Veiligheid en cyberspace

Ducheine, P.A.L.

Published in:
BLIND : Interdisciplinair Tijdschrift

online interdisciplinair tijdschrift | ziedaar.nl

BLIND editie 49 Digitale wereld
13 februari 2018

Veiligheid en cyberspace

Veiligheid tegen (w)elke prijs?

door Paul Ducheine

--

Eén van de primaire doelstellingen van de Staat is het bieden van veiligheid aan zijn burgers. Dit lijkt vanzelfsprekend, maar de nationale veiligheid wordt flink op proef gesteld door recente ontwikkelingen binnen het digitale domein en informatie als belangrijke machtsfactor. Hoe beschermt de Staat zijn burgers tegen digitale bedreigingen en hoe bevordert zij de digitale veiligheid? Dit artikel bespreekt de vitale belangen die ten grondslag liggen aan de nationale veiligheid en op welke manier digitale veiligheid hier onder zou kunnen vallen.

Prof. mr. Paul Ducheine, brigade-generaal van de Militair Juridische Dienst, is militair jurist en hoogleraar Military Law of Cyber Operations & Cyber Security aan de Universiteit van Amsterdam. Daarnaast is hij (hoofdzakelijk) hoogleraar Cyber Warfare aan de Nederlandse Defensie Academie.

--

De raison d´être van de staat is veiligheid bieden.[1] Deze functie wordt in sociale contracttheorieën verklaard.[2] Volgens die theorie dragen individuele burgers hun recht veiligheid voor zichzelf (lijf en bezittingen) te organiseren over aan de staat.[3] In ruil hiervoor verschaft de staat het collectief veiligheid. Veiligheid is een randvoorwaarde voor individueel welzijn en collectieve welvaart waardoor de mens, economie en maatschappij floreert, zoals Hobbes duidelijk maakt:

> *[Without security] there is no place for industry...no arts, no letters, no society: and which is worst for all, continued fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and*

short.

Die collectieve veiligheid heeft wel een prijs. Veiligheidsorganisaties moeten bekostigd worden en bovendien moeten ze bevoegdheden toebedeeld krijgen om effectief te zijn. Die kosten brengen burgers op door een overdracht van rechten en aanspraken. Denk aan geld (bijvoorbeeld via belastingen) en toegelaten inperkingen op grondrechten (o.a. privacy). Zonder budget en bevoegdheden kan de staat geen veiligheid leveren.

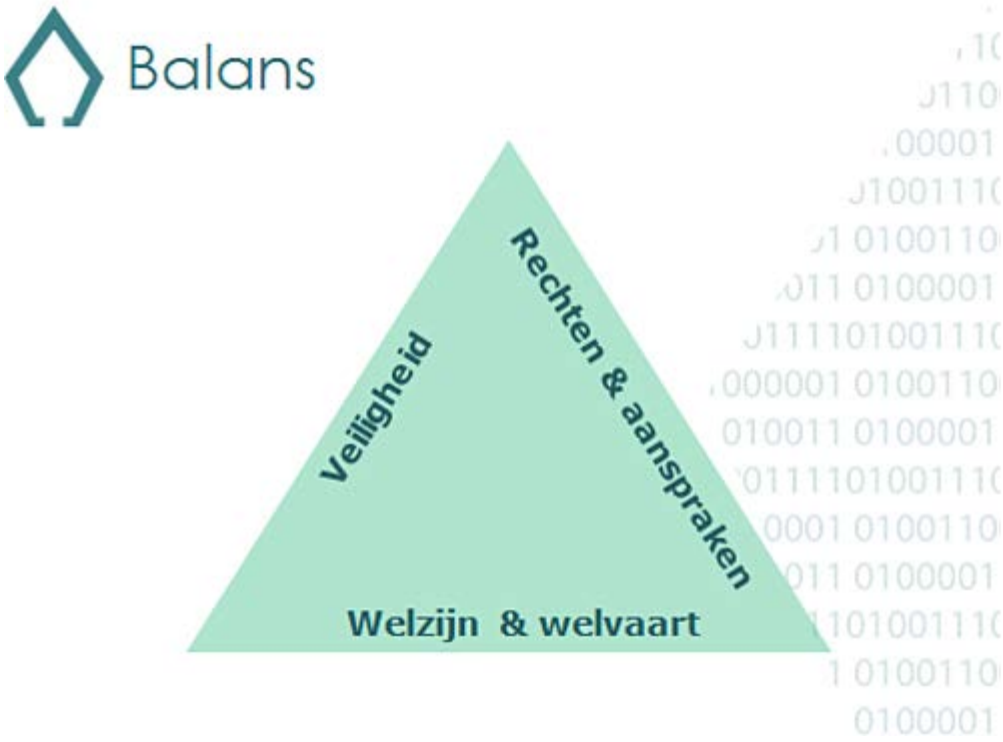
Veiligheid is dus niet gratis en de vraag is vanaf welk moment en tot welke prijs burgers veiligheid van de overheid verlangen. En wat dit in termen van individueel welzijn of collectieve welvaart oplevert.

