Internationaal Cybersecuritybeleid

Literatuurstudie

In opdracht van IOB

Keri van Douwen & Nour Gjaltema

februari 2021

Vrije Universiteit Amsterdam

Deze literatuurstudie is opgesteld door Keri van Douwen en Nour Gjaltema in opdracht van, en in nauwe samenwerking met, IOB. De opvattingen, bevindingen en conclusies zoals verwoord in dit rapport vallen onder de verantwoordelijkheid van de auteurs.

Samenvatting

Dit rapport beschrijft, op basis van (voornamelijk academische) literatuur, recente ontwikkelingen omtrent het cyberdomein en de dreigingen vanuit statelijke en daaraan gelieerde actoren, en geeft een overzicht van aanbevelingen die worden gedaan in de literatuur.

De dreiging
Een groot aantal staten, inclusief Nederland, identificeert cybersecurity als een van de belangrijkste aandachtspunten voor de nationale veiligheid. Het *Cybersecuritybeeld Nederland* spreekt dan ook van permanente digitale dreiging. De afgelopen vijf jaar is politieke oorlogsvoering verder genormaliseerd. Het cyberdomein biedt staten nieuwe mogelijkheden om handelingen uit te voeren die in het grijze gebied tussen 'oorlog' en 'vrede' vallen. Rusland maakt bijvoorbeeld actief gebruik van het cyberdomein om chaos en verdeling te zaaien binnen democratieën en internationale organisaties zoals de EU. Ook Nederland is het slachtoffer geweest van Russische cyberoperaties. Waar enkele jaren geleden nog werd gesproken van een zestal staten die over offensieve cybercapaciteiten zouden beschikken, stellen experts dat er inmiddels 100 staten zijn die een cyberaanval kunnen lanceren. Als gevolg van technologische ontwikkelingen worden cybercapaciteiten steeds goedkoper. Ook is er sprake van een verwevenheid tussen statelijke actoren en criminele netwerken en zouden staten zogenaamde '*cyber proxies*' inzetten. Dit compliceert het accuraat in kaart brengen van de dreiging die uitgaat van statelijke actoren. Daarnaast heerst er in de internationale gemeenschap onenigheid over wat *digitale dreiging* precies inhoudt. In het Westen wordt gesproken over *cybersecurity*, Rusland en China refereren naar *information security.* In China en Rusland wordt, in tegenstelling tot het Westen, vrije toegang tot informatie gezien als potentieel nationaal veiligheidsrisico. Experts spreken als gevolg van de verslechterende relaties tussen de VS en China en Rusland ook wel over een mogelijk einde van het mondiale internet.

De ontwikkelingen van de afgelopen jaren hebben ook een negatieve impact op de online mensenrechten. Door surveillance technieken lopen burgers wereldwijd het risico om slachtoffer te worden van mensenrechtenschendingen. Inspanningen om handel in dit soort technieken te reguleren zijn tot nog toe niet succesvol gebleken. Ook in de Europese Unie is een trend zichtbaar waarin het beschermen van de waarheid in toenemende mate van belang wordt geacht. Door sommige staten wordt de bescherming tegen valse informatie als een legitieme reden gezien om de vrijheid van meningsuiting aan banden te leggen.

Cybersecurity en internationaal recht
Hoewel Nederland nadrukkelijk stelt dat het internationaal recht van toepassing is op activiteiten die zich afspelen in het cyberdomein, is er nog veel onduidelijk. Zo bestaat er bijvoorbeeld geen duidelijke definitie van 'cybergeweld', wat het lastig maakt om vast te stellen wanneer staten mogen reageren op een cyberoperatie vanuit zelfverdediging. Alle staten hebben zich echter gecommitteerd aan de toepassing van het VN-Handvest op activiteiten die plaatsvinden in het cyberdomein. Dit betekent dat het non-interventie principe en het verbod op het gebruik van geweld moeten worden nageleefd. Het is echter lastig om vast te stellen welke cyberoperaties deze principes schenden. In respons op aanvallen hebben staten de mogelijkheid om individueel of in collectief verband retorsie-maatregelen te nemen (zoals het opleggen van sancties), en om individueel tegenmaatregelen in te zetten.

Zowel academici als staten zijn het erover eens dat mensenrechten *offline* en *online* gelden. Er bestaat echter onenigheid over de juiste toepassing van mensenrechtenverdragen in het cyberdomein. Doordat het niet mogelijk lijkt om op internationaal niveau consensus te bereiken, zijn

multilaterale en regionale mensenrechtenverdragen in belang toegenomen. Op internationaal niveau zijn staten het voornamelijk oneens over de verhouding tussen mensenrechten en soevereiniteit, en de extraterritoriale toepassing van mensenrechten. Met name China en Rusland spreken over 'internetsoevereiniteit'. Zij stellen dat staten het recht hebben om complete controle uit te oefenen over het cyberdomein binnen hun landsgrenzen. Nederland en andere westerse staten leggen de nadruk op het bewerkstellen van een open, vrij en veilig internet.

Internationaal cybersecuritybeleid en aanbevelingen
Middels de Europese Unie, de NAVO, de VN en de OVSE hebben staten gewerkt aan het opstellen van internationaal cybersecuritybeleid. In 2017 nam de EU een beleidsraamwerk aan wat het mogelijk maakt om in collectief EU-verband te reageren op vijandige cyberactiviteiten: de *cyber diplomacy toolbox.* In juli 2020 zijn voor het eerst sancties opgelegd tegen zes personen en drie entiteiten die verantwoordelijk worden geacht voor, of betrokken waren bij, verschillende cyberoperaties. Op die manier kan het sanctieregime indirect ingezet worden tegen statelijke actoren, maar dit blijft een ingewikkelde politieke keuze. Academici stellen daarnaast dat het onvoldoende duidelijk is hoe EU-cyberdiplomatie in de praktijk afschrikkend zou kunnen werken. Ook wordt beargumenteerd dat het oprichten van een nieuwe internationale organisatie nodig is om attributie geloofwaardiger te maken, staten daadwerkelijk verantwoordelijk te houden voor hun vijandige cyberoperaties, en om het inzetten van toekomstige operaties tegen te houden. In de literatuur worden in ieder geval de volgende aanbevelingen voor de EU gedaan:

- Integreer de cyber diplomacy toolbox in het Geïntegreerde Politieke Crisis Respons-mechanisme en andere EU-crisis management mechanismes;
- Stimuleer het continu delen van informatie tussen lidstaten;
- Combineer beperkende maatregelen (sancties) met andere instrumenten;
- Definieer *red lines* en niveaus van escalatiegereedheid per lidstaat.

De NAVO erkende het cyberdomein officieel als oorlogsdomein in 2016 en maakte in 2014 kenbaar dat het collectieve verdedigingsmechanisme van de Alliantie ook in het cyberdomein geldig is. Academici stellen dat het bondgenootschap een relevante, sterke militaire alliantie is die bewezen heeft in staat te zijn om te vernieuwen en mee te gaan met technologische ontwikkelingen. Daartegenover wordt ook gesteld dat, ondanks de belangrijke stappen die al zijn gezet, de NAVO nog onvoldoende in staat is om de toenemende en veranderende cyberdreiging het hoofd te bieden. Om die reden worden in ieder geval de volgende aanbevelingen gedaan:

- Creëer gedeelde *situational awareness* door middel van transparantie en het openen van de juiste kanalen voor het delen van (geclassificeerde) informatie tussen lidstaten en partnerorganisaties;
- Ontwikkel een beleidsstrategie waar een duidelijke bevelstructuur in is aangebracht en eenduidige definities in zijn opgenomen.

In 2004 werd door de VN de eerste *Group of Governmental Experts* (GGE) opgericht, bedoeld om verantwoord staatsgedrag in het cyberdomein te bevorderen. Sindsdien zijn er zes werkgroepen opgericht. In 2018 werd door de VN ook de Open-Ended Working Group (OEWG) opgericht. Het oprichten van deze verschillende groepen die beide werken aan het ontwikkelen van normen en regels voor het cyberdomein is niet alleen het gevolg van de tweedeling tussen staten die focussen op *cybersecurity* en staten die spreken van *information security*, maar heeft ook gezorgd voor verdere politisering en uiteendrijvende wereldbeelden. Dit draagt niet bij aan de mogelijkheid om de internationale rechtsorde in het cyberdomein te bevorderen. Zowel academici als staten hebben

kritiek geuit over de werkgroepen die door de VN zijn opgericht. In oktober 2020 heeft een groep van 40 staten, inclusief de EU-lidstaten, een voorstel gedaan om een *Programme of Action* aan te nemen, de GGE en de OEWG te beëindigen en in plaats daarvan een permanent VN-forum op te richten. Academici stellen dat het belangrijk is om gebruik te maken van het multi-stakeholderprincipe en ook regionale organisaties bij het normontwikkelingsproces te betrekken.

Op regionaal niveau heeft de EU online mensenrechten geïntegreerd in de EU-cybersecurity strategie. Pogingen binnen de VN om internationaal cyber-mensenrechtenbeleid te creëren hebben niet tot substantiële afspraken geleid. Ter bevordering van mensenrechten in het cyberdomein heeft Nederland de oprichting van de *Freedom Online Coalition* geïnitieerd. Dit soort internationale organisaties en fora, zoals de *Global Commission on the Stability of Cyber Space*, bieden staten de mogelijkheid om cybergedragsnormen te formuleren en verspreiden. Ook private bedrijven zoals Microsoft en ngo's zoals het Internationaal Comité van het Rode Kruis hebben cybergedragsnormen geformuleerd.

Staten hebben zich de afgelopen jaren ook ingezet om de cybercapaciteit van minder geavanceerde staten te vergroten, ten behoeve van de internationale veiligheid. Op deze manier kunnen staten ook cybergedragsnormen verspreiden. Academici benadrukken echter dat capaciteitsprojecten ook zouden kunnen leiden tot een verdere onderdrukking van online mensenrechten, in het bijzonder wanneer autoritaire staten middels capaciteitsopbouw hun positie in het cyberdomein kunnen versterken. Uit de literatuur blijkt daarnaast dat er een gebrek aan coördinatie tussen de verschillende capaciteitsprojecten bestaat. Hierdoor ontvangen sommige staten veel steun en anderen helemaal niet. Om de capaciteitsopbouw te verbeteren worden in de bestudeerde literatuur onder andere de volgende aanbevelingen gedaan:

- Stel per project een concreet beleidsplan op waarbij de focus op mensenrechten in elk onderdeel wordt geïntegreerd;
- Stem projecten af op de specifieke lokale situatie;
- Maak gebruik van het multi-stakeholder principe, dit kan bijdragen aan het creëren van lokale draagkracht en het bevorderen van online mensenrechten.

Academici en mensenrechtenorganisaties stellen dat er te weinig aandacht is voor de impact van cybersecuritybeleid op (online) mensenrechten. Dit zou het gevolg zijn van een gebrek aan samenwerking tussen mensenrechtenexperts en beleidsmakers. Om die reden wordt gesteld dat private actoren, zoals bedrijven en internetgebruikers, en mensenrechtenexperts in de toekomst betrokken zouden moeten worden bij het opstellen van *algemeen* internationaal cybersecuritybeleid. Een onafhankelijke evaluatie van de *Freedom Online Coalition,* opgericht ten behoeve van het beschermen van internetvrijheid, is ook kritisch op het beleid van westerse staten zoals de Verenigde Staten en het Verenigd Koninkrijk. Zij zouden de FOC gebruiken om eventuele kritiek op mensenrechtenschendingen binnen hun eigen nationale cyberdomein onderuit te halen. Over het internationale cybersecuritybeleid van de VS wordt door meer academici zeer kritisch geschreven. Zo zou er bij het opstellen en uitvoeren van het *Defend Forward* beleid onvoldoende rekening gehouden worden met het risico op escalatie in het cyberdomein. Daarbij wordt door enkele academici beargumenteerd dat het huidige Amerikaanse beleid onverenigbaar is met het idee van een open en vrij internet. Academici zijn wel positief over de Amerikaanse '*whole-of-government*' strategie, waarbij gebruik wordt gemaakt van de unieke expertise, middelen en autoriteiten van elk ministerie, en van elk middel, of elke combinatie van middelen, die het meest effectief is om een

bepaalde dreiging te verstoren. Ook het belang van coördinatie met de private sector wordt hierbij benadrukt.

Over het algemeen worden de verschillende activiteiten van BZ, de focus op publieke attributie, het herhaaldelijk uitspreken van de Nederlandse interpretatie van internationaal recht en de toepassing van mensenrechten in het cyberdomein en de steun aan verschillende internationale organisaties, positief beoordeeld. Sommige academici stellen zelfs dat Nederland in vergelijking met andere staten vooroploopt wat betreft het implementeren van cybergedragsnormen en het uitleggen van de toepasselijkheid van het internationaal recht. Desalniettemin zou een bijkomend negatief effect kunnen zijn dat de posities van staten hierdoor verder uiteen te komen liggen. De in de literatuur waargenomen scheidslijn bevindt zich in deze voornamelijk tussen westerse landen enerzijds en niet-westerse, meer autocratische landen – als China en Rusland – anderzijds. De Nederlandse positionering op het gebied van normstelling en internationaal recht zou ertoe kunnen leiden dat het uiteindelijk alleen maar lastiger wordt om overeenkomsten te bereiken met niet-gelijkgestemde staten.

Afkortingen

AI	Artificial intelligence
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
ASEAN	Association of Southeast Asian Nations
BZ	Ministerie van Buitenlandse Zaken
CBM	Confidence building measure
CDPF	Cyber Defense Policy Framework
DIMEFIL	Diplomatic, Information, Military, Economic, Financial, Intelligence, Law enforcement
EHRM	Europese Hof voor de Rechten van de Mens
EU	Europese Unie
FBI	Federal Bureau of Investigation
FOC	Freedom Online Coalition
GCHQ	Government Communications Headquarters
GCSC	Global Commission on the Stability of Cyberspace
GFCE	Global Forum on Cyber Expertise
GGE	Group of Governmental Experts
ICT	Informatie- en communicatietechnologie
ICRC	Internationaal Comité van het Rode Kruis
IGF	Internet Governance Forum
IOB	Directie Internationaal Onderzoek en Beleidsevaluatie
IVBPR	Internationaal Verdrag inzake Burgerrechten en Politieke Rechten
Ngo	Niet-gouvernementele organisatie
NAVO	Noord-Atlantische Verdragsorganisatie
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NSA	National Security Agency
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
OEWG	Open-Ended Working Group
OPCW	Organisatie voor het Verbod op Chemische Wapens
OVSE	Organisatie voor Veiligheid en Samenwerking in Europa
RvE	Raad van Europa
SCO	Shanghai Cooperation Organisation
UNHRC	Mensenrechtenraad
UVRM	Universele Verklaring van de Rechten van de Mens
VK	Verenigd Koninkrijk
VN	Verenigde Naties
VS	Verenigde Staten

Termen

Algorithmic surveillance: geautomatiseerde surveillance techniek waarmee op grote schaal data over personen wordt verzameld en geanalyseerd.[1]

Attributie: het identificeren van de dader van een cyberaanval.[2]

Beïnvloeding: het inzetten van middelen voor cognitieve doeleinden die het gedrag van een doelgroep bevorderen of veranderen.[3]

Capaciteitsopbouw: het helpen opbouwen en beveiligingen van cyber infrastructuur en beleid in minder ontwikkelende landen (qua cybercapaciteit). Dit kan gebeuren middels financiële, materiele en educatieve middelen en institutionele hervormingen.[4]

Computer network attacks: het compromitteren of manipuleren van computersystemen. Bijvoorbeeld: een systeem uitschakelen, gegevens wijzigen, bronnen misbruiken, en elke andere actie die de integriteit of beschikbaarheid van een systeem in gevaar brengt.[5]

Confidence-building measures: maatregelen gericht op het voorspelbaarder maken van het cyberdomein en het voorkomen van misverstanden.[6]

Cyberaanval: een cyberoperatie, offensief of defensief, waarvan redelijkerwijs kan worden verwacht dat deze leidt tot letsel of dood van individuen, schade of vernietiging aan objecten,[7] of schade aan individuen (bijvoorbeeld reputatie- of financiële schade).

Cyberdefensie: alle acties die worden uitgevoerd binnen het cyberdomein om specifieke bedreigingen te verslaan die inbreuk hebben gemaakt op *cybersecurity*-maatregelen of deze dreigen te schenden en om het systeem te herstellen.[8]

Cyberdiplomacy: het inzetten van diplomatieke middelen om nationale belangen in het cyberdomein veilig te stellen.[9]

Cyberdomein: conglomeraat van ICT-middelen en -diensten en entiteiten die digitaal verbonden (kunnen) zijn. Het domein omvat zowel permanente als tijdelijke of plaatselijke verbindingen, evenals de gegevens (o.a. data, programmacode, informatie) die zich in dit domein bevinden, waarbij geen geografische beperkingen zijn gesteld.[10]

Cybergedragsnormen: internationaal of regionaal afgesproken normen die uiteenzetten hoe staten zich dienen te gedragen in het cyberdomein.

Cyberoperatie: elke (kwaadwillige) cyberactiviteit, offensief of defensief.

Cyberproxy: tussenpersoon die een offensieve cyberoperatie uitvoert, of er direct aan bijdraagt, die bewust mogelijk wordt gemaakt door een begunstigde.[11]

---

[1] Margulies (2016), *Surveillance by Algorithm*, p. 1056, Bernal (2016), *Data Gathering, Surveillance and Human Rights*, p. 249.
[2] Eggenschwiler & Silomon (2018), *Challenges and Opportunities*, p. 14.
[3] Duncan Hollis in Sander (2019), *The Sound of Silence*, p. 7.
[4] Pijnenburg-Muller (2015), *Cyber Security Capacity Building*, p. 5.
[5] Winkler & Treu Gomes (2017), *Advanced Persistent Security*, p. 16.
[6] OSCE website. https://www.osce.org/secretariat/cyber-ict-security#:~:text=The%20OSCE%20tackles%20various%20cyber,from%20the%20use%20of%20ICTs.
[7] Schmitt (2017), *Tallinn Manual 2.0*, p. 415.
[8] DOD Dictionary of Military and Associated Terms (June 2020). Beschikbaar via: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
[9] Barrinha & Renard (2020), *The Emergence of Cyber Diplomacy*.
[10] De Nationale Cybersecurity Strategie NCSS, p. 7. Beschikbaar via: https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2.
[11] Maurer (2018), *Cyber Mercenaries*, p. xi.

Cybersecurity: alle maatregelen die worden genomen om het cyberdomein te beschermen tegen ongeoorloofde toegang tot, exploitatie van of schade aan computers, elektronische communicatiesystemen en andere informatietechnologie, evenals de data die daarin ligt opgeslagen.[12]

Cyberspionage: elke handeling die in het geheim of onder valse voorwendselen wordt ondernomen, waarbij gebruik wordt gemaakt van cybercapaciteiten om informatie te (proberen te) verzamelen.[13]

Deep fakes: audio- of videofragmenten die op zo'n geavanceerde manier zijn bewerkt dat het lijkt alsof 'echte' mensen dingen doen of zeggen, die ze in werkelijkheid nooit hebben gedaan of gezegd.[14]

Human security: beleidsbenadering die het vertrouwen en de veiligheid van burgers centraal stelt wanneer de noodzaak zich voordoet om cybermaatregelen en wetten die hun mensenrechten zouden kunnen schenden, aan te nemen.[15] Dit concept wordt ook wel gezien als de tegenhanger van *information security.*

Information security: beleidsbenadering gericht op het beschermen van data tegen ongeautoriseerd gebruik waarbij de nadruk ligt op het beschermen van soevereiniteit en de nationale veiligheid.[16] Dit concept wordt ook wel gezien als de tegenhanger van *human security*.

Internetsoevereiniteit: het recht op complete controle over het cyberdomein binnen staatsgrenzen (term geïntroduceerd door China).[17]

Multi-stakeholer model: beleidsmodel waarin de staat samenwerkt met actoren uit het bedrijfsleven en civiele organisaties bij het formuleren van beleid.[18]

New-Type Warfare: Russische afschrikkingsstrategie die ingezet wordt als verdedigingsmechanisme, bedoeld om eventuele (democratische/anti-Kremlin) revoluties af te weren (in het Russisch: voina novogo tipa).[19]

Online mensenrechten: reeds bestaande mensenrechten die worden toegepast in het cyberdomein. Daarbij kan men denken aan de vrijheid van meningsuiting en de vrijheid van vergadering.

Opinio juris: algemeen heersende opvatting in het (internationaal) recht.

Resilience: in het Nederlands letterlijk *veerkracht* of *elasticiteit.* Wordt vaak 'weerbaarheid' mee bedoeld, bijvoorbeeld in de zin dat een samenleving weerbaar is tegen buitenlandse desinformatiecampagnes.

Sabotage: het opzettelijk, zeer langdurig, aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten, mogelijk leidend tot vernietiging.[20]

Situational awareness: in het Nederlands letterlijk *omgevingsbewustzijn.* Verwijst naar de mate waarin

---

[12] DOD Dictionary of Military and Associated Terms (June 2020). Beschikbaar via: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

[13] Schmitt (2017), *Tallinn Manual 2.0*, p. 168.

[14] Chesney & Citron (2019), *Deep Fakes: A Looming Challenge*, p. 1758.

[15] Deibert (2018), *Toward a Human-Centric Approach*, p. 412, Schaake & Vermeulen (2016), *Towards a Values-Based European Foreign Policy*, p. 75.

[16] Hampson & Sulmeyer (eds) (2017), *Getting beyond Norms*, p. 15.

[17] Schmitt & Vihul (2017), *Sovereignty in Cyberspace*, p. 214.

[18] Tikk-Ringas (2016), *International Cyber Norms Dialogue*, p. 52, Eldem (2020), *The Governance of Turkey's Cyberspace*, p. 454.

[19] Thornton & Miron (2019), *Deterring Russian Cyber Warfare*, p. 258-259.

[20] NCTV (2018), *Cybersecuritybeeld Nederland,* p. 14.

een staat *subjectief* (cyber)dreiging ervaart:[21] staten die objectief gezien te maken hebben met een vergelijkbare dreiging, kunnen dit subjectief heel anders ervaren.

Spionage: het kopiëren of wegnemen van informatie door statelijke of daaraan gelieerde actoren.[22]

[21] Arts (2018), *Offense as the New Defense*, p. 6.
[22] NCTV (2018), *Cybersecuritybeeld Nederland*, p. 14.

Inhoudsopgave

Samenvatting 1
Afkortingen 5
Termen 6
1. Introductie 11
2. Methodologie 13
2.1. Literatuurstudie 13
2.2. Beperkingen van het onderzoek 14
2.3. Terminologie 15
3. Digitale dreiging 16
3.1. Belangrijke ontwikkelingen digitale dreiging 2015-2020 17
3.1.1. Online mensenrechten 27
3.2. Verwachte ontwikkelingen 2020-2025 30
4. Internationaal recht 34
Inleiding internationaal recht 34
4.1. Aanvallen 36
4.2. Respons op aanvallen 40
4.3. Online mensenrechten 42
5. Internationaal beleid 48
Inleiding internationaal beleid 49
5.1. Cybersecurity 49
5.1.1. Europese Unie 49
5.1.2. NAVO 52
5.1.3. VN en OVSE 53
5.2. Online mensenrechten 54
5.2.1. Verschillende beleidsmodellen 55
5.2.2. Human security versus information security 56
5.2.3. Europese Unie 57
5.2.4. Verenigde Naties 58
6. Verwachte ontwikkelingen rechtsregels, normen, beleid 59
Inleiding verwachte ontwikkelingen rechtsregels, normen, beleid 60
7. Lessen internationaal cybersecuritybeleid 65
Inleiding lessen internationaal cybersecuritybeleid 67
7.1. Diplomatieke inzet en financiële steun 67
7.1.1. Adequaat reageren 68

7.1.2. Bevorderen internationale rechtsorde in het cyberdomein 77
7.1.3. Capaciteitsopbouw 82
7.1.4. Bevorderen mensenrechten in het cyberdomein 87
7.2. Lessen internationale gemeenschap 89
Bibliografie 95
Academisch 95
Overheids-, organisatie- en juridische documenten 104
Non-academisch en blogs 107

1. Introductie

In dit rapport onderzoeken we, op basis van (voornamelijk academische) literatuur, recente ontwikkelingen omtrent het cyberdomein en de dreigingen vanuit statelijke en daaraan gelieerde actoren. Het rapport is geschreven op verzoek van de directie Internationaal Onderzoek en Beleidsevaluatie (IOB) met als doel bij te dragen aan het evaluatieonderzoek van het internationale cybersecuritybeleid van het ministerie van Buitenlandse Zaken.

Het rapport is gebaseerd op acht hoofdvragen en verdeeld in zeven hoofdstukken. In hoofdstuk 2 worden de gebruikte methodologie en de beperkingen van het onderzoek besproken, en cyber-terminologie geïntroduceerd. Aan het begin van de overige hoofdstukken is steeds een korte samenvatting toegevoegd. In hoofdstuk drie tot en met zeven wordt, steeds aan de hand van relevante literatuur, een antwoord geformuleerd op de volgende vragen:

Hoofdstuk 3:

- Wat zijn de belangrijkste ontwikkelingen in de afgelopen jaren op het gebied van de digitale dreiging van statelijke en daaraan gelieerde actoren, in het bijzonder richting Nederland?
- Hoe hangen deze dreigingen samen met ontwikkelingen omtrent mensenrechten in het cyberdomein?
- Wat zijn de verwachte ontwikkelingen op het gebied van de dreiging van statelijke en daaraan gelieerde actoren in de komende jaren?

Hoofdstuk 4:

- Hoe ziet het huidige internationaal recht eruit qua wat staten al dan niet mogen doen in het cyberdomein ten opzichte van andere staten?
- Hoe ziet het huidige internationaal recht eruit qua wat staten al dan niet mogen doen ten opzichte van mensenrechten in het digitale domein?

Hoofdstuk 5:

- Wat zijn de belangrijkste internationale ontwikkelingen in de afgelopen jaren op het gebied van internationaal cybersecuritybeleid gericht tegen de dreiging van statelijke en daaraan gelieerde actoren (voor zover relevant voor Nederland)?
- Hoe zien de belangrijkste huidige internationale beleidsmechanismen eruit?
- Wat zijn de belangrijkste internationale ontwikkelingen in de afgelopen jaren op het gebied van mensenrechten in het cyberdomein?

Hoofdstuk 6:

- Zijn er belangrijke verwachte internationale ontwikkelingen op het gebied van internationale rechtsregels, normen, en/of cybersecuritybeleid gericht op de cyberdreiging van staten die nu nog niet gelden maar wel in de komende 3 jaar verwacht worden, en zo ja, welke?

Hoofdstuk 7:

- Volgens de literatuur: a) wat gaat er goed, b) wat gaat er niet goed, en c) welke aanbevelingen worden er gedaan over het beleid en de activiteiten van het Nederlandse internationale cybersecuritybeleid?

- Volgens de literatuur: a) wat gaat er goed, b) wat gaat er niet goed, en c) welke aanbevelingen worden er gedaan over de internationale samenwerkingsverbanden?
- Volgens de literatuur: a) wat gaat er goed, b) wat gaat er niet goed, en c) welke aanbevelingen worden er gedaan over de organisaties en projecten die Nederland financieel ondersteunt?
- Volgens de literatuur: a) wat gaat er goed, b) wat gaat er niet goed, en c) welke aanbevelingen worden er gedaan over het internationaal cybersecuritybeleid gericht op het promoten van mensenrechten in het digitale domein?
- Welke lessen kunnen worden geleerd van wat andere individuele staten doen met hun internationale cybersecuritybeleid?

2. Methodologie

Deze literatuurstudie is een samenvatting en analyse van de beschikbare literatuur omtrent cybersecurity-vraagstukken. De studie is niet gericht op het meten van de impact van het Nederlandse internationale cybersecuritybeleid op de (inter)nationale veiligheid. Het is namelijk niet mogelijk om de huidige situatie te vergelijken met hoe de situatie zou zijn geweest zonder, of met andere, Nederlandse inspanningen in het cyberdomein. Daarnaast zijn een aantal van de Nederlandse doelen moeilijk te meten, en is er een gebrek aan betrouwbare, verifieerbare datasets en andere gegevens. Het doel van deze literatuurstudie is dan ook het schetsen van de belangrijkste ontwikkelingen in het cyberdomein van de afgelopen jaren, zowel qua digitale dreiging gericht tegen staten, als de respons van staten en internationale organisaties. Aangezien over de meeste thema's die in dit rapport worden besproken geen consensus bestaat, zijn tegenstrijdigheden onoverkoombaar. Deze reflecteren de mate waarin academici, evenals statelijke actoren, het oneens met elkaar zijn over de 'juiste' veiligheidsstrategie met betrekking tot het cyberdomein.

2.1. Literatuurstudie

Het literatuuronderzoek is zodanig afgebakend dat het alleen focust op Nederlandse *internationale* activiteiten die zijn gericht op het tegengaan van cyberdreiging vanuit statelijke en daaraan gelieerde actoren. Dit betekent dat de nationale aspecten van het Nederlandse cybersecuritybeleid, die onder de verantwoordelijkheid van andere ministeries vallen, niet zijn meegenomen in de studie. Daarbij moet als kanttekening worden geplaatst dat het internationale en het nationale beleid (deels) met elkaar verweven zijn.

Bij het verzamelen van literatuur is rekening gehouden met een brede interpretatie van *cybersecurity.* Een zoektocht naar relevante termen (o.a. *cybersecurity*, *hybrid threats*, *cyber attacks*, *deterrence, cyber strategy*, *influence)*, debatten (bijvoorbeeld *information security & human security, Tallinn Manual, GGE, OEWG, confidence-building measures*) en beleidspunten (*capacity building, online human rights)* heeft geleid tot een uitgebreide literatuurlijst. Tijdens dit proces is rekening gehouden met de bovengenoemde afbakening van het onderzoek.

Bronnen

De literatuurstudie is gebaseerd op academische artikelen van cyberexperts, onderzoeksrapporten, ngo-rapporten en overheidspublicaties. De voorkeur is gegeven aan artikelen die zijn gepubliceerd in academische tijdschriften, rapporten van vooraanstaande onderzoeksinstituten en contributies van relevante cyberconferenties. Aangezien het cybersecuritydomein onderhevig is aan snelle technologische ontwikkelingen en veranderende theorieën en strategieën, hebben we de voorkeur gegeven aan de meeste recent gepubliceerde bronnen. In het rapport wordt ook gerefereerd naar rapporten en documenten die zijn gepubliceerd door verschillende organisaties die zich bezighouden met ontwikkelingen in het cyberdomein, internationale verdragen en juridische initiatieven, zoals de *Tallinn Manual.*

Er is in de afgelopen jaren veel literatuur verschenen over thema's gerelateerd aan cybersecurity. Dit betekent dat er keuzes zijn gemaakt wat betreft het gebruik van bepaalde bronnen. Waar nodig is er een afweging gemaakt gebaseerd op de publicatiedatum en academische relevantie (aan de hand van bijvoorbeeld de ranking van het academisch tijdschrift waarin het artikel is gepubliceerd). Over specifieke onderdelen van het Nederlandse beleid, waaronder de focus op

online mensenrechten, zijn juist weinig academische publicaties beschikbaar. Wanneer er weinig literatuur over een onderwerp beschikbaar is, wordt dit duidelijk in de tekst weergegeven.

In de lopende tekst wordt altijd gerefereerd naar de gebruikte bronnen. Deze worden genoemd in voetnoten. We hebben ervoor gekozen dit niet te doen in de samenvattingen, om deze zo kort en overzichtelijk mogelijk te houden.

2.2. Beperkingen van het onderzoek

Het feit dat dit rapport is gebaseerd op een literatuuroverzicht brengt bepaalde beperkingen met zich mee. Ten eerste zijn de bevindingen in dit rapport gebaseerd op onderzoeken uitgevoerd door andere onderzoekers. Hoewel we de kwaliteit van elke bron hebben beoordeeld aan de hand van de ranking van het academisch tijdschrift waarin het artikel is gepubliceerd en, waar mogelijk, de reputatie van de auteur, missen we inzicht in hoe auteurs gegevens hebben geanalyseerd en conclusies hebben geformuleerd. Met andere woorden: we hebben beperkt inzicht in de methodologische nauwkeurigheid van de bronnen waarnaar wordt verwezen in dit rapport. Hiermee moet rekening worden gehouden bij het lezen van dit rapport.

Ten tweede is het, vanwege de grote hoeveelheid relevante bronnen, niet mogelijk om alle verschillende perspectieven even uitgebreid te behandelen. De focus van het rapport ligt op het uiteenzetten van de belangrijkste debatten omtrent cybersecurity. Daarnaast is uit de bestudeerde literatuur gebleken dat er over veel cyber-gerelateerde onderwerpen geen consensus bestaat. In het rapport zal duidelijk worden dat er op veel vragen waarop deze literatuurstudie is gebaseerd, geen eenduidig antwoord gegeven kan worden. De verschillende standpunten omtrent deze onderwerpen zijn zo duidelijk mogelijk uiteengezet.

Het onderzoek is ook gelimiteerd door het gebruik van enkel bronnen die in het Engels of Nederlands zijn verschenen. Er is in deze talen bijvoorbeeld weinig literatuur over de Chinese of Russische cyberstrategieën en -perspectieven beschikbaar. Hierdoor ontstaat het risico dat het rapport voornamelijk een bespreking is van westerse ideeën, perspectieven en ontwikkelingen.

Een laatste beperking van het onderzoek wordt gevonden in de snelle ontwikkeling van het cyberdomein. Zowel technologische ontwikkelingen als veranderend beleid maken het lastig om een volledig en correct overzicht te geven van de *huidige* situatie in het internationale cybersecuritydomein. Veel onderwerpen die worden besproken in dit rapport zijn onderhevig aan geopolitieke en technologische ontwikkelingen. Dit rapport loopt daardoor in zekere zin achter de feiten aan. Tegen de tijd dat dit rapport is gepubliceerd zouden er al relevante ontwikkelingen kunnen hebben plaatsgevonden. We proberen hier rekening mee te houden in de hoofdstukken waar we focussen op de verwachte ontwikkelingen in de komende jaren.

2.3. Terminologie

Het probleem omtrent terminologie is tot op zekere hoogte een vijfde beperking van het onderzoek. Als gevolg van het internationale karakter van het cyberdomein worden cyberdebatten in het Engels gevoerd. Het vertalen van termen naar het Nederlands, of andere talen, levert soms problemen op. Sommige termen laten zich lastig 'accuraat' vertalen. Dit heeft ertoe geleid dat we er in sommige gevallen voor hebben gekozen om de Engelse term aan te houden. Een voorbeeld hiervan is *computer network attack.* Hoewel het mogelijk is om deze term direct te vertalen naar 'computernetwerkaanval', zijn we van mening dat het rapport hiermee aan helderheid verliest. In de lijst met termen (p. 6) worden definities geformuleerd.

Daarnaast is het formuleren van definities binnen het cyberdomein een gevoelige zaak. Sterker nog, academici geven aan dat het gebrek aan consensus over de betekenis van alleen al het concept 'cyberdreiging' een onmiddellijk probleem heeft veroorzaakt.[23] Onduidelijke of dubbelzinnige terminologie bemoeilijkt het onderscheiden van verschillende perspectieven, concepten en strategieën.[24] Een belangrijke eerste stap in het begrijpen van internationaal cyberbeleid is het opstellen van een verduidelijkende definitie.[25] Maar zelfs wanneer definities worden geformuleerd blijft er vaak ruimte over voor verschillende interpretaties. We zijn van mening dat het belangrijk is om duidelijke definities op te stellen zodat het voor eenieder die dit rapport leest helder is wat precies wordt bedoeld wanneer specifieke termen worden gebruikt. Gezien de onenigheid over, en overvloed aan, definities, hebben we keuzes moeten maken. Bij het lezen van dit rapport moet rekening gehouden worden met de mogelijkheid dat andere auteurs voor andere definities zouden hebben gekozen.

[23] Zie bijvoorbeeld Hollis (2012), *Is a Use of Force the Same as an Armed Attack?*, Harknett & Smeets (2020), *Cyber Campaigns and Strategic Outcomes*, p. 4, Lawson & Middleton (2019), *Cyber Pearl Harbor*.
[24] Hoffman (2019), *Is Cyber Strategy Possible?*, p. 133.
[25] Lonsdale (2016), *Britain's Emerging Cyber-Strategy*, p. 53.

3. Digitale dreiging

Samenvatting

De bestudeerde literatuur laat zien dat sinds 2015 een toegenomen aantal staten, inclusief Nederland, cybersecurity als een van de belangrijkste aandachtspunten voor de nationale veiligheid identificeert. Ook is gebleken dat politieke oorlogsvoering steeds verder is genormaliseerd, waardoor de grens tussen oorlog en vrede vervaagt. Dit is onder andere merkbaar aan de continue cyberspanning en -dreiging. Rusland maakt bijvoorbeeld actief gebruik van het cyberdomein om chaos en verdeling te zaaien binnen democratieën en internationale organisaties zoals de EU. Daarnaast is er een tweedeling zichtbaar tussen de VS en bondgenoten aan de ene kant, en China en Rusland (en bondgenoten) aan de andere kant. De twee kampen hebben andere ideeën over digitale dreiging. In het Westen wordt gesproken van *cybersecurity*, Rusland en China refereren naar *information security*.

Door technologische ontwikkelingen worden cybercapaciteiten steeds goedkoper en is er een sterke toename zichtbaar in het aantal staten dat beschikt over offensieve cybercapaciteiten. Sinds 2016 is er steeds meer aandacht voor spionage en beïnvloedingsoperaties. Ook grootschalige economisch-technologische spionage kan op termijn negatieve (economische) gevolgen hebben. Daarnaast raken statelijke actoren en criminele netwerken steeds meer met elkaar verweven in het cyberdomein. Dit compliceert het vaststellen van de dreiging vanuit statelijke actoren en de mogelijkheid om een operatie correct te attribueren. Ondanks de complexiteit kiezen voornamelijk westerse staten er steeds vaker voor om cyberoperaties publiekelijk te attribueren, in een poging om dreiging tegen te gaan. De Nederlandse internetinfrastructuur wordt regelmatig gebruikt als doorvoerhaven bij het uitvoeren van cyberoperaties gericht tegen derde staten. Deze ontwikkeling zorgt niet direct voor een dreiging richting Nederland, maar zou kunnen leiden tot reputatieschade.

Technologische ontwikkelingen vormen ook een dreiging voor de online mensenrechten. *Algorithmic surveillance* biedt staten de mogelijkheid om op grote schaal burgers in zowel binnen- als buitenland te controleren. Hierdoor lopen burgers wereldwijd het risico om slachtoffer te worden van mensenrechtenschendingen. Deze technologieën, die voornamelijk worden ontwikkeld in westerse staten, worden doorverkocht aan bijvoorbeeld Saoedi-Arabië en Iran. Autoritaire staten gebruiken deze technologie bijvoorbeeld om politieke dissidenten in de gaten te houden en te vervolgen. Inspanningen om deze handel te reguleren zijn tot nog toe niet succesvol geweest. In reactie op digitale dreigingen hebben meerdere staten wetgeving ingevoerd, bijvoorbeeld gericht op het tegengaan van desinformatie, die potentieel online mensenrechten kunnen inperken. Het beschermen van de waarheid wordt in toenemende mate gezien als een legitieme reden om de vrijheid van meningsuiting aan banden te leggen.

In de toekomst zullen nieuwe technologieën waarschijnlijk reeds bestaande dreigingen vergroten en de online mensenrechten verder onder druk zetten. Experts spreken daarnaast over een paradigmaverschuiving in de wereldorde. De ontwikkelingen in het cyberdomein zouden daarbij een belangrijke rol spelen. Ook wordt verwacht dat statelijke en niet-statelijke actoren verder verweven zullen raken en actief blijven samenwerken.

Inleiding digitale dreiging

De afgelopen jaren wordt in de *Cybersecuritybeeld Nederland* rapporten één duidelijke boodschap benadrukt: de digitale dreiging is permanent.[26] Er zijn de laatste jaren veelvuldig digitale aanvallen waargenomen, zowel in het buitenland als in Nederland.[27] Ook de Nederlandse overheid en topsectoren worden structureel digitaal aangevallen.[28] Dankzij de positie die Nederland inneemt als internationale speler, lid van de Verenigde Naties (VN)-Veiligheidsraad in 2018 en van de NAVO en de Europese Unie (EU), alsmede de hoogontwikkelde en innovatieve Nederlandse economie, hebben statelijke actoren een bovengemiddelde interesse in Nederland.[29] Om die reden wordt gesteld dat cyberoperaties uitgevoerd door staten de grootste dreiging voor de nationale veiligheid vormen.[30] Tegelijkertijd benadrukken experts dat de grenzen tussen cyberactoren vervagen. Daardoor kan er niet altijd een duidelijk onderscheid gemaakt worden tussen statelijke actoren en criminele netwerken.[31] Het is, nog los van de vervaging tussen verschillende actoren, gecompliceerd om traditionele concepten en afbakeningen omtrent veiligheidsvraagstukken toe te passen op het cyberdomein. Om die reden vereist 'digitale dreiging' een verandering in (nadenken over) organisatorische en bestuurlijke aanpak.[32]

De digitale dreiging richting Nederland, maar ook in het algemeen, is in de afgelopen jaren toegenomen en de verwachting is ook dat deze trend de komende jaren blijft doorzetten. De dreiging wordt door experts bepaald aan de hand van de intenties, cybercapaciteiten en activiteiten van actoren.[33] Daarnaast spelen bredere geopolitieke ontwikkelingen en technologische innovaties een belangrijke rol. Deze ontwikkelingen zullen gezamenlijk worden besproken.

In dit hoofdstuk worden de volgende vragen beantwoord:

- 3.1. Wat zijn de belangrijkste ontwikkelingen in de afgelopen jaren op het gebied van de digitale dreiging van statelijke en daaraan gelieerde actoren, in het bijzonder richting Nederland?
- 3.1.1. Hoe hangen deze dreigingen samen met ontwikkelingen omtrent mensenrechten in het cyberdomein?
- 3.2. Wat zijn de verwachte ontwikkelingen op het gebied van de dreiging van statelijke en daaraan gelieerde actoren in de komende jaren?

3.1. Belangrijke ontwikkelingen digitale dreiging 2015-2020

Sinds 2015 identificeert een toegenomen aantal staten, inclusief Nederland, cybersecurity als het belangrijkste, of een van de belangrijkste, aandachtspunt(en) omtrent de nationale veiligheid.[34] Het

[26] NCTV (2020), *Cybersecuritybeeld Nederland,* p. 7.
[27] NCTV (2015), *Cybersecuritybeeld Nederland,* p. 9, NCTV (2020), *Cybersecuritybeeld Nederland,* p. 15-16.
[28] NCTV (2016), *Cybersecuritybeeld Nederland,* p. 19, NCTV (2020), *Cybersecuritybeeld Nederland,* p. 19.
[29] AIVD (2017), *Jaarverslag 2017*, p. 8.
[30] NCTV (2018), *Cybersecuritybeeld Nederland,* p. 13
[31] NCTV (2018), *Cybersecuritybeeld Nederland,* p. 13-15.
[32] King & Gallagher (2020), *Cyberspace Solarium Commission* p. 31-45, Broeders (2014), *Investigating the Place and Role of the Armed Forces*, p. 23, 25-26.
[33] Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 16, NCTV (2019), *Cybersecuritybeeld Nederland,* p. 16, De Bruijne et al. (2017), *Towards a New Cyber Threat Actor Typology*, p. 40.
[34] Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 23.

veilig houden van het cyberdomein wordt dus van groeiend belang geacht in het waarborgen van de algemene nationale veiligheid. Dit hangt samen met de potentieel grootschalige gevolgen van cyberaanvallen. De ontwikkelingen van de afgelopen vijf jaar geven een duidelijk beeld van de toenemende digitale dreiging, zowel richting Nederland als in het algemeen. In de volgende paragrafen worden zowel cyber-specifieke ontwikkelingen, als ontwikkelingen die zich onder andere voordoen in het cyberdomein, besproken. Er is tussen de inhoud van sommige van deze ontwikkelingen sprake van een bepaalde mate van overlap. De volgende ontwikkelingen worden kort toegelicht:[35]

- Politieke oorlogsvoering is steeds verder genormaliseerd, dit brengt met zich mee dat er continu sprake is van (cyber)spanningen en dat de grens tussen 'oorlog' en 'vrede' vervaagt;
- Sinds 2016 is er meer aandacht voor spionage en beïnvloeding;
- De opkomst van grootschalige economisch-technologische spionage kan op termijn de economische slagkracht van staten ondermijnen;
- De Verenigde Staten (VS) komen steeds meer tegenover China en Rusland te staan;
- Rusland maakt actief gebruik van het cyberdomein om chaos en verdeling te zaaien in democratische staten en om internationale organisaties uiteen te drijven;
- Er is sprake van een sterke toename in het aantal staten dat beschikt over offensieve cybercapaciteiten;
- Statelijke actoren en criminele netwerken raken verweven in het cyberdomein;
- Technologische ontwikkelingen zorgen ervoor dat cybercapaciteiten makkelijk te verkrijgen zijn en goedkoop ingezet kunnen worden;
- Cyberoperaties worden vaker publiekelijk geattribueerd;
- De Nederlandse internetinfrastructuur wordt regelmatig gebruikt als doorvoerhaven bij het uitvoeren van cyberoperaties. Deze ontwikkeling zorgt niet direct voor een dreiging richting Nederland maar zou kunnen leiden tot reputatieschade.

Normalisering politieke oorlogsvoering

Politieke oorlogsvoering is geen nieuw fenomeen, maar is de afgelopen jaren bezig aan een opmars.[36] De term refereert naar het inzetten van militaire, diplomatieke, financiële en andere middelen in vredestijd om het (buitenland) beleid van andere staten zo aan te passen dat het de belangen van de dader dient.[37] Het cyberdomein biedt nieuwe mogelijkheden voor het uitvoeren van zogenoemde hybride activiteiten.[38] Zo wordt verondersteld dat de mogelijkheden die het cyberdomein biedt de drempel verlagen om een aanval uit te voeren: staten zouden eerder besluiten om een aanval te plegen via het cyberdomein, dan wanneer ze afhankelijk zijn van meer conventionele en openlijk agressieve middelen.[39] Het gevolg van het verlagen van deze drempel is dat politieke oorlogsvoering genormaliseerd wordt en de grenzen tussen oorlog en vrede vervagen. Dit leidt tot een permanente situatie – "*unpeace*" – waarin de spanningen tussen staten continu kunnen oplopen.[40]

---

[35] De volgorde impliceert geen ordening qua dreigingsniveau voor Nederland. Op basis van de beschikbare literatuur is niet duidelijk te beoordelen welke dreiging het meest van belang is voor Nederland en waarom dit het geval zou zijn.
[36] AIVD (2017), *Jaarverslag 2017*, p. 9.
[37] Pronk (2019), *The Return of Political Warfare*, p.
[38] Torossian et al. (2020), *Hybrid Conflict*, p. 2.
[39] Shea (2018), *Cyberspace as a Domain of Operations*, p. 140.
[40] Broeders et al. (2019), *Foreign Intelligence in the Digital Age*, p. 3.

