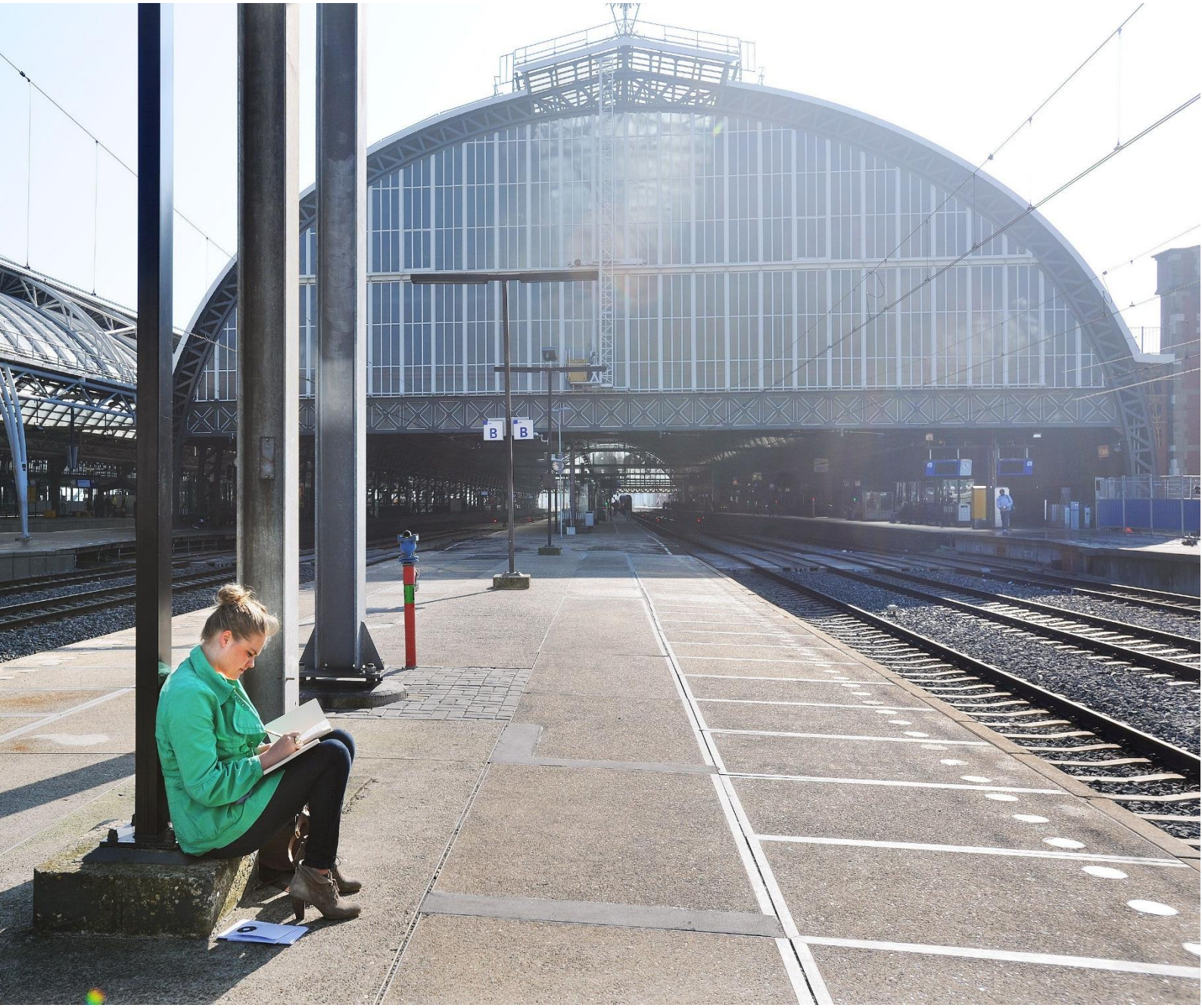
Rathenau Instituut

Cyberspace zonder conflict

Op zoek naar de-escalatie van het internationale informatieconflict



Rapport

Auteurs
Jurriën Hamer, Rinie van Est & Lambèr Royakkers, met medewerking van Nicole Alberts

Redactie
Arnold Vonk

Infographics
Rikkers Infographics

Foto omslag
Amsterdam Centraal tijdens een computerstoring die het treinverkeer heeft stilgelegd, 2012. Foto: Guus Dubbelman / Hollandse Hoogte

Bij voorkeur citeren als:
Hamer, J., R. van Est, L. Royakkers, met medewerking van N. Alberts (2019). *Cyberspace zonder conflict – Op zoek naar de-escalatie van het internationale informatieconflict*. Den Haag: Rathenau Instituut

Voorwoord

Cyberaanvallen vinden dagelijks plaats, en hebben soms grote gevolgen. Rusland pleegde cyberaanvallen in Oekraïne. China hackt en bespioneert buitenlandse bedrijven. En de Verenigde Staten hebben via cyberspace sabotage uitgevoerd. We zijn zo in een complexe, onvoorspelbare en dreigende internationale situatie terechtgekomen. Ook Nederland loopt risico; hier vielen buitenlandse hackers onder meer ziekenhuizen en de Rotterdamse haven aan. Wat kan Nederland met andere landen doen om escalatie te voorkomen? Daarover gaat dit rapport.

Het Rathenau Instituut heeft als taak de politieke besluitvorming en het publieke debat over de impact van technologie op de samenleving te ondersteunen. Die taak heeft ook betrekking op het terrein van cyberaanvallen. Dit rapport sluit aan op eerdere onderzoeken, zoals ons rapport *Een nooit gelopen race*. We hopen ermee te bereiken dat, naast deskundigen en bestuurders, ook burgers snappen wat er in de cyberspace gebeurt, en dat ze erover mee kunnen praten.

Dit rapport geeft een overzicht van de internationale situatie en richt zich op de cyberwapenopbouw en het diplomatieke beleid van landen. Uit literatuur en gesprekken blijkt dat staten over cyberaanvallen geen heldere afspraken hebben gemaakt; we spreken van een informatieconflict. Dat maakt de huidige internationale situatie riskant en zorgwekkend. Als Nederland wil bijdragen aan het de-escaleren van dit informatieconflict, dan zijn vijf acties van belang: internationale samenwerking en heldere afspraken, coördinatie van de aanschaf van cyberwapens, en samenwerking met bedrijven. Tot slot roepen we de overheid op burgers te betrekken bij beslissingen over cyberveiligheid.

Juist in een tijd van internationale conflicten is het goed om stil te staan bij de kracht van burgers. Tijdens de Koude Oorlog waren veel mensen bang voor ‘de bom’. Er ontstond een debat over het gebruik van kernwapens. Dit laat zien dat burgers de overheid niet alleen nodig hebben om hen te beschermen; ze moeten zelf ook de overheid vragen om actie. In het informatieconflict zijn burgers directer betrokken, en is het militaire aspect meer verweven met de samenleving. Samen kunnen we op zoek gaan naar een cyberspace zonder conflict. Daarvoor moeten burgers en hun overheden ook de kennis hebben van wat er gebeurt en wat er kan. Met de bevindingen uit dit onderzoek willen we daar aan bijdragen.

Dr. ir. Melanie Peters
Directeur Rathenau Instituut

Samenvatting

Steeds meer landen kunnen cyberaanvallen uitvoeren die grote schade aanrichten aan bedrijven, mensen en overheidsinstellingen. Vrijwel alle landen gebruiken deze cyberwapens ook. Ze bespioneren elkaar en proberen in elkaars digitale systemen te infiltreren; sommige staten voeren zelfs cybersabotage uit of verspreiden desinformatie. Door middel van informatietechnologie ontstaat een nieuw conflict. In dit rapport spreken we van een informatieconflict.

Wat kan de Nederlandse bijdrage zijn aan de de-escalatie van dit informatieconflict? Dit rapport biedt vijf oplossingsrichtingen. Het roept op burgers te betrekken bij het politieke en maatschappelijke debat over internationale cyberveiligheid. Vooral zij worden immers geraakt door die cyberaanvallen. Tegelijk zijn zij ook degenen die zowel overheid als politiek kunnen oproepen tot de-escalatie.

Dit rapport bouwt voort op eerdere publicaties van het Rathenau Instituut, zoals *Een nooit gelopen race*, *Digitalisering van het nieuws* en *Just ordinary robots: Automation from love to war*.

Het karakter van cyberaanvallen
Dit rapport beschrijft allereerst wat cyberaanvallen zijn, en vergelijkt deze met conventionele militaire aanvallen. Dit levert het volgende beeld op.

Cyberaanvallen kunnen veelal vanaf grote afstand plaatsvinden, kunnen zich razendsnel verspreiden en zijn soms lastig te detecteren – zeker als het geraffineerde spionage betreft, of hoogwaardige vervalsingen van beeld en geluid. Cyberaanvallen worden soms zelfs als een dienst aangeboden. Cyberaanvallers variëren van inlichtingendiensten tot cybercriminelen, en hoeven zelden te vrezen voor de gevolgen, zoals berechting.

Tegelijkertijd zijn cyberaanvallen niet per se schadelijker dan conventionele aanvallen. Sterker nog: Cyberaanvallen richten zelden ernstige fysieke schade aan en kunnen in veel gevallen onschadelijk gemaakt worden. Eenmaal bekend kan *malware* automatisch gedetecteerd en geweerd worden, mits leveranciers en gebruikers hun softwaresystemen tijdig updaten.

De opkomst van cyberaanvallen creëert daarom niet alleen serieuze veiligheidsrisico’s, maar ook mogelijkheden om de schade te verzachten.

Drie tredes op een escalatieladder

Elke dag zijn er cyberaanvallen. Dit rapport geeft een overzicht van wie ze uitvoert, waarbij we de rol van de grote cybermachten – de Verenigde Staten, Rusland en China – benadrukken, en ook Nederland en een aantal andere Europese landen bespreken. Dit doen we door de activiteiten te markeren op een zogenoemde cyberescalatieladder, die drie tredes telt:

1. Een trede gekenmerkt door **cybervrede**, waarin landen niet met digitale middelen spioneren en ook geen sabotage uitvoeren of desinformatie verspreiden.
2. Een trede gekenmerkt door **informatieconflict**, waarin staten overgaan tot cyberspionage en, in sommige gevallen, het verspreiden van desinformatie en het saboteren van digitale systemen.
3. Een trede gekenmerkt door **cyber-fysieke oorlog**, waarbij de schade die staten aanrichten zo ernstig is dat er sprake is van gewapende aanvallen. Tijdens een cyber-fysieke oorlog vallen alle soorten cyberaanvallen overigens onder het internationaal recht, en niet alleen de weinige cyberaanvallen die op zichzelf een gewapende aanval constitueren.

De meeste huidige handelingen van invloedrijke staten passen in wat we hierboven beschrijven als het informatieconflict. Landen zijn in vredestijd hun cybersecurity aan het opbouwen en ze proberen zo onzichtbaar mogelijk te infiltreren in de digitale systemen van andere landen. Rusland kenmerkt zich daarnaast door het actief verspreiden van desinformatie. Dat is een strategie die andere autocratische landen, tenminste naar het buitenland toe, nog niet breed lijken toe te passen, maar die wel naadloos aansluit bij de ambitie om de informatie die burgers bereikt te sturen, te censureren en te manipuleren. Daarnaast zijn er enkele voorbeelden van ernstige cybersabotage, zoals de operatie Olympic Games, die aan Israël en de Verenigde Staten wordt toegeschreven, en de WannaCry-aanval, die aan Noord-Korea wordt toegeschreven. Cyberaanvallen hebben tot nu toe nog nooit een cyber-fysieke oorlog uitgelokt; van ‘cyberoorlog’ is wat dat betreft geen sprake. Wel vormt cyber steeds meer een onderdeel van oorlogsvoering, zoals goed te zien is bij het conflict in Oekraïne.

Internationale samenwerking

Het voortdurende informatieconflict vraagt om internationale diplomatie en afspraken. Daarom brengen we in dit rapport ook de samenwerking op dit vlak in kaart. In internationale en regionale gremia proberen staten stappen te zetten om een veilige en vrije digitale wereld te realiseren.

Staten zijn er niet in geslaagd om voor cyberaanvallen heldere afspraken met elkaar te maken. Dit betekent niet dat er geen regels van toepassing zijn op cyberaanvallen. Maar omdat deze aanvallen zelden de drempel overschrijden van

een ‘gewapende aanval’, en daarmee het internationaal humanitair recht activeren, zijn er alleen algemene normen beschikbaar, zoals het geweldsverbod. En die kunnen vooralsnog op allerlei manieren worden uitgelegd. Er wordt gewerkt aan nieuwe afspraken, maar deze zijn er nog niet.

Vijf oplossingsrichtingen voor de-escalatie
Het informatieconflict kan escaleren. De huidige internationale situatie is riskant en zorgwekkend, zo laat ons rapport zien. Op basis van onze bevindingen formuleren we vijf oplossingsrichtingen die kunnen bijdragen aan de-escalatie van dit conflict.

1. **Blijf samenwerken om de internationale cybersecurity te verhogen**
   Internationaal zijn er belangrijke initiatieven ontplooid om de veiligheid van cyberspace te verbeteren, zoals de IMPACT-coalitie, het Europese netwerk van Cyber Emergency Incident Response Teams en de NAVO-cyberoefeningen. Nederland heeft zich hierbij aangesloten. Deze samenwerkingen blijven van groot belang.

2. **Maak heldere internationale afspraken voor de-escalatie op het gebied van cybersabotage, desinformatie en cyberspionage**
   Hoewel Nederland en andere landen belangrijke stappen hebben gezet om internationale regels voor cyberaanvallen te formuleren, zoals het Tallinn Handboek en de Paris Call for Trust and Security in Cyberspace, zijn de regels algemeen. Het is belangrijk concretere afspraken te maken, ook over het informatieconflict. Daarbij kan gedacht worden aan een cyberverdrag.

3. **Zorg dat het cyberarsenaal verantwoord wordt beheerd**
   Het is belangrijk verdere verspreiding (proliferatie) van cyberwapens tegen te gaan. Dit vraagt om een internationale coördinatie van de aanschaf van cyberwapens, en om een effectieve samenwerking met technologie-bedrijven die kwetsbaarheden in hun producten kunnen verhelpen. Deze samenwerking vraagt ook, zeker onder bondgenoten, om zo veel mogelijk openheid.

4. **Bescherm de onafhankelijkheid van technologiebedrijven**
   Technologiebedrijven vervullen een cruciale rol in de beveiliging van de digitale omgeving. Zij dichten de gaten in hun software en kunnen robuuste digitale toepassingen op de markt brengen. Het is belangrijk om bedrijven te ondersteunen om zo veilig mogelijk te opereren. Overheden nemen een risico als ze van bedrijven eisen de veiligheid van producten heimelijk te verzwakken. Overheden moeten zowel de technologie als de technologie-bedrijven dus verstandig reguleren.

5. Investeer in debat over internationale cyberveiligheid

Het informatieconflict is bij uitstek een onderwerp voor democratisch debat: juist burgers worden geraakt door cyberaanvallen. Ze moeten weerbaar zijn. Ook is het aan hen om richting te geven aan de digitale toekomst. De-escalatie van het informatieconflict vraagt daarom om een maatschappelijk en politiek debat.

Inhoud

Inleiding

1.1 De opkomst van cyberaanvallen

Stel je voor dat op maandagochtend alle medewerkers van de Belastingdienst de volgende woorden met chocoladeletters op hun scherm zien staan:

‘YOUR COMPUTER HAS BEEN HACKED BY THE MOTHERLAND WARRIORS’

Hun computers zijn gehackt, en de hackers blijken toegang te hebben tot allerlei gevoelige belastinggegevens. Niet alleen de Belastingdienst is geraakt: vele maatschappelijke sectoren zijn getroffen door de ‘Motherland Warriors’. Banksites zuchten onder zware cyberaanvallen die hun dienstverlening stilleggen. Ook telecombedrijven zijn geïnfiltreerd. De Nederlandse Aardolie Maatschappij kan niet bij haar leveringsgegevens. Tot overmaat van ramp wordt de online omgeving van ziekenhuizen gegijzeld. Overal klinkt hetzelfde dreigement: als de economische sancties op Rusland niet onmiddellijk worden opgeheven, zal essentiële informatie van de computersystemen gewist worden, en privéinformatie openbaar worden gemaakt. Hoewel niets met zekerheid kan worden bewezen, zijn er sterke aanwijzingen dat de aanvallen vanuit Rusland worden gelanceerd.

Dit scenario is niet denkbeeldig. Het is actueler dan ooit. De technologie bestaat namelijk om alle aanvallen uit het voorbeeld uit te voeren. Sterker: dit soort aanvallen hebben allemaal al eens plaatsgevonden:

- In 2012 haalde een van de grootste oliebedrijven ter wereld, Saudi Aramco, vijf maanden lang alle dienstverlening offline omdat het werd aangevallen door een groep die zichzelf ‘Cutting Sword of Justice’ noemde. Deze aanval werd aan Iran toegeschreven (Iasiello 2015, Sanger 2018).
- Van 2011 tot 2013 werd het Belgische telecombedrijf Belgacom (nu: Proximus) gehackt (Boffey 2018). Hackers zouden toegang hebben verkregen tot communicatie binnen de NAVO, de Europese Raad, de Europese Commissie en het Europees Parlement. De Belgische openbaar aanklager heeft de Britse inlichtingendienst GCHQ aangewezen als dader.
- In 2015 werd bij een hack van de federale belastingdienst van de Verenigde Staten, de Internal Revenue Service, de gegevens gestolen van meer dan 700.000 burgers (Crawford 2016). Het is niet bekend wie de daders waren.
- In de zomer van 2017 gingen ziekenhuizen in heel Europa, en met name in het Verenigd Koninkrijk, gebukt onder de Wannacry-*malware*, die kostbare

gegevens gijzelde (Ehrenfeld 2017). De aanval werd toegeschreven aan Noord-Korea (Sanger 2018).
- En begin 2018 hadden de netwerken van de banken ING en ABN Amro last van een venijnige Distributed Denial of Service-aanval (DDoS), waarschijnlijk gepleegd door Jelle S., een 18-jarige jongen (Modderkolk 2018).

1.2 Een complexe en dreigende internationale situatie

Landen (ook wel: 'statelijke actoren') hebben steeds meer mogelijkheden om via cyberspace te saboteren, te spioneren en te manipuleren. Zo hebben de Verenigde Staten in het verleden grote cyberaanvallen uitgevoerd, en lijken ze hun aanzienlijke verzameling digitale wapens steeds actiever te willen gebruiken (Sanger 2018, United States Cybercommand 2018b). China hackt en bespioneert buitenlandse bedrijven om economisch en militair lucratieve geheimen te stelen (Klimburg 2017). En Rusland heeft grootschalige cyberaanvallen gepleegd in Oekraïne, en probeert Amerikaanse energiecentrales te infiltreren (Sanger 2018, Klimburg 2017).

Dit heeft geleid tot een complexe, onvoorspelbare en dreigende internationale situatie. Inmiddels hebben alle wereldmachten militaire cybercommando's opgericht en hun inlichtingendiensten hervormd. In sommige staten bestaan er nauwe banden tussen overheidsonderdelen en patriottistische of – zoals in Rusland – criminele hackers (Klimburg 2017). Landen opereren hierbij vaak onder de radar, en kunnen cyberaanvallen zo verhullen dat het soms moeilijk is om vast te stellen welke 'cyberactor' verantwoordelijk is voor welke cyberaanval.

Staten grijpen niet langer alleen te land, ter zee, in de lucht en in de ruimte in. De digitale ruimte – cyberspace – wordt de vijfde dimensie genoemd, waar staten, bewapend met virussen, gijzelsoftware en geheime kwetsbaarheden, hun belangen behartigen (NAVO 2016b, The Economist 2010). Nederland zal in deze nieuwe wereld zijn belangen, zoals veiligheid, welvaart en het beschermen van de democratische rechtsstaat, moeten waarborgen.[1]

Daartoe zijn al verschillende stappen gezet. Zo heeft ook Nederland een militair cybercommando, gericht op het verzamelen van inlichtingen, de verdediging van eigen netwerken en het uitvoeren van cyberaanvallen. Bovendien kunnen de militaire inlichtingendienst MIVD en de algemene inlichtingendienst AIVD cyberoperaties uitvoeren. Verder streven de Nederlandse overheidsdiensten, maar ook bedrijven, maatschappelijke organisaties en burgers, er al jaren naar de

1 De literatuur en beleidsdocumenten spreken in deze context ook van Vitale Belangen. Zie Ducheine 2018.

cyberveiligheid op orde te krijgen. Het moet lastig zijn om Nederlandse instellingen en bedrijven aan te vallen, en het moet gemakkelijk gemaakt worden om schade te herstellen. In het rapport *Een nooit gelopen race* gaat het Rathenau Instituut uitgebreid in op dit vraagstuk (Munnichs et al. 2017). Ook heeft het Rathenau Instituut onderzoek gepubliceerd over de digitalisering van het nieuws, en aangegeven hoe de Nederlandse overheid de samenleving weerbaar kan maken tegen de verspreiding van desinformatie (Van Keulen et al. 2018).

Maar hoe stelt Nederland zich in de internationale arena op als het waarschijnlijk is dat een andere staat achter een cyberaanval zit? Is het dan zaak om, samen met bondgenoten, terug te slaan met gelijke munt, bijvoorbeeld door de Russische belastingdienst aan te vallen? Kwalificeren we dit dan als een 'oorlogsdaad' (AIV CAVV 2011)? Of is het verstandig om andere, diplomatiekere middelen in te zetten? Terwijl er steeds meer expertise en beleid ontstaat op het gebied van cybersecurity, is dat minder het geval op het gebied van het internationaal inzetten van cybercapaciteiten (Van der Meer 2018b).

Hoe kan Nederland er aan bijdragen dat landen cybercapaciteiten op de juiste manier ontwikkelen, reguleren en inzetten? De doelstelling van dit rapport is die vraag te verhelderen. Daarvoor kijken we zowel naar de achtergrond van offensieve cybercapaciteiten als naar de internationale omgeving waarbinnen deze capaciteiten worden verworven en gebruikt. Daarbij bekijken we welke juridische regels, gegeven de eigenschappen van cyberaanvallen, op dit moment van toepassing zijn op offensieve cybercapaciteiten. Hierbij kijken we ook naar het internationaal humanitair recht of humanitair oorlogsrecht (soms ook oorlogsrecht genoemd). Dat recht bepaalt welk gedrag van strijdende partijen in oorlogssituaties toelaatbaar is of niet. Het rapport sluit hier aan bij de ambitie van Nederland en andere Europese landen, zoals het Verenigd Koninkrijk en Duitsland, om cybercapaciteiten in te bedden in heldere internationale regelkaders (UK Government 2016, German Federal Ministry of the Interior 2011, Ministerie van Buitenlandse Zaken 2017).

De omgang met cybercapaciteiten is van groot maatschappelijk belang. De Nederlandse reactie op schadelijke en ondermijnende buitenlandse cyberaanvallen kan daarom niet uitsluitend een zaak van experts zijn: het is belangrijk dat ook burgers zich erover uitspreken. Te meer omdat we zullen zien dat juist zij zo vaak het slachtoffer zijn van cyberaanvallen: ze worden misleid of gechanteerd, hun computers worden gehackt en vitale maatschappelijke voorzieningen worden aangetast. Het Rathenau Instituut heeft als taak de politieke besluitvorming en het publieke debat over de impact van technologie op de samenleving te ondersteunen. Dat is ook nodig op het gebied van offensieve cybercapaciteiten. Met dit rapport hopen we eraan bij te dragen dat niet alleen experts en bestuurders, maar ook

burgers kennis kunnen nemen van de onzekere en dreigende situatie die hen omgeeft.

1.3 De cyberescalatieladder

In dit rapport introduceren we een onderscheid tussen **cybervrede**, **informatieconflict** en **cyber-fysieke oorlogsvoering.** Dit is het centrale denkkader waarmee we offensieve cybercapaciteiten zullen analyseren, en dat we toevoegen aan het vocabulaire waarmee over cyberaanvallen wordt gesproken.

- **Cybervrede** verwijst naar een toestand waarin een staat andere staten niet aanvalt met offensieve cybercapaciteiten.
- **Informatieconflict** slaat op een fase waarin een staat cyberaanvallen lanceert in en tegen een ander land. Deze fase kan saboterende aanvallen kennen, maar ook spionage- en desinformatieaanvallen.
- Ten slotte treedt een staat een fase van **cyber-fysieke oorlogsvoering** binnen, als de staat een zodanig zware cyberaanval uitvoert dat de juridische drempel van een gewapende aanval wordt overschreden, en het land in een staat van oorlog verkeert met het aangevallen land.

Deze drie fases vormen samen een **cyberescalatieladder** (zie figuur 1), beginnend bij cybervrede en eindigend bij cyber-fysieke oorlogsvoering. In dit rapport zullen we concluderen dat vrijwel alle staten met één of meerdere landen in een informatieconflict verkeren – en dat juist op het gebied van dat informatieconflict voldoende duidelijke en breed nageleefde regelkaders ontbreken.

Er zijn daarom verstandige internationale normen nodig, die bijdragen aan de de-escalatie van het informatieconflict. Bij het formuleren van nieuwe normen is het van belang om burgers en hun civiele voorzieningen in bescherming te nemen, en deze zoveel mogelijk vrij te waren van aanvallen die zijn rechten ondermijnen, zoals zijn recht op privacy, op veiligheid, en zijn rol als democratische burger.

1.4 Afbakening

Dit rapport beschrijft de capaciteiten van statelijke of door staten gesponsorde actoren om cyberaanvallen uit te voeren door middel van **cybersabotage**, **cyberspionage** en de verspreiding van **desinformatie**.[2] Deze categorieën zijn gekozen op basis van de literatuur en beleidsstukken (zie bijvoorbeeld AIVD 2019). Cybercriminaliteit valt dus buiten het bereik van deze studie, tenzij staten welbewust van cybercriminaliteit gebruik maken om hun belangen te dienen.

- **Cyberspionage** is het verwerven van inlichtingen door gebruik te maken van digitale technologie.
- **Cybersabotage** is het bewust schade aanbrengen aan personen, objecten of dataverzamelingen door gebruik te maken van digitale technologie.
- **Desinformatie** doelt op het verspreiden van onware, inaccurate of misleidende informatie die bewust wordt gecreëerd en verspreid omwille van economisch profijt of om een persoon, sociale groep, organisatie of land te schaden (Van Keulen et al. 2018, 14).

Deze drie middelen kunnen de samenleving in uiteenlopende mate schade berokkenen, en zullen daarom in dit rapport omschreven worden als **cyberwapens**. Ze kunnen gecombineerd worden om bepaalde strategische effecten te sorteren. In verkiezingstijd bijvoorbeeld kan een kwaadwillende partij de website van een politieke organisatie platleggen (cybersabotage), gevoelige geheimen stelen (cyberspionage) en onware berichten verspreiden (desinformatie). De totale verzameling van cyberwapens die een actor beheert noemen we zijn **cyberarsenaal**.

Het vermogen om deze cyberaanvallen in te zetten noemen we in dit onderzoek **offensieve cybercapaciteit**.[3] Hieronder verstaan we niet alleen de toegang tot de technologie, maar bijvoorbeeld ook het bezitten van kundige hackers die aanvallen kunnen uitvoeren, en strategisch beleid die deze capaciteit aanstuurt. Een **cyberoperatie** is een verzameling handelingen van bijvoorbeeld een inlichtingendienst waarbij gebruik gemaakt wordt van digitale technologie, zoals een cyberspionageoperatie.

Er bestaat ook wapentuig dat conventionele militaire technologie combineert met digitale technologie, zoals een bewapende drone of een digitaal aangestuurde raketinstallatie. Het Rathenau Instituut publiceerde al eerder over militaire robots (Royakkers & Van Est 2016). Op dit soort technologie richten we ons niet. In dit rapport ligt de nadruk op de schade die de ene staat aan de andere staat kan

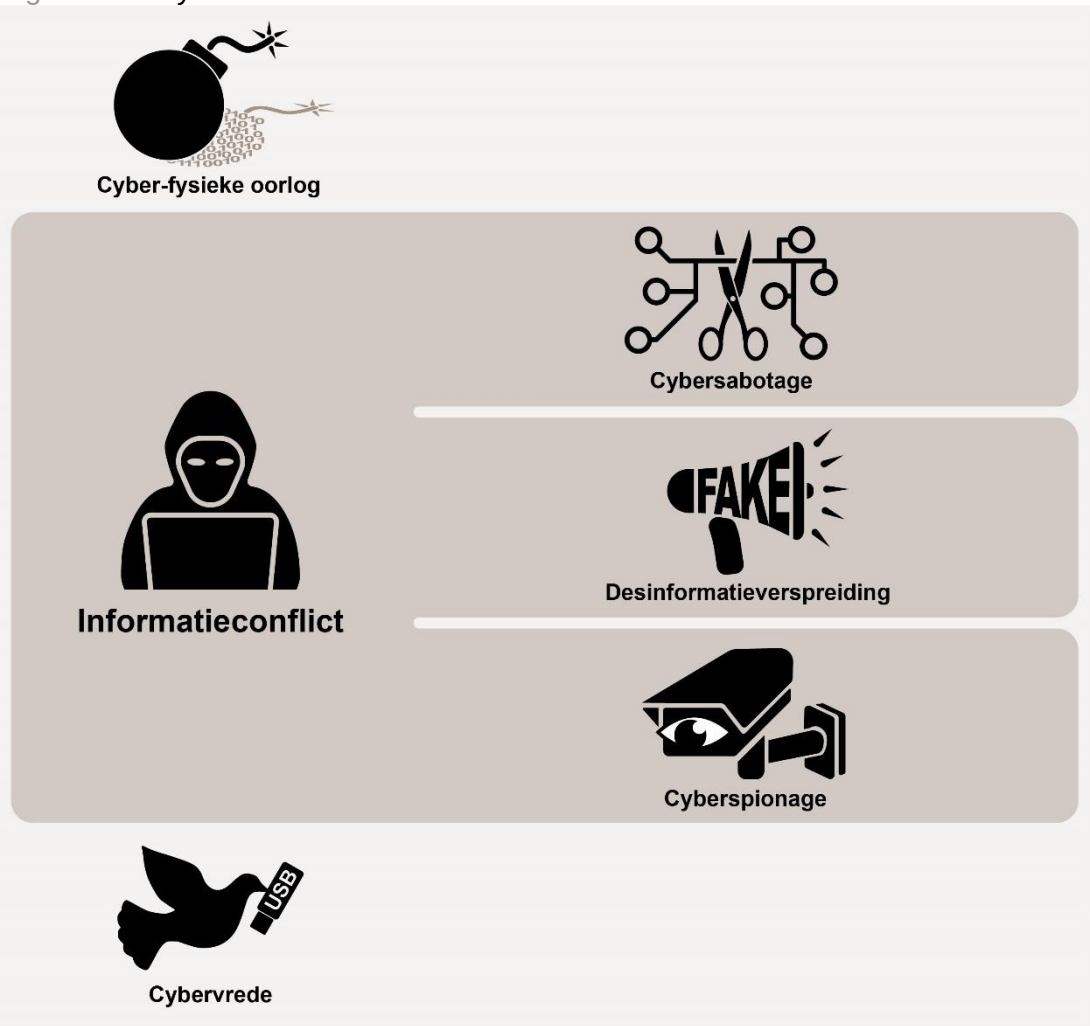
2 De term ‘aanval’ verwijst hier niet uitsluitend naar aanvallen in een militair conflict, maar wordt breder bedoeld.
3 Ook over deze terminologie wordt verschillend gedacht. Zie bijvoorbeeld Ducheine en Van Haaster 2014.

berokkenen door middel van computercode of met gebruik van digitale apparaten zoals geïnfecteerde usb-sticks of wifi-routers.

Verder richt het rapport zich expliciet op de internationale context. We bespreken de nationale ontwikkelingen voor zover ze relevant zijn voor de Nederlandse oriëntatie. Ook bouwt dit rapport voort op de analyse van het nationale cybersecuritybeleid die we eerder maakten in het rapport *Een nooit gelopen race* (Munnichs et al. 2017).

In figuur 1 is de cyberescalatieladder, inclusief de verschillende cyberaanvallen, grafisch vormgegeven.

Figuur 1 De cyberescalatieladder



1.5 De onderzoeksvragen

Door de opkomst van offensieve cybercapaciteiten is de internationale omgeving van Nederland veranderd. De centrale onderzoeksvraag van dit rapport luidt daarom:

Hoe kan Nederland, gezien de opkomst van offensieve cybercapaciteiten, bijdragen aan het de-escaleren van het informatieconflict?

Om deze vraag te beantwoorden schetsen we in dit rapport de internationale omstandigheden op het gebied van offensieve cybercapaciteiten. Dit doen we in drie stappen.

Allereerst verhelderen we in het rapport de aard van offensieve cybercapaciteiten: **Wat zijn offensieve cybercapaciteiten?** Bij het beantwoorden van deze vraag wordt onder meer gekeken naar verschillende aspecten van cyberoperaties en wat deze betekenen voor de verhouding tussen aanvallers en verdedigers. Ook wordt de vergelijking gemaakt met conventionele spionage, propagandaverspreiding en oorlogscapaciteiten.

Vervolgens brengen we de capaciteitsopbouw van enkele wereldspelers in kaart: **Welke offensieve cybercapaciteiten ontwikkelen de Verenigde Staten, Rusland, China, Nederland en Europese landen?**

Ten slotte inventariseren we de manieren waarop landen met elkaar en met maatschappelijke partners internationaal samenwerken aan maatregelen die offensieve cybercapaciteiten reguleren en die kunnen bijdragen aan een duurzame cybervrede: **Hoe werkt de internationale gemeenschap samen om een veilige en vrije digitale wereld te borgen?**

Op basis van de verheldering van de internationale omstandigheden beantwoorden we de hoofdvraag.

1.6 De onderzoeksmethode

Dit onderzoek bestaat hoofdzakelijk uit desk research, ondersteund door oriënterende interviews en expertconsultaties.

Desk research en expertconsultatie
Een combinatie van overheidsdocumentatie, journalistieke en academische literatuur geeft het meeste inzicht om de opkomst en inzet van offensieve

cybercapaciteiten vanuit een internationaal perspectief te onderzoeken. De overheidsdocumentatie geeft weer wat staten en intergouvernementele organisaties zelf mededelen over hun offensieve cybercapaciteiten. Zo publiceert het Amerikaanse ministerie van Defensie regelmatig strategische visies en rapporteren organen van de Verenigde Naties overlegresultaten aan de Algemene Vergadering.