De uitruil betekent óók dat bij gebrek aan offers van burgers, veiligheid niet op te eisen valt of niet volledig waargemaakt kán worden. Ik betwijfel of iedereen hiervan doordrongen is. Hoewel het regelmatig voorkomt, is het uiterst merkwaardig (en zelfs onbehoorlijk) wél veiligheid te vragen of te eisen, daarvoor zelfs taken te laten toebedelen, maar daarbij géén middelen (budget en bevoegdheden) te voegen. Oftewel; zonder overdracht van (voldoende) aanspraken of rechten, kan men geen veiligheid verlangen, en van welvaart en welzijn profiteren.

> Laat ik dit uitleggen via het eenvoudige voorbeeld van een studentenfiets.
>
> Stel: u studeert rechten aan de UvA. Uw mobiliteitsconcept (de fiets) is voor anderen een essentiële schakel in een malafide economisch businessmodel (oftewel, criminaliteit). Ondanks uw eigen voorzorgsmaatregelen – u had de fiets met een goed slot voor uw grachtenwoning vastgezet – wordt uw fiets ten derde male ontvreemd. Tot nu nam u uw verlies. Maar met de derde diefstal is de maat vol. U benadert de gemeente en eist – tezamen met uw grachtbewoners – van uw overheid méér veiligheid.
> Uw lokale overheid doet u prompt een voorstel. Boven uw voordeur – met uitzicht op uw fietsenstalling – komt een bewakingscamera. Dat zal fietsendieven afschrikken en in ieder geval opsporing en vervolging vereenvoudigen. Denkend aan uw al dan niet ‘wisselende contacten’ als student, stelt u – terecht – dat u ‘niets te verbergen hebt, maar dat hoeft niemand te weten’. Oftewel: u wijst een inperking van een van uw vrijheden, uw recht op privacy af.
> Uw overheid is niet voor één gat te vangen: ze biedt een alternatief. Aan het begin en einde van de gracht komt 24/7 een BOA te staan.[4] De kosten, 100.000 euro, worden hoofdelijk over de grachtbewoners omgeslagen en via gemeentelijke belastingen geïnd. Ook dit voorstel verwerpt u: een vijfde of zesde fiets of een goede verzekering zijn goedkopere alternatieven. Het ongemak dat u wellicht nogmaals een lege fietsenstalling aantreft en uw ‘mobiliteit’ ernstige gebreken vertoont, neemt u op de koop toe.
>
> *(Oratie Ducheine)*

De rol van de wetgever

Los van de individuele keuzeruimte uit het voorbeeld geldt dit spanningsveld ook – of vooral – binnen de overheid zelf. In onze democratische rechtsstaat bepaalt de wetgever immers waar die balans *veiligheid-rechten-welvaart* in dit opzicht ligt (zie Figuur 1). Oftewel: hoeveel veiligheid levert de overheid, wat ‘kost’ dat in termen van geld (via belastingen) en inperking-van-rechten, en wat levert dit ons (burgers en maatschappij) op? Deze keuzes hebben we in Nederland aan de wetgever (regering plus parlement) toevertrouwd. En die keuzes zijn actueel. Ook bij veiligheid in het digitale domein.



