015 vonden Rusland en China elkaar in een bilaterale cyberovereenkomst over 'non-agressie in cyberspace' en 'cyber-soevereiniteit'. Het akkoord bouwt voort op de eerdergenoemde gedragscode van de SCO. De non-agressie-toezegging was vooral bedoeld om wederzijdse cyberspionage te beperken. Het gedeelte over soevereiniteit dient een breder politiek en strategisch doel. Beide landen beklemtonen de soevereine status van internet, waarin overheidsgezag geldt voor binnenlandse aangelegenheden; zonder enige inmenging van buitenaf. Rusland en China hebben daarom een gemeenschappelijk belang bij 'cyber-soevereiniteit', een standpunt dat haaks staat op het Amerikaanse pleidooi voor wereldwijde 'cyber-vrijheid'.[29]

Ook de VS en China besloten in 2015 hun onderlinge cyber-samenwerking te intensiveren. Belangrijkste drijfveer voor een overeenkomst was de Amerikaanse wens om China's economische cyberspionage een halt toe te roepen.[30] Hoewel het akkoord niet is gepubliceerd, zijn enkele afspraken toch bekend geworden. Zo kwamen de landen overeen zich te onthouden van cyber-diefstal van intellectueel eigendom, bedrijfsgeheimen of andere vertrouwelijke zakelijke informatie. Ook kwamen beide landen overeen zich in te spannen voor normen op het gebied van overheidsgedrag in cyberspace.[31] Wat de VS heeft toegezegd aan China in ruil voor deze overeenkomst, is verder niet bekend.

Een jaar later is de voorlopige conclusie van het Amerikaanse cybersecuritybedrijf FireEye dat de Chinese economische cyberspionage inderdaad is gedaald.[32] Ondanks de vermeende afname van het aantal hack-activiteiten, is het prematuur om te concluderen dat China zijn overheidsgestuurde (economische) cyberspionage daadwerkelijk heeft verminderd, laat staan permanent beëindigd. Misschien houdt China zich vooralsnog gedeisd, uit schaamte voor de openbaring van de staatsgesteunde cyberspionage, die in 2014 resulteerde in een Amerikaanse aanklacht tegen vijf Chinese militaire hackers.[33] Of China grijpt deze 'gevechtspauze' aan om technologisch meer geraffineerde capaciteiten te ontwikkelen, waarmee het voortaan wél onopgemerkt kan blijven.

De afgelopen vijf jaar zijn dergelijke bilaterale akkoorden niet meer gesloten.[34] Afspraken lijken gewenst, maar de magere resultaten laten tegelijk zien dat er een kloof bestaat tussen idealisme en pragmatisme.

27 White House Office of the Press Secretary. *Factsheet US-Russian agreement on cooperation on information and communications technology security*, 17 juni 2013. Zie: https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

28 U.S. Department of State International Security Advisory Board, *Final Report of the International Security Advisory Board (ISAB) on U.S.-Russia Relations*, 9 december 2014, 3. Zie: http://www.state.gov/documents/organization/235118.pdf

29 Yuxi Wei, *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty* (Jackson School of International Studies, University of Washington, 21 juni 2016). Zie: https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/.

30 Scott Warren Harold, *The US-China Cyber Agreement, a good first step*, (RAND corporation, 1 augustus 2016). Zie: https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html.

31 White House Office of the Press Secretary. *Fact sheet 'President Xi Jinping's State Visit to the United States*, 25 september 2015. Zie: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-States.

32 Reuters World News, 'Chinese economic cyber-espionage plummets in U.S.: experts', 21 juni 2016. Zie: http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D.

33 U.S. Department of Justice, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage', 19 mei 2014. Zie: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

34 Mochten er wel (geheime) bilaterale akkoorden op dit gebied zijn gesloten, dan zijn de resultaten daarvan op moment van schrijven niet publiekelijk bekend.

*Een Amerikaanse militair bereidt zich voor op een cyber-readiness-oefening*

## Acht obstakels op weg naar cyber-CBM

Uit het voorgaande blijkt dat cyber-CBM ontwikkelen moeizaam gaat. Implementatie van voorgestelde maatregelen blijkt evenwel nog lastiger. Hieronder beschrijf ik acht aspecten die mondiale cyber confidence-building measures belemmeren.

**1. Geen eenduidige terminologie**

De verschillende cyber-CBM-initiatieven tonen dat afspraken over een gemeenschappelijke cyberterminologie onbereikbaar lijken. Binnen internationale organisaties, zoals de VN, NAVO, OVSE en de EU, alsook binnen individuele landen, worden andere woorden gebruikt om hetzelfde te zeggen, of juist dezelfde woorden gebruikt om iets anders uit te drukken (cyber security, information security, ICT-security, cyberspace, information space, information warfare, cyber warfare, cyber attack, cyber incident).

Daarnaast hechten landen vaak andere waarden aan dezelfde begrippen (zoals soevereiniteit, privacy, interne aangelegenheden, vrijheid van meningsuiting). Het gebrek aan eenduidige definities en verschillende interpretaties creëert een voedingsbodem voor misverstanden. Sterker, ze staan een goede discussie over cyber-CBM in de weg.