Maar deze documenten alleen geven geen volledig beeld. Veel cyberoperaties vinden plaats in het geheim, en defensieorganisaties en inlichtingendiensten houden details over hun cyberarsenaal doorgaans buiten de pers. Dat betekent dat, om een beter beeld te kunnen krijgen van de internationale ontwikkelingen, het bijhouden van onderzoeksjournalistiek, tech-blogs en de publicaties van cybersecuritybedrijven essentieel is – deze bronnen brengen de details van cyberoperaties vaak naar buiten.

Ten slotte is het belangrijk om academische publicaties te lezen en is het van belang om goed op de hoogte te zijn van de relevante ontwikkelingen in het internationaal recht. Voorafgaand aan het onderzoek hebben we daarom interviews afgenomen. De resultaten zijn voorgelegd aan een aantal experts uit het veld: Paul Ducheine van de Faculteit Militaire Wetenschappen; Sico van der Meer van het Instituut Clingendael; Frank Slijper van PAX en Dimitri Tokmetzis van De Correspondent. Ook spraken we Pim Takkenberg van Northwave. We willen hen daarvoor hartelijk danken.

2 Offensieve cybercapaciteiten

Kader 1 Drie voorbeelden van cyberspionage

Rond 2003 constateerde het Amerikaanse ministerie van Defensie dat er steeds meer aanvallen werden gepleegd op hun netwerken. Deze aanvallen gingen jarenlang door, en werden gezamenlijk 'Titan Rain' genoemd (Adkins 2013, Bowcott 2008). Sommige aanvallen zouden de netwerken hebben gepenetreerd, maar het is onduidelijk wat voor spionage- en sabotageactiviteiten hebben plaatsgevonden. De Verenigde Staten en het Verenigd Koninkrijk beschuldigden Chinese hackersgroepen (Bowcott 2008).

In 2013 onthulde Edward Snowden de uitvoerige spionageoperaties van het Amerikaanse veiligheidsagentschap NSA (Sanger 2018, Ball et al. 2013). Dat zou in samenwerking met de Britse GCHQ beveiligd verkeer op onder andere Facebook en Gmail inzien, de communicatie van Europese bondgenoten afluisteren en samenwerken met IT-producenten om kwetsbaarheden aan hun producten toe te voegen.

In april 2016 werd het netwerk van het Democratische Nationale Comité gehackt. Dit comité bestuurt de Amerikaanse Democratische Partij. Chatgesprekken werden in de gaten gehouden en e-mails werden gemonitord en gehackt. Later wijzen onder meer de NSA, en de overheidsdiensten FBI en CIA (zie kader 4) de Russische overheid aan als schuldige (DHS, ODNI, FBI 2016). Speciaal aanklager Mueller klaagt op 13 juli 2018 twaalf Russische inlichtingenofficieren aan voor, onder andere, deze hack (Ward 2018).

In dit hoofdstuk bespreken we de drie verschillende offensieve cybercapaciteiten die in hoofdstuk 1 zijn geïntroduceerd: cyberspionage, cybersabotage en de verspreiding van desinformatie. We geven een beknopt technisch overzicht van deze capaciteiten, vergelijken ze met conventionele militaire middelen en bekijken de manieren waarop de samenleving zich tegen de offensieve cybercapaciteiten kan weren. Ook geven we telkens in kaders enkele voorbeelden van cyberaanvallen.

2.1 Cyberspionage

2.1.1 Technologie

We definiëren cyberspionage als het verwerven van inlichtingen door gebruik te maken van digitale technologie. Deze inlichtingenverzameling richt zich grofweg op twee doelen: staatsgeheimen en economische geheimen. Beide vormen van spionage komen in het digitale domein op grote schaal voor (AIVD, MIVD 2017). Het kan voor een staat, en voor de bedrijven verbonden met die staat, interessant zijn om intellectueel eigendom te stelen, zoals een nieuw ontwerp voor een elektrische auto. Net zo goed kan het defensieapparaat van een staat beslag willen leggen op staatsgeheime plannen voor een nieuwe straaljager. Zie kader 1 voor een aantal voorbeelden van cyberspionage.

De meeste cyberaanvallen bestaan grofweg uit twee fasen: binnendringen en een actie ondernemen (AIVD, MIVD 2017, Ducheine & Van Haaster 2014, Andress & Winterfeld 2011, Janczewski & Colarik 2007).[4] Eenmaal binnengedrongen zijn er twee acties mogelijk: het uitvoeren van cyberspionage of het uitvoeren van cybersabotage. Cyberspionage lijkt op een verkenningsvliegtuig: het vliegtuig moet eerst het vijandelijk territorium binnendringen, en vervolgens wordt informatie ingewonnen. Cybersabotage (zie paragraaf 2.2) is te vergelijken met een bommenwerper: het vliegtuig moet wederom eerst het vijandelijk territorium binnendringen, en levert vervolgens een schadelijke lading af (Herr & Rozenzweig 2013). Cybersabotage en cyberspionage vereisen dus voor een deel dezelfde handelingen, maar hebben een ander doel.

Cyberspionage wordt ingezet bij het binnendringen van informatiesystemen waartoe een actor geen reguliere toegang heeft. Hierbij kunnen we onderscheid maken tussen het wel en niet inzetten van software. Organisaties kunnen namelijk ook door oplichterij ofwel *social engineering* geïnfiltreerd worden: een persoon kan zich bijvoorbeeld voordoen als klant en op een onbewaakt moment achter de computer van een verkoper kruipen, of in een telefoongesprek de inloggegevens van een goedgelovig persoon aftroggelen. Om deze reden hoort bij cyberveiligheid ook fysieke veiligheid, en is het van groot belang te controleren wie toegang heeft tot computers en welke informatie gedeeld mag worden buiten de organisatie.

4 Alle genoemde auteurs stellen complexere structuren voor, die op verschillende kleine aspecten van elkaar verschillen. Zo vragen de AIVD en MIVD meer aandacht voor het behouden van toegang tot een digitaal systeem. Het onderscheid dat wij voorstellen biedt een handzame vereenvoudiging van deze discussie.

Cyberspionage via phishing, spearphishing en spoofing
Een van de meest voorkomende manieren om digitaal en op afstand in een informatiesysteem in te breken is *phishing*. Hierbij stuurt men mails naar mensen die personen verleiden op een bepaalde link te drukken of om iemand op te bellen en hun inloggegevens te verstrekken. Soms wordt een bepaalde mail naar een grote hoeveelheid mailadressen gestuurd – de zogenoemde spam-mail. En soms wordt een mail of een site waarnaar wordt doorverwezen precies op maat gemaakt om een bepaalde persoon te verleiden – dit wordt *spearphishing* genoemd. Een verwante strategie is *spoofing*; daarbij lijkt het alsof een mail is verstuurd door een bekende en vertrouwde persoon of organisatie, zoals iemands baas – terwijl dat niet zo is.

Deze strategieën komen veel voor bij bankfraude. Iemand ontvangt bijvoorbeeld een nepmail van de directeur van de bank waarin staat dat er een transactiefout is gevonden en dat klanten moeten inloggen bij de bank. Wie op de link klikt, bereikt vervolgens een nepversie van de banksite, waar gegevens ingevoerd worden (Politie 2018). Wanneer de klant dat doet, kan de crimineel vervolgens geld stelen en overmaken naar een derde rekening.

Of het nu gaat over *phishing*, *spearphishing* of *spoofing*, het zijn allemaal pogingen om een persoon ertoe te brengen iets te doen. Als iemand niet op bepaalde links klikt en geen gegevens invoert, komt de inbreker het informatiesysteem van de betreffende persoon niet binnen. Bovendien zijn deze strategieën duidelijk waar te nemen – met zijn mail of zijn belletje heeft de inbreker zich aan zijn slachtoffer gepresenteerd.

Cyberspionage via zero days exploits
De technologie om op de meest onopvallende manier ergens binnen te dringen, maakt gebruik van zogeheten *zero days exploits*. Dit zijn nog niet bekende kwetsbaarheden in de broncode van software van bijvoorbeeld Windows, Android of een wifi-installatie (Bilge & Dumitras 2012).

De term *zero day* slaat op het feit dat de softwarefabrikant niet weet van de kwetsbaarheid en nog geen enkele dag (nul dagen) de gelegenheid heeft gehad om de kwetsbaarheid in zijn programmacode te repareren. Vanaf het ontdekken van de fout geldt de kwetsbaarheid dus technisch gezien niet langer als een *zero day*. Toch blijven bekende kwetsbaarheden veel langer bruikbaar, omdat het even kan duren voordat een producent door middel van een stukje software (*patch*) een kwetsbaarheid heeft verholpen, en ook omdat oudere systemen soms slecht of zelfs niet actueel worden gehouden. Bovendien krijgen bij bekendmaking ook andere kwaadwillende partijen kennis van een kwetsbaarheid. Sommige auteurs beweren daarom dat na bekendmaking het misbruik van *zero days* toeneemt,

omdat meer actoren aanvallen kunnen plegen op systemen die niet voldoende geactualiseerd zijn (Bilge & Dumitras 2012).

Zero days zijn uitermate geschikt voor spionagedoeleinden: als het slachtoffer niet weet van de *zero day*, dan glipt de spion ongezien een systeem binnen, en kan hij misschien wel maandenlang – of jarenlang – relevante activiteiten in de gaten houden.

Cyberspionage via hardware
Ten slotte kan iemand ook via hardware een systeem binnendringen: bijvoorbeeld door een geïnfecteerde usb-stick in een apparaat te steken, of door al bij het produceren van een computer of een router een spionageonderdeel in te bouwen.

Vaak gaat het om een combinatie van verschillende technologieën
Samengevat zijn er dus vele manieren om een systeem binnen te dringen, die in combinatie kunnen worden ingezet. Bij de infiltratie van de uraniumverrijkingsinstallatie in de Iraanse plaats Natanz werd bijvoorbeeld een virus een afgesloten netwerk binnengesmokkeld door een persoon met een geïnfecteerde usb-stick met daarop enkele *zero days* (Zetter 2011). Ook kan eerst een relatief goedkope *phishing*-aanval uitgeprobeerd worden, voordat duurdere *zero days* worden overwogen.

Bovendien zijn spionageoperaties vaak getrapt. Eerst dringt iemand bijvoorbeeld een zwak beveiligde gebruikersaccount binnen, van een persoon die binnen het informatiesysteem weinig bevoegdheden en rechten heeft – en voor wie dus lang niet alle informatie en functies toegankelijk zijn. Vervolgens probeert de inbreker via deze eerste account meer rechten te verkrijgen, bijvoorbeeld door in te breken op de account van een systeembeheerder of administrator. Zo probeert de inbreker stap voor stap het informatiesysteem bloot te leggen, en gebruikt hij verschillende strategieën om zijn einddoel te bereiken.

2.1.2 Vergelijking met conventionele spionage

Digitale spionage is ten opzichte van conventionele spionage om allerlei redenen aantrekkelijk. Met een klik op de knop kunnen enorme bestanden ineens van de ene naar de andere kant van de wereld verplaatst worden, in plaats van dat heimelijk met allerlei dossiers gesjouwd moet worden. Bovendien kan een cyberspion vanachter zijn computer in korte tijd in verschillende landen proberen in te breken.

Digitale spionage is dus veel efficiënter. Als de digitale spion zijn werk goed doet, kan het jaren duren voordat een bepaalde overheidsdienst doorheeft dat het in de gaten is gehouden, of dat er documenten zijn ingezien. Dit is ook wat inlichtingendiensten nastreven: een structurele en verborgen toegang tot de geheimen van de tegenstander (zie bijvoorbeeld U.S. Department of Defense 2018, U.S. Cybercommand 2018b). Om die toegang te vergemakkelijken kunnen cyberspionnen, eenmaal in het systeem, ook achterdeurtjes in de beveiligingsmuur inbouwen (AIVD, MIVD 2017). Op dit punt wordt cyberspionage duidelijk schadelijk, aangezien de veiligheid van het gehele systeem door middel van achterdeurtjes wordt verzwakt.

Maar het grootste verschil tussen digitale en conventionele spionage ligt in de relatieve veiligheid van cyberspionage voor spionnen. We kennen allemaal de spannende verhalen over spionnen die altijd bang zijn ontdekt te worden en enorme risico's lopen. Zo bang hoeven cyberspionnen niet te zijn. Hoewel voor sommige vormen van cyberspionage een organisatie ook fysiek geïnfiltreerd moet worden, kan elke met het internet verbonden computer op grote afstand gehackt worden. Dit maakt rondneuzen een heel stuk minder riskant voor de cyberspion – de kans op vervolging is klein als de spionage plaatsvindt onder de bescherming en vanuit het territorium van een andere staat. Daarbij is het soms moeilijk aan te wijzen wie een cyberaanval heeft gepleegd. Dit wordt het attributieprobleem genoemd. Aanvallers kunnen bijvoorbeeld een andere computer, of zelfs een serie van computers hacken, en hun aanvallen vanuit die computers lanceren. Zo kan een spoor ontstaan dat door verschillende staten loopt, en dat soms alleen met medewerking van al die staten gevolgd kan worden.

Dit gebrek aan risico's heeft ongetwijfeld te maken met de schaal van cyberspionage. In veel staten wordt met regelmaat geprobeerd belangrijke overheidssystemen binnen te dringen (AIVD, MIVD 2017). Het karakter van cyberspionage kan daarom tegelijkertijd heimelijk en brutaal zijn: bedrijven en overheden weten niet precies wie ze aanvalt, maar kunnen, zeker bij minder verfijnde aanvallen, wel doorhebben dat er vele spionagepogingen worden ondernomen. Cyberspionage is daarom veelal zichtbaarder dan het traditionele schaduwspel tussen geheime diensten en spionnen.

2.1.3 Weerbaarheid

Overheden, bedrijven, maatschappelijke organisaties en burgers proberen spionagepogingen natuurlijk te stoppen. Maar dat is moeilijk. Een infiltrant heeft meestal slechts een enkele fout of zwakke plek nodig om te infiltreren, terwijl een

aangevallen organisatie tegelijkertijd heel veel goed moet doen (Farwell & Rohozinski 2012).

Als bijvoorbeeld een gebruiker in een organisatie van honderden medewerkers in een onbezonnen moment op een link in een *phishing*-mail klikt, sluipt de *malware* het netwerk al binnen. Bovendien kan de aanvaller met behulp van een *zero day* allerlei beveiligingen, zoals *firewall*-software, omzeilen. Sommige experts stellen daarom dat alle digitale netwerken in principe te infiltreren zijn.

Toch zijn veiligheidsmaatregelen wel zinvol. Een versleutelde connectie waarvoor alleen een wachtwoord nodig is, is gemakkelijker te hacken dan versleuteling met twee-factorauthenticatie, die bijvoorbeeld ook een scan van een vingerafdruk omvat. Ook maakt het bouwen van beveiligingsmuren tussen delen van een digitaal systeem (segmentatie) infiltratiepogingen niet onmogelijk, maar wel veel moeilijker.[5]

Het is bovendien belangrijk om te wijzen op het verschil in verfijndheid en expertise tussen de ene en de andere cyberaanval. *Phishing*-mails kunnen overtuigend zijn gemaakt, of juist knullig en gemakkelijk te herkennen. En het is voor een cyberaanvaller gemakkelijker om een *phishing*-mail te sturen dan om *zero days* in handen te krijgen – die zijn zeldzaam en zeer waardevol. Zerodium, een informatieveiligheidsbedrijf dat kennis over kwetsbaarheden doorverkoopt aan bedrijven en overheden, betaalt bijvoorbeeld tot anderhalf miljoen dollar voor sommige kwetsbaarheden in het besturingssysteem van de iPhone (Zerodium 2018). Goede weerbaarheidsmaatregelen, zoals het maken van back-ups en het gebruiken van sterke wachtwoorden, beschermen wellicht niet tegen de meest geavanceerde aanvallen, maar zullen een groot deel van relatief simpele aanvallen wel afslaan.

Uiteindelijk kan de verhouding tussen cyberaanvallers en verdedigers het beste gekarakteriseerd worden als een race, waarin, tenminste op dit moment, de aanvallers in het voordeel lijken te zijn (Munnichs et al. 2017). Zij kunnen vaak zonder repercussies aanvallen uitvoeren, en ze hoeven slechts enkele zwakke plekken uit te buiten. Tegelijkertijd zijn er veiligheidssystemen, zoals het besturingssysteem van de iPhone, die zeer moeilijk gehackt kunnen worden. Maar de race heeft geen finish: betrouwbare veiligheidssystemen worden op den duur toch binnengedrongen, wat weer vraagt om nieuwe veiligheidsmaatregelen.

5 Deze en andere aanbevelingen om de cyberveiligheid te bevorderen zijn opgesomd en toegelicht in het rapport *Een nooit gelopen race* (Munnichs et al. 2017).

2.2 Cybersabotage

Kader 2 Drie voorbeelden van cybersabotage

In 2007 lanceerden Russische patriottistische hackers een cyberaanval op buurland Estland. Er was een geschil tussen beide landen over de verplaatsing van een Russisch oorlogsmonument in de Estse hoofdstad Tallinn. Toen de Esten het monument verhuisden, reageerden de hackers met een verlammende cyberaanval op de websites van de Estse regering, de media en banken. Bijna een week lang konden deze instellingen geen zaken online doen, en konden burgers geen contact met hen opnemen (Karatzogianni 2008). Rusland ontkent betrokkenheid.

In 2010 werd een *malware*-aanval gepleegd op een uraniumverrijkingsinstallatie bij Natanz in Iran. De *malware*, genaamd Stuxnet, is tijdens de operatie ‘Olympic Games’ door de VS in samenwerking met Israël ontwikkeld en door beide staten gebruikt om het nucleaire programma van Iran te saboteren. Het nucleaire programma is door deze aanval maanden (en misschien zelfs meer dan een jaar) vertraagd (Gross 2011).

In 2015 viel twee dagen voor kerstmis op verschillende plaatsen in Oekraïne de stroom uit (E-ISAC SANS ICS 2016, Zetter 2016). Op het moment van de aanval was het nacht en vroor het bijna. Binnen een paar uur wisten de ingenieurs de stroom handmatig weer aan te zetten. Dit was de eerste cyberaanval waarbij een elektriciteitscentrale succesvol werd afgesloten. De aanval omvatte ook een DDoS-aanval die de klantenservice saboteerde. De Oekraïense geheime diensten stellen zonder twijfel dat de Russische overheid achter de aanval zat.

2.2.1 Technologie

Met een cyberaanval kan men ook proberen een digitaal systeem te saboteren en schade aan te richten. Er zijn allerlei sabotages mogelijk, aangezien veel

verschillende toepassingen digitaal verbonden zijn. In kader 2 hebben we een aantal ingrijpende voorvallen onder elkaar gezet.

Naast de voorbeelden van kader 2 kunnen we ons ook andere sabotages voorstellen:

- Iemand kan op afstand inbreken in een online verbonden zelfrijdende auto en deze laten verongelukken.
- Iemand kan het netwerk van een ziekenhuis binnendringen en, aan de hand van gijzelsoftware (*ransomware*), patiëntendossiers vergrendelen en losgeld eisen.
- Iemand kan toegang forceren tot een staatsgeheim AIVD-dossier en de inhoud ervan op openbare sites zetten.
- Iemand kan een wifi-gestuurde pacemaker binnendringen en uitzetten.

Bedenk hierbij dat cyberaanvallen dikwijls bestaan uit verschillende sabotage- en spionage-elementen. Zo werd tijdens de Stuxnet-operatie (zie kader 2) het systeem via een usb-stick geïnfecteerd, en stond op die usb-stick zelf saboterende code (Zetter 2011).

Een speciaal type cybersabotage zijn de DDoS-aanvallen. Die zijn namelijk niet afhankelijk van het binnendringen van een computersysteem. Een DDoS-aanval bestaat uit het versturen van serviceverzoeken naar een site of andere digitale dienst, om deze zo te overbelasten dat de dienst niet meer functioneert. Een grote groep computergebruikers kan dus gezamenlijk, zonder verder malware in te zetten, zo'n aanval in gang zetten. Klimburg schrijft in deze context over de vele computers van Chinese burgers die de Chinese staat kan gebruiken om een DDoS-aanval uit te voeren (Klimburg 2017). Vaak wordt echter een groot aantal computers gehackt, om via een zogenoemd *botnet* vanuit nog veel meer bronnen serviceverzoeken te versturen. In zo'n geval heeft een DDoS-aanval juist een uitgebreide fase van binnendringen. In deze context is het geautomatiseerd hacken van digitale apparaten een groot probleem. Door slimme software kan een hacker op hoog tempo duizenden bots verzamelen en met relatief weinig moeite een enorme aanval op poten zetten. DDoS-aanvallen zijn onverminderd populair, en er ontstaan meer geavanceerde en moeilijker te detecteren varianten.

2.2.2 Vergelijking met conventionele wapens

Cybersabotage verschilt op interessante wijze van conventioneel wapentuig. Het meest in het oog springende onderscheid betreft het schadepotentieel. Bommenwerpers, granaten, tanks en raketinstallaties kunnen mensen doden en in veel gevallen fysieke objecten, van bruggen tot energiecentrales, met de grond

gelijk maken. We leven in een wereld gevuld met kernwapens, die de menselijke beschaving geheel kunnen vernietigen. Hoewel cyberwapens in sommige gevallen fysieke schade aan kunnen richten, zoals de operaties in Oekraïne en in Natanz lieten zien, verbleekt hun schadepotentieel in vergelijking met conventioneel wapentuig. Dit verklaart hoogstwaarschijnlijk dat staten tot dusver heel anders reageren op cyberaanvallen dan op conventionele aanvallen. Als Rusland het hoofdkantoor van de Rabobank niet met een virus maar met bommen zou bestoken, zouden de NAVO-landen zeer waarschijnlijk Rusland de oorlog verklaren. Op dit vraagstuk gaan we in hoofdstuk 4 dieper op in.

Zoals gezegd is het schadepotentieel van cyberwapens nog volop in ontwikkeling. Wellicht is een verrassende en buitengewoon schadelijke cyberaanval, door sommigen ook wel een *Cyber Pearl Harbor* genoemd, een reële mogelijkheid, en kunnen toekomstige cyberwapens een samenleving ingrijpend ontwrichten (Trautman 2016). Maar in dat geval zou de beleving van een cyberaanval alsnog heel anders kunnen zijn dan de beleving van een oorlogshandeling die direct levens kost of gebouwen met de grond gelijk maakt. Een energiecentrale met de grond gelijk maken is iets anders dan de technologie dusdanig te manipuleren dat de centrale wekenlang geen stroom kan leveren.

In sommige gevallen is de schade van cyberaanvallen ook goed te herstellen (Libicki 2016). Een verloren leven is voor altijd verloren, en een historische kerk is niet zomaar herbouwd. Maar als een banksite een paar uur offline gaat en daarna weer werkt, heeft niemand het idee dat er voorgoed iets verloren is gegaan. Er is natuurlijk nog steeds serieuze schade: reparaties moeten uitgevoerd worden, nieuwe veiligheidsmaatregelen moeten ingekocht en opgesteld worden en belangrijke dienstverlening wordt uitgesteld. Maar de meeste mensen zullen het cyberincident snel vergeten. Dit is natuurlijk niet altijd het geval: een cyberaanval kan bijvoorbeeld ook cruciale documenten wissen die niet zomaar zijn herschreven.

Vanwege deze herstelbaarheid zien sommige auteurs cyberwapens daarom als een elegant alternatief voor conventionele wapens (Rid 2013). Misschien zou het prachtig zijn als een land dermate digitaal overwicht heeft dat het enkel met de dreiging van cyberwapens internationale conflicten kan beslechten. Toch zou dit narratief ook naïef kunnen zijn. Misschien vervangen cyberwapens conventionele wapens niet, maar scheppen ze een nieuwe, snel escalerende fase van internationale belangenbehartiging, die opeens over kan slaan in geweldshandelingen. In hoofdstuk 4 gaan we dieper op deze spanning in.

Een ander groot verschil met conventionele militaire middelen ligt in de mogelijkheden om de cyberwapens zelf onklaar te maken. De mogelijkheden om cyberwapens onklaar te maken zijn veel groter dan bij een conventioneel geweer of

een raket. Cyberwapens zijn wat dat betreft te vergelijken met virusziektes en inentingen. Als een effectieve inenting bestaat, kan een virusziekte geheel uitgeroeid worden. Net zo goed neemt de effectiviteit van een cyberwapen sterk af, als de kwetsbaarheid waar de schadelijke code zich op richt niet meer bestaat. Dit vereist dat computersystemen updates krijgen, wat vaak niet gebeurt. Maar de dynamiek is vergelijkbaar. Een effectieve update kan de angel uit een cyberwapen halen. Dit aspect verschilt sterk van conventionele wapens zoals jachtgeweren en kernbommen. Een enkel fysiek wapen kan vernietigd worden, en men kan allerlei verdedigingsmiddelen ontwerpen, maar het soort wapen houdt een aanzienlijk schadepotentieel.

Tegelijkertijd is een cyberaanvaller, in vergelijking met een reguliere militair, bijna niet te ontwapenen (Libicki 2016). Het is in verreweg de meeste ontwikkelde landen gemakkelijker om een computer te kopen dan een vuurwapen – en zeker geavanceerde militaire wapens zijn alleen voor hele specifieke actoren verkrijgbaar. Dus zelfs als de Verenigde Staten in staat zijn om vijandelijke computers onbruikbaar te maken, kan een cyberaanvaller op een nieuwe computer een volgende aanval plannen. Dit stelt vraagtekens bij plannen om cyberaanvallers tegen te houden door ze zelf met cybertechnologie aan te vallen – het is vrijwel onmogelijk om een tegenstander op die manier voorgoed onschadelijk te maken (Libicki 2016).

Ten slotte kunnen cyberwapens zich veel gemakkelijker verspreiden dan conventioneel wapentuig. Met een druk op de knop kan een virus in secondes van de ene naar de andere kant van de wereld worden gestuurd – dit geldt niet voor vuurwapens of kernraketten. Cyberaanvallers kunnen vanuit elke denkbare plek ter wereld een aanval plegen, zolang er maar verbinding is met het internet. Een aanval kan zich dus ook met een enorm tempo verspreiden. Dit gebeurde bijvoorbeeld met Stuxnet, dat zich vanuit Iran verspreidde naar computers in Europa (Zetter 2011). Bovendien kan een partij, soms van grote afstand, cyberwapens stelen – zo wist het hackerscollectief de ‘Shadowbrokers’ de NSA van allerlei wapens te beroven, die later online werden gezet (Sanger 2018).

Er bestaat een groot risico dat cyberwapens hergebruikt worden door andere partijen, en dat, zoals in het geval van Stuxnet, schadelijke code onbedoeld allerlei andere doelwitten treft. Het probleem van nevenschade (*collateral damage*) speelt natuurlijk ook bij de inzet van conventionele militaire middelen, en ook die middelen worden gestolen of gekopieerd door de tegenstander. Maar de schaal is anders. Een bombardement raakt misschien ook het ziekenhuis nabij de militaire basis, maar een verdwaald virus gericht op een computer in Nederland kan zomaar even later in Engeland schade aanrichten.

Het mondiale karakter van het internet compliceert zo de inzet van cyberwapens. De kans is aanzienlijk dat andere partijen uiteindelijk ook van de gevaarlijke code gebruikmaken, en dat er allerlei onvoorziene boemerangeffecten ontstaan.

2.2.3 Weerbaarheid

Voor een deel zijn de beschermingsmaatregelen tegen cybersabotage besproken. Als je ervoor zorgt dat een hacker niet in een systeem kan infiltreren, en binnen systemen zijn bevoegdheden niet kan uitbreiden, kan er in de meeste gevallen ook niet gesaboteerd worden. Als een hacker eenmaal binnen is, én de benodigde bevoegdheden heeft verzameld, zijn allerlei sabotages mogelijk.

Hierbij geldt dat er voor de ene sabotage meer expertise nodig is dan voor de andere. Om bijvoorbeeld *malware* te schrijven voor een petrochemische fabriek moet een hacker verstand hebben van de industriële software. Maar voor veel schadelijke sabotage is deze expertise niet nodig. Sterker nog: voor diensten als het versturen van spam-mail, het inzetten van een DDoS-aanval, het schrijven van *malware* en het rekruteren van bots bestaat een lucratieve markt (Libicki 2016). Zo lanceren sommige criminelen een DDoS-aanval tegen een onbeschermde site voor 100 dollar per dag, terwijl je voor een tegen DDoS beschermde site 400 dollar betaalt (Markushin 2017). De kosten voor de partij die door een cyberaanval wordt getroffen kunnen daarentegen flink oplopen. Kaspersky schat de kosten voor een klein bedrijf gemiddeld op bijna 90.000 dollar en de kosten voor een groot bedrijf op bijna 900.000 dollar (Kaspersky 2016). Het verschil in kosten tussen aanvaller en verdediger kan dus gigantisch zijn – en dan hebben we nog niet gekeken naar de inkomsten van de aanvallers.

Al deze aspecten schetsen een zorgwekkend beeld: veel soorten cyberaanvallen zijn goedkoop, kunnen door leken besteld worden en zijn soms moeilijk verdedigbaar. Niet voor niets wordt telkens weer gewezen op de grote uitdagingen van cyberweerbaarheid (NCTV 2018). Tegelijkertijd laat de vergelijking met conventionele wapens zien dat de schade die cybersabotage tot dusver heeft aangericht wel ernstig is, maar geen mensenlevens opeist, een maatschappij niet schokt zoals een terroristische aanslag, en de samenleving niet ontwricht zoals een economische crisis, een zware droogte of een overstroming. Hoewel vitale infrastructuur wel door cyberaanvallen is aangetast, is deze infrastructuur meestal binnen een aantal uur weer op niveau gebracht. Toch biedt de relatieve mildheid van cyberaanvallen natuurlijk geen garanties voor de toekomst.

De verdediging tegen cyberaanvallers kan ook bestaan uit het beschadigen van die cyberaanvaller, bijvoorbeeld door die aanvaller uit te schakelen of af te schrikken.

We hebben al genoemd dat het soms lastig is om cyberaanvallers te identificeren, – maar dat is zeker niet onmogelijk. Zo zijn in het verleden verschillende cybercriminelen succesvol vervolgd en veroordeeld, en beweren inlichtingendiensten in sommige gevallen dat ze zeker weten wie de daders van een bepaalde aanval zijn geweest (Westcott 2018, Ward 2018). Maar wanneer de aanval plaats vindt door, of met toestemming van, een andere staat, is niet gelijk duidelijk hoe er gehandeld moet worden – en welke strategie de cyberveiligheid uiteindelijk zal kunnen bevorderen. Vanaf hoofdstuk 3 zullen we dieper op dit vraagstuk ingaan.

2.3 De verspreiding van desinformatie

Kader 3 Drie voorbeelden van desinformatie

In de aanloop naar de Amerikaanse presidentsverkiezingen van november 2016 kwam er op online fora steeds meer leugenachtige informatie in omloop (Faris et al. 2017, Ritchie 2016). De paus zou Donald Trump steunen. Hillary Clinton zou wapens verkopen aan de groepering Islamitische Staat (IS). En John Podesta, de campagneleider van Clinton, zou samen met andere hooggeplaatste medewerkers structureel kinderen misbruiken.

Russische media, politiek-rechtse groeperingen en Donald Trump verspreidden sinds 2008 de aantoonbare leugen dat Barack Obama niet in de Verenigde Staten is geboren, en daarom geen president zou mogen zijn (Haberman 2017). Deze complottheorie wordt *birtherism* genoemd, en bleef maar herhaald worden, zelfs nadat Obama's geboorteakte aan het publiek was vrijgegeven. Uiteindelijk gaf Trump tijdens een persconferentie toe dat Obama in de Verenigde Staten was geboren.

In de aanloop naar de Franse presidentsverkiezingen van mei 2017 verscheen er op Pastebin, een site waar documenten gedeeld kunnen worden, het document EMLEAKS, met daarin allerlei foutieve informatie over toenmalig presidentskandidaat Macron – bijvoorbeeld dat hij een geheime bankrekening had op de Kaaimaneilanden (Valance 2017).

2.3.1 Technologie

De verspreiding van desinformatie is niet noodzakelijkerwijs verbonden met digitale technologie, maar wordt vergemakkelijkt door digitale kanalen. Cyberaanvallen, bijvoorbeeld de aanval op het Oekraïense energienetwerk, omvatten dikwijls ook een desinformatiecampagne. Wat bedoelen we eigenlijk met desinformatie?

De Raad van Europa onderscheidt drie types van perverse informatieverspreiding: het verspreiden van desinformatie, misinformatie en pijnlijke informatie (Wardle & Derakhshan 2017).

- **Desinformatie** betekent het bewust creëren en verspreiden van onware, inaccurate of misleidende informatie omwille van economisch profijt of om een persoon, sociale groep, organisatie of land te schaden (zie ook Van Keulen et al. 2017). Zo kan iemand bijvoorbeeld via een Twitter-account het foutieve bericht verspreiden dat een bekende politicus een zedendelict heeft begaan.
- **Misinformatie** betekent het verspreiden van inaccurate informatie, terwijl de gebruiker denkt dat deze informatie correct is. Dus als weer een ander persoon het bericht over de politicus retweet, omdat hij het gelijk gelooft, mis-informeert hij anderen.
- **Pijnlijke informatie** betekent het verspreiden van pijnlijke, maar kloppende informatie, om een persoon of organisatie zwart te maken en anderen tegen die organisatie op te ruien.

Zoals gezegd richt dit rapport zich op de verspreiding van desinformatie; zie kader 3 voor een aantal voorbeelden hiervan.[6] Misinformatie speelt daarbij wel een rol: de instigator hoopt dat foutieve berichten door anderen voor waar worden aangezien en worden verspreid. Een voorbeeld van desinformatie is het bericht op de site WTOE 5 News dat paus Franciscus Donald Trump steunde als kandidaat voor het presidentschap. Dat was niet zo. Tot de dag van vandaag zijn wetenschappers, journalisten en het Amerikaanse Federal Bureau of Investigation (FBI) bezig helder te krijgen hoeveel desinformatie er tijdens de Amerikaanse presidentsverkiezingen van 2016 is verspreid, en wie dat precies heeft gedaan (Ferrara 2017).

Iedereen met een Twitter- of Facebookaccount kan leugens verspreiden. Maar dikwijls wordt desinformatie verspreid door anonieme accounts en door online profielen, de zogeheten bots, die door software gestuurd worden en op basis van algoritmes berichten plaatsen en verspreiden (Varol et al. 2017). Met name op Twitter zijn er veel bots. Onderzoekers schatten in maart 2017 het aantal bots tussen de 9% en 15% van alle Twitteraccounts. Dat zouden dus bijna 48 miljoen

6 Desinformatie gericht op economisch profijt wordt niet besproken, omdat dit fenomeen geen rol van betekenis speelt in de relatie tussen staten.

accounts kunnen zijn (Varol et al. 2017). Die enorme botzwermen spelen een cruciale rol in het verspreiden van desinformatie. Stel je eens voor dat je leugenachtige bericht geretweet wordt door 500.000 bots.

