Cyberoperaties in de gray zone

Juridische overwegingen omtrent de rol voor de krijgsmacht

Willemijn A. Bos en Peter B.M.J. Pijpers*

Met de doctrine van 'Persistent Engagement' geven de Verenigde Staten aan dat zij in vredestijd naast inlichtingenoperaties ook cyberoperaties buiten de eigen landgrenzen verrichten: een juridisch controversieel thema. Lastig, want terwijl de regelgeving inzake grensoverschrijdende cyberactiviteiten onder het niveau van geweld nog niet is uitgekristalliseerd, vinden juist in deze 'gray zone' de meeste cyberactiviteiten plaats. In dit artikel onderzoeken we de juridische grenzen voor activiteiten in de gray zone, zoals bepaald door de beginselen van soevereiniteit en non-interventie in cyberspace, en tasten we af welke rol de krijgsmacht hierin heeft. Nederland staat voor een dilemma: de krijgsmacht is niet voorbestemd om zonder mandaat op te treden in de gray zone, terwijl opponenten zich hier juist op toeleggen.

Cyberactiviteiten zijn aan de orde van de dag, niet alleen binnen een staat maar ook tussen staten onderling. Of het nu gaat om kwaadaardige software (hierna: *malware*) op een computer zetten; een netwerk vertragen of tijdelijk buiten werking stellen door grootschalige *Distributed Denial of Service* (DDoS)-'aanvallen'; of door het beïnvloeden van de publieke

* Kornet Willemijn A. Bos is jurist en reservist bij de Koninklijke Marechaussee en is vanuit het Defensity College werkzaam geweest bij de NLDA. Kolonel Peter B.M.J. Pijpers is universitair hoofddocent Cyber Operations bij de Faculteit Militaire Wetenschappen aan de NLDA. De auteurs danken lt-kol Arnold MSc, bgen prof. dr. Ducheine & prof. dr. Zwanenburg voor hun reflecties op eerdere versies van het artikel.

1 Zie bijvoorbeeld FireEye, 'APT28: A Window Into Russia's Cyber Espionage Operations?', *Fire Eye Threat Research*, 27 oktober 2014. Zie: https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

opinie via gefabriceerde *social media*-berichten. Het scala aan activiteiten dat actoren uitvoeren via cyberspace en het internet is groot, net zo groot als de variëteit aan actoren: van *script kiddies* op zolder tot aan zogeheten *Advanced Persistent Threats* (APT), professionele *hackers* en socialemedia-experts, vaak gelieerd aan statelijke inlichtingendiensten.[1]

Oefening met elektromagnetische en cybermiddelen. Wat zijn de juridische grenzen in de gray zone, en welke rol heeft de krijgsmacht?

FOTO MCD, JARNO KRAAYVANGER

De vraag die de bovengenoemde voorbeelden oproepen is: mag dit wel? Naast politieke en ethische overwegingen gaat het in dit artikel primair om de vraag of dit internationaalrechtelijk (in de relatie tussen staten) is toegestaan. Een vervolgvraag is: en wat betekent dit voor de inzet van de krijgsmacht? Een andere staat de wil opleggen is van oudsher een activiteit waarin het militaire machtsinstrument, veelal de krijgsmacht, een prominente rol heeft, zeker tijdens een gewapend conflict.

Het gros van de cyberactiviteiten vindt echter niet plaats tijdens oorlog en conflict, maar juist onder het niveau van geweld, zoals bedoeld in artikel 2(4) VN-Handvest dat interstatelijk geweldgebruik verbiedt.[2] Juridisch betekent dit, dat noch het *ius ad bellum*, het recht omtrent interstatelijk geweldgebruik,[3] noch het *ius in bello* (humanitair oorlogsrecht), het geldende regime tijdens gewapend conflict, van toepassing zijn. Echter, het feit dat (cyber) activiteiten onder het niveau van geweld blijven, betekent niet dat ze daarom zijn toegestaan onder het internationaal recht. Ook onder het niveau van geweld zijn interstatelijke activiteiten gereguleerd. Zo moet een staat onder meer de soevereiniteit van andere staten respecteren en mag hij zich niet mengen in de interne aangelegenheden van een andere staat – het beginsel van non-interventie.

De vraag naar de rol van de krijgsmacht is daarmee nog interessanter. Waar het prerogatief van de krijgsmacht lag bij conflict en oorlog, zien we in cyberspace – waar de grens tussen oorlog en vrede vervaagt – dat krijgsmachten buiten de landsgrenzen zeer (pro-)actief zijn onder het niveau van geweld; in de zogeheten gray zone.[4] Denk daarbij aan de Russische beïnvloedingsoperaties tijdens de Amerikaanse verkiezingen van 2016 of de eufemistisch genaamde 'persistent engagement' of 'hunt forward'-activiteiten van het U.S. Cyber Command,[5] activiteiten die strategisch interessant, maar juridisch controversieel zijn.[6]

De centrale vraag in dit artikel is: 'wat is het juridische kader voor staten bij grensoverschrijdende operaties in cyberspace onder het niveau van geweld, en welke rol heeft de krijgsmacht in de zogenoemde gray zone'? Het doel van dit artikel is de onduidelijkheid over het optreden in de grijze zone te verkleinen en de discussie over de rol van de krijgsmacht daarin te starten. Eerst staan wij stil bij de vraag wat cyberoperaties zijn om vervolgens het juridisch raamwerk te schetsen voor grensoverschrijdende activiteiten onder het niveau van geweld, met daarbij de nadruk op de beginselen van soevereiniteit en non-interventie. Aansluitend toetsen wij de cyberoperaties aan het juridische raamwerk. Na enkele reflecties op de consequenties voor de krijgsmacht sluiten wij af met een conclusie.

De beperking van dit artikel is dat het cyberoperaties in de gray zone analyseert vanuit internationaal publiekrechtelijk perspectief en daarmee wegblijft van nationale wetgeving, de rol van nationale rechtshandhavers,[7] of van een politieke of ethische duiding. Voor de toepassing van het internationale recht in cyberspace hanteren wij de *Tallinn Manual*.[8] Verder zijn de

2 Harriet Moynihan, 'The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention', *Chatham House*, 2 december 2019, 22.

3 Zoals bijvoorbeeld het geweldsverbod uit artikel 2(4) en de zelfverdedigingsclausule uit artikel 51 van het VN-Handvest.