**2. Te veel belanghebbenden**

Internationale betrekkingen drijven van oudsher op interactie tussen soevereine staten. Bij gesprekken over eerdere CBM (voor nucleaire, biologische en chemische wapens, of beperking van conventionele en strategische wapens) waren slechts die partijen betrokken die derge-

FOTO U.S. DEPARTMENT OF DEFENSE, FRANKLIN R. RAMOS

lijke wapens hadden. Echter, door de huidige interconnectiviteit en internationale verwevenheid van netwerken en systemen kunnen cyberaanvallen overal ter wereld vandaan komen en overal ter wereld effecten creëren. Het aantal potentiële gesprekspartners neemt daardoor significant toe. Intergouvernementele organisaties zoals de VN, WTO, IMF en EU, alsook niet-gouvernementele en multinationale organisaties worden steeds invloedrijker en spelen een steeds grotere rol bij onderhandelingen. Bovendien is het aantal partijen dat is betrokken bij ontwerp, bouw, beheer en gebruik van cyberspace enorm.[35] Alle partijen hebben eigen meningen, waardes en belangen; vaak uiteenlopend, soms verstrengeld, soms tegengesteld.

Een voorbeeld van toegenomen invloed kwam in 2014 van Microsoft. Het bedrijf kwam met een voorstel voor zes cyberveiligheidsnormen voor het gedrag van overheden in cyberspace, '[…] *to better define what type of government behaviors in cyberspace should be "out of bounds"* […]',[36] om de kans op oorlog voeren te beperken. De wereld op zijn kop: een commercieel bedrijf dat landen 'voorschrijft' hoe hun overheden zich (onderling) in cyberspace moeten gedragen.

Er zijn te veel gesprekspartners met elk hun eigen standpunten. Dit leidt tot een paradox. Voor een optimaal resultaat van het cyber-CBM-proces is een brede discussie nodig tussen (veel te) veel belanghebbenden. Tegelijkertijd blokkeert die overmaat aan gesprekspartners ditzelfde proces.

### 3. Diepgeworteld wantrouwen

In 1998 stelde Rusland een VN-wapenbeheersingsverdrag voor dat het gebruik van cyberspace voor militaire doeleinden zou uitsluiten.[37] Rusland was de enige voorstander van deze (ontwerp)resolutie. In 2005 keerde het tij, nogal ironisch, doordat de VS voor het eerst actief *tegen* het voorstel stemde. Beide grootmachten mobiliseerden medestanders voor hun standpunt en in 2009 stond de teller op 30 vóór het Russische voorstel, inclusief China. Een jaar later herzag de VS plotseling zijn mening en sloot zich aan bij het Russische voorstel, waarschijnlijk in een poging hierop inhoudelijk invloed te kunnen uitoefenen.[38]

In 2001 diende de Chinees-Russisch geleide Shanghai Cooperation Organisation een voorstel in voor een gedragscode. Ook dit voorstel stuitte op weerstand. Westerse democratieën wilden dat

35 Denk onder andere aan internet-serviceproviders, internet-beheerorganisaties, grote technologiebedrijven zoals Apple, Alphabet (het moederbedrijf van Google), Microsoft, Facebook en Amazon, commerciële bedrijven, inlichtingsdiensten, criminele organisaties, activistische hackers, individuele gebruikers, en een scala aan belanghebbenden die zich bezighouden met internationaal recht, soevereiniteit, privacy, vrije informatiestromen, universele mensenrechten, sociale, economische, historische en culturele aspecten.

36 Angela McKay (et al), *International Cybersecurity Norms, Reducing conflict in an Internet-dependent world*, (Microsoft, December 2014) 11. Zie: https://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf.

37 Ziolkowski, *Confidence Building Measures for Cyberspace*, 533.

38 Ibidem, 571.

overheden ook verantwoordelijk zouden zijn voor cyberaanvallen van niet-statelijke actoren die opereren vanaf hun grondgebied. Het voorstel ging echter niet in op verantwoordelijkheid voor niet-statelijke proxy-actoren (partijen die acties uitvoeren namens anderen).[39]

Een westers voorstel, de Convention on cybercrime van de EU,[40] werd juist weer tegengewerkt door invloedrijke landen zoals China, Rusland, India en Brazilië. Deels omdat deze landen niet waren betrokken bij de ontwerpresolutie, deels omdat zij meenden dat de rechten van individuen en landen niet goed werden gewaarborgd.[41] Bovendien waren Rusland en enkele gelijkgestemde landen tegen het voorstel, omdat goedkeuring hun soevereiniteit zou schaden.[42]

De onderlinge geopolitieke en economische strijd van de VS, China en Rusland lijkt een zero-sum game en werkt effectieve onderhandelingen tegen. Een compromis over vertrouwenwekkende maatregelen blijft uit, zolang de grootmachten niet enigszins hetzelfde denken over soevereiniteit, territoriale integriteit, internetbeheer, privacy, anonieme operaties, cyberspionage, cyberaanvallen, inzet van proxies, geheime operaties en het (gedogen van) schadelijke activiteiten.

### 4. Cyberspace is ondoorzichtig

Een relevant aspect van CBM betreft transparantie.[43] Cyberspace is echter verre van transparant. De manier waarop cyberspace is geconstrueerd, staat een hoge mate van anonimiteit

39 Tim Maurer, 'Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security', *Discussion Paper 2011-11* (Cambridge, Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School, september 2011) 6.

40 Council of Europe, *Convention on Cybercrime*, Budapest, 23 november 2001.

41 Sinha Shalini, 'Budapest Convention on Cybercrime – An Overview' (Center for Communication and Governance New Delhi, Legally India, Article 03, maart 2016). Zie: https://www.legallyindia.com/blogs/budapest-convention-on-cybercrime-an-overview.

42 Keir Giles, 'Russia's Public Stance on Cyberspace Issues', in: Cristian Czosseck, Rain Ottis, Katharina Ziolkowski (red.) *4th International Conference on Cyber Conflict 2012* (NATO CCD COE Publications, Tallinn, 2012) 65.