Ten slotte is het van belang te vermelden dat desinformatie kan worden verspreid via vervalste videobeelden of audiofragmenten (Rathenau Instituut 2019). Digitale toepassingen kunnen bijvoorbeeld steeds overtuigender filmpjes maken waarin politici een bepaalde uitspraak lijken te zeggen. De gemiddelde leek kan vaak het verschil niet meer zien tussen een authentieke en een gefabriceerde opname. De laatste tijd wordt veel gewaarschuwd tegen deze nieuwe technologie, die de impact van desinformatiecampagnes aanzienlijk zou kunnen verhogen (Polyakova & Boyer 2018).

Door desinformatie te verspreiden wordt het publieke debat gemanipuleerd. De precieze manipulatie hangt van de doelstelling af. Toch valt op dat desinformatie vaak polariserend werkt, en, naast het ondersteunen van een bepaalde boodschap of agenda, een evenwichtig en inhoudelijk publiek debat vooral kan ondermijnen (Wardle & Derakhshan 2017). Zoals het Rathenau Instituut schrijft in het rapport *Digitalisering van het nieuws*: ‘Desinformatie wijst vaak bewust op verschillen en zet tot verdeeldheid aan tussen aanhangers van verschillende politieke partijen of tussen groepen van verschillende nationaliteit, ras, etniciteit, religie of klasse. Eenmaal ingebracht, kunnen dergelijke ideeën worden gebruikt om zondebokken te creëren, vooroordelen te populariseren, tegenstellingen te verharden en zelfs geweld te katalyseren en te rechtvaardigen’ (Van Keulen et al. 2018, 49).

2.3.2 Vergelijking met conventionele propaganda

De belofte van desinformatiecampagnes is groot: wie de samenleving kan beïnvloeden, kan haar voor zijn eigen karretje spannen en beleid beïnvloeden. Het is natuurlijk de vraag hoe effectief die campagnes zijn, en hoe groot het vermogen van burgers en hun instituties is om desinformatie te ontmaskeren en onschadelijk te maken. Macron kon, tegengewerkt door een desinformatiecampagne, nog steeds een ruime verkiezingswinst behalen, terwijl Hillary Clinton, ook tegengewerkt door desinformatie, de verkiezingen nipt van Donald Trump verloor.

Die onzekerheid over het effect weerhoudt sommige staten geenszins van experimenten. Net als het uitvoeren van DDoS-aanvallen is het verspreiden van desinformatie goedkoop en kan het in hoge mate geautomatiseerd worden. Dat maakt het mogelijk om structureel het publieke debat te blijven beïnvloeden. Bovendien hoeft de verspreider van desinformatie zelden rekening te houden met persoonlijke gevolgen. Ook hier speelt het probleem van het identificeren van de

precieze dader, en het feit dat daders zich op het territorium en onder de vleugels van een vijandelijke staat kunnen verschuilen. Het is dus waarschijnlijk dat desinformatiecampagnes, al dan niet gesponsord door staten, ook in de toekomst een rol van betekenis blijven spelen.

2.3.3 Weerbaarheid

Kan een samenleving zich tegen desinformatie beschermen? Voor een deel ligt die verantwoordelijkheid bij de mediaplatformen waarop de desinformatie gepubliceerd wordt. We noemen kort een paar voorbeelden.

- Zo probeert Twitter bots automatisch te signaleren en uit te schakelen (Crowell 2017). Helaas worden twitterbots steeds verfijnder gefabriceerd en zijn ze in de toekomst steeds moeilijker van menselijke gebruikers te onderscheiden (Van Keulen et al. 2018, Rathenau Instituut 2019).
- Platforms zouden ook een andere communicatiearchitectuur kunnen invoeren, die bijvoorbeeld vereist dat iedere account gekoppeld is aan een geauthentiseerde menselijke gebruiker. Hier is echter ook weer wat op af te dingen, aangezien online anonimiteit ook voordelen heeft. Zoals wanneer het verkondigen van een bepaalde boodschap gevaarlijk is voor de afzender.
- Ten slotte zouden sociale platforms inzage kunnen geven over hoe hun algoritmes werken. Daardoor wordt bewustzijn gecreëerd bij burgers over de algoritmische beïnvloeding van hun informatievoorziening (Van Keulen et al. 2018). Uit het onderzoek van psycholoog Robert Epstein bleek bijvoorbeeld hoe zoekresultaten de voorkeuren van kiezers sterk kunnen beïnvloeden door slechts de volgorde van de resultaten in een zoekmachine, zoals Google, te wijzigen (Epstein 2015).

De politiek kan ook een actievere rol spelen, bijvoorbeeld door onafhankelijke instellingen te faciliteren. Dat kan door zogenoemde *factcheckers*, die de nieuwsvoorziening kunnen monitoren, en die informatie in publieke (on- en offline) debatten op juistheid controleren (Harambam 2017). Maar hier dreigt een gevaar. Westerse democratieën kennen een vrije, niet door de staat gecontroleerde pers. In een goed werkende democratie ligt de verantwoordelijkheid om leugens bloot te leggen primair bij een open publiek debat.

Voor de journalistiek en voor burgers zelf zijn daarom belangrijke rollen weggelegd. De journalistiek kan online en offline een kwalitatieve band opbouwen met het publiek, door diepgravend onderzoek te doen waarbij feiten grondig worden gecheckt, en door uit te leggen hoe journalisten te werk gaan. Daarnaast zou de journalistiek zich meer online kunnen profileren. Een voorbeeld hiervan is de

dagelijkse podcast *The Daily* van The New York Times, waarin de redactie laat zien hoe ze te werk gaat en waarin ze interviews soms bewust integraal laat horen.[7]

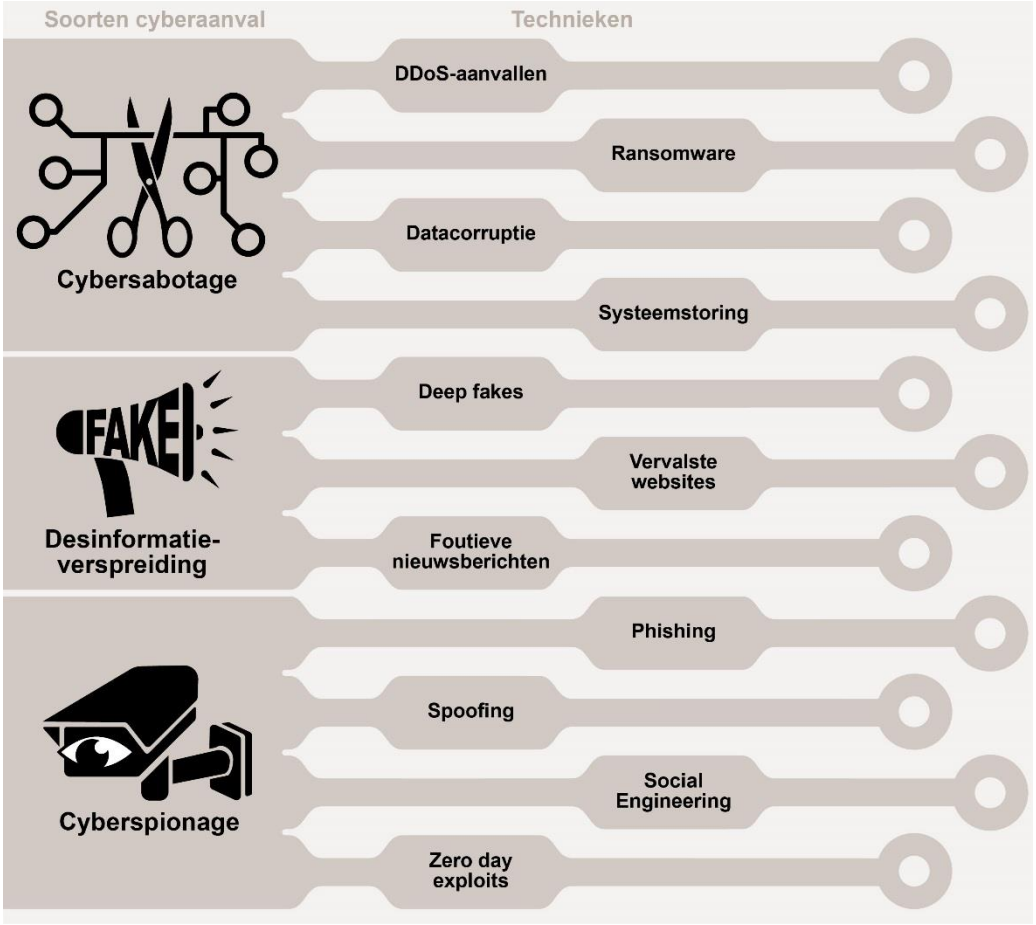
Ten slotte heeft de samenleving technologisch vaardige burgers nodig: burgers die begrijpen hoe de verspreiding van desinformatie werkt, die daarover kritisch kunnen nadenken en die inzien welke impact een desinformatiecampagne kan hebben op zijn leefwereld (Van Keulen et al. 2018). Deze burgers zouden desinformatie kunnen signaleren en aan de kaak kunnen stellen, waardoor dit soort beïnvloeding minder effectief kan worden. In Zweden, bijvoorbeeld, krijgen leerlingen van 10 jaar en ouder verplicht onderwijs in digitale competentie (Roden 2017). Een belangrijk onderdeel hiervan is de beheersing van bronnenkritiek.

2.4 Conclusie

Dit hoofdstuk gaf een overzicht en analyse van de technologische ontwikkelingen met betrekking tot offensieve cybercapaciteiten. De verschillende soorten cyberaanvallen zijn in figuur 2 grafisch vormgegeven.

[7] Zie https://www.nytimes.com/column/the-daily.

Figuur 2 Verschillende soorten cyberaanvallen



Dit zijn de belangrijkste bevindingen:

- **We maakten een onderscheid tussen drie soorten cyberaanvallen: cyberspionage**, **cybersabotage** en de **verspreiding van desinformatie**. Deze cyberaanvallen zijn sterk onderling verbonden: cyberspionage gaat bijvoorbeeld vaak vooraf aan cybersabotage, en de verspreiding van desinformatie werd tijdens de aanval op de Amerikaanse verkiezingen van november 2016 gecombineerd met het hacken van de mailserver van de Democraten.

- **Cyberaanvallen verschillen op punten wezenlijk van conventionele aanvallen.** Cyberspionnen lopen veel minder risico dan conventionele spionnen, en kunnen op grote afstand meerdere digitale systeem structureel infiltreren en monitoren. Digitalisering heeft spionage tegelijkertijd brutaler en ongrijpbaarder gemaakt. Cybersaboteurs lopen ook veel minder risico, en

kunnen net zo onvoorspelbaar en wijdverbreid schade toebrengen. Het schadepotentieel verschilt echter wezenlijk van dat van conventioneel wapentuig. Veel schade is herstelbaar en zware fysieke schade is zeldzaam. Ten slotte maakt het internet de verspreiding van desinformatie mogelijk op een niet eerder vertoonde schaal, en kunnen leugens vanuit vele profielen en kanalen media bereiken. Dit maakt het lastig om te achterhalen wie propaganda verspreidt en waarom – digitalisering vormt zo een zegen voor actoren die door middel van propaganda hun doelen nastreven en debatten willen polariseren.

- **Het is soms zeer moeilijk om cyberaanvallen af te weren, en goede cybersecurityvoorzieningen vereisen een serieuze inzet van middelen en mensen**. In vergelijking met cyberverdedigers kunnen cyberaanvallers vanuit de schaduw toeslaan en vaak tegen lage kosten aanvallen uitvoeren of uitbesteden. Tegelijkertijd maakt de expertise van aanvaller en verdediger veel uit: sommige aanvallen zijn gemakkelijker af te slaan dan andere. Uiteindelijk neemt de aanvaller het tegen de verdediger op in een race zonder finish. Toch lijkt de aanvaller op dit moment in het voordeel te zijn.

3 Het informatieconflict

In dit hoofdstuk en in hoofdstuk 4 wordt een analyse gegeven van de internationale ontwikkelingen op het gebied van offensieve cybercapaciteiten. We inventariseren in dit hoofdstuk in hoeverre de Verenigde Staten, Rusland, China, Nederland en de overige EU-landen de capaciteiten verwerven om cyberspionage, cybersabotage en desinformatiecampagnes uit te voeren, waarom ze dat doen, hoe ze die capaciteiten hebben ingezet, en of we overeenkomsten en verschillen tussen het gedrag van die staten kunnen observeren. Daarbij bespreken we ook de private, en soms criminele, markt voor cyberwapens in de verschillende landen.

We hebben de Verenigde Staten, Rusland en China geselecteerd omdat deze landen wereldspelers zijn in het huidige internationale digitale landschap. De EU-landen bespreken we vanwege het belang van de Europese omgeving voor Nederland. Aan het einde van dit hoofdstuk wordt de escalatieladder (zie hoofdstuk 1) verder toegelicht. Deze zullen we gebruiken om de activiteiten van de verschillende staten te kunnen markeren. Op basis van deze escalatieladder concluderen we dat de huidige internationale situatie het beste gekarakteriseerd kan worden als een informatieconflict.

Een voorbehoud is hier op zijn plaats: dit hoofdstuk geeft geen volledig overzicht van de capaciteitsopbouw per land, en behandelt veel landen niet – zo bespreekt het Noord-Korea niet en Iran slechts zijdelings, terwijl deze staten wel door andere landen primaire bedreigingen worden genoemd (U.S. Department of Defense 2018). Een volledig overzicht geven is ook niet onze bedoeling – het doel is om te verhelderen met welke keuzes Nederland zichzelf geconfronteerd ziet.

3.1 De Verenigde Staten

3.1.1 In het kort

De VS zijn altijd een dominante actor geweest in de ontwikkeling van ICT-technologie. Het land stond aan de wieg van het internet en is met bedrijven als Apple, Amazon, Google en Microsoft de grote commerciële voorloper in het maken en verkopen van ICT-producten en -diensten (Curran et al. 2012). Kenmerkend voor de Amerikaanse omgang met ICT-technologie is de openstelling van het

internet. Sinds de late jaren ’80 is deze technologie steeds toegankelijker geworden voor marktpartijen, en ligt het beheer van het internet bij private partijen zoals de Internet Corporation for Assigned Names and Numbers (ICANN) (Klimburg 2017).

Tegelijkertijd beschouwt de Amerikaanse overheid zich als de machtigste actor in deze nieuwe omgeving – en streeft ze er naar deze positie te behouden (U.S. Cybercommand 2018b). Niet voor niets beschouwt de Amerikaanse overheid cyberspace als een vijfde domein van militair conflict, naast het land, de zee, de lucht en de ruimte. De Amerikaanse strategie kan daarom worden samengevat als de wens de zwaarbewapende voorvechter te zijn van de digitale vrije wereld. Het spreekt vanzelf dat de twee aspecten van deze wens tegen elkaar in kunnen werken: een vrije digitale omgeving is niet per se geholpen met een kampioen die hardhandig dreigingen te lijf gaat. Op deze spanning zullen we later terugkomen.

Kader 4 Offensieve cybercapaciteiten van de Verenigde Staten

De VS spenderen verreweg het meeste aan defensie ter wereld: de militaire uitgaven in 2017 worden door het Stockholm International Peace Research Institute geschat op 609 miljard dollar (SIPRI 2018). De uitgaven waren van 2007-2013 hoger, en zullen het komende jaar weer stijgen. Ter vergelijking: China, de op-een-na grootste investeerder in militaire capaciteit, gaf hieraan in 2017 228 miljard dollar uit.

De VS richtten in 2009 het U.S. Cyber Command op (Graham 2016). Dit legercommando rapporteerde aanvankelijk aan het hogere Strategic Command, maar valt sinds 2018 direct onder de minister van Defensie. Het commando is vanaf 17 mei 2018 volledig operationeel en heeft onder meer 133 cybermissieteams, bestaande uit ruim 6.000 personen, die zowel aanvallende als verdedigende taken kunnen uitvoeren (U.S. Cybercommand 2018a).

De VS hebben 16 inlichtingendiensten, waaronder de Central Intelligence Agency (CIA), de National Security Agency (NSA) en de Defense Intelligence Agency (DIA). Deze diensten ontplooien allemaal cyberactiviteiten. De NSA heeft een speciale verantwoordelijkheid om op communicatie- en informatiesystemen zogeheten Signals Intelligence (SINGINT) te verzamelen (NSA 2018).

Het Amerikaanse cyberbudget in 2019 is ongeveer 15 miljard dollar (Nodurft 2018). Meer dan de helft hiervan gaat naar het ministerie van Defensie. Hoewel de afgelopen jaren allerlei bezuinigingen zijn doorgevoerd, wordt juist voor cyberoperaties en cybersecurity steeds meer geld vrijgemaakt. Let wel: bovenop de publieke cijfers moeten bijdrages van het geheime ‘*black budget*’ van de inlichtingendiensten opgeteld worden. Dit budget werd in 2013 met hulp van klokkenluider Edward Snowden in de Washington Post bekend gemaakt. Analyses van de Washington Post laten een sterke stijging zien sinds 2001, gerelateerd aan de aanslagen van 11 september en de daarop volgende oorlog tegen terrorisme (Washington Post 2013). Het totale *black budget* bedroeg in 2013 52,6 miljard dollar. De CIA en de NSA ontvingen het meeste geld. 4,3 miljard van de 52,6 miljard dollar was geoormerkt voor het uitvoeren van cyberoperaties.

3.1.2 Strategische ontwikkeling

De VS hebben hun digitale aanvalskracht al zeer vroeg ontwikkeld. Hoewel het nooit is bewezen, zouden ze in de vroege jaren ’80 het industrieel controlesysteem van gasleidingen in de Sovjet-Unie hebben gesaboteerd (Reed 2005). Daardoor zou er een ontploffing hebben plaatsgevonden en zou het leidingnetwerk zijn beschadigd. Waar of niet, vandaag de dag willen de VS de capaciteit bezitten dergelijke schade aan te richten, en zou het kunnen dat het land deze capaciteiten al heeft. De Amerikaanse overheid geeft van alle staten al jaren verreweg het meeste geld uit aan het opbouwen van cybercapaciteiten, zowel bij inlichtingendiensten als bij andere defensieonderdelen, en profiteert al decennia van haar dominante rol in cyberspace (zie kader 4). Gelijk aan de conventionele wapenindustrie heeft zich in de VS ook een cyberwapenindustrie gevormd, waar voor vele miljarden spionage- en sabotagewapens aan defensieorganisaties worden verkocht (Stockton & Golabek-Goldman 2013, The Economist 2018).

De VS legden al snel de verbanden tussen informatietechnologie, inlichtingenverwerving en defensie. In de jaren ’90 investeerde defensie in ‘*network-centric warfare*’, het vermogen om in oorlogssituaties via elektronische netwerken snel te communiceren, en de communicatienetwerken van de tegenstander juist uit te schakelen (Cebrowski & Garstka 1998). In de jaren ’90 werd het verzamelen en bekijken van internetverkeer, zoals e-mails, toegevoegd aan de inlichtingenpraktijk (Wright 1998). Binnen de overheidsdiensten groeide gestaag het besef dat met de opkomst van cyberspace nieuwe veiligheidsrisico’s ontstonden, alsook de mogelijkheid om zelf van die risico’s gebruik te maken. Deze ontwikkeling kreeg extra vaart in 2001 na de terroristische aanslagen, waarna inlichtingendiensten verregaande bevoegdheden kregen om burgers, verdacht of niet, te surveilleren en informatie te verzamelen (Jaeger et al. 2003).

Sindsdien zijn een aantal strategische publicaties uitgebracht en uitspraken gedaan die weergeven hoe binnen het Amerikaanse ministerie van Defensie en de inlichtingendiensten over offensieve cybercapaciteiten wordt gedacht (U.S. Department of Defense 2018, U.S. Cybercommand 2018b, U.S. Secretary of Defense 2018, Clapper 2013). Een belangrijke trend is dat cyberspace expliciet gezien wordt als het vijfde domein van oorlogsvoering – vitale Amerikaanse belangen kunnen door middel van cyberactiviteiten beschadigd worden. Daarom hebben de VS machtige offensieve cybercapaciteiten opgebouwd; zie kader 4.

De tweede trend bestaat uit het scheiden van economische inlichtingenverzameling en niet-economische spionageactiviteiten. Economische spionage wordt gezien als illegaal en provocerend, maar spionage gericht op buitenlandse overheidsinstellingen is niet illegaal (Clapper 2013). Dit betekent dat de VS in de

jaren 2000 en het gros van de jaren ’10 voorstander waren van een ongereguleerde internationale praktijk van niet-economische cyberspionage.

Ook cybersabotage werd soms acceptabel bevonden in de VS, zoals vooral de operatie ‘Olympic Games’ bewees. Het is belangrijk hier wat dieper op in te gaan. De Verenigde Staten zijn samen met een groot deel van de internationale gemeenschap in een strijd met Iran verwikkeld om te voorkomen dat Iran een kernwapen in handen krijgt. Het is zeer waarschijnlijk dat de Verenigde Staten, ondersteund door de Israëlische overheid, de Iraanse verrijkingscentrifuges in Natanz met het Stuxnet-virus hebben besmet. De ene na de andere centrifuge ging kapot, en aanvankelijk had Iran niets door. Later verspreidde het virus zich naar andere plekken, en werd de aard en herkomst van het virus door beveiligingsbedrijven gereconstrueerd (Zetter 2011). Iran kwam achter de aanval, en sloeg in 2012 terug door financiële instellingen op Wall Street aan te vallen (Gorman & Barnes 2012). Iran zette zijn cybercapaciteiten ook tegen andere landen in, bijvoorbeeld door een verwoestende aanval te lanceren op Saudi Aramco, een staatsoliebedrijf van Saudi Arabië, dat vijf maanden nodig had om de schade ongedaan te maken (Sanger 2018). Op 23 maart 2018 beschuldigde het Amerikaanse ministerie van Justitie negen Iraniërs; sinds 2013 zouden ze medeverantwoordelijk zijn voor het infiltreren van de netwerken van onder meer 144 Amerikaanse universiteiten, de Verenigde Naties en het ministerie van Arbeid (U.S. Department of Justice 2018).

De gebeurtenissen rondom Stuxnet laten zien dat technologische dominantie de VS in staat heeft gesteld deze cyberaanval uit te voeren, en dat deze tegelijk niet heeft voorkomen dat de VS zouden worden geraakt. De Iraniërs hadden veel minder middelen tot hun beschikking, maar konden toch terugslaan.

De VS zijn de afgelopen vijftien jaar veel vaker met succes aangevallen.

- Geheime technologie, waaronder *zero day*-kwetsbaarheden, zijn van de NSA gestolen;
- vertrouwelijke personeelsgegevens van honderdduizenden federale ambtenaren zijn op straat komen te liggen; en
- vanuit Rusland zijn in 2016 zelfs de vrije Amerikaanse presidentsverkiezingen aangetast (Zetter 2015, Schneider 2017).

Juist omdat de VS vooroplopen in het ontwikkelen en toepassen van digitale technologie, zijn allerlei sectoren er kwetsbaar voor cyberaanvallen (Klimburg 2017). Met name onder de regering van Obama werd dan ook getwijfeld aan de strategie van cyberspace-dominantie. Zo zijn er voorstellen gedaan om minder snel en omvangrijk te surveilleren en om zo weinig mogelijk *zero days* achter te houden (Zetter 2014). President Obama koos op twee belangrijke momenten ook voor de

diplomatieke weg: toen bedrijfsspionage uit China grote vormen aannam, sloot hij met de Chinese president Xi een akkoord om de aanvallen te verminderen (Klimburg 2017). En in de nasleep van aanvallen tijdens de verkiezingen van 2016 koos hij ervoor Russische diplomaten uit te zetten (The New York Times Editorial Board 2016).

Tegelijkertijd waren tijdens de Obama-regeringen (2009-2017) de spionageactiviteiten zeer omvangrijk. De onthullingen van Edward Snowden (2013) lieten zien dat Amerikaanse diensten honderden infiltrerende aanvallen pleegden, en niet alleen tegenstanders bespioneerden, maar ook burgers en zelfs bondgenoten zoals Duitsland, Italië en de Europese Unie in de gaten hielden (Poitras & Rosenbach 2013). Bovendien wordt er gesuggereerd dat de VS in reactie op de hack bij Sony het digitale netwerk van Noord-Korea heeft aangevallen (Van der Meer 2018b). Gedurende de Obama-jaren hinkte de Amerikaanse overheid dus op twee benen.

De laatste tijd lijkt de strategie van Amerikaanse cyberspace-dominantie weer in opmars. In een strategie uit 2018, met de veelzeggende titel ‘Achieve and Maintain Cyberspace Superiority’, bepleit het Amerikaanse ministerie van Defensie dat er ‘voorwaarts verdedigd’ moet worden (U.S. Cybercommand 2018b). Dit betekent dat de VS een snelle toegang moeten hebben tot, en vaak al geïnfiltreerd moeten zijn in, de systemen van mogelijk gevaarlijke tegenstanders. Met andere woorden: veel netwerken moeten bij voorbaat al gehackt zijn, en de gelegenheid bieden snel terug te slaan.

De gedachte is dat in deze omstandigheden hackers de VS niet meer durven aan te vallen, omdat onmiddellijk en krachtig op iedere infiltratie in een Amerikaans systeem gereageerd kan worden. Absolute dominantie zorgt zo voor een hoog afschrikkingsniveau. Of zoals de recente National Cyber Strategy het uitdrukt: ‘*preserve peace through strength*’ (White House 2018, 20). De VS willen ook met gelijkgestemde landen samenwerken om aanvallen snel af te slaan en gezamenlijk terug te slaan. Bovendien wordt er in de politiek en het bedrijfsleven al een tijd gediscussieerd over het creëren van een ‘terughack’-bevoegdheid voor bedrijven, zodat ook zij aanvallers kunnen afschrikken (Kallberg 2015).

Ook lijkt de Amerikaanse regering steeds meer bereid om onwaarheden te verspreiden, bijvoorbeeld over de kosten van de grensmuur met Mexico en de grootte van het publiek dat de inauguratie van president Trump bijwoonde. Het is niet duidelijk of deze uitspraken gepaard gaan met campagnes om in het buitenland desinformatie te verspreiden. Zijn regering overweegt in ieder geval meer actieve informatiecampagnes – zoals het intensiveren van uitzendingen in het Farsi, om de bevolking van Iran te beïnvloeden (Morello 2018).

Ten slotte slaan de VS ook een hardere toon aan tegenover internationale technologiebedrijven die verbonden zijn met staten die de VS hebben aangevallen, met name het Chinese Huawei Technologies en het Russische Kaspersky Labs. De regering wil niet afhankelijk zijn van deze leveranciers, omdat ze ervan verdacht worden samen te werken met hun overheden. Huawei zou bijvoorbeeld spionagetoepassingen kunnen installeren in de 5G-netwerken die het aanlegt. Bovendien arresteerden de Canadese autoriteiten op verzoek van de VS in 2018 Wanzhou Meng, de *chief financial officer* van Huawei, vanwege het schenden van de sancties tegen Iran (Tweed & Martin 2018). Commentatoren zien deze beweging als een nieuwe stap om Huawei, en in het verlengde daarvan de China's technologische positie, te beschadigen.

Met de keuze voor cyberspace-dominantie blijven de VS trouw aan het uitgangspunt dat ze al in de jaren '90 innamen: ze willen de bewapende voorvechter zijn van een vrije digitale wereld. Maar het is de vraag of al deze dreiging de tegenstander echt buiten de deur houdt: juist tijdens de regeringsperiode van Trump neemt de Chinese cyberspionage weer toe, en lijkt er van de diplomatieke afspraak tussen Obama en Xi weinig over te zijn (Sanger & Myers 2018).

Het is daarom belangrijk hier een kanttekening te plaatsen: diverse wetenschappers stellen dat de afschrikkingsstrategie van de VS niet effectief is en juist averechtse gevolgen heeft (Libicki 2009, Van der Meer 2015, 2018a). Afschrikking door vergelding, '*deterence by retaliation*', is effectief als voor de aanvaller de mogelijke kosten van de aanval hoger liggen dan de voordelen (Krepinevich, 2012). Hier is met name bij kernwapens sprake van: die richten afschuwelijke schade aan die moeilijk te verdedigen is. Staten grepen in de Koude Oorlog dan ook naar de strategie van wederzijds gegarandeerde vernietiging (Goodman 2010).

Maar cybertechnologie verschilt in relevante opzichten van kernwapentechnologie.

1. Ten eerste zijn cyberaanvallen veel minder destructief, waardoor een kwaadwillende actor ze eerder durft uit te voeren. De drempel om een kernwapen te lanceren is nu eenmaal veel hoger dan de drempel om desinformatie te verspreiden.
2. Ten tweede zijn onmiddellijke cybertegenaanvallen niet altijd mogelijk. De kans bestaat dat juist offensieve cybercapaciteiten door de cyberaanval worden uitgeschakeld (Goodman 2010).
3. Ten derde weet een staat lang niet altijd wie een aanval gepleegd heeft, en over welke cybercapaciteiten bepaalde tegenstanders eigenlijk beschikken (Iasiello 2013). Tijdens de Koude Oorlog wisten zowel de VS als de Sovjet-

> Unie zeer goed waar de andere toe in staat was, maar uit angst voor sabotage houden staten vandaag de dag hun cybercapaciteiten doorgaans geheim (Clarke & Knake 2010, Libicki 2013). Als de tegenstander eenmaal weet welk cyberwapen je hebt, kan het nutteloos gemaakt worden.

Al deze onzekerheid zet een effectieve afschrikkingsstrategie onder druk, en creëert een mistige ruimte waarbinnen staten juist met cyberaanvallen weg kunnen komen – zelfs als de aangevallen staat over machtige cyberwapens beschikt.

3.2 Rusland

3.2.1 In het kort

Ook Rusland heeft een lange geschiedenis met digitale technologie. Van de jaren ’40 tot ‘70 maakten Sovjet-technici grote stappen in de computerwetenschap en werden vele prototypen van mainframe-computers ontworpen (Klimburg 2017). De Sovjet-Unie, waar Rusland onderdeel van was, was een totalitaire staat, waarin digitale technologie al vroeg werd geïdentificeerd als een centraal element in het beheersen van informatiestromen tussen burgers en de staat en tussen burgers onderling. Toch wist niet de communistische Sovjet-Unie maar de Verenigde Staten het internet te ontwikkelen en uit te rollen. Volgens sommige experts komt dit juist door de Russische neiging om van staatswege de ontwikkeling van technologie tot in detail te controleren, in plaats van deze vrij te geven en aan te laten vullen door burgers, bedrijven en een breder scala van overheidsdiensten (Klimburg 2017, Harari 2018).

In ieder geval beschikte Rusland na het einde van de Koude Oorlog in 1989 en 1990 zowel over een lange digitaal-wetenschappelijke traditie als over een totalitair verleden. Deze twee elementen hebben de ontwikkeling van Rusland in de digitale wereld bepaald. Het huidige regime van president Poetin streeft er namelijk naar om via het beheersen van informatiestromen zijn binnen- én buitenlandse belangen veilig te stellen. In de ogen van het Kremlin is informatie een wapen waarmee je oorlog kunt voeren (Government of Russia 2014). Door middel van cyberspionage, cybersabotage en bovenal de verspreiding van desinformatie probeert de Russische overheid haar eigen bevolking onder de duim te houden en buitenlandse machten uit balans te brengen (Polyakova & Boyer 2018).

Kader 5 Offensieve cybercapaciteiten van Rusland

De Russische defensie-uitgaven zijn de afgelopen jaren sterk gestegen, van 27 miljard dollar in 2006 naar 60 miljard dollar in 2016 (schatting DIA 2017, SIPRI heeft geen cijfers). De uitgaven vallen echter weer terug. In 2014 kondigde het leger aan dat er 500 miljoen dollar besteed zou worden aan speciale cybertroepen en aan het opzetten van een coördinerend legeronderdeel dat direct rapporteert aan de generale staf – de Amerikaanse DIA (zie kader 4) denkt dat Rusland sinds 2010 werk maakt van het integreren van cybersoldaten in het Russische leger (DIA 2017).

De belangrijkste inlichtingendienst van Rusland is de FSB. Deze dienst heeft officieel een op het binnenland gerichte taakstelling, maar is ook actief in voormalige Sovjet-landen en daarbuiten (Klimburg 2017). Informatie over de precieze opzet en financiering van de FSB is schaars. De FSB omvat onderdelen die vergelijkbaar zijn met de Amerikaanse NSA. Naast de FSB verdient de GRU een vermelding. Dat is een inlichtingendienst die verbonden is aan het Russische leger, maar een breder mandaat heeft dan de Amerikaanse DIA (Klimburg 2017).

Diverse hackersgroepen zijn in verband gebracht met het Kremlin, zoals Advanced Persistent Threat (APT) 28 en 29 (FireEye 2018). APT 28, ook wel Fancy Bear of Sofacy genoemd, is in verband gebracht met een aanval op het Duitse parlement en speelde een rol bij de cyberaanval op het Democratische Nationale Comité in 2016 (Valance 2017). APT 29, of Cozy Bear, werd door de AIVD in verband gebracht met de cyberaanvallen op de Amerikaanse verkiezingen van 2016 (Modderkolk 2018).

Rusland heeft een groot crimineel circuit op het internet (Klimburg 2017). Zo zou de organisatie Russian Business Network (RBN) in 2007 verantwoordelijk zijn geweest voor 60% van de wereldwijde internetcriminaliteit. In 2012 zou met Russische cybercriminaliteit rond 4,5 miljard dollar zijn verdiend. Het is zeer waarschijnlijk dat de Russische overheid gebruik maakt van deze cyberactoren om indirect aanvallen uit te voeren of gevaarlijke software te ontwikkelen (Klimburg 2017). Deze samenwerking stelt de Russische overheid nog meer in staat om vanuit de schaduw te opereren.

3.2.2 Strategische ontwikkeling

Na de val van de Sovjet-Unie begin jaren ’90 marginaliseerde de rol van Rusland op het wereldtoneel. Voormalige satellietstaten werden zelfstandige naties en grote delen van het ooit machtige Sovjetleger werden afgedankt (DIA 2017). In de jaren die volgden veranderde het land in een oligarchie: een land waar de economische en politieke macht ligt bij een kleine groep Russen rondom de president, Vladimir Poetin (Stoner & McFaul 2015). Zo was de autoritair georganiseerde staat terug, na een korte wereldwijde ‘ontspanning’ eind jaren ’90. En daarmee de controle over de – inmiddels digitale – informatiestroom.