Dat politieke oorlogsvoering in de afgelopen jaren verder is genormaliseerd wordt duidelijk uit het toenemende aantal cyberoperaties. Zo zijn staten in vergelijking met voorgaande jaren meer actief in het uitvoeren van cyberspionage,[41] *computer network attacks* en beïnvloedingscampagnes.[42] Het aantal gerapporteerde, significante cyberincidenten is tussen 2008 en 2018 flink toegenomen: vergeleken met tien jaar eerder hebben er wereldwijd in 2018 minstens zeven keer zoveel incidenten plaatsgevonden.[43]

In 2019 hebben meerdere statelijke actoren sociale media platformen gebruikt voor het uitvoeren van beïnvloedingcampagnes. Volgens Facebook en Twitter maken in ieder geval China, India, Iran, Pakistan, Rusland, Saudi-Arabië en Venezuela zich aan dit soort praktijken schuldig.[44] Daarnaast voeren verschillende staten ook cyberaanvallen uit op kritieke infrastructuren. Rusland, China, Iran en Noord-Korea voeren het vaakst dit soort aanvallen uit. De Verenigde Staten, Zuid-Korea, India en Oekraïne zijn het vaakst het doelwit van deze aanvallen.[45] De Verenigde Staten heeft zelf ook aanvallen uitgevoerd op de kritieke infrastructuren van Iran, Noord-Korea en Rusland.[46]

Spionage en beïnvloeding

De MIVD onderkende in 2019 diverse cyberspionage-activiteiten tegen Nederland, andere westerse staten en bondgenootschappelijke belangen.[47] Het Australische *Strategic Policy Institute* onderzocht 97 verkiezingen en 31 referenda van november 2016 tot april 2019 en ontdekte dat er in tenminste twintig staten – waaronder Nederland – buitenlandse inmenging heeft plaatsgevonden.[48] Rusland zou geprobeerd hebben om de Nederlandse verkiezingen van 2017 te beïnvloeden door middel van het verspreiden van desinformatie.[49] Daarnaast wordt Rusland beschuldigd van het steunen van Nederlandse anti-EU-groepen die actief waren tijdens het Oekraïne referendum in 2016.[50] De Russische *Internet Research Agency* creëerde en verspreidde een nepvideo waarin een groep Oekraïense soldaten een Nederlandse vlag verbranden en dreigen met het plegen van terroristische aanslagen als Nederlanders tegen het referendum zouden stemmen.[51] Zowel staten als internationale organisaties lijken de afgelopen jaren meer aandacht te hebben gekregen voor de (politieke) effecten van cyberoperaties die niet per se leiden tot directe fysieke vernietiging of ontwrichting.[52]

---

[41] Cyberspionage wordt niet per definitie gezien als een uiting van politieke oorlogsvoering. Zie hoofdstuk 4 voor een uitgebreidere bespreking van deze activiteit.
[42] Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 25.
[43] Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 26.
[44] Bradshaw & Howard (2018), *The Global Disinformation Disorder*, p. 5. In dit rapport wordt Nederland ook genoemd in een lijst met landen die manipulatiecampagnes via sociale media uitvoeren. Zie ook: Broeders (2020), *Creating Consequences for Election Interference*.
[45] Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 36.
[46] Faesen et al. (2020), *Conflict in Cyberspace*.
[47] NCTV (2020), *Cybersecuritybeeld Nederland,* p. 15.
[48] Hanson et al. (2019), *Hacking Democracies*, p. 8.
[49] Hanson et al. (2019), *Hacking Democracies*, p. 22.
[50] Treverton et al. (2018), *Addressing Hybrid Threats*, p. 52, Applebaum (2016), *The Dutch Just Showed the World*.
[51] Committee on Foreign Relations (2018), *Putin's Assymetric Assault*, p. 113, Higgins (2017), *Fake News, Fake Ukrainians*.
[52] Nye (2017), *Deterrence and Dissuasion in Cyberspace*, Jean-Claude Juncker, president van de Europese Commissie, verklaarde in 2017 dat cyberaanvallen gevaarlijker kunnen zijn voor de stabiliteit van democratieën en economieën dan geweren en tanks. Zie: Popescu & Secrieru (2018), *Hacks, Leacks and Disruptions*, p. 65.

In 2012 schreef Duncan Hollis dat experts het inhoudelijk gezien niet eens zijn over de betekenis van 'cyberdreiging'.[53] De ambiguïteit en onzekerheid omtrent deze nieuwe dreiging hebben ertoe geleid dat er volop gebruik werd gemaakt van metaforen en analogieën. Het bekendste voorbeeld is het 'cyber-Pearl Harbor' scenario waarin kritieke infrastructuren worden aangevallen via het cyberdomein, met massavernietiging, ontwrichting en sociale en economische chaos tot gevolg.[54] Gedurende minstens 20 jaar werd in de VS, wanneer gesproken werd over cyberdreiging, gedoeld op dit soort grootschalige cyberaanvallen met aanzienlijke gevolgen voor de bevolking.[55] Aanvallen op deze schaal hebben echter niet plaatsgevonden en het gebruik van de 'cyber-Pearl Harbor' analogie is in de laatste jaren teruggelopen.[56] Nye schrijft dat de cyberdreiging op Pearl Harbor schaal waarschijnlijk overdreven is,[57] en ook anderen hebben betoogd dat het gebruik van de metafoor negatieve gevolgen zou kunnen hebben op het vermogen om cyberdreigingen te begrijpen en af te wenden.[58] Dit zou zijn gebleken uit de Russische inmenging in de Amerikaanse presidentsverkiezingen van 2016 en het gebrek aan een tijdige reactie. Sindsdien is de focus verschoven richting andere cyberdreigingen, zoals (grootschalige) cyberspionage, buitenlandse beïnvloeding en desinformatiecampagnes. Hoewel dit soort cyberoperaties minder vaak directe fysieke schade berokkenen, kunnen zij op langere termijn de democratische rechtsstaat ondermijnen en het vertrouwen in instituties dusdanig verminderen dat deze niet goed meer kunnen functioneren.[59] Wanneer er bijvoorbeeld een algemeen wantrouwen jegens informatie ontstaat, kan dit ook de legitimiteit van betrouwbare, onafhankelijke journalisten aantasten.[60]

Grootschalige economisch-technologische spionage

Uit onderzoek van de AIVD blijkt dat steeds meer staten schuldig zijn aan het uitvoeren van economische cyberspionage-operaties. Ook Nederland is het doelwit van operaties waarbij data, intellectuele eigendommen en technische informatie worden gestolen.[61] In 2017 werd digitaal ingebroken bij diverse Europese multinationals en onderzoeksinstellingen in de energie-, hightech- en chemische sector. Hierbij zijn terabytes aan vertrouwelijke gegevens gestolen en is substantiële economische waarde verloren gegaan. Dergelijke cyberoperaties zijn gericht op het stelen van bedrijfsstrategieën en plannen, intellectueel eigendom en kostbare onderzoeks- en ontwikkelingsprojecten. Het gevolg is dat de positie van Nederlandse bedrijven op de internationale markt wordt ondermijnd, de daders een (oneerlijke) voorsprong hebben en het economisch verdienvermogen van Nederland wordt bedreigd.[62]

---

[53] Hollis (2012), *Is a Use of Force the Same as an Armed Attack?* Zie ook: Harknett & Smeets (2020), *Cyber Campaigns and Strategic Outcomes*, p. 4.
[54] Nye (2017), *Deterrence and Dissuasion in Cyberspace*, Lawson & Middleton (2019), *Cyber Pearl Harbor.*
[55] In 2012 verklaarde Panetta, toenmalig Amerikaanse minister van Defensie, dat een cyber-Pearl Harbor net zo destructief zou kunnen zijn als de terroristische aanslag van 9/11; zou kunnen leiden tot paniek, vernietiging en het verlies van mensenlevens; de natie zou verlammen en choqueren, en een diep gevoel van kwetsbaarheid zal creëren. Zie: Lawson & Middleton (2019), *Cyber Pearl Harbor*.
[56] Lonsdale (2016), *Britain's Emerging Cyber-Strategy*, p. 54.
[57] Nye (2017), *Deterrence and Dissuasion in Cyberspace*.
[58] Lawson & Middleton (2019), *Cyber Pearl Harbor*.
[59] Sharp (2018), *Hiding in Plain Sight*, p. 46.
[60] Hwang (2017), *Digital Disinformation: A Primer*, p. 2.
[61] NCTV (2020), *Cybersecuritybeeld Nederland,* p. 15 & 30, NCTV (2019), *Cybersecuritybeeld Nederland,* p. 26.
[62] AIVD (2017), *Jaarverslag 2017*, p. 9, Lotrionte (2014), *Countering State-Sponsored Cyber Economic Espionage*, p. 452.

De Amerikaanse *Federal Bureau of Investigation* (FBI) concludeert dat deze vorm van diefstal op lange-termijn wellicht de grootse dreiging voor de economische en nationale veiligheid van vrije samenlevingen kan betekenen.[63] De FBI waarschuwt in het bijzonder voor economische spionage-operaties uitgevoerd door China. Inmiddels hebben de VS, het Verenigd Koninkrijk (VK), Australië, Canada, Japan en Nieuw-Zeeland de Chinese overheid verantwoordelijk gesteld voor een economische spionage-operatie uit 2018.[64] Naast China worden ook Iran en Rusland door de VS aangewezen als meest actieve en bekwame economische spionage-actoren.[65]

Verenigde Staten versus China en Rusland (cyber- versus informationsecurity)

Dat er onenigheid bestaat tussen de cybergrootmachten wordt alleen al duidelijk uit de verschillende benamingen die de staten gebruiken omtrent veiligheid in het cyberdomein. Waar de VS en bondgenoten spreken over *cybersecurity*, geven onder andere China en Rusland de voorkeur aan de term *information security.* Dit verschil komt voort uit wat staten als dreiging voor de nationale veiligheid beschouwen. In China en Rusland wordt, in tegenstelling tot het Westen, vrije toegang tot informatie gezien als potentieel veiligheidsrisico. In de meeste democratieën wordt 'informatie' niet als dreiging beschouwd (hoewel dit onderwerp met de opkomst en verspreiding van desinformatie wel meer onder de aandacht is gebracht).[66] De afgelopen jaren worden echter gekarakteriseerd door de continu verslechterende relatie tussen de cybergrootmachten, met de Verenigde Staten aan de ene, en China en Rusland aan de andere kant. Deze verslechterende relatie heeft ook effect op het open en internationale karakter van het cyberdomein. Experts hebben het over "data nationalisme" en het einde van het mondiale internet.[67]

Waar eerder nog dialoog mogelijk was over *confidence-building measures* (CBMs) en samenwerking in de vorm van een *cybersecurity task force*,[68] zijn de posities van de VS en China en Rusland steeds verder uiteengedreven. Zowel de beslissing van Rusland om Edward Snowden politiek asiel te verlenen als de beslissing van de VS om vijf Chinese legerofficieren aan te klagen vanwege cyberspionage, hebben geleid tot het beëindigen van de bilaterale gesprekken en samenwerking.[69] In september 2020 heeft Rusland zich tot de VS gericht met de suggestie om een nieuw programma op te richten, bedoeld om de betrekkingen tussen de twee staten omtrent informatie- en communicatietechnologie (ICT)-gebruik weer op te bouwen.[70] De VS heeft hier nog niet publiekelijk op gereageerd.

Gedurende de ambtsperiode van president Trump (2016-2020) zijn de politieke en economische spanningen tussen de VS en China verder opgelopen en is er een toename in het aantal cyberincidenten waargenomen.[71] Daarnaast zorgt de concurrentie tussen de VS en China omtrent

---

[63] Thompson (2020), *FBI director: China's Economic Espionage Threatens Free Societie.*
[64] NCTV (2020), *Cybersecuritybeeld Nederland,* 26.
[65] NCSC (2018), *Foreign Economic Espionage in Cyberspace*, p. 5-10.
[66] Zie bijvoorbeeld: Keir & Hagestad (2013), *Divided by a Common Language*, p. 3.
[67] Bendiek et al. (2017), *The EU's Revised Cybersecurity Strategy*, p. 1, NCTV (2020), *Cybersecuritybeeld Nederland,* p. 39.
[68] De VS en Rusland sloten in 2013 een overeenkomst om het risico op conflicten in het cyberdomein te verminderen door o.a. te communiceren over incidenten die van belang zijn voor de nationale veiligheid. Zie: Nakashima (2013), *U.S. and Russia Sign Pact*.
[69] Chuanying (2020), *Forging Stability in Cyberspace*, p. 128.
[70] Statement by President of Russia Vladimir Putin on a comprehensive program of measures for restoring the Russia - US cooperation in the field of international information security. Zie: http://en.kremlin.ru/events/president/news/64086.
[71] Faesen et al. (2020), *Conflict in Cyberspace*, p. 5.

technologische dominantie voor groeiend wantrouwen. Dit heeft ertoe geleid dat de VS meer dan honderd Chinese bedrijven op een zwarte lijst heeft gezet.[72] Volgens politicoloog Ian Bremmer is er een technologische Koude Oorlog tussen China en de VS aan het ontstaan,[73] en ook Secretaris-Generaal van de VN António Guterres waarschuwt voor een dergelijk conflict tussen de twee grootmachten.[74] President Xi Jinping heeft aangegeven geen intentie te hebben om een (koude) oorlog met welk land dan ook aan te gaan.[75]

Activiteit Rusland

Rusland heeft de motivatie, gelegenheid en middelen om een aanzienlijke dreiging voor West- en Centraal Europa te vormen.[76] Hierbij is het creëren van chaos om het vertrouwen in de democratie uit te hollen en westerse politieke legitimiteit te schaden het belangrijkste doel.[77] Het verzwakken van westerse instituties en het ondermijnen van trans-Atlantische consensus hoort daar ook bij.[78] Rusland heeft daarnaast waarschijnlijk verschillende motivaties ten opzichte van verschillende regio's in Europa. Zo zou het uitvoeren van cyberoperaties in West-Europa voornamelijk gericht zijn op het afdwingen van respect voor Rusland als grote mogendheid en het beïnvloeden van EU- en NAVO-beleid om regionale belangen veilig te stellen.[79]

De afgelopen jaren is Rusland de meest zichtbare en gepropageerde cyberactor in Europa:[80] er wordt gesteld dat de meeste kwaadwillige cyberactiviteiten gericht tegen Europa afkomstig zijn uit Rusland.[81] Sinds 2004 heeft de Russische overheid cyberoperaties, desinformatiecampagnes en financiële middelen ingezet om zich te kunnen mengen in de binnenlandse politiek van tenminste 27 Europese en Noord-Amerikaanse staten,[82] waaronder Nederland.[83] Vanwege het neerhalen van vlucht MH17 en het strafproces in Den Haag is het strategisch belang van Nederland (voor Rusland) sterk toegenomen.[84]

In 2018 bereidde Rusland een cyberoperatie voor op de in Nederland gevestigde Organisatie voor het Verbod op Chemische Wapens (OPCW).[85] Zoals hierboven al werd vermeld, zou Rusland ook geprobeerd hebben om de Nederlandse verkiezingen van 2017 te beïnvloeden door desinformatie te verspreiden.[86] Deze gebeurtenissen tonen aan dat Rusland zich niet tegengehouden voelt om gebruik te maken van het cyberdomein om samenlevingen, internationale organisaties en bondgenootschappen uiteen te drijven.[87] Ruslands buurlanden zijn echter vaker het doelwit van

---

[72] Van Bemmel & Vervaeke (2020), *Aan het Front van de Techoorlog*.
[73] Brouwers (2020), *VS en Europa Zien Chinese Dreiging Compleet Anders*.
[74] UN News (2020), *UN Chief Appeals for Global Solidarity*.
[75] Righton (2020), *Trump Eist in VN-Toespraak Actie*.
[76] Cohen & Radin (2019), *Russia's Hostile Measures in Europe*, p. 141.
[77] Paterson & Hanley (2020), *Political Warfare in the Digital Age*, p. 443.
[78] Polyakova & Boyer (2018), *The Future of Political Warfare*, p. 3.
[79] Invloed in West-Europa wordt gezien als de belangrijkste strategische 'prijs' buiten de VS. Zie: Cohen & Radin (2019), *Russia's Hostile Measures in Europe*, p. 106.
[80] Torossian et al. (2020), *Hybrid Conflict*.
[81] Popescu & Secrieru (2018), *Hacks, Leacks and Disruptions*, p. 68.
[82] Treverton et al. (2018), *Addressing Hybrid Threats*, p. 10.
[83] Hanson et al. (2019), *Hacking Democracies*, p. 22.
[84] NCTV (2019), *Cybersecuritybeeld Nederland,* p. 16.
[85] NCTV (2019), *Cybersecuritybeeld Nederland,* p. 18.
[86] Hanson et al. (2019), *Hacking Democracies*, p. 22.
[87] Pronk (2019), *The Return of Political Warfare*, Bundesambt für Verfassungsschutz (2018), *Cyber Attacks Controlled by Intelligence Services*, p. 6-18.

(cyber)aanvallen dan bijvoorbeeld Nederland,[88] en Rusland maakt gebruik van een beperkter scala aan instrumenten in West-Europa in vergelijking met Oost-Europa.[89] Landen die geografisch dichtbij Rusland liggen, of waar politieke of sociale verdeeldheid heerst, zijn in het bijzonder kwetsbaar voor Russische inmenging of beïnvloeding.[90] Daarnaast zijn tijdens de COVID-19 pandemie desinformatiecampagnes tegen de EU en NAVO ingezet, waarvan Rusland wordt beschuldigd.[91]

Volgens Russische bronnen zou de Russische strategie, *new-type warfare* genoemd, noodzakelijkerwijs worden ingezet als verdedigingsmechanisme, bedoeld om eventuele (democratische/anti-Kremlin) revoluties af te weren.[92] Cybermethodes en de mogelijkheden die *new-type warfare* biedt zijn dan ook waardevolle instrumenten voor het Poetin regime. Ten tijde van de Arabische Lente werd onder Russische academici geschreven over de cyberstrategie van de Verenigde Staten: Amerikaanse cyberoperaties zouden hebben bijgedragen aan het destabiliseren van enkele Arabische landen en daarmee het non-interventieprincipe hebben geschonden.[93] Dezelfde methodes zouden door de VS tegen de Russische staat zijn ingezet. Vanuit het Russische perspectief is het de Verenigde Staten die offensieve methodes inzet via het cyberdomein om de Russische staat te ondermijnen en tegelijkertijd wereldwijde overheersing te bewerkstelligen.[94] Rusland zou dus geleerd hebben van Amerikaanse activiteiten, de effectiviteit van cyberoperaties hebben afgekeken, en vanuit preventief oogmerk diezelfde strategie inzetten.[95]

Toename offensieve cybercapaciteiten

De afgelopen jaren is wereldwijd fors geïnvesteerd in offensieve (en defensieve) cybercapaciteit.[96] In 2010 werd er nog gesproken over een zestal staten met offensieve cybercapaciteiten.[97] Eind 2016 werd echter publiekelijk bekend dat er al meer dan 30 staten bezig waren om dergelijke capaciteiten te ontwikkelen.[98] Vervolgens werd in 2017 een lijst gepubliceerd waarin wordt gesproken over 100 staten die de capaciteit hebben om een cyberaanval te lanceren.[99] De AIVD schat in dat het aantal staten met een offensief cyberprogramma ook de komende jaren toe blijft nemen.[100]

---

[88] In de afgelopen jaren zijn in ieder geval Georgië, Oekraïne, Estland het doelwit geweest van Russische cyberoperaties. Ilves et al. (2016), *European Union and NATO*, p. 128.

[89] De buurlanden van Rusland hebben te maken met economische, diplomatieke, spionage, cyber- en andere middelen. Tegen staten in West-Europa zet Rusland vooral beïnvloedingscampagnes en informatieoperaties in. Zie: Van der Putten et al. (2018), *Hybrid Conflict*, p. 5.

[90] Treverton et al. (2018), *Addressing Hybrid Threats*, p. 65.

[91] Zie bijvoorbeeld: Emmot (2020), *Russia Deploying Coronavirus Disinformation*.

[92] Thornton & Miron (2019), *Deterring Russian Cyber Warfare*, p. 259.

[93] Thornton & Miron (2019), *Deterring Russian Cyber Warfare*, p. 260.

[94] Thornton & Miron (2019), *Deterring Russian Cyber Warfare*, p. 260.

[95] De Amerikaanse inlichtingendiensten schatten de kans groot dat Poetin ook in 2020 de Amerikaanse verkiezingen tracht te beïnvloeden. Zie: Ramdharie (2020), *CIA Rapport*.

[96] NCTV (2015), *Cybersecuritybeeld Nederland,* p. 22.

[97] Maurer (2018), *Cyber Proxies*, p. 171.

[98] Foreign Cyber Threats to the United States, 115th Cong. (2017) (joint statement of James R. Clapper, Director of National Intelligence, Marcel Lettre, Undersecretary of Defense for Intelligence, and Michael S. Rogers, US Cyber Command Director, National Security Agency), https://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threatsto-the-united-states.

[99] Levine (2017), *Russia Tops List of 100 Countries*. Uit een studie van het *Harvard Belfer Center* blijkt dat de VS, China, het VK, Rusland en Nederland (in die volgorde) de vijf staten met de meeste cybercapaciteit zijn (maar niet offensieve capaciteit per se), Zie: Vavra (2020), *Chinese Cyber Power is Neck-and-Neck with US*.

[100] AIVD (2019), *Offensief Cyberprogramma* p. 8.

Volgens de NCTV zetten in ieder geval China, Rusland en Iran cybercapaciteiten in tegen Nederland.[101] Rusland heeft een offensief cyberprogramma voor verstoring en sabotage van de kritieke infrastructuur. Naast Rusland zetten ook China en Iran veelvuldig cyberspionage in. Zowel ministeries als Nederlandse ambassades in het Midden-Oosten en Centraal-Azië zijn doelwit van dit soort aanvallen.[102] Enkele van de veronderstelde doelwitten van onder andere Rusland zijn bondgenoten, of bondgenoten van bondgenoten, van Nederland.[103] Dit brengt ook een bepaalde dreiging voor Nederland met zich mee: Rusland, China, Iran en Noord-Korea hebben de mogelijkheid, en in verschillende mate de intentie, om de veiligheid van de NAVO of EU-lidstaten te bedreigen door middel van cyberaanvallen.[104] Het is, mede daarom, wellicht niet onverwacht dat ook de perceptie dat spanningen in het cyberdomein verder gaan escaleren, is toegenomen.[105]

Verwevenheid statelijke actoren en criminele netwerken

Naast dat het aantal actoren die een dreiging voor de nationale veiligheid vormen in de afgelopen jaren is toegenomen, is duidelijk geworden dat er sprake is van een bepaalde mate van verwevenheid tussen statelijke actoren en criminele netwerken.[106] Actoren doen zich daarnaast bewust voor als iemand anders, creëren valse sporen in de richting van andere actoren en innoveren continu om te kunnen inspelen op ontdekte kwetsbaarheden.[107] De AIVD verwacht om die reden dat het steeds lastiger zal worden om verschillende cyberactoren van elkaar te onderscheiden. Dit compliceert de mogelijkheid om cyberoperaties correct toe te schrijven aan de verantwoordelijke actor.[108]

Daarnaast beargumenteert Tim Maurer, een van de deelnemers aan het wetenschappelijk debat over de vraag of er een 'cyberoorlog' zal plaatsvinden, dat staten niet alleen de mogelijkheid hebben om zogeheten *cyber proxy's* in te zetten, maar dat sommigen hier ook actief gebruik van maken.[109] Een cyber proxy wordt gedefinieerd als een tussenpersoon die een offensieve cyberoperatie uitvoert, of er direct aan bijdraagt, welke bewust mogelijk wordt gemaakt door een begunstigde.[110] Staten kunnen een dergelijke operatie *actief* mogelijk maken door bijvoorbeeld de cyber proxy financieel of technisch te ondersteunen. Wanneer een staat een cyberoperatie bewust niet tegenhoudt is er sprake van het *passief* mogelijk maken van de operatie, en wordt de staat – volgens deze definitie – ook beschouwd als begunstigde.[111]

---

[101] NCTV (2019), *Cybersecuritybeeld Nederland,* p. 7. Dit betekent dat deze landen digitale middelen inzetten om geopolitieke, economische, militaire of ideologische doelstellingen te bereiken ten koste van Nederlandse belangen.

[102] NCTV (2019), *Cybersecuritybeeld Nederland,* p. 16-18.

[103] Pronk (2019), *The Return of Political Warfare.*

[104] Ilves et al. (2016), *European Union and NATO*, p. 128, Cohen & Radin (2019), *Russia's Hostile Measures in Europe*.

[105] Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 130, Pronk (2019), *Global Security Pulse.*

[106] Zo bleek in 2019 bijvoorbeeld dat een aan een staat gelieerde hackersgroep zich bezighield met zowel spionage als financieel gemotiveerde cyberoperaties. Zie: NCTV (2020), *Cybersecuritybeeld Nederland,* p. 16.

[107] NCTV (2017), *Cybersecuritybeeld Nederland,* p. 20.

[108] NCTV (2018), *Cybersecuritybeeld Nederland,* p. 13, Teichmann (2020), *Five Threats that Influence the Cyber Landscape*, p. 23, AIVD (2019), *Offensief Cyberprogramma* p. 8.

[109] Maurer (2018), *Cyber Mercenaries*, p. 15.

[110] Maurer (2018), *Cyber Mercenaries*, p. xi.

[111] Maurer schrijft over verschillende soorten state-proxy relaties: *delegation, orchestration* en *sanctioning.* Bij de eerste twee relaties is er sprake van een actieve rol voor de begunstigde. Sanctioning is gebaseerd op het idee dat de begunstigde een oogje dichtknijpt omdat deze indirect profiteert van de actie. Zie: Maurer (2018), *Cyber Mercenaries*, p. 42.

Het cyber proxy-fenomeen is relatief nieuw en de VN wijst het inzetten van cyber proxy's af.[112] Het kan echter om verschillende redenen voordelig zijn voor staten om cyber proxy's in te zetten. Zo wordt bijvoorbeeld gesteld dat het inzetten van cyber proxy's een mogelijkheid biedt om betrokkenheid te ontkennen.[113] Dit zou vooral voor technisch minder geavanceerde staten aanlokkelijk zijn, omdat zij hun activiteit minder goed kunnen verhullen met technische middelen.[114] Maar ook technisch geavanceerde staten maken gebruik van cyber proxy's.

In Rusland en China werken zeer geavanceerde niet-statelijke actoren samen met hun overheden. Deze "internet milities"[115] kunnen worden ingezet om overheidsbeleid uit te voeren.[116] Ook de VS, Iran en Syrië hebben de afgelopen jaren gebruik gemaakt van cyber proxy's.[117] Uit de academische literatuur kan derhalve worden opgemaakt dat het gebruik van niet-statelijke actoren voor cyberoperaties recentelijk is toegenomen, en dat daarmee ook het dreigingsbeeld aan verandering onderhevig is. Focussen op de cybercapaciteit van slechts traditioneel 'statelijke actoren' leidt dus tot zowel een gelimiteerd als misleidend beeld van de digitale dreiging.[118]

Technologische ontwikkelingen

In de afgelopen jaren is gebleken dat het cyberdomein niet alleen nieuwe middelen voor politieke oorlogsvoering biedt, maar ook significant de kosten van dit soort operaties verlaagt.[119] Nieuwe sociale media platformen maken het inzetten van propaganda- en beïnvloedingscampagnes vele malen goedkoper en makkelijker, en het bereik, de snelheid en de nauwkeurigheid van propaganda- en beïnvloedingscampagnes is verbeterd.[120] Daarbij bieden online platformen de mogelijkheid om een grote groep mensen te bereiken en is er – in de meeste gevallen – geen sprake van verificatie voordat een bericht gepost kan worden. Er zijn weinig kosten verbonden aan het gebruiken van nauwkeurige statistieken en diensten die zijn ontworpen voor marketingdoeleinden.[121] Zo werden in 2016, tijdens de Amerikaanse presidentsverkiezingen, berichten gericht op het creëren van verdeeldheid via Facebook verspreid. Het promoten van deze berichten kostte slechts 100.000 dollar, maar ze bereikten wel 150 miljoen Facebook- en Instagramgebruikers.[122] Dit soort nieuwe middelen zijn niet alleen sneller en goedkoper maar maken het ook makkelijker in de anonimiteit te opereren en betrokkenheid te ontkennen.

Nieuwe technologieën zoals kunstmatige intelligentie (AI) en kwantumcomputing kunnen een positieve bijdrage leveren aan het beveiligen van het cyberdomein, maar ook negatieve gevolgen hebben.[123] Hoewel deze technologieën ontwikkeld worden vanwege hun precisie, verdwijnt er ook een bepaalde mate van controle en dat zou ervoor kunnen zorgen dat aanvallen onverwachte

---

[112] VN Algemene Vergadering A/70/174, para. 28(e).
[113] Sigholm (2016), *Non-State Actors in Cyberspace Operations*, p. 24, Maurer (2018), *Cyber Mercenaries*, p. 25.
[114] Maurer (2018), *Cyber Mercenaries*, p. 25, Klimburg (2011), *Mobilising Cyber Power*, p. 43.
[115] Klimburg (2011), *Mobilising Cyber Power*, p. 51.
[116] Klimburg (2011), *Mobilising Cyber Power*, p. 43-44.
[117] Maurer (2018), *Cyber Mercenaries*, p. 69-120.
[118] Maurer (2018), *Cyber Mercenaries,* p. xii.
[119] Treverton et al. (2018), *Addressing Hybrid Threats*, p. 3.
[120] Van der Putten et al. (2018), *Hybrid Conflict*, p. 5.
[121] Hwang (2017), *Digital Disinformation: A Primer*, p. 7.
[122] Polyakova & Boyer (2018), *The Future of Political Warfare*, p. 10.
[123] NCTV (2020), *Cybersecuritybeeld Nederland,* p. 25, Raban & Hauptman (2018), *Foresight of Cyber Security*.

consequenties hebben.[124] Het gaat dan bijvoorbeeld om *supply chain*-aanvallen[125] die het risico van ongecontroleerde verspreiding met zich meebrengen, doordat een virus wordt verspreid via software die wereldwijd wordt gebruikt.[126] Met de toenemende mate waarin ook Nederland digitaliseert, groeit het cyber-aanvalsoppervlak. Slimme, zelflerende algoritmes kunnen bijvoorbeeld worden gecorrumpeerd. Dit houdt in dat een aanvaller het gedrag van het systeem kan overnemen en ervoor kan zorgen dat het systeem geen gegevens meer kan interpreteren.[127] Daarbij kan het gebruik van deze snelle technologie de kans op escalatie in het cyberdomein verhogen. Wanneer (tegen)aanvallen worden uitgevoerd door slimme systemen in plaats van door mensen, ontstaat er een gebrek aan controle en, wellicht, terughoudendheid.[128]

Wanneer technologische ontwikkelingen worden besproken in de context van (internationale) veiligheid, is het volgens Eilstrup-Sangiovanni belangrijk om hier een kanttekening bij te plaatsen. Technologische ontwikkelingen vormen namelijk zelden de beslissende factor in het maken van strategische keuzes en de meeste wapenwedlopen vloeien voort uit politieke overwegingen en beslissingen.[129] Met andere woorden: technologische ontwikkelingen vormen zelden per definitie een dreiging voor de (inter)nationale veiligheid.

Publieke attributie

Het identificeren van de actor achter een digitale aanval is complex en vergt een zeer specifieke set aan capaciteiten. En hoewel onbetwistbare attributie steeds meer haalbaar lijkt,[130] is het niet altijd mogelijk om bewijs naar buiten te brengen zonder het toekomstige gebruik van de eigen inlichtingeninstrumenten te schaden.[131] Desalniettemin hebben verschillende overheden in 2019 publiekelijk digitale aanvallen geattribueerd aan staten.[132] Tot dusver zijn het voornamelijk westerse staten die dit doen,[133] om zo de strategische waarde van het publiekelijk attribueren proberen te achterhalen.[134] China en Rusland hebben bijvoorbeeld nog geen formele toeschrijvingen gedaan, hoewel ze het Westen regelmatig beschuldigen van cyberspionage en inbreuk op hun systemen.[135] Sommige staten attribueren cyberoperaties niet publiekelijk omdat ze weten dat ze – vanwege diplomatieke betrekkingen – geen maatregelen zullen nemen.[136] In de gevallen dat staten wel maatregelen hebben genomen, overschreden die meestal niet de ondergrens van 'retorsie'. Dit zijn

---

[124] Polyakova & Boyer (2018), *The Future of Political Warfare*, p. 2.
[125] Supply chain-aanvallen nemen veel vormen aan. Het gaat bijvoorbeeld om het kapen van software-updates waar kwaadaardige codes in worden geïnjecteerd. Wanneer dit niet op tijd ontdekt wordt, leidt het uitvoeren van de update (wat overal ter wereld tegelijkertijd kan gebeuren) tot schade.
[126] NCTV (2018), *Cybersecuritybeeld Nederland,* p. 16.
[127] Teichmann (2020), *Five Threats that Influence the Cyber Landscape*, p. 21.
[128] Teichmann (2020), *Five Threats that Influence the Cyber Landscape*, p. 22.
[129] Eilstrup-Sangiovanni (2018), *Why the World Needs an International Cyberwar Convention*, p. 388.
[130] Hier lijkt onenigheid over te bestaan. Volgens sommigen is definitieve attributie bijna onmogelijk. Zie: Eggenschwiler & Silomon (2018), *Challenges and Opportunities*, p. 14.
[131] Van der Meer (2018), *State-Level Responses to Massive Cyber-Attacks*, p. 2.
[132] NCTV (2019), *Cybersecuritybeeld Nederland,* p. 18.
[133] In 2018 attribueerden de VS, het VK, Canada, Australië, Nieuw-Zeeland, Japan, Denemarken, Estland, Letland, Litouwen, Noorwegen, Zweden en Finland de NotPetya-aanval aan Rusland. Zie: Stilgherrian (2018), *Blaming Russia for NotPetya.*
[134] De Australische Cyber ambassadeur stelt dat *naming & shaming* onderdeel is van de afschrikkingstheorie, en is bedoeld om aan tegenstanders duidelijk te maken dat er gevolgen zullen zijn voor hun gedrag in het cyberdomein. Zie: Stilgherrian (2018), *Blaming Russia for NotPetya*.
[135] Broeders et al. (2019), *Foreign Intelligence in the Digital Age*, p. 4.
[136] Broeders et al. (2019), *Foreign Intelligence in the Digital Age*, p. 5.

maatregelen die volgens het internationaal recht geen bewijs vereisen. In hoofdstuk 4 wordt dit verder toegelicht.

Tot dusver zijn publieke attributies in het algemeen ondersteund met minimaal bewijsmateriaal. Met name omdat staten en hun inlichtingendiensten een evenwicht moeten vinden tussen het vrijgeven van informatie over eigen inlichtingeninstrumenten en de politieke wens om een cyberoperatie (collectief) te attribueren.[137] Ondanks de moeilijkheden die bij attributie komen kijken, wordt verwacht dat de vraag naar attributie en consequenties zullen toenemen zolang de spanningen in het cyberdomein hoog blijven.[138] De EU heeft de eerste stap gezet richting het operationaliseren van consequenties door een kader voor cybersancties op te stellen. In hoofdstuk 5 wordt het beleid van de EU beschreven.

Nederland als doorvoerhaven

Uit onderzoek van de NCTV blijkt dat de Nederlandse informatie- en communicatietechnologie (ICT)-infrastructuur wordt misbruikt door (onder andere) statelijke actoren bij cyberoperaties waarvan Nederland niet het doelwit is. De Nederlandse infrastructuur zou de afgelopen jaren onder andere gebruikt zijn door Iran, Noord-Korea en Rusland bij het uitvoeren van cyberoperaties.[139] Deze internetinfrastructuur is aantrekkelijk voor dit soort misbruik vanwege haar snelheid, lage kosten en betrouwbare aard.[140] Zo is ook gebleken dat een Nederlandse Tor server[141] waarschijnlijk is gebruikt bij het hacken van de Amerikaanse democratische partij tijdens de Amerikaanse verkiezingen van 2016.[142] Hoewel deze ontwikkeling niet een directe dreiging voor de nationale veiligheid vormt, raakt Nederland hierdoor wel ongewild betrokken bij de verspreiding van cyberoperaties.[143] Dit soort misbruik kan het internationale imago van Nederland schaden en slecht zijn voor bondgenootschappelijke belangen en de integriteit van de Nederlandse ICT-infrastructuur.[144]

3.1.1. Online mensenrechten

Toegang tot het internet biedt vele mogelijkheden, onder andere het gemakkelijk delen van meningen en het vergaren van kennis over uiteenlopende onderwerpen. In 2018 maakten ongeveer 3.2 miljard mensen gebruik van sociale media platformen.[145] Hoewel deze platformen niet specifiek zijn opgericht om politieke idealen na te streven, is het gebruik van sociale media onlosmakelijk verbonden geraakt aan het bevorderen van bepaalde mensenrechten.[146] In het Westen wordt de vrije toegang tot informatie gezien als mensenrecht. Daartegenover staan bijvoorbeeld China en Rusland die, zoals eerder werd genoemd, de vrije toegang tot het internet en (online) informatie als een dreiging voor de nationale veiligheid beschouwen. Deze tweedeling (*information security* versus

[137] Broeders et al. (2019), *Foreign Intelligence in the Digital Age*, p. 4.
[138] Broeders et al. (2019), *Foreign Intelligence in the Digital Age*, p. 5.
[139] NCTV (2019), *Cybersecuritybeeld Nederland,* p. 18.
[140] AIVD (2019), *Offensief Cyberprogramma* p. 4.
[141] Tor is een gratis software en open netwerk dat gebruikers in staat stelt zichzelf te beschermen tegen netwerk surveillance.
[142] Viganò et al. (2020), *Cybersecurity of Critical Infrastructure*, p. 163.
[143] AIVD (2019), *Offensief Cyberprogramma* p. 4.
[144] NCTV (2020), *Cybersecuritybeeld Nederland,* p. 18.
[145] Shandler & Canetti (2019), *A Reality of Vulnerability and Dependence*, p. 77-78.
[146] Moise (2016), *Cybersecurity and Human Rights*, p. 162.

cybersecurity) hangt samen met ontwikkelingen omtrent mensenrechten in het cyberdomein, in het bijzonder wat betreft het ontwikkelen van beleid (zie paragraaf 5.2).[147]

Door academici wordt ook gesproken over het toevoegen van een nieuw mensenrecht: het recht op toegang tot een vrij internet.[148] In dit rapport wordt echter verder geen uitgebreide bespreking opgenomen van dit soort mogelijke nieuwe 'online' mensenrechten. Met *online mensenrechten* wordt gedoeld op de bestaande mensenrechten die worden toegepast in het cyberdomein. In de paragrafen die volgen worden enkele ontwikkelingen op het gebied van mensenrechten in het cyberdomein besproken. Deze hangen samen met ontwikkelingen omtrent de digitale dreiging die in de voorgaande paragraaf zijn toegelicht. De volgende ontwikkelingen worden besproken:

- Technologische ontwikkelingen op het gebied van online surveillance vormen een steeds grotere dreiging voor de online mensenrechten;
- De verkoop van surveillancetechnologie maakt het mogelijk voor andere staten om online mensenrechten te schenden (in zowel binnen- als buitenland). Regulering van deze handel op EU-niveau blijft achter en stuit op weerstand;
- Als reactie op de ontwikkelingen in het cyberdomein wordt wereldwijd wetgeving ingevoerd die de online mensenrechten kunnen inperken.

Surveillance

Hoewel het internet werd ontwikkeld door de private sector als een virtueel domein zonder territoriale grenzen, proberen staten tegenwoordig steeds meer controle uit te oefenen over het cyberdomein. Overheden gebruiken technologieën op manieren die de vrijheid van meningsuiting en het recht op privacy onder druk zetten.[149] Sinds publiekelijk bekend werd op welke schaal de VS online communicatie in de gaten houdt, is er steeds meer aandacht gekomen voor geautomatiseerde AI-surveillancetechnologieën, ook wel *algorithmic surveillance* genoemd.[150] In tegenstelling tot traditionele surveillancetechnieken hoeft er bij *algorithmic surveillance* geen specifieke keuze gemaakt te worden wie er wordt gevolgd. Het geautomatiseerde karakter van deze nieuwe techniek maakt het mogelijk om op een grotere schaal dan ooit mensen in het digitale domein in de gaten te houden. De schaal waarop deze surveillancetechniek kan worden toegepast heeft niet alleen effect op het recht op privacy, maar ook op de vrijheid van meningsuiting, vrijheid van vergadering en het verbod op discriminatie.[151] Zo biedt *algorithmic surveillance* de mogelijkheid om specifieke bevolkingsgroepen te monitoren op basis van leeftijd, religie, etniciteit of nationaliteit. Hierdoor kan discriminatie geautomatiseerd worden.[152] Ook worden de resultaten van geautomatiseerde surveillancetechnologieën vaak beïnvloed door ingebouwde vooroordelen in het AI-sturingsprogramma.[153] Een recent voorbeeld is de toeslagenaffaire bij de Nederlandse

[147] Maurer (2018), *Cyber Mercenaries*, p. 6.
[148] Reglitz (2020), *The Human Right to Free Internet Access*, p.328, Kilovaty (2020), *An Extraterritorial Human Right*, p. 52, Shackelford (2019), *Should Cybersecurity be a Human Right* p. 17.
[149] Liaropoulos (2016), *Reconceptualising Cyber Security*, p. 32, 35.
[150] Margulies (2016), *Surveillance by Algorithm*, p. 1056, Bernal (2016), *Data Gathering, Surveillance and Human Rights*, p. 249.
[151] Het recht op privacy is cruciaal voor de uitvoering van deze mensenrechten. Zie: Kosta (2020), *Algorithmic State Surveillance*, p. 1, Bernal (2016), *Data Gathering, Surveillance and Human Rights*, p. 245, Margulies (2016), *Surveillance by Algorithm*, p. 1056, Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 77.
[152] Bernal (2016), *Data Gathering, Surveillance and Human Rights*, p. 254, 258.
[153] Kosta (2020), *Algorithmic State Surveillance*, p. 1.

Belastingdienst, waarbij burgers op basis van hun nationaliteit door het geautomatiseerde controlesysteem werden aangemerkt als risicovol. Dit was volgens de Autoriteit Persoonsgegevens in strijd met de privacywet en de Algemene Verordening Gegevensbescherming.[154]

Als gevolg van geautomatiseerde surveillancetechnieken lopen mensen over de hele wereld, door gebruik te maken van het cyberdomein, het risico om slachtoffer te worden van online mensenrechtenschendingen.[155] In de afgelopen jaren zijn vooral liberale democratieën meer gebruik gaan maken van AI-surveillance. Meer dan de helft van de liberale democratieën gebruikt deze technologie, tegenover 37 procent van de autocratieën. Veel staten, waaronder Nederland, gebruiken AI-technieken voor de digitalisering van stedelijke voorzieningen, gezichtsherkenningssoftware en ter ondersteuning van de justitiële diensten.[156]

Cyber export naar autoritaire staten

Met de komst van steeds geavanceerdere technologieën zijn autoritaire staten ICT gaan gebruiken om politieke dissidenten in de gaten te houden en te vervolgen.[157] Dit wordt veelal mogelijk gemaakt doordat westerse staten – waaronder Nederland, Israël en China – surveillancetechnologieën verkopen aan staten als Syrië, Tunesië, Saoedi-Arabië en de Verenigde Arabische Emiraten, en elkaar.[158] De EU probeert hier sinds 2015 richtlijnen voor op te stellen. Echter zijn sommige EU-lidstaten geen voorstander van het idee om private bedrijven te verplichten na te gaan welke impact hun product kan hebben op de bescherming van mensenrechten in het buitenland.[159]

Een onlangs gepubliceerd rapport van *Amnesty International* beschrijft hoe een Nederlands bedrijf emotieherkenningssoftware en gedragsanalysetechnologie heeft verkocht aan verschillende Chinese instanties. Het rapport werpt een kritische blik op de EU-regelgeving omtrent de export van cybertechnologieën en beargumenteert dat deze ontoereikend is in het beschermen van mensenrechten.[160]

De verdere verspreiding van geavanceerde cybertechnologieën is problematisch. In toenemende mate zijn mensenrechtenactivisten, kritische bloggers en civiele organisaties het doelwit van surveillance en cyberoperaties georganiseerd door staten.[161] Deze cyberdreigingen houden echter niet op bij de landsgrenzen. Ook mensenrechtenactivisten die verblijven in staten waar een vrij internetbeleid wordt gehandhaafd kunnen het slachtoffer worden van surveillance door buitenlandse regimes.[162] Staten als Iran, Ethiopië en Saoedi-Arabië gebruiken bijvoorbeeld Europese en Israëlische technologieën om de e-mailadressen en digitale apparaten van activisten die in de EU verblijven te hacken.[163]

---

[154] Autoriteit Persoonsgegevens (2020), *Werkwijze Belastingdienst*.
[155] Liaropoulos (2016), *Reconceptualising Cyber Security*, p. 35.
[156] Feldstein (2019), *The Global Expansion of AI Survaillance*, p. 10, 26.
[157] El-Ashy et al. (2019), *Big Brother in the Middle-East and North Africa*, p.230, Liaropoulos (2016), *Reconceptualising Cyber Security*, p. 35-36.
[158] Kanetake (2019), *The EU's Export Control*, p. 155, Schaake & Vermeulen (2016), *Towards a Values-Based European Foreign Policy*, p. 82.
[159] Kanetake (2019), *The EU's Export Control*, p. 161.
[160] Amnesty International (2020), *Out of Control*, p. 29, 47.
[161] El-Ashy et al. (2019), *Big Brother in the Middle-East and North Africa*, p. 234, Amnesty International (2019), *State-Sponsored Hackers*, Liaropoulos (2016), *Reconceptualising Cyber Security*, p. 36, Fidler (2012), *Cyberattacks and International Human Rights Law*, p. 327-328.
[162] Liaropoulos (2016), *Reconceptualising Cyber Security*, p. 35.
[163] Michaelsen (2017), *Far Away, So Close*, p. 468, HRW (2020), *EU: Strengthen Rules on Surveillance Tech Exports*.

Reactie op nieuwe dreigingen
Hoewel de afweging tussen het beschermen van mensenrechten en de nationale veiligheid niet alleen speelt met betrekking tot technologische ontwikkelingen of het cyberdomein, is het duidelijk dat er meer aandacht is gekomen voor het reguleren van online informatie. Dit brengt dilemma's met zich mee: er moeten keuzes worden gemaakt tussen het waarborgen van verschillende mensenrechten en nationale (veiligheids)belangen. Een voorbeeld hiervan is de spanning tussen de vrijheid van meningsuiting en het tegengaan van buitenlandse bemoeienis.[164]

Om de digitale dreigingen zoals beschreven in 3.1 tegen te gaan, proberen veel staten steeds meer controle te krijgen over het cyberdomein. De online mensenrechten komen hierdoor niet enkel meer in het geding door staten die het beschermen van mensenrechten niet als prioriteit zien, maar ook door staten die zeggen te strijden voor een cyberdomein waar mensenrechten gelden.[165] Zo heeft Australië (uit angst voor Chinese bemoeienis) nieuwe wetten aangenomen waarin het een brede en vage afbakening van de nationale veiligheid hanteert. Over de wetgeving wordt geschreven dat deze burgerlijke vrijheden mogelijk ingrijpend inperkt. De brede en vage afbakening van termen zou het strafbaar kunnen maken om politieke verandering teweeg te brengen. Zo zou bijvoorbeeld een samenwerking tussen Australische burgers en internationale organisaties op het gebied van klimaat- en vluchtelingenbeleid onder de nieuwe wetgeving kunnen resulteren in een celstraf van twintig jaar.[166] Daarnaast is het verboden om politieke of economische informatie te delen met andere staten of internationale organisaties zoals de VN, ook wanneer dit onbewust wordt gedaan. Volgens critici maakt dit het onmogelijk te rapporteren over eventuele mensenrechtenschendingen die de Australische overheid zelf begaat in het cyberdomein.[167]

Ook in Zuidoost-Azië wordt op grote schaal wetgeving ontwikkeld waarmee de staat kan optreden tegen 'valse informatie'. Deze nieuwe wetten lijken het begin van een trend te zijn, waarin het beschermen van de 'waarheid' gezien wordt als een geaccepteerde reden om de vrijheid van meningsuiting aan banden te leggen.[168]

3.2. Verwachte ontwikkelingen 2020-2025

De digitale dreiging zal naar verwachting de komende jaren niet afnemen. Zoals eerder al werd beschreven, drijven de cybergrootmachten juist steeds verder uit elkaar. Daarnaast vinden er snelle technologische ontwikkelingen plaats, wat het cyberdomein onvoorspelbaar en complex maakt. Vanwege de nieuwe uitdagingen die het cyberdomein met mee zich mee heeft gebracht, is het lastig voor staten om te weten welk internationaal cybersecuritybeleid de meeste veiligheid en stabiliteit zal opleveren op de lange termijn. Het is daarnaast onduidelijk wat de effecten zijn van het huidige beleid. In de literatuur wordt geschreven over de volgende verwachte ontwikkelingen:

- De vraag naar cyber proxy's alsmede hun capaciteiten zullen toenemen;
- Experts spreken over een paradigmaverschuiving in de wereldorde. Deze zou al eerder zijn ingezet, maar zou zich de komende jaren verder kunnen manifesteren en de ontwikkelingen in het cyberdomein spelen daarin een belangrijke rol;
- Nieuwe technologieën zullen reeds bestaande dreigingen vergroten;

[164] AIV (2020), *Regulering van Online Content*, p. 5-6, 45.
[165] Schaake & Vermeulen (2016), *Towards a Values-Based European Foreign Policy*, p. 77.
[166] Mack (2020), *An Era of Foreign Political Interference*, p. 376
[167] Mack (2020), *An Era of Foreign Political Interference*, p. 377.
[168] Schuldt (2019), *Truth vs. Free Speech*.