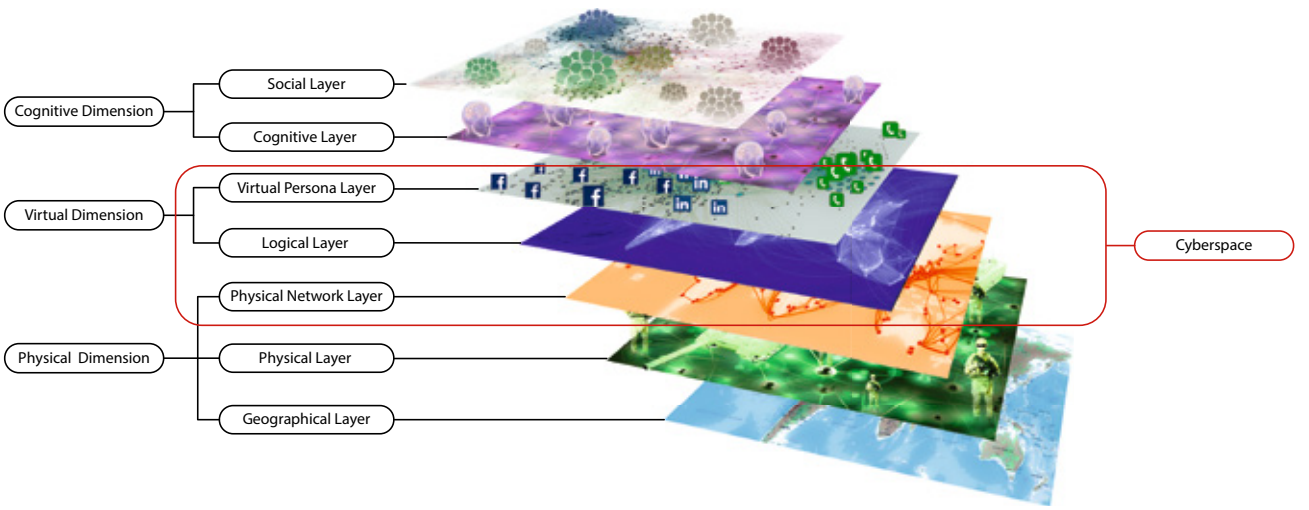
4 Elizabeth G. Troeder, 'A Whole-of-Government Approach to Gray Zone Warfare', *U.S. Army War College SSI*, 26 december 2019, 2; Michael N. Schmitt, 'Grey Zones in the International Law of Cyberspace', in: *The Yale Journal of International Law* 42 (2017) (2) 1–21. Juridisch bestaat het grijze gebied uit a) het vraagstuk of soevereiniteit een beginsel of een bindende verplichting is in cyberspace; en b) of een 'remote cyber operation' die geen schade aanricht wederrechtelijk is.

5 Zie bijvoorbeeld Louk L.C. Faessen en Deborah Lassche, 'Persistent Engagement in het Cyberdomein: Stabilisatie of Escalatie?', in: *Militaire Spectator* 189 (2020) (12) 636–47; Paul M. Nakasone and Michael Sulmeyer, 'How to Compete in Cyberspace: Cyber Command's New Approach', *Foreign Affairs*, 2020; Joshua Rovner, 'More Aggressive and Less Ambitious: Cyber Command's Evolving Approach', *War On The Rocks*, 2020.

6 Michael P. Fischerkeller and Richard J. Harknett, 'Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace', *Lawfare*, 2018; Robert Chesney, 'The Domestic Legal Framework for US Military Cyber Operations', *Hoover Institution Aegis Paper*, 2020; Max Smeets, 'Cyber Command's Strategy Risks Friction With Allies', *Lawfare*, 2019.

7 Te denken valt aan de hack-back bevoegdheid van het Digital Intrusion Team van de politie op grond van wet Computer Criminaliteit III.

8 De *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (hierna: *Tallinn Manual*) uit 2017 is een gezaghebbend 'handboek' dat beschrijft hoe het internationale recht van toepassing is op cyberoperaties (tussen staten onderling). Het handboek is geen wetboek, maar geschreven door een internationale groep experts op het gebied van internationaal recht. De opzet van de TM2 is gefaciliteerd en begeleid door het NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE).



Figuur 1 Cyberspace en de informatieomgeving[11]

casus en het juridische kader instrumenteel voor het doel van het artikel en daarmee vereenvoudigd weergegeven.

Cyberoperaties

Een cyberoperatie is voor dit artikel gedefinieerd als een activiteit die effecten genereert in of via cyberspace.[9] Cyberspace bestaat uit een fysiek en een virtueel deel. De virtuele dimensie van cyberspace bestaat uit de 'virtual personae' en de logische laag.[10] Virtual personae geven mensen en organisaties de mogelijkheid om cyberspace te betreden via een digitale identiteit, zoals een e-mailadres of een *username*, en daarmee toegang te krijgen tot de tweede 'logische' virtuele laag. De logische laag bevat de firmware, operating systems, software, applicaties maar ook de data van cyberspace. De virtuele dimensie van cyberspace leunt op de fysieke netwerklaag, bestaande uit fysieke componenten zoals computers, routers en kabels. De drie lagen van cyberspace bevatten tevens de potentiële objecten die relevant zijn voor defensieve en offensieve militaire cyberoperaties.

Cyberoperaties zijn in te delen in hard- en soft-cyberoperaties.[12] Een cyberoperatie die met een digitaal 'wapen' effecten genereert in cyberspace, zoals het veranderen van de software of het manipuleren van data, is een hard-cyberoperatie. Ook het langs digitale weg vernietigen van soft- of hardware valt hieronder. Het gebruikte digitale 'wapen' om objecten en data in cyberspace te manipuleren is code, ofwel een programma van 'nullen en enen'. Soft-cyberoperaties, zoals het beïnvloeden van verkiezingen met desinformatiecampagnes, hebben geen initieel effect in cyberspace, maar gebruiken cyberspace als vector om effecten te bereiken in de cognitieve dimensie – perceptie, begrips- en besluitvorming. Het 'wapen' van soft-cyberoperaties is de inhoud (*content*) van een bericht.

9 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, Cambridge University Press, 2013) 258; Cyberspace en het cyberdomein zijn inwisselbaar, in dit artikel gebruiken wij cyberspace. Naast het domein van cyberspace bestaan onder meer het land-, lucht-, zee-, en ruimtedomein. Zie voor de dimensies en de domeinen ook de Nederlandse Defensie Doctrine (2019), hoofdstuk 4.

10 Peter B.M.J. Pijpers en Kraesten L. Arnold, 'Conquering the Invisible Battleground', in: *Atlantisch Perspectief* 44 (2020) (4).

11 Figuur 1 is gebaseerd op een indeling van de informatieomgeving gebaseerd op werk van Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, 'Manoeuvring and Generating Effects in the Information Environment', in: Paul A.L. Ducheine and Frans P.B. Osinga (red.), *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis - NL ARMS 2017*, 2017; Jelle van Haaster, 'On Cyber: The Utility of Military Cyber Operations During Armed Conflict', 2018. Noot: volgens Van Haaster bevat cyberspace ook de 'geographical layer', zie On Cyber, blz. 159.

12 Pijpers en Arnold, 'Conquering the Invisible Battleground'. Zie ook eerdere gedachten hierover in: Paul A.L Ducheine en Jelle van Haaster, 'Cyber-Operaties en Militair Vermogen', in: *Militaire Spectator* 182 (2013) (9) 378.