Het beheersen van de digitale informatiestroom was ook om een andere reden aantrekkelijk. In de eerste Tsjetsjeense oorlog (1994-1996) hadden de Russische autoriteiten vergeefs geprobeerd onafhankelijke media af te sluiten en elk bericht van het slagveld te censureren (Giles 2016). Het lukte daardoor niet het beeld te ontkrachten van dappere Tsjetsjenen die vochten tegen kille onderdrukkers met een bovendien zeer verouderd en beschadigd militair apparaat (DIA 2017). Daarom koos Rusland in de jaren 2000 voor een integrale veiligheidsstrategie, waarin informatietechnologie een cruciale rol speelt. Kortweg luidt de doctrine dat Rusland militaire, politieke én economische middelen in naadloze samenhang moet inzetten om de Russische belangen te behartigen (Giles 2016, Conley et al. 2016). De strategie wordt hybride oorlogsvoering genoemd, en de Gerasimov-doctrine, naar het hoofd van de generale staf van het Russische leger (Bartles 2016).

Rusland heeft deze doctrine de afgelopen jaren regelmatig in de praktijk gebracht. Een van de belangrijkste redenen hiervoor is wederom de val van de Sovjet-Unie. Door die val brak de grote door Russen gedomineerde unie uiteen in vele zelfstandige staten, waarin Moskou veel minder te zeggen had. Het Rusland van Poetin wil deze invloed herwinnen, en heeft daarom op vele vlakken geïntervenieerd in de oude satellietstaten (Conley et al. 2016). Dit ging met vallen en opstaan. Zo resulteerde het gewapende conflict met Georgië in 2008 wel tot een Russische overwinning, maar werden tegelijkertijd ernstige tekortkomingen geconstateerd in zowel de conventioneel-militaire als in de informatietechnologische capaciteiten (Giles 2016).

Een andere belangrijke les werd gedurende de verkiezingsprotesten van 2011 en 2012 geleerd. Het Russische leiderschap kwam er toen achter dat de informatieoorlog niet alleen met twitterbots en D-Dos-aanvallen gewonnen kan worden en dat het domineren van online massabewustzijn de betrokkenheid van ‘echte mensen’ vereist, die goed kunnen spreken en gebruik kunnen maken van doordachte argumenten (Giles 2016). Het leidde tot het opzetten van het Internet Research Agency, ook wel het Russische Trollenleger genoemd, een organisatie

van mensen die online propaganda verspreiden, alsmede het opzetten van kanalen zoals RT (voorheen Russia Today), Sputnik en Russia Direct, die met een zweem van objectiviteit overheidspropaganda aan het publieke debat toevoegen. Alle elementen van de Russische strategie kwamen samen in het conflict in Oekraïne. Wederom wilde een oude satellietstaat zich onttrekken aan de Russische invloed, en wederom wilde Poetin daar een stokje voor steken.

De precieze operaties worden tot op de dag van vandaag nog gereconstrueerd - maar de hoofdlijnen zijn duidelijk. Rusland maakte gelijktijdig van verschillende middelen gebruik: het stuurde troepen zonder insigne naar Oost-Oekraïne en de Krim, leverde wapens aan rebellen in Oost-Oekraïne, en dreigde met een grote troepenaanwezigheid (Franke 2015). Vervolgens namen de troepen op de Krim essentiële communicatie-infrastructuur in, zoals telefoonnetwerken en tv-stations, werd er disinformatie gebruikt en ondersteunde RT bepaalde verhalen met fragmenten van afgetapte telefoontjes van bijvoorbeeld Amerikaanse diplomaten. Bovendien gebruikte Rusland cyberwapens om energiecentrales, ziekenhuizen en financiële instellingen aan te vallen en zo de Oekraïense staat verder te destabiliseren.

Het creëerde een moeilijk te ontwarren informatiechaos, waardoor westerse media en bijvoorbeeld de Europese Unie geen zicht hadden op wat zich precies afspeelde, en waardoor politici daar dus ook geen harde conclusies aan konden verbinden (Franke 2015). Ook op 27 juni 2017 werd Oekraïne aangevallen; ditmaal met het NotPetya-virus. Naar schatting duizend organisaties werden geraakt, van banken tot ziekenhuizen; overigens ook ver over de landsgrenzen. De aanval werd door de Amerikaanse regering toegeschreven aan de GRU (Greenberg 2018).

De Russische desinformatie wordt ook buiten de oude satellietstaten verspreid. Soms direct via een kanaal als RT, maar soms ook via valse profielen op sociale media, die berichten massaal of juist gericht doorsturen. Dit brengt ons bij de inmenging van Rusland in de Amerikaanse verkiezingen van 2016. De afgelopen jaren deed de FBI onderzoek naar een mogelijke samenspanning tussen de Russische overheid en de Trump-campagne. Twaalf Russen werden op 13 juli 2018 beschuldigd. In de aanklacht van FBI-aanklager Robert Mueller staat onder meer dat de Russen jarenlang bezig zijn geweest om een verfijnde beïnvloedingscampagne voor te bereiden, en dat daar tientallen miljoenen dollars mee gemoeid waren (District Court of Columbia 2018, Ward 2018).

Het lijkt het erop dat Rusland doorgaat met het verspreiden van desinformatie. Rusland zou zijn pijlen gericht hebben op de Amerikaanse tussentijdse verkiezingen van 2018 (Chan & Nour 2018), en de Franse Gele-Hesjesbeweging (Kool 2019, Avaaz 2019).

3.3 China

3.3.1 In het kort

Het communistische, centraal geleide China heeft sinds 1976 zijn economie geopend voor buitenlandse investeerders (Tisdell 2009). Sindsdien heeft de Chinese economie een ontzagwekkende ontwikkeling doorgemaakt. Vandaag de dag is China de tweede economie ter wereld (Word Bank 2018). Die groei is gepaard gegaan met meer economische vrijheid en internationale samenwerking, maar niet met de politieke vrijheden die westerse landen kennen (Freedom House 2018).

Dit tekent het perspectief van China op digitalisering: de communistische partij wil de sterkste speler zijn in de digitaliserende wereldeconomie, en tegelijkertijd zorgen dat de digitale voortuitgang haar macht niet bedreigt maar juist bestendigt.

3.3.2 Strategische ontwikkeling

De Chinese overheid is bijzonder actief in het inzetten van digitale middelen om de eigen bevolking te sturen en te monitoren (zie ook kader 6). Net als Rusland censureert China online nieuwsomgevingen, en ook sociale media worden scherp in de gaten gehouden (zie bijvoorbeeld McDonald 2012, Hernandez & Mou 2018). Tegen dissidenten wordt onder de regering van president Xi steeds harder opgetreden, bijvoorbeeld door ze te arresteren en op te sluiten (Schell 2016). Bovendien zal de regering in 2020 het ‘sociaal kredietsysteem’ introduceren, dat Chinezen een persoonlijke score geeft (Kobie 2018). ‘Slecht gedrag’, roken waar dat niet mag, al te kritische berichten plaatsen op sociale media en ‘te lang’ gamen kunnen iemands score verlagen. Hoewel nu nog pilotversies getest worden en het definitieve systeem nog niet is ingevoerd, tekenen de consequenties zich al af. Zo zouden mensen met een lage score niet meer mogen vliegen, alleen langzaam internet ontvangen of hun kinderen niet meer naar de beste scholen kunnen sturen.

Zonder digitale technologie is een dergelijk systeem ondenkbaar en onuitvoerbaar: burgers kunnen online nauwgezet in de gaten gehouden worden, en sancties zouden geautomatiseerd kunnen worden opgelegd. Dit systeem lijkt de verwezenlijking te zijn van de overheid als een totalitaire Big Brother, die burgers aanstuurt en monitort op het gebied van vrijwel ieder aspect van het leven.

Kader 6 Offensieve cybercapaciteiten van China

Met de groei van de Chinese economie is China fors meer gaan investeren in het leger: van 31 miljard dollar in 1998 naar 108 miljard dollar in 2008 en naar 228 miljard dollar in 2017 (SIPRI 2018). Het Chinese leger heeft 2 miljoen voetsoldaten. Het wordt stevig gemoderniseerd: luchtvaart, maritieme macht, rakettechnologie en zeker ook cybercapaciteiten worden steeds dominanter (Chase et al. 2015, Klimburg 2017).

Het leger heeft een complexe commandostructuur. Voor de Chinese cybercapaciteiten zijn tenminste drie onderdelen van het Volksbevrijdingsleger (PLA) relevant: 3PLA, 4PLA en de Strategic Support Force (SSF). 3PLA is het Chinese equivalent van de Amerikaanse NSA (zie kader 4), maar heeft zeer waarschijnlijk veel meer personeel; rond de 130.000 3PLA-medewerkers (tegen 35.000 man bij de NSA; schatting Klimburg 2017). Het beschikt over verschillende sub-bureaus, waarvan alleen al het ‘2e bureau’, dat gericht is op Engelstalige inlichtingen en dat wordt gelinkt aan spionageaanvallen op het Amerikaanse ministerie van Defensie, duizenden mensen in dienst heeft (FireEye 2014, Inkster 2016).

4PLA is het legeronderdeel dat gericht is op het uitvoeren van cyberaanvallen in oorlogstijd. Het is het centrale aansturingspunt voor reservisten, milities en private actoren die kunnen bijdragen aan een cyberaanval. Dit is van belang, omdat China, het land met het meeste internetgebruikers, waarschijnlijk over tienduizenden mensen beschikt die een rol kunnen spelen in het opbouwen en uitvoeren van offensieve cybercapaciteit (Klimburg 2017). Denk aan gespecialiseerde hackers aan een universiteit. Deze patriotten spelen ook een centrale rol in de censuur van de Chinese cyberspace en in het verspreiden van propaganda.

Tegelijkertijd streeft president Xi Jinping wel naar modernisering van dit enorme, hybride geheel aan cyberstrijders. Het leger moet directere controle hebben over nog sterkere en meer geavanceerde cybercapaciteiten (Klimburg 2017). In 2015 richtte de Chinese overheid daarom de Strategic Support Force (SSF) op, een onderdeel dat ruimte-, cyber- en elektronische capaciteiten ontwikkelt en implementeert, en zo het Chinese leger in volle breedte ondersteunt (Pollpeter et al. 2017).

De afgelopen twintig jaar is China er in geslaagd een alternatief digitaal domein te creëren. Ook zijn de Chinese internetbedrijven Alibaba en Baidu tot giganten uitgegroeid; ze opereren steeds internationaler (Economist 2017). Westerse bedrijven als Facebook en Google mogen wel zakendoen in China, maar moeten zich aan allerlei voorwaarden houden (McDonald 2012). Meestal voldoen deze bedrijven aan die voorwaarden, ook als ze neerkomen op censuur.

Google werd bijvoorbeeld gevraagd staatsonvriendelijke content weg te filteren uit de zoekresultaten. Aanvankelijk ging Google akkoord, en kon het bedrijf profiteren van de data van het gigantische aantal Chinese internetgebruikers. Maar in 2010 bleek de Chinese overheid cyberaanvallen uit te voeren om, onder andere, de Gmail-accounts van mensenrechtenactivisten te hacken (Branigan 2010). Toen gaf Google Chinese gebruikers, door middel van een omleiding via het relatief vrije Hong Kong, toegang tot zijn ongecensureerde zoekmachine. Binnen enkele maanden was Google niet meer bereikbaar voor Chinese burgers. Sindsdien heeft Google zich geheel uit China teruggetrokken, hoewel het probeert opnieuw toegang te krijgen tot de Chinese markt (zie Deibert et al. 2018).

De Chinese digitale bedrijvigheid gaat niet alleen hand in hand met interne spionage en censuur, maar ook met het bespioneren van buitenlandse staten. China heeft in de loop van de jaren 2000 op grote schaal geprobeerd via digitale infiltratie zowel economische geheimen als staatsgeheimen te stelen (Inkster 2016). Deze operaties wekten in de VS zo veel wrevel op dat president Obama en president Xi in september 2015 afspraken dat hun overheden niet willens en wetens economische cyberspionage zouden uitvoeren en/of ondersteunen (Zetter 2015).

China houdt zich in toenemende mate bezig met een grootschalige en meer militair-georiënteerde opbouw van offensieve cybercapaciteiten (Klimburg 2017). China beschikt vandaag de dag over een enorm leger van cybersoldaten. Het stuurt grote groepen vrijwilligers aan die, bijvoorbeeld in naam van het vaderland, gezamenlijk een D-DoS-aanval in kunnen zetten (zie kader 6).

In het boek *Unrestricted warfare* van twee Chinese kolonels wordt een strategie besproken hoe China technologisch superieure staten zou kunnen verslaan zonder gebruik van conventionele wapens (Qiao & Xiangsui 2015). Dit is precies waar de Chinese strategie op is gebaseerd: conflicten winnen door middel van efficiënte en overweldigende cyberaanvallen, zonder daarbij gebruik te maken van conventionele wapens en fysiek geweld.

Andere landen (naast de VS) rapporteren eveneens cyberaanvallen vanuit China, zoals de regionale rivalen India en Taiwan (Wagstaff 2015, Yu 2018). Het

cybersecuritybedrijf FireEye concludeerde dat de regering tenminste een deel van de vele hackactiviteiten waarschijnlijk ondersteunt. China voert daar vooral cyberspionage uit. Ook rapporteert Taiwan dat China in algemene zin overheidssystemen wil binnendringen, en groeit de vrees dat China de capaciteiten wil opbouwen om fysiek schadelijke cyberaanvallen uit te voeren (Yu 2018).

Ten slotte voert China ook in het buitenland een actieve propagandacampagne, waarbij de nadruk niet ligt op het publiceren van valse berichten die het publieke debat ondermijnen, maar op het verspreiden van een positief beeld van China (Recorded Future 2019). Zo heeft het land voor grote bedragen advertenties ingekocht op Facebook, een platform dat grotendeels wordt geblokkeerd in China zelf (Mozur 2017).

Al met al streeft de regering van China ernaar een digitale supermacht te worden die de touwtjes strak in handen heeft – zowel op militair als op economisch en cultureel gebied.

3.4 Nederland en andere Europese landen

3.4.1 In het kort

In veel opzichten lijkt de digitale ontwikkeling van Nederland en andere Europese landen op die van de Verenigde Staten. Deze landen behoren tot de meest digitaal verbonden landen ter wereld, en hebben een grote en groeiende digitale economische sector. Europese landen hebben daarom cybersecurity hoog op de agenda gezet en versterken hun cyberdefensie en inlichtingendiensten om hun digitale infrastructuur te kunnen verdedigen.

Toch verschillen ze in twee opzichten van de VS. Ten eerste gaan Europese landen verder dan de VS in het reguleren van het digitale bedrijfsleven. Ten tweede werken Europese landen onder meer in EU-verband steeds hechter samen om de cyberveiligheid te bevorderen. Aangezien we deze internationale activiteiten in het volgende hoofdstuk bespreken, zal de beschrijving hiervan iets beknopter zijn. We kijken naar Nederland en geven voorbeelden van Franse, Duitse en Britse ontwikkelingen. Deze landen zijn in Europa van bijzonder belang, vanwege hun economische en, zeker in het geval van Frankrijk en het Verenigd Koninkrijk, militaire macht.

3.4.2 Strategische ontwikkeling

De Europese economieën, en zeker de Nederlandse, zijn sterk gedigitaliseerd. Europese landen vormen al een interessante afzetmarkt voor Amerikaanse giganten als Microsoft, Google en Apple (Europese Commissie 2018a). Bovendien is er veel eigen digitale bedrijvigheid, zoals op het gebied van de financiële technologie. Toch heeft Europa geen cybergigant van de grootte van Facebook of Alibaba ontwikkeld. Dat roept de vraag op wat Europese landen tegenover al deze economische slagkracht zetten. De invloed van grote digitale techbedrijven stuit op weerstand, bijvoorbeeld op het gebied van persoonsgegevens en Facebook (Solon 2018) en op het gebied van AirBnB en de hotelbranche (Coldwell 2014). Op Europees niveau zijn talrijke initiatieven ontplooid om de digitale economie te reguleren. Verschillende daarvan zullen we in het volgende hoofdstuk bespreken.

Kader 7 Offensieve cybercapaciteiten van Europese landen

Nederland, Frankrijk, Duitsland en het Verenigd Koninkrijk bouwen allemaal offensieve cybercapaciteiten op. Zo heeft de Nederlandse overheid in 2014 het Defensie Cybercommando opgericht, dat direct onder de Commandant der Strijdkrachten valt. Het commando beschikte begin 2017 over 80 man; het huidige kabinet wil hier in de toekomst meer in investeren (Rigter 2017, De Telegraaf 2018).

Frankrijk streeft ernaar in 2019 te beschikken over een ‘vierde leger’ van 3.200 cybersoldaten (Pennetier 2017) en Duitsland wil in 2021 beschikken over een defensief gericht legeronderdeel van 13.500 soldaten en medewerkers (O’Conner 2017). Duitsland maakte onlangs ook bekend dat het cyberdefensietechnologie zelf wil ontwikkelen, in plaats van aan te kopen bij buitenlandse bedrijven (Delcker 2018). Het Verenigd Koninkrijk heeft op dit gebied de 77th brigade opgericht, bestaande uit rond de 1.500 reguliere soldaten en reservisten (MacAskill 2015, Sengupta 2015).

Nederland en andere Europese landen hebben ook inlichtingendiensten die offensieve cybercapaciteiten opbouwen. Nederland beschikt over de AIVD en de MIVD. Op de AIVD is in 2013 fors bezuinigd; het budget werd teruggebracht van 195 naar 125 miljoen euro (Versteegh 2017). Maar in de jaren erna is, mede vanwege de toenemende cyberdreigingen, het budget weer uitgebreid, uiteindelijk tot ongeveer 250 miljoen euro (Rijksbegroting 2018). De dienst wil in de komende jaren beschikking hebben over tussen de 2.000 en 2.200 fte’s, en zet steeds meer in op cybercapaciteit. Bij de MIVD is eenzelfde trend te zien: er wordt steeds meer in cybercapaciteit geïnvesteerd en het budget is opgelopen tot ongeveer 100 miljoen euro in 2018 (Rijksbegroting 2018). Ter vergelijking: de Britse GCHQ, de equivalent van de AIVD, ontving in 2013 rond de 1 miljard pond (1,11 miljard euro) en had zo’n 6.100 mensen in dienst (Hopkinds et al. 2013).

In de omgang met offensieve cybercapaciteiten is eenzelfde combinatie van enerzijds meedoen en anderzijds normeren zichtbaar: Europese landen als Nederland, Frankrijk, het Verenigd Koninkrijk en Duitsland willen net als de Verenigde Staten het vermogen hebben om zich te kunnen verweren in cyberconflicten. En ook in de Europese Unie is een lucratieve markt ontstaan voor

offensieve cybercapaciteiten, waar allerlei bedrijven hun diensten aanbieden (Stockton & Golabek-Goldman 2013). Tegelijkertijd willen deze landen hun offensieve capaciteiten inbedden in heldere nationale en internationale regelkaders (UK Government 2016, Federal Ministry of the Interior 2011, Ministerie van Buitenlandse Zaken 2017, France Diplomatie 2018, Mackenzie 2019).

Een voorbeeld hiervan is de nieuwe Nederlandse Wet op de Inlichtingen- en Veiligheidsdiensten (WIV). Deze wet vergroot de bevoegdheden van de inlichtingen- en veiligheidsdiensten, maar bevat ook waarborgen, bijvoorbeeld op het gebied van hackbevoegdheden van de AIVD. Bij de invoering van de wet ontstond veel discussie in de samenleving. Die leidde onder meer tot het organiseren van een raadgevend referendum waarin voor of tegen de wet gestemd kon worden. Kiezers stemden in kleine meerderheid tegen, waarna het kabinet enkele aanvullende waarborgen toezegde en de wet invoerde. Dit proces illustreerde dat de Nederlandse politiek de normenkaders op het gebied van offensieve cybercapaciteiten serieus neemt, en dat het mogelijk is om rond deze thematiek een vruchtbaar publiek debat te organiseren.

De nadruk op normontwikkeling kenmerkt ook de Nederlandse inbedding van offensieve cybercapaciteiten in het leger. Zo is er een militaire cyberdoctrine ontwikkeld die periodiek wordt bijgewerkt. Ook publiceert het ministerie van Defensie een cyberstrategie (Ministerie van Defensie 2018). Maar de normontwikkeling dient, wat Nederland betreft, niet alleen op nationaal niveau, maar juist ook op het niveau van internationale samenwerkingsverbanden, zoals de NAVO en de VN, plaats te vinden (Ministerie van Buitenlandse Zaken 2017).

Europese inlichtingendiensten, zoals die van het VK en Frankrijk, zijn steeds meer in staat om digitale systemen te hacken, informatie te verzamelen en cybersabotage uit te voeren (zie kader 7). Deze capaciteiten worden ook actief ingezet. Uit de Snowden-onthullingen bleek bijvoorbeeld dat de Britse dienst GCHQ, in samenwerking met de Amerikaanse NSA, veel e-mailverkeer aftapte. Verder zou de Nederlandse AIVD essentiële informatie over de daders van de aanvallen op de Amerikaanse verkiezingen van november 2016 hebben doorgespeeld aan hun Amerikaanse collega’s (Modderkolk 2018).

Er is geen aanwijzing dat Nederland, Duitsland, Frankrijk of het VK desinformatiecampagnes opzetten, maar hier zetten we een kanttekening bij. Uit de Snowden-onthullingen bleek dat de GCHQ verschillende tools heeft ontwikkeld om bijvoorbeeld nepmails aan te maken of online polls te beïnvloeden (NBC 2014). Het is dus maar de vraag of de grote Europese landen als één man het verspreiden van desinformatie afzweren.

Ten slotte lijken de onderzochte staten geen ernstig saboterende cyberaanvallen uit te voeren. Ook hier is het natuurlijk mogelijk dat sommige aanvallen niet gerapporteerd worden. Onlangs nog dreigde Jeremy Fleming, de directeur van de GCHQ, de vergiftiging van ex-KGB agent Sergei Skripal en zijn dochter te vergelden met offensieve cybercapaciteiten (Binding 2018). Nederland, Frankrijk, Duitsland en het VK bouwen het vermogen om cybersabotage uit te voeren steeds verder op, maar hebben dit arsenaal nog niet op een duidelijk waarneembare manier ingezet.

3.5 De internationale opstelling van de staten: een overzicht

We zullen nu een kort overzicht geven van de activiteiten van de besproken staten.

De **Verenigde Staten** zijn zeer actief in het verwerven van inlichtingen over andere staten, en proberen over een structurele en verborgen toegang tot vijandelijke digitale netwerken te beschikken. De VS hebben voor zover bekend geen doelgerichte desinformatiecampagnes gevoerd in het buitenland. De tijd zal uitwijzen of de opstelling van de huidige regering uitmondt in het internationaal verspreiden van desinformatie. De Stuxnet-operatie bewijst dat de VS met cybermiddelen ernstige fysieke schade hebben berokkend (Rid 2012). Ook de aanval op de Noord-Koreaanse digitale infrastructuur, in de nasleep van de Sony-hack, wijst op de bereidheid van de VS om cybersabotages uit te voeren. Maar er zijn ook tekenen dat de regering en de defensieorganen worstelen met dit vermogen. De laatste tijd zijn er signalen dat de VS wel degelijk zwaardere cybersabotage wil inzetten als het land te veel wordt geprovoceerd, bijvoorbeeld door Iran.

Wat **Rusland** betreft valt te concluderen dat zowel in de binnenlandse politieke processen, als in de politieke processen van andere staten, de Russische overheid actief bezig is de rechtsstaat en de vrije democratie te ondermijnen. Rusland maakt van spionage en desinformatie gebruik om een democratische proces te beschadigen en de samenleving te destabiliseren. Maar in de eigen regio gaat Rusland verder: daar is cybersabotage meermaals ingezet om ernstige fysieke schade toe te dienen, bijvoorbeeld bij de aanvallen in Oekraïne. De cyberactiviteiten van Rusland in Oekraïne vallen samen met conventionele militaire inzet.

Ook **Chinese** overheidsdiensten proberen zeer waarschijnlijk op grote schaal de systemen van andere staten te hacken en hebben zich schuldig gemaakt aan

economische spionage. Ook gebruikt de Chinese overheid de digitale omgeving om binnen China desinformatie te verspreiden; de buitenlandse informatiecampagne is vooral gericht op het verspreiden van een positief beeld van China. China wil bovendien in staat zijn om zwaardere cybersabotage uit te voeren en zelfs een oorlog te winnen. Het heeft echter, in tegenstelling tot Rusland, deze capaciteiten nog niet of nauwelijks uitgeprobeerd.

Ook de inlichtingendiensten van **Nederland en andere Europese landen zoals het VK, Frankrijk en Duitsland** voeren cyberspionage uit. Op het buitenland gerichte desinformatiecampagnes lijken vooralsnog niet of nauwelijks voor te komen, hoewel de Britse GCHQ het vermogen zulke campagnes uit te voeren al heeft ontwikkeld. Voorbeelden van saboterende Europese hackaanvallen met serieuze fysieke consequenties zijn niet te vinden. Dit sluit niet uit dat dergelijke aanvallen, of minder ernstige cybersabotage, wel plaatsvinden. Verder is er een schaalverschil tussen, bijvoorbeeld, de inlichtingenactiviteiten van de Britse GCHQ en de Nederlandse AIVD. Er zijn tot slot geen bekende voorbeelden van cyberaanvallen die duidelijk hebben geleid tot een oorlogssituatie.

3.6 De cyberescalatieladder

3.6.1 Het informatieconflict

Uit het overzicht vallen een aantal zaken op. Staten integreren hun offensieve cybercapaciteiten steeds professioneler in hun militaire en inlichtingenorganisatie. Diverse landen durven de militaire grootmacht de Verenigde Staten voortdurend aan te vallen. Maar het meest opvallend is dat deze operaties nooit leiden tot oorlogsverklaringen. Zo heeft Rusland herhaaldelijk Amerikaanse vitale infrastructuur bestookt, en verkeert het toch niet in een staat van oorlog met de VS (Klimburg 2017). China bespioneert andere landen al meer dan een decennium, maar drijft tegelijkertijd vreedzaam handel met ze.

Cyberaanvallen gebeuren dan ook meestal in een situatie tussen oorlog en vrede in. Ze scheppen een nieuwe dimensie van strijd en belangenbehartiging, die wij het **informatieconflict** noemen. De doelen in dit informatieconflict lopen uiteen:

- soms zoekt een staat economische voordelen door te spioneren;
- soms wil een staat juist het militaire slagveld in zijn voordeel prepareren; en
- soms wil een staat de politieke besluitvorming in een andere staat onder druk zetten of manipuleren.

Het informatieconflict heeft één cruciaal kenmerk: burgers liggen in het informatieconflict onder vuur. Als een buitenlandse mogendheid toegang wil krijgen tot het digitale systeem van een bedrijf, kan dat door het thuisnetwerk van een medewerker te hacken, en te hopen dat hij daar zijn werkcomputer op aansluit. Evengoed richten desinformatiecampagnes zich op de informatievoorziening van burgers, onder meer door bepaalde politici valselijk te beschuldigen en kiezers te manipuleren. Ten slotte hebben, bedoeld of onbedoeld, civiele voorzieningen last van cyberaanvallen – denk aan het bancaire verkeer, de energiesector en zelfs ziekenhuizen – en raken de gevolgen van een aanval de burgers.

Cyberaanvallen treffen zo het vitale hart van de samenleving. Hier dient de vergelijking met conventionele oorlogsvoering zich aan: een van de hoofddoelstellingen van het oorlogsrecht is juist om civiele voorzieningen te vrijwaren, en te zorgen dat strijdende partijen zich uitsluitend richten op deelnemers aan het militaire conflict. Dit roept de vraag op of cyberaanvallen niet aan dezelfde regels zouden moeten voldoen. Op deze vraag gaan we in hoofdstuk 4 nader in.

3.6.2 Cybervrede en cyber-fysieke oorlogsvoering

Het informatieconflict is te beschrijven als een conflict tussen vrede en oorlog in, en heeft daarmee gevolgen voor hoe we nadenken over vredestijd en oorlogstijd. Vredestijd is te onderscheiden van **cybervrede**, en oorlog kunnen we begrijpen als **cyber-fysieke oorlog**.

In een tijd van cybervrede is het namelijk niet alleen vredestijd, maar is er ook geen informatieconflict met een bepaalde staat. Landen voeren geen cyberspionage bij elkaar uit en zetten geen cybermiddelen in om schade te berokkenen in een ander land. Ook zijn er geen desinformatiecampagnes. De nadruk ligt in deze situatie op het versterken van de cybersecurity. Een land kan er zelfs voor kiezen zich pacifistisch op te stellen, geen offensieve vermogens op te bouwen en bijvoorbeeld zo veel mogelijk *zero day*-kwetsbaarheden vrij te geven. Maar staten kunnen ook cybersoldaten trainen en wapens aanschaffen. Het vermogen offensieve cybercapaciteiten op te bouwen in vredestijd is echter beperkt: het winnen van inlichtingen over de cybercapaciteiten en -systemen van de tegenstander is nodig voor zowel het opzetten van een eigen verdediging als voor het creëren van offensieve capaciteit.

Ook ons begrip van oorlog verdient nuancering. In oorlogstijd zullen offensieve cybercapaciteiten waarschijnlijk een belangrijke rol spelen: steeds meer militair materieel digitaliseert, en het kan bijvoorbeeld zeer voordelig zijn om de luchtafweer van de tegenstander door middel desinformatie om de tuin te leiden.

Daarom is het zinvol om te spreken van **cyber-fysieke oorlogsvoering**, waarbij digitale toepassingen worden geïntegreerd in het conventionele oorlogsarsenaal, zoals op afstand bestuurbare drones die explosieven kunnen werpen.

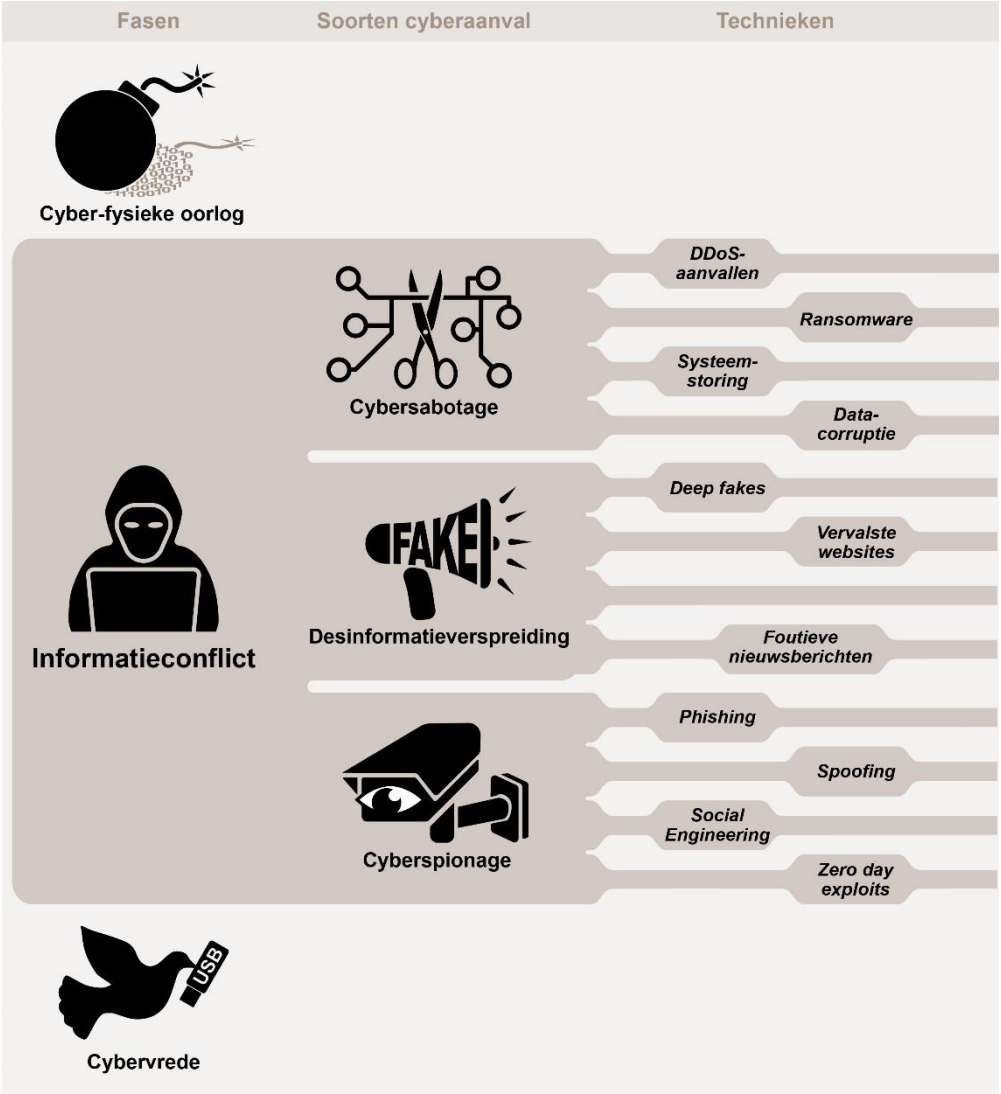
Tabel 2 De cyberescalatieladder

Trede	Situatie	Intentie	Schade	Kenmerk conflict
3	**Cyber-fysieke oorlog** *- in oorlogstijd*	Militaire overwinning	Schadeberokkening gedefinieerd als gewapende aanval	Integratie cyber in militaire operaties
2	**Informatieconflict** *- in vredestijd*	- wapenexperimenten, - politieke druk, - voorbereiden digitaal slagveld, - politieke destabilisatie, - versterken eigen cyberverdediging	Ernstige fysieke schadeberokkening, ongewenste verspreiding van informatie, manipulatie door desinformatie	Nieuwe vorm van conflict
1	**Cybervrede** *- in vredestijd*	Vrede / neutraliteit	Geen schade	Streven naar blijvende vrede

Samenvattend spreken we van een **cyberescalatieladder**. Deze ladder omvat de drie fases van internationale verhoudingen die zijn genoemd: een fase tussen staten van cybervrede, informatieconflict en cyber-fysieke oorlogsvoering (zie tabel 2). Deze fases zijn te zien als tredes. Van beneden naar boven wordt het steeds gevaarlijker voor de samenleving: er kan een escalatie plaatsvinden van vrede naar informatieconflict, en van informatieconflict naar cyber-fysieke oorlogsvoering.

Gegeven de handelingen en strategieën van de onderzochte staten, is de huidige internationale situatie het beste te omschrijven als een informatieconflict. In figuur 3 hebben we het informatieconflict grafisch vormgegeven.