- Ook van nieuwe dreigingen wordt verwacht dat ze een negatief effect zullen hebben op de bescherming van online mensenrechten.

Toename aantal cyber proxy's en capaciteiten
Maurer beargumenteert dat de vraag naar cyber proxy's de komende jaren zal toenemen en er dus meer cyber proxy's actief zullen zijn, met meer geavanceerde capaciteiten en mogelijkheden om schade aan te richten. Deze conclusie is gebaseerd op de observatie dat een toenemend aantal staten geïnteresseerd is in het ontwikkelen van mogelijkheden om het cyberdomein te gebruiken voor politieke en militaire doeleinden.[169] Wanneer staten ervoor kiezen om cyber proxy's in te zetten, kunnen deze niet-statelijke actoren toegang krijgen tot meer geavanceerde technieken. Op deze manier vindt er een leerproces plaats tussen statelijke en niet-statelijke actoren.[170] Zeker op de lange termijn kan het inzetten van cyber proxy's risico's met zich meebrengen die kunnen leiden tot internationale escalatie.[171]

Paradigmaverschuiving
Meerdere academici hebben de afgelopen jaren geschreven over de crisis waarin de liberale wereldorde zich bevindt.[172] Duncombe en Dunne stellen zelfs dat alle mainstream internationale betrekkingen-theoretici het erover eens zijn dat de hegemonie van de liberale wereldorde voorbij is.[173] Barrinha en Renard analyseerden de literatuur over de (post-)liberale orde en opperen dat de huidige internationale spanningen voortvloeien uit het feit dat de liberale orde niet langer een afspiegeling is van het internationale machtsevenwicht, noch van de waarden en institutionele voorkeuren van opkomende machten.[174] Dit leidt tot het betwisten van de heersende liberale wereldorde door een groep staten.[175] Deze groep beargumenteert dat het internationale systeem een 'update' vereist als gevolg van de mondiale ontwikkelingen die de afgelopen decennia plaatsvonden.[176]

De ontwikkelingen in het cyberdomein zijn direct verbonden aan de ontwikkelingen binnen het internationale politieke systeem. Daarbij heeft de opkomst van het cyberdomein geleid tot een nieuw speelveld voor internationale betrekkingen en biedt het een mogelijkheid voor nieuwe internationale en transnationale dynamieken en relaties.[177] Zo beargumenteren Barrinha en Renard dat cyberdiplomatie bij uitstek *post-liberaal* is: de noodzaak voor cyberdiplomatie komt voort uit de erkenning dat het cyberdomein omstreden is en een dreiging vormt voor internationale veiligheid en

[169] Maurer (2018), *Cyber Mercenaries*, p. 27.
[170] DOD Science Defense Board (2013), *Task Force Report*, p. 21.
[171] Een geavanceerde hackersgroep die losse banden heeft met de staat kan zich bijvoorbeeld tegen de staat keren wanneer zij het oneens zijn met/gefrustreerd zijn over het gevoerde (inter)nationale beleid, dit zou kunnen leiden tot zowel nationale of internationale instabiliteit. Zie: Maurer (2018), *Cyber Mercenaries*, p. 110. Daarnaast kan het lastig blijken voor een staat om niet-statelijke actoren te controleren. Zie: Sigholm (2016), *Non-State Actors in Cyberspace Operations*, p. 26.
[172] Barrinha & Renard (2020), *Power and Diplomacy*, p. 752, Ikenberry (2018), *The End of the Liberal International Order?*, p. 7, Duncombe & Dunne (2018), *After Liberal World Order*, p. 27, Nye (2019), *The Rise and Fall*, p. 64.
[173] Duncombe & Dunne (2018), *After Liberal World Order*, p. 25.
[174] Barrinha & Renard (2020), *Power and Diplomacy*, p. 765.
[175] Broeders et al. (2019), *A Coalition of the Unwilling?*, p. 1.
[176] Noesselt (2016), *Contested Global Order(s)*, p. 640.
[177] Barrinha & Renard (2020), *Power and Diplomacy*, p. 764.

stabiliteit.[178] Volgens Barrinha en Renard zijn (of waren) liberale staten van mening dat de opkomst van het cyberdomein niet tot internationale concurrentie zou leiden.

De snelle ontwikkelingen die plaatsvinden in het cyberdomein worden geïdentificeerd als motor achter de (reeds ingezette) paradigmaverschuiving. Het gaat zowel om technologieën die een gevaar voor de democratie kunnen vormen, het feit dat het voor een toenemend aantal actoren makkelijker wordt om buiten de grenzen van de op regels gebaseerde internationale orde te opereren, de ongelijkheid waarmee nieuwe technologieën over de wereld zijn verdeeld en hun concentratie binnen de private sector. Dit zou kunnen leiden tot een (her)verspreiding van macht – weg van staten – en de opkomst van geheel nieuwe bestuursmodellen.[179] Zo stelt Nye dat individuen en particuliere organisaties, zoals private bedrijven, ngo's en sociale bewegingen, meer macht krijgen en regeringen meer moeite zullen hebben met het aansturen van actie op wereldniveau.[180]

Verschillende actoren – in ieder geval Japan, de Verenigde Arabische Emiraten, het *European Strategy and Policy Analysis System,* het *Center for Strategic and International Studies* en het *World Economic Forum* – verwachten dat er een nieuwe golf van interstatelijke concurrentie zal plaatsvinden via het cyberdomein.[181] Uit analyse van Sweijs en Pronk blijkt dat Nederland dit sentiment – dat cyberontwikkelingen zullen leiden tot een verstoring van de huidige machtsverdelingen – vooralsnog niet lijkt te delen.[182]

Nieuwe technologieën verergeren reeds bestaande problemen

De volgende technologieën worden verwacht een aanzienlijke impact (zowel positief als negatief) te hebben op cybersecurity: autonome technologieën (waarbij menselijke besluitvorming niet langer nodig is) zijn kwetsbaar voor hackers; *Internet of Things* zorgt voor meer digitale afhankelijkheid en dus een groter aanvalsoppervlak; kwantumcomputing vormt een potentiële bedreiging voor alle systemen die gebruikmaken van cryptografie; en militaire toepassingen van kunstmatige intelligentie kunnen zowel leiden tot meer geautomatiseerde aanvallen, als helpen bij het voorspellen en voorkomen van aanvallen.[183]

Daarnaast wordt verwacht dat nieuwe cybertechnologieën de effectiviteit van politieke oorlogsvoeringcampagnes vergroten. Sommige technologieën, in het bijzonder *deep fakes*, zullen bijvoorbeeld bijdragen aan het verbeteren van de mate waarin desinformatie 'echt' lijkt. *Deep fakes* zijn audio- of videofragmenten die zo geavanceerd zijn bewerkt dat het lijkt alsof echte mensen dingen doen of zeggen die ze in werkelijkheid nooit hebben gedaan of gezegd. Goed getimede *deep*

---

[178] Barrinha & Renard (2020), *Power and Diplomacy*, p. 749.

[179] Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 126.

[180] "Complexity is growing, and world politics will soon not be the sole province of governments. Individuals and private organizations—from corporations and nongovernmental organizations to terrorists and social movements—are being empowered, and informal networks will undercut the monopoly on power of traditional bureaucracies. Governments will continue to possess power and resources, but the stage on which they play will become ever more crowded, and they will have less ability to direct the action." Zie: Nye (2016), *Will the Liberal Order Survive?*, p. 14.

[181] Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 122.

[182] "The sentiment that cyber- and/ or IT-related innovations are likely to upset existing power dynamics (whether military or otherwise) constitutes a marked departure from the Dutch view on cyber threats. Whereas the Netherlands perceives cyber threats almost exclusively through the lens of cyberattacks (i.e., the threatening use case), several actors – the UAE, the ESPAS, Japan, the CSIS, and the WEF – view the cyber domain as one which is likely to form the backdrop of a new wave of interstate competition." Zie: Sweijs & Pronk (2020), *Between Order and Chaos?*, p. 122.

[183] Raban & Hauptman (2018), *Foresight of Cyber Security*.

fakes kunnen ingezet worden om burgers te misleiden, kiezers te beïnvloeden tijdens verkiezingen en politieke spanningen te verergeren.[184] De technologie die dit mogelijk maakt ondergaat een snelle ontwikkeling.[185] Zowel het manipuleren van de integriteit van data, als het onbewust vertrouwen op valse informatie worden dus gezien als groeiende dreiging.

Online mensenrechten

In de academische literatuur worden geen duidelijke voorspellingen gedaan over hoe potentiële nieuwe technologieën of politieke ontwikkelingen een impact kunnen hebben op mensenrechten binnen het cyberdomein. Wel waarschuwt *Amnesty International* voor het aanpassingsvermogen van kwaadwillende actoren. Wanneer mensenrechtenactivisten een nieuwe online communicatiemethode gebruiken om surveillance van buitenlandse regimes te voorkomen, veranderen de methodes van deze regimes mee.[186] Ook worden de hackmethodes van deze regimes steeds geavanceerder. In de toekomst zal ook vaker gebruik worden gemaakt van *NSO-spyware*. Met deze technologie kunnen complete browseromgevingen worden onderschept en worden computers of telefoons vervolgens gemakkelijk gehackt.[187]

De ontwikkelingen in het cyberdomein vinden zo snel plaats dat het ingewikkeld is om eventuele implicaties op mensenrechten te voorspellen. Er bestaat een spanning tussen de vraag naar meer veiligheid enerzijds en de bescherming van mensenrechten anderzijds. Een toenemend aantal staten verkiest de nationale veiligheid boven het beschermen van online mensenrechten.[188] Met de komst van nieuwe technologieën en dreigingen zullen staten deze afweging telkens opnieuw moeten maken, met mogelijk negatieve gevolgen voor mensenrechten.

[184] Polyakova & Boyer (2018), *The Future of Political Warfare*, p. 1.
[185] Chesney & Citron (2019), *Deep Fakes: A Looming Challenge*, p. 1758.
[186] Amnesty (2020), *Digital Surveillance Threats for 2020.*
[187] Amnesty (2020), *Digital Surveillance Threats for 2020.*
[188] AIV (2020), *Regulering van Online Content*, p. 6.

4. Internationaal recht

Samenvatting

Nederland is van mening dat het bestaand internationaal recht van toepassing is op activiteiten in het cyberdomein. Dit betekent dat het non-interventieprincipe en het geweldsverbod ook gelden voor cyberoperaties. Er bestaan echter geen duidelijke rechtsregels over wat wel en niet is toegestaan. De rechtmatigheid van handelingen is afhankelijk van context en kan dus niet met zekerheid vooraf bepaald worden. De inzet van voornamelijk westerse staten om overeenkomst te bereiken over regels heeft geleid tot het opstellen van de *Tallinn Manual.* Op mondiaal niveau bestaat nog steeds veel onenigheid over een aantal belangrijke zaken. Hoewel er bijvoorbeeld consensus bestaat over de toepassing van het verbod op het gebruiken van en dreigen met geweld in het cyberdomein, is er veel discussie over de betekenis van 'cybergeweld'. Staten zijn het oneens over de vraag of een cyberoperatie daadwerkelijk fysieke gevolgen moet hebben om te spreken van cybergeweld. Deze onenigheid leidt bijvoorbeeld tot onduidelijkheid omtrent de mogelijkheid tot zelfverdediging in reactie op een cyberoperatie.

Volgens internationaal recht is spionage niet verboden in vredestijd. Slechts de manier waarop cyberspionage ingezet wordt, kan volgens de Tallinn experts onrechtmatig zijn. Wel lijkt er een verbod te ontstaan op economisch-technologische spionage, voornamelijk via bilaterale en multilaterale overeenkomsten. Gebaseerd op bestaand internationaal recht is het lastig vast te stellen of cyberbeïnvloedingsoperaties onrechtmatig zijn. Vooraanstaande juristen stellen dat dit type operatie in een grijze zone valt wat betreft het schenden van territoriale integriteit, omdat er in het internationaal recht een duidelijk onderscheid wordt gemaakt tussen *beïnvloeding* (in principe niet verboden) en *dwang* (wel verboden). Academici stellen ook dat het *due diligence* principe geldig is met betrekking tot cyberoperaties. Dit wil zeggen dat staten niet bewust mogen toestaan dat de nationale infrastructuur wordt gebruikt voor handelingen die staten onrechtmatig treffen. Gebeurt dit wel, dan kan dit leiden tot staatsaansprakelijkheid. In respons op cyberoperaties mogen staten onder internationaal recht zowel retorsie als tegenmaatregelen inzetten.

Er bestaat mondiale consensus over de geldigheid van mensenrechten in het cyberdomein, maar onenigheid over de exacte toepassing van mensenrechtenverdragen. Sommige staten verheffen 'internetsoevereiniteit' boven mensenrechten en zijn van mening dat zij niet verantwoordelijk zijn voor mensenrechtenschendingen buiten hun eigen grondgebied. Door nieuwe technologieën is fysieke aanwezigheid echter geen vereiste om controle over individuen te kunnen uitoefenen. Daarom pleiten sommige academici voor een *personal model* van jurisdictie in plaats van *territoriale* jurisdictie. Het concept 'internetsoevereiniteit' wordt met name gepromoot door China en Rusland, als tegenhanger van het westerse vrije, open internetbeleid. China en Rusland beargumenteren, gebaseerd op het soevereiniteitsprincipe, dat staten het recht hebben om complete controle uit te oefenen over het cyberdomein binnen hun landsgrenzen.

Door het gebrek aan internationale consensus zijn multilaterale en regionale verdragen in belang toegenomen. De verdragen waar Nederland lid van is, zoals het Europees Verdrag voor de Rechten van de Mens, geven striktere richtlijnen voor het tijdelijk opschorten van mensenrechten dan andere regionale verdragen, zoals het Amerikaanse Verdrag inzake de Rechten van de Mens. Naast deze verdragen baseren staten zoals Australië, de VS en EU-lidstaten hun cyberstrategie voornamelijk op normen zoals uiteengezet in regionale richtlijnen en afspraken. Voor Nederland zijn de *EU Human Rights Guidelines on Freedom of Expression Online and Offline* van belang.

Inleiding internationaal recht

Voor Nederland bestaat er geen twijfel: internationaal recht is van toepassing op activiteiten die zich afspelen in het cyberdomein.[189] Ook is Nederland van mening dat mensenrechten zowel offline als online gelden. Verschillende vooraanstaande experts op het gebied van internationaal recht concluderen hetzelfde. In 2013 werd middels een consensusrapport, opgesteld onder de auspiciën van de Verenigde Naties, vastgesteld dat "internationaal recht, en in het bijzonder het Handvest van de VN, van toepassing is en essentieel is voor het handhaven van vrede en stabiliteit en het bevorderen van een open, veilige, vreedzame en toegankelijke ICT-omgeving."[190] Hoewel China en Rusland betrokken waren bij het opstellen van het consensusrapport, hebben zij twijfel geuit over de toepasbaarheid van bestaande regimes binnen het internationaal recht en benadrukken het belang van een speciaal cyberverdrag.[191] Pogingen om onderhandelingen voor een cyberverdrag te starten worden tot dusver afgewezen door een groep westerse staten.[192]

Internationale en regionale gesprekken zijn tot dusver gericht op het *herformuleren* van regels over hoe het bestaand internationaal recht van toepassing is in het cyberdomein. Een van de bekendste en meest geciteerde uitkomsten van expertdiscussies is de *Tallinn Manual on the International Law Applicable to Cyber Warfare.*[193] In 2017 verscheen de *Tallinn Manual 2.0*,[194] welke door betrokkenen wordt omschreven als *"the most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations."*[195] De Tallinn Manual is bedoeld als een objectieve herformulering van *lex lata* – bestaand internationaal recht – en is dus niet gericht op (het leveren van een bijdrage aan) het ontwikkelen van nieuwe regels.[196]

---

[189] Ministerie van Buitenlandse Zaken (2019), *Bijlage: Internationaal Recht in het Digitale Domein (Cyberspace)*.

[190] 2013 *Group of Governmental Experts* (GGE), VN Algemene Vergadering A/68/98, para. 19, VN Algemene Vergadering A/70/174, para. 24.

[191] Rusland deed in 2009 een voorstel om het gebruik van cyberwapens door staten preventief te verbieden. De VS wees het voorstel af en beargumenteerde dat dit verbod het onmogelijk zou maken om effectief te kunnen verdedigen tegen cyberaanvallen. Zie: Nye (2010), *Cyber Power*, p. 18. In 2011 dienden Rusland, China, Tajikistan en Oezbekistan opnieuw een voorstel in bij de VN Algemene Vergadering (Draft Intl. Code of Conduct for Information Security). Zie: Eilstrup-Sangiovanni (2018), *Why the World Needs an International Cyberwar Convention*, p. 388. In 2015 werd een geüpdatete versie van de Code of Conduct, opgesteld door Rusland, China, Kazachstan, Kyrgyzstan, Tajikistan en Oezbekistan, gedeeld met VN-lidstaten (A/69/723). Zie: Rõigas (2015), *An Updated Draft of the Code of Conduct*.

[192] Eilstrup-Sangiovanni (2018), *Why the World Needs an International Cyberwar Convention*, p. 388.

[193] In 2009 startte de NAVO Cooperative Cyber Defence Centre of Excellence (CCD COE) een project met een onafhankelijke groep vooraanstaande experts en academici op het gebied van internationaal recht. Onder leiding van Professor Michael Schmitt stelden 8 juridische en 2 technische experts (allen westers), naast peer reviewers, waarnemers en juridisch onderzoekers, de Manual op. Zie voor een complete lijst met namen: Schmitt (2013), *Tallinn Manual*, p. 6-9.

[194] Het opstellen van de Tallinn Manual 2.0 werd opnieuw geleid door Professor Michael Schmitt, maar de groep experts (17 juridische en 1 technische expert) was groter en niet langer exclusief westers (experts afkomstig uit o.a. Belarus, China en Thailand). Zie: Schmitt (2017), *Tallinn Manual 2.0*, p. xii - xviii.

[195] CCDCOE (2020), *Tallinn Manual 2.0*.

[196] Schmitt (2017), *Tallinn Manual 2.0*, p. 2-3. De praktische waarde van de Tallinn Manual (in het bijzonder de eerste versie) als instrument om cyberconflict te bestrijden of voorkomen is volgens enkele academici bescheiden vanwege tenminste twee redenen: 1. De Manual heeft nauwelijks steun gevonden in de bredere internationale gemeenschap (maar wordt vooral geprezen/naar verwezen door NAVO-lidstaten), 2. De interpretatie van de toepassing van het internationaal recht in het cyberdomein, zoals beschreven in de Tallinn Manual, zou geen invloed hebben op staatspraktijk of *opinio juris.* Zie: Eilstrup-Sangiovanni (2018), *Why the World Needs an International Cyberwar Convention*, p. 388, Lucas (2017), *Ethics of Cyberwarfare*, p. 40, 76.

Het uitgangspunt van dit hoofdstuk is in lijn met de Nederlandse visie dat het bestaand internationaal recht van toepassing is in het cyberdomein en volgt daarmee in grote lijnen de Tallinn Manual. Hoewel Nederland het niet per definitie eens is met alles wat in de Manual staat beschreven, wordt het document van belangrijke waarde geacht en reflecteert het over het algemeen de Nederlandse positie.[197] Desalniettemin bestaan er geen duidelijke regels over wat wel en niet mag in het cyberdomein: veel is afhankelijk van de context en kan dus niet met zekerheid vooraf bepaald worden. Daarnaast hebben ook de Tallinn experts over veel specifieke casussen simpelweg geen consensus weten te bereiken. Om die reden wordt er in dit hoofdstuk ook aandacht besteed aan de verschillende posities die experts of staten innemen.

In dit hoofdstuk worden de volgende vragen beantwoord:

- 4.1. Hoe ziet het huidige internationaal recht eruit qua wat staten al dan niet mogen doen in het cyberdomein ten opzichte van andere staten, in het bijzonder met betrekking tot spionage, sabotage en beïnvloeding?
- 4.2. Hoe ziet het huidige internationaal recht eruit qua wat staten al dan niet mogen doen in respons op een aanval die wordt uitgevoerd via het cyberdomein?
- 4.3. Hoe ziet het huidige internationaal recht eruit qua wat staten al dan niet mogen doen ten opzichte van mensenrechten in het cyberdomein?

4.1. Aanvallen

Ter bevordering van de internationale veiligheid bevat het internationaal recht enkele fundamentele principes die zijn vastgelegd in het Handvest van de VN. Het gaat om het non-interventie principe en het verbod op het dreigen met, of gebruiken van, geweld.[198] Het soevereiniteitsbeginsel (staten hebben exclusieve autoriteit over de politieke, sociale, culturele, economische en juridische orde)[199] ligt ten grondslag aan het non-interventieprincipe.[200] Voor zowel het verbod op illegale interventie als het verbod op het gebruik van geweld bestaan twee uitzonderingen. Ten eerste is er geen sprake van schending van een internationale wettelijke verplichting wanneer de VN-Veiligheidsraad (hierna: Veiligheidsraad) een (cyber)operatie autoriseert. Ten tweede hebben staten de mogelijkheid om zich te beroepen op het recht op zelfverdediging (zie 4.2). Wanneer een (cyber)operatie gecategoriseerd moet worden als schending van een van deze fundamentele principes is contextueel. In de paragrafen die volgen wordt inzichtelijk gemaakt wat volgens het huidig internationaal recht verboden, verplicht en toegestaan is, in het bijzonder met betrekking tot spionage, sabotage en beïnvloeding. Hierbij komende de volgende punten aan bod:

- De correcte toepassing van het verbod op het gebruik van geweld in het cyberdomein is omstreden, vanwege de nieuwe mogelijkheden voor oorlogsvoering. Zowel staten als academici verschillen van mening over wat 'cybergeweld' precies inhoudt en of dit fysieke

[197] Blok (2018), *Toespraak minister Blok over 1-jarig bestaan Tallinn Manual 2.0*.
[198] VN Handvest, art. 2(1) en art. 2(4).
[199] Schmitt (2017), *Tallinn Manual 2.0*, p. 11.
[200] De status van het soevereiniteitsprincipe (m.b.t. het cyberdomein) wordt echter betwist door sommigen. Zo beargumenteert de VS dat soevereiniteit ten grondslag ligt aan het internationaal recht, maar dat het desalniettemin een abstract principe is waaruit geen bindende regels voortvloeien. De Tallinn Manual onderstreept deze interpretatie van het soevereiniteitsbeginsel niet. Zie: Väljataga (2018), *Tracing Opinio Juris*, p. 5, Sander (2019), *The Sound of Silence*, p. 18.

gevolgen moet hebben.[201] Hierdoor is het lastig om vast te stellen wanneer een cyberoperatie geclassificeerd moet worden als *geweld* of *gewapende aanval*, en dus wanneer staten aanspraak kunnen maken op het recht op zelfverdediging;

- Spionage in vredestijd is niet verboden volgens het internationaal recht. Slechts de manier waarop cyberspionage ingezet wordt, kan onrechtmatig zijn;
- De rechtmatigheid van een cyberoperatie die zich manifesteert op het grondgebied van een soevereine staat wordt beoordeeld op basis van: (1) de mate van inbreuk op de integriteit van de aangevallen staat, en (2) of er sprake is van inmenging binnen inherente overheidsfuncties;
- Om te spreken van een illegale interventie is het nodig om vast te stellen dat er sprake is van *opzet* en *dwang.* Dit leidt ertoe dat het lastig is om cyberbeïnvloedingsoperaties, waarbij sprake is van beïnvloeding in plaats van dwang, als illegale interventie aan te duiden.

Cyberspionage

Het internationaal recht bevat geen verbod op spionage in vredestijd. Desalniettemin blijkt uit statenpraktijk dat staten het recht hebben om individuen die worden betrapt op het uitvoeren van spionage-operaties te vervolgen, of andere (diplomatieke) maatregelen te nemen tegen de verantwoordelijke staat.[202] Cyberspionage wordt in de Tallinn Manual gedefinieerd als "elke handeling die in het geheim of onder valse voorwendselen wordt ondernomen, waarbij gebruik wordt gemaakt van cybercapaciteiten om informatie te (proberen te) verzamelen."[203] Volgens Kilovaty is het echter een misvatting dat *cyber*spionage een simpele 'uitbreiding' is van traditionele spionagepraktijken. Cyberspionage is niet gelimiteerd door geografische afstand en maakt massa-infiltratie mogelijk op een ongekende schaal.[204] Het internationaal recht reflecteert deze nieuwe realiteit echter (nog) niet[205] en dus stelt ook de Tallinn Manual dat slechts de methode waarop cyberspionage ingezet wordt onrechtmatig kan zijn.[206] Wanneer dat het geval is, is ook de cyberspionage operatie zelf onrechtmatig.

In de praktijk wordt er (in ieder geval de laatste jaren) een onderscheid gemaakt tussen politiek-militaire en economisch-technologische spionage.[207] Het verschil wordt duidelijk wanneer gelet wordt op de motivatie achter de spionageoperatie. Wanneer gespioneerd wordt met als doel

---

[201] Van den Bosch (2019), *Oorlog Voeren Zonder Geweld*, p. 17.

[202] Sulmasy & Yoo (2007), *Counterintuitive: Intelligence Operations and International Law*, p. 627, Lotrionte (2014), *Countering State-Sponsored Cyber Economic Espionage*, p. 460.

[203] Schmitt (2017), *Tallinn Manual 2.0*, p. 168.

[204] Kilovaty (2016), *World Wide Web of Exploitations*, p. 53.

[205] Hoewel internationale discussies over (de gevolgen van) cyberspionage worden gevoerd, zijn de Tallinn experts het erover eens dat er sprake is van onvoldoende *state practice* en *opinio juris* om te stellen dat er een nieuwe norm van gewoonterecht is ontstaan. Een aantal staten heeft zelfs hun veiligheidsdienst wettelijk gemachtigd om cyberspionage operaties uit te voeren. Zie: Schmitt (2017), *Tallinn Manual 2.0*, p. 169.

[206] De meerderheid van de Tallinn experts is van mening dat een cyberspionage operatie onrechtmatig is wanneer deze onderdeel is van een grotere cyberoperatie die het non-interventieprincipe of het verbod op het gebruiken van/dreigen met geweld schendt. Wanneer een cyberspionage operatie onvoorziene consequenties heeft, zoals het wegvallen van functionaliteit van kritieke infrastructuren, kan deze operatie ook als onrechtmatig worden beoordeeld. Een cyberspionage operatie die bijvoorbeeld het mensenrecht op privacy schendt, is onrechtmatig. Wanneer politiek-militaire informatie vergaard d.m.v. een cyberspionage operatie wordt gebruikt om later een traditioneel kinetische aanval uit te voeren (dus zonder cybermiddelen), moeten de cyberoperatie en de aanval afzonderlijk van elkaar beoordeeld worden. Zie: Schmitt (2017), *Tallinn Manual 2.0*, p. 170-172.

[207] Lotrionte (2014), *Countering State-Sponsored Cyber Economic Espionage*, p. 459.

het vergaren van inlichtingen voor de nationale veiligheid, is er sprake van politiek-militaire spionage. Wanneer de operatie echter bedoeld is om een financieel concurrentievoordeel te behalen door bijvoorbeeld intellectuele eigendommen te stelen, dan wordt er gesproken over economisch-technologische spionage. Het verbod op het verzamelen van informatie ter verrijking van nationale bedrijven en economie lijkt, op aansporen van de VS, vanaf 2015 te worden geaccepteerd.[208] In een aantal bilaterale en multilaterale overeenkomsten stellen onder andere de VS, het VK, China en G20-leden dat zij geen economische cyberspionage operaties zullen uitvoeren.[209]

Cybersabotage

De rechtmatigheid van cyberoperaties die zich manifesteren op het grondgebied van een soevereine staat wordt door de Tallinn experts beoordeeld op basis van: (1) de mate van inbreuk op de integriteit van de aangevallen staat, en (2) of er sprake is van inmenging in inherente overheidsfuncties. Wat betreft inbreuk op de integriteit van een aangevallen staat wordt gelet op fysieke schade, verlies van functionaliteit en inbreuk die de ondergrens van verlies van functionaliteit niet bereikt.[210] De meerderheid van de experts is van mening dat cyberoperaties die resulteren in fysieke schade of verlies van functionaliteit een schending van de soevereiniteit betreffen. Er is geen consensus over wanneer of 'hoeveel' functionaliteitsverlies precies nodig is om te spreken van een schending. Deze ondergrens is dus onbeslist.[211] De experts zijn het daarnaast eens dat cyberoperaties die interfereren met gegevens of diensten die gebruikt worden voor de uitoefening van inherente overheidsfuncties het soevereiniteitsprincipe schenden, ongeacht of de operatie leidt tot fysieke schade of verlies van functionaliteit.[212]

Wanneer een cybersabotage operatie bedoeld is om een andere staat zijn keuzevrijheid te ontnemen en die staat te dwingen om op een bepaalde manier te handelen, dan is er sprake van illegale interventie.[213] Niet alleen operaties die fysieke gevolgen hebben kunnen geclassificeerd worden als illegale interventie: wanneer er sprake is van *dwang* en *opzet* schendt een operatie het non-interventieprincipe.[214] Met andere woorden: een cybersabotage operatie die opzettelijk door een staat wordt uitgevoerd om ervoor te zorgen dat een andere staat gedwongen wordt om bijvoorbeeld zijn buitenlandbeleid aan te passen, schendt het non-interventieprincipe. Of de operatie het doel bereikt is onbelangrijk.[215] Het kan desalniettemin lastig zijn om een onderscheid te maken tussen dwingende en niet-dwingende cyberoperaties.[216]

Cyberbeïnvloeding

---

[208] Rascoff (2016), *The Norm against Economic Espionage*, p. 250.
[209] Nakashima & Mufson (2015), *The U.S. and China Agree*, Nakashima (2015), *World's Richest Nations Agree*, UK-China Joint Statement 2015: https://www.gov.uk/government/news/uk-china-joint-statement-2015.
[210] Schmitt (2017), *Tallinn Manual 2.0*, p. 20.
[211] Schmitt (2017), *Tallinn Manual 2.0*, p. 20-21.
[212] Schmitt (2017), *Tallinn Manual 2.0*, p. 22.
[213] Schmitt (2017), *Tallinn Manual 2.0*, p. 317.
[214] Schmitt (2017), *Tallinn Manual 2.0*, p. 318.
[215] Schmitt (2017), *Tallinn Manual 2.0*, p. 322.
[216] Het kan desalniettemin lastig zijn om een onderscheid te maken tussen dwingende en niet-dwingende operaties. 'Dwang' wordt namelijk niet gedefinieerd in internationaal recht. De Tallinn experts zijn het echter eens dat het gebruik van cybergeweld door een staat tegen een andere staat per definitie een dwingende operatie is en dus als illegale interventie telt. Schmitt (2017), *Tallinn Manual 2.0*, p. 317-319.

Cyberbeïnvloedingsoperaties resulteren in het algemeen niet in fysieke schade of verlies van functionaliteit van kritieke infrastructuren.[217] Derhalve konden de Tallinn experts het niet eens worden over de vraag of beïnvloedingsoperaties en andere cyberoperaties die geen fysieke schade als gevolg hebben, ook het soevereiniteitsprincipe kunnen schenden.[218] Duncan Hollis schrijft dat er weinig precedent bestaat voor het classificeren van de puur cognitieve effecten van beïnvloedingsoperaties als een inbreuk op soevereiniteit.[219] Michael Schmitt concludeert dat cyberbeïnvloedingsoperaties in een grijze zone vallen wat betreft het schenden van territoriale integriteit.[220] Desalniettemin beargumenteert Schmitt dat cyberoperaties waarbij niet-publieke informatie wordt gehackt en gelekt op kritieke momenten in een verkiezing, evenals operaties waarbij "legers van trollen met valse identiteiten" worden ingezet, ernstiger zijn dan andere beïnvloedingscampagnes.[221] Volgens Schmitt is er in dit soort gevallen sprake van "*weaponization*" van data en informatie:[222] het classificeren van dit soort operaties als schending van het soevereiniteitsprincipe zou daarom enigszins te ondersteunen zijn.[223]

Zoals hierboven al werd beschreven, wordt er in het internationaal recht een duidelijk onderscheid gemaakt tussen dwang en beïnvloeding. Dit maakt het lastig om (cyber)beïnvloedingsoperaties te classificeren als illegale interventie. Het doel van beïnvloedingsoperaties is, uiteraard, het *beïnvloeden* van het doelwit, en dus niet het onder dwang opleggen van een bepaalde onvrijwillige handeling.[224] De laatste jaren is er onder academici echter meer steun voor het oprekken van de betekenis van 'dwang'. Dit zou betekenen dat een handeling of operatie die het gezag van een staat verstoort, compromitteert of verzwakt ook als illegale interventie wordt gezien.[225] Volgens deze meer uitgebreide benadering van dwang zouden slechts handelingen die verwaarloosbaar impact op de autoriteit van een staat hebben, geclassificeerd moeten worden als **niet**-dwingend. Buchan stelt dat dit bijvoorbeeld operaties zijn die alleen ongemak veroorzaken: alle cyber(beïnvloedings)operaties die méér dan ongemak veroorzaken zouden dan gekarakteriseerd kunnen worden als illegale interventie.[226]

Misbruik digitale infrastructuur

Aangezien is gebleken dat de Nederlandse internetinfrastructuur regelmatig door andere staten of staatsgelieerde actoren wordt gebruikt voor het uitvoeren van cyberoperaties gericht tegen derde staten (zie hoofdstuk 3), wordt hier kort de bespreking van de Tallinn experts over misbruik van digitale infrastructuren uiteengezet.

Een staat mag niet bewust toestaan dat de nationale cyberinfrastructuur, die zich op zijn grondgebied of onder exclusieve overheidscontrole bevindt, wordt gebruikt voor handelingen die andere staten nadelig of onrechtmatig treffen.[227] Het internationaal recht verplicht staten dus om

---

[217] Sander (2019), *The Sound of Silence*, p. 19.
[218] Schmitt (2017), *Tallinn Manual 2.0*, p. 21.
[219] Duncan Hollis in Sander (2019), *The Sound of Silence*, p. 19.
[220] Schmitt (2018), *Virtual Disenfranchisement*, p. 45.
[221] Sander (2019), *The Sound of Silence*, p. 20.
[222] Met 'weaponization' wordt bedoeld dat het verspreiden van desinformatie gebruikt kan worden als een strategisch instrument en staten dus minder (vergeleken met vroeger) afhankelijk zijn van traditionele wapens om strategische doelen te behalen. Zie: Kilovaty (2016), *World Wide Web of Exploitations*, p. 52.
[223] Schmitt (2018), *Virtual Disenfranchisement*, p. 47.
[224] Sander (2019), *The Sound of Silence*, p. 21.
[225] Sander (2019), *The Sound of Silence*, p. 22.
[226] Russell Buchan in Sander (2019), *The Sound of Silence*, p. 23.
[227] Schmitt (2017), *Tallinn Manual 2.0*, p. 33.

passende maatregelen te nemen om de rechten van andere staten te beschermen, dit is het *due diligence* principe.[228] De Tallinn experts stellen dat *due diligence* van toepassing is op een staat door wiens infrastructuur de cyberoperatie wordt doorgevoerd als de staat op de hoogte is van de kwaadaardige activiteit en in staat is om adequate maatregelen te treffen om een einde aan de operatie te maken.[229] Een schending van het *due diligence* principe kan leiden tot staatsaansprakelijkheid.

Daarnaast zijn de Tallinn experts het erover eens dat het feit dat een cyberoperatie is gerouteerd via de cyberinfrastructuur van staat X niet voldoende bewijs is om de operatie aan staat X toe te schrijven.[230] In een dergelijke situatie kan niet worden aangenomen dat staat X betrokken is bij de cyberoperatie.[231]

4.2. Respons op aanvallen

Het internationaal recht biedt meerdere mogelijkheden voor staten om te reageren op een onrechtmatige cyberoperatie waarvan zij het doelwit zijn. Middels diplomatieke of juridische procedures kan geschillenbeslechting worden toegepast. Handelingen die door individuen worden gepleegd kunnen strafbaar worden gesteld en vervolgd binnen de grenzen van het internationaal en toepasselijk nationaal recht. In de paragrafen die volgen worden alleen de regels besproken die van toepassing zijn op maatregelen die staten kunnen besluiten in te zetten zonder dat de dader daarmee akkoord hoeft te gaan (wat bijvoorbeeld het geval is bij vreedzame geschillenbeslechting). Een voorbeeld van een dergelijke maatregel is een *hackback*, waarbij sprake is van actieve cyberverdediging door bijvoorbeeld het systeem van de hacker te beschadigen.[232] Hierbij komen de volgende regels aan bod (juridische termen worden in de loop van de tekst uiteengezet):

- Staten hebben te allen tijde de mogelijkheid om te reageren op cyberoperaties met bijvoorbeeld het opleggen van sancties en het beperken van diplomatieke banden. Dit type maatregelen wordt in het internationaal recht aangeduid als 'retorsie';
- Wanneer een cyberoperatie het non-interventie principe of het geweldsverbod schendt zonder dat daarbij sprake is van een gewapende aanval (*armed attack),* heeft de benadeelde staat de mogelijkheid om een tegenmaatregel in te zetten. Aangezien een tegenmaatregel in principe een internationaal onrechtmatige daad is, moet de maatregel aan bepaalde criteria voldoen om rechtmatig geacht te worden;

[228] Schmitt (2017), *Tallinn Manual 2.0*, p. 33, Internationaal Gerechtshof (1980), United States Diplomatic and Consular Staff in Tehran (*United States of America* v. *Iran*), paras. 67-68.
[229] Schmitt (2017), *Tallinn Manual 2.0*, p. 33.
[230] Schmitt (2017), *Tallinn Manual 2.0*, p. 40.
[231] Ten tijde van een gewapend conflict gelden andere regels en kan de neutraliteit van een staat wiens cyberinfrastructuur gebruikt wordt voor het uitvoeren van cyberoperaties in het geding komen. Zie Wet van Neutraliteit. De regels en normen die in dit hoofdstuk besproken worden zijn gebaseerd op het internationaal publieksrecht. Wanneer het humanitair oorlogsrecht van kracht is, gelden andere, meer specifieke regels waarbij niet gelet wordt op het soevereiniteits- of non-interventieprincipe maar vooral aandacht wordt besteed aan het beschermen van burgers. Het is tijdens een gewapend conflict bijvoorbeeld verboden om een (cyber)aanval op een ziekenhuis uit te voeren. Er wordt over het algemeen van uitgegaan dat dezelfde normen in vredestijd gelden, maar afhankelijk zijn van de interpretatie van een ander regime. Zo zou een cyberaanval van een staat op een ziekenhuis geclassificeerd kunnen worden als een overtreding van het verbod op het gebruik van geweld.
[232] Zie bijvoorbeeld: Schweighofer et al. (2020), *Malicious Cyber Operations*, p. 227.

- Wanneer er sprake is van noodzakelijkheid mag een aangevallen staat maatregelen nemen om de dreiging tegen te gaan, zonder dat daarbij vastgesteld moet worden dat de operatie daadwerkelijk is uitgevoerd door een andere staat. Het is voldoende wanneer is vastgesteld dat de dreiging afkomstig is van het grondgebied van een staat;
- Wanneer een cyberoperatie wordt geclassificeerd als gewapende aanval heeft de benadeelde staat het recht om zichzelf (individueel of in collectief verband) te verdedigen.

Retorsie

Retorsie omvat elk 'onvriendelijk' gedrag dat niet in strijd is met de internationale rechtsplichten van alle betrokken staten. Voorbeelden zijn het verbieden of beperken van normale diplomatieke betrekkingen of andere contacten, verscheidene soorten embargo's of het intrekken van vrijwillige hulpprogramma's.[233] Sancties worden ook vaak ingezet als vorm van retorsie. Dergelijke acties zijn legaal zolang ze niet onverenigbaar zijn met een internationale verplichting. Staten en intergouvernementele organisaties mogen retorsie individueel of in collectief verband inzetten (in respons op cyberoperaties).

Tegenmaatregelen

De tegenmaatregel-doctrine geeft een staat wiens rechten door een andere staat zijn geschonden de mogelijkheid om een maatregel in te zetten die in normale omstandigheden wordt geclassificeerd als internationaal onrechtmatige daad. Tegenmaatregelen vormen een horizontaal handhavingsmechanisme en worden niet geautoriseerd of beoordeeld door een onafhankelijke organisatie.[234] Tegenmaatregelen mogen echter alleen genomen worden wanneer voldaan wordt aan vijf condities:[235]

(1) de tegenmaatregel wordt ingezet tegen een staat die verantwoordelijk is voor een internationaal onrechtmatige daad,[236]

(2) de tegenmaatregel wordt alleen ingezet zolang de verantwoordelijke staat zijn verplichtingen niet nakomt,[237]

(3) de tegenmaatregel is proportioneel,[238]

(4) alvorens het nemen van de tegenmaatregel maakt de benadeelde staat kenbaar aan de verantwoordelijke staat dat deze van plan is om een tegenmaatregel in te zetten (tenzij er sprake is van noodzaak),[239]

---

[233] Articles on State Responsibility, Chapter II of Part 3, para. 3 of Commentary.

[234] Ter contrast: tegenmaatregelen die genomen worden in reactie op een dispuut m.b.t. een Wereld Handels Organisatie-verdrag, moeten eerst worden geautoriseerd door de Raad voor geschillenbeslechting (dit is een *verticaal* handhavingsmechanisme). Zie: Fitzgerald (2016), *Helping States Help Themselves*, p. 77.

[235] Er bestaat dus een kans dat, wanneer het dispuut voor het Internationaal Gerechtshof wordt gebracht, het Hof besluit dat een staat zich niet aan de voorwaarden heeft gehouden en zich dus alsnog schuldig heeft gemaakt aan het uitvoeren van een onrechtmatige daad. Zie bijvoorbeeld: Internationaal Gerechtshof (1997). *Gabcikovo-Nagymaros Project (Hungary/Slovakia),* Judgment, I.C.J. Reports.

[236] Responsibility of States for Internationally Wrongful Acts (2001), art. 49(1).

[237] Responsibility of States for Internationally Wrongful Acts (2001), art. 49(2).

[238] Responsibility of States for Internationally Wrongful Acts (2001), art. 51.

[239] In bepaalde omstandigheden kan het echter nodig zijn dat een benadeelde staat onmiddellijk handelt om verdere schade te voorkomen. Wanneer zo'n situatie zich voordoet, kan deze staat tegenmaatregelen nemen zonder zijn voornemen daartoe te melden. Dit geldt ook wanneer kennisgeving van het voornemen om tegenmaatregelen te nemen die maatregel zinloos zou maken. Responsibility of States for Internationally Wrongful Acts (2001), art. 52(1), Schmitt (2017), *Tallinn Manual 2.0*, p. 120.

(5) de tegenmaatregel bestaat niet uit het dreigen met/gebruiken van geweld, schendt geen fundamentele mensenrechten, komt niet neer op represailles die onder het humanitair oorlogsrecht verboden zijn, of is in strijd met internationaal afgesproken normen waarvan *nooit* afgeweken mag worden[240] (zogenaamde *jus cogens* normen).[241]

Met betrekking tot het cyberdomein kan het lastig zijn om aan deze voorwaarden te voldoen, vooral vanwege het gebrek aan duidelijke definities. Corn en Jensen beargumenteren dat de restricties verbonden aan tegenmaatregelen ertoe zouden kunnen leiden dat staten eerder geneigd zijn om 'onvriendelijke' cyberoperaties te kwalificeren als daad van geweld of gewapende aanval, omdat ze dan kunnen reageren vanuit zelfverdediging.[242]

Noodzakelijkheid

Staten kunnen zich beroepen op de *plea of necessity*, zoals die wordt genoemd in de Artikelen inzake Staatsaansprakelijkheid. Er zijn twee criteria verbonden aan de mogelijkheid om een maatregel die in principe onrechtmatig is, in te zetten gebaseerd op noodzakelijkheid. Ten eerste moet de maatregel de enige optie bieden voor de staat om een wezenlijk belang te beschermen tegen een ernstig en dreigend gevaar. Ten tweede mag de maatregel een wezenlijk belang van de staat of staten waartegen deze wordt ingezet, of van de internationale gemeenschap als geheel, niet ernstig schaden.[243] Daarnaast mag de staat die de maatregel wil inzetten zelf niet hebben bijgedragen aan de noodsituatie.[244]

Zelfverdediging

Het recht op (individueel en collectieve) zelfverdediging is vastgelegd in artikel 51 van het VN-Handvest. Een rechtmatige uitoefening van het recht op zelfverdediging in reactie op activiteiten in het cyberdomein moet aan drie voorwaarden voldoen. Ten eerste moet het een reactie zijn op een cyberoperatie die geclassificeerd kan worden als gewapende aanval. Ten tweede moet de reactie noodzakelijk en proportioneel zijn. Ten derde moet de reactie gerapporteerd worden aan de Veiligheidsraad en gestopt worden wanneer de Veiligheidsraad maatregelen ter handhaving van de internationale vrede en veiligheid heeft genomen.[245]

4.3. Online mensenrechten

In zowel de academische wereld als de internationale politieke arena is er consensus dat mensenrechten zowel offline als online gelden.[246] Dit gegeven is onderschreven door de VN-Mensenrechtenraad (hierna: Mensenrechtenraad), de VN-Algemene Vergadering (hierna: Algemene Vergadering) en door verschillende staten. In 2003 hebben 180 staten, waaronder China en Rusland, bevestigd dat de Universele Verklaring van de Rechten van de Mens (UVRM) volledig toepasbaar is online.[247] In resoluties van de Mensenrechtenraad uit 2012, 2014, 2016 en 2018 wordt expliciet

[240] Responsibility of States for Internationally Wrongful Acts (2001), art. 50(1).
[241] O.a. Genocide, marteling, slavernij.
[242] Corn & Jensen (2018), *The Use of Force and Cyber Countermeasures*, p. 129.
[243] Responsibility of States for Internationally Wrongful Acts (2001), art. 25(1).
[244] Responsibility of States for Internationally Wrongful Acts (2001), art. 25(2).
[245] VN Handvest, art. 51.
[246] Mačák (2017), *From Cyber Norms to Cyber Rules*, p. 885.
[247] Declaration of Principles, World Summit on the Information Society, Gabor & Aarons (2016), *State Responsibility to Respect*, p. 504-505.

benoemd dat dezelfde rechten die mensen offline genieten ook online moeten worden beschermd.[248] Zoals ook beschreven in paragraaf 3.1.1 bestaat er echter een discussie over de inhoud en reikwijdte van de toepassing van mensenrechtenverdragen in het cyberdomein, in het bijzonder over de vraag of toegang tot informatie een mensenrecht is of een kwestie van nationale veiligheid.[249]

Sommige staten stellen dat toegang tot het internet een online mensenrecht is.[250] Een resolutie van de Mensenrechtenraad uit 2016 veroordeelt staten die moedwillig hun burgers afschermen van toegang tot het vrije internet. Hoewel meer dan zeventig staten instemden met deze niet-bindende resolutie, weigerden onder andere China, Rusland, Zuid-Afrika en India de resolutie te bekrachtigen. De inwoners van deze staten vormen echter het grootste deel van het totale aantal internetgebruikers.[251]

De discussie over de toepassing van mensenrechten binnen het cyberdomein concentreert zich voornamelijk rondom twee vragen. Deze vragen gaan over de verhouding tussen mensenrechten en soevereiniteit en de extraterritoriale applicatie van mensenrechten. In de volgende paragrafen worden deze twee discussies uiteengezet. Ook wordt uiteengezet welke harde regels en zachte normen met betrekking tot online mensenrechten zijn ontstaan, en hoe deze verschillen per regio. Daarmee zal inzichtelijk worden hoe het internationaal recht bepaalt wat staten al dan niet mogen doen ten opzichte van mensenrechten in het cyberdomein. Hierbij zullen de volgende punten aan bod komen:

- Ondanks de algemene consensus dat mensenrechten online gelden zijn staten het oneens over de toepassing van het recht op activiteiten in het cyberdomein;
- Sommige academici pleiten voor een *personal model* van jurisdictie in plaats van jurisdictie gebaseerd op territoriale controle, aangezien staten door nieuwe technologieën niet fysiek dichtbij of aanwezig hoeven te zijn om controle te kunnen uitoefenen over individuen;
- Multilaterale en regionale verdragen zijn in belang toegenomen. De verdragen waar Nederland lid van is, stellen striktere richtlijnen voor het tijdelijk opschorten van mensenrechten dan andere regionale verdragen;
- Australië, de VS en EU-lidstaten baseren hun cyberstrategie voornamelijk op zachte recht-*standaarden* zoals regionale richtlijnen en afspraken.

Soevereiniteit

Wanneer discussies over online mensenrechten plaatsvinden, vallen met name China en Rusland terug op argumenten gebaseerd op soevereiniteit. De door China geïntroduceerde term 'internetsoevereiniteit' stelt dat staten het recht hebben om complete controle uit te oefenen over het cyberdomein binnen hun landsgrenzen. Mensenrechten zouden volgens China en Rusland ondergeschikt zijn.[252] Het idee van 'internetsoevereiniteit' wordt ondertussen door China gepresenteerd als de beste manier om digitale belangen veilig te stellen.[253] China stimuleert dit idee

[248] Mačák (2017), *From Cyber Norms to Cyber Rules*, p. 884.
[249] Shandler & Canetti (2019), *A Reality of Vulnerability and Dependence*, p. 78, Gabor & Aarons (2016), *State Responsibility to Respect*, p. 503-504, Maurer (2018), *Cyber Mercenaries*, p. 6.
[250] Onder andere Spanje, Frankrijk, Finland, Costa Rica en Griekenland hebben erkend dat hun burgers recht hebben op toegang tot het internet.
[251] Shackelford (2019), *Should Cybersecurity be a Human Right* p. 166.
[252] Schmitt & Vihul (2017), *Sovereignty in Cyberspace*, p. 214.
[253] McKune & Ahmed (2018), *Authoritarian Practices in the Digital Age*, p. 3835.

zo actief bij andere staten dat sommige academici stellen dat er een mogelijkheid bestaat dat er een nieuwe internationale norm ontstaat, waarbij soevereiniteit boven mensenrechtelijke belangen komen te staan. Aangezien het cyberdomein en cybernormen nog volop in ontwikkeling zijn, kunnen volgens sommige auteurs de ontwikkeling van een dergelijke nieuwe norm en de bijbehorende acties van staten snel impact hebben op het gewoonterecht.[254] Dit kan vergaande gevolgen hebben voor de bescherming van de online mensenrechten wereldwijd. Met name voor burgers van staten waar internetsoevereiniteit is geaccepteerd, maar potentieel ook voor burgers wiens online mensenrechten wel gerespecteerd worden door hun eigen staat.[255]

Het soevereiniteitsprincipe is ook gericht op het tegenhouden van buitenlandse invloeden. China stelt dat er een verbod bestaat op het schenden van internetsoevereiniteit van andere staten. China heeft deze positie bekrachtigd middels de Wuzhen Verklaring uit 2014, waarin de Chinese overheid stelt dat alle staten elkaars rechten op de ontwikkeling, het gebruik en bestuur van het cyberdomein moeten respecteren.[256] De meeste westerse staten nemen een andere positie in ten opzichte van 'internetsoevereiniteit'. De VS en VK stellen zelfs dat soevereiniteit een abstract principe is waaruit geen bindende publieksrechtelijke regels voortvloeien.[257]

Extraterritorialiteitsprincipe

In de internationale gemeenschap wordt ook gedebatteerd over de extraterritoriale toepassing van mensenrechten. Dit heeft betrekking op de vraag of staten verplicht zijn de online mensenrechten te respecteren van individuen die zich in het buitenland bevinden.[258] Volgens artikel 2(1) van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) moeten lidstaten erop toezien dat de rechten van individuen binnen hun jurisdictie worden bewaakt.[259] Dit is bekrachtigd door uitspraken van het VN-Mensenrechtencomité en het Europese Hof voor de Rechten van de Mens (EHRM), waarin wordt gesteld dat staten mensenrechten moeten beschermen binnen gebieden onder hun effectieve controle.[260] De Verenigde Staten en Israël spreken echter tegen dat het IVBPR hen verplicht toe te zien op de extraterritoriale applicatie van mensenrechten.[261]

Volgens academici hebben nieuwe technologieën de toepassing van het IVBPR in het cyberdomein minder relevant gemaakt: veel van deze nieuwe technologieën kunnen ingezet worden zonder dat er territoriale controle nodig is, maar hebben wel grote impact op individuele

---

[254] Het gewoonterecht is gebaseerd op de handelingen en gewoonten van staten. Een regel binnen het gewoonterecht kan worden gecreëerd op basis van consistente statenpraktijk en uitgesproken aanvaarding van recht (opinio juris) van verschillende staten. Zie: Thirlway (2015), *Human Rights in Customary Law*, p. 496.

[255] McKune & Ahmed (2018), *Authoritarian Practices in the Digital Age*, p. 3849.

[256] Creemers (2020), *China's Conception of Cyber Sovereignty*, p. 114.

[257] Schmitt & Vihul (2017), *Sovereignty in Cyberspace*, p. 214, Väljataga (2018), *Tracing Opinio Juris*, p. 7.

[258] Kilovaty (2020), *An Extraterritorial Human Right*, p. 37.

[259] Watt (2017), *The Role of International Human Rights Law,* p. 6, Kilovaty (2020), *An Extraterritorial Human Right*, p. 34.

[260] Kilovaty (2020), *An Extraterritorial Human Right*, p. 44, Gabor & Aarons (2016), *State Responsibility to Respect*, p. 507, Human Rights Committee (2004), General Comment No. 31: "The Nature of the General Legal Obligations Imposed on States Parties to the Covenant", para. 10, European Court of Human Rights (1995), Loizidou v. Turkey (Preliminary Objections), paras. 61-62.

[261] Heupel (2020), *Indirect Accountability*, p. 173, Chauhan (2019), *A Causal Model*, p. 108, Watt (2017), *The Role of International Human Rights Law,* p. 7, Gabor & Aarons (2016), *State Responsibility to Respect*, p. 507.
Het is onduidelijk wat 'effectieve controle' binnen het cyberdomein inhoudt. Zo bestaat er geen consensus over de vraag of er sprake kan zijn van effectieve controle wanneer handelingen in het cyberdomein plaatsvinden zonder een uitvoering van fysieke controle. Zie: Kilovaty (2020), *An Extraterritorial Human Right*, p. 44.

mensenrechten.[262] Om die reden beargumenteren academici dat het extraterritorialiteitsprincipe, gebaseerd op territoriale jurisdictie, in zekere zin niet meer is opgewassen tegen de enorme schaal waarop, en het gemak waarmee, mensenrechten te schenden zijn.[263] Organisaties als de Amerikaanse *National Security Agency* (NSA) kunnen middels deze nieuwe technologieën controle uitoefenen over de communicatie van burgers van andere staten, zonder daar fysiek bij aanwezig te zijn. Dit doen zij door middel van het afluisteren en filteren van online communicatie, het aanpassen van online informatie, en het doorbreken van vergevorderde encryptie methodes.[264] Mensenrechtenactivisten pleiten daarom voor een *personal model* van jurisdictie, waarbij de nadruk ligt op de digitale controle van staten over een individu in plaats van dat er sprake moet zijn van territoriale controle.[265]

Harde rechtsregels versus zachte normen

Volgens Schmitt worden bepaalde provisies uit de UVRM en het IVBPR gezien als onderdeel van internationaal gewoonterecht. Echter bestaat er geen definitieve uiteenzetting van welke mensenrechtenprincipes onder het gewoonterecht vallen. Daarnaast zijn niet alle staten lid van dezelfde mensenrechtenverdragen of zijn ze het niet eens over de toepassing en reikwijdte daarvan.[266] Door het gebrek aan consensus over de regels die onder het gewoonterecht vallen en de extraterritoriale toepassing van mensenrechten zijn bilaterale en multilaterale verdragen en afspraken in belang toegenomen.[267]

Verschillende multilaterale verdragen stellen echter andere eisen. Zo staat het Amerikaanse Verdrag inzake de Rechten van de Mens een bredere interpretatie van de dreiging voor de nationale veiligheid toe dan bijvoorbeeld het IVBPR en het Europees Verdrag voor de Rechten van de Mens.[268] Deze twee verdragen, waarvan Nederland beide lid is, stellen dat staten mensenrechten van ieder individu binnen hun jurisdictie moeten beschermen en garanderen. Hierbij moeten staten ook stappen nemen om mensenrechtenschendingen door andere staten binnen hun eigen grondgebied te voorkomen.[269] Als lid van deze verdragen kan Nederland dus niet alleen verantwoordelijk gehouden worden voor de online mensenrechtenschendingen door eigen toedoen, maar ook voor de acties van private personen, instituties en andere staten die plaatsvinden binnen de Nederlandse landsgrenzen. Dit is het *due diligence* principe (zie paragraaf 4.1): staten worden verwacht haalbare en proportionele maatregelen te treffen om mensenrechten te beschermen.[270]

Het belang van nationale en regionale wetgevende instituten en rechtbanken is ook toegenomen.[271] De Raad van Europa (RvE) heeft recentelijk een verdrag uit 1981, de *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, geüpdatet. Dit is

[262] Watt (2017), *The Role of International Human Rights Law,* p. 10.
[263] Kilovaty (2020), *An Extraterritorial Human Right*, p. 45.
[264] Watt (2017), *The Role of International Human Rights Law,* p. 10.
[265] Watt (2017), *The Role of International Human Rights Law,* p. 8, Kilovaty (2020), *An Extraterritorial Human Right*, p. 51.
[266] Schmitt (2017), *International Human Rights Law*, p. 179-180.
[267] Kilovaty (2020), *An Extraterritorial Human Right*, p. 47.
[268] Schmitt (2017), *International Human Rights Law*, p. 208.
[269] Gabor & Aarons (2016), *State Responsibility to Respect*, p. 506.
[270] Schmitt (2017), *International Human Rights Law*, p. 182, Kilovaty (2020), *An Extraterritorial Human Right*, p. 48-49
[271] Shandler & Canetti (2019), *A Reality of Vulnerability and Dependence*, p. 78.

het eerste juridisch bindende verdrag waarin individuen worden beschermd tegen de gevolgen van het verzamelen van persoonlijke data.[272]

Los van de discussie over welke mensenrechtenprincipes onder het gewoonterecht vallen, bevatten mensenrechtenverdragen duidelijke rechtsregels die burgers beschermen tegen hun eigen overheid. Hierbij moet gedacht worden aan het recht op privacy, de vrijheid van meningsuiting en het recht op een eerlijke rechtsgang.[273] Deze rechten mogen slechts tijdelijk worden opgeschort op momenten dat de nationale veiligheid in het geding is.[274] De verwachting is dan ook dat lidstaten het gros van de tijd hun verdragsverplichtingen nakomen.[275] Zoals uiteengezet in mensenrechtenverdragen moeten staten die zich omwille van de nationale veiligheid genoodzaakt zien tot een (tijdelijke) inperking van mensenrechten aan drie eisen voldoen: (1) de nationale wetgeving moet het uitvoeren van de actie toestaan, (2) de actie moet enkel worden ingezet voor legitieme doeleinden, (3) er moet een assessment worden gemaakt van de noodzakelijkheid en proportionaliteit van de actie.[276]

Door een gebrek aan consensus over de toepassing van mensenrechten in het cyberdomein zijn andere normen in belang toegenomen. Staten hebben meerdere overeenkomsten, die niet voldoen aan de status van een verdrag, ondertekend.[277] Hoewel dit soort normen en afspraken niet-bindend zijn, worden ze door sommigen als meer effectief gezien dan harde rechtsregels.[278] Australië, de VS en EU-lidstaten baseren hun cyberstrategie bijvoorbeeld voornamelijk op zachte recht-*standaarden* zoals regionale richtlijnen en afspraken.[279] Voor Nederland zijn de *EU Human Rights Guidelines on Freedom of Expression Online and Offline* uit 2014 van belang. Deze richtlijnen benadrukken het belang van de bescherming van de vrijheid van meningsuiting online en zetten uiteen hoe en wanneer de vrijheid van meningsuiting online mag worden gelimiteerd.[280] Hoewel de richtlijnen in dit document niet bindend zijn, tonen ze wel een duidelijke politieke uitdrukking van de Europese prioriteiten op het gebied van de online mensenrechten. Samen met de handelingen van staten en de uitgedragen *opinio juris* kunnen deze aanbevelingen in de loop der tijd een onderdeel gaan vormen van Europees (regionaal) gewoonterecht.[281] Dit betekent dat de handelingen van individuele staten zoals Nederland actief bijdragen aan de vestiging van normen. Derhalve wordt van Nederland verwacht dat zij zich houdt aan de zelf naar voren gebrachte uitingen van *opinio juris.*

In een brief naar het Nederlandse parlement heeft het ministerie van Buitenlandse Zaken (BZ) de juridische benadering met betrekking tot activiteiten in het cyberdomein duidelijk uiteengezet.[282] Nederland onderschrijft dat mensenrechten zowel offline als online gelden.

---

[272] Natoli (2019), *Testing the Analogy*, p. 151.
[273] De vrijheid van meningsuiting is echter niet absoluut. Het EHRM heeft bepaald dat de vrijheid van meningsuiting niet mag leiden tot de inperking of vernietiging van andere rechten binnen het Europese Verdrag voor de Rechten van de Mens, Garaudy v. France, 24 June 2003 (decision).
[274] Natoli (2019), *Testing the Analogy*, p. 149.
[275] Kilovaty (2020), *An Extraterritorial Human Right*, p. 46.
[276] Kilovaty (2020), *An Extraterritorial Human Right*, p. 33.
[277] Klimburg & Faesen (2020), *A Balance of Power in Cyberspace*, p. 162.
[278] Belli & Venturini (2016), *Private Ordering and the Rise of Terms of Service*, p. 15, Weber (2012), *Future Design of Cyberspace Law*, p. 3.
[279] Wiking - Häger & Dackö (2017), *Cybersecurity Law Overview*, p. 2.
[280] Council of Europe (2014), *EU Human Rights Guidelines on Freedom of Expression Online and Offline*, Foreign Affairs Council Meeting, Brussels.
[281] Wouters & Hermez (2016), *EU Guidelines on Human Rights*, p. 14
[282] Ministerie van Buitenlandse Zaken (2019). Kamerbrief Inzake Internationale Rechtsorde in het Digitale Domein.

Daarnaast stelt Nederland dat staten zowel de negatieve verplichting hebben om niet zelf mensenrechten te schenden, alsmede de positieve verplichting hebben om mensenrechten van de eigen bevolking te beschermen tegen schendingen door andere actoren. Door herhaaldelijk de nadruk te leggen op een veilig, open en vrij internet staat de juridische positie van Nederland recht tegenover die van staten die soevereiniteit gebruiken als argument om de controle te verkrijgen over mensenrechten online.[283]

[283] Schmitt (2019), *The Netherlands Releases a Tour de Force*.

5. Internationaal beleid

Samenvatting

De bestudeerde literatuur laat zien dat er de afgelopen jaren belangrijke beleidsontwikkelingen hebben plaatsgevonden binnen intergouvernementele organisaties zoals de VN, de EU en de NAVO. De EU nam in 2013 de eerste EU Cyber Security Strategy aan. Sinds 2017 beschikt de EU over een zogeheten *Cyber Diplomacy Toolbox*, die de mogelijkheid biedt om vijf soorten maatregelen te nemen in respons op vijandelijke cyberactiviteiten. Onder deze maatregelen vallen bijvoorbeeld preventieve en samenwerkingsmaatregelen en het opleggen van sancties. In 2019 heeft de EU een actieplan opgezet voor het opsporen, analyseren en tegengaan van desinformatie. Voor zowel de EU als de NAVO heeft het weerbaar maken en beveiligen van hun eigen netwerken, organisatie en missies de hoogste prioriteit. De NAVO erkende het cyberdomein in 2016 als vierde oorlogsdomein (naast land, zee en lucht). Twee jaar eerder werd duidelijk dat de NAVO-lidstaten een beroep kunnen doen op het collectieve verdedigingsmechanisme wanneer een cyberaanval (met effecten vergelijkbaar met die van een gewapende aanval) plaatsvindt. Eind 2017 werd aangekondigd dat de NAVO gebruik zou gaan maken van de offensieve cybercapaciteiten van lidstaten, om de Alliantie beter te beschermen en verdedigen tegen cyberdreigingen. Tegelijkertijd werd verklaard dat er geen offensieve cyberoperaties zullen worden uitgevoerd onder de NAVO-vlag. Verschillende staten hebben publiekelijk verklaard dat ze bereid en in staat zijn om hun cybercapaciteiten beschikbaar te stellen voor de NAVO, waaronder het Verenigd Koninkrijk, de Verenigde Staten, Nederland, Estland en Denemarken.

Het beleid van de VN en de OVSE is voornamelijk gericht op het creëren van cybernormen. Deze normen zouden het gedrag van staten binnen het cyberdomein moeten beïnvloeden, zowel op mondiaal als regionaal niveau. Om dit te bereiken zijn zowel de GGE als de OEWG-werkgroepen opgericht. Nadat in 2015 consensus werd bereikt over elf vrijwillige, niet-bindende normen, is er een duidelijke tweedeling ontstaan tussen de *cybersecurity* en de *information security* kampen. Deze werkgroepen zijn daardoor gepolariseerd geraakt en het bereiken van verdere consensus is uitgebleven.

Staten zijn ook verdeeld wat betreft de ideeën over het beleid omtrent online mensenrechten. Autoritaire staten wijzen naar soevereiniteit en het beschermen van de nationale veiligheid om volledige controle over het cyberdomein te rechtvaardigen; de VS focust op vrijheid van meningsuiting en marktregulering; en de EU neemt een middenpositie in, waarbij de nadruk ligt op het vertrouwen en de veiligheid van burgers. In de laatste jaren heeft binnen de EU een verschuiving plaatsgevonden richting een sterkere rol voor de overheid, met strenge regelgeving op het gebied van privacy en online informatie. De EU en de VN hebben meerdere pogingen ondernomen om beleid te creëren voor de bescherming van online mensenrechten. De EU heeft online mensenrechten geïntegreerd in de Cyber Security Strategy en de *Communication on Resilience, Deterrence and Defense*. De pogingen binnen de VN hebben niet tot substantiële afspraken geleid.

Inleiding internationaal beleid

Niet alleen individuele staten hebben een internationaal cybersecuritybeleid. Ook intergouvernementele organisaties zoals de Verenigde Naties, de Europese Unie en de NAVO houden zich bezig met ontwikkelingen in het cyberdomein en hebben de afgelopen jaren beleid ontwikkeld.

In dit hoofdstuk worden de volgende vragen beantwoord:

- 5.1. Wat zijn de belangrijkste internationale ontwikkelingen in de afgelopen jaren op het gebied van internationaal cybersecuritybeleid van deze organisaties gericht tegen de dreiging van statelijke en daaraan gelieerde actoren?
- 5.1. Hoe zien de belangrijkste internationale beleidsmechanismen eruit?
- 5.2. Wat zijn de belangrijkste internationale ontwikkelingen in de afgelopen jaren op het gebied van mensenrechten in het cyberdomein?

5.1. Cybersecurity

Verscheidene intergouvernementele organisaties waar Nederland bij betrokken is, hebben zich in de afgelopen decennia beziggehouden met cybersecurity in het internationale domein. In de paragrafen die volgen worden de onderstaande punten besproken:

- De Europese Unie nam in 2013 de EU Cyber Security Strategie aan, waar cyberdefensie ook in is opgenomen. Sinds 2017 heeft de EU een zogenaamde *Cyber Diplomacy Toolbox*, die de mogelijkheid biedt om vijf soorten maatregelen, waaronder het opleggen van sancties, te nemen in respons op vijandelijke cyberactiviteiten;
- De NAVO erkende het cyberdomein in 2016 als vierde oorlogsdomein (naast ter land, ter zee en in de lucht).[284] Twee jaar eerder publiceerde de NAVO al een cyberbeleidsdocument waaruit duidelijk werd dat de NAVO-lidstaten een beroep kunnen doen op het collectieve verdedigingsmechanisme wanneer een cyberaanval (met effecten vergelijkbaar met die van een gewapende aanval) plaatsvindt;[285]
- Het beleid van de VN en de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) is gericht op het creëren van cybernormen om zo het gedrag van staten te beïnvloeden, op respectievelijk mondiaal en regionaal niveau.

5.1.1. Europese Unie

In 2013 nam de EU een eerste cyberstrategie aan, getiteld "*An Open, Safe and Secure Cyberspace*." Deze strategie omvat de belangrijkste aspecten van de Europese benadering van cyberdefensie en -security. De EU beschouwt het cyberdomein als een domein waar vrijheid en fundamentele rechten gelden. De EU stelt dat ze dit domein ook zo zal blijven promoten. Hoewel de EU zelf niet actief inzet op het creëren van CBMs en gedragsnormen, stimuleert de organisatie deze initiatieven wel: de EU

[284] Warsaw Summit (2016). Zie: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[285] Pernik (2014), *Improving Cyber Security: NATO and the EU*, p. 6.

is geen voorstander van het creëren van een nieuw internationaal juridisch instrument voor cyberkwesties.[286]

Doel 3 en 5 van de EU-strategie zijn het meest relevant voor internationale cybersecurity.[287] Wat betreft cyberdefensie ligt de focus op het opsporen van, reageren op, en herstellen van cyberdreigingen en -aanvallen. De strategie onderschrijft het belang van het stimuleren van samenwerking tussen de civiele en militaire sector, ondersteuning door onderzoek en meer samenwerking tussen overheden, de private sector en academici binnen de EU. Uit de strategie wordt niet duidelijk wat de EU doet wanneer er een (grootschalige) cyberaanval plaatsvindt. Een belangrijke ontwikkeling op dit gebied is de hernieuwde interpretatie van de 'solidariteitsclausule' (art. 222, Verdrag betreffende de werking van de EU). Deze clausule stelt zowel de Unie als de lidstaten in staat om individueel of in collectief verband actie te ondernemen in respons op een situatie die een ernstige impact kan hebben op mens, milieu of eigendom – en omvat dus een gezamenlijke reactie in geval van een cyberaanval.[288]

Met oog op het behalen van doel 3 van de Strategie werd in 2014 het *Cyber Defense Policy Framework* (CDPF) door de Europese Raad aangenomen.[289] Middels dit document heeft de EU het cyberdomein erkend als oorlogsdomein.[290] Het beleidsraamwerk bestaat uit vijf prioriteiten, zoals het verbeteren van nationale defensiecapaciteiten van lidstaten en het bevorderen van civiel-militaire betrekkingen, om zo de bestaande capaciteitstekorten in de lidstaten aan te pakken en de samenwerking binnen de EU en met internationale spelers versterken.[291] In 2018 werd een geüpdatete CDPF gepubliceerd waarin zes prioriteiten worden benadrukt (waarvan vijf een herhaling van 2014 zijn).[292]

In 2016 kwam de *EU Global Strategy* uit, waarin wordt vermeld dat de EU de politieke, operationele en technische cybersamenwerking tussen lidstaten steunt. Daarnaast wordt gesteld dat de cybersecuritysamenwerking met kernpartners zoals de VS en de NAVO wordt versterkt.[293]

In 2017 werd een beleidsraamwerk aangenomen wat het mogelijk maakt om in collectief EU-verband te reageren op kwaadwillige cyberactiviteiten: de *cyber diplomacy toolbox.* In 2019 stelde de EU het actieplan tegen desinformatie op. Deze beleidsmechanismen worden in de volgende paragrafen besproken.

Cyber diplomacy toolbox

---

[286] European Commission (2013), *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, p. 15.

[287] De Strategie bestaat uit vijf doelen in totaal. Doel drie: "het ontwikkelen van cyberdefensiebeleid en – capaciteiten gerelateerd aan het Common Security and Defense Policy (CSDP)." Doel 5: "het opstellen van een coherent internationaal cyberdomein beleid voor de Europese Unie en het promoten van EU-kernwaarden."

[288] Bendiek & Pander - Maat (2019), *The EU's Regulatory Approach to Cyber-Security*, p. 22.

[289] Van der Meulen et al. (2015), *Cybersecurity in the European Union and Beyond*, p. 55.

[290] Van der Meulen et al. (2015), *Cybersecurity in the European Union and Beyond*, p. 56.

[291] Council of the European Union (2014), *EU Cyber Defence Policy Framework*, p. 4-13.

[292] Ondersteuning van de ontwikkeling van het cyberdefensievermogen van lidstaten; verbetering van de bescherming van CDPF ICT-systemen; bevordering van civiel-militaire betrekkingen; onderzoek en technologie; verbetering van mogelijkheden voor onderwijs, trainingen en oefeningen; verbetering van de samenwerking met relevante internationale partners. Council of the European Union (2018), *EU Cyber Defence Policy Framework,* p. 9-24.

[293] European Union (2016), *Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign and Security Policy*, p. 22.

In 2016, ten tijde van het bekleden van de voorzitterschapsrol van de Raad van de Europese Unie, deed Nederland het voorstel om een gezamenlijke diplomatieke reactie tegen dwingende cyberoperaties te ontwikkelen.[294] Het beleidsraamwerk voor een gezamenlijk Europese reactie op cyberdreigingen en -aanvallen werd in 2017 aangenomen en is bedoeld om het gedrag van potentiële kwaadwillige cyberactoren te beïnvloeden of zelfs te ontmoedigen om zo een bijdrage te leveren aan het veilig houden van de EU en haar lidstaten.[295] De toolbox biedt mogelijkheid tot het inzetten van vijf soorten maatregelen: preventieve maatregelen;[296] samenwerkingsmaatregelen;[297] stabiliteitsmaatregelen;[298] restrictieve maatregelen (sancties); ondersteuning van rechtmatige respons van individuele lidstaten.[299]

Wanneer de verschillende maatregelen ingezet kunnen worden, bijvoorbeeld in respons op cyberspionage, -sabotage of -beïnvloedingsoperaties, wordt niet expliciet benoemd. In de richtlijnen voor implementatie staat dat cybersancties ingezet kunnen worden wanneer een cyberoperatie met (potentieel) significante effecten plaatsvindt, of een poging daartoe wordt gedaan wordt.[300] In principe zou het cybersanctieregime dus van toepassing zijn op een staat die kwaadwillende cyberactiviteiten uitvoert of verantwoordelijk is voor de acties van een niet-statelijke actor die onder zijn leiding of controle handelt. Het type sanctie dat wordt besproken (het bevriezen van tegoeden en economische middelen)[301] is echter alleen gericht tegen individuen of entiteiten, niet staten.[302]

Actieplan tegen desinformatie

Met inachtneming van de Europese parlementsverkiezing en de meer dan 50 presidents-, nationale of lokale verkiezingen die in 2020 zouden plaatsvinden, stelde de EU in 2019 het actieplan tegen desinformatie op.[303] Hierin wordt benadrukt dat "het blootleggen van desinformatie in buurlanden van de Unie complementair is met de aanpak van het probleem binnen de Unie."[304] Er wordt dus actief samengewerkt met partners ten oosten en zuiden van de Unie om onder andere Russische desinformatie te weren. Het actieplan is gericht op het verbeteren van de capaciteit van EU-instituten om desinformatie op te sporen, te analyseren en aan het licht te brengen; het versterken van gecoördineerde en gezamenlijke reacties op desinformatie; het mobiliseren van de particuliere sector om desinformatie aan te pakken; en het bewustmaken en verbeteren van maatschappelijke veerkracht. Het actieplan heeft geleid tot het opzetten van een systeem dat via een speciale technologische infrastructuur real-time waarschuwingen doorgeeft over desinformatie-

---

[294] Council of the European Union (2016), *Non-paper: Developing a Joint EU Diplomatic Response against Coercive Cyber Operations,* p. 1.
[295] Council of the European Union (2017), *Draft Council Conclusions On A Framework For A Joint EU Diplomatic Response To Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),* p. 5.
[296] Bijvoorbeeld confidence-building measures, capaciteitsopbouw in landen buiten Europa, het verspreiden van kennis over EU-beleid.
[297] Bijvoorbeeld politieke en thematische dialogen.
[298] Verklaringen van de Hoge Vertegenwoordiger van de EU, namens de Raad van de EU, en andere signalen.
[299] Ivan (2019), *Responding to Cyberattacks*, p. 5. Volgens de conventionele interpretatie van het internationaal recht mag alleen de gedupeerde staat tegenmaatregelen nemen. Aangezien de maatregelen die genoemd worden in de Cyber Diplomacy Toolbox onder 'retorsie' vallen, mogen deze wel in collectief verband worden ingezet. Zie hoofdstuk 4.
[300] Bendiek & Pander - Maat (2019), *The EU's Regulatory Approach to Cyber-Security*, p. 25.
[301] Bendiek & Pander - Maat (2019), *The EU's Regulatory Approach to Cyber-Security*, p. 25.
[302] Ivan (2019), *Responding to Cyberattacks*, p. 8, Botek (2019), *European Union Establishes a Sanction Regime.*
[303] European Commission (2018), *Action Plan Against Disinformation.*
[304] European Commission (2018), *Action Plan Against Disinformation.*

campagnes.[305] Daarnaast verwacht de EU dat lidstaten hun eigen communicatie over de waarden en het beleid van de EU verbeteren om zo te zorgen dat samenlevingen meer weerstand weten te bieden wanneer er (vanuit het buitenland) anti-EU-campagnes worden gevoerd.

Uit het actieplan wordt niet duidelijk hoe de EU reageert op desinformatiecampagnes die ingezet zijn door statelijke actoren. Tot dusver lijkt het beleid van de EU vooral gericht op het voorkomen, en het vroegtijdig ontdekken van informatie-operaties – en niet op het formuleren van een respons met diplomatieke middelen of andere maatregelen.

5.1.2. NAVO

Voor de NAVO is, net als voor de EU, cybersecurity een strategisch probleem dat zowel de organisatie zelf als de lidstaten beïnvloedt. Voor beide organisaties heeft het weerbaar maken en de veiligheid van hun eigen netwerken, organisatie en missies de hoogste prioriteit. De cybersecurity van NAVO/EU-lidstaten wordt grotendeels overgelaten aan individuele staten en beschouwd als een nationale verantwoordelijkheid.[306] Desalniettemin maakte de NAVO in 2014 kenbaar dat het collectieve verdedigingsmechanisme ook in het cyberdomein geldig is. Oftewel, NAVO-lidstaten kunnen een beroep doen op Artikel 5 van het Verdrag bij een cyberaanval met effecten vergelijkbaar met die van een gewapende aanval.[307] In 2016 herkende de NAVO het cyberdomein als vierde oorlogsdomein.[308] De Atlantische Raad beslist wanneer een cyberaanval kan leiden tot het inroepen van Artikel 5. Hier bestaan geen uitgesproken richtlijnen voor: elke casus wordt afzonderlijk beoordeeld.[309] De NAVO heeft niet aangegeven hoe het bondgenootschap reageert op verschillende type cyberoperaties, zoals spionage, sabotage of beïnvloeding.

Volgend op de 2016 NAVO-top in Warschau, hebben de NAVO-defensieministers gevraagd om de ontwikkeling van een militaire visie en strategie om de cyberverdediging van de Alliantie te versterken en, indien nodig, cyberoperaties in te kunnen zetten om tactische of strategische doelstellingen te bereiken.[310] Eind 2017 kondigde secretaris-generaal Jens Stoltenberg een belangrijke beleidsverandering aan door te stellen dat de NAVO gebruik zou gaan maken van de offensieve cyberwapens van lidstaten, om de Alliantie beter te beschermen en verdedigen tegen cyberdreigingen.[311] Daartegenover staat dat de NAVO duidelijk heeft verklaard *geen* offensieve cyberoperaties uit te zullen voeren onder de NAVO-vlag. Maar, wanneer dit nodig wordt geacht, zal de NAVO de offensieve cybercapaciteiten van bondgenoten integreren. Verschillende staten hebben publiekelijk verklaard dat ze bereid en in staat zijn om hun cybercapaciteiten beschikbaar te maken voor de NAVO, waaronder het Verenigd Koninkrijk, de Verenigde Staten, Nederland, Estland en Denemarken.[312]

Sinds 2010 vinden er regelmatig informele bijeenkomsten plaats tussen NAVO en EU staf die zich bezighouden met cybersecurity.[313] Sinds 2016 is een regeling tussen de twee organisaties van

---

[305] Rapid Alert System.
[306] Pernik (2014), *Improving Cyber Security: NATO and the EU*, p. 6.
[307] Pernik (2014), *Improving Cyber Security: NATO and the EU*, p. 6.
[308] Warsaw Summit (2016). Zie: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[309] NATO (2014), *Wales Summit Declaration.*
[310] Shea (2018), *Cyberspace as a Domain of Operations*, p. 134.
[311] Arts (2018), *Offense as the New Defense*, p. 4.
[312] Lewis (2019), *What is NATO Really Doing in Cyberspace?, Arts (2018), Offense as the New Defense, p.* 2., Emmot (2018), *NATO Cyber Command*, Ministerie van Defensie (2018), *Defensie Cyber Strategie 2018*, p. 8.
[313] Pernik (2014), *Improving Cyber Security*, p. 7.

kracht die het mogelijk maakt om technische informatie te delen, bedoeld om de preventie en detectie van cyberoperaties, alsmede een mogelijke respons, te verbeteren.[314] Dit heeft geleid tot de huidige EU-NAVO samenwerking die uit (onder andere) de volgende activiteiten bestaat: (1) uitwisseling van concepten en doctrines; (2) wederzijdse deelname aan cyberoefeningen; (3) uitwisseling van informatie over trainings- en onderwijscursussen en dreigingsindicatoren; (4) gedeelde bijeenkomsten over cybercrisismanagement; (5) regelmatige vergaderingen.[315] Daarnaast voeren de NAVO en de EU sinds 2016 gezamenlijk oefeningen uit en ontwikkelen ze gecoördineerd defensiecapaciteiten.[316]

5.1.3. VN en OVSE

De Verenigde Naties onderkent sinds het begin van de 21e eeuw de potentiële dreiging voor de internationale vrede en veiligheid als gevolg van de ontwikkeling van nieuwe technologieën. De organisatie probeert actief bij te dragen aan de internationale veiligheid en de veiligheid van het cyberdomein door de ontwikkeling van cybergedragsnormen te stimuleren. In 2004 werd de eerste VN *Group of Governmental Experts* (GGE) opgericht, bedoeld om verantwoord staatsgedrag ("*responsible state behaviour*") in het cyberdomein te bevorderen. Sindsdien zijn er zes werkgroepen opgericht, de meest recente is gestart in 2019. Een Nederlandse afgevaardigde was aanwezig bij de bijeenkomsten van de vijfde GGE (2016-2017)[317] en neemt deel aan de zesde GGE (2019-2021).[318]

In 2018 werd ook de VN Open-Ended Working Group (OEWG) opgericht, net als de GGE bedoeld om regels, normen en principes van verantwoord staatsgedrag te ontwikkelen en implementeren. Staten hoeven zich voor deze werkgroep niet aan te melden of geselecteerd te worden: alle geïnteresseerde lidstaten kunnen een bijdrage leveren. Zoals eerder beschreven is er op mondiaal niveau een tweedeling zichtbaar wat betreft de denkbeelden die staten hebben over veiligheid in het cyberdomein: westerse staten spreken veelal over *cybersecurity*, terwijl China en Rusland refereren naar *information security*.[319] Deze tweedeling is duidelijk zichtbaar in de VN, en heeft er toe geleid dat er twee verschillende, parallelle werkgroepen zijn opgericht: de GGE en de OEWG. Tijdens deze werkgroepen wordt gedebatteerd over de normen die zouden moeten gelden in het cyberdomein, en in feite, hoe het cyberdomein gereguleerd zou moeten worden. Onder andere door onenigheid tussen de cybergrootmachten en verschillende ideeën over de meest relevante dreiging en normen zijn deze debatten de laatste jaren steeds verder gepolariseerd.[320]

Betrokken deskundigen bereikten tijdens de GGE-bijeenkomsten in 2015 consensus over elf vrijwillige, niet-bindende normen. Het GGE-rapport werd vervolgens unaniem aangenomen door de

---

[314] Ilves et al. (2016), *European Union and NATO*, p. 136.
[315] Fifth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.
[316] European Union (2016), *Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign and Security Policy*, p. 37.
[317] Behalve de vijf permanente leden van de Veiligheidsraad moeten alle lidstaten een officieel verzoek indienen om deel te nemen aan de werkgroepen. Deze worden samengesteld op basis van geografische spreiding, politiek evenwicht, de aangetoonde belangstelling voor het onderwerp en het aantal keren dat een staat deelnam aan eerdere GGE's. Zie: https://dig.watch/processes/un-gge#view-7541-3.
[318] https://www.un.org/disarmament/group-of-governmental-experts/
[319] Keir & Hagestad (2013), *Divided by a Common Language*.
[320] Finnemore & Hollis (2016), *Constructing Norms for Global Cybersecurity*, p. 448, Tikk & Kerttunen (2017), *The Alledged Demise of the UN GGE*, p. 6.

Algemene Vergadering.[321] Er mag naar aanleiding van het rapport bijvoorbeeld van staten verwacht worden dat zij: maatregelen nemen om ICT-praktijken te voorkomen waarvan wordt erkend dat ze schadelijk zijn of een bedreiging kunnen vormen voor de internationale vrede en veiligheid;[322] niet (bewust) toestaan dat hun grondgebied gebruikt wordt voor internationaal onrechtmatige handelingen uitgevoerd middels het cyberdomein;[323] en dat zij, wanneer ICT-incidenten plaatsvinden alle relevante informatie beschouwen, inclusief de bredere context waarin het incident plaatsvindt, de complexiteit van attributie en de aard en omvang van de gevolgen van het incident.[324]

Het lukte de GGE die samenkwam in 2016-2017, waar Nederland ook bij betrokken was, niet om consensus te bereiken. Aan het werk van de groep kwam een einde toen onenigheid ontstond over, onder andere, of staten die worden aangevallen via het cyberdomein mogen reageren door middel van een militaire operatie waarbij gebruik wordt gemaakt van traditionele oorlogsmiddelen.[325] Vervolgens werd de OEWG opgericht. Sindsdien wordt ook wel gesteld dat de VS de GGE-werkgroepen gebruikt voor het promoten van internetbeleid gericht op vrijheid, terwijl Rusland staten middels de OEWG stimuleert om het internet strenger te reguleren en controleren.[326] In paragraaf 7.1.2 worden een aantal aanbevelingen besproken waarvan academici stellen dat ze een positief effect zouden kunnen hebben op de inspanningen van de VN.

De G7-staten hebben in 2019 het *Cyber Norm Initiative* opgericht, waarin praktijken en *lessons learned* over de implementatie van vrijwillige, niet-bindende normen worden gedeeld.[327] Op regionaal niveau is de OVSE betrokken bij de operationalisering van de GGE-normen. Deze cybergedragsnormen worden vertaald in CBMs, welke zijn bedoeld om het cyberdomein voorspelbaarder te maken en misverstanden te voorkomen.[328]

5.2. Online mensenrechten

De posities die staten over het beleid omtrent online mensenrechten innemen op internationaal niveau zijn sterk verdeeld. In het Westen ligt de focus op internetvrijheid en wordt samengewerkt met verschillende stakeholders.[329] In andere delen van de wereld beogen staten meer controle te

---

[321] Over het algemeen is er sprake van een 'zachte norm' wanneer een rapport van de GGE en/of OEWG wordt aangenomen door de VN Algemene Vergadering. Alleen de resoluties die worden aangenomen door de VN-Veiligheidsraad onder hoofdstuk 7 van het VN-Handvest gelden als bindend, alle andere VN-resoluties worden gezien als raadgevend.

[322] VN Algemene Vergadering A/70/174, para. 13(a).

[323] VN Algemene Vergadering A/70/174, para. 13(c).

[324] VN Algemene Vergadering A/70/174, para. 13(b).

[325] Geneva Internet Platform (2020), *UN GGE and OEWG.* Zie: https://dig.watch/processes/un-gge#view-7541-3

[326] Ruhl et al. (2020), *Cyberspace and Geopolitics*, p. 8, Finnemore & Hollis (2016), *Constructing Norms for Global Cybersecurity*, p. 448.

[327] G7 France: Foreign Ministers Meeting (2019), Dinard Declaration on the Cyber Norm Initiative.

[328] De 57 deelnemende OSVE-lidstaten hebben sinds 2013 twee series (van in totaal 16) CBMs aangenomen, dit zijn vrijwillige, niet-bindende normen. Bijvoorbeeld: De deelnemende staten zullen vrijwillig hun nationale opvattingen over verschillende aspecten van nationale en transnationale bedreigingen van en bij het gebruik van ICT delen. De omvang van dergelijke informatie wordt bepaald door de verstrekkende partijen; De deelnemende staten zullen op vrijwillige basis en op het gepaste niveau overleg plegen om het risico van misvattingen en het mogelijke ontstaan van politieke of militaire spanningen of conflicten die kunnen voortvloeien uit het gebruik van ICT, te verkleinen, en om kritieke nationale en internationale ICT-infrastructuren, inclusief hun integriteit, te beschermen. OVSE 1092nd Plenary Meeting. PC.DEC/1202, para. 1 & 3.

[329] Mihr (2017), *Justice*, p. 30, Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 232

krijgen over het internet. In China, Rusland en in veel staten in het Midden-Oosten wordt een open en vrij cyberdomein gezien als een bedreiging voor het zittende regime.[330] In hoofdstuk 4.3 is aan de orde gekomen hoe deze verschillende visies leiden tot een conflicterende interpretatie van internationale mensenrechten. Dit is ook zichtbaar in de verschillende voorstellen omtrent het opstellen van internationaal beleid ten aanzien van mensenrechten. Staten hebben sterke en uiteenlopende voorkeuren wat betreft regulering.[331] Dit hoofdstuk zal verder ingaan op deze verschillende voorkeuren. Daarbij komen de volgende onderwerpen aan bod:

- Voor de beleidsbenadering met betrekking tot. mensenrechten zijn mondiaal drie modellen te herkennen. Autoritaire staten trachten volledige controle te krijgen over het cyberdomein; de VS voert een beleid waarbij de nadruk ligt op de vrijheid van meningsuiting; de EU neemt een middenpositie in;
- De afgelopen jaren vindt er in de EU een verschuiving plaats richting een sterkere rol voor de overheid in het cyberdomein;
- De EU neemt bij het opstellen van beleid meer een *human security approach* terwijl China en Rusland gebruikmaken van een *information security approach*;
- De EU heeft bijgedragen aan de ontwikkeling van internationaal beleid voor de bescherming van de online mensenrechten middels de Cyber Security Strategie uit 2013 en de *Communication on Resilience, Deterrence and Defense* uit 2017;
- Op VN-niveau zijn de afgelopen jaren herhaaldelijk pogingen ondernomen om beleid te creëren voor de bescherming van de online mensenrechten. Deze pogingen hebben echter niet tot substantiële afspraken geleid.

5.2.1. Verschillende beleidsmodellen

Het internationale beleid voor de bescherming van de online mensenrechten kan worden onderverdeeld in drie modellen waarmee staten het internet en de online mensenrechten willen reguleren (of trachten te beschermen). Het internetbeleid van autoritaire staten, het eerste beleidsmodel, is gericht op het creëren van sociale cohesie en controle en het bevorderen van de nationale veiligheid. Autoritaire staten bestrijden middels hun internetbeleid criminaliteit en terrorisme maar ook politieke dissidenten (door het inzetten van vergaande cybersurveillancetechnieken). Het tweede beleidsmodel, ontwikkeld door de VS, wordt vaak genoemd als 'tegenhanger' van het internetbeleid van autoritaire staten. Het Amerikaanse beleid zou zijn gebaseerd op een visie van commerciële en individuele internet-vrijheid waarbij de vrijheid van meningsuiting centraal staat en regulering wordt overgelaten aan de private sector.[332] Gegeven de Snowden-onthullingen en de recente uitspraak dat het Amerikaanse massa-surveillance programma een schending van de grondwet betreft,[333] moeten hier wel kanttekeningen bij worden geplaatst.

In de EU, waar het derde beleidsmodel wordt gevonden, wordt de nadruk op de vrijheid van meningsuiting ook onderschreven. Maar in Europa en ook Nederland is de laatste jaren sprake van een verschuiving richting een sterkere rol van de overheid in het cyberdomein. Deze verschuiving zou juist plaatsvinden om bepaalde grondrechtelijke waarden te kunnen beschermen. Een belangrijk verschil tussen de Europese Unie en de VS is dan ook dat de EU meer bereidheid toont om burgers te

[330] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 232, Henriksen (2019), *The End of the Road for the UN GGE Process*, p. 5.
[331] AIV (2020), *Regulering van Online Content*, p. 6.
[332] AIV (2020), *Regulering van Online Content*, p. 19-20.
[333] Reuters (2020), *NSA Surveillance Exposed by Snowden was Illegal, Court Rules Seven Years On*.

beschermen door middel van strengere regelgeving op het gebied van privacy en de regulering van online informatie.[334]

Met complete controle aan de ene kant, een ogenschijnlijke focus op (volledige) vrijheid aan de andere kant en Europa in het midden, is het bijna onmogelijk om consensus over internationaal beleid ten aanzien van mensenrechten te vinden op internationaal niveau. Toch zijn er ook overeenkomsten. Zowel de VS als de EU maken binnen hun beleidsvorming gebruik van een gedecentraliseerd multi-stakeholder principe.[335] Dit houdt in dat de staat samenwerkt met actoren uit het bedrijfsleven en civiele organisaties. Het multi-stakeholder principe is gebaseerd op het idee dat een staat niet de bescherming van data kan waarborgen zonder de hulp van private actoren. Dit beleidsprincipe roept echter wel de vraag op welke actoren betrokken moeten worden bij dit proces, gezien er kan worden gekozen uit een groot scala aan verschillende bedrijven en maatschappelijke organisaties.[336]

Aan de andere kant stellen staten zoals Rusland, China, India en Iran dat het nationale overheden zijn die autoriteit hebben als het gaat om het reguleren van het cyberdomein, niet maatschappelijke organisaties of private bedrijven. Dit kan vergaande gevolgen hebben voor de bescherming van de online mensenrechten. Daarbij verkiezen deze staten het multilaterale model boven het multi-stakeholder model. In het multilaterale model is een grote rol weggelegd voor een door de VN geleide instantie die beleid kan maken voor, en controle kan uitvoeren over, het cyberdomein. Binnen dit model zou de soevereiniteit van staten over het nationale cyberdomein centraal moeten staan en zouden overheden een grote mate van controle over dit domein moeten kunnen uitoefenen.[337]

De *Shanghai Cooperation Organisation* (SCO), waarvan Rusland, China en India lid zijn en Iran waarnemersstatus geniet, is opgericht volgens het multilaterale model. Het doel van de SCO is het militaire vertrouwen binnen de Euraziatische regio te versterken. Via deze intergouvernementele organisatie coördineren onder andere China, Rusland en India hun cyberbeleid en -operaties gericht op het bestrijden van politieke onrust.[338]

5.2.2. Human security versus information security

Door groeiende zorgen over de privacy en veiligheid van burgers in het cyberdomein is cybersecurity in de afgelopen twintig jaar een van de belangrijkste punten geworden op de politieke en wetgevende agenda van de EU.[339] Bij het opstellen van beleid volgt de EU in toenemende mate een *human security approach.* Dat betekent dat het vertrouwen en de veiligheid van burgers centraal staan wanneer de noodzaak zich voordoet om cybermaatregelen en wetten aan te nemen die mogelijkerwijs mensenrechten kunnen schenden.[340] Hoewel er een verschuiving richting een sterkere rol van de overheid binnen het cyberdomein plaatsvindt, neemt de EU daarbij wel het effect op mensenrechten in acht. Deze benadering staat in sterk contrast met het beleid van China en Rusland: zij kiezen voor

---

[334] AIV (2020), *Regulering van Online Content*, p. 19-20.
[335] Tikk-Ringas (2016), *International Cyber Norms Dialogue*, p. 52, Eldem (2020), *The Governance of Turkey's Cyberspace*, p. 454.
[336] Liaropoulos (2015), *A Human-Centric Approach to Cybersecurity*, p. 21.
[337] Eldem (2020), *The Governance of Turkey's Cyberspace*, p. 454
[338] Liaropoulos (2015), *A Human-Centric Approach to Cybersecurity*, p. 20-21.
[339] Bendiek & Pander - Maat (2019), *The EU's Regulatory Approach to Cyber-Security*, p. 3.
[340] Deibert (2018), *Toward a Human-Centric Approach*, p. 412, Schaake & Vermeulen (2016), *Towards a Values-Based European Foreign Policy*, p. 75.

een *information security approach*. Dit is in lijn met de manier waarop deze staten over veiligheid in het cyberdomein spreken (zie paragraaf 3.1.1).[341]

Information security gaat over het beschermen van data tegen ongeautoriseerd gebruik en legt de nadruk op het beschermen van soevereiniteit en nationale veiligheid.[342] Volgens verschillende westerse academici proberen onder andere China en Rusland, met begrippen zoals internetsoevereiniteit en *information security*, te rechtvaardigen dat ze de informatie waar hun burgers toegang tot hebben, beperken.[343] Deze staten zouden, zoals eerder beschreven in paragraaf 3.1.1, een vrij toegankelijk en open internet zien als een bedreiging voor de overheid en nationale veiligheid.[344] Dit heeft een negatieve impact op online mensenrechten, met name de vrijheid van meningsuiting.[345] EU-lidstaten hebben zich expliciet uitgesproken tegen de *information security approach*. Zo stelden het Verenigd Koninkrijk en Zweden dat "het gebruik van de term *information security* mogelijk voor verwarring zorgt omdat het door sommige staten en organisaties wordt gebruikt als onderdeel van een doctrine die informatie beschouwt als een bedreiging waartegen aanvullende bescherming nodig is."[346] Het VK en Zweden erkennen de geldigheid van *information security* in deze context niet, omdat de term gebruikt zou kunnen worden om controle op de vrijheid van meningsuiting te legitimeren op een manier die niet overeenkomt met de UVRM en het IVBPR.[347]

5.2.3. Europese Unie

De Europese Unie heeft ook pogingen gedaan tot het ontwikkelen van gemeenschappelijk internationaal beleid op het gebied van de online mensenrechten. De EU Cybersecurity Strategie uit 2013 bevat een duidelijke verwijzing naar de geldigheid van mensenrechten online.[348] Zo stelt de strategie dat beleidsposities en wetten alleen rechtmatig zijn wanneer deze zijn gebaseerd op de fundamentele rechten en vrijheden die voortvloeien uit het Handvest van de grondrechten van de Europese Unie.[349] In dit Handvest zijn zowel de bescherming van data als het recht op vrijheid van meningsuiting en het recht op privacy opgenomen.[350] Deze positie werd in 2017 nogmaals bevestigd middels de *Joint Communication on Resilience, Deterrence and Defence*. In dit document wordt herhaald dat mensenrechten die offline gelden ook online van toepassing zijn.[351] Ondanks deze ontwikkelingen blijkt ook uit het EU-beleid dat het lastig is om het bewaken van de veiligheid af te wegen tegen het beschermen van de online mensenrechten. In 2018 deed de Europese Commissie

---

[341] Eldem (2020), *The Governance of Turkey's Cyberspace*, p. 452.
[342] Hampson & Sulmeyer (eds) (2017), *Getting beyond Norms*, p. 15, Schaake & Vermeulen (2016), *Towards a Values-Based European Foreign Policy*, p. 76.
[343] Hampson & Sulmeyer (eds) (2017), *Getting beyond Norms*, p. 15, Schaake & Vermeulen (2016), *Towards a Values-Based European Foreign Policy*, p. 76.
[344] In Europa erkennen juist steeds meer staten dat toegang tot het internet onlosmakelijk verbonden is met de uitvoering van verscheidene mensenrechten. Zie: Shackelford (2019), *Should Cybersecurity be a Human Right* p. 166.
[345] Hampson & Sulmeyer (eds) (2017), *Getting beyond Norms*, p. 15, Schaake & Vermeulen (2016), *Towards a Values-Based European Foreign Policy*, p. 76.
[346] A/68/156, A/69/112.
[347] Tikk & Kerttunen (2017), *The Alledged Demise of the UN GGE*, p. 19.
[348] Liaropoulos (2015), *A Human-Centric Approach to Cybersecurity*, p. 20, Bendiek & Pander - Maat (2019), *The EU's Regulatory Approach to Cyber-Security*, p. 5.
[349] Claessen (2020), *Reshaping the Internet*, p. 152.
[350] Ilves et al. (2016), *European Union and NATO*, p. 133.
[351] Claessen (2020), *Reshaping the Internet*, p. 152.

een voorstel om de verspreiding van terroristische informatie online te reguleren. Het EU Bureau voor de Grondrechten uitte direct zorgen over de bescherming van de vrijheid van meningsuiting.[352] Uiteindelijk is het voorstel aangenomen in 2019.[353] In relevante verdragen, bijvoorbeeld een EU-verdrag voor de bestrijding van cybercriminaliteit, wordt wel expliciet verwezen naar Europese kernwaarden: het promoten van fundamentele rechten zoals de vrijheid van meningsuiting.[354]

5.2.4. Verenigde Naties

De VN heeft herhaaldelijk geprobeerd om beleid en normen te creëren met betrekking tot de bescherming van online mensenrechten. Vanaf 2009 wordt tijdens de jaarlijkse bijeenkomst van het *Internet Governance Forum* (IGF) gezocht naar beleid voor, en een toepassing van, mensenrechten in het cyberdomein.[355] Ook de GGE (zie 5.1.3.) heeft aandacht besteed aan online mensenrechten.[356] De GGE identificeerde in 2013 de noodzaak om mensenrechten te beschermen in het cyberdomein en stelde dat mensenrechten zowel offline als online gelden.[357] Volgens verscheidene experts die betrokken waren bij de werkgroepen was het echter onwaarschijnlijk dat er concrete beleidsafspraken op het gebied van de online mensenrechten gemaakt zouden worden. In het GGE-rapport van 2015 worden enkel meermaals vermeldingen gemaakt van de UVRM en andere mensenrechtelijke instrumenten.[358]

Daarnaast heeft David Kaye, als Speciale Rapporteur voor de bevordering en bescherming van de vrijheid van meningsuiting van de Mensenrechtenraad (augustus 2014 tot juli 2020), bijgedragen aan de totstandkoming van normen en beleid middels twee rapporten, gepubliceerd in 2018 en 2019. Kaye heeft herhaaldelijk uitspraken gedaan over online mensenrechten en het belang van de vrijheid van meningsuiting online.[359] Ook heeft Kaye uitgebreid gerapporteerd over de regulering van het cyberdomein. Zo beargumenteerde hij dat overheden verplicht zijn om de uitoefening van de vrijheid van meningsuiting online voor hun burgers mogelijk te maken en te beschermen.[360]

---

[352] Bendiek & Pander - Maat (2019), *The EU's Regulatory Approach to Cyber-Security*, p. 13.
[353] European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online.
[354] Ilves et al. (2016), *European Union and NATO*, p. 132.
[355] Florek & Eroglu (2019), *The Need for Protection of Human Rights*, p. 30.
[356] Liaropoulos (2015), *A Human-Centric Approach to Cybersecurity*, p. 20.
[357] Henriksen (2019), *The End of the Road for the UN GGE Process*, p. 3, Lewis (2017), *Revitalizing Progress*, p. 14
[358] Tikk (2020), *International Law in Cyberspace*, p. 19, Lewis (2017), *Revitalizing Progress*, p. 15.
[359] Gabor & Aarons (2016), *State Responsibility to Respect*, p. 515.
[360] AIV (2020), *Regulering van Online Content*, p. 30.

6. Verwachte ontwikkelingen rechtsregels, normen, beleid

Samenvatting

Het cyberdomein is onderhevig aan snelle veranderingen en ontwikkelingen. Het is om die reden vanzelfsprekend dat internationaal cybersecuritybeleid meeverandert en er ook de komende jaren veel ontwikkelingen plaatsvinden op het gebied van cyberregels, -normen en -beleid.

De afgelopen jaren is er veel geschreven over de voor- en nadelen van een nieuw cyberverdrag. Het zijn voornamelijk westerse staten die onderhandelingsvoorstellen afwijzen. Zij beargumenteren dat bestaand internationaal recht van toepassing is in het cyberdomein en daarmee voldoende richtlijnen biedt. Enkele academici beargumenteren echter dat het afwijzen van onderhandelingen over een internationaal normatief verdrag waarschijnlijk in het nadeel van de VS (en bondgenoten) zal uitpakken, gezien het feit dat China en Rusland ondertussen ook cybergrootmachten zijn. Zij stellen daarnaast dat de onderhandelingen zelf waardevol kunnen zijn omdat een dergelijk proces licht schijnt op onenigheden. Daarnaast wordt beargumenteerd dat, gezien het cyberdomein officieel erkend wordt als oorlogsdomein en een groot aantal staten offensieve cybercapaciteiten hebben ontwikkeld of hiermee bezig zijn, een cyberverdrag nodig is om te bepalen hoe cyberoorlog – mocht het daartoe komen – het beste gereguleerd kan worden. In een dergelijk verdrag zou de nadruk liggen op het toepassen van principes zoals militaire noodzaak, onderscheid, proportionaliteit en neutraliteit op cyberactiviteiten. Experts verwachten echter niet dat er binnenkort internationale overeenkomst bereikt zal worden op dit gebied. De mogelijkheid bestaat wel dat er, in de afwezigheid van een speciaal verdrag, gewoonterecht ontstaat. De evolutie van statenpraktijk tot bindende norm is echter in de meeste gevallen een langdurig proces.

Recente voorstellen die aan bod zijn gekomen in de OEWG schetsen een beeld van toekomstige gedragsnormen en de *opinio juris* van staten met betrekking tot het cyberdomein. Deze voorstellen gaan bijvoorbeeld over de integriteit van ICT en het openbare internet. Anderzijds zijn staten en academici niet hoopvol over de mogelijkheid om consensus te bereiken in de VN-werkgroepen. In oktober 2020 hebben meer dan veertig staten, inclusief de EU-lidstaten, een voorstel gedaan om een *Programme of Action* op te stellen, om een einde te maken aan de parallelle werkgroepen en de mogelijkheden te verkennen voor het oprichten van een permanent VN-forum. Door een gebrek aan consensus binnen de VN-werkgroepen zijn ook steeds meer private actoren zich gaan mengen in de discussie over cybernormen. Bedrijven en ngo's zoals Microsoft, de *Global Commission on the Stability of Cyberspace* en het Internationaal Comité van het Rode Kruis hebben zelf cybergedragsnormen geformuleerd.

Inleiding verwachte ontwikkelingen rechtsregels, normen, beleid

Het cyberdomein is onderhevig aan snelle veranderingen en ontwikkelingen. Het is om die reden vanzelfsprekend dat internationaal cybersecuritybeleid mee verandert. In dit hoofdstuk wordt de volgende vraag beantwoord: zijn er belangrijke verwachte internationale ontwikkelingen op het gebied van internationale rechtsregels, normen, en/of cybersecuritybeleid gericht op de cyberdreiging van staten die nu nog niet gelden maar wel in de komende 3 jaar verwacht worden, en zo ja, welke? De volgende punten zullen kort worden toegelicht:

- Er is de afgelopen jaren veel geschreven over de voor- en nadelen van een nieuw cyberverdrag. Experts verwachten niet dat er binnenkort internationale overeenkomst bereikt zal worden over een verdrag waarin cybergedragsnormen worden vastgelegd;
- De evolutie van statenpraktijk tot bindende norm is een langdurig proces, en nieuwe normen zullen dus waarschijnlijk niet uitgekristalliseerd zijn binnen drie of vijf jaar;
- De voorstellen die tijdens de OEWG worden gedaan, schetsen een beeld van toekomstige cybergedragsnormen en de *opinio juris* van staten met betrekking tot het cyberdomein;
- In oktober 2020 hebben meer dan veertig staten, inclusief de EU-lidstaten, een voorstel gedaan om een *Programme of Action* op te stellen ter bevordering van verantwoord staatsgedrag in het cyberdomein, om een einde te maken aan de parallelle werkgroepen (de GGE en OEWG), en te verkennen wat de mogelijkheden zijn om een permanent VN-forum op te richten;
- Verschillende ngo's en private bedrijven doen voorstellen voor cybergedragsnormen. De *Global Commission on the Stability of Cyberspace* (GCSC) heeft acht algemene normen voorgesteld en ook Microsoft en Siemens hebben cybergedragsnormen geformuleerd in de hoop dat overheden zich aan deze regels zullen binden en er zo een normatief cybergedragskader ontstaat.

Discussie omtrent wenselijkheid internationaal cyberverdrag

Ondanks de groeiende digitale dreiging bestaat er geen internationaal cybersecurity- of cyberwapenverdrag. Het zijn voornamelijk westerse staten die onderhandelingsvoorstellen afwijzen. Zij beargumenteren dat bestaand internationaal recht van toepassing is in het cyberdomein en daarmee voldoende richtlijnen biedt. Daarnaast is menig academicus van mening dat de beste verdediging in het cyberdomein offensief van aard is.[361] Indien dit het geval is, zou een internationaal cyberverdrag waarmee het inzetten van offensieve cybercapaciteiten wordt ingeperkt negatieve consequenties kunnen hebben. Er bestaat onder experts en academici echter geen consensus over het beste cybersecuritybeleid, over de definitie van cybergeweld, de toepassing van het verbod op het gebruik van geweld in het cyberdomein, of over het nut van een speciaal cyberverdrag.[362] Ook pleiten sommige academici voor een cyber-non-proliferatieverdrag,[363] terwijl anderen dit juist afraden of de haalbaarheid betwisten.[364]

---

[361] Eilstrup-Sangiovanni (2018), *Why the World Needs an International Cyberwar Convention*, p. 280.

[362] Zie voor een overzicht van contributies uit 2012, gepubliceerd door US News (zes van de zeven experts stellen om verscheidene redenen dat er geen verdrag moet komen): *Should There Be an International Treaty on Cyberwarfare?* https://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare, en de reactie van Hollis (2012), *Should There Be an International Treaty on Cyberwarfare?*

[363] Barbieri et al. (2018), *Non-Proliferation Regime for Cyber Weapons*, p. 38, Morgus et al. (2017), *Countering the Proliferation of Offensive Cyber Capabilities*, p. 184.

[364] Franklin (2018), *An International Cyber Warfare Treaty*, p. 156, Arimatsu (2012), *A Treaty for Governing Cyber-Weapons*, p. 100.

Kilovaty en Mann beargumenteren dat het afwijzen van onderhandelingen over een internationaal normatief verdrag waarschijnlijk in het nadeel van de VS (en bondgenoten) zal uitpakken, gezien het feit dat China en Rusland ondertussen ook cybergrootmachten zijn. Zij stellen daarnaast dat de onderhandelingen zelf waardevol kunnen zijn omdat een dergelijk proces licht schijnt op onenigheden en tegelijkertijd de wapenwedloop kan beperken. De positie die onder andere China en Rusland innemen – dat de toepassing van het humanitair oorlogsrecht tot militarisering van het cyberdomein leidt – wordt gedeeld door Kilovaty en Mann en beschouwd als een ongewenste ontwikkeling. Omdat zij beargumenteren dat de meeste cyberoperaties niet de drempel overschrijden die het in werking treden van oorlogsrecht rechtvaardigt, stellen ze dat een internationaal cyberverdrag beter in staat zal zijn om cyberoperaties te beperken die geen fysieke of lichamelijke schade aanrichten.[365]

Daarnaast wordt beargumenteerd dat, gezien het cyberdomein officieel erkend wordt als het vierde (of vijfde) oorlogsdomein[366] en een groot aantal staten offensieve cybercapaciteiten hebben ontwikkeld of hiermee bezig zijn, een cyberverdrag nodig is om te bepalen hoe cyberoorlog – mocht het daartoe komen – het beste gereguleerd kan worden. In een dergelijk verdrag zou de nadruk liggen op het toepassen van principes zoals militaire noodzaak, onderscheid, proportionaliteit en neutraliteit op cyberactiviteiten.[367]

Broeders, Adamson en Creemers stellen dat westerse staten een solide verhaal nodig hebben om hun afwijzing van een speciaal cyberverdrag te ondersteunen, willen ze voorkomen dat China en Rusland een meerderheid van de internationale gemeenschap overreden.[368] Desalniettemin verwachten experts niet dat er binnenkort internationale overeenkomst bereikt zal worden over een verdrag gericht op het vastleggen van cybergedragsnormen.[369]

Staatspraktijk en opinio juris

Internationaal recht ontstaat niet alleen door het opstellen van bindende verdragen maar ook door middel van statenpraktijk en *opinio juris,* dit wordt 'gewoonterecht' of *customary international law* genoemd. De evolutie van statenpraktijk tot een bindende norm duurt over het algemeen echter meerdere jaren[370] en veel staten tonen een sterke mate van terughoudendheid met betrekking tot het bijdragen aan de ontwikkeling van cyber-gewoonterecht.[371] Staten zijn zelden transparant over hun eigen activiteiten in het cyberdomein en slechts enkele staten doen duidelijke uitspraken over hoe zij de toepassing van internationaal recht op cyberkwesties interpreteren (*opinio juris).* Väljataga beargumenteert dat onder andere Nederland, Frankrijk en Australië middels hun nationale cyberstrategie bijdragen aan het ontwikkelen van *opinio juris.* Zo werd in 2011 al door Nederlandse experts gesteld dat een cyberaanval als gewapende aanval kan worden aangemerkt wanneer deze leidt tot een ernstige verstoring met langdurige gevolgen.[372] Deze positie is in 2019 overgenomen

[365] Kilovaty & Mann (2016), *Towards a Cyber-Security Treaty*.
[366] Sommigen beschouwen naast land, zee en lucht, de ruimte ook al als oorlogsdomein. Anderen spreken over de vier oorlogsdomeinen.
[367] Hughes (2010), *A Treaty for Cyberspace*, p. 540.
[368] Broeders et al. (2019), *A Coalition of the Unwilling?*, p. 14.
[369] Kadri (2019), *Trends in International Law for Cyberspace*, Kilovaty (2016), *World Wide Web of Exploitations*, p. 46, Zie voor meer informatie over de obstakels die overwonnen moeten worden bijvoorbeeld ook: Goldsmith (2011), *Cybersecurity Treaties: A Skeptical View*.
[370] Kadri (2019), *Trends in International Law for Cyberspace*. In het geval van 'instant custom' kan gesproken worden van een uitzondering, zie bijvoorbeeld: Scharf (2014), *Accelerated Formation of Customary International Law*, p. 306.
[371] Mačák (2016), *Is the International Law of Cyber Security in Crisis?*, p. 130.
[372] AIV/CAVV (2011), *Cyber Warfare*, p. 21.

door de Nederlandse regering.[373] Ook Frankrijk en Australië stellen beide dat ze de *scale and effects* test zullen toepassen om te bepalen of een cyberaanval gekarakteriseerd moet worden als een gewapende aanval.[374] Voor de verdere ontwikkeling van cyber-gewoonterecht is het van belang dat meer staten verklaren hoe zij de toepassing van het internationaal recht in het cyberdomein zien.[375]

Voorstellen OEWG

Aangezien alle geïnteresseerde VN-lidstaten kunnen bijdragen aan het OEWG-proces, schetsen de voorstellen die bij deze bijeenkomsten worden gedaan een beeld van de richting waarin, in ieder geval een aantal staten, ontwikkelingen verwachten. De volgende voorstellen werden gedaan:

- Staten dienen hun commitment voor de internationale vrede en veiligheid bij het gebruik van ICT te bevestigen;
- Staten dragen de primaire verantwoordelijkheid voor het handhaven van een veilige en betrouwbare ICT-omgeving;
- Het uitvoeren van cyberoperaties die de kritieke infrastructuur (die essentieel is voor politieke processen of medische voorzieningen) kan aantasten moet verboden zijn;
- De beschikbaarheid en integriteit van het openbare internet moet beschermd zijn;[376]
- Staten en niet-statelijke actoren mogen geen cyberoperaties uitvoeren, ondersteunen of bewust toestaan die bedoeld zijn om infrastructuur die essentieel is voor verkiezingen, referenda of volksraadplegingen te verstoren;[377]
- De integriteit van de ICT-*supply chain* moet beschermd zijn;
- Het beschermen van supranationale kritieke infrastructuur is een gedeelde verantwoordelijkheid van alle staten.[378]

In reactie op het OEWG pre-draft rapport stelt Nederland dat een groot aantal staten tijdens een OEWG-meeting heeft aangegeven dat zij het humanitair oorlogsrecht van toepassing achten op activiteiten in het cyberdomein en dat dit ook in het rapport gereflecteerd zou moeten worden. Daarnaast is Nederland van mening dat het rapport, ondanks de hoeveelheid staten die hebben aangegeven dat zij de toepassing van mensenrechten online van groot belang achten, onvoldoende aandacht besteed aan mensenrechten. Daarbij benadrukt Nederland expliciet dat staten bij het ontwikkelen en implementeren van cyberbeleid of cyber-gerelateerde wetten hun internationale mensenrechtenverplichtingen dienen na te leven. Daarnaast heeft Nederland een aantal concrete voorbeelden gegeven van situaties die, afhankelijk van de specifieke omstandigheden, gekwalificeerd kunnen worden als een schending van internationaal recht:

- Vijandige cyberoperaties gericht op gezondheidssystemen en -faciliteiten;
- Cyber(informatie)operaties die interveniëren met bijvoorbeeld nationale crisisresponsmechanismen tijdens een gezondheidscrisis;
- Cyberoperaties gericht op gezondheidsfaciliteiten zijn ten tijde van een gewapend conflict verboden wanneer deze het humanitair oorlogsrecht schenden.

---

[373] Ministerie van Buitenlandse Zaken (2019). Kamerbrief Inzake Internationale Rechtsorde in het Digitale Domein (zie bijlage, p.4).

[374] Väljataga (2018), *Tracing Opinio Juris*, p. 13.

[375] Broeders et al. (2019), *A Coalition of the Unwilling?*, p. 14. Zie voor een analyse van de opvattingen van verschillende staten bijvoorbeeld: Roguski (2020), *Application of International Law to Cyber Operations*.

[376] Voorstel van Nederland. Zie: The Kingdom of the Netherlands' response to the pre-draft report of the OEWG. https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf.

[377] Voorstel van Nederland. Zie: The Kingdom of the Netherlands' response to the pre-draft report of the OEWG.

[378] OEWG (2020), *Second "Pre-Draft" of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security*, p. 42.

Programme of Action
Een groep van veertig staten[379] heeft in oktober 2020 voorgesteld om een einde te maken aan de GGE en OEWG-werkgroepen en in plaats daarvan te gaan werken aan een '*Programme of Action for Advancing Responsible State Behaviour in Cyberspace'.* In het voorstel wordt beschreven dat de staten van mening zijn dat het tijd is om onenigheden te overstijgen en toe te werken naar één inclusief, op vooruitgang en de lange termijn-gericht programma waarin reeds ondernomen werk kan worden voortgezet. Het voorstel wordt vergeleken met het eerder opgerichte *Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons.*[380]

Voorstellen ngo's en private sector
Sinds pogingen om consensus te bereiken in de VN GGE faalden in 2017 (zie 5.1.3.) is het aantal niet-overheidsinitiatieven gericht op het bevorderen van verantwoordelijk gedrag in het cyberdomein aanzienlijk toegenomen.[381] Eggenschwiler beargumenteert dat de voorstellen van Microsoft en Siemens heel bewust politieke termen bevatten, zoals *Geneva Convention* en *Charter*, die onderliggende politieke aspiraties blootleggen.[382] Hoewel deze voorstellen een idee kunnen geven van de wensen van cyber-stakeholders, kunnen alleen staten internationaal recht 'maken'.[383] Microsoft's *Digital Geneva Convention for Peacetime* omvat tien clausules die zijn bedoeld om grootschalige schade en cybercriminaliteit te voorkomen, en het recht op privacy te beschermen.[384]

De *Global Commission on Stability in Cyberspace* heeft in samenspraak met meerdere stakeholders acht normen geformuleerd ter bescherming van het internet, kritieke infrastructuren en democratische processen.[385]

---

[379] De EU-lidstaten, Argentinië, Colombia, Ecuador, Egypte, El Salvador, Gabon, Georgië, Japan, Marokko, Moldavië, Noord-Macedonië, Noorwegen, Singapore, het Verenigd Koninkrijk en Zuid-Korea.
[380] The future of discussions on ICTs and cyberspace at the UN. Zie: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.
[381] Eggenschwiler (2019), *International Cybersecurity Norm Development*, p. 4.
[382] Eggenschwiler (2019), *International Cybersecurity Norm Development*, p. 6.
[383] Zie bijvoorbeeld Woodward (2010), *Global Civil Society in International Lawmaking and Global Governance*, voor een bespreking van de rol van niet-statelijke actoren in het ontwikkelen van internationaal recht.
[384] Zie af van het aanvallen van systemen waarvan de vernietiging een negatief effect heeft op de veiligheid en beveiliging van particulieren; van systemen waarvan de vernietiging de wereldeconomie zou kunnen schaden; van het hacken van persoonlijke accounts/privégegevens van journalisten en particulieren betrokken bij verkiezingsprocessen; van het inzetten van ICT om intellectuele eigendommen te stelen; van het plaatsen/vereisen van 'achterdeuren' in commerciële technologieproductie; maak duidelijk beleid voor het verwerven, behouden, beveiligen, gebruiken en rapporteren van kwetsbaarheden; wees terughoudend met het ontwikkelen van cyberwapens, bewaar deze in een veilige omgeving; spreek af om de verspreiding van cyberwapens te beperken, niet te verspreiden en niet toe te staan dat anderen ze verspreiden, beperk het inzetten van cyber offensieve operaties; ondersteun inspanningen van de particuliere sector om cyberoperaties te detecteren, in te dammen, erop te reageren en weer te herstellen. Zie: Microsoft (2018), *A Digital Geneva Convention to Protect Cyberspace*, https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.
[385] Bescherm de beschikbaarheid en integriteit van het internet; de integriteit van kritieke infrastructuur essentieel voor verkiezingsprocessen; de producten en diensten in ontwikkeling; zie af van frauderen van het ontwikkelingsproces; van het gebruik van ICT voor het inzetten van botnets; creëer een transparant framework voor het beoordelen van het openbaren van bekende kwetsbaarheden of gebreken; producenten van producten en diensten waarvan de stabiliteit van het cyberdomein afhangt, dienen: (1) prioriteit te geven aan veiligheid en stabiliteit, (2) redelijke maatregelen te nemen om ervoor te zorgen dat hun producten of diensten vrij zijn van significante kwetsbaarheden, en (3) maatregelen te nemen om tijdig te kunnen reageren op kwetsbaarheden die later worden ontdekt en om transparant te zijn over dit proces. Alle actoren hebben de plicht om informatie over kwetsbaarheden te delen om kwaadwillende cyberactiviteiten te helpen voorkomen

Het Internationaal Comité van het Rode Kruis (ICRC)[386] stelt in discussies over nieuwe normen dat staten hun bestaande internationale verplichtingen (onder het humanitair oorlogsrecht) als uitgangspunt moeten nemen. Het ICRC benadrukt dat de bijzondere kwetsbaarheid van gezondheidszorgfaciliteiten het formuleren van een nieuwe aanvullende norm rechtvaardigt, en heeft in 2020 voorgesteld dat de volgende norm wordt ontwikkeld: "staten mogen geen ICT-activiteiten uitvoeren, of willens en wetens ondersteunen, die medische diensten of medische faciliteiten zouden schaden, en zouden maatregelen moeten nemen om medische diensten tegen schade te beschermen."[387] In reactie op het toegenomen aantal cyberoperaties gericht tegen medische faciliteiten tijdens de COVID-19 pandemie, hebben veertig internationale actoren (overheden, internationale en non-gouvernementele organisaties en de academische wereld) een oproep van de ICRC ondertekend waarin wordt geëist dat overheden samenwerken om internationale regels die dergelijke acties verbieden, te bevestigen en te volgen.[388]

of beperken; staten dienen passende maatregelen te nemen, waaronder wet- en regelgeving, om 'cyberhygiëne' te waarborgen; niet-statelijke actoren mogen geen offensieve cyberoperaties uitvoeren en statelijke actoren moeten dergelijke activiteiten voorkomen en reageren als ze zich voordoen. Zie: The GSCS Proposed Norms, https://cyberstability.org/report/#6-norms.

[386] Hoewel het ICRC in de loop der jaren door de internationale gemeenschap erkend is als hoeder van het humanitair oorlogsrecht, betekent dit niet dat het ICRC zelf de capaciteit heeft om zelf wettelijk bindende normen te creëren. Zie bijvoorbeeld: Layover & Maresca (1999), *The Role of the ICRC*, Gazzini (2010), *A Unique Non-State Actor*.

[387] ICRC (2020), *Norms for Responsible State Behavior*.

[388] ICRC (2020), *Call to Governments*.

7. Lessen internationaal cybersecuritybeleid

Samenvatting

In de bestudeerde literatuur komen verscheidene lessen naar voren met betrekking tot het Nederlandse internationale cybersecuritybeleid. Ook kan Nederland lessen trekken uit het internationale cybersecuritybeleid van andere staten.

Het eerste doel van het Nederlandse internationale cybersecuritybeleid is de mogelijkheid om adequaat te reageren, al dan niet in coalitieverband. Uit de literatuur blijkt dat het lastig is om vast te stellen wat een adequate reactie op een cyberdreiging in zou moeten houden. Academici stellen dat de karakteristieken van het cyberdomein het nemen van een adequate respons bemoeilijken. Onderdeel van de Nederlandse strategie is het publieke attributiebeleid, aangezien dit een afschrikkend effect zou hebben op potentieel kwaadwillenden. Uit de bestudeerde literatuur blijkt echter dat er weinig empirisch of theoretisch bewijs is voor de veronderstelling dat publieke attributie afschrikkend werkt of tot een stabieler cyberdomein leidt. Dit betekent echter niet dat de overheid publieke attributie nooit zou moeten overwegen. Des te waardevoller de (politieke, economische of sociale) relatie wordt geacht door de beschuldigde (met de beschuldiger), hoe groter het effect van de beschuldiging. Daarbij wordt ook gesteld dat politieke attributie, waarbij staten de retoriek van het internationaal recht vermijden, een cruciale rol kan spelen in het identificeren van bestaand recht en het ontwikkelen van nieuwe rechtsregels, en zo de internationale rechtshandhaving kan bevorderen.

Wat betreft de nieuwe mate van verwevenheid tussen statelijke en niet-statelijke actoren betogen academici dat het belangrijk is dat er niet langer gewerkt wordt met strikt gescheiden ministeries omdat hierdoor een situatie zou kunnen ontstaan waarin problemen over het hoofd gezien worden. Een mogelijk nieuw beleidsraamwerk dat kan helpen dit probleem op te lossen, wordt gevonden in het DIMEFIL-model.

Op EU-niveau kunnen lidstaten collectief reageren op een cyberoperatie middels het EU-cybersanctieregime. In juli 2020 is voor het eerst besloten om sancties op te leggen tegen zes personen en drie entiteiten. Het blijft een politiek ingewikkelde keuze om deze maatregel in te zetten. Academici stellen daarnaast dat het onvoldoende duidelijk is hoe EU-cyberdiplomatie in de praktijk afschrikkend zou kunnen werken. Tegelijkertijd zijn sommige academici van mening dat de ontwikkelingen op Europees niveau, en in het bijzonder het cybersanctieregime, zouden kunnen bijdragen aan het versterken van de wereldwijde naleving van bestaande cybernormen. Over zowel de EU als de NAVO wordt geschreven dat de lidstaten in verschillende mate over cybercapaciteiten beschikken en dat dit het nemen van een collectieve actie kan bemoeilijken. Het zou vooral van belang zijn om een betere gedeelde *situational awareness* te creëren. Over het algemeen zijn academici het eens over de positieve effecten van, en mogelijkheden voor, meer samenwerking tussen de NAVO, de EU en de VS. In hoofdstuk 7.1.1 worden enkele aanbevelingen uiteengezet.

Het tweede doel van de Nederlandse internationale cybersecuritystrategie, het bevorderen van de internationale rechtsorde in het cyberdomein, wordt onder andere bereikt door in organisaties en fora bij te dragen aan de ontwikkeling van normen. De discussies in de VN-werkgroepen zijn echter gepolarieerd en academici verwachten niet dat consensus bereikt zal worden. Andere fora, zoals de *Freedom Online Coalition* (FOC) en de *Global Commission on the Stability of Cyber Space*, zijn daardoor

in belang toegenomen. Hoewel uit de bestudeerde literatuur blijkt dat deze fora over het algemeen goed zijn ontvangen, bestaat er ook kritiek. Zo zouden enkele staten de FOC gebruiken om eventuele kritiek op mensenrechtenschendingen binnen hun eigen nationale cyberdomein onderuit te halen. In hoofdstuk 7.1.2 worden aanbevelingen met betrekking tot de verschillende fora besproken.

Het derde doel omvat het bevorderen van de internationale veiligheid middels cybercapaciteitsprojecten. Uit de literatuur blijkt dat dergelijke capaciteitsopbouwprojecten een positief effect kunnen hebben op de internationale veiligheid, maar de kans op mondiale consensus over cybernormen verkleint. Academici staan ook kritisch tegenover het gebrek aan coördinatie tussen de staten en organisaties die de projecten aanbieden. Sommige staten ontvangen bijvoorbeeld steun van verschillende donoren, terwijl andere staten vergeten worden. Ook wordt in de literatuur geschreven over een gebrek aan draagvlak binnen ontvangende staten. Dit heeft een negatief effect op de implementatie van de capaciteitsprojecten en de bijbehorende strategieën. Ook kunnen capaciteitsprojecten vergaande gevolgen hebben voor mensenrechten, in het bijzonder wanneer de cybercapaciteit van autoritaire staten toeneemt. In hoofdstuk 7.1.3 worden aanbevelingen gedaan omtrent cybercapaciteitsopbouw.

Het laatste doel is de bescherming van online mensenrechten en het bevorderen van mensenrechten in het cyberdomein. BZ heeft bijvoorbeeld het oprichten van de FOC geïnitieerd en steunt ngo's zoals *Digital Defenders Parnership* en *Access Now*. Daarnaast is de Nederlandse diplomatieke inzet gericht op het herhaaldelijk uitspreken dat mensenrechten ook van toepassing zijn in het cyberdomein. Deze handelingen worden positief ontvangen door academici. Echter blijkt uit de bestudeerde literatuur dat mensenrechten vaak enkel oppervlakkig worden betrokken bij het opstellen van cybersecuritybeleid. Academici betogen dat er meer kennis over de implicaties van het algemene beleid op mensenrechten zal ontstaan wanneer mensenrechtenexperts meedenken over het algehele cybersecuritybeleid. In hoofdstuk 7.1.4 worden een aantal aanbevelingen gericht op het bevorderen van mensenrechten in het cyberdomein uiteengezet.

De afgelopen jaren is door academici veel geschreven over het internationale cybersecuritybeleid van de VS, Israël en Estland. Over het algemeen kan er een onderscheid worden gemaakt tussen twee typen staten in het cyberdomein. Sommige staten focussen voornamelijk op het creëren van internationale normen door middel van discussies en bijeenkomsten (bijvoorbeeld Estland), anderen creëren (indirect) 'normen' door middel van hun gedrag (bijvoorbeeld de VS en Israël). Nederland kan hieruit relevante lessen trekken. Zo beargumenteren meerdere academici dat het *Defend Forward* beleid van de VS schadelijk is voor de stabiliteit van het cyberdomein en incompatibel is met een open en vrij internetbeleid. Gebaseerd op de handelingen van Israël en de VS, in het bijzonder de Stuxnet-operatie, concluderen enkele academici dat cybersabotage-operaties gecombineerd moeten worden met andere instrumentele bedreigingen en positieve aansporingen om hun doel te bereiken. Daarbij is het gecompliceerd om een vergelijking te maken tussen cyberoperaties en kinetische operaties voor wat betreft de kans op escalatie. Estland wordt in de literatuur vooral beschouwd als een succesverhaal, omdat het als kleine staat is gelukt om cybernormen op een internationaal niveau te promoten. Academici wijzen er echter wel op dat de verdere ontwikkeling van breed gedragen internationale cybernormen niet zal plaatsvinden zonder belangrijke spelers zoals China en Rusland. In paragraaf 7.2 worden de relevante lessen voor Nederland expliciet beschreven.

Inleiding lessen internationaal cybersecuritybeleid

In dit hoofdstuk worden enkele lessen die in de academische literatuur worden besproken, gepresenteerd. Het hoofdstuk is bedoeld om een duidelijk overzicht te geven van de lessen en aanbevelingen die worden gedaan over de verschillende hoofddoelstellingen van het Nederlandse internationale cybersecuritybeleid.[389] De lessen en aanbevelingen die in dit hoofdstuk aan bod komen, worden niet tegen elkaar afgewogen en zouden in theorie tegenstrijdig kunnen zijn. Om een zo compleet mogelijk beeld van de evaluatieve literatuur over internationaal cybersecuritybeleid te creëren, zijn ook aanbevelingen die slechts worden ondersteund door een enkele bron meegenomen in dit overzicht.

De volgende vragen worden in dit hoofdstuk beantwoord:

- 7.1 Volgens de literatuur: a) wat gaat er goed, b) wat gaat er niet goed, en c) welke aanbevelingen worden er gedaan over het beleid en de activiteiten van het Nederlandse internationale cybersecuritybeleid?
- 7.1.2 Volgens de literatuur: a) wat gaat er goed, b) wat gaat er niet goed, en c) welke aanbevelingen worden er gedaan over de internationale samenwerkingsverbanden?
- 7.1.3 Volgens de literatuur: a) wat gaat er goed, b) wat gaat er niet goed, en c) welke aanbevelingen worden er gedaan over de organisaties en projecten die Nederland financieel ondersteunt?
- 7.1.4. Volgens de literatuur: a) wat gaat er goed, b) wat gaat er niet goed, en c) welke aanbevelingen worden er gedaan over het internationaal cybersecuritybeleid gericht op het promoten van mensenrechten in het digitale domein?
- 7.2. Welke lessen kunnen worden geleerd van wat andere staten doen met hun internationale cybersecuritybeleid?

7.1. Diplomatieke inzet en financiële steun

Het internationale cybersecuritybeleid van het ministerie van Buitenlandse Zaken (BZ) bestaat uit de volgende activiteiten: (1) diplomatieke inzet in multilaterale fora zoals de VN, de OVSE, EU en de NAVO; multistakeholder fora zoals het *Global Forum for Cyber Expertise* en de *Freedom Online Coalition*; bilaterale relaties en ad-hoc coalities van gelijkgezinde landen; en (2) financiële steun aan multilaterale en multi-stakeholder fora; ngo's; projecten zoals de *Global Commission on the Stability of Cyberspace* en *The Hague Norms Project*. In de literatuur wordt de (potentiële) effectiviteit van diplomatieke inzet niet vergeleken met, of onderscheiden van, de (potentiële) effectiviteit van financiële steun, dus dat zal in dit hoofdstuk ook niet aan de orde komen. In plaats daarvan wordt gekeken naar de rol die het beleid van BZ, intergouvernementele organisaties, multi-stakeholder fora en ngo's spelen in het adequaat reageren op cyberoperaties, het bevorderen van de internationale rechtsorde in het cyberdomein, capaciteitsopbouw en het bevorderen van mensenrechten in het

[389] Deze hoofddoelstellingen zijn: (1) Nederland is in staat adequaat te reageren bij digitale aanvallen door statelijke actoren, al dan niet in coalitieverband zoals middels de EU Cyber Diplomacy Toolbox; (2) Nederland bevordert de internationale rechtsorde in het digitale domein, waaronder de waarborging van mensenrechten; (3) Nederland draagt bij aan de versterking van de cybersecuritycapaciteit van minder ontwikkelde landen om te zorgen dat de 'zwakste schakels' in de wereldwijde cybersecurityketen worden versterkt. Zie: Nederlandse Cyber Security Agenda (2018).

cyberdomein. De lessen die in dit hoofdstuk worden besproken, hebben alleen betrekking op het beleid van BZ. Dat betekent bijvoorbeeld dat de militaire component van 'adequaat reageren' niet aan de orde komt.[390] De volgende onderwerpen worden in paragraaf 7.1. besproken:

- Academici zijn het oneens over de mate waarin het mogelijk is om kwaadwilligen af te schrikken in het cyberdomein. Er bestaat daardoor onenigheid over wat een 'adequate' respons op een kwaadwillige cyberoperatie zou moeten inhouden;
- Bij het opstellen van beleid gericht op het adequaat reageren op cyberdreigingen is het van belang om rekening te houden met de actoren waar de dreiging van uitgaat. Gezien de toenemende mate waarin statelijke actoren en criminele netwerken zijn verweven, betogen academici dat het belangrijk is dat er gebruik wordt gemaakt van een *'whole-of-government'* aanpak;
- Het EU-cybersanctieregime is eenmalig ingezet (in juli 2020). Academici stellen dat het onvoldoende duidelijk is hoe EU-cyberdiplomatie in de praktijk afschrikkend zou kunnen werken;
- EU- en NAVO-lidstaten beschikken in verschillende mate over cybercapaciteiten, dit heeft volgens de literatuur een nadelig effect op de gedeelde *situational awareness* en bemoeilijkt het nemen van een beslissing omtrent een collectieve reactie;
- De NAVO heeft de afgelopen jaren sterke vooruitgang geboekt wat betreft het integreren van cybercapaciteiten in defensieoperaties, maar moet blijven ontwikkelen om de veranderende cyberdreiging vanuit statelijke actoren het hoofd te kunnen bieden;
- Zowel de EU, de NAVO als de VS zijn gebaat bij nauwere samenwerking en meer onderlinge transparantie;
- De VN GGE- en OEWG-debatten omtrent cybergedragsnormen zijn gepolariseerd. Er wordt volgens academici niet verwacht dat er middels deze werkgroepen consensus zal worden bereikt;
- Bij internationale fora gericht op het verspreiden van cybergedragsnormen heerst een behoefte aan een inclusievere aanpak en een beter gecoördineerde organisatie;
- Cybercapaciteitsopbouw is een effectieve methode voor het bevorderen van de internationale veiligheid maar kan ook een negatieve impact hebben op de bescherming van online mensenrechten. De huidige projecten kunnen op verschillende manieren verbeterd worden, alsook de onderlinge coördinatie tussen donoren;
- De Nederlandse focus op het bevorderen van mensenrechten in het cyberdomein wordt positief beoordeeld. Wereldwijd wordt het mensenrechtenaspect volgens de bestudeerde literatuur echter te oppervlakkig betrokken bij het opstellen van cybersecuritybeleid.