FOTO GAGE SKIDMORE

Podium voor een campagnebijeenkomst van Hillary Clinton in 2016. De Russische hack van de Democratische Partij en Clintons campagne was een hard-cyberoperatie, daarna volgde een cyberoperatie gericht op de cognitieve dimensie

Om de cyberoperaties tastbaarder te maken en te kunnen toetsen aan een juridisch raamwerk van soevereiniteit en non-interventie, volgen enkele gray zone-casussen van hard- en soft-cyberoperaties;[13] in Oekraïne, Georgië en de Verenigde Staten (VS).

Op 23 december 2015 meldde een Oekraïens regionaal distributiebedrijf storingen in de elektriciteitslevering.[14] Kort na de storing beweerden Oekraïense regeringsfunctionarissen dat de uitval was veroorzaakt door een cyberaanval en dat Russische veiligheidsdiensten, meer specifiek de 'Sandworm'-APT, daarvoor verantwoordelijk waren.[15] Bij deze aanval, waarbij 225.000 klanten gedurende drie uur geen stroom hadden, is gebruik gemaakt van 'BlackEnergy malware' om via e-mails toegang te krijgen tot de controlesystemen van de energiecentrale.[16] Vervolgens is de geïmplanteerde KillDisk-software geactiveerd om data te wissen. Tot slot is de centrale van de buitenwereld afgesloten door het overbelasten van de telefoonverbindingen (Telephony Denial of Service (TDoS)), waardoor zij de storing niet direct waarnam.

Tijdens dit incident op het Oekraïense elektriciteitsnet is voor het eerst een digitaal wapen gebruikt om een elektriciteitsnet met een cyberactiviteit vanuit het buitenland plat te leggen, zonder fysiek in de doelstaat aanwezig te zijn. Vele zouden volgen, zoals in Georgië.[17] Op 28 oktober 2019 zijn meerdere cyberaanvallen uitgevoerd tegen Georgië, door het verstoren, schenden, ongewenst aanpassen (*defacement*) en onderbreken van meer dan 2.000 private en publieke websites waaronder van de nationale televisiemaatschappij. De actie is wederom toegeschreven aan de Sandworm-APT van de Russische militaire inlichtingendienst.[18]

Naast hard-cyberoperaties kan een cyberoperatie zich ook direct richten op de cognitieve dimensie, zonder effecten teweeg te brengen in cyberspace.[19] Het Mueller-rapport, een onderzoeksrapport naar aanleiding van mogelijke verstoring in aanloop naar de presidentsverkiezingen van 2016 in de VS, geeft aan dat de 'Russian government interfered in the 2016 presidential election in sweeping and systematic fashion.'[20] Het gaat daarbij vooral om het lekken van informatie en data rondom presidentskandidate Clinton, na een eerdere hack (een hard-cyberoperatie) in de bestanden van de Democratische Partij en het campagneteam van Clinton, en het stelselmatige uitbuiten van

13 Zie voor meer voorbeelden: https://cyberlaw.ccdcoe.org/wiki/Main_Page of https://www.cfr.org/cyber-operations/. Noot: In de praktijk zijn hard- en soft-cyberoperaties minder goed te scheiden zoals bij de hack-and-leak-operaties, zie James Shires, 'Hack-and-Leak Operations: Intrusion and Influence in the Gulf', in: *Journal of Cyber Policy* 4 (2019) (2) 235–56.

14 Robert Lee, Michael Assante, en Tim Conway, 'Analysis of the Cyber Attack on the Ukrainian Power Grid', *SANS Industrial Control Systems Security Blog*, 2016.

15 De groep Sandworm-APT is onder meer bekend onder de volgende namen: Sandworm Team, Black Energy (/BlackEnergy), Quedagh, Voodoo Bear, TEMP.Noble, Electrum, TeleBots en Iron Viking. Zie ook: United States District Court, Indictment (United States v Andrienko) "Sandworm" (2020).

16 'Cyber Law Toolkit: Power Grid Cyberattack in Ukraine (2015)', CCDCoe, 2020. Zie: https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

17 Voor een overzicht zie: Council on Foreign Relations, Cyber Operations Tracker, https://www.cfr.org/cyber-operations/#Timeline.

18 United States Department of State, 'The United States Condemns Russian Cyber Attack Against the Country of Georgia', (2020).

19 Denk daarbij aan beïnvloeding van referenda (2016 Brexit) of verkiezingen (Franse verkiezingen in 2017, verkiezingen VS van 2016 en 2020). Zie bijvoorbeeld: Office of the Director of National Intelligence, 'Foreign Threats to the 2020 US Federal Elections', 2021.

20 Robert S. Mueller, 'Report On The Investigation Into Russian Interference In The 2016 Presidential Election', vol. I and II, 2019, 1.

sociale media door de aan de Russische regering gelieerde 'trollenfabriek' Internet Research Agency (IRA), met als doel 'to provoke and amplify political and social discord in the United States.'[21]

Het juridisch kader

Een staat die, buiten een gewapend conflict, een weloverwogen operatie uitvoert in een andere staat via cyberspace, bevindt zich geenszins in een soort wetteloos Wilde Westen.[22] Een (virtuele) inmenging in een ander land is, net als bij een fysieke ingreep, gebonden aan regels van internationaal recht, in het bijzonder het verbod op interventie en respect voor de soevereiniteit van andere staten.[23] Meerdere rechtsbeginselen reguleren het gedrag van staten, zoals verplichtingen uit mensenrechtenverdragen, het zelfbeschikkingsrecht of *due diligence*.[24] Dit deel beschrijft echter specifiek soevereiniteit en non-interventie omdat de casussen uitgaan van de slachtofferstaat, en daarnaast omdat het specifiek om statelijke actoren gaat. Beide beginselen zijn ook geldig bij activiteiten in cyberspace, met als premisse dat de actie is toe te rekenen aan een staat.

Soevereiniteit

Staten zijn soeverein, ongeacht de grootte of samenstelling ervan.[25] Een gezaghebbende omschrijving van soevereiniteit is die van de arbiter in de Island of Palmas-zaak uit 1928: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[26]

Soevereiniteit is derhalve gebaseerd op territoriale integriteit en politieke onafhankelijkheid, inhoudende dat een staat de exclusieve bevoegdheid en beschikkingsmacht heeft over zijn grondgebied, bevolking en activiteiten op dat grondgebied.[27]

Het internationaal publiekrecht is van toepassing op cyberspace,[28] zo ook het principe van staatssoevereiniteit.[29] De *Tallinn Manual* verwoordt dit als volgt: '[a] State must not conduct cyber operations that violate the sovereignty of another State.'[30]

Figuur 2 Cyberaanvallen van Staat A op Staat B

Cyberoperaties kunnen plaatsvinden door Staat A, vanaf het territoir van Staat B, gericht op Staat B. Staat A is dan fysiek al binnengedrongen in het territoir van Staat B (de groene pijlen in figuur 2). De casus rondom schending van territoriale integriteit is dan juridisch relatief eenvoudig en analoog aan een fysieke inbreuk.[31] Een statelijk orgaan van A, dat cyberoperaties uitvoert in (en tegen) Staat B, en aanwezig is zonder toestemming of rechtvaardigingsgrond schendt diens soevereiniteit.

21 Mueller, 'Report on the Investigation', 4.
22 Michael N. Schmitt, 'Taming the Lawless Void: Tracking the Evolution of International Law', in: *Texas National Security Review* 3 (2020) (3) 33.
23 Paul A.L. Ducheine, 'Militar Cyber Operations', in: Terry D. Gill en Dieter Fleck (red.), *The Handbook of the International Law of Military Operations*, 2nd ed. (Oxford, Oxford University Press, 2015) 465-470.
24 Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law", in: *Chicago Journal of International Law* 19 (2018) (1) 53-58.
25 Artikel 2(1) VN-Handvest.
26 PCA, Island of Palmas Case (The Netherlands v United States), II Reports of International Arbitral Awards 829–71 (1928) 838.
27 Hieronder valt naast het territoir ook de territoriale zee en het luchtruim boven het territoir en territoriale zee.
28 United Nations GGE 2015 Report, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174', vol. 12404, 2015.
29 Niet alle staten zijn overtuigd dat soevereiniteit ook een bindende regel van recht is in cyberspace, zie bijvoorbeeld Jeremy Wright, 'Cyber and International Law in the 21st Century', 2018.
30 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge, Cambridge University Press, 2017); Rule 4, 17.
31 Schmitt, Rule 4 (6) 18-19. Zie ook: RIIA, Rainbow Warrior (New Zealand v France) (1990). Franse agenten brachten in Nieuw Zeeland een schip van Greenpeace tot zinken.

Lastiger is het bij cyberaanvallen die niet zijn gepleegd vanaf het grondgebied van Staat B, maar 'op afstand'. Naast dat het in de praktijk lastig te bepalen is wie de aanval heeft uitgevoerd,[32] veroorzaken deze *remote cyber-attacks* in ieder geval geen fysieke inbreuk op het territoir van de Staat B.

Om te bepalen of deze remote cyber-attacks een schending van de soevereiniteit op kunnen leveren, noemt de *Tallinn Manual* een aantal toetsingscriteria, opgesplitst naar schendingen van de territoriale integriteit en de politieke onafhankelijkheid; beide kunnen een schending van soevereiniteit opleveren.

Territoriale integriteit is geschonden wanneer bij een actie fysieke schade is ontstaan of gewonden zijn gevallen. Dit kan gebeuren wanneer malware de aansturing van mechanische systemen ontregelt, zoals in de 'Stuxnet'-operatie,[33] waarbij het Iraanse nucleaire verrijkingsprogramma in Natanz het doelwit was. Functionele schade is een tweede criterium. Denk daarbij aan het hacken van een computer en het verspreiden van een virus waardoor computers, harde schijven, routers of hele netwerken niet langer functioneren, wat kan resulteren in de noodzaak om computers of software te vervangen. De 'Shamoon'-cyber-operatie is hier een voorbeeld van.[34] Hoewel de *Tallinn Manual* -experts het eens waren dat verlies van functionaliteit 'schade' oplevert en daarmee een inbreuk op de soevereiniteit kan zijn, bereikten zij geen consensus over de precieze drempel voor functionele schade.[35] Cyberactiviteiten onder het niveau van fysieke of functionele schade, tot slot, kenmerken zich in het vertragen van de processorsnelheid van een computer; een tijdelijke onbruikbaarheid van cyberinfrastructuur of een website; of het kopiëren van gegevens zonder verdere gevolgen. De experts kwamen niet tot overeenstemming of remote cyber-attacks, die geen fysieke of functionele gevolgen hebben, te kwalificeren zijn als een schending van de soevereiniteit.[36]

Naast de territoriale integriteit kan een remote cyber-attack ook de politieke onafhankelijkheid van een staat schenden. Het gaat daarbij om het overnemen van of bemoeienis met inherente overheidsactiviteiten (ofwel: *state functions*),[37] gedefinieerd als 'an activity that is so intimately related to the public interest as to mandate performance by government personnel.'[38] Dit zijn overheidstaken die enkel de overheid kan uitvoeren, gekoppeld aan de vitale belangen van de staat, zoals het houden van verkiezingen, het innen van belasting, de nationale verdediging of rechtshandhaving. Materiële schade is bij deze schendingen via cyberspace niet vereist. Een inbreuk op de politieke onafhankelijkheid vindt plaats bij het (zonder toestemming) overnemen van inherente overheidsactiviteiten.[39] Bijvoorbeeld als Staat A, zonder toestemming van B, verdachten aanhoudt in B, of informatie verzamelt in politiedatabases in Staat B. Naast het overnemen van taken kan ook bemoeienis (*interference*) met de inherente overheidstaken, zoals het platleggen van de site van de belastingdienst waardoor het innen van belasting onmogelijk is, een schending van de politieke onafhankelijkheid en daarmee soevereiniteit opleveren. De grens tussen onrechtmatige en ongezochte bemoeienis is echter lastig te trekken, niet in de laatste plaats omdat staten steeds nauwer samenwerken, bindende verdragen sluiten en deels integreren.

Non-interventie

Het beginsel van non-interventie, een regel van internationaal gewoonterecht, verbiedt staten

32 Essentieel is dat de remote cyber-attack toe te schrijven is aan een staat of een groep onder staatscontrole, immers de notie van soevereiniteit geldt enkel tussen staten. Zie Schmitt, *Tallinn Manual 2.0*, Commentaar bij Rule 4.

33 Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', in: *Security Studies* 22 (2013) (3) 365-366.

34 Bij deze aanval is het Saoedische staatsoliebedrijf Saudi Aramco zwaar getroffen, zie: Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', in: *Strategic Studies Quarterly* 12 (2018) (3) 93.

35 Schmitt, *Tallinn Manual 2.0*, Rule 4(13) 20-21.

36 Moynihan, 'The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention', 21-24; Schmitt, *Tallinn Manual 2.0*, Rule 4(14) 21.

37 Schmitt, *Tallinn Manual 2.0*, Rule 4 (15-19) 21-23.

38 U.S. Department of the Interior, Federal Activities Inventory Reform (FAIR) Act of 1998. Zie: https://www.doi.gov/pam/programs/acquisition/fair-activities-inventory-reform-act.