43 Ziolkowski, *Confidence Building Measures for Cyberspace*, 12.

*Cyberaanvallen kunnen overal ter wereld vandaan komen en overal ter wereld effecten creëren*

FOTO UK MINISTRY OF DEFENCE

toe. Het is mogelijk om weinig tot geen traceerbare sporen en privéinformatie achter te laten, waardoor cyberaanvallers hun werkelijke identiteit en intenties kunnen verhullen en overheden de verantwoordelijkheid voor cyberacties vrij gemakkelijk kunnen ontkennen. De toewijzing van activiteiten aan een dader is daardoor veelal een tijdrovende en forensische uitdaging ('het attributieprobleem'). De mogelijkheid om operaties quasi-anoniem uit te voeren, draagt bij aan misverstanden en valse beschuldigingen.

Een aanvaller in het cyberdomein heeft als voordeel dat een aanval voor het doelwit veelal onvoorspelbaar en onzichtbaar is. Om het risico op ontdekking te verkleinen, kan een agressor de aanval bovendien laten uitvoeren door een proxy-actor. Deze kan hiertoe de digitale identiteit van onschuldige derden vervalsen en misbruiken. Pas zodra de aard en omvang van de effecten zich openbaren, kan het slachtoffer een inschatting maken waar de aanval vandaan komt. Aangezien attributie vaak een probleem vormt, blijft het een uitdaging om de verantwoordelijke achter een aanval aan te wijzen.

Een voorbeeld van een attributieprobleem is discussie rond de verantwoordelijkheid voor de in 2014 uitgevoerde cyberaanval op Sony Pictures. De Amerikaanse FBI wees Noord-Korea aan als vermeende dader; het land ontkende. Verscheidene journalisten en cyberveiligheidsexperts twijfelden openlijk aan de beschuldiging.[44] Hackers kunnen cyberidentiteiten nabootsen en daarmee de verdenking van schadelijke activiteiten neerleggen bij anderen. Inmiddels is een scala aan partijen aangemerkt als dader, waaronder Noord-Korea, Rusland, China, de Verenigde Staten, de FBI, Sony-werknemers, hacktivisten en de (cyber)criminele Lazarus Group.

Transparantie speelt ook een belangrijke rol bij het beschermen van cyberspace, vooral bij het beschermen van vitale infrastructuur die nationale grenzen overstijgt.[45] Het VN GGE-rapport 2015 deed een voorstel voor normen in die richting.[46] De voorgestelde normen impliceerden dat verantwoordelijk overheidsgedrag onder meer inhoudt dat landen – vanaf hun grondgebied – geen acties stimuleren of gedogen die dit soort kritieke infrastructuur bedreigt. Van landen werd verwacht dat zij de integriteit van de gehele IT-keten garanderen. Landen moeten afstand nemen van het manipuleren van hardware, software of protocollen, en afzien van verspreiding van schadelijke cybermiddelen en technieken. Zolang die normen er niet zijn, kunnen overheden fabrikanten dwingen (bewust) kwetsbaarheden of 'achterdeurtjes' in te bouwen in hun soft- en hardwareproducten.[47]

Dat vrijwel de gehele IT-keten (hardware, software, protocollen en dergelijke) kan worden gemanipuleerd, bleek wel uit Edward Snowdens gelekte documenten over de Amerikaanse National Security Agency (NSA). De NSA bleek meerdere kwetsbaarheden uit te buiten in producten van Microsoft, Cisco en Huawei. De dienst onderschepte bepaalde – door hun doelwitten bestelde – elektronica, en voorzag die van kwaadaardige software.[48] Die geheime 'elektronische achterdeurtjes' waren voornamelijk gericht op (het misbruiken van kwetsbaarheden in) firewalls en routers.[49] Eenmaal ingebouwd zijn dergelijke elektronische achterdeurtjes lastig te ontdekken. En eenmaal ontdekt, is het lastig de daadwerkelijke daders met zekerheid aan te wijzen.

Anonimiteit en het attributieprobleem zorgen ervoor dat identiteiten en intenties kunnen worden verhuld, waardoor overheden de verantwoordelijkheid voor schadelijke cyber-

44 Post Staff Report, 'New evidence Sony hack was 'inside' job, not North Korea', *New York Post*, 30 december 2014. Zie: http://nypost.com/2014/12/30/new-evidence-sony-hack-was-inside-job-cyber-experts/; Kim Zetter, 'The evidence that North Korea hacked Sony is flimsy', *Wired Magazine*, 17 december 2014. Zie: https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/.

45 Zoals elektriciteitsnetwerken, olie- en gaspijpleidingen, internetverbindingen.

46 UN document A/70/174.

47 Christian Czosseck, 'State Actors and their Proxies in Cyberspace', in: Katharina Ziolkowski (red.), *Peacetime Regime for State Activities in Cyberspace*, (NATO CCD COE Publication, Tallinn, 2013) 14.

48 Spiegel Staff, 'Documents Reveal Top NSA Hacking Unit', *Spiegel Online International*, 29 december 2013. Zie: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

49 Bruce Schneier, 'Major NSA/Equation Group Leak', *Schneier on Security,* 16 augustus 2016. Zie: https://www.schneier.com/blog/archives/2016/08/major_nsaequati.html.

acties vrij gemakkelijk kunnen ontkennen. Cyberspace is ondoorzichtig, terwijl transparantie juist essentieel is voor vertrouwenwekkende afspraken.