7.1.1. Adequaat reageren

Vergeleken met de conventionele oorlogsdomeinen (land, zee, lucht), bemoeilijken de karakteristieken van het cyberdomein de mogelijkheden voor een adequate respons, zo stellen academici. In het bijzonder wanneer 'adequaat' betekent dat de statelijke actor die verantwoordelijk is voor de aanval wordt afgeschrikt en zijn aanvallen stopt. Met andere woorden: er zijn wel maatregelen die ingezet kunnen worden, maar in de academische literatuur wordt benadrukt dat het

[390] Zie voor meer informatie bijvoorbeeld: King & Gallagher (2020), *Cyberspace Solarium Commission.*

niet per definitie duidelijk is in hoeverre die daadwerkelijk effectief ('adequaat') zijn.[391] Volgens conventionele afschrikkingstheorie is afschrikking alleen mogelijk wanneer het (potentiele) slachtoffer de aanvaller kan identificeren (attributie), en een geloofwaardige dreiging (retorsie/tegenmaatregel) kan communiceren (signalering).[392] Volgens sommigen is deze theorie niet toepasbaar in het cyberdomein.[393] In theorie betekent dit dat het gecompliceerd is om beleid te voeren dat een afschrikkend effect heeft op (potentieel) vijandige actoren. Andere academici beargumenteren echter dat afschrikking in het cyberdomein wel degelijk tot de opties behoort.[394] De middenpositie houdt in dat afschrikking wel mogelijk is, maar dat de analogie tussen afschrikking van cyberaanvallen en afschrikking van kinetische aanvallen onjuist is.[395] Bij het ontwikkelen van cyberdefensiebeleid zou dus expliciet rekening gehouden moeten worden met de specifieke, strategische aard van het cyberdomein.[396]

Een belangrijk onderdeel van het Nederlandse internationale cybersecuritybeleid is het reageren op een cyberoperatie middels een actief politiek attributiebeleid. Zo stelt de Defensie Cyber Strategie van 2018 dat dergelijk beleid "bijdraagt aan het afschrikkend vermogen en het minder aantrekkelijk maken van Nederland als doelwit van cyberaanvallen."[397] Max Smeets beargumenteert dat er weinig empirisch of theoretisch bewijs is voor de veronderstelling dat publieke attributie afschrikkend werkt of tot een stabieler cyberdomein leidt. Desondanks stelt Smeets dat dit niet betekent dat de overheid publieke attributie nooit zou moeten overwegen, maar dat dit proces veel afwegingen en factoren omvat.[398] Ook Finnemore en Hollis stellen dat beschuldigingen niet in elke context hetzelfde effect hebben. De effectiviteit van publieke attributie zou worden beïnvloed door de relatie tussen de beschuldigde en de beschuldiger: des te waardevoller de (politieke, economische of sociale) relatie, hoe groter het effect.[399] Volgens Roguski hebben de afwezigheid van juridisch taalgebruik en hard bewijs een negatief effect op het afschrikkingseffect van publieke attributie.[400] Daartegenover stellen Finnemore en Hollis dat ook politieke attributie, waarbij staten de retoriek van het internationaal recht vermijden, een cruciale rol kan spelen in het identificeren van bestaand recht

---

[391] Taddeo (2020), *Norms and Strategies for Stability in Cyberspace*, p. 6, Fischerkeller & Harknett (2017), *Deterrence is Not a Credible Strategy*, p. 381.
Investeren in cyberdefensie zou wel de kosten-baten analyse kunnen beïnvloeden waardoor een potentiële aanvaller overtuigd wordt dat de benodigde aanvalsinvestering te hoog is. Dit is afhankelijk van het afgeven van een geloofwaardige signalering over defensiecapaciteiten. Zie: Van der Putten et al. (2015), *Afschrikking als Veiligheidsconcept*, p. 56.
[392] Taddeo (2018), *Deterrence and Norms to Foster Stability in Cyberspace*, p. 324.
[393] Lan et al. (2010), *Global Cyber Deterrence*, p. 2.
[394] Crosston (2011), *World Gone Cyber MAD*, p. 100.
[395] Taddeo (2018), *Deterrence and Norms to Foster Stability in Cyberspace*, p. 324. Omdat kinetische en cyberconflicten op cruciale aspecten verschillen: o.a. duidelijkheid van attributie, de vernietigende kracht van de aanslagen, de aard van de betrokken actoren en doelwitten. Zie ook: Burton (2018), *Cyber Deterrence: A Comprehensive Approach?*.
[396] De mogelijkheid om adequaat te reageren wordt ook beïnvloed door het wel of niet (tijdig) kunnen identificeren van de dader en het aanleveren van overtuigend bewijsmateriaal. Onderzoek uit 2016 toonde aan dat het gemiddeld 146 dagen duurt voordat een kwaadwillige cyberoperatie wordt ontdekt. Zie: Bigelow (2017), *Mission Assurance: Shifting the Focus of Cyber Defence*, p. 5.
[397] Ministerie van Defensie (2018), *Defensie Cyber Strategie 2018*, p. 7, zie ook het voortgangsrapport van de Nederlandse Cybersecurity Agenda van 2019.
[398] Smeets (2019), *Werkt de Nederlandse Wijzende Vinger bij Cyberaanvallen?.*
[399] Finnemore & Hollis (2020), *Beyond Naming and Shaming*, p. 28.
[400] Roguski (2020), *Russian Cyber Attacks Against Georgia*.

en het ontwikkelingen van nieuwe rechtsregels, en zo de internationale rechtshandhaving kan bevorderen.[401]

Bij het opstellen van beleid gericht op het adequaat reageren op cyberdreigingen is het ook van belang om rekening te houden met de actoren waar de dreiging van uitgaat. Zoals in hoofdstuk 3 werd besproken, is er een ontwikkeling gaande die het moeilijk maakt om statelijke en niet-statelijke actoren van elkaar te onderscheiden. In de praktijk raken statelijke actoren en criminele netwerken steeds meer met elkaar verweven, wat betekent dat criminele cyberdreiging en statelijke cyberdreiging niet langer volledig van elkaar gescheiden kunnen worden. Wat betreft een adequate reactie op deze nieuwe dreiging betogen academici dat het belangrijk is dat er gebruik wordt gemaakt van een *'whole-of-government'* aanpak. Zo wordt betoogd dat, omdat cyberaanvallen de raakvlakken tussen ministeries benutten, het van cruciaal belang is dat een uitwisselingsysteem op nationaal niveau wordt ontwikkeld.[402] Een succesvolle cyberstrategie vereist dat gebruik wordt gemaakt van de unieke expertise, middelen en autoriteiten van elk ministerie, en van elk middel, of elke combinatie van middelen, die het meest effectief is om een bepaalde dreiging te verstoren.[403] Een voorbeeld van een dergelijk beleidsraamwerk is het DIMEFIL-model.[404] Het inzetten en combineren van deze verschillende instrumenten zou mogelijkheden bieden om de dreiging vanuit statelijke actoren (en hun cyber proxy's) te mitigeren.[405] Daarnaast wordt ook het belang van betere samenwerking tussen publieke en private sectoren benadrukt.[406]

In de volgende paragrafen worden de lessen besproken die uit de literatuur naar voren komen over het cybersecuritybeleid van de Europese Unie, de NAVO en de samenwerking tussen de EU, de NAVO en de VS – gericht op het adequaat reageren op cyberoperaties en -dreigingen.

Europese Unie

Een collectieve reactie op een cyberoperatie zou in theorie geloofwaardiger over kunnen komen en een groter afschrikwekkend effect kunnen hebben.[407] De mogelijkheid om over te gaan tot een gezamenlijke Europese respons wordt echter bemoeilijkt door enkele factoren. Ten eerste is de effectiviteit van de respons afhankelijk van de cybercapaciteit van de verscheidene lidstaten. Hoewel het lastig is om dit met zekerheid te stellen vanwege een bepaalde mate van ondoorzichtigheid, wordt er gesproken van een kloof in capaciteiten tussen EU-lidstaten.[408] Slechts enkele lidstaten zouden beschikken over de benodigde cyber- en inlichtingeninstrumenten om cyberoperaties correct te attribueren.[409] Dit bemoeilijkt een collectieve reactie op cyberactiviteiten gericht tegen één of meerdere EU-lidstaten. De lidstaten die beschikken over de attributiecapaciteiten kunnen bijvoorbeeld weigeren om deze te delen en moeten rekening houden met complexe internationale belangen. Ten tweede moeten de 27 lidstaten unaniem besluiten om in collectief EU-verband

[401] Finnemore & Hollis (2020), *Beyond Naming and Shaming*, p. 37.
[402] Leinhos (2020), *Cyber Defence in Germany: Challenges and the Way Forward*, p. 9.
[403] Carlin (2016), *Detect, Disrupt, Deter: Whole-of-Government Approach*, p. 394.
[404] Diplomatic, information, military, economic, financial, intelligence and law enforcement.
[405] Maurer (2018), *Cyber Proxies*, p. 179, Zie bijvoorbeeld ook: Rodriguez et al. (2020), *Putting the "FIL" into "DIME"*, p. 122.
[406] Carlin (2016), *Detect, Disrupt, Deter: Whole-of-Government Approach*, p. 396, King & Gallagher (2020), *Cyberspace Solarium Commission* p. 31, Leinhos (2020), *Cyber Defence in Germany: Challenges and the Way Forward*, p. 12.
[407] Ivan (2019), *Responding to Cyberattacks*, p. 3.
[408] Van der Meulen et al. (2015), *Cybersecurity in the European Union and Beyond*, p. 17.
[409] Ivan (2019), *Responding to Cyberattacks*, p. 6. Het zou gaan om het Verenigd Koninkrijk, Frankrijk, Duitsland, Nederland, Denemarken, Finland en enkele CEE-landen.

maatregelen te nemen.[410] Verschillen in opvattingen tussen EU-lidstaten over het juiste beleid vis-à-vis bijvoorbeeld Rusland[411] zou een poging om collectieve maatregelen tegen Russische cyberactiviteit te nemen, in de weg kunnen zitten.

Ondanks de ontwikkelingen in het Europese cybersecuritybeleid van de afgelopen jaren, heeft de EU nog nooit als collectief een cyberoperatie geattribueerd aan een staat.[412] Volgens de EU is dit een soevereine politieke beslissing die elke lidstaat per geval zelf moet overwegen.[413] Wel heeft de Raad van de EU in juli 2020 voor het eerst besloten om sancties op te leggen tegen zes personen en drie entiteiten[414] die verantwoordelijk worden geacht voor, of betrokken waren bij, verschillende cyberoperaties: de poging tot een cyberoperatie op de OPCW en de operaties die bekend werden als *WannaCry*, *NotPetya* en *Operation Cloud Hopper*.[415]

Het Europese sanctieregime is gericht op personen en niet-statelijke entiteiten, en bedoeld om een 'nauwkeurig' doelwit dat een bedreiging vormt, te schaden. Op die manier wordt de bevolking niet getroffen en wordt de impact op mensenrechten geminimaliseerd.[416] In de praktijk kunnen personen die werkzaam zijn voor, of banden hebben met, een staat wel op de sanctielijst worden geplaatst. Aleksei Morenets, Evgenii Serebriakov en Oleg Sotnikov staan op de cybersanctielijst vanwege hun deelname aan de poging tot het uitvoeren van een cyberoperatie tegen de OPCW en zijn alle drie "cyberoperator van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU)".[417] Op die manier kan het sanctieregime ook indirect ingezet worden tegen statelijke actoren, maar dit blijft een ingewikkelde politieke keuze. Academici stellen daarnaast dat het onvoldoende duidelijk is hoe EU-cyberdiplomatie in de praktijk afschrikkend zou kunnen werken.[418] Verscheidene academici beargumenteren dat het oprichten van een nieuwe internationale organisatie nodig is om attributie geloofwaardiger te maken, staten daadwerkelijk verantwoordelijk te houden voor hun vijandige cyberoperaties, en om het inzetten van toekomstige operaties tegen te houden.[419] Met een 'internationaal attributie mechanisme' bedoelen Shany en Schmitt een "entiteit die multinationaal en divers qua samenstelling is, bestaande uit overheidsfunctionarissen of private personen, die verantwoordelijk is voor het identificeren van de

---

[410] Wanneer een deel van de EU samenwerkt is er nog steeds sprake van een collectieve reactie, maar voor het besluit om beperkende maatregelen op te leggen geldt dat dit door de Raad met eenparigheid van stemmen moet worden aangenomen. Zie: Aannemings- en evaluatieprocedure voor EU-sancties, https://www.consilium.europa.eu/nl/policies/sanctions/adoption-review-procedure/.

[411] Hongarije en Bulgarije bekritiseren bijvoorbeeld het EU-Rusland beleid, het opleggen van sancties zou te hard zijn. Zie: Snyder (2018), *How the European Union Became Divided on Russia*, Emmot et al. (2019), *EU Divisions over Russia Mount*,

[412] Ivan (2019), *Responding to Cyberattacks*, p. 5, Botek (2019), *European Union Establishes a Sanction Regime.*

[413] "Gerichte beperkende maatregelen moeten worden onderscheiden van het aansprakelijk stellen van een derde staat voor cyberaanvallen. De toepassing van gerichte beperkende maatregelen komt niet neer op aansprakelijkheidsstelling, wat een soeverein politiek besluit is dat op individuele basis wordt genomen. Het staat iedere lidstaat vrij om de aansprakelijkheidsstelling van een derde staat met betrekking tot cyberaanvallen zelf te bepalen." Besluit (GBVB) 2019/797 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen, para. 9.

[414] Uitvoeringsverordening (EU) 2020/1125 van de Raad van 30 juli 2020 tot uitvoering van verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de unie of haar lidstaten bedreigen.

[415] Raad van de EU (2020), *EU Legt voor het Eerst Sancties op tegen Cyberaanvallen*.

[416] Botek (2019), *European Union Establishes a Sanction Regime.*

[417] Uitvoeringsverordening (EU) 2020/1125 van de Raad van 30 juli 2020 tot uitvoering van verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de unie of haar lidstaten bedreigen.

[418] Bendiek et al. (2017), *The EU's Revised Cybersecurity Strategy*, p. 2.

[419] Shany & Schmitt (2020), *An International Attribution Mechanism*, p. 221, Mueller et al. (2019), *Cyber Attribution,* p. 107.

statelijke of niet-statelijke actoren die een vijandige cyberoperatie hebben uitgevoerd of daarbij betrokken zijn geweest."[420] Idealiter zou de organisatie een manier vinden om de analytische middelen van overheidsinstanties te combineren met de technische expertise die aanwezig is in de private cybersecuritysector.[421] Uit het onderzoek van Shany en Schmitt is gebleken dat vooral minder technisch geavanceerde staten vatbaar zijn voor het idee om een dergelijke organisatie op te richten, evenals staten die minder succesvol zijn in het mobiliseren van internationale steun.[422]

In de literatuur wordt gesteld dat de ontwikkelingen op Europees niveau, en in het bijzonder het cybersanctieregime, zouden kunnen bijdragen aan het versterken van de wereldwijde naleving van bestaande cybernormen. Zo wordt beargumenteerd dat EU-cybersancties het gesprek over soortgelijke maatregelen binnen VN-verband kunnen bevorderen.[423] In die zin is de *cyber diplomacy toolbox* een stap voorwaarts, maar in de literatuur worden ook een aantal problemen geïdentificeerd. Academici stellen dat belangrijke definities en wetgeving missen. Het is bijvoorbeeld nog onduidelijk welk gedrag aanvaardbaar is en wanneer operaties beantwoord moeten worden met sancties.[424]

Wat betreft het bredere EU-cyberdefensiebeleid wordt in de academische literatuur gesproken van institutionele en financiële fragmentatie.[425] De betrokkenheid van veel verschillende instituties zouden een complex landschap nog ingewikkelder maken. Academici waarschuwen dan ook voor de tendens om nieuwe initiatieven te verkiezen boven de reeds bestaande structuur en agentschappen, omdat overlappende mandaten zouden kunnen leiden tot duplicatie en inefficiëntie.[426]

In de literatuur worden de volgende aanbevelingen gedaan met betrekking tot het verbeteren van de mogelijkheid om adequaat te reageren op cyberdreigingen of –aanvallen in EU-verband:

1. Integreer de *cyber diplomacy toolbox* in het Politieke Crisis Respons-mechanisme en andere EU-crisis management mechanismes;[427]
2. Stimuleer het continu delen van informatie tussen lidstaten;[428]
3. Combineer beperkende maatregelen (sancties) met andere instrumenten;[429]
4. Creëer een uniforme standaard voor attributie;[430]
5. Definieer *red lines* en niveaus van escalatiegereedheid per lidstaat;[431]

[420] Shany & Schmitt (2020), *An International Attribution Mechanism*, p. 201.
[421] Shany & Schmitt (2020), *An International Attribution Mechanism*, p. 215.
[422] Shany & Schmitt (2020), *An International Attribution Mechanism*, p. 201.
[423] Moret & Pawlak (2017), *The EU Cyber Diplomacy Toolbox*, p. 2, Bendiek & Pander - Maat (2019), *The EU's Regulatory Approach to Cyber-Security*, p. 25.
[424] Ivan (2019), *Responding to Cyberattacks*, p. 8.
[425] Bendiek et al. (2017), *The EU's Revised Cybersecurity Strategy*, p. 3.
[426] Van der Meulen et al. (2015), *Cybersecurity in the European Union and Beyond*, p. p.117.
[427] European Court of Auditors (2019), *Challenges to Effective EU Cybersecurity Policy*, p. 43.
[428] European Court of Auditors (2019), *Challenges to Effective EU Cybersecurity Policy*, p. 43.
[429] Bijv. diplomatieke handelingen, handelsbesprekingen, samenwerking met andere landen/ multilaterale organisaties/private sector, en in sommige gevallen militaire afschrikking. Moret & Pawlak (2017), *The EU Cyber Diplomacy Toolbox*, p. 3.
[430] Finnemore & Hollis (2020), *Beyond Naming and Shaming*, p. 35.
[431] Bendiek et al. (2017), *The EU's Revised Cybersecurity Strategy*, p. 6.

6. Bouw een netwerk van relaties tussen overheden en de technische wereld. De expertise die uit nauwe werkrelaties kan ontstaan is met name gunstig met betrekking tot het toezicht op de naleving en het uitwisselen van informatie over de nieuwste bedreigingen.[432]

NAVO

Uit de literatuur blijkt dat er grote vooruitgang is geboekt sinds de NAVO is begonnen met het integreren van cybercapaciteiten in defensieoperaties. Er worden met enige regelmaat oefeningen uitgevoerd die bedoeld zijn om nieuwe uitdagingen te identificeren en meer kennis op te doen van strategische en operationele concepten om zo het beleid adequaat te kunnen updaten.[433] Dat de NAVO ondertussen in staat is om dit soort oefeningen (succesvol) uit te voeren, wordt door academici gezien als bewijs dat het integreren van cyberoperaties in de tweede fase terecht is gekomen.[434] Zij stellen dat de volgende fase in de ontwikkeling pas is aangebroken wanneer de oefeningen uit gecompliceerdere scenario's bestaan, zodat getest wordt of de Alliantie daadwerkelijk in staat is om effectief samen te werken wanneer er dreiging uitgaat van meerdere, verschillende soorten cyberaanvallen tegelijkertijd.[435]

In de bestudeerde literatuur wordt positief gesproken over de stappen die de NAVO in korte tijd heeft gezet om cyberdreigingen aan te pakken. Deze stappen zijn veelbelovend en worden gezien als bewijs dat het bondgenootschap een relevante, sterke militaire alliantie is die in staat is om te vernieuwen en mee te gaan met technologische ontwikkelingen.[436] Daartegenover wordt gesteld dat de gezette stappen slechts fundamenteel zijn,[437] en de NAVO nog onvoldoende mogelijkheden heeft om de toenemende en veranderende cyberdreiging vanuit statelijke actoren het hoofd te bieden.[438] In september 2018 werd beoordeeld dat het bondgenootschap slechts op ongeveer 10 procent gereed is wat betreft het begrijpen, reageren op en voorkomen van cyberdreigingen.[439] Daarnaast mist er volgens een enkele academicus duidelijk beleid en een bevelstructuur in de uitvoering van de operaties.[440] Naast de algemene aanbeveling dat de NAVO zich verder zal moeten blijven ontwikkelen, worden in de literatuur ook een aantal specifieke adviezen geformuleerd.

Ten eerste wordt beargumenteerd dat de NAVO zich meer zou moeten focussen op de lange(re) termijn door bijvoorbeeld te investeren in onderzoek en ontwikkeling, het uitvoeren van

---

[432] Moret & Pawlak (2017), *The EU Cyber Diplomacy Toolbox*, p. 4.

[433] In dit soort oefeningen wordt bijvoorbeeld gefocust op het veilig houden van verkiezingen en het beschermen van kritieke infrastructuren. Ablon et al. (2019), *Operationalizing Cyberspace*, p. 12.

[434] Waar een eerste fase zou bestaan uit het ontwikkelen van beleid en individuele trainingen, omhelst de tweede fase het uitvoeren van oefeningen op strategisch, operationeel en tactisch niveau. Wanneer er sprake is van een oefening waarbij het volledige scala aan cyberoperaties wordt ingezet, bevindt de NAVO zich in de derde fase. (In het Engels wordt gesproken over de *crawl/walk/run* strategie). Zie: Ablon et al. (2019), *Operationalizing Cyberspace*, p. 13.

[435] Bigelow (2017), *Mission Assurance: Shifting the Focus of Cyber Defence*, p. 7.

[436] Ablon et al. (2019), *Operationalizing Cyberspace*, p. 31.

[437] Ilves et al. (2016), *European Union and NATO*, p. 138.

[438] Ilves et al. (2016), *European Union and NATO*, p. 128.

[439] Arts (2018), *Offense as the New Defense*, p. 1.

[440] Arts (2018), *Offense as the New Defense*, p. 1.

experimenten en haalbaarheidsstudies.[441] Deze activiteiten zouden inzichten kunnen bieden over de intenties van tegenstanders, waardoor de Alliantie beter kan anticiperen op dreigingen. Daarnaast kan kennis van buitenlandse cybercapaciteiten, van bijvoorbeeld China en Rusland, dienen als inspiratiebron om de cyberstrategie en -capaciteiten van de NAVO te verbeteren.[442]

Ten tweede zou de NAVO tegen eenzelfde probleem aanlopen als de EU. Namelijk dat niet alle lidstaten beschikken over dezelfde cybercapaciteiten en sommigen zich meer zorgen maken over cybersecurity dan anderen.[443] De oplossing is het ontwikkelen of verbeteren van de gedeelde *situational awareness*. Om dit te bereiken is het delen van informatie tussen lidstaten cruciaal.[444] In de literatuur worden meerdere voorstellen genoemd die allen gericht zijn op het creëren van een nieuw initiatief waarin (NAVO/EU-) lidstaten informatie delen over o.a. aanwijzingen en waarschuwingen,[445] door middel van open source, geanonimiseerde en opgeschoonde informatie uit openbare en niet-openbare bronnen, inclusief geclassificeerde bronnen.[446] Dit zou de gedeelde *situational awareness* bevorderen en bijdragen aan de mogelijkheid om als collectief te reageren wanneer er sprake is van cyberdreiging. Weerstand tegen meer transparantie zou vooral afkomstig zijn van de Verenigde Staten.[447] Academici beargumenteren dat dit gebrek aan transparantie ervoor zorgt dat het voor de NAVO moeilijk zal blijven om in te schatten welke capaciteiten beschikbaar zijn en hoe bestaande hiaten het beste kunnen worden opgevuld.[448]

In de bestudeerde literatuur wordt ook geadviseerd om duidelijke definities op te stellen. Omdat er geen internationale afspraken bestaan wat betreft het definiëren en meten van cyberaanvallen, zouden gegevens uit verschillende nationale contexten moeilijk te vergelijken zijn.[449] Uiteindelijk zou dit het delen van informatie, wanneer dat gebeurt, ineffectief maken: zonder standaarden en waarneembare statistieken zijn waarschuwingen namelijk niet juist te interpreteren en dus onbruikbaar.[450] Tot dusver heeft de NAVO ervoor gekozen om geen definities te publiceren om zo strategische ambiguïteit te behouden en te voorkomen dat ze het slachtoffer worden van aanvallen die opzettelijk onder een bepaalde grens blijven. Deze strategie zou echter evengoed grijze gebieden creëren die geëxploiteerd kunnen worden en is er weinig bewijs dat het gebrek aan definities effectief is in het voorkomen van aanvallen.[451] Daarnaast wordt gesteld dat het eenduidig definiëren van cyberaanvallen en het opstellen van een reeks basisprincipes met betrekking tot het inzetten van cyberoperaties bijdragen aan het vermogen om adequaat te reageren. Academici beargumenteren dat het individueel beoordelen van elke cyberdreiging of -aanval, en het daarbij horende politieke besluitvormingsproces, een snelle en proportionele respons in de weg zou kunnen

---

[441] Ablon et al. (2019), *Operationalizing Cyberspace*, p. 31.
[442] Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 6.
[443] Staten met de meeste cybercapaciteiten zijn beter in staat om vast te stellen dat ze het slachtoffer zijn van een cyberoperatie. Staten met minder sterk ontwikkelde cybercapaciteiten zouden (onjuist) kunnen stellen dat ze zich minder onveilig voelen of minder onveilig zijn, omdat ze niet de capaciteiten hebben om een correct 'bewustzijn' te creëren. Zie: Burton (2015), *NATO's Cyber Defence*, p. 312, Jinghua (2018), *What Really Matters in 'Defending Forward'?*.
[444] Arts (2018), *Offense as the New Defense*, p. 6.
[445] Ablon et al. (2019), *Operationalizing Cyberspace*, p. 28.
[446] Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 3.
[447] Arts (2018), *Offense as the New Defense*, p. 6.
[448] Ablon et al. (2019), *Operationalizing Cyberspace*, p. 11.
[449] Arts (2018), *Offense as the New Defense*, p. 2.
[450] Soesanto (2018), *In Cyberspace, Governments Don't Know How to Count*.
[451] Arts (2018), *Offense as the New Defense*, p. 8.

staan.[452] Daarnaast zou het gebrek aan duidelijke afspraken ertoe kunnen leiden dat de NAVO-lidstaten, gekarakteriseerd door een zwakke mate van cohesie en uiteenlopende cyberdreigingservaringen, geen consensus weten te bereiken gedurende een crisissituatie.[453] Om die reden wordt geadviseerd dat de NAVO een duidelijke strategie formuleert, inclusief besluitvormingsproces, waarin weinig ruimte voor interpretatie overblijft.[454] Daarbij zou ook aandacht moeten worden besteed aan het potentiële risico op escalatie, in het bijzonder wanneer de NAVO richting een offensieve cyberdefensie dreigt te bewegen.[455]

Verschillende academici betogen dat de NAVO op de goede weg is. Maar om de toenemende en veranderende cyberdreiging het hoofd te kunnen bieden, wordt benadrukt dat de NAVO zich moet blijven ontwikkelen.

De belangrijkste aanbevelingen die in de literatuur worden genoemd, worden hieronder kort samengevat:

1. Focus op de lange termijn door middel van onderzoek naar de cybercapaciteiten van tegenstanders. Dit maakt het mogelijk om beter te anticiperen op dreigingen en kan dienen als inspiratiebron voor vernieuwing van de NAVO-cyberstrategie en -capaciteiten;[456]
2. Creëer gedeelde *situational awareness* door middel van transparantie en het openen van de juiste kanalen voor het delen van (geclassificeerde) informatie tussen lidstaten en partnerorganisaties;[457]
3. Ontwikkel een beleidsstrategie waar een duidelijke bevelstructuur in is aangebracht en eenduidige definities in zijn opgenomen;[458]
4. Stel een memorandum op waarin overeenstemming over het integreren van offensieve cybercapaciteiten wordt bereikt. Dit helpt de onenigheid tussen de bondgenoten te verminderen; en het vertrouwen, de transparantie en de doeltreffendheid van het verstoren en afschrikken van de activiteiten van tegenstanders in het cyberdomein te vergroten;[459]

Ontwikkel een beleidsstrategie voor het offensieve gebruik van het cyberdomein, waarin het collectieve gebruik van offensieve capaciteiten volgens de regels van de Alliantie wordt uiteengezet en regelingen worden opgenomen wat betreft de lastenverdeling en het inzetten van troepen.[460]

Samenwerking EU-NAVO-VS

[452] Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 7.
[453] Arts (2018), *Offense as the New Defense*, p. 6.
[454] Shea (2020), *NATO in the Fourth domain: How Well is it Doing?*, p. 9.
[455] Arts (2018), *Offense as the New Defense*, p. 8.
[456] Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 6.
[457] Arts (2018), *Offense as the New Defense*, p. 6, Ablon et al. (2019), *Operationalizing Cyberspace*, p. 28, Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 3.
[458] Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 7.
[459] Smeets (2020), *US Cyber Strategy*, p. 449.
[460] Shea (2020), *NATO in the Fourth domain: How Well is it Doing?*, p. 9.

In de literatuur wordt ook het belang van samenwerkingen met partnerorganisaties steeds duidelijk benadrukt.[461] Trans-Atlantische samenwerking wordt gezien als essentiële factor in het voorkomen, opsporen en afschrikken van cyberoperaties.[462] Met name de EU en NAVO worden in de academische literatuur beschouwd als belangrijke partners. Daarnaast wordt beargumenteerd dat het voor zowel de VS als de EU voordelig zou zijn om een EU-NAVO-VS-samenwerking aan te gaan.[463] In het bijzonder op het gebied van *cyber forensics*, voor het verbeteren van attributie-mogelijkheden, en het vergroten van de weerbaarheid tegen cyberdreigingen zou nauwere samenwerking tussen deze actoren een verschil kunnen maken.[464] De toenemende mate waarin de EU en de NAVO in de afgelopen jaren zijn gaan samenwerken wordt derhalve door zowel academici als de twee organisaties als een positieve ontwikkeling beschouwd die ook in de toekomst van groot belang zal zijn.[465]

Het samenwerkingsproject tussen de EU en de NAVO wordt, naast het politieke conflict tussen Turkije en Cyprus, volgens academici gehinderd doordat er geen directe lijn tussen de NAVO en de EU bestaat die het mogelijk maakt om geclassificeerde informatie te delen. Ook zou er sprake zijn van een gebrek aan communicatie waardoor het onduidelijk is of de algemene strategie wel in lijn is met de bredere inspanningen van de NAVO/EU.

Lété en Pernik doen de volgende aanbevelingen voor een effectievere EU/NAVO-samenwerking:

1. Creëer een *joint cyber threat analysis hub* waar waarschuwingsindicatoren worden gemonitord en geanalyseerd. De output kan gebruikt worden bij het opstellen van operationeel en strategisch beleid. Dit zou ook kunnen bijdragen aan het opbouwen van een civiel-militair en publiek-privaat netwerk. Ter verbetering van onderling vertrouwen zou ook beleid opgesteld kunnen worden met betrekking tot welk type informatie moet worden gedeeld, wie deze informatie moet ontvangen, en wanneer deze moet worden gedeeld;

2. Creëer een *cyber innovatie comité*, bestaande uit civiele en militaire officieren, onderzoekers, experts en technologieondernemers. Het comité kan een rol spelen in het dichten van de kloof in technologische capaciteit tussen de lidstaten, en tussen de publieke en private sector, door relevante innovatieve instrumenten te identificeren. Daarnaast is een dergelijke samenwerking nuttig voor het delen van *best practices* en *lessons learned*;[466]

[461] Arts (2018), *Offense as the New Defense*, p. 6 , Ilves et al. (2016), *European Union and NATO*, p. 136-137 , Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 1, Burton (2015), *NATO's Cyber Defence*, p. 310.
[462] Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 3.
[463] Nauwere samenwerking tussen de EU en NAVO wordt voornamelijk in de weg gestaan door het Cyprus-Turkije conflict. Zie: Pernik (2014), *Improving Cyber Security: NATO*, p. 9, Koops (2017), *Theorising Inter-Organisational Relations*, p. 330, Nordic Monitor (2020), *Turkey Blocked EU-NATO Partnership Programs*.
[464] Ilves et al. (2016), *European Union and NATO*, p. 137.
[465] Voornamelijk vanwege de groeiende cyberdreiging afkomstig van statelijke actoren, een herrijzend Rusland en een nieuwe vorm van conflict waarbij kinetische operaties gepaard zullen gaan met cyberaanvallen. Maar ook de COVID-19 pandemie heeft de waarde en de relevantie van de NAVO-EU samenwerking bewezen. Zie: Fifth Progress Report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.
[466] Ablon et al. (2019), *Operationalizing Cyberspace*, p. 21.

3. Richt een *joint working group* op die de crisis respons teams van de EU en de NAVO synchroniseert. Voor een effectieve samenwerking moet een crisisresponsstrategie ontwikkeld worden waarin het volledige scala aan EU/NAVO-cybercapaciteiten worden meegenomen. Gezien de EU en de NAVO over verschillende instrumenten beschikken, is het cruciaal dat deze op elkaar worden afgestemd. Daarnaast zou de werkgroep kunnen verduidelijken hoe verantwoordelijkheid wat betreft attributie en het nemen van tegenmaatregelen is verdeeld (op nationaal/supranationaal niveau);

4. Ontwikkel een reeks EU/NAVO-basisprincipes die verduidelijken in welke omstandigheden een collectieve reactie is vereist. Voor een effectieve samenwerking is consensus over welke normen en gedragsregels gelden in het cyberdomein van cruciaal belang, in het bijzonder wanneer het recht op (digitale) zelfverdediging wordt geactiveerd en welke acties onder het collectieve defensiemechanisme zijn toegestaan.[467]

7.1.2. Bevorderen internationale rechtsorde in het cyberdomein

Het bevorderen van de internationale rechtsorde in het cyberdomein vindt voornamelijk plaats in intergouvernementele organisaties en internationale fora. Ook uitspraken van individuele staten, bijvoorbeeld in reactie op cyberoperaties, dragen bij aan het stimuleren van cybergedragsnormen.[468] Zo stelde Nederland begin 2020 bijvoorbeeld dat Rusland, middels de cyberaanval op Georgië, de normen van verantwoord staatsgedrag heeft overtreden.[469] Naast het leveren van een diplomatieke bijdrage in de reeds bestaande platformen gericht op het bevorderen van cybernormen,[470] heeft Nederland zelf ook dergelijke platformen opgericht. De *Global Commission for the Stability of Cyber Space* is bijvoorbeeld een samenwerking tussen Nederland en twee vooraanstaande denktanks.[471] Nederland wordt daarom ook wel door sommige academici een 'meta' norm-entrepreneur genoemd.[472] In de volgende paragrafen wordt de beschikbare literatuur over de organisaties waar Nederland bij betrokken is, besproken: de VN GGE en OEWG; *Freedom Online Coalition* (FOC)*; Global Forum on Cyber Expertise* (GFCE); *Global Commission on the Stability of Cyberspace* (GCSC).

Over het algemeen worden de activiteiten van Nederland, inclusief het herhaaldelijk uitspreken van de Nederlandse interpretatie van internationaal recht in het cyberdomein, positief beoordeeld.[473] Daarnaast is bij sommigen het beeld ontstaan dat Nederland, in vergelijking met andere staten, vooruitloopt wat betreft het stimuleren van bepaalde normen.[474] De posities van

[467] Lété & Pernik (2017), *EU-NATO Cybersecurity*, p. 4-7.
[468] Finnemore & Hollis (2020), *Beyond Naming and Shaming*, p. 37.
[469] The Netherlands considers Russia's GRU responsible for cyberattacks against Georgia, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia.
[470] Schmitt (2018), *International Cyber Norms*, p. 12.
[471] Henriksen (2019), *The End of the Road for the UN GGE Process*, p. 7.
De twee denktanks zijn The Hague Center for Strategic Studies en het East-West Institute.
[472] Adamson & Homburger (2019), *Let Them Roar*, p. 229.
[473] Moynihan (2019), *The Application of International Law*, p. 2, Schmitt (2018), *International Cyber Norms*, p. 12, Adamson & Homburger (2019), *Let Them Roar*, p. 234.
[474] Adamson & Homburger (2019), *Let Them Roar*, p. 227.

staten dreigen hierdoor verder uiteen te komen liggen en dit zou er toe kunnen leiden dat het lastiger wordt om overeenkomsten te bereiken met niet-gelijkgestemde staten.[475]

VN GGE en OEWG

In enkele van de voorgaande hoofdstukken is benadrukt dat de debatten die op internationaal niveau gevoerd worden over het reguleren van het cyberdomein, zijn gepolariseerd. Het oprichten van twee verschillende groepen die beide onder de VN-auspiciën werken aan het ontwikkelen van normen en regels voor het cyberdomein is niet alleen het gevolg van de tweedeling tussen staten die focussen op *cybersecurity* en staten die spreken van *information security*, maar heeft ook gezorgd voor verdere polarisatie en uiteendrijvende, soms zelfs conflicterende, wereldbeelden. Zo wordt door academici gesteld dat de VS en gelijkgestemde staten de GGE gebruiken om hun eigen cybergedragsnormen te verspreiden. De VS zou gebruikmaken van de GGE om voor internetbeleid gericht op vrijheid te strijden, en Rusland zou via de OEWG het strenger controleren van het internet promoten.[476] Dit draagt niet bij aan de mogelijkheid om de internationale rechtsorde in het cyberdomein te bevorderen via de VN.

Ook is er kritiek van zowel academici als verschillende staten op het exclusieve karakter van de GGE.[477] Een beperkt aantal staten kan per GGE aanwezig zijn bij de bijeenkomsten. Het gevolg zou zijn dat, zelfs wanneer de betrokken experts consensus bereiken, er geen sprake is van *mondiale* consensus.[478] Hoewel het aantal toegestane deelnemers sinds de eerste GGE is verhoogd, van 15 tot 25, is de OEWG open voor alle lidstaten die geïnteresseerd zijn.[479] Het nadeel hiervan is dat het moeilijker is om tot een overeenkomst te komen.[480]

Sommige academici achten het zeer onwaarschijnlijk dat er nog verdere consensus bereikt zal worden middels de GGE of OEWG. Zij pleiten daarom voor een meer regionale en individuele aanpak.[481] Deze organisaties kunnen de discussie omtrent cybernormen verder bevorderen waar mondiale consensus uitblijft. Mochten de GGE en OEWG-bijeenkomsten toch worden voortgezet, dan zouden regionale organisaties daar zo veel mogelijk bij moeten worden betrokken. Ondertussen worden hiertoe eerste pogingen ondernomen. Dit wordt dan ook gezien als een positieve ontwikkeling.[482] Schmitt, Ott en Osula pleiten ook voor meer samenwerking met ngo's, academici en private actoren via een multi-stakeholder model.[483] Schmitt beargumenteert daarnaast dat staten het beste herhaaldelijk uitspraak kunnen doen over specifieke toepassingen van het internationaal recht in het cyberdomein, aangezien ook deze individuele (of collectieve) uitspraken bijdragen aan de ontwikkeling en verspreiding van normen.[484]

---

[475] Crandall & Allan (2015), *Small States and Big Ideas*, p. 347.
[476] Ruhl et al. (2020), *Cyberspace and Geopolitics*, p. 8, Finnemore & Hollis (2016), *Constructing Norms for Global Cybersecurity*, p. 448.
[477] Ruhl et al. (2020), *Cyberspace and Geopolitics*, p. 6.
[478] Hampson & Sulmeyer (eds) (2017), *Getting beyond Norms*, p. 21.
[479] Ruhl et al. (2020), *Cyberspace and Geopolitics*, p. 8.
[480] Ruhl et al. (2020), *Cyberspace and Geopolitics*, p. 8.
[481] Brown et al. (2017), *Briefing Document: Cybersecurity Policy and Human Rights*, p. 10.
[482] Ott & Osula (2019), *The Rise of the Regionals*, p. 6-7.
[483] Schmitt (2018), *International Cyber Norms*, p. 4, Ott & Osula (2019), *The Rise of the Regionals*, p. 19.
[484] Schmitt (2018), *International Cyber Norms*, p. 4.

In de bestudeerde literatuur worden in ieder geval de volgende drie aanbevelingen gedaan met betrekking tot diplomatieke inzet (via de VN-werkgroepen):

1. Creëer internationale cybergedragsnormen via een bottom-up aanpak waarbij wordt samengewerkt met stakeholders vanuit de private sector, ngo's en de academische wereld;[485]
2. Draag publiekelijk, maar niet per se via de GGE of OEWG, standpunten uit over de specifieke toepassingen van het internationaal recht in het cyberdomein;[486]

Betrek regionale organisaties bij de GGE en OEWG, dit zou de discussie omtrent cybernormen verder kunnen bevorderen waar mondiale consensus uitblijft.[487]

Freedom Online Coalition

De FOC is opgericht in Den Haag in 2011 als een coalitie van vijftien staten die focussen op de bescherming van internetvrijheid. In 2020 is de coalitie uitgegroeid tot dertig leden, waaronder veertien EU-lidstaten.[488] Het belangrijkste uitgangspunt van de coalitie is dat mensenrechten online gelden en dat een vrij en open internet bijdraagt aan de verbetering van mensenrechten en economische ontwikkeling.[489] Daarbij committeren de leden zich aan de normen en waarden zoals uiteengezet in de Tallinn Manual: mensenrechten en veiligheid online worden gezien als twee complimenterende concepten.[490] De coalitie coördineert diplomatieke pogingen om de vrijheid van meningsuiting, vergadering en privacy online te beschermen. Hiervoor delen zij informatie, gezamenlijke publieke statements, en nemen ze deel aan internationale overleggen.[491]

De FOC wordt in de literatuur neergezet als een nuttige en effectieve poging om een betere balans te creëren tussen nationale veiligheid en de bescherming van mensenrechten binnen het cyberdomein.[492] Zo wordt gesteld dat de staten die onderdeel uitmaken van deze coalitie het goede voorbeeld geven aan de rest van de wereld.[493] Aangezien de FOC inzet op samenwerking met stakeholders via meerdere speciaal opgerichte werkgroepen, kan de coalitie in discussie blijven met experts en *civil society*. Deze werkgroepen bieden de mogelijkheid om experts te spreken en kennis op te doen over onderwerpen zoals internetvrijheid. Daarnaast zorgt de FOC er ook voor dat kennis over technologische ontwikkelingen en de eventuele impact daarvan op mensenrechten wordt gedeeld met de lidstaten.[494]

In de bestudeerde literatuur komen ook punten van kritiek naar voren, met name over hoe de coalitie in de praktijk functioneert. Zo wijzen verscheidene bronnen erop dat meerdere lidstaten de afgesproken normen en waarden met betrekking tot mensenrechten niet volgen. Er zijn dan ook

[485] Schmitt (2018), *International Cyber Norms*, p. 4.
[486] Schmitt (2018), *International Cyber Norms*, p. 4.
[487] Ott & Osula (2019), *The Rise of the Regionals*, p. 1-2.
[488] Garside (2020), *Democracy and Digital Authoritarianism*, p. 12, Adamson & Homburger (2019), *Let Them Roar*, p. 227.
[489] Morgan (2016), *Clarifying Goals, Revitalizing Means*, p. 5.
[490] Piccone (2018), *Democracy and Digital Technology*, p. 32, Mann et al. (2018), *The Limits of (Digital) Constitutionalism*, p. 372.
[491] Wagner et al. (2015), *Surveillance and Censorship*, p. 22.
[492] Adamson & Homburger (2019), *Let Them Roar*, p. 228, Piccone (2018), *Democracy and Digital Technology*, p. 34.
[493] Piccone (2018), *Democracy and Digital Technology*, p. 34.
[494] Morgan (2016), *Clarifying Goals, Revitalizing Means*, p. 8-9.

beschuldigingen geuit richting Mongolië, het VK en de VS. Zij zouden de FOC gebruiken om eventuele kritiek op mensenrechtenschendingen binnen hun eigen nationale cyberdomein onderuit te halen.[495] De onthullingen van Snowden over de NSA en het Britse *Government Communications Headquarters (GCHQ)* hebben aangetoond dat staten in de praktijk afwijken van de FOC-normen waaraan zij zich hebben gecommitteerd. [496] Dat staten zich hebben aangesloten bij de FOC betekent dus niet dat ze de normen en waarden van de organisatie daadwerkelijk doorvoeren in hun nationale wetgeving.[497] Zo schendt de Australische wetgeving bijvoorbeeld de normen van de FOC.[498] Sinds Australië lid is geworden van de FOC in 2015, is het niveau van de Australische internetvrijheid zelfs gedaald.[499]

In 2016 werd een onafhankelijke evaluatie van de FOC uitgevoerd. Hieruit bleek dat er een gebrek is aan verantwoordingsmechanismen binnen de organisatie. Er was volgens dit onderzoek te weinig controle op het nakomen van de gemaakte afspraken.[500] Dit onderzoek kaartte ook aan dat er op veel organisatorische aspecten ruimte is voor verbetering. Zo werd gesteld dat een stabieler financieel stelsel er bijvoorbeeld toe zou kunnen leiden dat de FOC professionaliseert. Dit zou bereikt kunnen worden door het huidige systeem van vrijwillige donaties te vervangen door een vaste lidmaatschapsbijdrage. Ook bestonden er geen goede afspraken over het niveau waarop lidstaten betrokken zijn bij de besluitvoering. Hierdoor was er sprake van onvoldoende participatie van hooggeplaatste officieren of ministers. De aanwezige afgezanten waren echter niet geautoriseerd om daadwerkelijk beslissingen te maken. Daarnaast was er een gebrek aan transparantie tussen zowel de FOC en de werkgroepen, als tussen de FOC en de buitenwereld. Het is voor veel van de deelnemers van deze werkgroepen ook niet duidelijk wat er gebeurt met de uitkomsten van hun werk. Ook bestond er te weinig transparantie over hoe de organisatie wordt gefinancierd. Het gebrek aan transparantie zorgde er ook voor dat weinig niet-FOC-leden doorhebben wat de organisatie teweegbrengt op diplomatiek vlak. De FOC zou dit kunnen verhelpen door een concreet doel te formuleren en dit vervolgens actief naar de buitenwereld uit te dragen.[501] Het laatste punt van kritiek kwam van enkele deelnemers. Zij stelden dat de nadruk binnen de organisatie te veel op veiligheid ligt, in plaats van op mensenrechten.[502]

Het onafhankelijke onderzoek naar de FOC, gepubliceerd in 2016, bevat onder andere de volgende aanbevelingen:

1. Voer duidelijke verantwoordingsmechanismen in zodat staten en stakeholders gemakkelijker zorgen kunnen uitdrukken;
2. Stel een financieel meerjarenplan op en voer een betaald lidmaatschap in;
3. Leg een formele link aan tussen de werkgroepen en de coalitie, stel een beleidsplan op waaruit duidelijk wordt wat gedaan wordt door welke werkgroep;

[495] Wagner et al. (2015), *Surveillance and Censorship*, p. 22.
[496] Mann et al. (2018), *The Limits of (Digital) Constitutionalism*, p. 12.
[497] Morgan (2016), *Clarifying Goals, Revitalizing Means*, p. 11, Mann et al. (2018), *The Limits of (Digital) Constitutionalism*, p. 4-5.
[498] Het recht op privacy is niet beschermd in de grondwet. Vrijheid van meningsuiting is enkel indirect beschermd via het recht op politieke communicatie.
[499] Mann et al. (2018), *The Limits of (Digital) Constitutionalism,* p. 12.
[500] Morgan (2016), *Clarifying Goals, Revitalizing Means*, p. 10, 19.
[501] Morgan (2016), *Clarifying Goals, Revitalizing Means*, p. 4, 9. 10, 17.
[502] Morgan (2016), *Clarifying Goals, Revitalizing Means*, p. 10.

4. Formuleer concrete doelen en normen, draag deze publiekelijk uit en rapporteer transparant over activiteiten. [503]

Global Forum on Cyber Expertise

Het GFCE wordt in de literatuur beoordeeld als ideaal platform voor het uitwisselen van ideeën over capaciteitsopbouw.[504] Het GFCE is opgericht door Nederland en is ondertussen uitgegroeid tot een mondiaal platform waar staten, internationale organisaties en private bedrijven samenkomen.[505] Ott en Osula stellen dat het forum in de toekomst een belangrijke *facilitator* kan zijn voor kennis- en normuitwisseling tussen verschillende regio's. Dit kan onnodige duplicatie van activiteiten binnen verschillende regionale organisaties voorkomen. Daarnaast kan het forum een belangrijke rol spelen bij cybercapaciteitsprojecten.[506] De verwachting is dat het forum voornamelijk gebruikt zal worden voor het verzamelen en bespreken van ideeën, niet dat de organisatie een coördinerende rol op zich gaat nemen. Daarbij schrikt de focus op een vrij en open internet niet-gelijkgestemde staten zoals Rusland en China af. Dit staat verdere samenwerking en kennisuitwisseling tussen verschillende regio's in de weg.[507]

In de literatuur worden de volgende aanbevelingen gedaan voor het GFCE:

1. Focus op multilaterale coördinatie om een verbindende rol in te nemen in de capaciteitsopbouw-sector;[508]
2. Neem een inclusievere benadering aan, betrek zowel donoren als ontvangers;[509]
3. Creëer een sterkere band met regionale organisaties, zoals de Afrikaanse Unie, om nauwere samenwerking tussen staten te stimuleren.[510]

Global Commission on the Stability of Cyberspace

Sinds pogingen om consensus te bereiken in de VN GGE faalden in 2017 (zie paragraaf 5.1.3), zijn door civiele actoren georganiseerde activiteiten in belang toegenomen. Zo zijn verschillende samenwerkingsverbanden ontstaan tussen denktanks, onderzoeksinstituten en overheden. De GCSC is een dergelijk samenwerkingsverband, opgericht door Nederland[511] om het GGE-proces aan te vullen.[512] De GCSC heeft veel succes gehad in het aankaarten van cruciale debatten over het cyberdomein en wordt in de bestudeerde literatuur dan ook beschouwd als een belangrijke stap in de

[503] Morgan (2016), *Clarifying Goals, Revitalizing Means*, p. 10, 17, 18.
[504] Van Horenbeeck (2018), *The Future of Internet Governance*, p. 7, Ott & Osula (2019), *The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level*, p. 17.
[505] Ott & Osula (2019), *The Rise of the Regionals*, p. 17, Calderaro & Craig (2020), *Transnational Governance of Cybersecurity*, p. 921.
[506] Ott & Osula (2019), *The Rise of the Regionals*, p. 17.
[507] Hohmann et al. (2017), *Advancing Cybersecurity Capacity Building*, p. 21-22.
[508] Hohmann et al. (2017), *Advancing Cybersecurity Capacity Building*, p. 22.
[509] Hohmann et al. (2017), *Advancing Cybersecurity Capacity Building*, p. 22.
[510] Ott & Osula (2019), *The Rise of the Regionals*, p. 17, Hohmann et al. (2017), *Advancing Cybersecurity Capacity Building*, p. 22.
[511] Henriksen (2019), *The End of the Road for the UN GGE Process*, p. 7.
[512] Nye (2017), *Normative Constraints on Cyber Arms*, p. 19.

verdere opbouw van normen en expertise.[513] De EU heeft normen die door de GCSC zijn voorgesteld opgenomen in haar beleidsdocumenten. Ook zijn enkele GCSC-normen opgenomen in *de Paris Call for Trust and Security in Cyberspace*. Deze normen gaan met name over verantwoord gedrag binnen het cyberdomein en de bescherming van de integriteit van het internet.[514]

De Commissie wordt vooral vooruitstrevend genoemd in het combineren van expertises uit verschillende academische disciplines. De deelname van vooraanstaande experts verhoogt het aanzien van de GCSC.[515] De Commissie wordt echter ook bekritiseerd. Zo wordt de GCSC grotendeels gefinancierd door westerse staten. Hierdoor is het beeld ontstaan dat de organisatie is toegespitst op liberale democratieën. Ondanks de deelname van vooraanstaande experts heeft het private karakter van de Commissie ertoe geleid dat er sprake is van een gebrek aan autoriteit. Aanbevelingen worden dan ook niet automatisch geïmplementeerd door (betrokken) overheden. Ook de focus op het creëren van nieuwe normen wordt door sommige academici en staten bekritiseerd.[516] Dit zou niet nuttig zijn en er zou, in plaats daarvan, meer moeten worden gekeken naar de verspreiding en het promoten van reeds ontwikkelde normen.[517]

In de literatuur worden de volgende aanbevelingen gedaan voor de GCSC:

1. Focus op zaken die bij het GGE-proces niet aan bod komen ;[518]
2. Werk nauw samen met civiele actoren en overheden, dat kan ervoor zorgen dat de Commissie meer impact heeft en aanbevelingen vaker worden geïmplementeerd;[519]
3. Focus op het verspreiden van normen in plaats van het creëren van nieuwe normen, dit heeft op de lange termijn meer effect;[520]
4. Focus op het creëren van internationaal draagvlak voor vrijwillige, niet-bindende normen.[521]

7.1.3. Capaciteitsopbouw

In de afgelopen tien jaar zijn capaciteitsopbouwprojecten in toenemende mate een cruciaal beleidsonderdeel geworden van zowel staten als internationale organisaties om cyberdreigingen en -misdaad tegen te gaan.[522] Naast het bestrijden van cybercriminaliteit en het bevorderen van economische ontwikkeling wordt capaciteitsopbouw ondertussen ook gezien als methode om de

[513] Ruhl et al. (2020), *Cyberspace and Geopolitics*, p. 3, Eggenschwiler (2020), *Expert Commissions and Norms,* p. 100.
[514] Eggenschwiler (2020), *Expert Commissions and Norms,* p. 101.
[515] Eggenschwiler (2020), *Expert Commissions and Norms,* p. 100.
[516] Volgens een delegatie van de VS naar een VN-cybersecurity expert groep in 2017 was het effectiever om andere VN-lidstaten aan te sporen reeds ontwikkelde normen aan te nemen dan om een continue stroom aan nieuwe normen te creëren. Zie: https://www.nextgov.com/cybersecurity/2017/02/new-international-cyber-rules-likely-table-un-experts-group/135193/.
[517] Ruhl et al. (2020), *Cyberspace and Geopolitics*, p. 10.
[518] Nye (2017), *Normative Constraints on Cyber Arms*, p. 21.
[519] Eggenschwiler (2020), *Expert Commissions and Norms* p. 103.
[520] Ruhl et al. (2020), *Cyberspace and Geopolitics*, p. 10.
[521] Adamson & Homburger (2019), *Let Them Roar*, p. 228.
[522] Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 3, Hameed et al. (2018), *Analysing Trends and Success Factors*, p. 1.

internationale veiligheid te waarborgen.[523] De academische literatuur onderschrijft het belang van cybercapaciteitsopbouw voor de bevordering van de internationale veiligheid en de veiligheid van internetgebruikers.[524]

Aangezien het cyberdomein territoriale landsgrenzen overstijgt, kunnen dreigingen vanuit alle delen van de wereld komen. Om deze dreigingen tegen te gaan moet er actief worden samengewerkt met andere overheden. Dit wordt bemoeilijkt wanneer deze staten niet over geavanceerde cybertechnologieën beschikken of er een gebrek aan communicatie is.[525] Capaciteitsopbouwprojecten vergroten het vertrouwen en de samenwerking tussen verschillende cyberactoren en helpen met het verspreiden van cybernormen. Daarnaast creëren deze projecten nieuwe routes voor staten en organisaties om te communiceren over veiligheidsstrategieën en de ontwikkeling van nieuwe technologieën. Hierdoor kunnen capaciteitsopbouwprojecten volgens academici bijdragen aan de bevordering van de internationale veiligheid.[526] De huidige internationale capaciteitsopbouw-strategie kan desalniettemin verbeterd worden om meer positieve effecten te bewerkstelligen. In de paragrafen die volgen worden vier onderwerpen besproken die in de literatuur naar voren komen: de voor- en nadelen van de veranderde focus op veiligheid; de focus op het verspreiden van normen; het gebrek aan een consequente aanpak; en het gebrek aan een lokaal draagvlak. In de laatste paragraaf worden de effecten van capaciteitsopbouwprojecten op (online) mensenrechten uiteengezet.

Veranderde focus heeft specifieke vereisten

De vernieuwde mondiale focus van staten en internationale organisaties op (inter)nationale veiligheid, in plaats van economische ontwikkeling, brengt extra uitdagingen met zich mee. De huidige capaciteitsprogramma's gaan niet meer enkel over het overbruggen en verhelpen van ongelijkheid maar ook over het waarborgen van de veiligheid van staten.[527] Dit kan een positieve impact hebben op de eigen nationale veiligheid.[528] Daar staat wel tegenover dat de aanbieders van deze programma's (organisaties en staten) een belangrijke verantwoordelijkheid hebben. De hulp biedende staten hebben namelijk aanzienlijke invloed op de ontwikkeling van het cybersecuritybeleid van de ontvangende staat. Zo zijn de staten die een dergelijk programma aanbieden in de meeste gevallen verantwoordelijk voor de identificatie van dreigingen richting de ontvangende staat. Zij hebben tenslotte meer ervaring met, en kennis over, ICT. Om dit goed te kunnen uitvoeren, zal de aanbieder een duidelijk beeld moeten hebben van de actoren en risico's waartegen de ontvangende staat gewapend moet worden. Dit vergt een concrete en gedetailleerde strategie waarbij er goed moet worden gekeken naar de lokale dynamieken.[529]

Verspreiding van normen

---

[523] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 227.
[524] Calandro & Berglund (2019), *Unpacking Cyber-Capacity Building*, p. 16, Calderaro & Craig (2020), *Transnational Governance of Cybersecurity*, p. 933, Langø (2016), *Cyber Security Capacity Building*, p. 6, Dutton et al. (2019), *Cybersecurity Capacity,* p. 302.
[525] Klimburg & Zylberberg (2015), *Cyber Security Capacity Building*, p.15.
[526] Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 7,
[527] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 227-227.
[528] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 232, 238, Calderaro & Craig (2020), *Transnational Governance of Cybersecurity*, p. 921, Klimburg & Zylberberg (2015), *Cyber Security Capacity Building*, p. 15.
[529] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 228-229.

Capaciteitsopbouwprojecten zijn zo ingericht dat ze een bijdrage kunnen leveren aan het creëren en promoten van gedragsnormen. Staten kunnen namelijk middels capaciteitsopbouw in het buitenland invloed uitoefenen op de cybernormen van de staten die zij ondersteunen.[530] Dit kan beïnvloeden hoe de ontvangende staten het internationaal recht binnen het cyberdomein interpreteren en toepassen. Staten en internationale organisaties zijn dan ook actief bezig geweest om andere staten aan zich te binden via capaciteitsopbouwprojecten om zo hun cybernormen te kunnen verspreiden. Zo heeft de RvE herhaaldelijk pogingen ondernomen om staten van over de hele wereld te overtuigen om zich aan te sluiten bij de *Convention on Cybercrime*. Dit verdrag vormt de basis voor een groot scala aan capaciteitsopbouwprojecten waarbij de nadruk ligt op het versterken van cyberwetgeving, samenwerking en de implementatie van het verdrag.[531] Dit is echter niet altijd even succesvol gebleken; alleen de Filipijnen hebben een afspraak gemaakt met de EU (van de tien Associatie van Zuidoost-Aziatische Naties (ASEAN)-staten). Ook andere staten en organisaties proberen via capaciteitsopbouwprojecten hun cybernormen te verspreiden. Vooral China is zeer actief op dit vlak. Via de SCO en met gebruik van de *International Code of Conduct for Information Security* tracht China cybernormen rond internetsoevereiniteit en *information security* te verspreiden in de ASEAN-regio en Afrika.[532]

Doordat verschillende regionale instituties via capaciteitsopbouw strijden om toegang tot dezelfde staten, zijn zogeheten "*swing states"* ontstaan. Deze staten zijn het strijdtoneel geworden van de geopolitieke doeleinden van rijkere en cyber-geavanceerde staten. Sommige ontvangende staten profiteren van deze situatie door samenwerkingen aan te gaan met staten aan beide zijden van het strijdtoneel.[533] Armenië en Servië zijn bijvoorbeeld lid geworden van de *Convention on Cybercrime* terwijl zij tegelijkertijd ook ontvangers zijn van officiële Russische cyberontwikkelingssteun.[534] Ook Ghana is zowel lid van het Europese capaciteitsproject als ontvanger van Chinese cyberontwikkelingssteun.[535] De geopolitieke strijd binnen de capaciteitsopbouw zorgt voor een verdere fragmentatie van geaccepteerde cybergedragsnormen op internationaal niveau. Door capaciteitsopbouwprojecten wordt het namelijk beter mogelijk om normen en ideologieën te promoten in andere staten. Onder andere doordat een toename in cybercapaciteiten het mogelijk maakt de gedeelde normen te implementeren. Tegelijkertijd leiden deze gepolitiseerde projecten ertoe dat het lastiger wordt om internationale consensus te bereiken over de correcte interpretatie van cybernormen en bedreigingen in het cyberdomein. Deze onderwerpen worden hiermee ook verder gepolariseerd.[536] In de bestudeerde literatuur wordt dus

---

[530] Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 3, Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 232.

[531] The Convention on Cybercrime, ook wel het Boedapest Verdrag genoemd, uit 2001 is ondertekend door 65 staten. Het verdrag tracht de wetgeving en de aanpak van cybercriminaliteit mondiaal aan te pakken. Daarbij legt het verdrag vast dat illegale toegang, illegale onderschepping en data en systeem bemoeienis criminele activiteiten zijn. Belangrijke spelers als China en Rusland zijn geen lid van dit verdrag. Zie: Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 233, Council of Europe (2020), *Cybercrime Programme Office.*
Het verdrag wordt ingezet door de RvE als basis voor verscheidene capaciteitsopbouwprojecten waarbij zij inzetten op het versterken van cyberwetgeving, samenwerking en de implementatie van het verdrag. Zie: Council of Europe (2020), *Cybercrime Programme Office.*

[532] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 234-235.

[533] Schia (2016), *Cyber Security Capacity Building*, p. 83.

[534] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 236.

[535] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 237.

[536] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 237.

gesteld dat capaciteitsprojecten een positieve impact hebben op de internationale veiligheid, maar tegelijkertijd bijdragen aan de verdere fragmentatie van cybergedragsnormen.

Gebrek aan consequente aanpak

De hoge en toenemende interesse in cybercapaciteitsopbouw heeft geleid tot een onoverzichtelijke hoeveelheid beleid, principes en organisaties. Er is een gebrek aan coördinatie en strategie tussen de westerse staten en instanties die hierbij betrokken zijn; de VS, Canada, EU-lidstaten, de Raad van Europa en de VN.[537] Zij hanteren allen andere aanpakken en benadrukken verschillende regels en normen.[538] Mede hierdoor hebben de EU-projecten niet altijd goed uitgepakt. De wetten en projecten die de EU heeft helpen ontwikkelen en die door de *European Development Fund* zijn gefinancierd, worden beoordeeld als tegenstrijdig en mager vormgegeven. Cybercrime-experts hebben aangekaart dat verschillende provisies binnen voorgestelde nieuwe wetten niet voldeden aan de regels van de *Convention on Cybercrime*.[539] Recente pogingen om een meer gestroomlijnde aanpak te creëren, zoals de richtlijnen vanuit de *EU Cyber Capacity Building Strategy*, worden positief ontvangen.[540]

Door voorgaande samenwerkingsverbanden en -mechanismen zijn sommige beleidsvelden binnen de capaciteitsopbouw verder ontwikkeld dan anderen. Programma's gericht op cybercrime en -dreigingen hebben veel aandacht gekregen terwijl meer ontwikkelingsgeoriënteerde aspecten zoals *gender* en *good governance* vaak enkel als bijzaak worden gezien. Sommige academici beargumenteren daarom dat er meer samenwerking moet komen tussen de beleidsvelden van veiligheid en ontwikkelingssamenwerking.[541] Zij stellen dat dit ertoe zou kunnen leiden dat nieuwe technologieën actief kunnen bijdragen aan sociale, economische en politieke ontwikkeling op internationaal vlak.[542] Daarnaast moet er meer coördinatie komen tussen verschillende donoren over welke staten financiering dienen te krijgen en in welke mate. Senegal, bijvoorbeeld, wordt financieel gesteund door zowel de EU als Nederland, de VS en Zuid-Korea. Middels betere communicatie zou kunnen worden voorkomen dat populairdere landen zoals Senegal, in de literatuur *Darlings* genoemd, veel financiële steun krijgen terwijl anderen worden vergeten, de zogenaamde *Orphans*.[543]

Gebrek lokaal draagvlak

In de literatuur wordt aangemerkt dat capaciteitsopbouwprojecten effectiever zouden kunnen zijn wanneer meer wordt samengewerkt met lokale overheden en bevolking. Zo wordt gesteld dat de programma's meer moeten worden toegespitst op de behoeften van een specifiek land.[544] Beide partijen moeten het belang van capaciteitsopbouw begrijpen en invloed hebben binnen de overheid van de ontvanger. Daarnaast is het volgens de literatuur belangrijk om volgens het multi-stakeholder

---

[537] Hameed et al. (2018), *Analysing Trends and Success Factors*, p. 1, Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 4, 10.
[538] Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 4.
[539] Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 11-12.
[540] Calderaro (2020), *Overcoming Fragmentation in Cyber Diplomacy*.
[541] Hameed et al. (2018), *Analysing Trends and Success Factors*, p. 3, Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 10.
[542] Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 15.
[543] Hameed et al. (2018), *Analysing Trends and Success Factors*, p. 1, Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 17.
[544] Hameed et al. (2018), *Analysing Trends and Success Factors*, p. 3, Pawlak (2014), *Riding the Digital Wave*, p. 68.

model meer verschillende stakeholders te betrekken bij het ontwerpen en implementeren van capaciteitsopbouwprojecten. Stakeholders kunnen helpen bij het identificeren van kwetsbaarheden en het zoeken van oplossingen.[545] Volgens *Global Partners Digital*, een onafhankelijke organisatie die samenwerkt met ngo's en overheden om de online mensenrechten te bevorderen, moeten bij dit multi-stakeholder proces ook de private sector, academici en mensenrechtengroeperingen worden betrokken.[546] Door middel van trainingen en technische opleidingen kunnen stakeholders op lange termijn een positieve bijdrage leveren.[547] Van oorsprong is er echter een lage of ineffectieve samenwerking met lokale stakeholders.[548] Daarnaast zijn er ook ontvangende staten die na een initiële toezegging om deel te nemen aan een project, de bijbehorende strategieën toch niet implementeren en ratificeren.[549]

Effect op de (online) mensenrechten

Volgens de literatuur kunnen capaciteitsopbouwprojecten een impact hebben op de (bescherming van) online mensenrechten. Zoals eerder beschreven zijn de capaciteitsprojecten gepolitiseerd geraakt. Staten die niet een open internetbeleid voeren, verspreiden middels capaciteitsopbouw normen die een negatief effect hebben op online mensenrechten.[550] Daarnaast gaan de normen en waarden van aanbieders, bijvoorbeeld de EU, niet altijd samen met lokale politieke economieën van ontvangers. Democratische normen en mensenrechten zoals de vrijheid van meningsuiting en het recht op privacy zijn niet in alle ontvangende staten een vanzelfsprekendheid. Hierdoor ontstaat er een spanning tussen de democratische grondslag van voorgestelde hervormingen en de lokale politieke economie. In veel gevallen missen staten ook de institutionele structuur en financiële middelen om deze maatregelen daadwerkelijk door te voeren.[551]

Calandro en Berglund stellen dat capaciteitsopbouw vergaande gevolgen kan hebben voor de online mensenrechten binnen meer autoritaire regimes.[552] Er ontstaat dan een spanning tussen ontwikkelingsdoelen en veiligheidsoverwegingen. Ook Turianskyi, Pawlak en Barmpaliou betogen dat een toename in de cybercapaciteiten van autoritaire staten kan leiden tot een versterking van de positie van de staat in het cyberdomein, waardoor online mensenrechten onder druk komen te staan.[553] Een oplossing zou gevonden kunnen worden in het multi-stakeholderprincipe. Middels dit principe kunnen aanbieders beter inzetten op de bescherming van de online mensenrechten en de internationale rechtsorde, en zo een liberaler en democratisch speelveld creëren.[554] Daarnaast is het belangrijk dat mensenrechten geïntegreerd worden binnen alle verschillende beleidsdimensies van capaciteitsprojecten, ook bijvoorbeeld bij cybersecurity. Een coherente integratie van

---

[545] Pijnenburg-Muller (2015), *Cyber Security Capacity Building*, p. 15, Calderaro (2020), *Overcoming Fragmentation in Cyber Diplomacy*.
[546] Shears et al. (2018), *Multistakeholder Approaches*, p. 12-13.
[547] Pijnenburg-Muller (2015), *Cyber Security Capacity Building*, p. 15, Calderaro (2020), *Overcoming Fragmentation in Cyber Diplomacy*.
[548] Calandro & Berglund (2019), *Unpacking Cyber-Capacity Building*, p. 1.
[549] Calandro & Berglund (2019), *Unpacking Cyber-Capacity Building*, p. 9.
[550] Calandro & Berglund (2019), *Unpacking Cyber-Capacity Building*, p. 1, Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 223.
[551] Calandro & Berglund (2019), *Unpacking Cyber-Capacity Building*, p. 1, 15.
[552] Calandro & Berglund (2019), *Unpacking Cyber-Capacity Building*, p. 8.
[553] Turianskyi (2020), *Africa and Europe: Cyber Governance Lessons*, p. 4, Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 13.
[554] Klimburg & Zylberberg (2015), *Cyber Security Capacity Building*, p. 13, Pawlak (2014), *Riding the Digital Wave*, p. 62.

mensenrechten binnen het beleidsplan zou onverwachte negatieve gevolgen kunnen helpen voorkomen.[555]

In de bestudeerde literatuur worden enkele lessen en aanbevelingen omtrent capaciteitsopbouw uiteengezet:

1. Zet cybercapaciteitsprojecten voort, capaciteitsopbouw is een effectieve methode voor het bevorderen van de internationale veiligheid;[556]
2. Wees bewust van de manier waarop capaciteitsprojecten worden ingezet en het effect op cybergedragsnormen;[557]
3. Stem projecten af op de specifieke lokale situatie;[558]
4. Stel per project een concreet beleidsplan op waarbij de focus op mensenrechten in elk onderdeel wordt geïntegreerd;[559]
5. Verbeter de coördinatie tussen donorstaten en -organisaties;[560]
6. Maak gebruik van het multi-stakeholder principe, dit kan bijdragen aan het creëren van lokale draagkracht en het bevorderen van online mensenrechten.[561]

7.1.4. Bevorderen mensenrechten in het cyberdomein

Het tweede doel van het Nederlandse cybersecuritybeleid (het bevorderen van de internationale rechtsorde) is ook gericht op het bevorderen van mensenrechten in het cyberdomein. Zo heeft BZ het oprichten van de *Freedom Online Coalition* geïnitieerd (zie paragraaf 7.1.2 voor een evaluatie). Ook steunt BZ ngo's zoals *Digital Defenders Parnership,*[562] een hulporganisatie voor mensenrechtenactivisten die digitale dreiging ervaren, en *Access Now,*[563] werkzaam in het beschermen en verdedigen van online mensenrechten wereldwijd. Timo Koster, voormalig cyberambassadeur van BZ, stelt dat Nederland gericht is op het ondersteunen, begeleiden en beïnvloeden van besluitvormers in alle sectoren met innovatieve, empirisch onderbouwde beleidsanalyses gericht op mensenrechten.[564] Behalve een onafhankelijke evaluatie van de FOC is er weinig literatuur verschenen over het Nederlandse internationale mensenrechtenbeleid gericht op

[555] Pawlak (2014), *Riding the Digital Wave*, p. 70.
[556] Calandro & Berglund (2019), *Unpacking Cyber-Capacity Building*, p. 5, Calderaro & Craig (2020), *Transnational Governance of Cybersecurity*, p. 917, Langø (2016), *Cyber Security Capacity Building*, p. 6, Dutton et al. (2019), *Cybersecurity Capacity,* p. 302.
[557] Homburger (2019), *The Necessity and Pitfall of Cybersecurity*, p. 237, Hameed et al. (2018), *Analysing Trends and Success Factors*, p. 1.
[558] Hameed et al. (2018), *Analysing Trends and Success Factors*, p. 3, Pawlak (2014), *Riding the Digital Wave*, p. 68.
[559] Hameed et al. (2018), *Analysing Trends and Success*, p. 3, Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 15.
[560] Hameed et al. (2018), *Analysing Trends and Success*, p. 1, Pawlak & Barmpaliou (2017), *Politics of Cybersecurity Capacity Building*, p. 17.
[561] Pijnenburg-Muller (2015), *Cyber Security Capacity Building*, p. 15, Calderaro (2020), *Overcoming Fragmentation in Cyber Diplomacy*, p. Klimburg & Zylberberg (2015), *Cyber Security Capacity Building*, p. 13, Pawlak (2014), *Riding the Digital Wave*, p. 62.
[562] https://www.digitaldefenders.org/
[563] https://www.accessnow.org/
[564] Koster (2020), *How to Counter Worsening Cyber-security Threats*, p. 19.

het cyberdomein. Volgens de wel beschikbare literatuur wordt de manier waarop Nederland zich uitspreekt over de bredere toepassing van het internationaal recht, inclusief mensenrechten, over het algemeen positief ontvangen.[565] In de literatuur wordt wel benadrukt dat ook de praktische toepassing van online mensenrechten besproken moet worden.[566] Volgens de *Association for Progressive Communication*[567] worden online mensenrechten over het algemeen slechts op een oppervlakkige wijze geïntegreerd in internationale beleidsinitiatieven.[568] De GCSC adviseert dan ook om te onderzoeken hoe de verschillende beleidsvoorstellen een impact zouden kunnen hebben op online mensenrechten.[569] Met betrekking tot het bevorderen van online mensenrechten zouden ook private actoren, zoals bedrijven en internetgebruikers, geïntegreerd moeten worden in het multi-stakeholder principe.[570]

Nog belangrijker is het betrekken van mensenrechtenexperts bij het opstellen van *algemeen* internationaal cybersecuritybeleid. Schnidrig en Aiken betogen dat er meer kennis over de implicaties van het algemene beleid op mensenrechten zal ontstaan wanneer mensenrechtenexperts meedenken over het algehele cybersecuritybeleid.[571] Mensenrechtenexperts zullen hierdoor ook meer vertrouwen hebben in de effectiviteit en positieve impact van het beleid.[572]

Tijdens het *Internet Governance Forum* (IGF) in 2017 kwamen cyberexperts, academici en mensenrechtenactivisten tot dezelfde conclusie: het betrekken van civiele actoren bij nationale delegaties die internationale conferenties bezoeken is niet voldoende. Zij stellen dat experts een onafhankelijke rol moeten krijgen zodat mensenrechten op een substantiëlere wijze worden geïntegreerd in verdragen. Multi-stakeholder processen zouden dus zowel inclusiever als meer interdisciplinair moeten worden. Daarnaast wordt beargumenteerd dat er idealiter een netwerk ontstaat van mensenrechtenexperts en technische- en veiligheidsexperts, zodat een concreet beeld over de implicaties van beleidsvoorstellen op online mensenrechten beschikbaar is.[573]

Deelnemers van het IGF waren van mening dat een breed gedragen internationaal cyberverdrag niet zou leiden tot meer aandacht voor online mensenrechten. Om het eens te worden over het verdrag zullen staten met uiteenlopende visies omtrent het cyberdomein en online mensenrechten dichter naar elkaar toe moeten bewegen. Een verdrag zou dus kunnen betekenen dat staten die momenteel een vrij internetbeleid voeren meer controle gaan uitoefenen over het cyberdomein en minder ruimte overlaten voor online mensenrechten.[574]

---

[565] Moynihan (2019), *The Application of International Law*, p. 2, Schmitt (2019), *The Netherlands Releases a Tour de Force*.
[566] Moynihan (2019), *The Application of International Law*, p. 58.
[567] De APC is een internationaal samenwerkingsverband van verschillende organisaties dat communicatie-infrastructuur levert aan groepen en individuen die zich inzetten voor vrede, mensenrechten, milieubescherming en duurzaamheid. Zie ook: https://www.apc.org/.
[568] Brown & Esterhuysen (2017), *A Rights-Based Approach to Cybersecurity*, p. 5.
[569] Global Commission on the Stability of Cyberspace (2019), *Advancing Cyberstability*, p. 19.
[570] Mihr (2014), *Good Cyber Governance*, p. 336.
[571] Schnidrig & Aiken (2020), *Engagement in Cyber Capacity Building*, p. 19.
[572] Schnidrig & Aiken (2020), *Engagement in Cyber Capacity Building*, p. 5.
[573] Brown & Esterhuysen (2017), *A Rights-Based Approach to Cybersecurity*, p. 6.
[574] Brown & Esterhuysen (2017), *A Rights-Based Approach to Cybersecurity*, p. 6.

In de literatuur worden de volgende aanbevelingen gedaan omtrent het bevorderen van online mensenrechten:

1. Maak duidelijke multilaterale en diplomatieke afspraken over de toepassing van normen in het cyberdomein,[575] geef daarbij concrete voorbeelden om uit te dragen hoe dit in de praktijk werkt;[576]
2. Integreer online mensenrechten in alle facetten van het cybersecuritybeleid om tegenstrijdigheden te voorkomen;[577]
3. Ontwikkel internationaal cybersecuritybeleid via een inclusiever en interdisciplinair multi-stakeholder model, zodat er een duidelijk beeld ontstaat van de eventuele impact van dit beleid op online mensenrechten.[578]

7.2. Lessen internationale gemeenschap

De afgelopen jaren worden gekenmerkt door een toename in het aantal officiële internationale cybersecuritystrategieën gepubliceerd door staten. In dit tweede deel van dit hoofdstuk worden kort een aantal lessen samengevat die naar voren komen uit de academische literatuur over het internationale cybersecuritybeleid van de VS, Israël en Estland. Over het algemeen kan er een onderscheid worden gemaakt tussen twee typen staten in het cyberdomein. Sommige staten focussen voornamelijk op het creëren van internationale normen door middel van discussies en bijeenkomsten (bijvoorbeeld Estland), anderen creëren (indirect) 'normen' door middel van hun gedrag (bijvoorbeeld de VS en Israël). Uit beide typen internationaal cybersecuritybeleid kunnen lessen worden getrokken die relevant zijn voor Nederland, vanwege bondgenootschappen maar ook op een theoretisch niveau. De volgende punten zullen in dit hoofdstuk worden besproken:

- Er wordt veelvuldig en kritisch geschreven over het huidige Amerikaanse cybersecuritybeleid *Defend Forward.* Volgens verscheidene academici zou dit beleid de stabiliteit van het cyberdomein schaden en incompatibel zijn met een open en vrij internet;
- Academici wijzen naar Israëlische handelingen in het cyberdomein als bewijs dat het gecompliceerd is om een vergelijking te maken tussen cyberoperaties en kinetische operaties voor wat betreft de kans op escalatie;
- Het Estse beleid wordt in de literatuur genoemd als succesverhaal omdat een kleine staat de mogelijkheid heeft gezien om cybernormen te promoten op internationaal niveau. Tegelijkertijd stellen academici dat deze ontwikkelingen nogmaals hebben benadrukt dat Rusland en China cruciaal zijn om de volgende fase in de ontwikkeling van internationale cybernormen te bereiken.

Verenigde Staten

[575] Van der Meer (2015), *Enhancing International Cyber Security*, p. 204.
[576] Moynihan (2019), *The Application of International Law*, p. 58, Schmitt (2019), *The Netherlands Releases a Tour de Force*.
[577] Global Commission on the Stability of Cyberspace (2019), *Advancing Cyberstability*, p. 19.
[578] Mihr (2014), *Good Cyber Governance*, p. 336, Schnidrig & Aiken (2020), *Engagement in Cyber Capacity Building*, p. 19, Brown & Esterhuysen (2017), *A Rights-Based Approach to Cybersecurity*, p. 6.

In de afgelopen jaren heeft er een belangrijke verschuiving plaatsgevonden in het internationale cybersecuritybeleid van de VS.[579] Waar de nadruk in eerste instantie lag op het ontwikkelen van normen middels dialoog, en afschrikking door ontkenning (*deterrence by denial),*[580] is het beleid de laatste jaren gefocust op afschrikking door vergelding (*deterrence by punishment)*[581] en *persistent force*.[582] Er zouden drie oorzaken ten grondslag liggen aan deze verandering. Ten eerste hebben recente technologische ontwikkelingen het in potentie mogelijk gemaakt om cyberoperaties te volgen en daders te identificeren. Ten tweede stellen verscheidene vooraanstaande Amerikaanse academici dat afschrikking door ontkenning niet werkt.[583] Ten derde wordt beargumenteerd dat de VS alleen internationale cybernormen kan ontwikkelen door cyberoperaties in te zetten die *actief* de parameters van acceptabel gedrag bepalen.[584]

Toen de Amerikaanse cyberstrategie in 2013 publiekelijk bekend werd, ontstond – zo stelt Alexander Klimburg – bij vijanden en bondgenoten de angst dat *persistent presence* gemakkelijk zou kunnen leiden tot *persistent engagement*.[585] In 2018 werd duidelijk dat deze zorg enigszins terecht was: het Amerikaanse ministerie van Defensie kreeg de bevoegdheid om cyberoperaties uit te voeren die niet direct ter verdediging van de eigen netwerken zijn bedoeld.[586] De huidige strategie – *Defend Forward* – wordt als volgt uitgelegd: *"[We] operate between defense and offense across the interconnected battlespace – globally – as close as possible to adversaries and their operations – and continuously – to create operational advantage for us while denying the same to our adversaries."*[587] In de woorden van Schneider, het VS Cyber Command team is *"everywhere, all the time and in all ways."*[588] Volgens Smeets en Lin heeft dit ertoe geleid dat kleinere staten zichzelf beter zijn gaan verdedigen in het cyberdomein, en een reden hebben gezien om te investeren in offensieve cybercapaciteiten.[589] Daarbij is het idee achter een offensief cyberdefensiebeleid zoals *Defend Foward* dat een staat zijn tegenstander afschrikt door niet alleen aan te tonen over bepaalde (destructieve) capaciteiten te beschikken, maar deze ook in te zetten (zie ook voetnoot 582). Het inzetten van offensieve cybercapaciteiten, en het openlijk pleiten daarvoor, kan volgens verscheidene academici op den duur de internationale vrede en veiligheid schaden en een toename

---

[579] Smeets (2020), *US Cyber Strategy*, p. 444.

[580] Afschrikking door ontkenning wordt bereikt wanneer de kosten-batenanalyse van een potentiële aanvaller wordt beïnvloed door verdedigingsmaatregelen genomen door het potentiële doelwit. De potentiële aanvaller wordt afgeschrikt door het idee dat een aanval het toch niet waard is omdat deze niet succesvol zal blijken. Zie: Ryan (2018), *Five Kinds of Cyber Deterrence*, p. 334.

[581] Deze strategie houdt in dat de reactie van een aangevallen staat zo negatief uitpakt voor de aanvallende staat dat deze besluit om de aanval te stoppen. In andere woorden: straf Y overtreft de opbrengst van aanval X waardoor een aanvallende staat beter af is wanneer deze de aanval staakt. Zie: Ryan (2018), *Five Kinds of Cyber Deterrence*, p. 332.

[582] Gen. Nakasone beschrijft *persistence force* als volgt "[it] will contest our adversaries' efforts in cyberspace to harm Americans and American interests. It will degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace." Zie: Nakasone (2019), *A Cyber Force for Persistent Operations*, p. 11.

[583] Wilner (2019), *US Cyber Deterrence*, p. 270, Ryan (2018), *Five Kinds of Cyber Deterrence*, p. 334, Fischerkeller & Harknett (2017), *Deterrence is Not a Credible Strategy*, p. 381.

[584] Fischerkeller & Harknett (2017), *Deterrence is Not a Credible Strategy*, p. 382.

[585] Klimburg (2020), *Mixed Signals*, p. 113.

[586] Smeets (2020), *US Cyber Strategy*, p. 444.

[587] Command Vision for US Cyber Command. https://www.cybercom.mil/Portals/56/Documents /USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

[588] Schneider (2019), *Persistent Engagement*.

[589] Smeets & Lin (2019), *A Strategic Assessment*, p. 91.

in het aantal cyberconflicten veroorzaken.[590] Daarnaast beargumenteert Healey dat de kwaliteiten die nodig zijn om (langdurige) stabiliteit te creëren middels een *persistent engagement* strategie mogelijk niet voldoende beschikbaar zijn in de VS (in 2019). Healey stelt dat er in ieder geval sprake moet zijn van vertrouwen van bondgenoten en de mogelijkheid om consistente signalen af te geven richting potentiele aanvallers.[591] Zo betoogt ook Max Smeets dat het doel om de bewegingsvrijheid van tegenstanders in het cyberdomein te beperken zou kunnen leiden tot frictie in de relatie tussen de VS en zijn bondgenoten.[592]

Uit de bestudeerde literatuur blijkt dat de Amerikaanse strategie ook vanwege andere redenen door academici wordt bekritiseerd. Smeets en Lin stellen dat het uit de strategie niet duidelijk wordt waar de prioriteit ligt qua doelstellingen en middelen.[593] Ze betogen dat het gevolg hiervan is dat er geen succesindicatoren lijken te bestaan en dat het onduidelijk is wanneer een strategie die zoveel belooft *ooit* succesvol kan zijn.[594] Schneider komt tot dezelfde conclusie en stelt dat succes momenteel alleen lijkt te zijn behaald wanneer er geen cyberoperaties meer tegen de VS (kunnen) worden uitgevoerd. Volgens Schneider worden bij een dergelijke succesindicator twee cruciale punten vergeten: (1) dat de strategie onderdeel is van het bredere beleid van een open en vrij internet, en (2) dat er voordelen te behalen vallen uit een open en vrij internet.[595] Schneider betoogt dus dat de Amerikaanse strategie zowel te breed (mondiaal en continu) als te nauw is (te weinig aandacht voor het idee van een open en vrij internet). Volgens Healey zou de huidige strategie, zelfs als deze stabiliserend werkt, onverenigbaar kunnen zijn met het Amerikaanse beleid voor een open en vrij internet.[596]

Daarnaast wordt gesteld dat de *persistent engagement* strategie (ook) bedoeld is om tegenstanders richting acceptatie van bepaalde normen te duwen.[597] Healey waarschuwt voor de mogelijkheid dat het huidige beleid – waarin wordt gesteld dat cyberoperaties vroegtijdig en zo dicht mogelijk bij de aanvaller onderschept worden – ertoe kan leiden dat het uiteindelijk lastiger wordt om (stilzwijgend) overeenkomst te bereiken over normen. Dit zou te maken hebben met de onwaarschijnlijkheid dat – omdat cyberoperaties vroegtijdig worden gestopt – in alle gevallen met zekerheid is vast te stellen wat de bedoeling van een dergelijke operatie is en of deze in strijd is met de internationale, door de VS geaccepteerde, normen. Wanneer de VS geen onderscheid maakt tussen verschillende operaties en tegenmaatregelen daarop afstemt, wordt de suggestie gewekt dat het inzetten van tegenmaatregelen altijd gerechtvaardigd is voor de VS (zie paragraaf 4.2 voor de criteria waar tegenmaatregelen aan moeten voldoen volgens internationaal recht).[598] Healey

---

[590] Klimburg (2020), *Mixed Signals*, p. 123, Jinghua (2018), *What Really Matters in 'Defending Forward'?*, Chesney (2018), *An American Perspective on a Chinese Perspective*, Buchanan & Williams (2018), *A Deepening U.S.-China Cybersecurity Dilemma*, Healey (2019), *The Implications of Persistent (and Permanent) Engagement*, p. 6. Daartegenover moet worden gesteld dat het bijna onmogelijk is om te bewijzen dat een bepaalde actie wel of niet zal leiden tot escalatie: daarvoor is escalatie te veel gebaseerd op (verschillende) percepties. Zie: Schneider (2019), *Persistent Engagement*.

[591] Healey (2019), *The Implications of Persistent (and Permanent) Engagement*, p. 2.

[592] Smeets (2020), *US Cyber Strategy*, p. 445, Smeets (2019), *Cyber Command's Strategy*.

[593] Smeets & Lin (2019), *A Strategic Assessment.*

[594] Schneider (2019), *Persistent Engagement*.

[595] Schneider (2019), *Persistent Engagement*.

[596] Healey (2018), *Triggering the New Forever War, in Cyberspace.*

[597] Fischerkeller & Harknett (2018), *Persistent Engagement and Tacit Bargaining.*

[598] Kosseff beargumenteert dat het internationaal recht voldoende ruimte biedt voor het uitvoeren van de *Defend Forward*-strategie, inclusief het inzetten van tegenmaatregelen en het uitvoeren van cyberoperaties op de systemen en netwerken van anderen. Zo wordt o.a. beargumenteerd dat de continue cyberdreiging gericht

beargumenteert dat dit ertoe zou kunnen leiden dat potentiële aanvallers niet het vertrouwen hebben dat zij, wanneer zij zich aan de normen houden, niet later alsnog het slachtoffer worden van normoverschrijdend gedrag van de VS, omdat het erop lijkt dat de VS er twee verschillende sets van normen op nahoudt: een voor zichzelf, en een voor anderen.[599] Lyu Jinghua, een Chinese academicus, bekritiseert de Amerikaanse strategie dan ook vanwege de afwezigheid van een verklaring waaruit duidelijk wordt hoe het beleid zich verhoudt tot meer fundamentele rechtsprincipes zoals territoriale integriteit en soevereiniteit.[600] Als laatste punt van kritiek stelt Healey dat het huidige Amerikaanse beleid, in tegenstelling tot beleid uit eerdere jaren, onvoldoende rekening houdt met het feit dat het cyberdomein in handen is van private actoren en individuen.[601]

Ter verduidelijking worden de lessen die getrokken kunnen worden uit het Amerikaanse internationale cybersecuritybeleid op een rij gezet:

1. Bij het opstellen van een veiligheidsstrategie moet expliciet rekening worden gehouden met de risico's die hieraan verbonden zijn en uiteengezet worden hoe deze het beste gemitigeerd kunnen worden;[602]
2. Het is wellicht te optimistisch om aan te nemen dat *persistent engagement* tot een stabieler cyberdomein leidt, in het bijzonder wanneer dezelfde strategie bedoeld is om superioriteit te behalen/behouden (en andere staten ook superioriteit beogen);[603]
3. Hoewel een staat zijn eigen beleid kan afschilderen als neutraal of defensief, kunnen anderen (zowel bondgenoten en private actoren als tegenstanders) dit betwijfelen. De les die hieruit getrokken kan worden is dat het belangrijk is dat een strategie militaire/cybercommunicatie incorporeert om er zeker van te zijn dat er geen misverstanden ontstaan over niet-intentionele operaties;[604]
4. Bij het opstellen van (internationaal) cyberbeleid is het belangrijk om rekening te houden met het feit dat het cyberdomein in handen is van private actoren en individuen, en dat dit beleid mogelijkerwijs het internet fundamenteel kan veranderen.[605] Om die reden is het voordelig om in te zetten op samenwerkingen met private actoren en individuen.[606]

Israël

Het internationale cybersecuritybeleid van de Israëlische staat is vergelijkbaar met de Amerikaanse strategie. Ook Israël legt de nadruk op het inzetten van offensieve cybercapaciteiten in de hoop tegenstanders voldoende af te schrikken. De strategie is gebaseerd op een idee van *cumulatieve* afschrikking. Volgens deze theorie wordt afschrikking bereikt door het regelmatig inzetten van 'gelimiteerde geweldsdaden' om zo de omvang van het conflict te beheersen en het gedrag van

tegen de VS, die tot het *persistent engagement*-beleid heeft geleid, voldoende is om te rechtvaardigen dat tegenmaatregelen ook continu worden genomen (en niet worden gestopt wanneer de onrechtmatige daad officieel is beëindigd omdat er dan alweer andere operaties uitgevoerd zouden worden tegen de VS). Zie: Kosseff (2019), *The Contours of 'Defend Forward'Under International Law*, p. 8.

[599] Healey (2019), *The Implications of Persistent (and Permanent) Engagement*, p. 7.

[600] Jinghua (2018), *What Really Matters in 'Defending Forward'?*.

[601] Healey (2019), *The Implications of Persistent (and Permanent) Engagement*, p. 11.

[602] Smeets & Lin (2019), *A Strategic Assessment*, Healey (2018), *Triggering the New Forever War, in Cyberspace*.

[603] Healey (2019), *The Implications of Persistent (and Permanent) Engagement*, p. 8.

[604] Healey (2019), *The Implications of Persistent (and Permanent) Engagement*, p. 8.

[605] Healey (2019), *The Implications of Persistent (and Permanent) Engagement*, p. 11.

[606] Wilner (2019), *US Cyber Deterrence*, p. 272.

tegenstanders te beïnvloeden. Het is dus niet het doel van deze strategie om alle cyberaanvallen te voorkomen.[607] Uri Tor stelt dat de effectiviteit van de Israëlische cumulatieve afschrikkingsstrategie niet is bewezen. Daarbij kan de strategie – omdat deze het vermogen en de bereidheid vereist om waar nodig kinetisch militaire instrumenten in te zetten – leiden tot negatieve gevolgen voor de internationale vrede en veiligheid.[608]

Een belangrijke les kan ook worden getrokken uit de offensieve Stuxnet-operatie, uitgevoerd door de Verenigde Staten en Israël op Iraanse nucleaire installaties (zoals bekend werd in 2011). De kosten van deze operatie worden geschat op 300 miljoen dollar. Het ontwikkelen van de computerworm heeft meer gekost dan Iran kwijt was aan het herstellen van de schade, en onthulde daarnaast technieken ter vergaring van intelligentie die in de toekomst gebruikt zouden kunnen worden voor andere operaties.[609] Daarnaast wordt gesteld dat de Stuxnet-operatie een aanleiding zou kunnen zijn voor de toename in het aantal cyberoperaties die gericht zijn op het verstoren van netwerken binnen de VS.[610] Het effect van de Stuxnet-operatie, in vergelijking met een kinetische aanval, voor wat betreft escalatie is dus lastig vast te stellen. In de literatuur wordt ook gesteld dat de Stuxnet-operatie alleen mogelijk niet voldoende was geweest om Iran te weerhouden van het ontwikkelen van nucleaire capaciteiten. Er was een bredere strategie voor nodig, waarin multilaterale diplomatieke inspanningen, diplomatiek isolement, economische sancties en het dreigen met militaire actie allemaal een rol speelden, om dit doel te bereiken.[611] Volgens Jensen was Stuxnet slechts een stukje van een grotere puzzel. De sabotage-operatie signaleerde aan Iran zowel de oplossing als de (toekomstige) risico's van verdere escalatie van de impasse. Valeriano, Jensen en Maness concluderen daarom dat operaties zoals Stuxnet gecombineerd moeten worden met andere instrumentele bedreigingen en positieve aansporingen om hun doel te bereiken.[612] De effecten van politieke oorlogsvoering, zo stellen de academici, zijn meestal indirect en vullen elkaar aan.[613]

Uit het Israëlische cybersecuritybeleid worden door experts de volgende lessen getrokken:

1. De effectiviteit van een cumulatieve afschrikkingstheorie waarbij waar nodig kinetische instrumenten ingezet worden, is niet bewezen;
2. Het is lastig te beoordelen in hoeverre een cyberoperatie bijdraagt aan (verdere) escalatie in het cyberdomein;
3. Cyberoperaties gericht op het beïnvloeden van tegenstanders zouden het meest effectief kunnen zijn wanneer deze onderdeel uitmaken van een bredere *carrot and stick*-aanpak.[614]

[607] Tor (2015), *Cumulative Deterrence*, p. 95.
[608] Tor (2015), *Cumulative Deterrence*, p. 108.
[609] Ter vergelijking: voor dezelfde kosten, meer garantie op succes en een grotere kans op een correcte inschatting van bijkomende schade, hadden de VS en Israël drie kruisraketten kunnen lanceren. Hoewel er uiteraard belangrijke kanttekeningen geplaatst moeten worden bij deze versimpelde 'afweging', toont het een interessante schaduwkant van cyberoperaties (en hoewel het lanceren van kruisraketten duidelijker de grens van gewapende aanval overschrijdt, kan ook beargumenteerd worden dat de Stuxnet-operatie de principes van territoriale integriteit en soevereiniteit hebben geschonden). Zie: Jensen (2017), *The Cyber Character*, p. 167.
[610] Healey (2019), *The Implications of Persistent (and Permanent) Engagement*, p. 9.
[611] Valeriano et al. (2018), *Cyber Strategy*, p. 90.
[612] Jensen (2017), *The Cyber Character*, p. 167.
[613] Jensen (2017), *The Cyber Character*, p. 167, Valeriano et al. (2018), *Cyber Strategy*, p. 90.
[614] Valeriano et al. (2018), *Cyber Strategy*, p. 90.

Estland

Sinds het in 2007 werd getroffen door cyberaanvallen,[615] heeft Estland, een kleine staat zonder significante militaire macht, moeten zoeken naar andere manieren om staten te beïnvloeden in het cyberdomein. Uit de bestudeerde literatuur blijkt dat Estland zich sindsdien, net als Nederland,[616] heeft weten te profileren als voorloper en promotor van internationale normen op het gebied van cyberoperaties en cybersecurity.[617] Dit heeft ertoe geleid dat Crandall en Allan stellen dat het mogelijk is om als kleine staat een bepaalde mate van succes te behalen bij het promoten van cybernormen, zeker binnen een groep van gelijkgestemde staten.[618] Door echter gebruik te maken van de NAVO voor het promoten van bepaalde normen, worden bijvoorbeeld China en Rusland per definitie uitgesloten van het normvormingsproces. Dit zou wellicht onnodige concurrentie kunnen hebben gecreëerd.[619]

De volgende lessen uit de literatuur zouden voor Nederland van belang kunnen zijn:

1. Kleine staten kunnen succesvol zijn in het promoten van internationale normen;
2. Niet alleen de VS maar ook staten zoals Rusland en China spelen een cruciale rol in het bereiken van de volgende fase in de ontwikkeling van internationale cybernormen. Bij het zoeken naar consensus over normen zou getracht kunnen worden dit zoveel mogelijk te laten plaatsvinden in een forum of organisatie waartoe niet alleen gelijkgestemde staten toegang hebben.[620]

[615] Estland was in 2007 het doelwit van cyberaanvallen afkomstig uit Rusland, gericht op de websites van de Estse president, het parlement, ministeries, banken en nieuwsorganisaties. De cyberaanvallen vonden plaats na een periode van onrust omtrent het verwijderen van een oorlogsmonument uit het Sovjettijdperk. Het is onduidelijk of de cyberaanvallen werden uitgevoerd door de Russische staat of door actoren gesteund door Rusland. Zie: Crandall & Allan (2015), *Small States and Big Ideas*, p. 351.

[616] Adamson & Homburger (2019), *Let Them Roar*, p. 229.

[617] Crandall & Allan (2015), *Small States and Big Ideas*, p. 354.

[618] Crandall & Allan (2015), *Small States and Big Ideas*, p. 363.

[619] Crandall & Allan (2015), *Small States and Big Ideas*, p. 347.

[620] De vraag is uiteraard of Estland uit is op het bereiken van *internationale* cybergedragsnormen of slechts op het verzekeren van veiligheidsgaranties van de VS en de NAVO.

Bibliografie

Academisch

Ablon, L., A. Binnendijk, Q. E. Hodgson, L. Bilyana, S. Romanosky, D. Senty, J. A. Thompson (2019). Operationalizing Cyberspace as a Military Domain: Lessons for NATO. Santa Monica, RAND Corporation.

Adamson, L., Z. Homburger (2019). "Let Them Roar: Small States as Cyber Norm Entrepreneurs." European Foreign Affairs Review **24**(2): 217-234.

AIV (2020). Regulering van Online Content: Naar een Herijking van het Nederlandse Internetbeleid. Den Haag, Adviesraad Internationale Vraagstukken.

Arimatsu, L. (2012). A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. 4th International Conference on Cyber Conflict (CyCon), Tallinn.

Arts, S. (2018). Offense as the New Defense: New Life for NATO's Cyber Policy. Policy Brief. Washington, The German Marshall Fund of the United States.

Barbieri, C.&J. Darnis&C. Polito (2018). Non-Proliferation Regime for Cyber Weapons. A Tentative Study. Rome, Istituto Affari Internazionali. **18**.

Barrinha, A., T. Renard (2020). "Power and Diplomacy in the Post-Liberal Cyberspace." International Affairs **96**(3): 749-766.

Belli, L., J. Venturini (2016). "Private Ordering and the Rise of Terms of Service as Cyber-Regulation." Internet Policy Review **5**(4): 1-17.

Bendiek, A., E. Pander - Maat (2019). The EU's Regulatory Approach to Cyber-Security. Berlin, German Institute for International and Security Affairs. **Working Paper No. 2**.

Bendiek, A., R. Bossong, M. Schulze (2017). "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges." SWP Comments: German Institute for International and Security Affairs **47**.

Bernal, P. (2016). "Data Gathering, Surveillance and Human Rights: Recasting the Debate." Journal of Cyber Policy **1**(2): 243-264.

Bigelow, B. (2017). Mission Assurance: Shifting the Focus of Cyber Defence. 9th International Conference on Cyber Conflict. H. Rõigas, R. Jakschis, L. Lindström and T. Minárik (eds.). Tallinn, NATO CCD COE Publications.

Bradshaw, S., P. N. Howard (2018). The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation. Computational Propagana Research Project. Oxford, Oxford Internet Institute.

Broeders, D. (2014). Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance, Department of Sociology. Rotterdam, Erasmus University Rotterdam.

Broeders, D. (2017). "Aligning the International Protection of "the Public Core of the Internet" with State Sovereigty and National Security." Journal of Cyber Policy **2**(3): 366-376.

Broeders, D. (2020) "Creating Consequences for Election Interference." Directions. Beschikbaar via: https://directionsblog.eu/creating-consequences-for-election-interference/.

Broeders, D. & F. Cristiano (2020) "Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road." Milano, Institute for International Political Studies (ISPI), Beschikbaar via: https://www.ispionline.it/it/pubblicazione/cyber-norms-and-united-nations-between-strategic-ambiguity-and-rules-road-25417.

Broeders, D., L. Adamson, R. Creemers (2019). A Coalition of the Unwilling? Chinese & Russian Perspectives on Cyberspace, The Hague, The Hague Program for Cyber Norms.

Brown, D., A. Esterhuysen (2017). A Rights-Based Approach to Cybersecurity: A Pipe Dream or a Critical Means to a Secure and Stable Internet? Internet Governance Forum pre-event, Geneva, Association for Progressive Communications (APC).

Broeders, D., S. Boeke, I. Georgieva (2019). Foreign Intelligence in the Digital Age: Navigating a State of "Unpeace". The Hague, The Hague Program for Cyber Norms.

De Bruijne, M., M. van Eeten, C. Hernández Gañán, W. Pieters (2017). Towards a New Cyber Threat Actor Typology, Delft, TUDelft.

Burton, J. (2015). "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation." Defence Studies **15**(4): 297-319.

Burton, J. (2018) "Cyber Deterrence: A Comprehensive Approach?" CCDCOE Online Publication. Beschikbaar via: https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_pa pe r _ April2018.pdf.

Calandro, E., N. Berglund (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC Case. GIGAnet Annual Symposium. Berlin.

Calderaro, A. (2020). Overcoming Fragmentation in Cyber Diplomacy: The Promise of Cyber Capacity Building. Commentary. Milano, Institute for International Political Studies (ISPI).

Calderaro, A., A. J. S. Craig (2020). "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." Third World Quarterly **41**(6): 917-938.

Carlin, J. P. (2016). "Detect, Disrupt, Deter: Whole-of-Government Approach to National Security Cyber Threats." Harvard National Security Journal **7**(2): 391-436.

Chesney, R., D. Citron (2019). "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." California Law Review **107**(1): 1753-1819.

Chauhan, A. (2019). "A Causal Model for the Extraterritorial Application of Human Rights Treaties Public Law Articles: Section X." Oxford University Undergraduate Law Journal **7**(1): 107-135.

Chuanying, L. (2020). "Forging Stability in Cyberspace." Survival **62**(2): 125-136.

Claessen, E. (2020). "Reshaping the Internet - The Impact of the Securitization of Internet Infrastructure on Approaches to Internet Governance: the Case of Russia and the EU." Journal of Cyber Policy **5**(1): 140-157.

Cohen, R. S., A. Radin (2019). Russia's Hostile Measures in Europe: Understanding the Threat, Santa Monica, RAND Corporation.

Corn, G., E. Jensen (2018). "The Use of Force and Cyber Countermeasures." Temple International & Comparative Law Journal **32**(2): 127-134.

Crandall, M. , C. Allan (2015). "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." Contemporary Security Policy **36**(2): 346-368.

Creemers, R. (2020). China's Conception of Cyber Sovereignty: Rhetoric and Realization. Governing Cyberspace: Behavior, Power and Diplomacy. D. Broeders and B. Van Den Berg (eds), New York - London, Rowman & Littlefield Publishers**:** 107-145.

Crosston, M. D. (2011). "World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence." Strategic Studies Quarterly **5**(1): 100-116.

Deibert, R. J. (2018). "Toward a Human-Centric Approach to Cybersecurity." Ethics & International Affairs **32**(4): 411-424.

Duncombe, C. , T. Dunne (2018). "After Liberal World Order." International Affairs **94**(1): 25-42.

Dutton, W. H., S. Creese, R. Shillair, M. Bada (2019). "Cybersecurity Capacity: Does It Matter?" Journal of Information Policy **9**(1): 280-306.

Eggenschwiler, J. (2019). International Cybersecurity Norm Development: The Roles of States Post-2017, EU Cyber Direct.

Eggenschwiler, J. (2020). "Expert Commissions and Norms of Responsible Behaviour in Cyberspace: a Review of the Activities of the GCSC." Digital Policy, Regulation and Governance **22**(2): 93-107.

Eggenschwiler, J., J. Silomon (2018). "Challenges and Opportunities in Cyber Weapon Norm Construction." Computer Fraud & Security **2018**(12): 11-18.

Eilstrup-Sangiovanni, M. (2018). "Why the World Needs an International Cyberwar Convention." Philosophy & Technology **31**(3): 379-407.

El-Ashy, O., I. Maroni, H. Mizyed, R. Nammar, M. Al-Maskati (2019). "Big Brother in the Middle-East and North Africa: The Expansion of Imported Surveillance Technologies and Their Supportive Legislation." Global Campus Human Rights Journal **3**(2): 229-249.

Eldem, T. (2020). "The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security." International Journal of Public Administration **43**(5): 452-465.

Faesen, L. , B. Torossian, E. Mayhew, C. Zensus (2020). Conflict in Cyberspace: Parsing the Threats and the State of International Order in Cyberspace. Strategic Monitor 2019 - 2020. The Hague, The Hague Centre for Strategic Studies.

Feldstein, S. (2019). The Global Expansion of AI Surveillance. Washington, Carnegie Endowment for International Peace.

Fidler, D. (2012). Cyberattacks and International Human Rights Law. Weapons under International Human Rights Law. S. Casey-Maslen (ed). Cambridge, Cambridge University Press**:** 299-333.

Finnemore, M., D. B. Hollis (2016). "Constructing Norms for Global Cybersecurity." The American Journal of International Law **110**(3): 425-479.

Finnemore, M., D. B. Hollis (2020). "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity." European Journal of International Law (forthcoming).

Fischerkeller, M. P., R. J. Harknett (2017). "Deterrence is Not a Credible Strategy for Cyberspace." Orbis **61**(3): 381-393.

Fischerkeller, M. P., R. J. Harknett (2018) "Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace." Lawfare. Beschikbaar via: https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

Fitzgerald, E. (2016). "Helping States Help Themselves: Rethinking the Doctrine of Countermeasures." Macquarie Law Journal **16**(1): 67-88.

Florek, I., S. Eroglu (2019). "The Need for Protection of Human Rights in Cyberspace." Journal of Modern Science **42**(3): 27-36.

Franklin, A. (2018). "An International Cyber Warfare Treaty: Historical Analgogies and Future Prospects." Journal of Law & Cyber Warfare **7**(1): 149-164.

Gabor, R., L. Aarons (2016). "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace." Journal of National Security Law & Policy **8**(3): 503-530.

Garside, S. (2020). Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom. EU Diplomacy Papers. Bruges, College of Europe.

Gazzini, T. (2010). "A Unique Non-State Actor: the International Committee of the Red Cross." Human Rights and International Legal Discourse **4**(1): 32-46.

Hameed, F., I. Agrafiotis, C. Weisser, M. Goldsmith, S. Creese (2018). Analysing Trends and Success Factors of International Cybersecurity Capacity-Building Initiatives. SECURWARE 2018 : The Twelfth International Conference on Emerging Security Information, Systems and Technologies. Venice.

Hamer, J., R. van Est, L. Royakkers, N. Alberts (2019). Cyberspace Zonder Conflict – Op Zoek naar De-Escalatie van het Internationale Informatieconflict. Den Haag, Rathenau Instituut.

Hampson, F. O., M. Sulmeyer (2017). Getting beyond Norms: New Approaches to International Cyber Security Challenges. Waterloo, Centre for International Governance Innovation.

Hanson, F., S. O'Connor, M. Walker, L. Courtois (2019). Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections. Barton, ASPI International Cyber Policy Centre.

Harknett, R. J. , M. Smeets (2020). "Cyber Campaigns and Strategic Outcomes." Journal of Strategic Studies **43**(1): 1-30.

Healey, J. (2019). "The Implications of Persistent (and Permanent) Engagement in Cyberspace." Journal of Cybersecurity **5**(1): 1-15.

Henriksen, A. (2019). "The End of the Road for the UN GGE Process: The Future Regulations of Cyberspace." Journal of Cybersecurity **5**(1): 1-9.

Heupel, M. (2020). "Indirect Accountability for Extraterritorial Human Rights Violations." International Studies Perspectives **21**(2): 172-197.

Hoffman, W. (2019). "Is Cyber Strategy Possible?" The Washington Quarterly **42**(1): 131-152.

Hohmann, M., A. Pirang, T. Benner (2017). Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach. Berlin, Global Public Policy Institute.

Homburger, Z. (2019). "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace." Global Society **33**(2): 224-242.

Hughes, R. (2010). "A Treaty for Cyberspace." International Affairs **86**(2): 523-541.

Hwang, T. (2017). Digital Disinformation: A Primer. Washington, Atlantic Council.

Ikenberry, G. J. (2018). "The End of the Liberal International Order?" International Affairs **94**(1): 7-23.

Ilves, L. K., T. J. Evans, F. J. Cilluffo, A. A. Nadeau (2016). "European Union and NATO Global Cybersecurity Challenges: A Way Forward." Prism **6**(2): 126-141.

Ivan, P. (2019). Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox. Europe in the World Programme, Brussels, European Policy Centre.

Jensen, B. (2017). "The Cyber Character of Political Warfare." The Brown Journal of World Affairs **24**(1): 159-171.

Kanetake, M. (2019). "The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches." Business and Human Rights Journal **4**(1): 155-162.

Keir, G., W. Hagestad (2013). Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. 5th International Conference on Cyber Conflict (CyCon), Tallinn.

Kilovaty, I. (2016). "World Wide Web of Exploitations-The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach." Columbia Science & Technology Law Review **18**(1): 42-78.

Kilovaty, I. (2020). "An Extraterritorial Human Right to Cybersecurity." Notre Dame Journal of International & Comparative Law **10**(1): 35-55.

King, A., M. Gallagher (2020). Cyberspace Solarium Commission United States of America.

Klimburg, A. (2011). "Mobilising Cyber Power." Survival **53**(1): 41-60.

Klimburg, A. (2017). The Darkening Web: The War for Cyberspace, London, Penguin Books.

Klimburg, A. (2020). "Mixed Signals: A Flawed Approach to Cyber Deterrence." Survival **62**(1): 107-130.

Klimburg, A., H. Zylberberg (2015). Cyber Security Capacity Building: Developing Access. Oslo, Norwegian Institute of International Affairs.

Klimburg, A., L. Faesen (2020). A Balance of Power in Cyberspace. Governing Cyberspace: Behavior, Power and Diplomacy. D. Broeders and B. Van Den Berg (eds.), New York - London, Rowman & Littlefield Publishers**:** 145-171.

Koops, J. A. (2017). "Theorising Inter-Organisational Relations: The "EU-NATO Relationship" as a Catalytic Case Study." European Security **26**(3): 315-339.

Kosseff, J. (2019). The Contours of 'Defend Forward' Under International Law. 11th International Conference on Cyber Conflict (CyCon), Tallinn.

Kosta, E. (2020). "Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights." Regulation & Governance **14**(3): 1-13.

Koster, T. (2020). "How to Counter Worsening Cyber-Security Threats: The International Strategy of the Dutch Government." Atlantisch Perspectief: 15-19.

Lan, T., Z. Xin, H. D. Raduege, D. I. Grigoriev, P. Duggal, S. Schølberg (2010). Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway. A. Nagorski (ed.), Brussels, East West Institute.

Langø, H. (2016). Cyber Security Capacity Building: Security and Freedom. Oslo, Norwegian Institute of International Affairs.

Lawson, S., M. K. Middleton (2019). "Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016." First Monday **24**(3).

Layover, J. , L. Maresca (1999). "The Role of the ICRC in the Development of International Humanitarian Law." International Negotiation **4**(3): 503-527.

Leinhos, L. (2020). "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr." Connections: The Quarterly Journal, **19**(1): 9-19.

Lété, B., P. Pernik (2017). EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions. Policy Brief Washington, The German Marshall Fund of the United States. **38**.

Lewis, J. A. (2017). Revitalizing Progress in International Negotiations on Cyber Security. Getting beyond Norms: New Approaches to International Cyber Security Challenges. F. O. Hampson and M. Sulmeyer (eds.), Waterloo, Centre for International Governance Innovation.

Liaropoulos, A. (2015). "A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia " Journal of Information Warfare **14**(4): 15-24.

Liaropoulos, A. (2016). "Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance." International Journal of Cyber Warfare and Terrorism (IJCWT) **6**(2): 32-40.

Lonsdale, D. J. (2016). "Britain's Emerging Cyber-Strategy." The RUSI Journal **161**(4): 52-62.

Lotrionte, C. (2014). "Countering State-Sponsored Cyber Economic Espionage under International Law." North Carolina Journal of International Law and Commercial Regulation **40**(1): 443-542.

Lucas, G. R. (2017). Ethics of Cyberwarfare: The Quest for Responsible Security in the Age of Digital Warfare. Oxford, Oxford University Press.

Mačák, K. (2016). Is the International Law of Cyber Security in Crisis? 8th International Conference on Cyber Conflict (CyCon), Tallinn.

Mačák, K. (2017). "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers." Leiden Journal of International Law **30**(4): 877-899.

Mack, D. (2020). "An Era of Foreign Political Interference: Impulsive, Overcompensation of Australia, and a Comparison of Legislative Schemes with the United States." Emory International Law Review **34**(1): 367-397.

Mann, M., A. Daly, M. Wilson, N. Suzor (2018). "The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)Balance in Australia." International Communication Gazette **80**(4): 369-384.

Margulies, P. (2016). "Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights." Florida Law Review **68**(4): 1045-1118.

Maurer, T. (2018). Cyber Mercenaries: The State, Hackers, and Power, Cambridge, Cambridge University Press.

Maurer, T. (2018). "Cyber Proxies and Their Implications for Liberal Democracies." The Washington Quarterly **41**(2): 171-188.

McKune, S., S. Ahmed (2018). "Authoritarian Practices in the Digital Age: The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda." International Journal of Communication **12**: 3835-3855.

Michaelsen, M. (2017). "Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran." Surveillance & Society **15**(3/4): 465-470.

Mihr, A. (2014). "Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach." Georgetown Journal of International Affairs **15**: 24-34.

Mihr, A. (2017). Justice. Cyber Justice: Human Rights and Good Governance for the Internet. Cham, Springer.

Moise, A. C. (2016). "Cybersecurity and Human Rights." Revista Universul Juridic **2**(3): 160-164.

Moret, E., P. Pawlak (2017). The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime? Paris, European Union Institute for Security Studies (EUISS).

Morgan, S. (2016). Clarifying Goals, Revitalizing Means: An Independent Evaluation of the Freedom Online Coalition. Internet Policy Observatory. Philadelphia, Centre for Global Communications Studies.

Moynihan, H. (2019). The Application of International Law to State Cyberattacks Sovereignty and Non-intervention. London, Chatham House, the Royal Institute of International Affairs.

Nakasone, P. M. (2019). "A Cyber Force for Persistent Operations." Joint Force Quarterly **92**(1): 10-14.

Natoli, T. (2019). Testing the Analogy: The CoE-ECHR System Pioneering Human Rights Protection in the Cyberspace. Borders, Legal Spaces and Territories in Contemporary International Law: Within and Beyond. T. Natoli and A. R. (eds.), Cham, Springer.

Noesselt, N. (2016). "Contested Global Order(s): Rising Powers and the Re-legitimization of Global Constitutionalization." International Journal of Constitutional Law **14**(3): 639-656.

Nye, J. S. Jr. (2010). Cyber Power. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Nye, J. S. Jr. (2016). "Will the Liberal Order Survive?" Foreign Affairs **96**(1): 10-16.

Nye, J. S. Jr. (2017). "Deterrence and Dissuasion in Cyberspace." International Security **41**(3): 44-71.

Nye, J. S. Jr. (2017). Normative Constraints on Cyber Arms. Getting beyond Norms: New Approaches to International Cyber Security Challenges. F. O. Hampson and M. Sulmeyer (eds.), Waterloo, Centre for International Governance Innovation.

Nye, J. S. Jr. (2019). "The Rise and Fall of American Hegemony from Wilson to Trump." International Affairs **95**(1): 63-80.

Ott, N., A. Osula (2019). The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level. 11th International Conference on Cyber Conflict: Silent Battle. T. Minárik, S. Alatalu, S. Biondi et al., Tallinn, NATO CCD COE Publications.

Paterson, T., L. Hanley (2020). "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes'." Australian Journal of International Affairs **74**(4): 439-454.

Pawlak, P. (2014). Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development. Paris, European Union Institute for Security Studies. **21**.

Pawlak, P., P. Barmpaliou (2017). "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity." Journal of Cyber Policy **2**(1): 1-22.

Pernik, P. (2014). Improving Cyber Security: NATO and the EU. Tallinn, International Center for Defence Studies.

Piccone, T. (2018). "Democracy and Digital Technology The Sur File on Internet and Democracy." Sur - International Journal on Human Rights **15**(27): 29-38.

Pijnenburg-Muller, L. (2015). Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities. Olso, Norwegian Institute of International Affairs.

Polyakova, A., S. P. Boyer (2018). The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition. The New Geopolitics: Europe. Stuttgart, Brookings - Robert Bosch Foundation Transatlantic Initiative (BBTI).

Popescu, N., S. Secrieru (2018). Hacks, Leacks and Disruptions: Russian Cyber Strategies, Paris, European Union Institute for Security Studies (EUISS).

Pronk, D. (2019). The Return of Political Warfare. Strategic Monitor 2018-2019. The Hague, Clingendael.

Raban, Y., A. Hauptman (2018). "Foresight of Cyber Security Threat Drivers and Affecting Technologies." Foresight **20**(4): 353-363.

Rascoff, S. J. (2016). "The Norm against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections " The University of Chicago Law Review **83**(1): 249-269.

Reglitz, M. (2020). "The Human Right to Free Internet Access." Journal of Applied Philosophy **37**(2): 314-331.

Rodriguez, C. A., T. C. Walton, H. Chu (2020). "Putting the "FIL" into "DIME": Growing Joint Understanding of the Instruments of Power." Joint Force Quarterly **97**(2): 121-128.

Roguski, P. (2020). Application of International Law to Cyber Operations: A Comparative Analysis of States' Views, The Hague, The Hague Program for Cyber Norms and Universiteit Leiden.

Roguski, P. (2020) "Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace." Just Security. Beschikbaar via: https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

Ruhl, C., D. B. Hollis, W. Hoffman, T. Maurer (2020). Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. Washington, Carnegie Endowment for International Peace

Ryan, N. J. (2018). "Five Kinds of Cyber Deterrence." Philosophy & Technology **31**(1): 331-338.

Sander, B. (2019). The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations. 11th International Conference on Cyber Conflict (CyCon), Tallinn.

Schaake, M., M. Vermeulen (2016). "Towards a Values-Based European Foreign Policy to Cybersecurity." Journal of Cyber Policy **1**(1): 75-84.

Scharf, M. P. (2014). "Accelerated Formation of Customary International Law." ILSA Journal of International and Comparative Law **20**(2): 305-342.

Schia, N. (2016). "Cyber Security Capacity Building, Digitalization and the Global South." European Cybersecurity Journal **2**(4): 82-94.

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, Cambridge University Press.

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, Cambridge University Press.

Schmitt, M. N., L. Vihul (2017). "Sovereignty in Cyberspace: Lex Lata Vel Non?" AJIL Unbound **111**: 213- 218.

Schmitt, M. N. (2018). "International Cyber Norms: Reflections on the Path Ahead." Militair Rechtelijk Tijdschrift **111**(3): 1-12.

Schmitt, M. N. (2018). "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." Chicago Journal of International Law **19**(1).

Schnidrig, D., K. Aiken (2020). "Engagement in Cyber Capacity Building - Lessons Learned after 5 years of GFCE." Global Cyber Expertise Magazine **7**.

Schweighofer, E. & I. Brunner & J. Zanol (2020). "Malicious Cyber Operations,"Hackbacks" and International Law: An Austrian Example as a Basis for Discussion on Permissible Responses." Masaryk University Journal of Law and Technology **14**(2): 227-258.

Shackelford, S. J. (2019). "Should Cybersecurity be a Human Right: Exploring the Shared Responsibility of Cyber Peace." Stanford Journal of International Law **55**(2): 155-184.

Shandler, R., D. Canetti (2019). "A Reality of Vulnerability and Dependence: Internet Access as a Human Right." Israel Law Review **52**(1): 77-98.

Shany, Y., M. N. Schmitt (2020). "An International Attribution Mechanism for Hostile Cyber Operations." International Law Studies **96**(1): 196-222.

Sharp, T. (2018). "Hiding in Plain Sight: Political Effects of Cyber Operations." Survival **60**(6): 45-53.

Shea, J. (2018). "Cyberspace as a Domain of Operations: What is NATO's Vision and Strategy?" Marine Corps University Journal **9**(2): 133-150.

Sigholm, J. (2016). "Non-State Actors in Cyberspace Operations." Journal of Military Studies **4**(1): 1-37.

Smeets, M. (2019) "Cyber Command's Strategy Risks Friction With Allies." Lawfare. Beschikbaar via: https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

Smeets, M. (2020). "US Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection." Intelligence and National Security **35**(3): 444-453.

Smeets, M., H. Lin (2019). A Strategic Assessment of the U.S. Cyber Command Vision. Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations. A. Zegart and H. Lin (eds.), Washington, Brookings Institution Press.

Sulmasy, G., J. Yoo (2007). "Counterintuitive: Intelligence Operations and International Law." Michigan Journal of International Law **28**(3): 625-638.

Sweijs, T., D. Pronk (2020). Between Order and Chaos? The Writing on the Wall Strategic Monitor 2019-2020. The Hague, The Hague Centre for Strategic Studies and Clingendael Netherlands Institute of International Relations.

Taddeo, M. (2018). "Deterrence and Norms to Foster Stability in Cyberspace." Philosophy & Technology **31**(3): 339-355.

Taddeo, M. (2020). Norms and Strategies for Stability in Cyberspace. The 2019 Yearbook of the Digital Ethics Lab. C. Burr and S. Milano (eds.), Cham, Springer**:** 31-44.

Teichmann, M. (2020). Five Threats that Influence the Cyber Landscape: New Cybercrime Operating Model Among High-profile Threat Groups. European Cyber Security Perspectives. K. van der Wekke. Amsterdam, KPN CISO. **7**.

Thirlway, H. (2015). "Human Rights in Customary Law: An Attempt to Define Some of the Issues." Leiden Journal of International Law **28**(3): 495-506.

Thornton, R., M. Miron (2019). "Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom." Journal of Cyber Policy **4**(2): 257-274.

Tikk, E. (2020). International Law in Cyberspace: Mind the gap. Research in Focus. Jyväskylä, Cyber Policy Institute.

Tikk, E., M. Kerttunen (2017). The Alledged Demise of the UN GGE: An Autopsy and Eulogy. Jyväskylä, Cyber Policy Institute.

Tikk-Ringas, E. (2016). "International Cyber Norms Dialogue as an Exercise of Normative Power." Georgetown Journal of International Affairs **17**(3): 47-59.

Tor, U. (2015). "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." Journal of Strategic Studies **40**(2): 92-117.

Torossian, B. , L. Fagliano, T. Görder (2020). Hybrid Conflict: Neither War, nor Peace. Strategic Monitor 2019- 2020. The Hague, The Hague Centre for Strategic Studies.

Treverton, G. F., A. Thvedt, A. R. Chen, K. Lee, M. McCue (2018). Addressing Hybrid Threats. Stockholm, Swedish Defence University.

Turianskyi, Y. (2020). Africa and Europe: Cyber Governance Lessons. African Perspectives Global Insights. Johannesburg, South African Institute of International Affairs.

Valeriano, B. & B. Jensen & R. C. Maness (2018). Cyber Strategy: The Evolving Character of Power and Coercion. New York, Oxford University Press.

Van den Bosch, G. L. C. (2019). Oorlog Voeren Zonder Geweld: Onderzoek naar de Regels binnen het Humanitair Oorlogsrecht voor Militaire Cyberoperaties die de Drempel van Aanval niet Halen, Amsterdam, Universiteit van Amsterdam.

Van der Meer, S. (2015). "Enhancing International Cyber Security: A Key Role for Diplomacy." Security and Human Rights **26**: 193-205.

Van der Meer, S. (2015). Foreign Policy Responses to International Cyber-Attacks: Some Lessons Learned. The Hague, Clingendael.

Van der Meer, S. (2018). State-Level Responses to Massive Cyber-Attacks: a Policy Toolbox. The Hague, Clingendael Spectator.

Van der Meulen, N., E. A. Jo, S. Soesanto (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Brussels, European Union.

Van der Putten, F., M. Meijnders, J. Rood (2015). Afschrikking als Veiligheidsconcept tegen Niet-Traditionele Dreigingen. Clingendael Monitor 2015. Den Haag, Clingendael.

Van der Putten, F., M. Meijnders, S. van der Meer, T. van der Togt (2018). Hybrid Conflict: The Roles of Russia, North Korea and China. The Hague, Dutch National Network of Safety and Security Analysts (ANV).

Väljataga, A. (2018) "Tracing Opinio Juris in National Cyber Security Strategy Documents." CCDCOE Online Publication. Beschikbaar via: https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf.

Van Horenbeeck, M. (2018). "The Future of Internet Governance and Cyber-Security." Computer Fraud & Security(5): 6-8.

Viganò, E., M. Loi, E. Yaghmaei (2020). Cybersecurity of Critical Infrastructure. The Ethics of Cybersecurity. M. Christen & B. Gordijn & M. Loi, Springer Nature.

Wagner, B., J. Bronowicka, C. Berger, T. Behrndt (2015). Surveillance and Censorship: The Impact of Technologies on Human Rights. Brussels, EU Parliament: Directorate-General for External Policies: Policy Department: Study.

Watt, E. (2017). The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance. 9th International Conference on Cyber Conflict. H. Rõigas, R. Jakschis, L. Lindström and T. Minárik (eds.), Tallinn, NATO CCD COE Publications.

Weber, R. H. (2012). "Future Design of Cyberspace Law: Laws are Sand (Mark Twain, the Gorky Incident)." Journal of Politics and Law **5**(4): 1-14.

Wiking - Häger, E., C. Dackö (2017). Cybersecurity Law Overview. Stockholm, Mannheimer Swartling.

Wilner, A. S. (2019). "US Cyber Deterrence: Practice Guiding Theory." Journal of Strategic Studies **43**(2): 245-280.

Woodward, B. (2010). Global Civil Society in International Lawmaking and Global Governance Theory and Practice, Leiden, Martinus Nijhoff Publishers.

Wouters, J., M. Hermez (2016). EU Guidelines on Human Rights as a Foreign Policy Instrument: An Assessment. Leuven, Leuven Centre for Global Governance Studies and the Institute for International Law. **Working Paper No. 170**.

Overheids-, organisatie- en juridische documenten

AIV/CAVV (2011). *Cyber Warfare*.

AIVD (2017). *Jaarverslag 2017*.

AIVD (2019). *Offensief Cyberprogramma.*

Amnesty (2020) "Digital Surveillance Threats for 2020." Amnesty International. Beschikbaar via: https://www.amnesty.ie/digital-surveillance-threats-for-2020/.

Amnesty International (2019) "State-Sponsored Hackers Target Amnesty International Hong Kong with Sophisticated Cyber-Attack." Amnesty International. Beschikbaar via: https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/.

Amnesty International (2020). Out of Control: Failing EU Laws for Digital Surveillance Export. London, Amnesty International.

Articles on State Responsibility, Chapter II of Part 3, para. 3 of Commentary.

Autoriteit Persoonsgegevens (2020) "Werkwijze Belastingdienst in Strijd met de Wet en Discriminerend." Autoriteit Persoonsgegevens, Beschikbaar via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/werkwijze-belastingdienst-strijd-met-de-wet-en-discriminerend.

Besluit (GBVB). 2019/797 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen, para. 9.

Blok, S. (2018). Toespraak minister Blok over 1-jarig bestaan Tallinn Manual 2.0. Beschikbaar via: https://www.rijksoverheid.nl/documenten/toespraken/2018/06/20/toespraak-minister-blok-over-eenjarig-bestaan-tallinn-manual.

Botek, A. (2019) "European Union Establishes a Sanction Regime for Cyber-Attacks." CCDCOE Online Publication. Beschikbaar via: https://ccdcoe.org/incyder-articles/european-union-establishes-a-sanction-regime-for-cyber-attacks/.

Brown, D., A. Esterhuysen, M. Knodel (2017). Briefing Document: Cybersecurity Policy and Human Rights, Association for Progressive Communications (APC).

CCDCOE (2020) "Tallinn Manual 2.0." CCDCOE. Beschikbaar via: https://ccdcoe.org/research/tallinn-manual/.

Committee on Foreign Relations (2018). Putin's Assymetric Assault on Democracy in Russia and Europe: Implications for US National Security. Beschikbaar via: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

Council of Europe (2014). EU Human Rights Guidelines on Freedom of Expression Online and Offline, Foreign Affairs Council Meeting, Brussels.

Council of Europe (2020). "Cybercrime Programme Office (C-PROC)." Council of Europe Portal. Beschikbaar via: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-.

Council of the European Union (2014) *EU Human Rights Guidelines on Freedom of Expression Online and Offline*, Foreign Affairs Council Meeting, Brussels.

Council of the European Union (2014). EU Cyber Defence Policy Framework.

Council of the European Union (2016). Non-paper: Developing a Joint EU Diplomatic Response against Coercive Cyber Operations.

Council of the European Union (2017). Draft Council Conclusions On A Framework For A Joint EU Diplomatic Response To Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

Council of the European Union (2018). EU Cyber Defence Policy Framework.

Court of European Auditors (2019). Challenges to Effective EU Cybersecurity Policy. Strasbourg.

De Nationale Cybersecurity Strategie NCSS (2013). Beschikbaar via: https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2

Declaration of Principles, World Summit on the Information Society.

DOD Science Defense Board (2013). Task Force Report: Resilient Military Systems and the Advanced Cyber Threat. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

Esterhuysen, A., D. Brown, D. Kumar (2019). Unpacking the GGE's Framework on Responsible State Behaviour: Cyber Norms, Global Partners Digital and the Association for Progressive Communications.

European Commission (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Policy. Brussels.

European Commission (2018), *Action Plan Against Disinformation.*

European Court of Auditors (2019), Challenges to Effective EU Cybersecurity Policy. Strasbourg.

European Court of Human Rights (1995). Loizidou v. Turkey (Preliminary Objections).

European Court of Human Rights (2008). Liberty and Others v. the United Kingdom, 2008-IV.

European Parliament (2019). legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online.

European Union (2016). Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign and Security Policy.

European Union (2020). EU Legt voor het Eerst Sancties op tegen Cyberaanvallen. Beschikbaar via: https://www.consilium.europa.eu/nl/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

Fifth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.

G7 France (2019). Foreign Ministers Meeting, Dinard Declaration on the Cyber Norm Initiative.

Global Commission on the Stability of Cyberspace (2019). Advancing Cyberstability. The Hague - New York, Global Commission on the Stability of Cyberspace **Final Report**.

HRW (2020). "EU: Strengthen Rules on Surveillance Tech Exports Member States Should Put Rights Ahead of Profits." Human Rights Watch. Beschikbaar via: https://www.hrw.org/news/2020/06/09/eu-strengthen-rules-surveillance-tech-exports.

Human Rights Committee (2004). General Comment No. 31: "The Nature of the General Legal Obligations Imposed on States Parties to the Covenant", supra note 9.

ICRC (2020). "Call to Governments: Work Together to Stop Cyber Attacks on Health Care." ICRC. Beschikbaar via: https://www.icrc.org/en/document/governments-work-together-stop-cyber-attacks-health-care.

ICRC (2020). "Norms for Responsible State Behavior on Cyber Operations Should Build on International Law." ICRC. Beschikbaar via: https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, para. 26-27. Ibid., para. 28.

Internationaal Gerechtshof (1997). Gabcikovo - Nagymaros Project (Hungary/Slovakia), Judgment.

Internationaal Gerechtshof (2008). United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), paras. 67-68.

Microsoft (2018). A Digital Geneva Convention to Protect Cyberspace. Beschikbaar via: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

Ministerie van Buitenlandse Zaken (2019). Bijlage: Internationaal Recht in het Digitale Domein (Cyberspace). Den Haag, Het Koninkrijk der Nederlanden.

Ministerie van Buitenlandse Zaken (2019). Kamerbrief Inzake Internationale Rechtsorde in het Digitale Domein.

Ministerie van Defensie (2018). Defensie Cyber Strategie 2018 - Investeren in Digitale Slagkracht Nederland.

Morgus, R., M. Smeets, T. Herr (2017). Countering the Proliferation of Offensive Cyber Capabilities. GCSC Issue Brief, Global Commission on the Stability of Cyberspace.

NATO (2014). Wales Summit Declaration.

NCTV (2015). Cybersecuritybeeld Nederland CSBN 2015. Den Haag, Nationaal Coördinator Terrorismebestrijding en Veiligheid.

NCTV (2016). Cybersecuritybeeld Nederland CSBN 2016. Den Haag, Nationaal Coördinator Terrorismebestrijding en Veiligheid.

NCTV (2017). Cybersecuritybeeld Nederland CSBN 2017. Den Haag, Nationaal Coördinator Terrorismebestrijding en Veiligheid.

NCTV (2018). Cybersecuritybeeld Nederland CSBN 2018. Den Haag, Nationaal Coördinator Terrorismebestrijding en Veiligheid.
NCTV (2019). Cybersecuritybeeld Nederland CSBN 2019. Den Haag, Nationaal Coördinator Terrorismebestrijding en Veiligheid.
NCTV (2020). Cybersecuritybeeld Nederland CSBN 2020. Den Haag, Nationaal Coördinator Terrorismebestrijding en Veiligheid.
OEWG "Initial "Pre-Draft" of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security." Beschikbaar via: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf.
OEWG (2020). "Second "Pre-Draft" of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security." Beschikbaar via: https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf.
OVSE 1092nd Plenary Meeting. PC.DEC/1202.
Responsibility of States for Internationally Wrongful Acts (2001).
Rõigas, H. (2015) "An Updated Draft of the Code of Conduct Distributed in the United Nations - What's New?" CCDCOE Online Publication. Beschikbaar via: https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/.
Shears, M., D Schnidrig, L. Kaspar (2018). Multistakeholder Approaches to National Cybersecurity Strategy Development. London, Global Partners Digital.
Uitvoeringsverordening (EU) 2020/1125 van de Raad van 30 juli 2020 tot uitvoering van verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de unie of haar lidstaten bedreigen.
UK-China Joint Statement (2015). Beschikbaar via: https://www.gov.uk/government/news/uk-china-joint-statement-2015.
VN Algemene Vergadering A/68/98, A/68/156, A/69/112, A/70/174.
VN Handvest.

Non-academisch en blogs

Applebaum, J. (2016) "The Dutch Just Showed the World how Russia Influences Western European Elections." The Washington Post. Beschikbaar via: https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fopinions%2frussias-influence-in-western-elections%2f2016%2f04%2f08%2fb427602a-fcf1-11e5-886f-a037dba38301_story.html.
Article 19 (2018) "UN HCR Maintains Consensus on Internet Resolution." Article 19. Beschikbaar via: https://www.article19.org/resources/un-hrc-maintains-consensus-on-internet-resolution/.
Brouwers, A. (2020) "VS en Europa Zien Chinese Dreiging Compleet Anders." de Volkskrant. Beschikbaar via: https://www.volkskrant.nl/nieuws-achtergrond/vs-en-europa-zien-chinese-dreiging-compleet-anders~bb3a3d63/.
Buchanan, B., R. B. Williams (2018) "A Deepening U.S.-China Cybersecurity Dilemma." Lawfare. Beschikbaar via: https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma.
Chesney, R. (2018) "An American Perspective on a Chinese Perspective on the Defense Department's Cyber Strategy and 'Defending Forward'." Lawfare. Beschikbaar via:

https://www.lawfareblog.com/american-perspective-chinese-perspective-defense-departments-cyber-strategy-and-defending-forward.

Emmot, R. (2018) "NATO Cyber Command to Be Fully Operational in 2023." Reuters. Beschikbaar via: https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9.

Emmot, R. (2020) "Russia Deploying Coronavirus Disinformation to Sow Panic in West, EU Document Says." Reuters. Beschikbaar via: https://www.reuters.com/article/us-health-coronavirus-disinformation-idUSKBN21518F.

Emmot, R., J. Irish, A. Rinke (2019) "EU Divisions over Russia Mount as France, Germany Seek Peace in Ukraine." Reuters. Beschikbaar via: https://www.reuters.com/article/us-ukraine-russia-eu/eu-divisions-over-russia-mount-as-france-germany-seek-peace-in-ukraine-idUSKCN1WL04D.

Goldsmith, J. (2011) "Cybersecurity Treaties: A Skeptical View." Hoover Institution. Beschikbaar via: https://www.hoover.org/research/cybersecurity-treaties-skeptical-view.

Healey, J. (2018) "Triggering the New Forever War, in Cyberspace." Cipher Brief. Beschikbaar via: https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace.

Higgins, A. (2017) "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote." The New York Times. Beschikbaar via: https://www.nytimes.com/2017/02/16/world/ europe/rus sia-ukr aine-fake-news-dutch-vote.html?auth=login-facebook.

Hollis, D. B. (2012) "Is a Use of Force the Same as an Armed Attack in Cyberspace?" OpinioJuris. Beschikbaar via: http://opiniojuris.org/2012/04/28/is-a-use-of-force-the-same-as-an-armed-attack-in-cyberspace/#:~:text=In%20other%20words%2C%20there%20is,US%20Gove rnmen t%20positio n%20for%20cyberspace.

Hollis, D. B. (2012) "Should There Be an International Treaty on Cyberwarfare?" OpinioJuris. Beschikbaar via: http://opiniojuris.org/2012/06/13/should-there-be-an-international-treaty-on-cyberwarfare/#comments.

Jinghua, L. (2018) "What Really Matters in 'Defending Forward'?" Lawfare. Beschikbaar via: https://www.lawfareblog.com/what-really-matters-defending-forward.

Kadri, K. (2019) "Trends in International Law for Cyberspace." CCDCOE Online Publication. Beschikbaar via: https://ccdcoe.org/incyder-articles/european-union-establishes-a-sanction-regime-for-cyber-attacks/.

Kilovaty, I., I. Mann (2016) "Towards a Cyber-Security Treaty." Just Security. Beschikbaar via: https://www.justsecurity.org/32268/cyber-security-treaty/?print.

Levine, M. (2017) "Russia Tops List of 100 Countries that Could Launch Cyberattacks on US." ABC News. Beschikbaar via: https://abcnews.go.com/US/russia-tops-list-100-countries-launch-cyberattacks-us/story?id=47487188.

Mačák, K., T. Rodenhäuser, L. Gisel (2020) "Cyber Attacks Against Hospitals and the Covid-19 Pandemic: How Strong are International Law Protections." Humanitarian Law & Policy. Beschikbaar via: https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/ **2020**.

Mueller, M., K. Grindal, B. Kuerbis, F. Badiei (2019). "Cyber Attribution: Can a New Institution Achieve Transnational Credibility?" The Cyber Defense Review **4**(1): 107-122.

Nakashima, E. (2013) "U.S. and Russia Sign Pact to Create Communication Link on Cyber Security." The Washington Post. Beschikbaar via: https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fworld%2fnational-security%2fus-and-russia-sign-pact-to-create-communication-link-on-cyber-security%2f2013%2f06%2f17%2fca57ea04-d788-11e2-9df4-895344c13c30_story.html.

Nakashima, E., S. Mufson (2015) "The U.S. and China Agree not to Conduct Economic Espionage in Cyberspace." The Washington Post. Beschikbaar via: https://www.washingtonpost.com /world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html.

Nordic Monitor (2020) "Turkey Blocked EU-NATO Partnership Programs." Nordic Monitor. Beschikbaar via: https://www.nordicmonitor.com/2020/01/turkey-blocked-eu-nato-partnership-programs/.

Ramdharie, S. (2020) "CIA Rapport: Grote Kans dat Poetin Beïnvloeding van de Amerikaanse Verkiezingen Leidt." de Volkskrant. Beschikbaar via: https://www.volkskrant.nl/nieuws-achtergrond/cia-rapport-grote-kans-dat-poetin-beinvloeding-van-de-amerikaanse-verkiezingen-leidt~b3d4a67f/.

Reuters (2020) "NSA Surveillance Exposed by Snowden was Illegal, Court Rules Seven Years On." The Guardian. Beschikbaar via: https://www.theguardian.com/us-news/2020/sep/03/edward-snowden-nsa-surveillance-guardian-court-rules.

Righton, N. (2020) "Trump Eist in VN-Toespraak Actie tegen China vanwege Coronacrisis, Xi Toont Zich Juist Verzoenend." de Volkskrant. Beschikbaar via: https://www.volkskrant.nl/nieuws-achtergrond/trump-eist-in-vn-toespraak-actie-tegen-china-vanwege-coronacrisis-xi-toont-zich-juist-verzoenend~b3eddobb/.

Schmitt, M. N. (2019) "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis." Just Security. Beschikbaar via: https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/. **2020**.

Schneider, J. (2019) "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy." Lawfare. Beschikbaar via: https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy.

Schuldt, L. (2019) "Truth vs. Free Speech: How Southeast Asia's War on Fake News Unfolds." Verfassungsblog on Matters Constitutional. Beschikbaar via: https://verfassungsblog.de/truth-vs-free-speech/.

Snyder, X. (2018) "How the European Union Became Divided on Russia." Geopolitical Features. Beschikbaar via: https://geopoliticalfutures.com/european-union-became-divided-russia/.

Soesanto, S. (2018) "In Cyberspace, Governments Don't Know How to Count." Defense One. Beschikbaar via: https://www.defenseone.com/ideas/2018/09/cyberspace-governments-dont-know-how-count/151629/.

Taddeo, M., L. Floridi (2018) "Regulate Artificial Intelligence to Avert Cyber Arms Race." Nature Publishing Group. Beschikbaar via: https://www.nature.com/articles/d41586-018-04602-6/.

Stilgherrian (2018). Blaming Russia for NotPetya Was Coordinated Diplomatic Action. ZDNet. Beschikbaar via: https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

UN News (2020) "UN Chief Appeals for Global Solidarity at General Assembly, Warns COVID is 'Dress Rehearsal' for Challenges Ahead." UN News. Beschikbaar via: https://news.un.org/en/story/2020/09/1072972.

Van Bemmel, N., L. Vervaeke (2020) "Aan het Front van de Techoorlog: het Chinese Streven naar Technologische Dominantie." de Volkskrant. Beschikbaar via: https://www.volkskrant.nl/wetenschap/aan-het-front-van-de-techoorlog-het-chinese-streven-naar-technologische-dominantie~b9 ofa1c5/?referrer=htt ps%3A%2F%2Fww w. google.com%2F.

Vavra, S. (2020) "Chinese Cyber Power is Neck-and-Neck with US, Harvard Research Finds." Cyberscoop. Beschikbaar via: https://www.cyberscoop.com/chinese-cyber-power-united-states-harvard-belfer-research/.

Verfassungsschutz (2018). Cyber Attacks Controlled by Intelligence Services. Bundesambt für Verfassungsschutz. Beschikbaar via: https://www.verfassungsschutz.de/en/download-manager/_publication-2018-05-cyber-attacks-controlled-by-intelligence-services.pdf.