39 Zoals het ontvoeren van Adolf Eichmann door Israël en daarmee de wetshandhavende taak van Argentinië overnemend. Zie: United Nations Security Council, 'Resolution 138 (1960) Question Relating to the Case of Adolf Eichmann', 138 § (1960).

met dwang in te grijpen in de interne of externe aangelegenheden van andere staten. Het interventieverbod is verwoord door het Internationaal Gerechtshof in de bodemprocedure in de zaak tussen Nicaragua en de Verenigde Staten uit 1986: 'A prohibited intervention must … be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.'[40]

De *Tallinn Manual* stelt daarom dat voor cyberspace: 'A State may not intervene, including by cyber means, in the internal or external affairs of another State.'[41]

Om een handeling, waaronder een cyberoperatie, te kwalificeren als onrechtmatige interventie, moet de handeling ten eerste betrekking hebben op die aangelegenheden waarin staten vrijelijk kunnen beslissen, zoals keuzes gerelateerd aan politiek, economie en buitenlands beleid.[42] Dit zogeheten *domaine réservé* is niet onbeperkt omdat staten rekening moeten houden met internationaal bindende verplichtingen,[43] zoals voortkomend uit internationale mensenrechtenverdragen.[44]

Ten tweede moet de handeling *coercive*, ofwel dwingend van aard zijn. Er is geen generieke definitie van dwang in het internationaal recht. In de digitale context suggereert de *Tallinn Manual* dat 'the coercive effort must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State'.[45] Cruciaal is dat de handeling het oogmerk heeft om de slachtofferstaat te dwingen een actie te ondernemen die hij anders niet zou ondernemen, of juist daarvan af te zien.[46]

Staten moeten ook bij grensoverschrijdende cyberactiviteiten de beginselen van soevereiniteit en non-interventie respecteren. Echter, doordat de toepassing van de beginselen van soevereiniteit en non-interventie in cyberspace nog niet is uitgekristalliseerd zijn er interpretatie-

FOTO MINISTERIE VAN BUITENLANDSE ZAKEN

Toenmalig minister van Buitenlandse Zaken Bert Koenders nam in februari 2013 de Tallinn Manual 2.0 in ontvangst. Dit handboek behandelt internationaal recht en cyberoperaties

verschillen opgetreden over 'hoe' het recht toe te passen is in cyberspace, waardoor 'normative uncertainty'[47] ontstaat. Deze interpretatieverschillen zorgen ervoor dat het lastig is een eensluidend juridisch oordeel te geven over gray zone- activiteiten, zoals bij onderstaande toetsing zal blijken, te meer omdat handelen van staten in de gray zone niet per definitie onrechtmatig is.

40 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US) (Merits) [1986] ICJ Rep 14, para 205.
41 Schmitt, *Tallinn Manual 2.0*, Rule 66, 312.
42 Denk ook aan de erkenning van staten en lidmaatschap van internationale organisaties. Zie: Ministry of Foreign Affairs, 'Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace' (2019) 3.
43 PCIJ, Nationality Decrees in Tunis and Morocco - Advisory Opinion, Series B PCIJ Reports (1923) 24; Katja S Ziegler, 'Domaine Réservé', in: *Max Planck Encyclopedia of International Law*, April 2013. Domaine réservé is de 'areas where States are free from international obligations and regulation'.
44 Schmitt, 'Grey Zones in the International Law of Cyberspace', 4.
45 Schmitt, *Tallinn Manual 2.0*, Commentaar bij Rule 66, para 19, blz. 318.
46 Schmitt, *Tallinn Manual 2.0*, Commentaar bij Rule 66, para 19, 21, 27, blz. 318; Zie ook: Ministry of Foreign Affairs, 'Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace' 3.
47 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law".

Het gros van de cyberactiviteiten vindt niet plaats tijdens oorlog en conflict, maar juist onder het niveau van geweld

Toetsing van cyberoperaties aan juridisch kader

In dit deel toetsen we de eerder beschreven cyberoperaties aan de interpretatie van soevereiniteit respectievelijk non-interventie in cyberspace. Mits toerekenbaar aan een staat zijn de criteria voor een schending van de soevereiniteit en non-interventie als volgt samen te vatten:

Schending van soevereiniteit:
- Is de territoriale integriteit geschonden?
  - Fysieke schade of gewonden;
  - Functionele schade;
  - Acties onder functionaliteitsverlies.
- Of, is politieke onafhankelijkheid geschonden?
  - Overnemen van, of
  - Bemoeienis met inherente overheidsfuncties.

Schending van het non-interventie beginsel:
- Is het *domaine réservé* geschonden?
- Was er sprake van dwang?

De cyberaanval op het Oekraïense elektriciteitsnet

Het platleggen van het Oekraïense elektriciteitsnet in 2015 lijkt op het eerste gezicht een duidelijke zaak. Er is sprake van fysieke schade doordat de geïnstalleerde malware een deel van de ICT-infrastructuur vernielde, en tevens trad functionele schade op door het wissen van bestanden. Activiteiten onder het niveau van functionaliteitsverlies vonden plaats in de vorm van de TDoS aanval en het installeren van malware.[48] Aangenomen dat de schending door een staat, of door een staat gecontroleerde groepen,[49] is verricht, is voldaan aan de criteria voor het schenden van de territoriale integriteit.

Of de politieke onafhankelijkheid is geschonden, hangt af van invulling van het begrip 'inherente overheidstaken'. Energievoorziening, in Oekraïne grotendeels in private handen, valt daar niet onder. De overheid maakt weliswaar energievoorzieningsbeleid, inclusief gerelateerd aan de invoering van nieuwe vormen van energie, maar de elektriciteitsvoorziening als geheel is geen generieke staatstaak.

Een schending van het interventieverbod vereist een inbreuk op het domaine réservé van Oekraïne. Energievoorziening is weliswaar geen 'inherent governmental function', maar valt wel onder het domaine réservé, omdat de rechtsmacht op dit vlak niet is ingeperkt door bindende regels van internationaal recht. Daarnaast moet de interventie op een dwingende wijze hebben plaatsgevonden. Een tijdelijke black-out van de energievoorziening in een ander land kan daar zeker onder vallen.[50] Het vermoeden is dat de Russische Federatie de intentie had Oekraïne te dwingen af te zien van verdere investeringen in alternatieve brandstof, wat ingaat tegen Russische economische belangen.

Concluderend stellen we dat in dit geval de soevereiniteit naar alle waarschijnlijkheid is geschonden op grond van een inbreuk op de territoriale integriteit. Mogelijk heeft er ook een onrechtmatige interventie plaatsgevonden.

48 Przemysław Roguski, 'Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach', in: Dennis Broeders en Bibi van den Berg (red.) *Governing Cyberspace*, 2020, 65–84.

49 Zie ook: Jake Styczynski and Nate Beach-Westmoreland, 'When the Lights Went Out', 2019; Tatiana Jancarkova and Kubo Macak, 'Cyber Law Toolkit: Scenario 03 - Cyber Operation against the Power Grid', CCDCoe, 2021. Zie: https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

50 Harriet Moynihan, 'Cyberspace: Sovereignty and Non-Intervention', *Just Security*, 2019. Zie de sectie over 'principles of non-intervention'. *Coercion* houdt dan onder meer in 'cyber-attacks on another state's critical infrastructure such as disrupting transport services, causing temporary black-outs, or restricting access to government websites'.