Figuur 3 Het informatieconflict



3.7 Conclusie

Dit hoofdstuk gaf een schets van de internationale omstandigheden op het gebied van offensieve cybercapaciteiten, op basis van een inventarisatie van grootmachten en Europese landen. Dit zijn de belangrijkste bevindingen:

- De traditionele militaire grootmachten de Verenigde Staten en Rusland, de nieuwe wereldmacht China en Europese landen erkennen dat de digitale wereld een nieuwe, vijfde dimensie van conflict en oorlog vormt. Deze landen willen allemaal in staat zijn om in de digitale wereld aanvallen af te slaan en zelf aanvallen uit te voeren. **Daarom is er een wereldwijde opbouw van**

offensieve cybercapaciteiten, en kunnen we spreken van een militarisering van de digitale wereld. Alle besproken landen hebben de afgelopen jaren intensief het vermogen opgebouwd om cyberspionage en –sabotage uit te voeren, en de meeste hebben het vermogen verworven om desinformatie te verspreiden.

- **Deze opbouw kan getypeerd worden als een wapenwedloop**. China, Rusland, de VS en Europese landen willen cyberaanvallers kunnen aftroeven en over superieure offensieve cybercapaciteiten beschikken. Dit heeft tot een wedloop geleid, waarbij de opbouw van capaciteiten in, bijvoorbeeld, China, aanleiding is voor de VS om verdere capaciteiten op te bouwen, wat weer aanleiding geeft voor China om betere cyberwapens aan te schaffen, etc.

- **Vrijwel iedere staat voert uitgebreide cyberspionage uit, waarbij in sommige gevallen zelfs bij bondgenoten heimelijk inlichtingen worden gewonnen.** China valt in dit opzicht op door de hoge mate van economische spionage. Deze vele hackaanvallen zijn allesbehalve schadeloos – ze vereisen het verbeteren van veiligheidsmaatregelen, het dichten van softwarelekken, etcetera. Dat kan afhankelijk van de aanval zeer kostbaar zijn.

- **Sommige landen, en met name Rusland, lanceren desinformatiecampagnes in andere landen.** Het is ook duidelijk dat autoritaire, antidemocratische regimes zoals de regeringen van China en Hongarije binnenlandse desinformatiecampagnes voeren – en ook de regering van de VS verspreidt geregeld desinformatie. Maar het is de vraag of deze campagnes ook welbewust ingezet worden tegen en in andere staten.

- **Het is aannemelijk dat Rusland en de VS zware cybersabotage hebben uitgevoerd.** Met name de NotPetya-aanval in Oekraïne en de Stuxnet-aanval in Iran geven aanleiding dit denken, hoewel de staten deze aanvallen niet hebben bevestigd. China en Europese landen lijken niet of zelden tot zware cybersabotage over te gaan – of doen dit effectief buiten zicht. Ten slotte ontstijgen de Russische operaties in Oekraïne het informatieconflict, aangezien ze samenvallen met conventionele militaire aanvallen.

- **De grote staten kennen verschillende strategische perspectieven**. Zo probeert Rusland, een staat die zelf geen werkende democratische rechtsorde heeft, buitenlandse democratieën te destabiliseren, en het publieke debat met onwaarheden te vervuilen. De VS en onderzochte Europese staten als Duitsland en Frankrijk zien zichzelf juist als de beschermers van die democratische rechtsorde. China is ten slotte wat informatiebeheersing en propaganda betreft voornamelijk intern gericht, en heeft naast het opbouwen

van defensiecapaciteiten een nadruk op economische spionage gelegd. **Geen van de onderzochte staten omarmt een expliciet vredesgericht perspectief**, dat erop is gericht om zo veel mogelijk te blijven handelen op de trede van cybervrede, weinig te spioneren en weinig offensieve cybercapaciteiten op te bouwen.

- **Burgers en civiele voorzieningen vormen centrale doelen van cyberaanvallen**. Van desinformatiecampagnes tot het infiltreren van energiecentrales en het bestoken van de financiële dienstverlening: burgers vormen een belangrijk doelwit van cyberaanvallen. Door burgers te misleiden, door hun geheimen te stelen en door hun voorzieningen te frustreren, hopen staten in andere landen invloed uit te kunnen oefenen.

- **Een losstaande cyberoorlog bestaat niet**. In ons onderzoek zijn we geen enkele situatie tegengekomen waarbij een losstaande cyberaanval gevolgd werd door een door landen uitgesproken staat van oorlog.

4 Internationale samenwerking voor een veilige en vrije digitale wereld

Dit hoofdstuk brengt in kaart op welke wijze Nederland en de eerder besproken landen met elkaar hebben samengewerkt voor een veilige en vrije digitale wereld. We kijken naar de belangrijkste internationale samenwerkingsverbanden, zoals de NAVO, de EU en de Verenigde Naties. Eerst bespreken we de belangrijkste wereldwijde organisaties en vervolgens kijken we naar de regionale verbanden. Ook hier zullen we een schets geven van de omgeving waarin Nederland zich bevindt. We streven niet naar een totaalbeeld van alle internationale initiatieven.

4.1 Wereldwijde organisaties

Diverse internationale organisaties dragen bij aan de internationale cybersecurity en cybervrede. We noemen de belangrijkste:

- de Verenigde Naties (VN);
- de Internationale Telecommunicatie-Unie (ITU);
- publiek-private wereldwijde verbanden, zoals
    a. de International Multilateral Partnership Against Cyber Threats (IMPACT);
    b. de Internet Corporation for Assigned Names and Numbers (ICANN);
    c. het Global Forum on Cyber Expertise;
    d. de Paris Call for Trust and Security in Cyberspace;
    e. het Cyber Security Tech Accord;
    f. het Global Forum on Cyber Expertise; en
    g. het mondiale Forum of Incident Response and Security teams (FIRST).

4.1.1 Verenigde Naties (VN)

De Verenigde Naties vormen een voor de hand liggend forum om wereldwijd geldende afspraken over offensieve cybercapaciteiten te maken. Ze hebben dat de afgelopen jaren ook geprobeerd.

Sinds 2001 zijn, aanvankelijk op initiatief van Rusland en vanuit het **Disarmament and International Security Committee**, verschillende edities ingesteld van de ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (kortweg de **UN GGE**).

Deze groep bestaat uit vertegenwoordigers van 15 staten, die samen geografisch representatief zijn voor de hele wereld. Het doel van de groep is om een consensus te bereiken over de principes, maatregelen en normen die landen moeten doorvoeren op het gebied van de omgang met informatietechnologie in de veiligheidscontext.

De groep heeft om de paar jaar een nieuw mandaat gekregen, en had sinds 2001 wisselende successen. Tussen 2009 en 2015 leek de UN GGE in opeenvolgende edities goede voortgang te boeken. Zo werd gesteld dat landen malafide cyberactiviteiten in hun territorium niet mogen toestaan, en dat landen met cybercapaciteiten kritieke infrastructuur niet mogen aanvallen, tenzij het internationaal recht dit toestaat (bijvoorbeeld als het land het slachtoffer is van een gewapende aanval) (UN GGE 2015). Hoewel het om vrijwillige afspraken gaat, geven ze steeds meer richting aan verantwoord staatsgedrag in de digitale omgeving.

Toch is er sinds 2015 weinig vooruitgang geboekt. De vijfde editie van de UN GGE slaagde er in 2017 niet in een rapport met overeengekomen afspraken naar de Algemene Vergadering van de VN te sturen. Het heikele punt lag in de concrete toepassing van het internationale recht, en in het bijzonder het internationaal humanitair recht, op cyberoperaties (Soesanto & D'Incau 2017). Zo wilden de Verenigde Staten afspreken dat een land dat een cyberaanval ondergaat, gerechtigd is om terug te slaan. Dit voorstel viel in slechte aarde bij Cuba, en waarschijnlijk ook bij Rusland en China. Cuba waarschuwde voor de militarisering van de cyberspace, en stelde dat de toepassing van het internationaal humanitair recht een oorlogsscenario in de cyberspace zou legitimeren. Het zou kunnen dat Rusland en China de superieure cybercapaciteiten van de VS vreesden, en liever onder de radar, zonder al te veel repercussies, hun eigen capaciteiten wilden opbouwen en uitproberen. Hoe het ook zij, door dit meningsverschil werd veel vooruitgang teniet gedaan, aangezien de eerdere afspraken nu ook op losse schroeven staan. De alom gedeelde conclusie luidt dat de normontwikkeling op het niveau van de Verenigde Naties tot stilstand is gekomen (Soesanto & D'Incau 2017).

De VN kent ook andere fora waar cybersecurity wordt onderzocht en besproken, en die resoluties kunnen voorleggen aan de algemene vergadering.

- Het **Economic and Financial Committee** heeft bijvoorbeeld in 2002, 2003 en 2009 resoluties voorgesteld om een 'mondiale cultuur van cybersecurity' te bevorderen.
- Het **Social, Humanitarian and Cultural Committee** heeft vooral privacy-kwesties geagendeerd.

- De **Economic and Social Council** geeft steeds meer aandacht aan het bestrijden van cybercriminaliteit (UN ECOSOC 2011).
- Zaken van internationale vrede en veiligheid worden natuurlijk ook besproken in de **Veiligheidsraad**.

Al deze fora hebben echter geen concretere aanknopingspunten geboden voor de omgang met statelijke cybercapaciteiten dan de voorstellen die zijn gedaan door de UN GGE.

4.1.2 Internationale Telecommunicatie-Unie (ITU)

De Internationale Telecommunicatie-Unie (ITU) is een speciaal agentschap van de VN dat zich richt op informatie- en communicatietechnologie. 193 staten zijn lid, en ongeveer 700 belangrijke spelers uit de IT-sector participeren in de organisatie. De ITU heeft officieel drie taken:

1. het toewijzen van radiofrequenties en het reguleren van satelliettechnologie;
2. het ontwikkelen van ICT-standaarden; en
3. het bevorderen van de toegang tot ICT (ITU 2018).

Vanuit de ITU zijn diverse initiatieven ontplooid om de wereldwijde cyberveiligheid te bevorderen.

In 2007 lanceerde de ITU de **Global Cybersecurity Agenda** (GCA), een project dat vertrouwen en veiligheid moet bevorderen in de digitale context (ITU 2018). De GCA moet onder meer leiden tot het verzamelen en bespreken van juridische en technische maatregelen, en het opzetten van internationale samenwerking. Om de GCA meer vorm te geven is een High-Level Expert Group (HLEG) opgericht, die weer bestaat uit cybersecurityexperts uit de hele wereld. De HLEG bracht bijvoorbeeld in 2008 een rapport uit met vele initiatieven om cybersecurity te verbeteren (ITU 2008). De HLEG faciliteert vooral een uitwisseling van goede ideeën, het stelt niet voor bepaalde maatregelen universeel op te leggen.

ITU organiseert ook het jaarlijkse **World Summit on the Information Society Forum** (WSIS-forum). Het doel van de bijeenkomst is zeer breed: het toegankelijk maken van ICT voor alle mensen, waar ook ter wereld, en het in goede banen leiden van die ontwikkeling. In deze context wordt op de WSIS-fora cybersecurity ook besproken. Het WSIS-forum verwelkomt een groot aantal participanten uit civil society, het bedrijfsleven en overheden en is één van de belangrijkste bijeenkomsten in het jaar op het gebied van ICT-governance.

De ITU houdt ook het niveau van cyberveiligheid van landen bij. Zo stond volgens de ITU in 2017 Nederland op de zeventiende plaats op een internationale ranglijst voor cyberveiligheid, de **Global Cybersecurity Index** (ITU 2018). De internationale lijst van de GCI rangschikt 193 landen, die beoordeeld worden op onderdelen als nationaal beleid, juridische aanpak en de aanwezigheid en expertise van organisaties die zich bezighouden met cyberveiligheid.

Ten slotte ondersteunt de ITU nationale **Cyber Emergency Incident Response Teams** (CERT's), biedt het landen hulp bij wetgevingsvraagstukken rondom cyberveiligheid, en informeert het ontwikkelingslanden over cybercriminaliteit (zie ook hieronder onder FIRST).

4.1.3 Publiek-private wereldwijde verbanden

International Multilateral Partnership Against Cyber Threats (IMPACT)
De International Multilateral Partnership Against Cyber Threats (IMPACT) is de eerste door de Verenigde Naties gesteunde cybersecurity-alliantie. In het kader van een samenwerkingsovereenkomst heeft IMPACT de taak om cybersecuritybijstand en ondersteuning te bieden aan de 193 lidstaten van de ITU en aan andere organisaties binnen de VN (IMPACT 2018).

Met een totaal van 152 landen die nu formeel deel uitmaken van de ITU-IMPACT-coalitie, en met sterke steun van multinationals, partners uit de academische wereld en internationale organisaties, is IMPACT de grootste cybersecurity-alliantie in zijn soort.

Internet Corporation for Assigned Names and Numbers (ICANN)
De Internet Corporation for Assigned Names and Numbers oefent misschien wel de belangrijkste taak in de digitale wereld uit: het beheren van het zogenoemde Domein Naam Systeem (DNS, ICANN 2018a). Dit systeem wordt omschreven als het adressenboek van het internet, dat alle domeinnamen registreert en ervoor zorgt dat als iemand een bepaalde naam of een bepaald nummer invoert in zijn browser, de browser daadwerkelijk naar het juiste adres navigeert (Klimburg 2017).

Het staat buiten kijf hoe essentieel deze dienst is voor het functioneren van het internet; als deze navigatie verstoord wordt is surfen onmogelijk. En als kwaadwillenden de navigatie verstoren, kunnen gebruikers ineens naar andere sites gestuurd worden. De cyberveiligheid van dit systeem heeft daarom voor ICANN zeer hoge prioriteit. In 2010 introduceerden ICANN en de Amerikaanse overheid verbeterde veiligheidsextensies, die sindsdien zijn overgenomen door vele belangrijke internetdomeinen, zoals .com en .de (ICANN 2018b).

ICANN is een veelzijdige. zogenoemde multistakeholderorganisatie, waarin het bedrijfsleven, de publieke sectoren, overheden, technologische experts en allerlei burgerorganisaties vertegenwoordigd zijn (ICANN 2018a). De gedachte is dat als het internet iedereen toebehoort, iedereen ook *bottom-up* moet kunnen participeren in het beheer van het internet. Sinds kort is ICANN ook een geheel onafhankelijke organisatie. De autoriteit om het Domein Naam Systeem te beheren was gebaseerd op het IANA-contract tussen ICANN en de Amerikaanse overheid (ICANN 2018a). Hierdoor was, in zeker zin, het internet meer van de Verenigde Staten dan van andere staten. Maar in oktober 2016 is de DNS-bevoegdheid na een lang proces geheel overgedragen aan ICANN.

Niet alle staten zijn even enthousiast over de brede maatschappelijke inbedding van de DNS-autoriteit. Zo hebben Rusland en China voorgesteld om de bevoegdheid over te dragen aan de ITU, waardoor staten een sterkere rol krijgen in het beheer van het internet, en bijvoorbeeld, nog beter dissidenten kunnen monitoren (Klimburg 2017). Maar dit scenario is sinds het opgeven van de DNS-bevoegdheid door de Amerikaanse overheid zeer onwaarschijnlijk geworden. Toch zien Rusland en China de huidige *governance*-situatie als voor hun nadelig en Westers georiënteerd (Klimburg 2017). Ze zoeken daarom naar alternatieven voor ICANN. Rusland zou samen met de andere zogenoemde BRICS-landen Brazilië, India, China en Zuid-Afrika een eigen internet willen ontwikkelen, met een eigen DNS-systeem (UAWIRE 2017). Dit zou, volgens de Russische overheid, hun digitale capaciteiten minder kwetsbaar maken voor Westerse aanvallen.

Paris Call for Trust and Security in Cyberspace

Op 12 november 2018 werd tijdens een conferentie in Parijs de Paris Call for Trust and Security in Cyberspace gepubliceerd, een document dat uitgangspunten formuleert voor een veilig cyberspace (France Diplomatie 2018, Matsakis 2018). Het stelt expliciet dat het internationaal recht van toepassing is op informatie- en communicatietechnologie, en onderstreept het belang van de normen die op VN-niveau zijn ontwikkeld. Hoewel het document niet de status heeft van een bindend internationaal verdrag, geven de ondertekenaars deze normen van verantwoord staatsgedrag zo weer meer autoriteit. Het UN GGE-proces was immers stil komen te liggen. Ook zouden de onderhandelingen die met dit document zijn begonnen kunnen uitmonden in bindende internationale afspraken.

Het document spreekt zich onder andere uit tegen terug-hacken door niet-statelijke actoren, pleit voor het tegengaan van de proliferatie van gevaarlijke ICT-tools, en kondigt nieuwe bijeenkomsten aan in 2019 om de uitgangspunten verder te ontwikkelen. Het document is ondertekend door meer dan 50 staten, waaronder

Frankrijk, het Verenigd Koninkrijk, Nederland, Duitsland, Canada, en Japan, maar ook vele Afrikaanse en andere Aziatische landen.

Verschillende belangrijke landen hebben de Paris Call for Trust and Security in Cyberspace níet ondertekend, zoals China, Iran, Israël, de Verenigde Staten, Rusland en Noord-Korea. Dit is veelzeggend: juist deze landen hebben zeer uitgebreide offensieve cyberprogramma's en hebben deze ook actief ingezet. Het geeft aan dat hoewel er een groeiende consensus bestaat over de noodzaak offensieve cybercapaciteiten te reguleren, een daadwerkelijk wereldwijde aanpak, waarin juist ook de huidige cybergrootmachten samenwerken, ver weg is.

Ten slotte hebben ook tal van maatschappelijke organisaties en universiteiten zich bij de Paris Call aangesloten. Het akkoord wordt daarmee ondersteund door een groot gedeelte van de belangrijke spelers in het cyberdomein.

Het Cybersecurity Tech Accord

De Paris Call is ook breed omarmd door het internationale bedrijfsleven. Zo wordt het document ondersteund door de ondertekenaars van het Cybersecurity Tech Accord (CTA 2018). Dit is een samenwerkingsakkoord tussen meer dan 60 bedrijven die wereldwijd actief zijn, waaronder Microsoft, Facebook, Dell, en KPN. Ook hebben bedrijven als Google en Samsung de Paris Call onderschreven.

Het Cybersecurity Tech Accord bevat een set gemeenschappelijke beloftes die consequenties hebben voor de manier waarop deze bedrijven zich verhouden tot overheden. Neem de belofte om overheden nooit te helpen cyberaanvallen te lanceren tegen onschuldige burgers en bedrijven, of de belofte om hun producten te beschermen tegen heimelijke beïnvloeding en sabotage. Hoewel de impact en precieze betekenis van het akkoord in de praktijk moeten blijken, zou deze samenwerking het vermogen van overheden kunnen aantasten om met hulp van bedrijven spionage- en sabotageoperaties op te zetten. In meerdere passages van het akkoord klinkt de boodschap door dat de bedrijven zich bewust zijn van de recente internationale ontwikkelingen, en zo min mogelijk betrokken willen worden bij de statelijke opbouw van offensieve cybercapaciteiten.

Het akkoord stoelt op 4 kernprincipes: *strong defense*, *no offence*, *capacity building* en *collective response*. Vooral de eerste twee zijn tekenend voor de positiebepaling van de bedrijven.

Global Forum on Cyber Expertise

Het Global Forum on Cyber Expertise is een samenwerkingsorganisatie van overheden, bedrijven en maatschappelijke organisaties die is voortgekomen uit de vierde editie van de Global Conference on Cyber Space, in 2015 gehouden in Den

Haag. Deze organisatie wil wereldwijd de cybercapaciteit en -expertise verbeteren, waaronder het bevorderen van toegang tot internet, het bewaken van online rechten en het bieden van cyberveiligheid. Deze ambities zijn uiteengezet in de 'Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building' (GFCE 2017).

De activiteiten van de GFCE draaien met name om kennisuitwisseling. De organisatie blijft de jaarlijkse conferentie organiseren en heeft specifieke werkgroepen die gericht zijn op een element van cybersecurity, zoals cybercrime, het beschermen van vitale infrastructuur en het ontwikkelen cyber securitystandaarden.

Forum of Incident Response and Security Teams (FIRST)
Het Forum of Incident Response and Security Teams (FIRST) is een wereldwijd samenwerkingsverband voor Computer Emergency Response Teams (CERT's) of Cyber Emergency Incident Response Teams (CSIRT's) (FIRST 2018). Deze teams worden ook wel de 'brandweermannen van het internet' genoemd, omdat ze bij grote incidenten te hulp schieten om digitale systemen weer operationeel te maken. Ze komen zowel uit de publieke als de private sector en kunnen bij FIRST leren van *best practice*-documenten, en ze kunnen technische colloquia en de jaarlijkse conferentie bijwonen.

De CERT van het Nederlandse ministerie van Defensie, DefCERT, heeft zich bij FIRST aangesloten, net als onder meer de teams van ING, KPN, Rabobank en SIDN.

4.2 Regionale organisaties

Regionale verbanden zijn voor Nederland minstens zo belangrijk als mondiale organisaties en samenwerkingen, in het bijzonder omdat Nederland internationaal veelal opereert binnen EU- en NAVO-verband. We bespreken ook de Shanghai Cooperation Organisation (SCO), de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE), het Five Eyes-samenwerkingsverband en SIGINT Seniors.

4.2.1 Europese Unie (EU)

Cybersecurity is een centraal thema in de algemene veiligheidsstrategie van de Europese Unie, waarover de Europese Commissie diverse strategische documenten heeft gepubliceerd (EC 2013). Meer concreet stelde de hoge vertegenwoordiger van de unie voor buitenlandse zaken en veiligheidsbeleid in april

2016 acties voor die Europa weerbaar moet maken tegen hybride dreigingen, waar cyberaanvallen een centraal onderdeel vanuit maken (EC 2016). In totaal noemt het document 22 acties, en ondertussen is een behoorlijk aantal van die 22 in concreet beleid omgezet.

We lopen de vier EU-initiatieven langs die het meest relevant zijn voor cybersecurity:

1. de in 2016 aangenomen Netwerk- en Informatiebeveiligingsrichtlijn (NIB);
2. de in 2018 voorgestelde Cybersecurity Act;
3. het in 2017 opgezette instrumentarium voor cyberdiplomatie; en
4. de EU-initiatieven tegen desinformatie.

De Netwerk- en Informatiebeveiligings-richtlijn (NIB)

De NIB-richtlijn is het resultaat van meer dan drie jaar werk van de Europese Commissie, de Europese Raad en het Europese Parlement, die hiervoor hebben samengewerkt met belanghebbenden uit Europa en de rest van de wereld. De NIB is bedoeld als een uniform antwoord op de groeiende zorgen over cyberbedreigingen. In Nederland is er een wet geschreven die de richtlijn uitwerkt en inmiddels door beide Kamers van de Staten-Generaal is goedgekeurd.

De richtlijn bestaat uit twee delen. Het eerste deel vereist dat aanbieders van essentiële diensten, zoals energiebedrijven en zorginstellingen, zorg dragen voor cyberveiligheid. Het stelt in mindere mate eisen aan aanbieders van digitale diensten, zoals online-marktplaatsen en online-zoekmachines. Het is vooral aan de lidstaten om deze verantwoordelijkheden te concretiseren.

Het tweede deel ziet toe op het formuleren van een nationale beveiligingsstrategie, en vereist dat lidstaten Computer Security Incident Response Teams (CSIRT, doelt op hetzelfde als CERT) opzetten, die cyberincidenten en -risico's kunnen detecteren, voorkomen en aanpakken. Vooral deze laatste eis is van groot belang voor de internationale samenwerking, aangezien deze teams elkaar ook internationaal kunnen ondersteunen.

CSIRT’s richten zich op noodsituaties in de beveiliging, bevorderen het gebruik van valide beveiligingstechnologie en verzekeren de continuïteit van belangrijke netwerken. In de praktijk betekent dit dat CSIRT’s zich vooral concentreren op het identificeren van kwetsbaarheden en het bevorderen van de communicatie tussen beveiligingsleveranciers, gebruikers en particuliere organisaties. Hoewel de meerderheid van de CSIRT’s zijn opgericht als niet-winstgevende organisaties, zijn er de afgelopen jaren veel overgegaan in publiek-private partnerschappen (Choucri e.a. 2014). Inmiddels zijn er meer dan 200 CSIRT’s in 43 landen actief. Ook in Nederland zijn tal van CSIRT’s operationeel.

Voorheen werkten de CSIRT's weinig effectief samen, omdat de methoden voor gegevensverzameling niet gestroomlijnd was en daardoor de beschikbaarheid en betrouwbaarheid van gerapporteerde informatie sterk uiteenliep (Choucri e.a. 2014). De NIB-richtlijn legt daarom de nadruk op een goede coördinatie tussen de lidstaten en schrijft voor dat er een CSIRT-netwerk wordt opgericht, waar ook een CSIRT op EU-niveau deel vanuit maakt. De CERT-EU krijgt de taak om in Europees verband gecoördineerd en effectief op te treden als Europese instellingen en organisaties te kampen hebben met cyberaanvallen. De CERT-EU zal nauw samenwerken met de CSIRT's van de EU-lidstaten zelf, met IT-beveiligingsbedrijven in Europa en met de NAVO.

De hoop is dat, door in de gehele EU informatie te delen, het steeds moeilijker wordt om netwerken aan te vallen, en dat het steeds gemakkelijker wordt om daders te identificeren en te vervolgen, wat een afschrikwekkend effect kan hebben. In de woorden van de Commissie:

> 'As long as the perpetrators of cyber-attacks – both non-state and state – have nothing to fear besides failure, they will have little incentive to stop trying. A more effective law enforcement response focusing on detection, traceability and prosecution of cyber criminals is central to building effective deterrence. (Europese Commissie 2017a, 3)

De Cybersecurity Act

In juni 2018 nam de Europese Unie op het gebied van cybersecurity nog meer het heft in handen. Ze stelde de Cybersecurity Act voor, een verordening die twee belangrijke onderdelen heeft: het uitbreiden van het mandaat en de taken van het Europese Agentschap voor netwerk- en informatiebeveiliging, en het introduceren van een EU-breed certificeringssysteem voor digitale diensten en producten (Europese Commissie 2017b). Aangezien verordeningen direct rechtsgeldig zijn en dus weinig interpretatieruimte bieden aan lidstaten, wordt de digitale omgeving van Europa hiermee nadrukkelijker door de Unie bestuurd. De verordening treedt bijna in werking. Op 12 maart 2019 is de verordening goedgekeurd door het Europees Parlement, en de wet moet nu alleen nog formeel goedgekeurd worden door de Europese Raad.

De certificering moet garanderen dat digitale producten en diensten overal in de Unie voldoen aan minimale veiligheidseisen, en zodoende vele zwakke schakels in het Internet of Things (IoT) versterkt worden. Hoofdstuk 2 laat al zien dat de opkomst van het IoT tal van veiligheidsrisico's met zich meebrengt, en middels deze verordening neemt de Commissie een duidelijke stap om dit probleem aan te pakken.

De uitbreiding van het agentschap moet het European Union Agency for Network and Information Security (ENISA) prominent naar voren schuiven als het belangrijkste Europese instituut op het gebied van cybersecurity. Als de verordening in werking treedt, is ENISA de voornaamste adviseur van de Europese Commissie op het gebied van cybersecurity. Ook moet ENISA lidstaten krachtig ondersteunen in het realiseren en straktrekken van de CSIRT-structuur die is opgezet op basis van de NIB-richtlijn. De uitbreiding van ENISA lijkt tegemoet te komen aan de wens om meer duidelijkheid te scheppen in de grote governancestructuur die de EU rond cybersecurity heeft opgericht (zie kader 8).

Kader 8 Overige EU-cybersecurity initiatieven

Binnen het EU inlichtingen- en situatiecentrum (IntCen), dat weer onderdeel is van de European External Action Service (EEAS), is een speciale ‘Hybrid Fusion Cell’ opgericht, die cyberincidenten analyseert en een platform vormt voor het delen van inlichtingen. Onlangs riep de Europese Commissie op de capaciteit van dit platform verder te vergroten (Europese Commissie 2017a).

In oktober 2017 werd in Helsinki het ‘Europese Center of Excellence voor hybride dreigingen’ officieel geopend, waar onderzoek gedaan wordt naar de aard van hybride dreigingen en de manieren waarop staten zich hiertegen kunnen verweren. Lidmaatschap van dit centrum staat open voor alle EU- en NAVO-lidstaten; Nederland heeft zich samen met veelal Noord-Europese landen en Amerika aangesloten.

ENISA, het Europese Agentschap voor netwerk- en informatiebeveiliging, is vanaf 2010 begonnen met het organiseren van grote cybersecurity-oefeningen, waarvan in juni 2018 de vijfde plaatsvond. Ditmaal simuleerde men escalerende cyberaanvallen in de luchtvaartsector. Tijdens deze oefening moesten negenhonderd cybersecurityprofessionals uit dertig Europese landen deze aanvallen onschadelijk maken (ENISA 2018).

Cyberdiplomacy toolbox
De Raad Buitenlandse Zaken (RBZ), bestaande uit de EU-ministers van Buitenlandse Zaken, heeft een zogeheten kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten goedgekeurd (Europese Raad 2017). Dit kader wordt ook het instrumentarium voor cyberdiplomatie genoemd en sluit aan bij bestaande diplomatieke kaders die onderdeel zijn van het Europese Buitenlands- en Veiligheidsbeleid. Zo kunnen als reactie op cyberaanvallen beperkende maatregelen genomen worden, zoals het instellen van handelssancties, het bevriezen van financiële tegoeden en het onderbreken van diplomatieke betrekkingen.

Deze toolbox is de eerste stap in een echt gezamenlijke reactie van Europese lidstaten op cyberaanvallen. Het is echter geen verplichtend regime. Lidstaten kunnen er zelf voor kiezen in meer of mindere mate een gezamenlijke reactie te ondersteunen en gebruik te maken van de richtlijnen rondom het instellen van sancties.

De EU-initiatieven tegen desinformatie
Het bestrijden van de verspreiding van desinformatie staat hoog op de agenda van de EU, en er zijn inmiddels verschillende maatregelen genomen (EC 2018c). Zo investeert het Europese Centrum voor Pers- en Mediavrijheid in internationale onderzoeksjournalistiek en heeft de Europese Commissie een speciale anti-desinformatietaakgroep gelanceerd: de EU vs. disinformation campaign (IJ4EU 2018, EUvsDisinfo 2018). Deze campagne omvat onder meer het onderhouden van een unieke en publiek toegankelijke database die voorbeelden van desinformatie verzamelt – tussen september 2015 en de lente van 2018 zijn meer dan 3800 desinformatiegevallen toegevoegd. De campagne traint ook lidstaten en EU-instellingen in het omgaan met desinformatie.

Ten slotte is er een ‘Code of Practice on Disinformation’ ontwikkeld, een niet-bindend document dat aangeeft hoe met name online platformen, sociale netwerken en adverteerders desinformatie tegen kunnen gaan (EC 2018b). Diverse grote techbedrijven, waaronder Twitter, Google en Facebook, hebben aangegeven zich aan de code te houden. Ze hebben plannen gepresenteerd om deze succesvol te implementeren (Euractiv 2018). De code eist onder meer dat bedrijven geen geld aannemen van adverteerders die misleidende informatie over zichzelf willen plaatsen, en wil de monitoring van advertenties significant verbeteren.

De initiatieven van de Commissie zijn soms omstreden. Bij sommige media, waaronder Nederlandse kranten en sites, leeft de angst dat de maatregelen zullen leiden tot censuur. Vooral de anti-desinformatietaakgroep is bekritiseerd, onder andere omdat bijdrages van onder meer De Gelderlander en The Post online

werden bestempeld als nepnieuws – deze beschuldigingen zijn inmiddels ingetrokken. In maart 2018 werd een Kamermotie aangenomen om EUvsDisinfo op te heffen, die het kabinet na enig verzet overnam (NOS 2018).

De EU ontplooit nog veel meer initiatieven om cyberveiligheid te bevorderen, waarvan we de belangrijkste in het kader hebben gezet.

4.2.2 Noord-Atlantische Verdragsorganisatie (NAVO)

Ook op het niveau van de NAVO wordt samenwerking gezocht. Op die samenwerking gaan we hier, gezien het belang voor Nederland, uitgebreider in.

In de nasleep van de cyberaanvallen op vitale Estse instellingen in 2007 kwam cyberveiligheid hoog op de agenda van de NAVO te staan (Healey & van Bochhoven 2011). Een lidstaat had immers ernstige schade geleden die zeer waarschijnlijk werd veroorzaakt, of tenminste werd toegestaan, door een andere staat: de Russische overheid. Sindsdien heeft de NAVO talrijke initiatieven ontplooid, die twee sporen volgen: het versterken van defensieve cybercapaciteit en het reguleren van de inzet van offensieve cybercapaciteit.

Versterken defensieve cybercapaciteit
De Noord-Atlantische Verdragsorganisatie NAVO is van oudsher een defensieve organisatie, gericht op het ondersteunen en coördineren van de capaciteit van lidstaten om vijandelijke aanvallen te weerstaan en slagvaardig terug te slaan. Er zijn sinds de NAVO-conferentie in Praag hierover in 2002 diverse conferentiedeclaraties, factsheets, en strategische visies uitgebracht die aangeven hoe de NAVO deze doelen in cyberspace probeert te bereiken (zie bijvoorbeeld NAVO 2002, 2008, 2011, 2016a). Concreet zijn allerlei maatregelen genomen, waarvan de volgende drie het meest belangrijk zijn.

Ten eerste richtte de Noord-Atlantische Raad, het primaire bestuursorgaan van de NAVO, in 2008 de **Cyber Defence Management Authority** (CDMA, NAVO CCDCOE 2018) op, die de defensiecapaciteiten van de lidstaten coördineert, beoordeelt en voorstellen doet om deze te verbeteren (Burton 2015). Dit gebeurt in nauw overleg met de lidstaten, aangezien de soldaten, tanks en ook cybertroepen en cybertechnologie horen bij of eigendom zijn van de lidstaten zelf. De CDMA maakt concrete afspraken met de regeringen van lidstaten over de verbetering van de cybercapaciteiten, door memoranda op te stellen die beide partijen ondertekenen.

Ten tweede kwam in 2012 uit een fusie van verschillende NAVO-onderdelen het **NAVO Communicatie en Informatie Agentschap** voort (NCI Agentschap 2018). Dit brede agentschap is van groot belang voor de cybercapaciteiten van de lidstaten. Zo is het verantwoordelijk voor de digitale verbinding tussen NAVO-troepen en ook voor de veiligheid van die digitale netwerken, levert het agentschap de IT-structuur van de NAVO-instituties zelf en certificeert het IT-technologie die wordt gebruikt door de legers van lidstaten (NCI Agentschap 2018). Het agentschap beheert ook de NAVO Computer Incident Response Capability (NCIRC), de CSIRT-teams van de NAVO, die zeer snel moeten kunnen assisteren bij cyberincidenten in één of meer lidstaten. Ten slotte organiseert het agentschap een forum waar inlichtingen uitgewisseld kunnen worden, en organiseert het grote conferenties op het gebied van cyberveiligheid, waar politici, legerstaf en private partners met elkaar in gesprek gaan.