Figuur 1. Spanning veiligheid – rechten – welvaart/welzijn

Zo is duidelijk dat burgers en bedrijven schade (kunnen) leiden door digitale criminaliteit en terreuraanslagen. Bedreigingen van onze vitale belangen die leunen op digitale processen, dienen te worden voorkomen. Denk maar aan inmenging in democratische processen zoals verkiezingen of referenda. Vandaar bijvoorbeeld de wetsvoorstellen om opsporingsbevoegdheden voor politie en Openbaar Ministerie[5] en het verzamelen van inlichtingen door de AIVD en MIVD aan te passen.[6] Over het eerste wetsvoorstel moet het Parlement zich nog uitspreken. Het tweede, de Wet op de Inlichtingen- en Veiligheidsdiensten, is al aangenomen maar wordt binnenkort onderwerp van een raadgevend referendum. En los daarvan nam de wetgever recent wetgeving aan die het melden van datalekken in vitale sectoren verplicht stelde.[7]

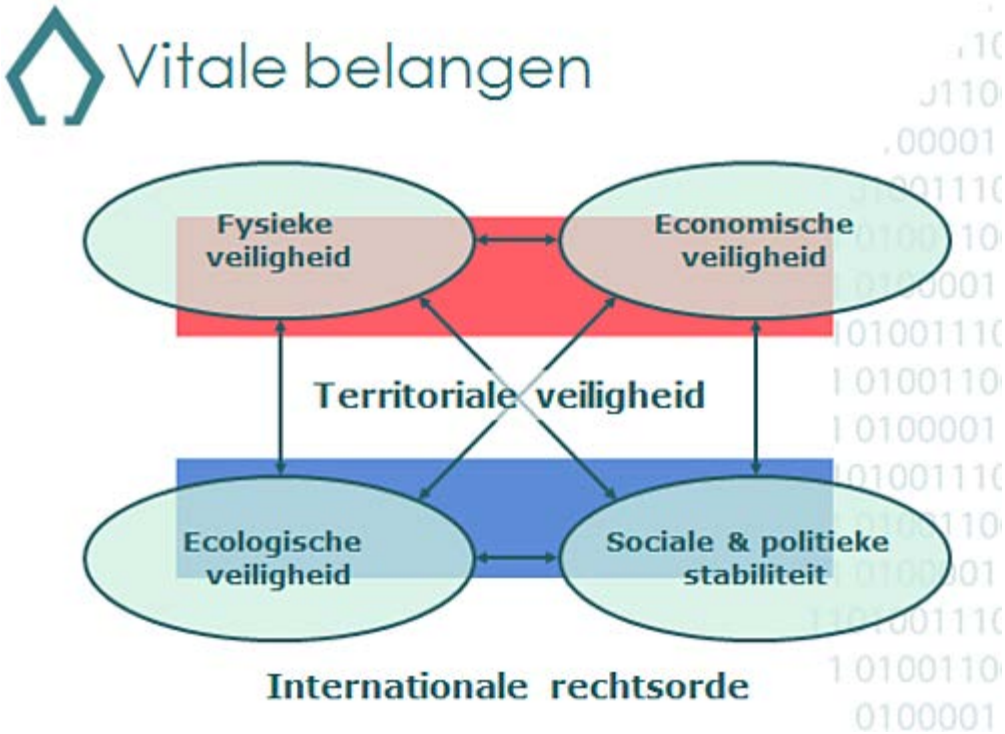
De balans bepalen in deze spanning tussen *veiligheid–rechten–welvaart* onderstreept op zichzelf al het belang van volksvertegenwoordigers en verkiezingen. Het onderstreept ook het belang van een goede informatiebasis om deze besluiten te nemen, zoals dat overigens voor alle ingrijpende overheidsbeslissingen geldt. Eveneens zijn de zorgen over de impact van dit soort nieuwe bevoegdheden om veiligheid (in het digitale) domein te verbeteren, niet meer dan logisch.

En laat ik helder zijn: hoe ingrijpender het overheidsoptreden - huidig of beoogd - des te belangrijker draagvlak, verantwoording en toezicht worden.[8] Ook over deze zorgen en ‘checks and balances’ of ‘tegenkrachten’ heeft de wetgever het voor het zeggen.