**5. Gebruik van proxies**

Landen mogen niet doelbewust toestaan dat hun grondgebied wordt gebruikt voor activiteiten die andere soevereine staten schaden.[50] In de *Tallinn Manual*,[51] een handleiding voor een juridische interpretatie van het internationale recht op het cyberdomein, wordt dit principe doorgetrokken naar cyberspace.[52] Zodra een land weet van een onrechtmatige daad die resulteert in ernstige schade voor een andere staat, moet het hiertegen optreden. Dit 'due diligence'-principe betekent overigens niet dat een land per definitie alles moet ondernemen om een aanval te vermijden.[53]

Desondanks maakt een overheid soms juist dankbaar gebruik van 'proxy-actoren', die namens hen schadelijke cyberaanvallen uitvoeren op andere landen. Dat kan zijn omdat overheden niet de juiste cybercapaciteiten hebben, maar een andere reden kan zijn dat bepaalde activiteiten niet stroken met de wettelijke, ethische of culturele waarden van het land. Het belangrijkste argument is echter de mogelijkheid dat een overheid (directe) betrokkenheid bij cyberaanvallen kan ontkennen door zich te verschuilen achter niet-statelijke actoren zoals patriottische hackers, criminelen of activisten. De benodigde capaciteiten zijn ook in te huren. Opvallend is dat deze 'cyber-crime-as-a-service' niet uit bekende schurkenstaten komt, maar vooral uit de VS (ongeveer 50 procent), het VK, Portugal, IJsland, Rusland en Nederland.[54]

De cyberaanval op het Amerikaanse Democratic National Committee (DNC) in 2016 werd in eerste instantie toegerekend aan Russische, staatsgesteunde proxies. Het technische bewijs (zoals gebruikte middelen, IP-adressen, taal en locatie-instellingen) wees op duidelijke betrokkenheid van de Russische overheid. Toch speelt ook hierbij het attributieprobleem. Je kunt 'technisch bewijs' vervalsen, Russische middelen en technieken hergebruiken, en taal- en locatie-instellingen eenvoudig instellen. Andere inlichtingenbronnen zijn dan ook onontbeerlijk om de daadwerkelijke daders te achterhalen. De verdenking van Russische inmenging werd overigens herhaald in het Mueller-rapport uit 2019, op basis waarvan twaalf medewerkers van de Russische militaire inlichtingendienst GRU zijn aangeklaagd voor hun betrokkenheid.[55]

In het conflict tussen Rusland en de Oekraïne waren meerdere proxy-actoren actief die offensieve acties uitvoerden voor, of namens de strijdende partijen. Russische hackers vielen Oekraïne aan met Denial-of-Service (DOS)-aanvallen en website defacements (waarbij de inhoud van een gehackte site wordt gewijzigd). Oekraïense hackers sloegen terug met soortgelijke cyberaanvallen op Russische doelen. Ook de NAVO gebruikte tijdens dit conflict een proxy, het Roemeense staatsbedrijf Rasirom, om de Oekraïense cyberverdediging te verbeteren.

Een overheid kan verklaren zich te houden aan afgesproken normen voor verantwoord gedrag in cyberspace. Echter, zolang overheden proxies blijven gedogen, stimuleren of steunen, en geen verantwoordelijkheid nemen voor hun acties, zijn dergelijke (in beginsel) vertrouwenwekkende toezeggingen van generlei waarde.

**6. Cyberwapens**

Cybermiddelen kun je gebruiken voor 'informatie-operaties' (beïnvloeding, psychologische

50 Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', in: Katharina Ziolkowski (red.), *Peacetime Regime for State Activities in Cyberspace*, (NATO CCD COE Publication, Tallinn, 2013) 204.

51 Michael N. Schmitt (red.), *Tallinn Manual 2.0 on the international law applicable to cyber warfare* (Cambridge, Cambridge University Press, 2017).

52 De Tallinn Manual is een academisch boekwerk met daarin verzamelde meningen en interpretaties van wetenschappers en academici en heeft tot doel bij te dragen aan de discussie omtrent de toepasbaarheid van het internationale recht op het cyberdomein. De handleiding is geen beschrijving van wetgeving of een normstellend document.

53 Robin Geiß en Henning Lahmann, 'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention', in: Katharina Ziolkowski (red.), *Peacetime Regime for State Activities in Cyberspace*, (NATO CCD COE Publication, Tallinn, 2013) 655.

54 Rick. M. Robinson, 'Cybercrime-as-a-Service Poses a Growing Challenge', *Security Intelligence*, 4 september 2016. Zie: https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/.

55 Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* (Volume II of II, maart 2019, Washington, D.C.). Zie: https://www.justice.gov/storage/report_volume2.pdf.


*Amerikaanse militairen oefenen cyberoperaties met hun Zuid-Koreaanse bondgenoten* U.S. DEPARTMENT OF DEFENSE, DEVON DOW

oorlogsvoering of strategische communicatie), maar ook voor traditioneel kinetische doeleinden. De middelen zijn vrij eenvoudig te verkrijgen: een computer, software en een internetverbinding volstaan. En hoewel de kennis en vaardigheden om die middelen effectief te benutten een uitdaging kunnen vormen, zijn ook die relatief eenvoudig toegankelijk (via online handleidingen of als aangeboden (betaalde) service). Dezelfde capaciteiten kunnen zowel defensief als offensief worden benut. In vergelijking met traditionele wapensystemen zijn cyberwapens relatief goedkoop te maken, gemakkelijk te verbergen, eenvoudig te transporteren en daardoor lastig te ontdekken. Toezeggingen om geen 'cyberwapens' te ontwikkelen, zijn dan ook gemakkelijk te omzeilen en niet verifieerbaar.

Met de toename van technologisch hoogwaardige middelen voor moderne krijgsmachten, nemen de mogelijkheden om hiertegen cybermiddelen in te zetten navenant toe. Cyberwapens zijn daardoor aantrekkelijk voor asymmetrische oorlogvoering, wat een risico op proliferatie impliceert. Toch staat de ontwikkeling van cyberwapens wereldwijd nog in de kinderschoenen. Dit geldt zeker voor cyberwapens die (direct of indirect) resulteren in de dood of lichamelijk letsel van mensen, of die leiden tot ernstige fysieke schade. Sinds de ontdekking van 'Stuxnet', de vermeende Amerikaans-Israëlische cyberaanval op een Iraanse uranium-verrijkingsinstallatie in 2010,[56] zijn er weinig cyberaanvallen bekend die een militair doel nastreefden.[57] Desondanks heeft Stuxnet het potentieel dodelijk en vernietigend effect van (toekomstige) cyberwapens gedemonstreerd.

Militaire systemen en netwerken vormen mogelijke doelwitten voor cyberoorlogvoering, maar een tegenstander kan in beginsel ieder digitaal object aanvallen. Objecten met een civiel-militaire functie (soms aangeduid als

56 John C. Richardson, 'Stuxnet as Cyberwarfare Applying the Law of War to the Virtual Battlefield', in: *The John Marshall Journal of Information Technology & Privacy Law* 29 (2011) (1).

57 Voorbeelden van militair gebruik van cyberwapens zijn te vinden in Estland (2007), Georgië (2008) en Oekraïne (2013-2015). Verder zijn er militaire cyberincidenten geweest in de Libische burgeroorlog (2011), de Syrische burgeroorlog (2013), en de strijd tussen Israël en Hamas (2014). Emilio Iasiello, 'Are Cyber Weapons Effective Military Tools?', in: *Military and Strategic Affairs* 7 (2015) (1). Zie: http://www.inss.org.il/uploadImages/systemFiles/2_Iasiello.pdf.

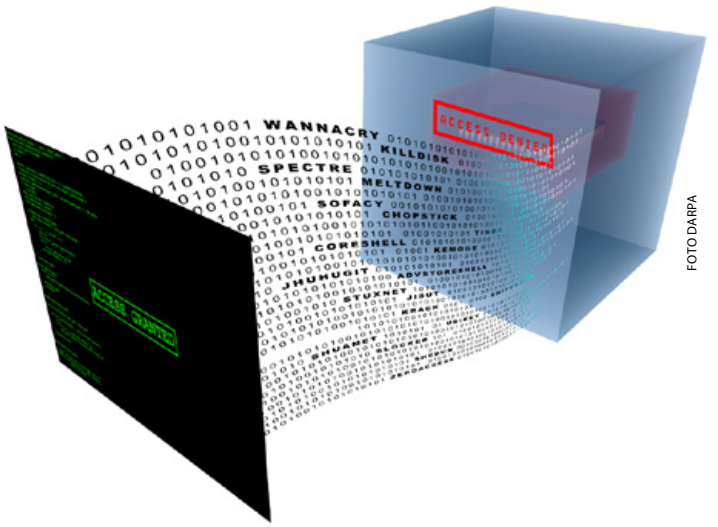


FOTO DARPA

*Het feit dat landen elkaar bespioneren, is natuurlijk niet nieuw, maar cyberspionage en de omvang ervan zijn dat wel*

dual-use) of zelfs volledig civiele vitale infrastructuur (waterwerken, drinkwatervoorziening) kunnen daardoor óók doelwit worden van kwaadwillende cyberaanvallers. Hoewel deze niet-militaire objecten volgens het humanitair oorlogsrecht geen doelwit zouden *mogen* zijn, *kunnen* deze objecten in de praktijk wel degelijk schade ondervinden; opzettelijk toegebracht of als onbedoelde nevenschade. Landen die hun tegenstanders niet kunnen treffen met traditionele wapens (letterlijk danwel figuurlijk) kunnen dit wel dankzij de nagenoeg onbeperkte reikwijdte en veelzijdige mogelijkheden van cyberwapens. Een pleidooi om tijdens een gewapend conflict of oorlog af te zien van relatief goedkope, maar doeltreffende cyberwapens is voor dergelijke landen niet aantrekkelijk.

Belangrijker dan cyberwapens zelf, zijn de kennis en vaardigheden om die cyberwapens te creëren. Mocht een land als vertrouwenwekkende maatregel verklaren geen cyberwapens te maken, dan kan het wel investeren in personele en technische capaciteiten om deze wapens later alsnog te ontwikkelen. En zegt een land toe zelf niet te investeren in offensieve cybercapaciteiten, dan kan een proxy dat gat wellicht opvullen.

Bij traditionele CBM zijn afspraken te maken over ontwerp, ontwikkeling, productie of testen van wapens. Die toezeggingen zijn te inspecteren en te verifiëren. Door de bijzondere kenmerken van cyberwapens zijn dezelfde afspraken voor cyberwapens nauwelijks te maken.

### 7. Cyberspionage

Industriële, commerciële, politieke, diplomatieke en veiligheidsgerelateerde data kun je vergaren uit open bronnen, maar ook verkrijgen via spionage. Het feit dat landen elkaar bespioneren, is natuurlijk niet nieuw. Maar cyberspionage en de omvang ervan zijn dat wel.

In 2009 wist China terabytes aan vertrouwelijke gegevens over de Amerikaanse Joint Strike Fighter (F-35) buit te maken.[58] En in 2013 kwamen Canadese onderzoekers naar buiten met real-time bewijs dat een voornamelijk in China gevestigd computerspionagenetwerk in 103 landen computers van overheden en private ondernemingen had gehackt.[59] Ook het Amerikaanse cybersecuritybedrijf Mandiant wees in 2013 met een beschuldigende vinger naar China vanwege massale externe spionageactiviteiten. In zijn rapport onthulde het bedrijf het bestaan van 'Unit 61398', een afdeling van het Chinese leger, gespecialiseerd in (commerciële) cyberspionage.[60]

Cybersecuritybedrijf FireEye claimde in 2014 voldoende bewijs te hebben om een langdurige spionage-inspanning in (Oost-)Europa – uitgevoerd door de Russische hackergroup 'APT-28' – te kunnen bestempelen als een 'door de Russische staat gesteunde actie'. Vermoedelijk begonnen de spionage-inspanningen al in 2007.[61]

58 Wendell Minnick, 'Chinese businessman pleads guilty of spying on F-35 and F-22', *Defense News*, 24 maart 2016. Zie: http://www.defensenews.com/story/breaking-news/2016/03/24/chinese-businessman-pleads-guilty-spying-f-35-and-f-22/82199528/.

59 'Cyber Spy Networks Hacks Computers in 103 Countries', *Fox News*, 30 maart 2009.

60 Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, 3. Zie: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

61 FireEye, Special Report, *APT28: A Window into Russia's Cyber Espionage Operations?*, 28. Zie: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

Nu worden China en Rusland wel vaker beschuldigd van cyberspionage, voornamelijk door de VS. Toch blijken zij niet de enige grootmachten die zich hieraan bezondigen. In 2013 onthulde de eerder genoemde Edward Snowden het bestaan van het 'PRISM-programma' van de Amerikaanse NSA,[62] een surveillanceprogramma waarmee de Amerikaanse overheid heimelijk gebruikersinformatie kon vergaren van bedrijven als Microsoft, Google, Apple en Yahoo.[63] Daarnaast gebruikte de NSA het programma om wereldwijd ambassades en niet-statelijke actoren te bespioneren.[64]

Ook Nederland houdt zich bezig met digitale spionage. Bijvoorbeeld door, op zoek naar bewijs voor cyberactiviteiten voor of namens de Russische overheid, computersystemen binnen te dringen van Russische hackergroepen zoals 'Cozy Bear'.[65]

Door computers, netwerken en bepaalde software te gebruiken, kun je tegenwoordig snel en relatief eenvoudig spioneren; op afstand en met beperkt risico.[66] Cyberspionage maakt computersystemen en netwerken van doelwitten (en derden) inherent onveilig en doet daarmee afbreuk aan het, voor cyber-CBM, noodzakelijke onderlinge vertrouwen en gewenste stabiliteit.

**8. Noodzaak snelle overeenkomst ontbreekt**

Hoewel meerdere cyber-CBM-initiatieven zijn gestart, lijken landen de huidige internationale situatie omtrent cyberveiligheid, een soort patstelling, acceptabel te vinden. De juiste omstandigheden kunnen een impuls geven aan veranderingen in veiligheidsdenken, waardoor landen willen meewerken aan veranderingen, maar vooralsnog lijken die gunstige omstandigheden afwezig. Pas als meerdere landen gezamenlijk een hoge mate van ontevredenheid over de huidige internationale cyber-veiligheidssituatie delen, kunnen vertrouwenwekkende maatregelen bijdragen aan het verbeteren van de onderlinge veiligheidsrelaties.[67]

Veel landen zien de potentiële risico's van cyberaanvallen tegen hun onderling verweven economieën en erkennen de noodzaak tot samenwerking om deze risico's te bestrijden.

Toezeggingen om geen cyberwapens te ontwikkelen zijn makkelijk te omzeilen en niet verifieerbaar

Dat verklaart de initiële medewerking van veel landen aan mondiale, regionale en lokale cyber-CBM-initiatieven. Grootschalige cyberaanvallen met desastreuze effecten zijn vooralsnog uitgebleven. Cyberaanvallen hebben nog niet geresulteerd in grote aantallen slachtoffers of aanzienlijke fysieke schade. Ondanks alarmerende waarschuwingen is de wereld nog niet getroffen door een cyber-Armageddon,[68] Pearl Harbor,[69] doomsday,[70] of 9/11.[71]

Zodra zich een apocalyptisch cyberscenario ontvouwt, zullen overheden en andere, niet-publieke partijen waarschijnlijk bereid zijn om snel vertrouwenwekkende cybermaatregelen op te stellen, af te spreken en na te leven. Tot die tijd zal die noodzaak niet breed worden gevoeld.

62 PRISM staat voor Planning tool for Resource Integration, Synchronization and Management.

63 T.C. Sottek and Joshua Kopstein, 'Everything you need to know about PRISM, a cheat sheet for the NSA's unprecedented surveillance programs', *The Verge*, 17 juli 2013. Zie: https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

64 Bruce Schneier, 'Espionage vs. Surveillance', *Schneier on Security*, 14 mei 2014. Zie: https://www.schneier.com/blog/archives/2014/05/espionage_vs_su.html.

65 Huib Modderkolk, *Het is oorlog maar niemand die het ziet* (Amsterdam, Uitgeverij Podium, 2019) 276.

66 Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage', in: Anna-Maria Osula en Henry Rõigas (red.), *International Cyber Norms, Legal, Policy & Industry Perspectives* (NATO CCD COE, Tallinn, 2016) 66.

67 James Macintosh, 'Confidence Building in the Arms Control Process: A Transformation View', Ottawa, Canada: Department of Foreign Affairs and International Trade, Arms Control and Disarmament Studies Number 2, 1996. JX 1974.M32 1996.

68 James Clapper, 'US Spy Chief Warns of Space Wars, North Korean Nukes, and Cyber Threats', *Vice News*, 9 februari 2016. Zie: https://www.vice.com/en/article/xw3m8q/us-spy-chief-warns-of-space-wars-north-korean-nukes-and-cyber-armageddon.

69 John Hamre, 'The 'electronic Pearl Harbor', *Politico Magazine*, 9 september 2015. Zie: https://www.politico.com/agenda/story/2015/12/pearl-harbor-cyber-security-war-000335/.

70 'Obama's doomsday cyberattack unrealistic – experts say', *NBC News*, 21 juli 2012. Zie: http://www.nbcnews.com/id/48265682/ns/technology_and_science-security/t/obamas-doomsday-cyberattack-scenario-unrealistic-experts-say/#.VyoRmvmLSM8.

71 Bert Koenders, *Speech at the Münchner Sicherheitskonferenz.*

Tenzij zich binnenkort één of meer cyberrampen voordoen, zal het ontwikkelen van mondiaal geaccepteerde, politiek-bindende cyber-CBM een langdurig, zoniet onmogelijk proces blijken.

**Tot slot**

Nederland onderschrijft het belang van cyber-CBM. De eerdergenoemde Global Conference on CyberSpace in 2015 leidde tot de lancering van het The Hague Program for Cyber Norms, een meerjarig onderzoeksprogramma naar het ontwikkelen en implementeren van internationale normen voor omgangsvormen in cyberspace.[72] Een ander Nederlands initiatief betrof de oprichting van de Global Commission on the Stability of Cyberspace (GCSC),[73] een internationale multi-stakeholder-organisatie, gericht op het bevorderen van stabiliteit in cyberspace.[74]

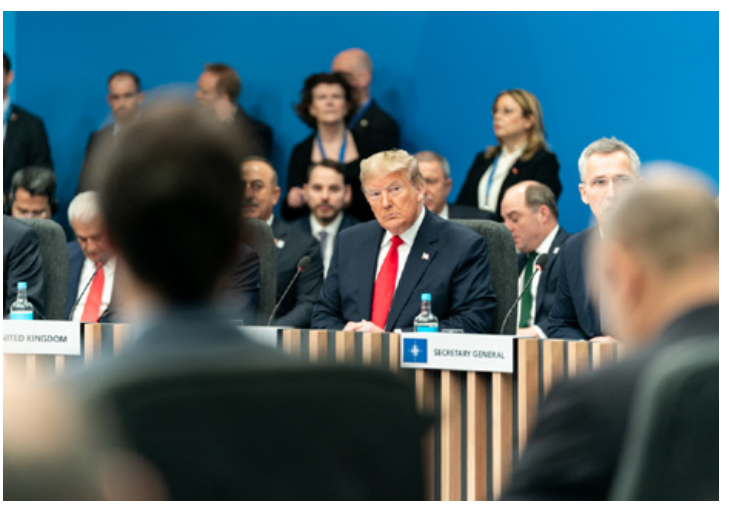


FOTO WHITE HOUSE, SHEALAH CRAIGHEAD

*Wantrouwen en het opzeggen van bestaande verdragen werken averechts*

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) adviseerde al eerder dat het internet een speerpunt moet zijn van het Nederlandse buitenlands beleid, met als doel een internationale norm die de publieke kern van het internet kan vrijwaren van oneigenlijke interventies van overheden.[75] Nederland zet zich actief in voor internationale, politiek aanvaardbare maatregelen en normen. De jarenlange ervaring met onderhandelen en samenwerken met allerlei belanghebbenden ('polderen') kan in zijn voordeel werken en Nederland een voortrekkersrol opleveren.[76]

Toch is niet iedereen onverdeeld positief over de Nederlandse visie op internationale afspraken over vertrouwenwekkende maatregelen en gemeenschappelijke normen. Zo constateert vredesorganisatie PAX in een recent verschenen artikel van het Rathenau Instituut dat niet alleen de VS, Rusland en China een dubbelrol spelen op dit gebied; ook Nederland doet dat. Diplomatie, de-escalatie en internationale afspraken over normen en verantwoord gedrag in cyberspace staan in de ogen van PAX haaks op de gelijktijdige ontwikkeling van offensieve cybercapaciteiten.[77]

De snelheid en het volume waarmee tegenwoordig digitale data worden gecreëerd, verstuurd of opgeslagen, zijn ongekend. Tegelijkertijd is onze maatschappij zo afhankelijk geworden van digitale netwerken, processen en systemen, dat kwaadwillenden dat kunnen misbruiken. Niet alleen criminelen buiten de zwakheden van onze computersamenleving uit. Uit het 'Cyber Security Beeld Nederland 2019' bleek andermaal dat in toenemende mate juist statelijke actoren onze maatschappij dreigen te ontwrichten door cyberactiviteiten zoals digitale spionage, sabotage en/of verstoring. Onvoldoende overeenstemming en verschillen van inzicht over

72 *The Hague Program for Cyber Norms* valt onder het the Institute of Security and Global Affairs (ISGA) bij de Faculty of Governance and Global Affairs van Leiden University. Zie: https://www.thehaguecybernorms.nl/about-us.

73 De *Global Commission on the Stability of Cyberspace* is geïnitieerd door twee onafhankelijke denktanks, The Hague Centre for Strategic Studies (HCSS) en de EastWest Institute (EWI). Zie: https://cyberstability.org/report/#appendix-c-history--goals-and-processes-of-the-gcsc.

74 Beide initiatieven zijn gelanceerd door het Ministerie van Buitenlandse Zaken, maar ook het Ministerie van Economische Zaken zet zich in voor dezelfde doelen. Dit leidde bijvoorbeeld tot de oprichting van het 'Nederlands Internet Governance Forum' (NL IGF) en het Electronic Commerce Platform Nederland (ECP) | Platform voor de InformatieSamenleving.

75 Wetenschappelijke Raad voor het Regeringsbeleid, *De publieke kern van het internet; Naar een buitenlands internetbeleid* (Amsterdam, Amsterdam University Press, 2015) 116.

76 ECP Platform voor de InformatieSamenleving, 'Nederland kan voorloper zijn op gebied van cybernormen', *Verslag van de Dag*, 14 november 2019 Zie: https://ecp.verslagvandedag.nl/artikel/%E2%80%9Cnederland-kan-voorloper-zijn-op-gebied-van-cybernormen%E2%80%9D/?encr=undefined.

77 Rathenau Instituut, 'Zonder gemeenschappelijke afspraken is uiteindelijk iedereen slechter af',22 mei 2020. Zie: https://www.rathenau.nl/nl/digitale-samenleving/zonder-gemeenschappelijke-afspraken-uiteindelijk-iedereen-slechter-af.

internationale normen en waarden voor cyberspace vergroten tegelijkertijd de digitale dreiging.[78]

Het U.S. Cyber Command onderkende ook de digitale dreiging van statelijke actoren en stelde in 2018 een 'Persistent Engagement'-strategie voor. Een aanpak waarbij de VS structureel en wereldwijd – dus ook buiten Amerikaanse netwerken en systemen – opereert in cyberspace; naadloos afwisselend tussen defensieve en offensieve acties.[79] Allereerst wil de VS zichzelf daarmee beschermen en zijn tegenstanders dwarszitten. Daarnaast wil de VS zichzelf hiermee een betere onderhandelingspositie verschaffen voor toekomstige onderhandelingen over (on)acceptabel gedrag in cyberspace.[80]

Diepgeworteld wantrouwen, conflicterende politieke, geopolitieke, sociale, economische en culturele agenda's, geheime operaties, spionage en de zero-sum-concurrentiestrijd van grootmachten om mondiale invloed, belemmeren ontwikkeling en implementatie van cyber-CBM. Inmenging in verkiezingen, handelsoorlogen en het opzeggen van bestaande, vertrouwenwekkende (!) verdragen werken averechts (de VS en Rusland zegden in 2019 het Intermediate range Nuclear Forces (INF)-verdrag op[81] en in 2020 trok de VS zich terug uit het Open Skies-verdrag).[82]

Pas als zich een *game-changing* mondiale cybercatastrofe voordoet (een soort cyber-coronavirus), ligt de weg open naar de creatie en implementatie van effectieve, wereldwijd acceptabele, politiek-bindende cyber-CBM. En zelfs zo'n mondiale catastrofe blijkt geen garantie voor internationale samenwerking en solidariteit.

Zullen die wereldwijde maatregelen er ooit komen? Mondiale consensus over ieder willekeurig onderwerp was problematisch in het verleden, is problematisch in het heden en is waarschijnlijk ook in de toekomst problematisch. Mondiale cyber-CBM zijn daarop geen uitzondering. Bestaande geopolitieke rivaliteit blijft een rol spelen in iedere discussie. Cybergerelateerde beslissingen kun je niet nemen zonder andere geopolitieke belangen af te wegen. De VN concludeerde reeds dat een wereldomvattend CBM-model in de praktijk onhaalbaar is; maatregelen moeten worden toegesneden op een specifieke situatie of regio. Deze constatering staat evenwel haaks op de pogingen van de achtereenvolgende expertgroepen van de VN (de UN GGE's) die vooralsnog alle juist een allesomvattende, mondiale cyber-CBM nastreefden; tot op de dag van vandaag zonder succes.

Cyberspace is een relatief nieuw domein en de ontwikkelingen rond (cyber-)CBM speelden zich af in recente jaren. In de discussies over de eventuele verschillen tussen cyberspace en andere disciplines waarop het CBM-proces van toepassing is, wordt vaak betoogd (voornamelijk door diplomaten), dat vooruitgang vooralsnog sneller gaat dan vooraf verwacht. De vraag is natuurlijk of dit optimisme ook op langere termijn is gerechtvaardigd, zeker als concrete, succesvolle eindresultaten uitblijven.

In het belang van internationale vrede en stabiliteit is het gewenst en noodzakelijk om de diplomatieke inspanningen voor vertrouwenwekkende maatregelen voor cyberspace te continueren, niet in de laatste plaats omdat de gesprekken, discussies en onderhandelingen op zichzelf al een wezenlijk onderdeel van het grotere confidence-building-proces behelzen. ■

78 Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), *Cybersecuritybeeld Nederland 2019* (Den Haag, 12 juni 2019) 39. Zie: https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019.

79 'Achieve and Maintain Cyberspace Superiority', *Command Vision for U.S. Cyber Command*, april 2018, 6.

80 Michael P. Fisherkeller en Richard J. Harknet, 'Persistent Engagement and Tacit Bargaining: a Path toward Constructing Norms in Cyberspace', *Lawfare* 9 november 2018. Zie: https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

81 'Opzegging van het verdrag betekent dat Rusland en de VS ongemoeid (nucleaire) raketten voor de middellange afstand kunnen stationeren, waardoor Europa in de gevarenzone komt te liggen.' Uit: Margriet Drent en Adája Stoetman, 'Opzegging van het INF-verdrag: Europa aan zet?', *Europa NU*, 25 februari 2019. Zie: https://www.europanu.nl/id/vkw7h56951x1/nieuws/opzegging_van_het_inf_verdrag_europa_aan?ctx=vhsjhdfktnpb.

82 U.S. Department of Defense, 'U.S. DOD Statement on Open Skies Treaty Withdrawal', 21 mei 2020. Zie: https://www.defense.gov/Newsroom/Releases/Release/Article/2195239/dod-statement-on-open-skies-treaty-withdrawal/source/GovDelivery/.