Ten derde stelde Estland in 2004 voor om binnen de NAVO een cyberdefensie-expertisecentrum op te richten. En op oktober 2008 werd het **Cooperative Cyber Defense Centre of Excellence** (NAVO CCDCOE) in Tallinn volledig als NAVO-organisatie geaccrediteerd. Inmiddels wordt het centrum gesponsord door de meeste NAVO-lidstaten, waaronder de Verenigde Staten, het Verenigd Koninkrijk, Frankrijk, Duitsland en Nederland. Binnen het centrum werken cyberdefensie-experts uit meer dan twintig landen samen om kennis over cyberveiligheid op te bouwen en onder de partners van het centrum te verspreiden. Ook organiseert het centrum de technische cyberdefensie-oefening Locked Shields en de conferentie CyCon. Een zeer belangrijke prestatie van het centrum is het ontwikkelen van de zogeheten Tallinn Handboeken (Schmitt 2013, 2017), waarin een speciale groep experts voorstellen doet over het toepassen van internationaal recht op het gebied van cyberoperaties. Dit initiatief brengt ons bij het tweede spoor van NAVO-activiteiten: het reguleren van de inzet van offensieve cybercapaciteiten.

Reguleren van de inzet van offensieve cybercapaciteiten

Zoals gezegd ligt de nadruk van het cyberbeleid van de NAVO op het versterken van de verdediging van de NAVO-lidstaten: ‘The keynote is defence, whether an attack comes from state, criminal or other sources’, aldus een NAVO-woordvoerder (Grant 2008). De defensieve NAVO-doctrine is met name gebaseerd op afschrikking door ontmoediging of passieve afschrikking: ‘deterence by denial’. Dit betekent dat beveiligingsmaatregelen zo worden versterkt dat het haast onmogelijk of in ieder geval zeer kostbaar wordt voor aanvallers om te infiltreren in systemen (Healey & van Bochoven 2012). De vraag is echter of passieve afschrikking toereikend is. Keer op keer blijkt dat geraffineerde en volhardende hackers sterk beveiligde systemen kunnen hacken. Kan de NAVO dan een meer offensieve rol oppakken? Hoewel het mogelijk is dat het politieke en militaire commando van de NAVO wordt geïnformeerd als een NAVO-lid betrokken is bij het uitvoeren van

offensieve cyberoperaties, met name als deze deel uitmaken van een bredere NAVO-missie, wordt niet verwacht dat het cybercommando van de NAVO een offensieve rol zal gaan vervullen (Burton 2015).

Toch is het de vraag of de opkomst van offensieve cybercapaciteiten iets aan het defensieve karakter van de NAVO gaat veranderen. Het belangrijkste verdragsartikel van de NAVO is artikel 5:

> ‘De partijen komen overeen dat een gewapende aanval tegen een of meer van hen in Europa of Noord-Amerika als een aanval tegen hen allen zal worden beschouwd; zij komen bijgevolg overeen dat, indien zulk een gewapende aanval plaatsvindt, ieder van hen de aldus aangevallen partij of partijen zal bijstaan, in de uitoefening van het recht tot individuele of collectieve zelfverdediging erkend in Artikel 51 van het Handvest van de Verenigde Naties, door terstond, individueel en in samenwerking met de andere partijen, op te treden op de wijze die zij nodig oordeelt met inbegrip van het gebruik van gewapend geweld om de veiligheid van het Noord-Atlantisch gebied te herstellen en te handhaven.’ (Noord-Atlantisch Verdrag Art. 5).

Het vorige hoofdstuk liet zien dat Rusland, China en landen als Iran en Noord-Korea de digitale netwerken van NAVO-landen met regelmaat bestoken. Is het dan niet denkbaar dat artikel 5 wordt geactiveerd? Dan zouden de NAVO-landen offensief moeten samenwerken om het aangevallen land bij te staan.

Deze kwestie heeft een langdurig intern debat binnen de alliantie opgeleverd. De hamvraag was of een cyberaanval telt als een ‘gewapende aanval’. De Estse minister van Defensie erkende in 2007 dat ‘[at] present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article 5 of the North Atlantic Treaty, or, in other words collective self-defense, will not automatically be extended to the attacked country’ (Traynor 2007). De grootschalige cyberaanval op Estse overheidsinstellingen in 2007 werd echter alom gezien als veiligheidskwestie die de NAVO aangaat (Traynor 2007). De institutionele aanpassing van de NAVO met betrekking tot de dreiging van cyberaanvallen werd in 2011 voortgezet met de vaststelling van een herziene Cyber Defence Policy, waarin de nadruk werd gelegd op minimumvereisten voor cyberdefensie van nationale netwerken, op een geïntegreerd systeem van cyber-governance binnen de NAVO, en de noodzaak van een pragmatische reactie op cyberaanvallen (NAVO 2011).

Uiteindelijk werd op een NAVO-top in Cardiff in 2014 besloten dat een cyberaanval ook aanleiding kan geven tot het verdedigingsmechanisme van artikel 5 (NAVO

2014). De alliantie sprak af doelbewust en proportioneel te reageren op elke significante cyberaanval, afhankelijk van de omvang van de schade, de mate van toerekening, en de motieven en identiteit van de aanvallers (Abrial 2011). Onder significante cyberaanvallen verstaat de NAVO aanvallen met ernstige gevolgen voor de economie, vitale infrastructuren en nationale veiligheid van NAVO-leden. Wat de proportionele reactie van de NAVO precies inhoudt, is echter nog onduidelijk. Is een cybertegenaanval proportioneel? Of een conventionele militaire aanval? Een concreet handelingsperspectief is dus niet gegeven. Wel nemen sommige lidstaten, zoals de Verenigde Staten, steeds meer een bepaalde positie in – bijvoorbeeld door te suggereren dat een conventionele tegenaanval, en zelfs een nucleaire tegenaanval, denkbaar is (U.S. Secretary of Defense 2018).

Juist op NAVO-niveau sterk is geïnvesteerd in het ontwikkelen van een gedeeld regulatief kader. Met betrokkenheid van Nederland is het zogeheten Tallinn Handboek opgesteld, dat uiteenzet hoe cyberoperaties door het internationale recht gereguleerd worden. Het handboek, waarvan nu een tweede editie is uitgebracht (Schmitt 2017a), heeft het juridische en strategische denken van de NAVO over belangrijke cyberveiligheidskwesties bevorderd, al blijven de nodige vragen en interpretatievraagstukken bestaan (zie o.a. Lucas 2017; Yoo 2015). Dit komt onder meer omdat digitale aanvallen die niet zijn verbonden aan conventioneel oorlogsgeweld vaak moeilijk zijn te kwalificeren als gewapende aanvallen (Fleck 2013). In paragraaf 4.3 gaan we dieper in op het Tallinn Handboek.

Samenvattend kunnen we stellen dat de NAVO op het gebied van de dreiging van cyberaanvallen haar defensieve taak zeer serieus neemt, en relevante stappen heeft gezet om op het gebied van offensieve cybercapaciteiten haar rol te verduidelijken. Maar veel vragen moeten nog verder worden beantwoord.

4.2.3 De Group of Seven (G7)

De ‘group of seven’, kortweg G7, is een interstatelijk overlegorgaan (G7 2019a). Op dit moment bestaat de groep uit Frankrijk, Duitsland, Italië, het Verenigd Koninkrijk, de Verenigde Staten, Japan en Canada. Afgevaardigden van de EU wonen ook alle bijeenkomsten bij. Rusland was tot 2014 lid van de groep, maar werd vanwege de annexatie van de Krim van het overleg uitgesloten. De groep voert voornamelijk overleg over kwesties van internationale veiligheid, economisch beleid en energiebeleid. Hierin onderscheidt het zich van de G20, de ‘group of twenty’, die zich hoofdzakelijk op economische zaken richt. Hoewel industriële grootmachten zoals China, Brazilië en Mexico geen deel uitmaken van de groep, vinden er wel besprekingen plaats tussen de G7 en deze landen.

De laatste jaren is het thema cyberveiligheid steeds prominenter op de agenda komen te staan. Zo werd onder andere in 2017 de G7 Declaration on Responsible Sattes Behavior in Cyberspace naar buiten gebracht, waarin onder andere de mogelijkheid wordt geopperd dat aangevallen staten tegenmaatregelen kunnen nemen, inclusief cybertegenaanvallen (G7 2017).

Daarna werd in 2018 de Charlevoix Commitment on Defending Democracy From Foreign Threats gepubliceerd, een lijst met actiepunten die de staten weerbaar moeten maken tegen aanvallen die democratische processen kunnen ondermijnen – waaronder cyberaanvallen (G7 2018). Er wordt onder meer opgeroepen tot het opzetten van een Rapid Response Mechanism, een procedure waarin staten snel met elkaar een reactie op een aanval kunnen coordineren. De precieze details van dit mechanisme moeten nog ingevuld worden.

Ook de recente G7 bijeenkomst in april 2019 leverde concrete resultaten op. Zo publiceerden de gezamenlijke ministers van Buitenlandse Zaken de Dinard Declaration on the Cyber Norm Initiative (G7 2019b). Deze niet-bindende declaratie ondersteunt de afspraken die op VN-niveau door de GGE's van 2010, 2013 en 2015 zijn gepubliceerd, en roept staten op relevante informatie uit te wisselen en intensiever met elkaar samen te werken. Ook werd er een communiqué van de ministers van Buitenlandse Zaken gepubliceerd, waarin wordt verwezen naar het Rapid Response Mechanism, en waarin de wens wordt uitgesproken gezamenlijk cyberaanvallen af te schrikken (G7 2019c).

4.2.4 Shanghai Cooperation Organisation (SCO)

De Shanghai Cooperation Organisation, ook wel het Shanghai Pact genoemd, is een internationale samenwerkingsorganisatie tussen Aziatische en Euraziatische landen. Het heeft acht leden: China, Rusland, India, Pakistan, Kirgizië, Tadzjikistan, Oezbekistan en Kazachstan (SCO 2017). Deze landen overleggen periodiek met elkaar en werken samen op talrijke gebieden, waaronder defensie en veiligheid, en strijden tegen de zogenoemde 'drie kwaden': extremisme, separatisme en terrorisme (SCO 2006).

Twee initiatieven van de SCO zijn met name van belang: in juni 2009 tekenden de lidstaten (waar India en Pakistan toen nog niet onder vielen) een akkoord 'on Cooperation in the Field of International Information Security', en dezelfde landen legden ook een 'International code of conduct for information security' voor aan de Algemene Vergadering van de VN (CCDCOE 2018).

Het eerste document bevat met name toezeggingen om de cyberveiligheid van het gehele SCO-gebied te verbeteren, bijvoorbeeld op het gebied van het bewaken van vitale infrastructuur en het opsporen van cybercriminelen.

Het tweede document stelt een gedragscode voor staten voor: zo moeten ze elkaars soevereiniteit respecteren en zich niet mengen in de aangelegenheden van andere staten of de politieke stabiliteit van een ander land aantasten.

In beide documenten komt het begrip *information security* prominent naar voren. Dit begrip is controversieel, omdat het geassocieerd wordt met het censureren en controleren van de inhoud van digitale informatie (Klimburg 2017). Zo kan een dictatoriaal regime onwelgevallige kritiek verbieden onder het mom van informatieveiligheid, en dissidenten op dezelfde grondslag opsluiten. Deze praktijken zijn de regeringen van verschillende SCO-lidstaten, waaronder China en Rusland, niet vreemd.

4.2.5 Organisatie voor Veiligheid en Samenwerking in Europa (OVSE)

Dit internationale samenwerkingsverband is de grootste regionale organisatie op het gebied van veiligheid en telt 57 lidstaten, waaronder ook veel landen buiten Europa, zoals de Verenigde Staten en Rusland. De OVSE is midden in de jaren ’70 opgericht, en diende tijdens de Koude Oorlog als een platform waar het Westen en Oosten overleg voerden. Onder ‘veiligheid’ valt volgens de OVSE veel, zoals duurzaamheid, democratie en cyberveiligheid. De organisatie ontplooit veel activiteiten om deze omvattende veiligheid in alle lidstaten te realiseren (OVSE 2018).

Op het gebied van cyberveiligheid richt de OVSE zich juist op het gebruik van informatietechnologie tussen lidstaten. De OVSE waarschuwt voor de gevaren van escalerend cyberconflict en pleit voor meer dialoog (OVSE 2016, De Gruyter 2018). Er is in 2016 een aantal zogeheten *confidence-building measures* aangenomen, waaronder het organiseren van communicatielijnen en regelmatige overleggen tussen de lidstaten en het bevorderen van transparantie over de terminologie die lidstaten gebruiken om zaken die zijn gerelateerd aan cybercapaciteiten te omschrijven (OVSE 2016). Ook worden lidstaten in de afspraken opgeroepen verantwoordelijk om te springen met kennis van digitale kwetsbaarheden en op transparante wijze een classificering van cyberaanvallen op te stellen. Vrijwel al deze aangenomen maatregelen zijn afgesproken op vrijwillige basis. Als een OVSE-lidstaat ze niet respecteert en bijvoorbeeld weigert periodieke overleggen bij te wonen, kan de OVSE geen sancties opleggen. Dit sluit aan bij de wens van het

OVSE om in de eerste plaats een plek te zijn waar dialoog plaats kan vinden – dit in contrast met een organisatie waar lidstaten harde, afdwingbare afspraken maken.

4.2.6 Five Eyes-samenwerkingsverband en SIGINT Seniors

In de nasleep van de Tweede Wereldoorlog vormden de VS, het VK, Canada, Nieuw-Zeeland en Australië de Five Eyes-samenwerking, waar met name SIGINT-inlichtingen (SIGINT staat voor signals intelligence: inlichtingen die verzameld worden op basis van elektronische signalen) worden uitgewisseld (Farrell 2013).

Binnen de 'Five Eyes' zijn de Amerikaanse National Security Agency (NSA) en de Engelse Government Communications Headquarters (GCHQ) waarschijnlijk de meest slagkrachtige diensten. De Five Eyes-samenwerking is in de jaren '80 verbreed om meer Europese landen te betrekken, waaronder Nederland, Frankrijk, Italië en Duitsland (Gallagher 2018). Deze bredere groep van 14 landen heet de SIGINT Seniors Europe; er bestaat ook een SIGINT Seniors Pacific. Deze landen hebben militaire en algemene inlichtingendiensten die onderling informatie uitwisselen. De Snowden-onthullingen lieten zien dat niet alleen de NSA, maar ook de GCHQ, de Duitse Bundesnachtrichtendienst (BND) en de Nederlandse inlichtingendiensten zeer actief inlichtingen verzamelen en onderling delen (zie bijvoorbeeld Modderkolk 2018, Gallagher 2017). In juni 2018 zijn in Nederland de mogelijkheden van de inlichtingendiensten om communicatie te onderscheppen uitgebreid, door middel van de vernieuwde Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv)

De samenwerking tussen de inlichtingendiensten betekent overigens niet dat alle beschikbare informatie wordt uitgewisseld; dat de spionagemethoden, waaronder gevoelige software kwetsbaarheden, altijd gedeeld worden, of dat deze landen elkaar niet bespioneren. Zo waren Franse en Duitse regeringen verbolgen toen naar buiten kwam dat de NSA de toenmalige Franse president François Hollande en de Duitse bondskanselier Angela Merkel had afgeluisterd (Agence France-Presse 2016).

4.3 De staat van internationale regelgeving

Met bescheiden succes hebben de afgelopen jaren verschillende samenwerkingsinitiatieven regels proberen vast te stellen op het gebied van de ontwikkeling en inzet van offensieve cybercapaciteiten: op VN-niveau liepen aanvankelijk vruchtbare gesprekken uiteindelijk vast, op NAVO-niveau werd na lang beraad een aantal belangrijke uitspraken gedaan, in NAVO-verband is het Tallinn

Handboek ontwikkeld en ook de SCO stelde een code voor, die echter binnen de VN op beperkt enthousiasme kon rekenen. Maar waar komen al deze initiatieven precies op neer en welke regels gelden er precies tussen staten? Voor een goed begrip van de huidige internationale situatie is het antwoord op deze vraag essentieel.

4.3.1 De aard van internationaal recht

Het antwoord vereist enkele opmerkingen over de aard van internationaal recht. Dit recht is duidelijk wanneer vrijwel alle landen een afspraak met elkaar hebben gemaakt, die afspraak door de verschillende landen op dezelfde manier wordt geïnterpreteerd, zij die afspraak in de praktijk ook naleven en een bron van rechterlijke uitspraken bestaat waarin de details van de afspraak nog eens worden geëxpliciteerd en bekrachtigd. Als in zo'n situatie één staat de regel overtreedt, kunnen andere staten de regering in kwestie aanwijzen als schender van het internationaal recht. Denk bijvoorbeeld aan de verdragsbepalingen die de EU in het leven heeft geroepen, en die bijvoorbeeld de Europese verkiezingen reguleren. Deze afspraken worden doorgaans uniform uitgelegd, opgelegd en nageleefd.

Veel internationaal recht, waaronder het internationaal recht over offensieve cybercapaciteiten, is echter niet zo eenduidig. Het kan en wordt door verschillende staten verschillend geïnterpreteerd. Dat begint al bij de meest basale vraag die men kan stellen: is het internationale recht überhaupt van toepassing op offensieve cybercapaciteiten?

Aanvankelijk leken op VN-niveau de landen binnen de UN GGE – United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – hierover overeenstemming te hebben bereikt (UN GGE 2015). Zo zou het internationaal recht van toepassing zijn op informatie- en communicatietechnologie, en principes als humaniteit, noodzakelijkheid en proportionaliteit gerespecteerd moeten worden bij de inzet van deze technologie. Maar de status van dit eerdere rapport uit 2015 is op dit moment onduidelijk, omdat de meest recente UN GGE-expertgroep geen overeenstemming kon bereiken over een eindrapportage (Soesanto & D'incau 2017).

Toch is er tussen staten en onder juridische experts een steeds grotere consensus ontstaan dat het internationaal recht wel degelijk iets te zeggen heeft over de inzet van offensieve cybercapaciteiten (zie bijvoorbeeld de Paris Call 2018). Maar wat dat precies betekent, is minder duidelijk. We geven hieronder bondig de discussie weer die onder experts gevoerd wordt, en nemen de tweede versie van het Tallinn

Handboek als belangrijkste vertrekpunt (Schmitt 2017a). Let wel: dat handboek is geen directe representatie van de opvattingen van de NAVO-lidstaten – op verschillende punten moeten die lidstaten hun interpretaties van generieke verplichtingen nog presenteren. Het is ook belangrijk te vermelden dat het Tallinn Handboek-project juist door Nederland is aangemoedigd, en zich onder andere baseert op het toonaangevende AIV/CAVV-advies[8] over digitale oorlogvoering dat in 2011 is uitgebracht – dit onderstreept dat het debat over de juridische betekenis van cyberaanvallen vanuit Nederland succesvol is geëntameerd (AIV/CAVV 2011).

4.3.2 Cyberaanvallen als schendingen van staatssoevereiniteit

De discussie draait met name om een van de kernprincipes van het internationaal recht: het respecteren van de nationale soevereiniteit van andere landen (Schmitt 2017a). Dit principe stelt dat een staat het recht heeft om onafhankelijk van andere staten op een bepaald deel van de wereld ‘de functies van een staat’ uit te oefenen. Denk bij deze functies bijvoorbeeld aan het heffen van belasting, het uitvaardigen van wetten en het oprichten van een leger. Soevereiniteit hangt ook samen met territorialiteit – staten zijn op eigen grondgebied soeverein – maar het begrip kan verder strekken. Zo heeft iedere staat een recht om een buitenlandse politiek te voeren en handelsrelaties met andere staten aan te gaan.

De internationale expertgroep is het erover eens dat het principe van soevereiniteit van toepassing is op cyberspace (Schmitt 2017a). De staatssoevereiniteit heeft in ieder geval betrekking op de fysieke infrastructuur die op het territorium van een land staat, de data, applicaties en protocollen aanwezig op die fysieke hardware en de personen die op het territorium handelingen in de cyberspace verrichten. Bovendien tasten cyberaanvallen de soevereiniteit van een staat aan als ze een kinetisch effect hebben op het grondgebied van een staat – als het iets in beweging brengt.

Cyberaanvallen kunnen de soevereiniteit van een staat in theorie dus schenden. Dat kan op verschillende manieren – de volgende drie zijn het meest belangrijk:

1. Een staat mag geen geweld gebruiken of met geweld dreigen tegen personen of fysieke objecten behorend tot een andere staat. Dit verbod is deels uitgewerkt in het internationaal volkenrecht, het zogeheten *ius ad bellum*.
2. Een staat mag niet dwingend interveniëren in de zaken van een andere staat.

8 De Adviesraad Internationale Vraagstukken (AIV) is een onafhankelijk adviesorgaan en adviseert de Eerste en Tweede Kamer over het buitenlandbeleid. De Commissie van advies inzake volkenrechtelijke vraagstukken CAVV is een onafhankelijk adviesorgaan dat de regering en de Eerste en Tweede Kamer adviseert over vraagstukken van internationaal recht.

3. Een staat kan de soevereiniteit van een andere staat in algemene zin inperken; we kunnen deze norm beschouwen als een restcategorie.

De vraag is of cyberaanvallen deze drie normen kunnen overtreden. Verreweg de meeste cyberaanvallen worden door experts niet als gewelddadig of als dwingend interveniërend gekwalificeerd (Schmitt & Vihul 2017b). We lichten dit punt nader toe, beginnend bij het geweldsverbod.

Ad 1. Cyberaanvallen als vormen van geweld?
Het geweldsverbod doelt op geweld dat bepaalde 'fysieke effecten' heeft (Schmitt 2013). Er is volgens het internationaal recht van geweld dus alleen sprake als dit leidt tot een feitelijk of mogelijk schadelijk fysiek effect op de staat die het doelwit is. Onder deze fysieke effecten verstaat het recht de dood, lichamelijk letsel of significante vernietiging van of schade aan vitale infrastructuren, militaire installaties of civiele goederen (Schmitt 2017a). De staat die dergelijk geweld begaat, kan daarmee zowel in overtreding zijn van het algemene geweldsverbod van artikel 2(4) VN Handvest als het verbod op 'gewapende aanvallen' van artikel 51 VN Handvest.

Dit onderscheid is van groot belang, omdat het uitvoeren van een gewapende aanval het recht op interstatelijke zelfverdediging (*ius ad bellum*) en het recht tijdens oorlogsvoering (*ius in bello*) activeert. Met andere woorden: als een staat ervoor kiest een gewapende aanval uit te voeren, gelden er allerlei regels waaraan de staat zich heeft te houden, zoals het kunnen aanvoeren van een geldige reden om de aanval te plegen.

Het verschil tussen een gewapende aanval en andersoortig geweldsgebruik is alleen soms moeilijk te maken. Gewapende aanvallen zijn ernstige en ontwrichtende daden van geweld, zoals het plegen van een raketaanval, het werpen van een nucleaire bom of het volledig platleggen van alle financiële dienstverlening (AIV/CAVV 2011). Maar het is moeilijk te zeggen wanneer een geweldsaanval dermate minder ernstig is, dat 'slechts' van een geweldsdaad sprake is. Wat als je de financiële dienstverlening platlegt, maar deze een dag later weer goed functioneert? Het internationaal recht geeft uiteindelijk vooral generieke regels en principes; de staten zelf zullen bepaalde interpretaties moeten voorstellen.

Wat betekent dit voor cyberaanvallen? Ten eerste is het duidelijk dat het gaat om de gevolgen van cyberaanvallen, niet om hun digitale aard – volgens het Tallinn Handboek sluit het internationaal recht geen enkel wapen uit (AIV/CAVV 2011, Schmitt 2013, 2017a). Ten tweede is het voorstelbaar dat cyberaanvallen kunnen leiden tot burgerslachtoffers of significante infrastructurele schade, bijvoorbeeld als gevolg van het langdurig uitschakelen van energiecentrales. Zo'n aanval kan dus,

theoretisch gezien, tot een geweldsdaad en zelfs tot een gewapende aanval worden gerekend (Condron 2007, Jensen 2002, Benatar 2009, Schmitt 2013).

Maar het is lastig om cyberaanvallen te vinden die aan de criteria van een gewapende aanval voldoen (Rid 2012, Schmitt 2013). Saboterende cyberaanvallen maken doorgaans geen burgerslachtoffers – in ieder geval niet in directe zin. En veruit de meeste saboterende cyberaanvallen veroorzaken wel maatschappelijke schade, maar leggen geen vitale infrastructuur plat. Zo onderbreken saboterende cyberaanvallen met enige regelmaat de dienstverlening van banken, maar is de gehele financiële sector nog nooit platgelegd. Evengoed is in Oekraïne de energievoorziening weleens platgelegd, maar gingen een aantal uren later de lichten weer aan. Zelfs de aanval op de centrifuges in Natanz leverde de nodige discussie op – hoewel de meerderheid van de experts uiteindelijk concludeerde dat dit een gewapende aanval was (Schmitt 2017a). Het AIV/CAVV concludeerde daarom al dat een ‘cyberoorlog’, bestaande uit losstaande digitale gewapende aanvallen, moeilijk denkbaar is (AIV/CAVV 2011).

Deze conclusie relativeert bepaalde beweringen over cyberconflicten. Zo zagen we dat in sommige landen in de context van cyberaanvallen regelmatig oorlogstaal wordt gebezigd – Amerikaanse generaals waarschuwen voor een ‘cyber Pearl Harbor’ en verkondigen letterlijk dat de VS zich in een staat van oorlog bevindt (zie bijvoorbeeld Stavridis 2017). Maar van oorlog in de zin van het internationale recht is op het gebied van cyberaanvallen vrijwel nooit sprake.

Dit betekent overigens niet dat het oorlogsrecht nooit van toepassing is op cyberaanvallen: als landen eenmaal in een oorlogssituatie verkeren moeten cyberaanvallen die onderdeel vormen van de militaire campagne aan het *ius in bello* voldoen. Dit verklaart waarom volgens het Tallinn Handboek 2.0 de cyberaanvallen op Estland niet, en de cyberaanvallen op de Oekraïne wel onder het oorlogsrecht vielen. De cyberaanvallen op de Oekraïense staat vonden namelijk plaats in de context van de militaire bezetting van delen van Oost-Oekraïne en de Krim.

Is het gemakkelijker cyberaanvallen te kwalificeren als een ‘normale’ geweldsaanval? In sommige gevallen is dit begrip wel duidelijk, zeker als experts zich af beginnen te vragen of de geweldsaanval misschien zelfs telt als gewapende aanval. De Stuxnet-aanval was bijvoorbeeld duidelijk een geweldsaanval, omdat de turbines in Natanz fysieke schade ondervonden. Evengoed zou een cyberaanval op een energiecentrale een geweldsaanval zijn, als belangrijke installaties kapot zouden gaan. Maar cyberaanvallen zijn moeilijker als geweldsaanval te kwalificeren, omdat ze niet tot directe fysieke schade leiden maar slechts een digitaal systeem verstoren. De Tallinn-experts presenteren daarom een aantal

criteria dat moet worden meegewogen, zoals de ernst, onmiddellijkheid en indringendheid van de cyberaanval (Schmitt 2017a). Uiteindelijk moeten de staten ook hier het nodige interpretatiewerk verrichten.

Ad 2: Cyberaanvallen als vormen van dwingende interventie?
Gezien de beperkte fysieke schade die cyberaanvallen aanrichten, zal voor het reguleren van het informatieconflict gekeken moeten worden naar het verbod op dwingende interventie en het verbod op soevereiniteitsinperking. Deze categorieën zijn nog algemener gedefinieerd dan het geweldsverbod. Het verbod op dwingende interventie zelden zal worden overschreden door cyberaanvallen, omdat cyberaanvallen meestal niet zo krachtig of zo ingrijpend zijn dat ze een staat effectief dwingen om een bepaald beleid te voeren (Schmitt & Vihul 2017). Dit kan veranderen: cyberaanvallen kunnen in de toekomst ernstiger worden en regeringen effectiever onder druk zetten. Maar daar is vooralsnog geen sprake van. Wat dus overblijft, is het algemene verbod op soevereiniteitsinperking.

Ad 3: Cyberaanvallen als vormen van soevereiniteitsinperking?
De experts leggen uit dat het constateren van soevereiniteitsschending afhangt van (1) de mate waarin de territoriale integriteit van een staat geschonden wordt, en (2) de mate waarin de belangrijkste functies van de ene staat door de andere staat wordt aangetast of overgenomen (Schmitt 2017a). Op het gebied van het eerste punt zou men kunnen denken aan het plegen van geweld of het beschadigen van infrastructurele systemen. Bij het tweede punt kan men denken aan het organiseren van verkiezingen, het heffen van belastingen of het voeren van een bepaald economisch beleid. Het zal geen verassing zijn dat veel saboterende cyberaanvallen deze norm lijken te schenden: denk aan DDoS-aanvallen op bancaire sites of het platleggen van een energiecentrale.

Ook cyberspionage lijkt de soevereiniteit van staten in te perken, maar hierover oordelen de experts anders: de internationale praktijk, waarin landen elkaar structureel bespioneren, onderschrijft deze norm te weinig (Schmitt 2017a). Cyberspionage vormt alleen een inbreuk van de soevereiniteit van een staat als het bespieden gepaard gaat met een vorm van schade: de corruptie van data, het verlies van functionaliteit van een systeem of het installeren van achterdeuren. Aangezien veel cyberspionage schadelijke sporen achterlaat, zoals geopende digitale achterdeuren, betekent dit dat de norm van soevereiniteitsschending toch nog op veel cyberspionage van toepassing is.

Het is niet duidelijk of het verspreiden van desinformatie te beschouwen valt als inbreuk op staatssoevereiniteit; hier doen de experts geen uitspraken over. Maar we zouden ons wel een vergelijkbaar debat voor kunnen stellen. Men kan beweren dat dergelijke campagnes de soevereiniteit aantasten omdat het organiseren van

een constructief publiek debat en het houden van eerlijke verkiezingen activiteiten zijn die horen bij de kernfuncties van een democratische rechtstaat – en dat deze activiteiten belemmerd worden door informationele wanorde. Maar men zou ook kunnen beweren dat staten altijd al in enige mate propaganda hebben verspreid en dat leugens alleen niet voldoende zijn om het effectief functioneren van een staat aan te tasten. Dit debat zal in de toekomst verder gevoerd worden.

Al met al kan de norm van soevereiniteitsschending een kader bieden om veel cyberaanvallen kritisch tegen het licht te houden en zelfs in strijd met het internationaal recht te verklaren. Echter, de norm is zeer algemeen geformuleerd en de schending van soevereiniteit vormt op zich een minder ernstig vergrijp dan een geweldsaanval of gewapende aanval. Een schending van het geweldsverbod rechtvaardigt een sterkere reactie dan een algemene schending van soevereiniteit – en het zou goed kunnen dat staten in sommige situaties juist een sterke tegenmaatregel willen nemen.

4.3.3 Internationaal recht dat veel interpretatie behoeft

We concluderen dat het internationaal recht dat van toepassing is op cyberaanvallen vaak generiek van aard is, en nog veel interpretatie behoeft. Dit is op zich niet verwonderlijk, gezien de recente opkomst van cyberaanvallen. Het kost tijd om abstracte principes te vertalen naar een nieuwe praktijk. We zien dat staten daar op allerlei fora stappen in zetten.

Tegelijkertijd bestaat er nog veel onzekerheid over het kwalificeren van cyberaanvallen en het formuleren van een juridisch houdbare reactie. Staten moeten in veel opzichten hun positie nog bepalen, en zijn er op mondiaal niveau niet in geslaagd verstrekkende en concrete afspraken met elkaar te maken.

Er is dus zowel reden voor optimisme als voor pessimisme. De volgende stap ligt in het opstellen van regelkader die inspelen op de specifieke eigenschappen van het informatieconflict.

4.4 Conclusie

In de voorgaande paragrafen hebben we de internationale samenwerkingsverbanden op het gebied van offensieve cybercapaciteiten in kaart gebracht. Daarbij ging bijzondere aandacht uit naar de internationale regulering van offensieve cybercapaciteiten. We komen tot de volgende conclusies.

- **Zowel op regionaal als op wereldwijd niveau werken landen steeds hechter met elkaar en met bedrijven en maatschappelijke organisaties samen om de cyberveiligheid van hun systemen te verhogen**. Zie de IMPACT- en FIRST-verbanden, maar ook de initiatieven die zijn ontplooid op het niveau van de EU en van de NAVO, zoals de totstandbrenging van het netwerk van CERT's, de certificering van IoT-producten en defensiesoftware, en de verschillende militaire en civiele oefeningen. De noodzaak de cyberveiligheid continu te verbeteren wordt internationaal duidelijk gevoeld en geagendeerd, en steeds meer omgezet in politieke keuzes en concreet beleid.

- **De offensieve cybercapaciteitsopbouw van staten wordt in veel mindere mate door deze regionale verbanden gecoördineerd**. Landen, waaronder EU-lidstaten, bouwen naar eigen inzicht hun offensieve cybercapaciteit op, en schaffen eigenstandig cyberwapens aan. Hoewel de roep om meer samenwerking, en zelfs om een Europees leger, steeds luider klinkt, is de offensieve capaciteit nog steeds volgens het traditionele idee van individuele staatssoevereiniteit opgebouwd. In het voorbereiden op zowel het informatieconflict als op een cyber-fysieke oorlog zien we daarom op cybergebied een gemengd beeld van samenwerking en individueel capaciteitsbeheer. Zo proberen de EU-lidstaten bijvoorbeeld aan de hand van de cyberdiplomacy-toolbox cyberaanvallen wel steeds meer van een gezamenlijke diplomatie reactie te voorzien, en waar nodig daarvoor de sancties in te zetten die de EU kan opleggen (zie 4.2.1). Maar deze sancties betreffen vooralsnog niet het zelf inzetten van offensieve cybermiddelen.

- Hoewel de bronnen hier beperkt zijn, lijkt dezelfde spanning zichtbaar in de samenwerking op het gebied van inlichtingenverzameling. **Westerse inlichtingendiensten werken wel met elkaar samen, ook in offensief opzicht, maar houden tegelijkertijd regelmatig de kaarten tegen de borst**. Verschillende samenwerkingsverbanden zijn bekend, en staten erkennen dat het essentieel is om informatie met bondgenoten te delen. Ook weten we af van bepaalde gezamenlijk uitgevoerde spionage- en sabotageoperaties, zoals operatie Olympic Games en de onthulde samenwerkingen tussen de Amerikaanse NSA en de Britse GCHQ (Sanger 2018). Maar inlichtingendiensten laten onderling zelden het achterste van hun tong zien.