Nationale veiligheid en vitale belangen

‘Veiligheid bieden’ geldt dus als een van de klassieke en ‘harde’ taken van de overheid.[9] Het Nederlandse veiligheidsbegrip is gebaseerd op de noties van vitale belangen en strategische belangen. Deze zijn tot nu toe in twee aparte veiligheidsstrategieën verwoord.
Uit de *Strategie Nationale Veiligheid* uit 2007 volgden vijf vitale belangen:[10] territoriale, fysieke, economische, ecologische veiligheid en politieke en sociale stabiliteit.[11]
De *Internationale Veiligheidsstrategie* (2013) hanteert drie strategische belangen: territoriale veiligheid, economische veiligheid en de internationale rechtsorde.[12] Ik noem ze hierna kortheidshalve: vitale belangen (zie Figuur 2).[13]

Deze zes vitale belangen zijn bepalend voor onze nationale veiligheid. Ze werken op elkaar in (interdependent).. Een ‘hack’ in een Oekraïens boekhoudprogramma legt via een update bij rederij Maersk hier de Rotterdamse haven plat en kost miljoenen.[14]



Figuur 2. De zes vitale belangen van Nederland

Een verstoring kan vanuit het buitenland of uit Nederland zelf komen.[15] Onze economische veiligheid is bijvoorbeeld afhankelijk van een stabiele en effectieve internationale rechtsorde die digitale en fysieke handel, transacties en dienstverlening mogelijk maakt. De Nederlandse overheid staat uiteindelijk voor de klassieke taak deze vitale belangen te bevorderen en beschermen. “Beschermen” is nodig tegen bedreigingen van die vitale belangen. “Bevorderen” betreft het inzetten van machtsinstrumenten om (vitale) belangen te dienen. Bijvoorbeeld via een militaire missie in het buitenland die tot herstel of behoud van de internationale rechtsorde moet leiden, dan wel tot herstel van de territoriale integriteit van eigen of bondgenootschappelijk grondgebied.
Beschermen en bevorderen van vitale belangen vergen investeringen, onder meer door de allocatie van machtsmiddelen en door een goede informatiepositie over dreigingen van vitale belangen en potentiele rivalen of (militaire) opponenten.[16]

Tekst loopt door onder foto.

Informatie als machtsfactor

Informatie als machtsbron is dankzij het digitale tijdperk toe aan een herwaardering.[17] Klassiek is de notie “kennis is macht”. Maar er is meer. Via directe dwang (b.v. sabotage), door institutionele macht (b.v. sleutelposities binnen ICANN) of structurele macht (b.v. eigendom van glasvezelnetwerk of Facebook) is dit al bekend terrein. Echter, vooral als productieve machtsfactor komt informatie tot wasdom.[18] Dat wil zeggen dat actoren met informatie de politieke agendavorming kunnen beïnvloeden of een debat kunnen starten, versterken en beïnvloeden.[19] Dit geheel faciliteert nieuwe ‘elites’ en actoren.

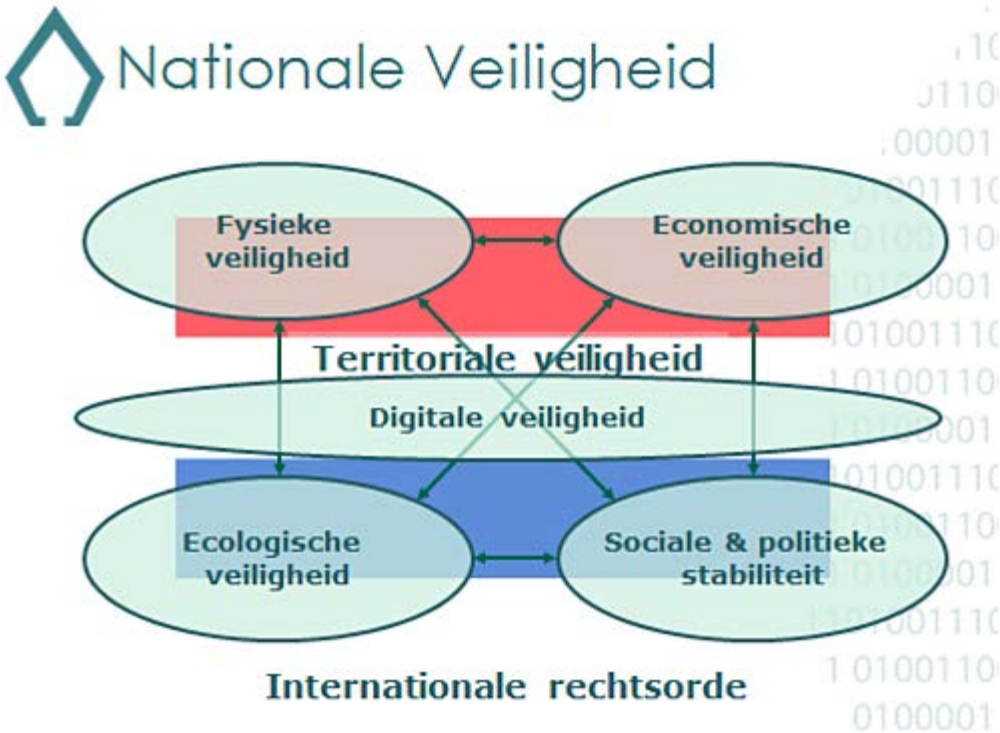
> *“In a ‘networked society’ – that is, one whose social structure is characterized by networks activated*

by information technology – new elites derive their power from an enhanced ability to delve between the layers of hardware and software from which cyberspace is constructed.”[20]

Niet alleen de bonafide ‘big five’ *Apple*, *Amazon.com*, *Microsoft*, *Facebook* en *Google*, bezitten zo’n enorme macht.[21] Ook een individu zoals *@realDonaldTrump* beschikt over productieve macht.[22]
Gelegenheidscoalities als *Anonymous* en #MeToo worden nu als machtsfactoren gezien.[23]
Bovenal is informatie essentieel om problemen en kansen te onderkennen, te begrijpen, te doorzien en in te zien wat nodig is ze te pareren dan wel benutten.

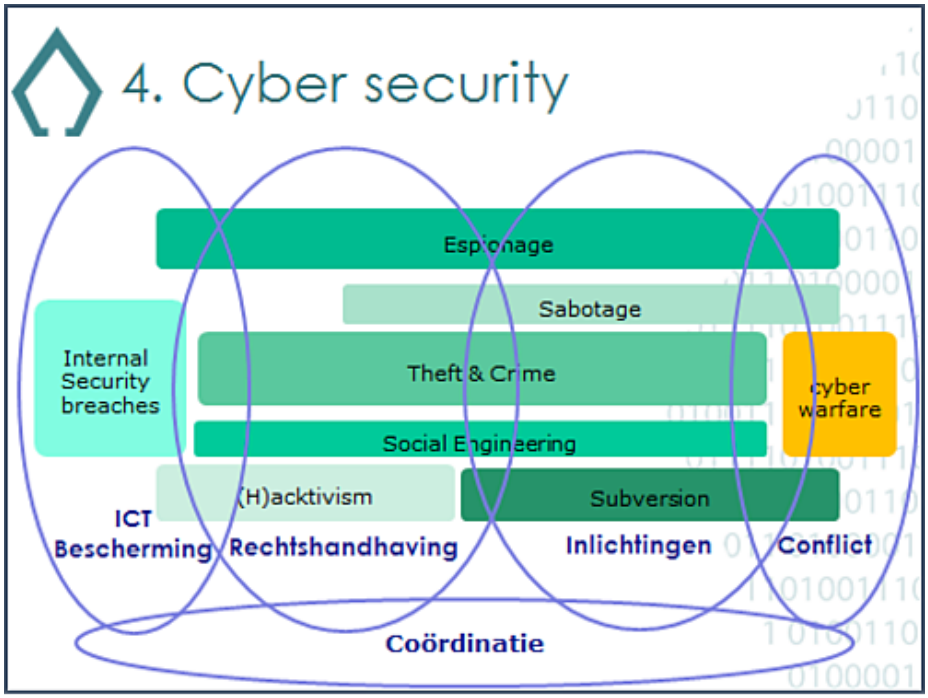
Cyber security als zevende vitale belang

De proliferatie en de brede maatschappelijke afhankelijkheid van ICT[24] brengt onze vitale economische, bestuurlijke, politieke en sociale processen binnen het bereik van deze actoren.[25] 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.[26] Bovendien brengt het digitale domein een militair conflict snel en eenvoudig dichtbij.[27]
In dat opzicht zou ons begrip van nationale veiligheid ondertussen een zevende vitale belang moeten bevatten: digitale veiligheid (zie Figuur 3).[28]



Figuur 3. Het zevende vitale belang van Nederland

Digitale veiligheid is in de *Nationale Cyber Security Strategie-2* gedefinieerd als: “het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan.”[29]
Inbreuken (en de daaruit volgende schade) kunnen verschillende vormen aannemen.[30] Ze variëren van technisch falen, menselijke fouten, bewust menselijk handelen zoals activisme, malversaties, spionage, sabotage en oorlogshandelingen (zie Figuur 4). Daarachter gaan statelijke en niet-statelijke actoren schuil.[31] Die laatste categorie omvat onder meer (combinaties van) criminelen, activisten, actiegroepen, terroristen, rebellen én commerciële bedrijven.



Figuur 4. Digitale onveiligheid en cyber security paradigma's

Het verbeteren van onze digitale veiligheid is rondom vier paradigma's geconstrueerd: bescherming van ICT, rechtshandhaving, inlichtingen en conflict.[32] Deze paradigma's bieden een bestuurlijk, juridisch en organisatorisch kader waarbinnen de overheid en private partijen hun bijdrage leveren (zie Figuur 4). De paradigma's bepalen allereerst de taak (inclusief de rechtsbasis daarvoor), het toe te passen rechtsregime, de gezagsrelaties en het toezichtmechanisme. Zo omvat het rechtshandhavingsraamwerk de taakstelling voor de politie[33] tot het opsporen van strafbare digitale feiten,[34] opsporingsbevoegdheden om digitaal te rechercheren[35] en verantwoordings- en toezichtstructuren zoals een openbare en onafhankelijke meervoudige rechtsgang. Het conflict paradigma is uit zijn aard belegd bij Buitenlandse Zaken en Defensie. Dit is het domein voor *cyber warfare*.
Deze vier paradigma's maken dat verschillende departementen een rol bij *cyber security* spelen. Om deze verschillende inspanningen onderling af te stemmen zodat dit beleid legitiem, efficiënt en bovenal effectief is, is een vijfde paradigma, horizontale coördinatie nodig. Althans in het Nederlandse staatsbestel. Elders, bv het Verenigd Koninkrijk, wordt dit langs hiërarchische weg opgelost.

Auteur: Paul Ducheine

Literatuurlijst

1. In de woorden van de Wetenschappelijke Raad voor het Regeringsbelid (WRR) is veiligheid de belangrijkste functie van de

overheid: ‘het verzekeren, [...] van de fysieke veiligheid van de burgers’. Zie: WRR, De toekomst van de nationale rechtsstaat, Den Haag: Sdu uitgevers 2002, p. 53.

2. Thomas Hobbes, Leviathan or the matter, form and power of a Common Weatlh ecllesiasticall and civil (M. Oakeshott, Red.) Oxford: Blackwell 1960.

3. Het recht op zelfverdediging in noodweersituaties blijft uiteraard bestaan.

4. Buitengewoon Opsporingsambtenaar.

5. De zogeheten Wet Cybercriminaliteit III.

6. De Wet op de Inlichtingen- en Veiligheidsdiensten 2017.

7. Wet gegevensverwerking en meldplicht cybersecurity.

8. Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), *Reactie CTIVD op concept-wetsvoorstel Wiv 20XX*, 2015, p. 1, ctivd.nl.

9. Zie: *WRR, De toekomst van de nationale rechtsstaat*, Den Haag: Sdu uitgevers 2002, p. 53.

10. *Kamerstukken* II 2006-07, 30 821, nr. 1, p. 3: “De nationale veiligheid is in het geding als vitale belangen van onze staat en/of onze samenleving zodanig bedreigd worden dat sprake is van (potentiële) maatschappelijke ontwrichting”...

11. *Kamerstukken* II, 2006-07, 30 821, nr. 2, Strategie Nationale Veiligheid, p. 3: “Vitaal belang: belang dat bepalend is voor de instandhouding van [nationale veiligheid. Bij] het deels of geheel verstoord raken of wegvallen van dat belang [komt] het functioneren van de staat en de samenleving in potentie of feitelijk in gevaar”..

12. *Kamerstukken* II 2012-13, 33 694, nr. 1, Internationale Veiligheidsstrategie – Veilige wereld, veilig Nederland; *Kamerstukken* II 2014-15, 33 694, nr. 6 bijlage, Beleidsbrief Internationale Veiligheid – Turbulente Tijden in een Instabiele Omgeving; *Kamerstukken* II 2015-16, 33 694, nr. 9 (Samenhang in missies).

13. P.A.L. Ducheine, *‘Je hoeft geen zwaard en schild te dragen om ridder te zijn’ - Mythen over digitale oorlogsvoering en recht* (Oratie UvA), Amsterdam: AUP, 2016, ook (verkort) via: militairespectator.nl, of webcollege: webcolleges.uva.nl.

14. Wouter van Noort, ‘Hack kost Maersk honderden miljoenen’, in: *NRC Handelsblad* (16-8-2017), via: nrc.nl: “De cyberaanval van eind juni dit jaar kost de Deense rederij 200 tot 300 miljoen dollar, zei het woensdag bij de presentatie van de kwartaalcijfers”.

15. Zie ook NCTV, *Contra Terrorisme Strategie 2016-2020*, p. 7: “Extern = Intern. Er is een sterke samenhang tussen de internationale, nationale en lokale dimensie van de dreiging”.

16. P. Ducheine, ‘Nationale veiligheid en hybride dreiging: twee kanten van dezelfde medaille’, in: *Magazine Nationale Veiligheid – Thema Hybride Dreiging* (2016-5), pp. 7-10. Via nctv.nl.

17. 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: ccdcoe.org

18. David J. Betz & Tim Stevens (2011), *Power and cyberspace*, Adelphi Series, pp. 35-54

19. Betz & Stevens, p. 45.

20. Jelle van Haaster, 2016, ‘Assessing Cyber Power’, in: N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.), *8th International Conference on Cyber Conflict: Cyber Power* (2016), pp. 7-22, via: ccdcoe.org.

21. New York Times, Tech’s ‘Frightful 5’ Will Dominate Digital Life for Foreseeable Future (20 January 2016), via: nytimes.com.

22. Time, The 30 Most Influential People on the Internet (5 March 2015), via: time.com.

23. Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London – New York: Verso 2015, pb).

24. European Institute for Security Studies, *A changing global environment 2014* (Chaillot Paper no. 133, December 2014), p. 29-30, via: iss.europa.eu.

25. Centre for European Policy Studies, More union in European defence (2015), p. 9, via ceps.eu.

26. McKinsey Global Institute, *Digital globalization: The new era of global flows*, March 2016, via: mckinsey.com.

27. P. Ducheine, De bevordering en bescherming van nationale belangen en militaire missies, Position Paper t.b.v. hoorzitting/rondetafelgesprek Tweede Kamer, Commissie BZK vanwege wetsvoorstel Wet op de inlichtingen- en Veiligheidsdiensten 20.., Dossiernr. 34 588, tweedekamer.nl.15-12-2016.

28. P. Ducheine, ‘Defensie in het digitale domein’, in: *Militaire Spectator*, 186-4 (2017), pp. 152-168, via:

militairespectator.nl. Zie ook de twee successievelijk en expliciete cyber security strategieën (I en II). In die zin ook het pleidooi voor een minister-zonder-portefeuille voor ICT, in: Het Financieele Dagblad, *Kabinet heeft minister van ICT nodig* (10 januari 2016), via: fd.nl. Hoewel de petitie daarvoor heden (21-9-2016) slechts 316 ondertekeningen kent, zie: < http://ministervanict.nl/>..

29. Ministerie van Veiligheid en Justitie, *Nationale Cyber Security Strategie-2 – Van Bewust Naar Bekwaam* (NCSS-2) Den Haag: NCTV 2013.

30. Ministerie van Veiligheid en Justitie, *Cybersecuritybeeld Nederland 2015*, Den Haag: NCSC 2015.

31. Zie NCSC, *Cybersecurity Beeld Nederland* (CSBN) 2011; CSBN-2 (2012); CSBN-3 (2013); CSBN-4 (2014); en CSBN-5 (2015) via: ncsc.nl.

32. P.A.L. Ducheine, 'The Notion of Cyber Operations', in: N. Tsagourias & R. Buchan, *Research Handbook on International Law and Cyber Space*, Cheltenham: Edward Elgar Publishing 2015, p. 211-232.

33. Artikel 3 Politiewet 2012.

34. Zoals bijvoorbeeld een 'DDOS-aanval' als in artikel 138b Sr.

35. J.J. Oerlemans en B.J. Koops (2012), 'Surveilleren en opsporen in een internetomgeving', in: WODC, *Justitiële verkenningen* 2012, 38-5, pp. 35-49.

http://www.ziedaar.nl/article.php?id=562
BLIND editie 49 Digitale wereld
13 februari 2018
issn 1879-8144