Cyberaanvallen op Georgië

Georgië was in oktober 2019 slachtoffer van een grootschalige cyberaanval. Van de aanval is niet bekend of materiële schade is ontstaan. De aanval betrof een defacement, een ongewenste aanpassing van websites, die in principe geen schade met zich meebrengt. Er is ook, voor zover bekend, geen sprake van functionele schade aan de cyberinfrastructuur. Desondanks had de actie significante gevolgen in Georgië: meer dan 2.000 overheids- en private websites waren (tijdelijk) ontoegankelijk waardoor veel Georgiërs hinder ondervonden. En dergelijk aanval op Georgië zou kunnen vallen in de laagste categorie zoals beschreven in de *Tallinn Manual*, namelijk onder het niveau van functionaliteitsverlies.

Naast de mogelijke schending van de territoriale integriteit door deze remote cyber-attack kan ook de politieke onafhankelijk van Georgië zijn ondermijnd. De cyberaanvallen ontsierden naast websites van private partijen en van non-gouvernementele organisaties ook sites van de centrale overheid en de rechterlijke macht, en er vielen uitzendingen van de staatsomroep stil.[51] De laatste categorie kan onderdeel uitmaken van de inherente overheidstaken. Daarnaast moet de aanval tot doel hebben die overheidstaak over te nemen of te verstoren, wat het geval is als de overheid via de getroffen websites publieke informatie communiceert.[52] Dit is echter lastig te beoordelen, omdat de Georgische overheid geen nadere toelichting op de effecten van de aanval heeft gegeven. Als de overheid een van haar taken niet meer had kunnen uitvoeren door deze cyberaanval, was er sprake geweest van soevereiniteitsschending op grond van een inbreuk op de politieke onafhankelijkheid.

Het domaine réservé van Georgië is met deze aanval geraakt. Onder het domaine réservé valt immers de bevoegdheid om wetgeving en overheidsbeleid vast te stellen dat ook het verkeer van private partijen reguleert.[53] De interventie is onrechtmatig als de schending van het domaine réservé op een dwingende wijze is verlopen.[54] Of dat in de Georgië-casus van toepassing is, is moeilijk te achterhalen. Rusland ontkent dit in ieder geval: 'Russia did not plan, and is not planning to, interfere in Georgia's internal affairs in any way.'[55]

Al met al zou de Georgische soevereiniteit kunnen zijn geschonden. De territoriale integriteit is aangetast maar vermoedelijk niet geschonden omdat er geen fysieke of functionele schade ontstond. Wel is het mogelijk dat de politieke onafhankelijkheid is geschonden, omdat een onrechtmatige bemoeienis met de inherente overheidsfuncties heeft plaatsgevonden. En hoewel het domaine réservé wel is aangetast, is een schending van het interventieverbod niet te bewijzen.

Beïnvloeding van de Amerikaanse presidentsverkiezingen

In de aanloop naar de presidentsverkiezingen van 2016 zijn computers gehackt en zijn de gestolen data gelekt, maar bovenal zijn sociale-mediaplatforms gebruikt om de maatschappij te ontwrichten, te polariseren en twijfel te zaaien bij de Amerikaanse kiezers.

Los van het binnendringen in de computers van de Democratische Partij, is het beïnvloeden van de Amerikaanse verkiezingen via sociale media primair een 'remote' soft-cyberoperatie die het territorium niet schendt. Bij gebrek aan fysieke of functionele schade maakt de beïnvloeding van de Amerikaanse verkiezingen daarom geen inbreuk op de territoriale integriteit. Omdat verkiezingen een inherente overheidsfunctie zijn, kan het bemoeilijken hiervan wel in strijd zijn met het beginsel van politieke onafhankelijkheid.

51 UK Government, 'UK Condemns Russia's GRU over Georgia Cyber-Attacks', 2020. Zie: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

52 Denk aan overheidscommunicatie over of crisismanagement tijdens Covid-19. Zie: Marko Milanovic en Michael N. Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic', in: *Journal of National Security Law & Policy* 11 (2020) 255.

53 Ziegler, 'Domaine Réservé', Bullet 2.

54 *Tallinn Manual 2.0*, Commentaar bij Rule 66, para 21; zie ook Ministerie van Buitenlandse Zaken, 'Letter to the President of the House of Representatives on the International Legal Order in Cyberspace – Appendix: International Law in Cyberspace', 5 juli 2019, 3.

55 Margarita Antidze en Jack Stubbs, 'Georgia, Backed by U.S. and Britain, Blames Russia for "paralyzing" Cyber Attack', *Reuters*, 2020. Zie: https://www.reuters.com/article/us-georgia-cyber-idUSKBN20E1W3.

FOTO MCD, VALERIE KUYPERS

Ook in cyberspace is het de taak van de krijgsmacht om de internationale rechtsorde en andere vitale belangen te beschermen. Voor de marechaussee is er bijvoorbeeld een rol in rechtshandhaving

De Russische beïnvloeding raakt een bevoegdheid uit het domaine réservé. Verkiezingen organiseren is een inherente overheidstaak, maar hoe een staat zijn verkiezingen regelt, is een onderdeel van zijn rechtsmacht, en daarmee het domaine réservé voor zover dit niet is ingeperkt.[56] De vraag is echter of de Russische acties coercive waren. Hier is geen eensluidend antwoord op te geven. De Russische intentie om de acties op een weloverwogen manier uit te voeren, is hoogstwaarschijnlijk aanwezig,[57] maar of Rusland het doel had het Amerikaanse beleid te veranderen op een manier die de Amerikanen niet zelf hebben gewild, blijft de vraag. Mogelijk is er geen dwang toegepast bij de beïnvloeding, maar de beïnvloeding via de socialemediaplatforms was wel manipulatief. Doordat Russische agenten gebruik maakten van onbewuste wijze van beïnvloeding (middels heuristieken) en zich voordoen als Amerikanen,[58] zijn de onafhankelijke keuzes en vrije wil van de kiezer ondermijnd, waardoor een zekere mate van dwang niet te ontzeggen is.

De conclusie is dat op basis van de hier gepresenteerde data de territoriale integriteit niet geschonden is, maar dat de soevereiniteit

56 Zo heeft in de EU iedere burger actief en passief kiesrecht bij de gemeenteraadsverkiezingen in de lidstaat van verblijf, ex. artikel 40 van het Handvest van de Grondrechten van de Europese Unie (2012/C 326/02).

57 Thomas Paterson en Lauren Hanley, 'Political Warfare in the Digital Age: Cyber Subversion, Information Operations and "Deep Fakes"', in: *Australian Journal of International Affairs* 74 (2020) (4) 443.

58 United States Senate Committee on Intelligence, 'Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media', vol. 2, 2019, 30.

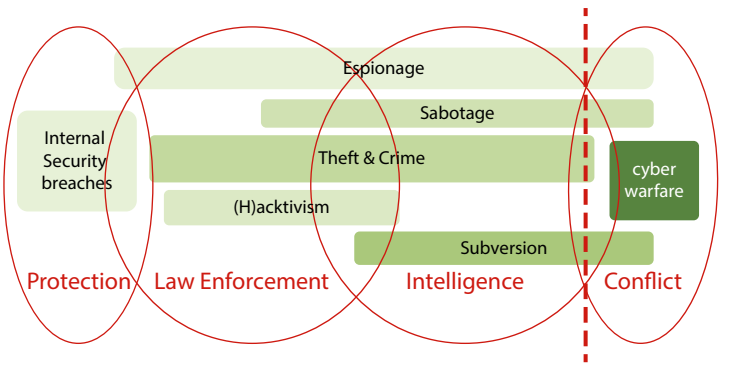
mogelijk wel geschonden is door een inbreuk op de politieke onafhankelijkheid door de bemoeienis met de verkiezingen, wat een inherente overheidstaak is. Of de inmenging ook een interventie heeft opgeleverd is lastig aan te tonen.

Reflectie op de rol van de krijgsmacht

Veel hedendaagse conflicten vinden plaats in de gray zone. Dit zijn grensoverschrijdende assertieve activiteiten onder het niveau van geweld. Uit de besproken casus komt naar voren dat, ondanks de onzekerheid over 'hoe' het internationale recht op cyberspace toepasbaar is, cyberoperaties al snel het soevereiniteitsbeginsel en/of het non-interventiebeginsel schenden.

Mede als gevolg van de onzekerheid en interpretatieverschillen ontstaat er een tweedeling tussen staten die de gray zone daardoor als een kans zien, en staten die zich geremd voelen om op te treden. De activiteiten in de gray zone vertroebelen nog verder omdat bij veel van deze remote cyber-attacks juist militaire cybereenheden of inlichtingendiensten opererend via cyberspace een prominente rol spelen, zoals de Russische GRU[59] of het Amerikaanse NSA/Cyber Command.[60]

Hoewel er een internationaalrechtelijk juridisch kader is, blijkt dat toepassing ervan op cyberacties in de gray zone lastig is. Feit is wel dat actoren actief zijn in de gray zone, ook tegen Nederland. De vraag is vervolgens welke rol de Nederlandse krijgsmacht heeft in de gray zone. Cyberspace lijkt ver weg te staan van de traditionele taak van de krijgsmacht: het verdedigen van het Koninkrijk. Is de krijgsmacht daarmee uitgespeeld? Nee, zeker niet! Ook in cyberspace is het de taak van de krijgsmacht om de internationale rechtsorde en andere vitale belangen te beschermen en waar mogelijk te bevorderen. Paul Ducheine c.s. onderkennen hierbij enkele rollen (of paradigma's) voor de krijgsmacht in cyberspace;[61] een beschermingstaak gericht op eigen (defensie-)ICT-infrastructuur; rechtshandhaving door de marechaussee, een inlichtingen- en veiligheidsrol van de



Figuur 3 Cyber Security Paradigms[63]

Militaire Inlichtingen- en Veiligheidsdienst en een conflict-gerelateerde rol van het Defensie Cybercommando (DCC).[62]

Het model in figuur 3 geeft vier paradigma's van staatsoptreden weer. Ieder paradigma vertegenwoordigt een institutioneel raamwerk waarbinnen de staat kan optreden, op basis van een vigerend rechtsregime.[64] Het paradigma conflict geeft de militaire operaties in cyberspace weer, zowel oorlogvoering als de inzet van de krijgsmacht voor stabilisatie- of vredesmissies in cyberspace.[65]

De paradigma's maken niet specifiek onderscheid naar inzet boven of onder het niveau van geweld, dan wel nationale of internationale

59 GRU (Glavnoje Razvedyvatel'noje Upravlenije) is de Russische inlichtingendienst van de Generale Staf van Defensie.

60 NSA (National Security Agency) is de Amerikaanse inlichtingendienst van het ministerie van Defensie, een agentschap gecoloceerd met en onder dezelfde leiding als het U.S. Cyber Command.

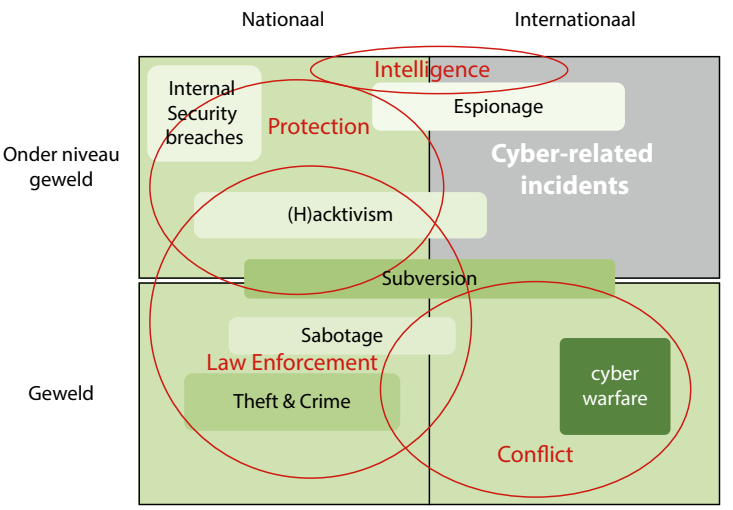
61 Paul A.L. Ducheine, 'Defensie in het Digitale Domein', in: *Militaire Spectator* 186 (2017) (4) 152–168; Paul A.L. Ducheine en Peter B.M.J. Pijpers, 'The Notion of Cyber Operations', in: Nicholas Tsagourias en Russell Buchan (red.), *Research Handbook on International Law and Cyberspace (Forthcoming)*, 2nd ed. (Edward Elgar, 2021).

62 De beschermende taak bij defensie ligt primair in handen van onder meer het Defensie Cyber Security Centre (DCSC). De indeling is schematisch, in de praktijk werken veel eenheden samen binnen deze paradigma's zowel binnen als buiten het ministerie van Defensie. Zo werkt de MIVD met de Algemene Inlichtingen en Veiligheidsdienst samen in de Joint Sigint Cyber Unit.

63 Ducheine, 'Defensie in het Digitale Domein', 157.

64 Ducheine en Pijpers, 'The Notion of Cyber Operations', 12.

65 Op basis van een mandaat van de VN-Veiligheidsraad, (collectieve) zelfverdediging zoals verwoord in artikel 51 van het VN-Handvest en artikel V van het NAVO-verdrag, of op uitnodiging van een andere staat.



Figuur 4 Gray zone: internationale cyberoperaties onder het niveau van geweld

inzet. In figuur 4 zijn, op basis van de paradigma's, de tegenstellingen (nationaal/ internationaal en boven/onder niveau van geweld) vereenvoudigd weergegeven, waarbij de gray zone inzichtelijk is gemaakt: het gebied van internationale cyberoperaties onder het niveau van geweld.[66]

In dit grijze kwadrant - waar het hierboven gepresenteerde juridische kader zich ook op richt - is de rol van de Nederlandse krijgsmacht, buiten activiteiten op basis van de Wet op de Inlichtingen en Veiligheidsdiensten (WIV) uit 2017, minimaal. Dit is echter exact de ruimte waar de Amerikaanse persistent engagement en de meeste cyberactiviteiten, inclusief de hiervoor beschreven casussen, plaatsvinden.

Wat betekent dit voor de Nederlandse krijgsmacht? De staat kan niet afzijdig blijven in de gray zone, niet in de laatste plaats omdat Nederland dagelijks doelwit is van cyberaanvallen vanuit het buitenland,[67] maar een pro-actievere houding levert een dilemma op. Wie gaat handelen en onder welk mandaat?

Kijkend naar de krijgsmacht heeft Nederland het DCC dat is voorbestemd om op te treden in cyberspace tijdens een conflict ter verdediging van, of om op te treden buiten, onze landsgrenzen: dit op basis van zelfverdediging, toestemming van het getroffen land, of een internationaal mandaat van de VN-Veiligheidsraad. De genoemde rechtsbases autoriseren echter geen optreden van het DCC in de gray zone. Optreden van de krijgsmacht buiten de landsgrenzen, onder het niveau van geweld is slechts beperkt mogelijk, en staat vaak op gespannen voet met het internationaal recht. Namens Nederland zou het DCC kunnen ondersteunen bij een (niet-gewelddadige) tegenmaatregel, na een eerder geweldgebruik van een andere staat, of zich beroepen op een *plea of necessity*,[68] waarbij het gaat om een rechtvaardigingsgrond van handelen dat in beginsel in strijd is met het internationaal recht. Ook zou het DCC kunnen optreden op basis van een nationaal mandaat voor speciale operaties,[69] maar dat vormt geen rechtsbasis onder internationaal recht.

Daarnaast is het verruimen van de bevoegdheden van de inlichtingen- en veiligheidsdiensten een optie. Zij kunnen nu na een lastgeving en binnen hun taakstelling op grondslag van de WIV grensoverschrijdende inlichtingenoperaties uitvoeren onder het niveau van geweld, ook in cyberspace.[70] De taak verruimen naar *alle* cyberoperaties – naar Amerikaans persistent engagement-model[71] – is op zijn minst controversieel omdat we daarmee

66 Grensoverschrijdende acties, onder het niveau van geweld, handelend conform de beginselen van het internationale recht, zoals een diplomatiek protest, zijn toegestaan en daarmee niet 'grijs'.

67 NCTV, 'Cybersecuritybeeld Nederland', 2020, 7-9.

68 Schmitt, *Tallinn Manual 2.0*, Rule 26, 135-142.

69 Paul A.L. Ducheine, Kraesten L. Arnold, en Peter B.M.J. Pijpers, 'Decision-Making and Parliamentary Control for International Miiltary Cyber Operations by The Netherlands Armed Forces', in: Rogier Bartels et al (red.), *Liber Amicorum*, 2020, 76-79. De inzet van de krijgsmacht voor operationele taken die passen binnen de eigen grondwettelijke taak van de krijgsmacht vindt plaats binnen een kader van voorwaarden in lijn met het geldende internationale recht. Het niet schenden van de soevereiniteit is een van die voorwaarden.

70 Het onderscheid tussen inlichtingenoperaties en (offensieve) cyberoperaties is lastig te maken, zie ook Herbert S. Lin en Amy Zegart (red.), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press, 2019) 6.

71 De VS heeft een separate wet voor inlichtingenoperaties (Executive Order 12333 United States Intelligence Activities van 4 december 1981), en voor cyberoperaties (Sectie 1642 van de John S. McCain National Defense Authorisation Act van 2019). Zie ook: Chesney, 'The Domestic Legal Framework for US Military Cyber Operations'.

de beginselen van soevereiniteit en non-interventie schenden.

Tot slot zou de krijgsmacht, en meer in het bijzonder de marechaussee, gebruik kunnen maken van nationale wetgeving,[72] en extra-territoriale rechtsopsporingsbevoegdheden (onder het *law enforcement*-paradigma) gebruiken om dreigingen in de gray zone tegen te gaan. Dit is echter primair een politietaak, waarbij de krijgsmacht slechts ondersteunt.

Conclusie

Dit artikel schetste een juridisch kader voor internationale digitale acties van statelijke actoren buiten de context van geweld en conflict. Hoewel in die situatie het geweldsverbod en het humanitair oorlogsrecht geen rol spelen, betekent dit niet dat er wetteloosheid heerst. De internationaalrechtelijke regels voor soevereiniteit en non-interventie regelen, ook in cyberspace, het gedrag van staten in een internationale context. Het is staten niet toegestaan de territoriale integriteit of de politieke onafhankelijkheid van andere staten te schenden (soevereiniteit). Daarnaast is een interventie niet geoorloofd wanneer die een dwingend karakter heeft, wat inhoudt dat er een intentie is om het regeringsbeleid te veranderen op een wijze waar de andere staat zelf niet voor zou kiezen.

Internationaal optreden onder het niveau van geweld in cyberspace is dus juridisch begrensd, maar niet verboden zolang de remote cyber-attacks het internationale recht niet schenden. Het vraagstuk hoe hierin op te treden, levert voor de Nederlandse krijgsmacht een duivels dilemma op.

Het is kiezen tussen twee kwaden. Ofwel Nederland gaat acteren in de gray zone en voert grensoverschrijdende activiteiten uit onder het niveau van geweld. Het verruimt daarmee de bevoegdheid van het DCC of de inlichtingendiensten, door niet alleen inlichtingenactiviteiten, maar alle activiteiten in cyberspace uit te voeren naar analogie van het Amerikaanse

De staat kan niet afzijdig blijven in de gray zone, niet in de laatste plaats omdat Nederland dagelijks doelwit is van cyberaanvallen vanuit het buitenland

persistent engagement. Hoewel menig land, naast de VS ook Rusland en China, al geruime tijd aanwezig is in deze gray zone, rekt Nederland hier de nationale taken voor de krijgsmacht op, waardoor deze op gespannen voet komen te staan met het internationaal recht, en de grens daarvan wellicht overschrijden.

Of Nederland, en dus zijn krijgsmacht, blijft weg uit de gray zone. Dit zou logischer zijn; met optreden in de gray zone schendt Nederland immers een van zijn eigen vitale belangen, namelijk een goed functionerende internationale rechtsorde.[73] Nadeel hiervan is dat anderen wel in de gray zone optreden, en dat Nederland ondanks een bewuste afzijdigheid wel een potentieel doelwit is. Wie gaat Nederland dan verdedigen, als de krijgsmacht niet aan zet is?

Hoe dan ook, niets doen is geen optie. ■

72 Denk daarbij aan de wet Computer Criminaliteit III, Kamerstukken II, 2015-2016, 34 372, nr. 3.

73 NCTV, 'Nationale Veiligheid Strategie 2019', 2019.