- Op het gebied van desinformatie liggen de kaarten anders. **Westerse internationale verbanden leggen de nadruk op het bestrijden van de verspreiding van desinformatie – vooral op EU-niveau**. Het gecoördineerd opbouwen van het vermogen om zelf desinformatie te verspreiden is geen onderwerp van discussie – wat niet betekent dat EU- of NAVO-lidstaten geen

desinformatie verspreiden (zie de discussie in 3.6). Tegen sommige bestrijdingsmaatregelen bestaat weerstand. Vooral de anti-desinformatietaakgroep is staatscensuur verweten.

- De spanning tussen internationale samenwerking en het eigenstandig inzetten van offensieve capaciteit is ook goed zichtbaar in de wereldwijde normontwikkeling op het gebied van cyberaanvallen. Aan de ene kant zien we vele gremia waar over normen gesproken wordt, zoals de UN GGE, de Paris Call, het Global Tech Accord en de OVSE. Deze overleggen zijn niet zonder resultaat geweest: de verschillende edities van de UN GGE hebben lijsten met vertrouwenwekkende maatregelen geproduceerd en doen uitspraken over het internationaal recht – en ook de publicaties van de G7, de Paris Call en het Tech Accord stellen normen voor en laten zien dat het internationaal recht op allerlei manieren ook van toepassing is op cyberaanvallen. Maar al deze overleggen hebben niet geleid tot wereldwijde afspraken. Het diplomatieke overleg van de VN international group of experts (UN GGE) is stopgezet, en op mondiaal niveau bestaat er vooralsnog geen vervanging van dit gremium. Het meest ambitieuze alternatief voor dit overleg lijkt de Paris Call te zijn, gezien de zeer brede en wereldwijde groep maatschappelijke partijen die dit document heeft ondertekend. Maar juist bij dit initiatief hebben verschillende cybergrootmachten zoals de Verenigde Staten en China zich niet aangesloten. **De normontwikkeling is dus wel op gang gebracht, maar het ontbreekt aan wereldwijde samenwerking.** Bovendien laat de discussie in het Tallinn Handboek zien dat de bestaande internationaalrechtelijke normen de nodige verdere interpretatie vereisen.

5 Conclusie

Steeds meer landen kunnen cyberaanvallen uitvoeren die grote schade aanrichten aan bedrijven, mensen en overheidsinstellingen. Vrijwel alle landen gebruiken deze cyberwapens ook. Ze bespioneren elkaar en proberen in elkaars digitale systemen te infiltreren; sommige staten voeren zelfs cybersabotage uit of verspreiden desinformatie. Door middel van informatietechnologie ontstaat een nieuw conflict. In dit rapport spreken we van een informatieconflict.

In dit onderzoek hebben we de vraag gesteld hoe Nederland kan bijdragen aan de-escalatie van dit informatieconflict. In dit slothoofdstuk stellen we vijf oplossingsrichtingen voor. Daarbij verwijzen we naar Nederlandse initiatieven die bij deze richtingen aansluiten. Maar eerst vatten we, op basis van de voorgaande hoofdstukken, de internationale stand van zaken samen.

5.1 De internationale stand van zaken

De afgelopen hoofdstukken gaven een overzicht van de recente ontwikkelingen op het gebied van offensieve cybercapaciteiten. Hoofdstuk 2 liet zien dat de digitalisering van de samenleving verschillende veiligheidsrisico's met zich meebrengt. Zo kunnen kwaadwillenden mobiele telefoons hacken en toegang krijgen tot privéfoto's of camerabeelden, en kunnen ze de computers van slimme apparaten inzetten bij een DDoS-aanval.

Vanwege dit grote en groeiende schadepotentieel spreekt men steeds meer over 'cyberwapens', 'cyberaanvallen' en 'cyberoperaties'. In dit rapport zijn deze nieuwe concepten beschreven. We maakten een onderscheid tussen drie vormen van cyberaanvallen: **cyberspionage**, **cybersabotage** en de **verspreiding van desinformatie**. Een aantal zaken viel daarbij op:

- Cyberaanvallen kunnen veelal op grote afstand en vanuit de schaduw plaatsvinden, zonder dat de dader hoeft te vrezen voor repercussies.
- Cyberwapens kunnen zich razendsnel verspreiden en na gebruik op onverwachte plaatsen schade aanrichten.
- Cyberaanvallen kunnen zowel technologisch geavanceerd als relatief simpel zijn. Geavanceerde aanvallen zijn voorbehouden aan machtige cyberactoren als inlichtingendiensten en goed georganiseerde criminelen. Simpelere aanvallen kan vrijwel iedereen uitvoeren of zelfs bestellen.

- Cyberwapens kunnen ontmanteld worden door systemen te updaten. Dit is pas mogelijk als de digitale kwetsbaarheid bekend is.
- De verspreiding van desinformatie is steeds moeilijker te doorzien, onder andere door hoogwaardige vervalsingen van beeld en geluid.

Drie tredes op een escalatieladder

Elke dag zijn er cyberaanvallen. In hoofdstuk 3 beschreven we wie ze uitvoert; daarbij benadrukten we de rol van de grote cybermachten – de Verenigde Staten, Rusland en China – en bespraken we ook Nederland en een aantal andere Europese landen. Dit deden we door de activiteiten te markeren op een zogenoemde cyberescalatieladder, die drie tredes telt:

1. Een trede gekenmerkt door **cybervrede**, waarin landen niet met digitale middelen spioneren en ook geen sabotage uitvoeren of desinformatie verspreiden.
2. Een trede gekenmerkt door **informatieconflict**, waarin staten overgaan tot cyberspionage en, in sommige gevallen, het verspreiden van desinformatie en het saboteren van digitale systemen.
3. Een trede gekenmerkt door **cyber-fysieke oorlog**, waarbij de schade die staten aanrichten zo ernstig is dat er sprake is van gewapende aanvallen. Tijdens een cyber-fysieke oorlog vallen alle soorten cyberaanvallen overigens onder het internationaal recht, en niet alleen de weinige cyberaanvallen die op zichzelf een gewapende aanval constitueren.

De meeste huidige handelingen van invloedrijke staten passen in wat we hierboven beschrijven als het informatieconflict. Landen zijn in vredestijd hun cybersecurity aan het opbouwen en ze proberen zo onzichtbaar mogelijk te infiltreren in de digitale systemen van andere landen. Rusland kenmerkt zich daarnaast door het actief verspreiden van desinformatie. Dat is een strategie die andere autocratische landen, tenminste naar het buitenland toe, nog niet breed lijken toe te passen, maar die wel naadloos aansluit bij de ambitie om de informatie die burgers bereikt te sturen, te censureren en te manipuleren. Daarnaast zijn er enkele voorbeelden van ernstige cybersabotage, zoals de operatie Olympic Games, die aan Israël en de Verenigde Staten wordt toegeschreven, en de WannaCry-aanval, die aan Noord-Korea wordt toegeschreven. Cyberaanvallen hebben tot nu toe nog nooit een cyber-fysieke oorlog uitgelokt; van ‘cyberoorlog’ is wat dat betreft geen sprake. Wel vormt cyber steeds meer een onderdeel van oorlogsvoering, zoals goed te zien is bij het conflict in Oekraïne.

Internationale samenwerking

Hoofdstuk 4 voegde het perspectief van internationale samenwerking toe aan de analyse. In internationale en regionale gremia proberen staten stappen te zetten om een veilige en vrije digitale wereld te realiseren. Staten zijn er niet in geslaagd

om voor cyberaanvallen heldere afspraken met elkaar te maken. Er is een duidelijk verschil tussen de samenwerking op het gebied van cybersecurity en de samenwerking op het gebied van offensieve cybercapaciteiten. De cybersecurity-initiatieven, binnen de EU en binnen internationale samenwerkingen zoals IMPACT en FIRST, gaan verder dan het agenderen van kwesties en leveren concreet geïmplementeerd en breed gedragen beleid op. Dat geldt niet voor de initiatieven op het gebied van offensieve cybercapaciteiten. Hoewel inlichtingendiensten met name in bilaterale relaties wel informatie delen en gezamenlijk optreden, zijn staten niet bij machte geweest om heldere regels af te spreken voor het informatieconflict.

Dit betekent niet dat er geen regels van toepassing zijn op cyberaanvallen. Maar omdat deze aanvallen zelden de drempel overschrijden van een ‘gewapende aanval’, en daarmee het internationaal humanitair recht activeren, zijn er alleen algemene normen beschikbaar, zoals het geweldsverbod. En die kunnen vooralsnog op allerlei manieren worden uitgelegd. Er wordt gewerkt aan nieuwe afspraken, maar deze zijn er nog niet.

Het informatieconflict kan escaleren. De huidige internationale situatie is riskant en zorgwekkend, zo laat ons rapport zien. Staten voeren voortdurend cyberaanvallen uit en er is een aanzienlijke kans dat dit gebeurt om burgers schade te berokkenen en dat dit escaleert. Dit heeft te maken met vier factoren, die we hieronder bespreken.

1. **De kwetsbaarheid van digitale systemen**
   We hebben in hoofdstuk 2 en 3 voorbeelden gezien van effectieve cyberaanvallen. Vrijwel geen enkele verdediging is volkomen veilig voor geavanceerde cyberaanvallen, en veel doelwitten zijn relatief simpel te infiltreren. Het verbeteren van de cyberverdediging heeft zin: door relatief simpele maatregelen kan veel leed voorkomen worden. Maar er is vooralsnog geen sprake van onneembare vestingen die aanvallers effectief ontmoedigen.

2. **De verdere verspreiding van wapens (wapenproliferatie)**
   Naast de gelegenheid om cyberaanvallen te plegen, zijn er ook veel cyberwapens beschikbaar. Ons overzicht laat zien dat grote en kleine staten offensieve cybercapaciteiten hebben opgebouwd. Ze willen beschikken over een hoogwaardig arsenaal waarmee complexe spionage, sabotage en desinformatieverspreiding uitgevoerd kan worden, en beheersen de simpelere methodes om cyberaanvallen te plegen. Deze ontwikkeling heeft geleid tot een private industrie die deze wapens levert. Ook het criminele circuit ontwikkelt cyberwapens en werkt soms samen met bepaalde overheden.

   Dit betekent dat een enorm aantal cyberwapens wordt ontwikkeld en

verspreid. Daarbij komt dat zelfs machtige cyberactoren bestolen kunnen worden, dat tegenstanders eenmaal gebruikte cyberwapens analyseren en hergebruiken en dat cyberwapens, eenmaal afgevuurd, in alle digitale hoeken van de wereld kunnen opduiken. Het spreekt voor zich dat wanneer de hoeveelheid cyberwapens zo toeneemt, de kans op cyberaanvallen groeit.

3. **De onzekerheid over de herkomst en kwalificering van cyberaanvallen**
Daarnaast is het moeilijk om achter de herkomst van cyberaanvallen te komen en deze met precisie te kwalificeren. Het blijft in veel gevallen lastig om de daders van cyberaanvallen snel en overtuigend te identificeren: een aanvaller kan bijvoorbeeld zijn operatie maskeren door via gehackte computers malware te versturen. Regelmatig wijzen inlichtingendiensten bepaalde daders aan, maar daarvoor kan onderzoek nodig zijn dat tijd vergt. De beschuldigde staat heeft weinig argumenten nodig om met enige plausibiliteit alle betrokkenheid te ontkennen (*plausible deniability*). Bovendien is het moeilijk om in te schatten hoe de cyberaanval er precies uitziet.

We hebben gezien dat cyberoperaties gelaagd zijn: om iets te saboteren is vaak eerst inlichtingenverwerving en infiltratie nodig. Maar inlichtingenverwerving en infiltratie kunnen op zichzelf staan, en geen voorbode zijn van een zwaardere cyberaanval. Dit kan misverstanden in de hand werken, omdat landen die constateren dat er in een systeem is geïnfiltreerd lang niet altijd kunnen inschatten welk doel die infiltratie dient – laat staan dat ze gelijk kunnen zien welke effecten bepaalde malware op een digitale voorziening sorteert.

Dit alles creëert onzekerheid en kan ervoor zorgen dat staten wachten met reageren, of misschien de dreiging verkeerd inschatten en te krachtig, of juist te zwak, reageren.

4. **Het gebrek aan uitgewerkte regels**
De huidige internationale situatie op het gebied van cyberaanvallen wordt gekenmerkt door een gebrek aan uitgewerkte regels: staten hebben op het gebied van het gebruik van offensieve cybercapaciteiten in situaties van informatieconflict geen op het cyberdomein toegespitste, bindende internationale regels afgesproken. Daarom kunnen ze alleen gebruik maken van abstracte internationaal-rechtelijke normen, die zeker op het gebied van cyberaanvallen nog veel interpretatie behoeven. Dit betekent dat als een staat aangevallen wordt, het niet duidelijk is welke reactie in overeenstemming is met het internationaal recht.

De bovenstaande vier factoren hebben geleid tot een riskant informatieconflict, waarin aanvallers de middelen en de gelegenheid hebben om kwetsbare systemen aan te vallen, en waarin deze aanvaller zich zelden met vergeldingen geconfronteerd ziet. In deze internationale situatie is het waarschijnlijk dat landen last blijven houden van cyberaanvallen door andere staten. Gelet op de bovengenoemde vier factoren is er een kans dat de cyberaanvallen escaleren, in die zin dat zowel de schadelijkheid als de frequentie van cyberaanvallen toenemen.

5.2 Vijf oplossingsrichtingen voor de-escalatie

Vanwege het gevaar voor de veiligheid van de digitale omgeving in Nederland en daarbuiten, is het daarom belangrijk om internationaal te werken aan een effectieve de-escalatie van cyberaanvallen. Daarbij zou de frequentie van cyberaanvallen omlaag moeten gaan, en de cyberaanvallen die de samenleving ondervindt zouden in ernst moeten afnemen. De vraag is hoe deze kentering teweeggebracht kan worden, en wie daarin welke verantwoordelijkheid neemt. We formuleren hieronder vijf oplossingsrichtingen die deze de-escalatie ondersteunen.

We bespreken ook een aantal beleidsopties en voorzien deze van commentaar. Hoewel Nederland in verschillende opzichten goede stappen heeft gezet, is er op internationaal niveau nog het nodige werk te verzetten.

5.2.1 Blijf samenwerken om de internationale cybersecurity te verhogen

Naast nationale stappen die gezet zijn om de weerbaarheid en cybersecurity te verhogen, en die het Rathenau Instituut heeft onderzocht in *Een nooit gelopen Race* (Munnichs et al. 2017), is het belangrijk dat Nederland blijft investeren in internationale cybersecurity samenwerkingen.

Dit nieuwe onderzoek laat zien dat op het niveau van de EU en van de NAVO intensief wordt samengewerkt om de digitale veiligheid verder te verbeteren: zo wordt er gewerkt aan het uitrollen van een breed netwerk van Cyber Emergency Incident Response Teams (het CERT-netwerk) en aan wetgeving voor de beveiliging van op het internet aangesloten apparaten (het Internet of Things), en investeren de organisaties in onderzoek, voorlichting en in trainingen. Bovendien zoeken de EU en de NAVO elkaar ook op om lessen te trekken en een gezamenlijke strategie te ontwikkelen.

Maar deze internationale ontwikkelingen betekenen niet dat de race tussen aanvallers en verdedigers in het voordeel van de verdedigers is beslecht. De aanvaller trekt nog geregeld aan het langste eind. Dit betekent dat internationale samenwerking geboden blijft. Dat is tot dusver ook het uitgangspunt geweest: Nederland heeft zich internationaal steevast bij cybersecurity-initiatieven aangesloten, en beziet deze initiatieven met een constructieve en kritische houding, bijvoorbeeld door op het gebied van de initiatieven van de EU te waarschuwen voor doublures (Minister van Buitenlandse Zaken 2018).

Van alle maatregelen om de dreiging van cyberaanvallen tegen te gaan, blijft het verhogen van de eigen cyberveiligheid de meest doeltreffende oplossing: het is minder riskant om een tegenstander te ontmoedigen en een informatieconflict te voorkomen dan om met dreigementen af te schrikken.

5.2.2 Maak heldere internationale afspraken voor de-escalatie op het gebied van cybersabotage, desinformatie en cyberspionage

Het overgrote deel van de cyberaanvallen vindt plaats in de fase van wat wij aanduiden als het informatieconflict. Hier zijn, zoals we beschreven, internationaal alleen generieke spelregels en normen voorhanden die landen verschillend kunnen interpreteren. Dit is in het voordeel van cyberaanvallers – zij gedijen bij de onzekerheid die een gebrek aan concrete spelregels en normen creëert.

Wanneer deze regels en normen geconcretiseerd worden, kan de internationale gemeenschap sneller en duidelijker reageren op een cyberaanval. Als dit bekend is, zal een land, voor het besluit aan te vallen, de baten van de aanval tegen de kosten afwegen.

De vraag is welke regels en normen er precies nodig zijn. Hier zijn belangrijke keuzes te maken. We zullen bespreken welke opties politici hebben. In ieder geval is het van belang dat de regels concreet zijn, en ondersteund worden in de praktijk en dat staten de afspraken naleven en verder uitwerken. We zullen eerst drie ideeën bespreken over de **vorm** die deze afspraken kunnen aannemen.

- Een veelgenoemd idee is een ‘Geneefse conventie voor cyberconflict’ (zie bijvoorbeeld Smith 2017). Zoals de Geneefse conventies regels geven voor conventionele oorlogsvoering, zou een cyberconventie normen kunnen formuleren voor cyberconflicten. Het is de vraag in hoeverre zo’n verdrag internationaal haalbaar is: de Geneefse conventies zijn grotendeels

ondertekend door China en Rusland, maar het is niet waarschijnlijk dat deze staten zich nu achter zo'n cyberverdrag scharen. Toch is het ook mogelijk met een kleinere groep staten een verdrag te ondertekenen. Gezien de generieke en soms ongeschreven aard van het relevante internationaal recht, zouden concretere normen die op papier staan een sterkere grond bieden om het gedrag van een staat te veroordelen en maatregelen te nemen.

- Naast een dergelijk juridisch verdrag kunnen ook meer vrijwillige afspraken gemaakt worden, als onderdeel van vertrouwenwekkende maatregelen (*confidence-building measures*). Deze maatregelen kunnen de samenwerking en transparantie tussen staten verbeteren, om zo het risico op misverstanden, escalatie en conflicten als gevolg van cyberbedreigingen te beperken (Van der Meer 2015). Zowel bilateraal als multilateraal kunnen deze maatregelen worden genomen. Denk aan het intensiveren van de inlichtingenuitwisseling over aanvallen op de vitale infrastructuur.

- Het is ook mogelijk dat staten eigenstandig aangeven hoe ze zullen omgaan met schendingen van hun soevereiniteit. Zeker wanneer staten eenzelfde houding aannemen, kan dit de wederzijdse verwachtingen stabiliseren. Onderdeel van die eigenstandige positie is bijvoorbeeld een taxatie van cyberaanvallen die aangeeft welke ernstiger bevonden worden dan andere, en wat voor reactie per soort aanval door cyberaanvallers verwacht mag worden. Dergelijke taxaties zijn al ontwikkeld door de Amerikaanse overheid en onlangs ook opgesteld door een Franse denktank (US-CERT 2018, Grisby 2018). Op deze manier zouden, bijvoorbeeld, de westerse landen samen grenzen kunnen stellen.

Ook op het gebied van de **inhoud** van internationale afspraken zijn er belangrijke keuzes te maken. Kwesties die in het oog springen zijn de omgang met spionage, de beoordeling van de verspreiding van desinformatie en de verschillende mogelijke tegenmaatregelen.

- Van oudsher wordt spionage tussen overheden geaccepteerd als *part of the deal*, zolang de spionage zich niet uitstrekt tot het beroven van private organisaties. Maar het is gezien de aard van cyberaanvallen de vraag in hoeverre deze traditionele afspraak in het huidige informatietijdperk houdbaar is – als een hacker eenmaal binnen in een systeem is, is sabotage binnen handbereik. Het zou bijvoorbeeld vertrouwen wekken als landen met elkaar zouden afspreken vitale systemen niet te infiltreren in vredestijd. Dat zou natuurlijk betekenen dat cybermachten als de Verenigde Staten en het Verenigd Koninkrijk macht inleveren. Ons onderzoek laat zien dat een situatie waarin landen elkaars cyberverdediging overhoop mogen halen, maar

vervolgens geacht worden van die toegang geen misbruik te maken, onhoudbaar is.

- De verspreiding van desinformatie kan in veel gevallen het functioneren van de democratische rechtsstaat, zowel op bepaalde kritieke momenten als meer sluipenderwijs op de wat langere termijn, ondermijnen. Deze destabilisatie is doorgaans ook het beoogde doel van een desinformatiecampagne. Dit soort cyberaanvallen kunnen, zo laat ons onderzoek zien, vergeleken worden met het gebruik van chemische wapens: een ontoelaatbaar middel voor een beschaafde democratische rechtsstaat. Staten als Rusland, Iran en China kennen nauwelijks een open en kritische informatievoorziening en het past een democratische staat niet om die informatievoorziening in een ander land nog verder te vertroebelen. Hoogstens kan het legitiem zijn om bijvoorbeeld Russische onafhankelijke journalistiek een steun in de rug te geven. Maar het verspreiden van desinformatie, die de rechtsorde verzwakt, kan geen middel zijn dat een fatsoenlijke staat hanteert.

- Ten slotte is er een fundamentele keuze te maken in het soort tegenmaatregelen dat in reactie op een cyberaanval genomen wordt. Men kan vuur met vuur bestrijden, en een vergelijkbare cybertegenaanval inzetten. We hebben hierboven al aangegeven dat dit in het geval van de ondermijning van een democratische rechtsorde onverantwoord is. Ook veel andere cyberaanvallen raken direct civiele instellingen en voorzieningen – doelwitten die volgens het humanitair oorlogsrecht zelfs in oorlogstijd zo veel mogelijk ontzien moeten worden. Het is daarom de vraag of democratische landen zoals Nederland met gelijke wapens kunnen reageren; ze kunnen ook met andere middelen reageren, door bijvoorbeeld gebruik te maken van het Europese sanctiepakket, en door diplomatieke en economische maatregelen te nemen. Ook het ontmaskeren van een cyberoperatie en het uitzetten van spionnen, zoals afgelopen april gebeurde, is een voorbeeld van een andersoortige sanctie (Boere 2018).

  Het overwegen van deze alternatieve middelen roept de vraag op of cybertegenaanvallen de cyberveiligheid structureel verhogen. Iedere aanval draagt bij aan de proliferatie van wapens, en cyberconflicten zijn tot dusver nog nooit geëindigd door een beslissende tegenaanval. Bovendien worden in de literatuur serieuze kanttekeningen geplaatst bij de effectiviteit van een dergelijke afschrikkingsstrategie (Goodman 2010, Iasiello 2013, Clarke & Knake 2010). Als toch tot een cybertegenaanval wordt overgegaan, dan is het zaak dit wel onmiddellijk en in samenwerking met bondgenoten te doen. Als er gedreigd wordt zonder dat opvolging plaatsheeft, valt het afschrikwekkend effect weg.

Op het gebied van internationale afspraken heeft Nederland, een traditionele voortrekker op het gebied van internationale samenwerking, al veel stappen gezet. Zo droeg Nederland bij aan de totstandkoming van het Tallinn Handboek en heeft de regering aangekondigd te zullen investeren in internationale normontwikkeling en cyberdiplomatie (Ministerie van Buitenlandse Zaken 2017, 2018). Maar juist op het gebied van internationale normen staan nog veel vragen open; het is belangrijk de Nederlandse inzet te versterken.

5.2.3 Zorg dat het cyberarsenaal verantwoord wordt beheerd

Zoals gezegd kan *malware* zich in seconden over de wereld verspreiden: dat is de prijs die we betalen voor een wereldomspannend internet. Wie een cyberwapen inzet, kan erop rekenen dat de gebruikte code in onvoorziene handen terechtkomt, en wellicht als een boemerang terugkeert. Dit betekent dat het belangrijk is om cyberwapens zorgvuldig in te zetten, en dat eenmaal ontdekte kwetsbaarheden gemeld worden. Bij de-escalatie van cyberconflicten is een grote rol weggelegd voor programmeurs; die kunnen veel *malware* onschadelijk maken.

Het is van belang dat inlichtingendiensten en defensieonderdelen internationaal samenwerken met softwareproducenten en chipfabrikanten om beveiligingsupdates door te voeren en deze onder gebruikers te verspreiden. Daarbij is het goed als inlichtingendiensten en defensieonderdelen zich continu afvragen wat de cyberveiligheid meer vergroot: het bezitten van een bepaald cyberwapen of het vrijgeven ervan? Als internationale bondgenoten meer open kaart met elkaar spelen, kunnen zij gezamenlijk de huishouding van kwetsbaarheden monitoren. Uiteindelijk weegt het langetermijnbelang van betrouwbare en veilige digitale toepassingen sterker dan het kortetermijnbelang, waarbij onveilige software wordt geduld om specifieke operaties mogelijk te maken.

Een verantwoord beheer van het cyberarsenaal heeft ook gevolgen voor de samenwerking met private partijen. Het gevaar bestaat dat een sterke private of malafide wapenindustrie uiteindelijk bijdraagt aan de proliferatie van wapens, en tegenstanders toegang geeft tot offensieve cybercapaciteit. Daarnaast bestaat altijd het risico dat private partijen bestolen worden. Niet voor niets heeft de Duitse overheid onlangs besloten om cyberwapens door een eigen staatsagentschap te laten ontwikkelen (Delcker 2018).

Een helder kader voor deze afwegingen kan de Nederlandse overheid helpen bij de vraag welke private partners bij de ontwikkeling van offensieve cybercapaciteit te betrekken, dan wel ontwikkelingen meer in eigen handen te nemen. Wanneer met

private partners samengewerkt wordt, is het belangrijk dat er voorwaarden gelden die ervoor zorgen dat gevaarlijke technologie niet in de handen valt van gevaarlijke regimes. Een internationale inzet op een systeem van exportvergunningen kan daarbij helpen (Ministerie van Buitenlandse Zaken 2018).

5.2.4 Bescherm de onafhankelijkheid van technologiebedrijven

Technologiebedrijven zoals Microsoft, Google en IBM vervullen een cruciale rol in de beveiliging van de digitale omgeving. Zij dichten de gaten in hun software en kunnen robuuste digitale toepassingen op de markt brengen. Dit betekent dat deze bedrijven hun onafhankelijkheid moeten kunnen behouden en geen verlengstukken worden van nationale overheden.

Het is belangrijk om bedrijven te ondersteunen om zo veilig mogelijk te opereren. Overheden nemen een risico als ze van bedrijven eisen de veiligheid van producten heimelijk te verzwakken. Overheden moeten zowel de technologie als de technologie-bedrijven dus verstandig reguleren.

Kaspersky Labs en Huawei Technologies staan vanwege hun verbondenheid met respectievelijk Rusland en China onder grote druk. En dat is niet onbegrijpelijk. De overheden van Rusland en China wenden hun macht regelmatig aan door voor en achter de schermen te interveniëren in bedrijven (Klimburg 2017, Kharpal 2019). En ook Amerikaanse bedrijven werken, al dan niet gedwongen, soms intensief samen met inlichtingendiensten, zoals in het recent hernieuwde PRISM-programma van de NSA (Volz 2018, Zetter 2013).

Hoe de Nederlandse regering in de toekomst precies omgaat met spelers zoals Huawei en Kaspersky, hangt af van de mate waarin de Chinese en Russische overheden invloed hebben op deze bedrijven. Het is belangrijk dat technologiebedrijven betrouwbaar en onafhankelijk kunnen werken en dat ze hun verantwoordelijkheid nemen voor veiligheid – zowel binnen daarvoor gestelde kaders als proactief. Bedrijven hebben zich via het Global Tech Accord, samen met landen als Nederland, aangesloten bij de Paris Call for Trust and Security in Cyberspace. De relatie tussen overheden en bedrijven ligt natuurlijk anders als het cyberwapenbedrijven betreft – cyberwapenproductie valt onder een eigen normenregime.

5.2.5 Investeer in een maatschappelijk debat over internationale cyberveiligheid

Het informatieconflict is bij uitstek een onderwerp voor democratisch debat: juist burgers worden geraakt door cyberaanvallen. Nog meer dan bij andere conflicten zijn zij het doelwit; zij worden misleid door desinformatie, vitale voorzieningen worden gehackt en bedrijven zals banken worden bespied. Daardoor staan fundamentele burgerrechten, zoals het recht op privacy, het recht op veiligheid en onze democratische rechten, op het spel. We moeten weerbaar zijn. Ook is het aan burgers om richting te geven aan de digitale toekomst. De afweging bepaalde wapens aan te schaffen en bepaalde operaties te autoriseren is niet alleen een aangelegenheid van experts en ambtenaren met een bijzondere bevoegdheid.

De-escalatie van het informatieconflict vraagt daarom om een maatschappelijk en politiek debat over dit voortdurende conflict, en de Nederlandse opstelling daarin. Daarvoor biedt ieder van de vier hierboven genoemde oplossingsrichtingen een belangrijk gespreksonderwerp.

Het belang van geheimhouding door inlichtingendiensten en defensie moet daarom per voorkomend geval afgewogen worden tegen het belang van Nederlandse burgers om inzicht te krijgen in de cyberoperaties van de overheid. Hoe groter de impact is van de internationale cyberconflicten op de samenleving, hoe groter het belang is om een relevant publiek debat hierover mogelijk te maken.

Om als burger weerbaar te kunnen zijn, is informatie hard nodig: geïnformeerde burgers kunnen desinformatie herkennen en ontmaskeren, en essentiële veiligheidsmaatregelen nemen. Het Rathenau Instituut pleitte al eerder voor het bevorderen van technologisch burgerschap (Van Est 2017, Van Keulen et al 2018), en in de discussie rondom offensieve cybercapaciteiten komen alle elementen hiervan terug. Burgers die begrijpen hoe technologie hun levens beïnvloedt, en die zinnige inspraak hebben in de politieke keuzes die op het gebied van nieuwe technologie gemaakt worden, zijn weerbaarder tegen ondermijnende cyberaanvallen dan burgers die dat niet kunnen.

De overheid heeft dan ook een bijzondere verantwoordelijkheid om dit technologisch burgerschap mogelijk te maken. Zeker wat betreft de voorlichting over en opleiding in mediawijsheid zet de overheid al goede stappen (Rijksoverheid 2018) – maar meer is nodig. Het is van belang om ook de keuzes en dilemma's, zoals hierboven aangegeven, in een maatschappelijk debat te bespreken. Juist dan kan Nederland op democratische wijze de internationale cyberdreiging het hoofd bieden en draagvlak creëren voor een internationale inspanning, zowel via diplomatie als via andere afspraken.

Literatuurlijst

Adkins, G. (2013). Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism. In: *Journal of Strategic Security* 6(3), 1-9.

Adviesraad Internationale Vraagstukken (AIV), Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) (2011), *Digitale Oorlogvoering*. Online beschikbaar: https://aiv-advies.nl/download/9fc55422-c96d-4563-9279-f434803c0afd.pdf.

Agence France-Presse (2016). 'Germany to further curb activities of spy agency in wake of NSA scandal'. The Guardian 28 juni 2016. Online beschikbaar: https://www.theguardian.com/world/2016/jun/28/germany-curb-spy-agency-nsa-scandal-angela-merkel.

Algemene Inlichtingen- en Veiligheidsdienst, Militaire Inlichtingen- en Veiligheidsdienst (2017). *Cyberespionage: Are you aware of the risks*?.

Algemene Inlichtingen- en Veiligheidsdienst (2019). *Cyberdreiging*. Online beschikbaar: https://www.aivd.nl/onderwerpen/cyberdreiging.

Andress, J. & S. Winterfeld (2011), *Cyber Warfare, Techniques, Tactics and Tools for Practitioners*, Syngress.

Avaaz (2019). 'Social media reports fail to address scale of threat: Avaaz calls for emergency steps to issue corrections for disinformation'. Avaaz website. Online beschikbaar: https://secure.avaaz.org/act/media.php?press_id=930.

Ball, J., J. Borger & G. Greenwald (2013). 'Revealed: how US en UK spy agencies defeat internet privacy and security'. The Guardian 6 september 2013. Online beschikbaar: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Bartles, C.K. (2016). Getting Gerasimov Right. In: *Military Review*, januari-februari: 30-38.

Benatar, M. (2009) The use of cyber force: Need for legal justification? In: Goettingen Journal of International Law 1, 375-396.

Bilge, L. & T. Dumitras, (2012), Before we knew it, an empirical study of zero-day attacks in the real world, In: *Proceedings of the 2012 ACM conference on Computer and communications security*, 833-844.

Binding, L. (2018). ‘GCHQ intelligence chief threatens 'brazen' Russia with UK's 'tools'. Sky News 7 september 2018. Online beschikbaar: https://news.sky.com/story/gchq-intelligence-chief-threatens-brazen-russia-with-uks-tools-11492237.

Boere, R. (2018), ‘Ontluisterend inkijkje in het werk van vier Russische spionnen’. Algemeen Dagblad 4 oktober 2018. Online beschikbaar: https://www.ad.nl/binnenland/ontluisterend-inkijkje-in-het-werk-van-vier-russische-spionnen~a86c66f1/.

Boffey, D. (2018). ‘British spies 'hacked into Belgian telecoms firm on ministers' orders'. The Guardian 21 september 2018. Online beschikbaar: https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report.

Bowcott, O., ‘China's hackers stealing US defence secrets, says congressional panel’. The Guardian 20 november 2008. Online beschikbaar: https://www.theguardian.com/world/2008/nov/20/america-china-hacking-security-obama.

Branigan, T. (2010). ‘Google to end censorship in China over cyber attacks’. The Guardian 13 januari 2010. Online beschikbaar: https://www.theguardian.com/technology/2010/jan/12/google-china-ends-censorship.

Burton, J. (2015), NATO ’s cyber defence: strategic challenges and institutional adaptation. In: *Defence Studies*, november, 1-22.

Cebrowski, A.K. & J.H. Garstka (1998). Network-Centric Warfare: Its Origin and Future. In: *US Naval Institute Proceedings*, 124(1), 28-35.

Chan, E. & A. Nour (2018). ‘Microsoft Thwarts Russia Hackers Targeting GOP Critics of Trump’. Bloomberg 21 augustus 2018. Online beschikbaar: https://www.bloomberg.com/news/articles/2018-08-21/microsoft-finds-new-russian-effort-to-hack-u-s-political-groups.

Chase, M.S., J. Engstrom, T.M. Cheung, K.A. Gunnes, S.W. Harold, S. Puska & S.K. Berkowitz (2015). *China's Incomplete military transformation*. Rand corporation.

Choucri, N., S. Madnick, & J. Ferwerda (2013), Institutions for Cyber Security: International Responses and Global Imperatives. In: *Information Technology for Development* 20(2), 96-121.

Clapper, J.R. (2013). *Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage*, Office of the Director of National Intelligence.

Clarke, R.A. & R. Knake (2010). *Cyber War*. HarperCollins.

Codron, S.M. (2007). Getting it right: Protecting American critical infrastructure in cyberspace. In: *Harvard Journal of Law & Technology* 20(2), 404-422. Online beschikbaar: http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech403.pdf.
Colarik, A.M. & L.J. Janczewski (Eds.) (2007), *Cyber Warfare and Cyber Terrorism*, IGI Global

Coldwell, W. (2014). 'Airbnb's legal troubles: what are the issues?'. The Guardian 8 juli 2014. Online beschikbaar: https://www.theguardian.com/travel/2014/jul/08/airbnb-legal-troubles-what-are-the-issues.

Conley, H.A., J. Mina, R. Stefanov & M. Vladimirov (2016). *The Kremlin Playbook*. Center for Strategic & International Studies.

Crawford, J. (2016), 'Massive IRS data breach much bigger than first thought', CBS news 29 februari 2016. Online beschikbaar: https://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/.

Crowell, C. (2017). 'Our approach to bots and misinformation'. Twitter 14 juni 2017. Online beschikbaar: https://blog.twitter.com/official/en_us/topics/company/2017/Our-Approach-Bots-Misinformation.html.

Curran, J., N. Fenton & D. Freedman (2012). *Misunderstanding the Internet*. Routledge.

Cybersecurity Tech Accord (2018). Online beschikbaar: https://cybertechaccord.org/.

Ducheine, P. & J. Van Haaster (2014). Fighting Power, Targeting and Cyber Operations. In: P. Brangetto, M. Maybaum & J. Stinissen (eds.), *6th international conference on cyber conflict*, Tallinn: NATO Publications.

Ducheine, P. (2018). Veiligheid en Cyberspace. In: Blind 49.

Defense Intelligence Agency (2017). *Russia Military Power*. Online beschikbaar: http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf.

Deibert, R., R. McKinnon, X. Qiang & T. Lokman, 'Open letter to Google on reported plans to launch a censored search engine in China'. Online beschikbaar: https://www.documentcloud.org/documents/4792329-Google-Dragonfly-Open-Letter.html.

Delcker, J. (2018). 'Germany to launch US-style agency to develop cyberdefense'. Politico 29 augustus 2018. Online beschikbaar: https://www.politico.eu/article/germany-to-launch-darpa-style-agency-to-develop-cyber-defense/.

DHS, ODNI, FBI (2016), 'Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity'. Online beschikbaar: https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity.

District Court of Columbia, Indictment 13 juli 2018. Online beschikbaar: https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf.
The Economist (2010). Special report on cyberwar: War in the fifth domain. 1 juli 2010.

The Economist (2017). China's internet giants go global. 20 april 2017. Online beschikbaar: https://www.economist.com/business/2017/04/20/chinas-internet-giants-go-global.

The Economist (2018). Defence companies target the cyber-security market. 26 juli. Online beschikbaar: https://www.economist.com/business/2018/07/26/defence-companies-target-the-cyber-security-market.

Ehrenfeld, J.M. (2017). Wannacry, Cybersecurity and Health Information Technology: a Time to Act. In: *Journal of Medical Systems* 41, 104.

Electricity Information Sharing and Analysis Center (E-ISAC), SANS Industrial Control Systems (SANS ICS) (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Online beschikbaar: zie https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf).

Epstein, R. (2015). 'How Google Could Rig the 2016 Election'. Politico 19 augustus 2015. Online beschikbaar: https://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548.

Est, van, R. (2017). *Technologisch burgerschap*, Den Haag: Rathenau Instituut. Online beschikbaar: https://www.rathenau.nl/nl/digitale-samenleving/technologisch-burgerschap-de-democratische-uitdaging-van-de-eenentwintigste.

Euractiv (2018). 'EU code of practice on fake news: Tech giants sign the dotted line'. Online beschikbaar: https://www.euractiv.com/section/digital/news/eu-code-of-practice-on-fake-news-tech-giants-sign-the-dotted-line/.

Europese Commissie (2013). *Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace*. Online beschikbaar: https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vj6ytdiaomzb.

Europese Commissie (2016). *Joint Framework on countering hybrid threats: a European Union response*. Online beschikbaar: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=SV.

Europese Commissie (2017a). *Joint Communication to the European Parliament and the Council*. Online beschikbaar: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450.

Europese Commissie (2017b). *Review of ENISA Regulation and laying down a EU ICT security certification and labelling*. Online beschikbaar: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3436811_en.

Europese Commissie (2018a). *Digital Single Market*. Online beschikbaar: https://ec.europa.eu/digital-single-market/.

Europese Commissie (2018b). *Code of Practice on Disinformation*. Online beschikbaar: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

Europese Commissie (2018c). *Fake news and online disinformation*. Online beschikbaar: https://ec.europa.eu/digital-single-market/en/fake-news-disinformation.

Europese Raad (2017). *Cyber attacks: EU ready to respond with a range of measures, including sanctions*. Online beschikbaar: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf, bezocht op 20-12-2018.

EU vs Disinfo (2018). website: https://euvsdisinfo.eu/about/.

Faris, R.M., H. Roberts, B. Etling, N. Bourassa, E. Zuckerman & Y. Benkler (2017), *Partisanship, Propaganda,and Disinformation: Online Media and the 2016 U.S. Presidential Election*. Berkman Klein Center for Internet & Society Research Paper.

Farrell, P. (2013), 'History of 5-Eyes – explainer'. The Guardian 2 december 2013. Online beschikbaar: https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

Farwell, J. & R. Rohozinski (2012). The new reality of cyber war. In: *Survival: Global Politics and Strategy* 54(4), 107-120.

Ferrara, E. (2017). *Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election*. Online beschikbaar: https://arxiv.org/abs/1707.00086.

FireEye (2014). *The PLA and the 8:00am-5:00pm Work Day: FireEye Confirms DOJ's Findings on APT1 Intrusion Activity*. Online beschikbaar: https://www.fireeye.com/blog/threat-research/2014/05/the-pla-and-the-800am-500pm-work-day-fireeye-confirms-dojs-findings-on-apt1-intrusion-activity.html.

FireEye (2018). Advanced Persistent Threat Groups. Online beschikbaar: https://www.fireeye.com/current-threats/apt-groups.html#apt29.

Fleck, D. (2013). Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict and Security Law* 18(2), 331–351.

Forum of Incident Response and Security Teams (2018), website: https://www.first.org/.

France Diplomatie (2018). *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*. Online beschikbaar: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-

and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Franke, U. (2015). *War by non-military means*. Swedish Defense Research Agency.

Freedom House (2018. *Freedom in the World 2018: Democracy in crisis*. Online beschikbaar: https://freedomhouse.org/report/freedom-world/freedom-world-2018.

Gallagher, R. (2017). 'NSA's Quiet Presence at a Base in England's Countryside Revealed in Snowden Documents'. The Intercept 13 september 2017. Online beschikbaar: https://theintercept.com/2017/09/13/digby-uk-nsa-gchq-surveillance/.

Gallagher, R. (2018). 'The Powerful Global Spy Alliance You Never Knew Existed'. The Intercept 1 maart 2018. Online beschikbaar: https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/.

Garamone, J. (2018) 'Cyber Tops List of Threats to U.S., Director of National Intelligence Says'. United States Department of Defense 13 februari 2018. Online beschikbaar: https://dod.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/.

German Federal Ministry of the Interior (2011). *Cyber Security Strategy for Germany*. Online beschikbaar: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany.

Giles, K. (2016), *Russia's 'new' tools for confronting the west*, Chatham House research paper. Online beschikbaar: https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf.

Global Forum on Cyber Expertise (2017), *Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building*. Online beschikbaar: https://www.thegfce.com/documents/publications/2017/11/24/delhi-communique.

Goodman, W. (2010). Cyber Deterrence. Tougher in Theory than in Practice? In: *Strategic Studies Quarterly* 2010 (3), 102-135.

Gorman, S. & J.E. Barnes (2012). 'Iran Blamed for Cyberattacks'. The Wall Street Journal 12 oktober 2012. Online beschikbaar: https://www.wsj.com/articles/SB10000872396390444657804578052931555576700
.

Government of Russia (2014), *Military doctrine of the Russian Federation*. Online beschikbaar: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf.

Greenberg, A. (2018). ‘The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History'. Wired 15 februari 2018,. Online beschikbaar: https://www.wired.com/story/white-house-russia-notpetya-attribution/.

Graham, M. (2016). U.S. Cyber Force: One War Away. In: *Military Review* 96(3), 111.

Grant, I. (2008). ‘Nato sets up Cyber Defence Management Authority in Brussels’. Computer Weekly 4 april 2008. Online beschikbaar: https://www.computerweekly.com/news/2240085580/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels.

Grisby, A. (2018). Three Takeaways from the French Cyber Defense Review. Council on Foreign Relations. Online beschikbaar: https://www.cfr.org/blog/three-takeaways-french-cyber-defense-review.

Group of Seven (2017). *G7 Declaration on Responsible States Behavior in Cyberspace*. Online beschikbaar: https://www.mofa.go.jp/files/000246367.pdf.

Group of Seven (2018). *Charlevoix Commitment on Defending Democracy from Foreign Threats.* Online beschikbaar: https://www.mofa.go.jp/files/000373846.pdf.

Group of Seven (2019a). Website: http://www.g7italy.it/en/history/.

Group of Seven (2019b). *Dinard Declaration on the Cyber Norm Initiative*. Foreign Ministers Meeting 6 april 2019. Online beschikbaar: https://www.diplomatie.gouv.fr/IMG/pdf/g7_-_dinard_declaration_on_cyber_initiative_cle811175.pdf.

Group of Seven (2019c). *Foreign Ministers Communiqué*. Foreign Ministers Meeting 6 april 2019. Online beschikbaar: https://www.diplomatie.gouv.fr/IMG/pdf/g7_-_foreign_ministers_communique_cle8245be.pdf.

Gross, M. (2011a). ‘The fog of cyber-war’. Vanity Fair april 2011, 155–198.

Gruyter, de, C. (2018). ‘De koude oorlog was voorspelbaarder, dit kan escaleren’. NRC 17 maart 2018. Online beschikbaar: : https://www.nrc.nl/nieuws/2018/03/27/de-koude-oorlog-was-vo

Haberman, C. (2017). ‘Who’s Fueling Conspiracy Whisperers’ Falsehoods?’. The New York Times 20 april 2017. Online beschikbaar: www.nytimes.com/2017/04/30/us/retro-report-conspiracy-theories-kennedy-trump.html.

Harambam, J. (2017). De politisering van de waarheid. *Sociologie* 13(1), 73-92.

Harari, Y.(2018). ‘Why technology favors tyranny’, The Atlantic oktober 2018. Online beschikbaar: https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/.

Healey, J. & L. van Bochhoven (2011). *NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow*, Issue Brief Atlantic Council. Online beschikbaar: https://www.files.ethz.ch/isn/169072/022712_ACUS_NATOSmarter_IBM.pdf.

Hernandez, J.C. & Z. Mou (2018). ‘I Am Gay, Not a Pervert’ Furor in China as Sina Weibo Bans Gay Content’. The New York Times 15 april 2018. Online beschikbaar: https://www.nytimes.com/2018/04/15/world/asia/china-gay-ban-sina-weibo-.html

Herr, T. & P. Rozenzweig (2013). Cyber Weapons and Export Control: Incorporating Dual Use with the PrEp Model. In: *Journal of National Security Law and Policy* 8, 301.

Hopkins, N., J. Borger & L. Harding (2013). ‘GCHQ: inside the top secret world of Britain's biggest spy agency’. The Guardian 2 augustus 2013. Online beschikbaar: https://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden.

Iasiello, E. (2015). Are Cyber Weapons Effective Military Tools? In: *Military and Strategic Affairs* 7(1), 23-40.

Inkster, N. (2016). *China’s Cyber Power*. Adelphi Series.

Insikt Group (2019). *Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion*. Recorded Future. Online beschikbaar: https://www.recordedfuture.com/china-social-media-operations/.

International Journalism for EU (2018), *IJ4EU: Funding cross-border investigative reporting in Europe*. Online beschikbaar: https://www.investigativejournalismforeu.net/guidelines/.

International Multilateral Partnership Against Cyber Threats (2018). Website: http://www.impact-alliance.org/home/index.html.

International Telecommunications Union (2008). *High-Level Experts Group Global Strategic Report*. Online beschikbaar: https://ccdcoe.org/sites/default/files/documents/ITU-080801-HLEGreport.pdf.

International Telecommunications Union (2018), website: see ww.itu.int.

The Internet Corporation for Assigned Names and Numbers (2018a). *Welcome to ICANN!*, Online beschikbaar: https://www.icann.org/resources/pages/welcome-2012-02-25-en.

The Internet Corporation for Assigned Names and Numbers (2018b). *Root DNSSEC*. Online beschikbaar: http://www.root-dnssec.org.

Jaeger, P.T., J.C. Bertot & C.R. McClure (2003), The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. In: *Government Information Quarterly* 20, 295-314.

Jensen, E.T. (2002). Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense. In: *Stanford Journal of International Law* 38, 207-240.

Kallberg, J., A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs. In: *IT Professional* 17(1), 30-35.

Kaplan, C. (2015). Air power's visual legacy: Operation Orchard and aerial reconnaissance imagery as ruses de guerre. In: *Critical Military Studies* 1(1), pp. 61-78.

Karatzogianni, A. (ed.) (2008). *Cyber-conflict and global politics*. London: Routledge.

Kaspersky Lab (2016). *Measuring the Financial Impact of IT-security on Businesses*. Online beschikbaar: https://media.kaspersky.com/en/business-security/kaspersky-it-security-risks-report-2016.pdf.

Keulen, van, I., I. Korthagen, P. Diederen & P. van Boheemen (2018). *Digitalisering van het nieuws – Online nieuwsgedrag, desinformatie en personalisatie in Nederland*. Den Haag: Rathenau Instituut.

Khalip, A. (2018). ‘U.N. chief urges global rules for cyber warfare’. Reuters 19 februari 2018. Online beschikbaar: https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.

Kharpal, A. (2019). ‘Huawei says it would never hand data to China’s government. Experts say it wouldn’t have a choice’. CNBC 5 maart 2019. Online beschikbaar: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

Klimburg, A. (2017). *The Darkening Web*. New York: Penguin Press.

Kobie, N. (2018). ‘The odd reality of life under China's all-seeing credit score system’. Wired 5 juni 2018. Online beschikbaar: https://www.wired.co.uk/article/china-social-credit.

Kool, Daan (2019), ‘Franse gelehesjesbeweging deelt veelvuldig nepnieuws’. De Volkskrant 13 maart 2019. Online beschikbaar: https://www.volkskrant.nl/nieuws-achtergrond/franse-gelehesjesbeweging-deelt-veelvuldig-nepnieuws~b6c0b4a4/.

Krepinevich, A.F. (2012). Strategy in a time of Austerity. In: *Foreign Affairs* november/december 2012. Online beschikbaar: https://www.foreignaffairs.com/articles/global-commons/2012-11-01/strategy-time-austerity.

Libicki, M.C. (2016). *Cyberspace in War and Peace*. Annapolis: Naval Institute Press.

Lucas, G.R. (2017). *Ethics and cyber warfare: The quest for responsible security in the age of digital warfare*. Oxford: Oxford University Press.

MacAskill, E. (2015). ‘Britain creates team of Facebook warriors’. The Guardian 31 januari 2015. Online beschikbaar: https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade.

Mackenzie, C. (2019). ‘French defense chief touts offensive tack in new cyber strategy’. Fifth Domain 18 januari 2019. Online beschikbaar: https://www.fifthdomain.com/global/europe/2019/01/18/french-defense-chief-touts-offensive-tack-in-new-cyber-strategy/.

Markushin, D. (2017). ‘The cost of launching a ddos attack’. Securelist 23 maart 2017. Online beschikbaar: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/.

Matishak, M. (2018). ‘What we know about Russia’s election hacking’. Politico 19 juli 2018. Online beschikbaar: https://www.politico.eu/article/russia-hacking-us-election-what-we-know/.

Matsakis, L. (2018). ‘The US Sits out an International Cybersecurity Agreement’. Wired 11 november 2018. Online beschikbaar: https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

McAfee (2011). *Global Energy Cyberattacks: ‘Night Dragon*’. Online beschikbaar: https://thanatosdotme.files.wordpress.com/2016/04/wp-global-energy-cyberattacks-night-dragon.pdf.

McDonald, M. (2012). ‘Adding more bricks to the great firewall of China’. The New York Times 23 december 2012. Online beschikbaar: https://rendezvous.blogs.nytimes.com/2012/12/23/adding-more-bricks-to-the-great-firewall-of-china/.

Meer, van der, S. (2015). Enhancing international cyber security. A key role for diplomacy. In: *Security and Human Rights* 26, 193-205.

Meer, van der, S. (2018a). ‘Nederland, gun de VS niet het recht van de sterkste in digitale oorlogvoering’. Trouw 12 april 2018.

Meer, van der, S. (2018b). *State-level responses to massive cyber-attacks: a policy toolbox*. Den Haag: Clingendael. Online beschikbaar: https://www.clingendael.org/sites/default/files/2018-12/PB_cyber_responses.pdf.

Mele, S. (2013). *Cyber-weapons: Legal and Strategic Aspects, Version 2.0*. Italian Institute of Strategic Studies.

Minister van Buitenlandse Zaken (2018). ‘Fiche: Mededeling weerbaarheid vergroten, versterken capaciteiten om hybride dreigingen aan te pakken’. Brief van de minister van buitenlandse zaken nr. 2693.

Ministerie van Buitenlandse Zaken (2017). *Internationale Cyberstrategie Digitaal Bruggen Slaan*. Online beschikbaar: https://www.rijksoverheid.nl/documenten/rapporten/2017/02/12/internationale-

cyberstrategie-naar-een-geintegreerd-internationaal-cyberbeleid-getitield-digitaal-bruggen-slaan.

Ministerie van Buitenlandse Zaken (2018). *Wereldwijd voor een veilig Nederland*. Oline beschikbaar: https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs.

Modderkolk, H. (2018). 'Dutch agencies provide crucial intel about Russia's interference in US-elections'. De Volkskrant 25 januari 2018. Online beschikbaar: https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/.

Modderkolk, H. (2018). 'In gesprek met Jesse S. (18), die met ddos-aanvallen de Belastingdienst en banken zou hebben platgelegd'. De Volkskrant 6 februari 2018. Online beschikbaar: https://www.volkskrant.nl/tech/in-gesprek-met-jelle-s-18-die-met-ddos-aanvallen-de-belastingdienst-en-banken-zou-hebben-platgelegd~a4567183/.

Morello, C. (2018). 'Mike Pompeo announces US government to increase broadcasting in Iran while likening country's rulers to the mafia'. Independent 23 juli 2018. Online beschikbaar: https://www.independent.co.uk/news/world/americas/mike-pompeo-iran-mafia-sanctions-rouhani-trump-twitter-a8459561.html.

Mozur, P. (2017). 'China spreads propaganda to U.S. on Facebook, a platform it bans at home'. The New York Times 8 november 2017. Online beschikbaar: https://www.nytimes.com/2017/11/08/technology/china-facebook.html.

Munnichs, G.M., M. Kouw & L. Kool (2017). *Een nooit gelopen race: over cyberdreigingen en versterking van weerbaarheid*. Den Haag: Rathenau Instituut.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Cybersecurity beeld Nederland* 2018.

National Security Agency (2018), website: https://www.nsa.gov/.

NBC (2014). 'Exclusive: Snowden Docs Show British Spies Used Sex and 'Dirty Tricks''. 7 februari 2014. Online beschikbaar: https://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-british-spies-used-sex-dirty-tricks-n23091.

The New York Times Editorial Board (2016). ‘President Obama punishes Russia, at last’. New York Times 29 december 2016. Online beschikbaar: https://www.nytimes.com/2016/12/29/opinion/president-obama-punishes-russia-at-last.html.

Noord-Atlantische Verdragsorganisatie (NAVO) Communications and Information Agency (2018). website: https://www.ncia.nato.int/Pages/homepage.aspx.

NAVO (2002). *Prague Summit Declaration*. Online beschikbaar: http://www.ccdcoe.org/sites/default/files/documents/NATO-021121-PragueSummitDeclaration.pdf.

NAVO (2008). *Bucharest Summit Declaration*. Online beschikbaar: https://www.nato.int/cps/us/natohq/official_texts_8443.htm.

NAVO (2011). *Defending the Networks, the NATO policy on cyber defence*. Online beschikbaar: https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

NAVO (2014). *Wales Summit Declaration*. Online beschikbaar: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NAVO (2016a). *NATO cyber defence*. Online beschikbaar: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

NAVO (2016b). *Warsaw Summit Communiqué*. Online beschikbaar: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NAVO Cooperative Cyber Defence Center of Excellence (NAVO CCDCOE) (2018). *Organisations: NATO*. Online beschikbaar: https://ccdcoe.org/nato.html.

NAVO CCDCOE (2018), *Shanghai Cooperation Organisation*. Online beschikbaar: https://ccdcoe.org/sco.html.

Nodurft, R. (2018). ‘Breaking down the numbers in Trump's proposed cyber budget’. The Hill 27 februari 2018. Online beschikbaar: https://thehill.com/opinion/cybersecurity/375812-breaking-down-the-numbers-in-trumps-proposed-cyber-budget.

NOS (2018), ‘Ook Ollongren wil nu af van Europese waakhond nepnieuws’. NOS 9 maart 2018. Online beschikbaar: https://nos.nl/artikel/2221353-ook-ollongren-wil-nu-af-van-europese-waakhond-nepnieuws.html.

O’Conner, T. (2017). ‘German military battles foreign hacking with new cyber soldiers’. Newsweek 4 mei 2017. Online beschikbaar: https://www.newsweek.com/german-military-launches-new-cyber-division-amid-russian-hacking-claims-579573.

Organisatie voor Vrede en Veiligheid in Europa (2018). Website: https://www.osce.org/.

Organisatie voor Vrede en Veiligheid in Europa (2016). *OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*. Decision no. 1202.

Os, van, P. (2017). ‘Het Poolse journaal bedrijft ongekende propaganda’, De Groene Amsterdammer 51-52.

Pennetier, M. (2017). ‘Under threat, France grooms army hackers for cyber warfare’. Reuters 5 april 2017. Online beschikbaar: https://www.reuters.com/article/us-france-cyber/under-threat-france-grooms-army-hackers-for-cyber-warfare-idUSKBN1771B2.

Peterson, A. (2013). ‘The NSA has its own team of elite hackers’. The Washington Post 29 augustus 2013. Online beschikbaar: https://www.washingtonpost.com/gdpr-consent/?destination=%2fnews%2fthe-switch%2fwp%2f2013%2f08%2f29%2fthe-nsa-has-its-own-team-of-elite-hackers%2f%3f&utm_term=.db94d0e0dd26.

Poitras, L. & M. Rosenbach (2013). ‘NSA Spied on European Union Offices’. Spiegel 29 juni 2013. Online beschikbaar: http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html.

Politie (2018). *Phishing*. Website: https://www.politie.nl/themas/phishing.html.

Pollpeter, K., M. Chase & E. Heginbotham (2017). *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*. Rand Corporation.

Polyakova, A. & S. Boyer (2018). *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*. Brookings-Robert Bosch Foundation.

Qiao, L. & W. Xiangsui (2015). *Unrestricted Warfare*. Shadow Lawn Press.

Rathenau Instituut (2018). *Zo werken de bots in Nederland*. Online beschikbaar: https://www.rathenau.nl/nl/digitale-samenleving/digitalisering-van-het-nieuws/desinformatie-zo-werken-bots-nederland
.
Rathenau Instituut (2019). *Desinformatie in Nederland*. *Bericht aan het parlement*. Online beschikbaar: https://www.rathenau.nl/nl/digitale-samenleving/desinformatie-nederland.

Rauscher, K.F. & Korotkov, A. (2011). *Towards rules for governing cyber conflict. Rendering the Geneva and Hague conventions in cyberspace*. Brussel: EastWest Institute.

Reed, T. (2005). *At the Abyss: an insider's history of the cold war*. Presidio Press.
Rid, T. (2012). Cyberwar will not take place. In: *Journal of Strategic Studies* 35, 5-32.

Rid, T. (2013). Cyberwar and Peace: Hacking Can Reduce Real-World Violence. In: *Foreign Affairs* 92, 77-87.

Rigter, N. (2017). 'Cybercommando nu al overvraagd'. De Telegraaf 17 februari 2017. Online beschikbaar: https://www.telegraaf.nl/nieuws/1319419/cybercommando-nu-al-overvraagd.

Rijksbegroting 2018. Online beschikbaar: http://www.rijksbegroting.nl/2018/voorbereiding/begroting.

Rijksoverheid 2019. *Campagne 'Desinformatie en nepnieuws'*. Online beschikbaar: https://www.rijksoverheid.nl/onderwerpen/campagnes/lopende-campagnes/campagne-desinformatie-en-nepnieuws.

Ritchie. H. (2016), 'Fake News stories of 2016'. CNBC 30 december 2016. Online beschikbaar: https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html.

Roden, L. (2017). 'Swedish kids to learn computer coding and how to spot fake news in primary school'. The Local 13 maart 2017. Online beschikbaar:

https://www.thelocal.se/20170313/swedish-kids-to-learn-computer-coding-and-how-to-spot-fake-news-in-primary-school.

Royakkers, L. & R. van Est (2016). *Just Ordinary Robots: Automation from Love to War*. CRC Press.

Sanger, D. (2018). *The Perfect Weapon*. Crown Publishing.

Sanger, D.E. & S.L. Myers (2018). 'After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology'. The New York Times 29 november 2018. Online beschikbaar: https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.

Sargentini, J. (2018). *Report on a proposal calling on the Council to determine, pursuant to Article 7(1) of the Treaty on European Union, the existence of a clear risk of a serious breach by Hungary of the values on which the Union is founded*. A8-0250/2018.

Schell, O. (2016). 'Crackdown in China: Worse and Worse'. The New York Review of Books 21 april 2016. Online beschikbaar: https://www.nybooks.com/articles/2016/04/21/crackdown-in-china-worse-and-worse/.

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

Schmitt, M. & L. Vihul (eds.) (2017a). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Schmitt, M. & L. Vihul (2017b). Sovereignty in Cyberspace: Lex Lata Vel Non?. *American Journal of International Law* 111, 213-218.

Schneider, B. (2017), 'Who are the Shadow Brokers?'. The Atlantic 23 mei 2017. Online beschikbaar: https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.

Sengupta, K. (2015). 'New British Army unit 'Brigade 77' to use Facebook and Twitter in psychological warfare'. Independent 31 januari 2015. Online beschikbaar: https://www.independent.co.uk/news/uk/home-news/return-of-the-chindits-mod-reveals-cunning-defence-plan-10014608.html.

The Shanghai Cooperation Organisation (2006). *Declaration on the Fifth Anniversary of SCO*. Online beschikbaar: http://www.chinadaily.com.cn/china/2006-06/15/content_618177_3.htm.

The Shanghai Cooperation Organisation (2017), *The Shanghai Cooperation Organisation*. Online beschikbaar: http://eng.sectsco.org/about_sco/20170109/190857.html.

Smith, B. (2017). 'The need for a Digital Geneva Convention'. Microsoft 14 februari 2017. Online beschikbaar: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv.

Soesanto, S. & F. D'Incau (2017). 'The UN GGE is dead: Time to fall forward', European Council on Foreign Relations 15 augustus 2017. Online beschikbaar: https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

Solon, O. (2018). 'A grand illusion': seven days that shattered Facebook's façade'. The Guardian 24 maart 2018. Online beschikbaar: https://www.theguardian.com/technology/2018/mar/24/cambridge-analytica-week-that-shattered-facebook-privacy.

Stavridis, J. (2017). 'The United States Is Not Ready for a Cyber-Pearl Harbor'. Foreign Policy 15 mei 2017. Online beschikbaar: https://foreignpolicy.com/2017/05/15/the-united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/.
Stockholm International Peace Research Institute (2018). *SIPRI Military Expenditure Database*. Online beschikbaar: https://www.sipri.org/databases/milex.

Stockton, P. & M.Golabek-Goldman. Curbing the Market for Cyber Weapons. In: Yale Law and Policy Review 32(1), 239-266.

Stoner, K. & M. McFaul (2015). Who Lost Russia (This Time)? Vladimir Putin. In: *The Washington Quarterly* 38(2), 167-187.

De Telegraaf (2018). 'Defensie komt met toekomstplannen'. De Telegraaf 26 maart 2018. Online beschikbaar: https://www.telegraaf.nl/nieuws/1836707/defensie-komt-met-toekomstplannen.

Tisdell, C. (2009). Economic reform and openness in China: China's development policies in the last 30 years. University of Queensland working paper no. 55.

Trautman, L.J. (2016). Is Cyberattack the Next Pearl Harbor? In: *North Carolina Journal of Law and Technology* 18(2), 233-289.

Traynor, I., 'Russia accused of unleashing cyberwar to disable Estonia'. The Guardian 17 mei 2007. Online beschikbaar: https://www.theguardian.com/world/2007/may/17/topstories3.russia.

Tweed, D. & P. Martin (2018). ''Shocking' Huawei Arrest Threatens to Upend Trump-Xi Trade Truce'. Bloomberg 6 december 2018,. Online beschikbaar: https://www.bloomberg.com/news/articles/2018-12-06/-shocking-huawei-arrest-threatens-to-upend-trump-xi-trade-truce.

UAWIRE (2017). 'Russia proposes to place root Internet name servers in BRICS countries'. UAWIRE 28 november 2017. Online beschikbaar: https://uawire.org/russia-offers-to-deploy-root-name-servers-in-brics-countries.

United Kingdom Government (2016). *National Cyber Security Strategy 2016-2021*. Online beschikbaar: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

United Nations Economic and Social Council (2011). *Cybersecurity: A global issue demanding a global approach*. Online beschikbaar: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). A/70/174
.
United States Cybercommand (2018a). website: https://www.cybercom.mil/About/History/.

United States Cybercommand (2018b). *Achieve and Maintain Cyberspace Superiority*. Online beschikbaar: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

United States Cyber Emergency Response Team. *NCCIC Cyber Incident Scoring System*. Online beschikbaar: https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

United States Department of Defense (2018). *Cyber Strategy 2018*. Online beschikbaar: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

United States Department of Justice (2018), 'Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps'. U.S. Department of Justice 23 maart 2018. Online beschikbaar: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

United States Secretary of Defense (2018). *Nuclear Posture Review*. Online beschikbaar: https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

Valance, C. (2017). 'Russian Fancy Bear hackers UK link revealed'. BBC 23 november 2017. Online beschikbaar: https://www.bbc.co.uk/news/technology-42056555.

Varol, O., F. Emilio, C.A. Davis, F. Menczer & A.Flammini (2017). Online Human-Bot Interactions: Detection, Estimation, and Characterization. Conference paper, International AAAI Conference on Web and Social Media. Online beschikbaar: arxiv.org/abs/1703.03107.

Versteegh, K. (2017). 'De AIVD groeit als kool'. NRC 4 april 2017. Online beschikbaar: https://www.nrc.nl/nieuws/2017/04/04/de-aivd-groeit-als-kool-7916563-a1553167.

Volz, D. (2018). 'Trump signs bill renewing NSA's internet surveillance program'. Reuters 19 januari 2018. Online beschikbaar: https://www.reuters.com/article/us-usa-trump-cyber-surveillance/trump-signs-bill-renewing-nsas-internet-surveillance-program-idUSKBN1F82MK.

Wagstaff, J. (2015). 'Chinese hackers target Southeast Asia, India, researchers say'. Reuters 13 april 2015. Online beschikbaar: https://www.reuters.com/article/us-cybersecurity-fireeye-report-idUSKBN0N40AD20150413.

Ward, A. (2018). 'Read: Mueller indictment against 12 Russian spies for DNC hack'. Vox 13 juli 2018. Online beschikbaar: https://www.vox.com/2018/7/13/17568806/mueller-russia-intelligence-indictment-full-text.

Wardle, C. & H. Derakhshan (2017). *Information Disorder, Toward an Interdisciplinary framework for Research and Policy Making*. Council of Europe Report.

Westcott, B. (2018). 'International cyber crime ring smashed after more than $530 million stolen'. CNN 8 februari 2018. Online beschikbaar: https://edition.cnn.com/2018/02/08/world/us-cyber-crime-ring-arrests-intl/index.html.

The Washington Post (2013). 'Inside the 2013 U.S. Intelligence 'black budget'. The Washington Post 29 augustus 2013. Online beschikbaar: https://www.washingtonpost.com/gdpr-consent/?destination=%2fapps%2fg%2fpage%2fnational%2finside-the-2013-us-intelligence-black-budget%2f420%2f%3f&utm_term=.d22792fa0970.

The White House (2018). *National Cyber Strategy*. Online beschikbaar: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

World Bank (2018). website: https://www.worldbank.org/en/country/china/overview.

Wright, S. (1998). *An appraisal of the technology of political control*. STOA.

Yoo, C.S. (2015). Cyber espionage or cyberwar? International law, domestic law, and self-protective measures. In: J.D. Ohlin, K. Govern & C. Finkelstein (eds*.). Cyberwar: Law and Ethics for Virtual Conflicts*. Oxford University Press, 175-194.

Yu, J.M. (2018). 'Chinese cyber attacks on Taiwan government becoming harder to detect: source'. Reuters 15 juni 2018. Online beschikbaar: https://www.reuters.com/article/us-taiwan-china-cybersecurity/chinese-cyber-attacks-on-taiwan-government-becoming-harder-to-detect-source-idUSKBN1JB17L.

Zerodium (2018). Website: https://zerodium.com/

Zetter, K. (2011). 'How digital detectives deciphered stuxnet, the most menacing malware in history'. Wired 7 juli 2011. Online beschikbaar: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Zetter, K. (2013). 'Google's Real Secret Spy Program? Secure FTP'. Wired 6 november 2013. Online beschikbaar: https://www.wired.com/2013/06/google-uses-secure-ftp-to-feds/.

Zetter, K. (2014). ‘Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA’. Wired 15 april 2014. Online beschikbaar: https://www.wired.com/2014/04/obama-zero-day/#comments.

Zetter, K. (2015). ‘US and China Reach Historic Agreement on Economic Espionage’. Wired 24 september 2015. Online beschikbaar: https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/.

Zetter, K. (2016). ‘Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid’. Wired 3 maart 2016. Online beschikbaar: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Open Access
Het Rathenau Instituut heeft een Open Access beleid. Rapporten, achtergrondstudies, wetenschappelijke artikelen, software worden vrij beschikbaar gepubliceerd. Onderzoeksgegevens komen beschikbaar met inachtneming van wettelijke bepalingen en ethische normen voor onderzoek over rechten van derden, privacy, en auteursrecht.

Contactgegevens
Anna van Saksenlaan 51
Postbus 95366
2509 CJ Den Haag
070-342 15 42
info@rathenau.nl
www.rathenau.nl

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut