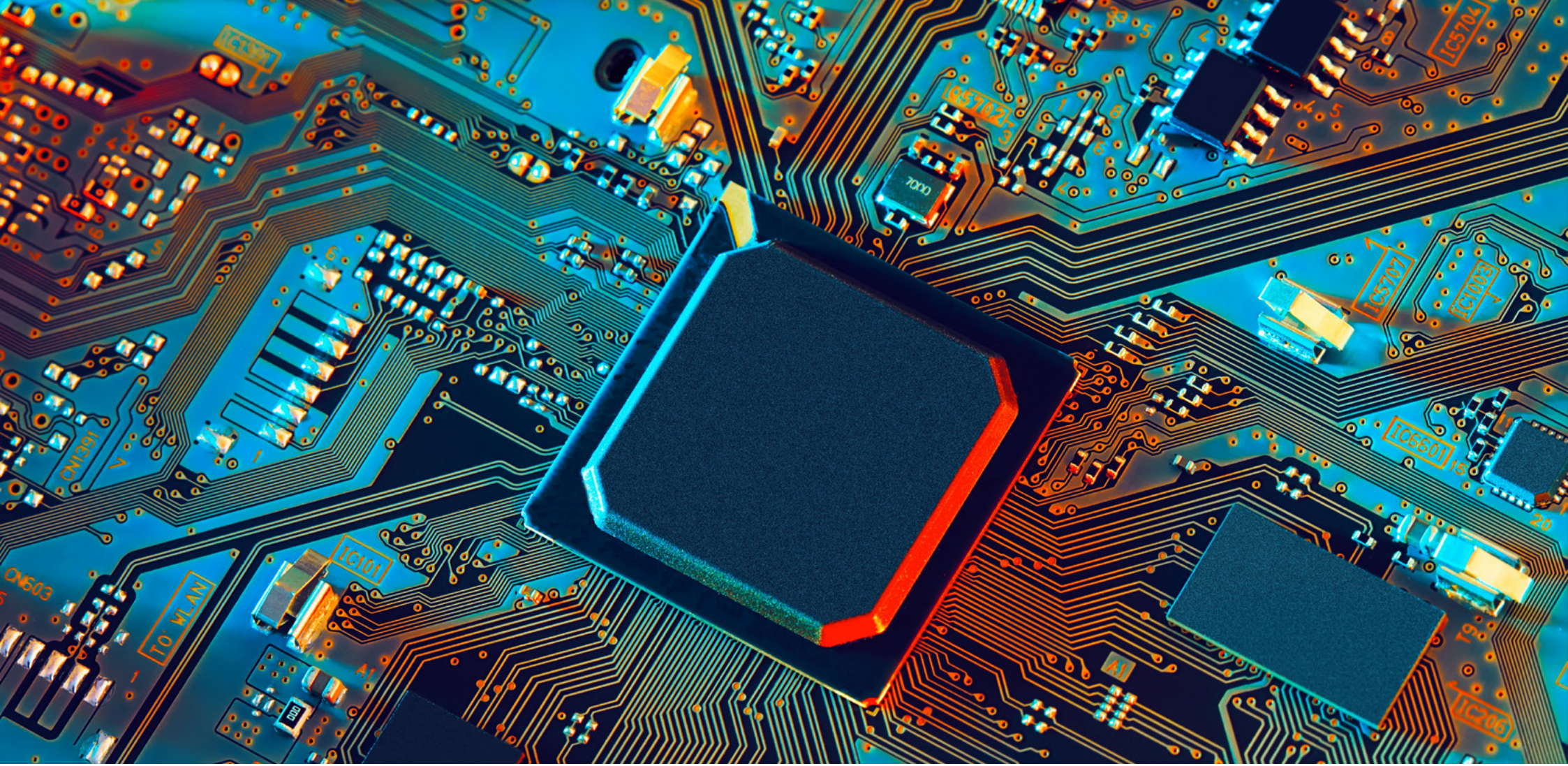

Verbeter de verbinding

Evaluatie internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken

Voorwoord

Cyberdreigingen en -incidenten nemen, versterkt door een veranderende geopolitieke situatie, wereldwijd toe. Ook Nederland moet rekening houden met dreigingen als het saboteren van kritieke infrastructuur, het verspreiden van desinformatie en (economische) spionage. Te midden van mondiale tegenstellingen, zet de Taskforce Cyber (TFC) van het ministerie van Buitenlandse Zaken (BZ) zich in om cyberdreigingen te mitigeren en mondiaal tot afspraken te komen over het gedrag van staten in cyberspace.

Het internationaal cybersecuritybeleid, waarbinnen de TFC sinds 2015 opereert, is als relatief jong beleidsterrein nog niet eerder geëvalueerd. Mede naar aanleiding van de urgentie van de uitdagingen in het cyberdomein heeft de directie Internationaal Onderzoek en Beleidsevaluatie (IOB) van het ministerie van Buitenlandse Zaken een evaluatie uitgevoerd van het internationaal cybersecuritybeleid van het ministerie in de periode 2015-2021.

De onderzoekers die namens IOB aan deze evaluatie hebben gewerkt zijn Gijs van Loon, Wendy van der Neut en Anouk Pietersen. Zij hebben hiervoor mede gebruik gemaakt van een speciaal voor dit onderzoek uitgevoerde literatuurstudie door Lianne Boer, Keri van Douwen en Nour Gjaltema van de Vrije Universiteit. IOB is de auteurs erkentelijk voor hun bijdrage.

Een externe referentiegroep heeft het onderzoek begeleid. Deze bestond behalve uit vertegenwoordigers van relevante beleidsdirecties van het ministerie van Buitenlandse Zaken uit drie experts op het gebied van internationaal cybersecuritybeleid: Prof. dr. Bibi van den Berg van de Universiteit Leiden, Prof. dr. Em. Terry Gill van de Universiteit van Amsterdam en Sico van der Meer van het Instituut Clingendael. De interne kwaliteitscontrole werd verzorgd door een klankbordgroep bestaande uit IOB-collega's Anne Bakker, Joep Schenk, Paul Westerhof en mijzelf (voorzitter). Namens IOB bedank ik alle leden van de externe referentiegroep en de klankbordgroep voor hun waardevolle adviezen en ondersteuning.

Een speciaal woord van dank gaat uit naar alle geïnterviewden en naar alle respondenten die de survey hebben ingevuld.

De eindverantwoordelijkheid voor het rapport berust bij IOB.

Arjan Schuthof
Waarnemend Directeur

Directie Internationaal Onderzoek en Beleidsevaluatie Ministerie van Buitenlandse Zaken

Inhoudsopgave

Afkortingen

ACEV	Ambtelijke Commissie Economische Veiligheid
AIV	Adviesraad Internationale Vraagstukken
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMAD	Ambassadeur in Algemene Dienst
AVVN	Algemene Vergadering van de Verenigde Naties
AZ	Ministerie van Algemene Zaken
BIS	Bureau Internationale Samenwerking (BZ)
BZ	Ministerie van Buitenlandse Zaken
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CLI	Cyber Law International
CSBN	Cybersecuritybeeld Nederland
CSIRT	Cyber Security Incident Response Team
DBV	Directie Bedrijfsvoering (BZ)
DGRR	Directoraat-Generaal Rechtspleging en Rechtshandhaving (JenV)
DIE	Directie Integratie Europa (BZ)
DIO	Directie Internationaal Ondernemen (BZ)
DJZ	Directie Juridische Zaken (BZ)
DMM	Directie Multilaterale Instellingen en Mensenrechten (BZ)
DSO	Directie Sociale Ontwikkeling (BZ)
DSR	Digital Silk Road van China
DVB	Directie Veiligheidsbeleid (BZ)
EU	Europese Unie
EZK	Ministerie van Economische Zaken en Klimaat
FIN	Ministerie van Financiën
FOC	Freedom Online Coalition
GBVS	Geïntegreerde Buitenland- en Veiligheidsstrategie
GCSC	Global Commission for the Stability of Cyberspace
GFCE	Global Forum on Cyber Expertise
GGE	United Nations Governmental Group of Experts (on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security)
GPD	Global Partners Digital
ICS	Internationale Cyberstrategie
ICT	Informatie- en Communicatie Technologie
IenW	Ministerie van Infrastructuur en Waterstaat
IMH	Directie Internationale Marktordening en Handelspolitiek (BZ)
IOB	Directie Internationaal Onderzoek en Beleidsevaluatie (BZ)
IOCS	Interdepartementaal Overleg Cyber Security
IOIC	Interdepartementaal Overleg Internationale Cybersecurity
ITU	International Telecommunications Union (VN)
JenV	Ministerie van Justitie en Veiligheid
MCEV	Ministeriële Commissie Economische Veiligheid
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NAM	Non-Aligned Movement
NAVO	Noord-Atlantische Verdragsorganisatie
NCSA	Nederlandse Cybersecurity Agenda
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap
OEWG	United Nations Open-Ended Working Group (on ICTs)
OM	Openbaar Ministerie
OPCW	Organisatie voor het Verbod op Chemische Wapens (Organisation for the Prohibition of Chemical Weapons)
OVSE	Organisatie voor Veiligheid en Samenwerking in Europa
PoA	Programme of Action (VN)
PV	Permanente Vertegenwoordiging
SZW	Ministerie van Sociale Zaken en Werkgelegenheid
TFC	Taskforce Cyber (BZ)
TFEV	Taskforce Economische Veiligheid
ToR	Terms of Reference
UVRM	Universele Verklaring van de Rechten van de Mens
VK	Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland
VN	Verenigde Naties
VNAC	Versterking van de Nationale Aanpak Cybersecurity
VS	Verenigde Staten van Amerika
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Termen

Deze lijst geeft weer wat er met een aantal vaker voorkomende termen in dit rapport wordt bedoeld. De meeste definities komen uit de als onderdeel van dit onderzoek uitgevoerde literatuurstudie van de Vrije Universiteit Amsterdam of uit het Cybersecurity Woordenboek (2019) van Cybersecurity Alliantie Nederland. Als er geen bronvermelding bij een term staat zijn de definities afkomstig van de auteurs van dit rapport.

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

Artificial Intelligence (kunstmatige intelligentie): 'Technologie waarbij digitale systemen reageren op data, bijvoorbeeld afkomstig uit sensoren, en op basis daarvan zelfstandig acties ondernemen.'[2] Toepassingen hiervan zijn veelledig, zoals bijvoorbeeld in gezichts- en spraakherkenning, zoekmachines, het genereren van content en aanbevelingen op (sociale) media, en cyberaanvallen.

Attributie: het aanwijzen van (een) dader(s) van een cyberaanval.

Capaciteitsopbouw: het helpen opbouwen en beveiligingen van digitale infrastructuur en cybersecuritybeleid in landen met ontwikkelende cybercapaciteiten. Dit kan gebeuren middels financiële, materiële en educatieve middelen, en institutionele hervormingen.[3]

Cyber Diplomacy Toolbox (EU): het beleidsraamwerk voor gezamenlijk EU-respons tegen kwaadaardige cyberactiviteiten, aangenomen in 2017. De toolbox biedt mogelijkheid tot het inzetten van vijf soorten maatregelen: preventieve maatregelen; samenwerkingsmaatregelen; stabiliteitsmaatregelen; restrictieve maatregelen (zoals sancties); en het ondersteunen van rechtmatige respons van individuele lidstaten.[4]

Cyberaanval: een gerichte aanval in of via het cyberdomein. Doelwitten kunnen zijn: personen, groepen, bedrijven, organisaties, overheden, en andere landen.[5]

Cybercriminaliteit: verwijst in brede zin naar activiteiten die gepleegd worden met ICT-middelen voor criminele doeleinden.[6]

Cyberdiplomatie: het inzetten van diplomatieke middelen om nationale belangen in het cyberdomein veilig te stellen.[7]

Cyberdomein: conglomeraat van ICT-middelen, -diensten en -entiteiten die digitaal verbonden (kunnen) zijn. Het domein omvat zowel permanente als tijdelijke verbindingen, evenals de gegevens (o.a. data, programmacode, informatie) die zich in dit domein bevinden.[8]

Cybernormen: internationaal of regionaal afgesproken normen die uiteenzetten hoe staten zich dienen te gedragen in het cyberdomein.[9]

Cyberproxy: een tussenpersoon die een offensieve cyberoperatie uitvoert, of er direct aan bijdraagt, die bewust mogelijk wordt gemaakt door een begunstigde.[10]

Cybersanctieregime (EU): het cybersanctieregime is een uitwerking van de *Cyber Diplomacy Toolbox* en is gericht op personen en niet-statelijke entiteiten. Het sanctieregime is in 2019 vastgesteld in Besluit 2019/797 en Verordening 2019/796. De eerste sancties zijn in juli 2020 vastgesteld.[11]

Cybersecurity: het beschermen van digitale netwerken, gegevens, systemen, infrastructuren, programma's, apparaten en andere hardware tegen aanvallen.

Defense Forward: aanpak waarbij mogelijke cyberoperaties proactief worden geobserveerd, gevolgd, en tegengegaan om kwaadwillende cyberoperaties te verstoren en te verslaan, waarbij alle daarvoor opportuun geachte instrumenten worden ingezet. Het doel is de kosten van cyberoperaties te verhogen en een normerend effect te bewerkstelligen.[12]

Desinformatie (ook wel nepnieuws): het doelbewust, veelal heimelijk, verspreiden van misleidende informatie, met het doel om schade toe te brengen aan het publieke debat, democratische processen, de open economie of nationale veiligheid.[13]

Digitalisering: het omzetten van informatie van analoog naar digitaal; maar ook de maatschappelijke en economische verandering als gevolg van de toenemende invloed van informatie- en communicatietechnologie.[14]

Diplomatieke respons: een diplomatieke reactie op een cyberaanval door of onder verantwoordelijkheid van een staat, zoals het – al dan niet publiekelijk en gezamenlijk met andere landen – aanwijzen van een dader (attributie), en het opleggen van sancties tegen de veronderstelde dader.

Dual-use: 'Het feit dat dezelfde digitale (genetwerkte) technologie gebruikt kan worden voor zowel militaire doelen als civiele doelen.'[15]

Economische spionage: cyberoperaties gericht op het stelen van bedrijfsstrategieën en -plannen, intellectueel eigendom en kostbare onderzoeks- en ontwikkelingsprojecten.[16]

Encryptie: de versleuteling van (gevoelige) informatie door middel van cryptografie: informatie omzetten in een code zodat een ander het niet kan lezen.[17]

Internationaal cybersecuritybeleid: beleid gericht op het voorkomen en mitigeren van cyberdreigingen en -aanvallen door staten en aan staten gelieerde actoren, die zijn gericht tegen (doelwitten in) andere staten.

Internationale rechtsorde: orde die gebaseerd is op het internationaal recht, het recht dat gaat over de relaties tussen staten onderling. In artikel 90 van de Nederlandse Grondwet staat dat de regering de ontwikkeling van de internationale rechtsorde bevordert.[18]

Internetsoevereiniteit: het recht van een staat op volledige controle over het cyberdomein binnen de eigen staatsgrenzen.[19]

Kwantumcomputer: 'Computer die informatie opslaat en bewerkt door de eigenschappen te gebruiken van deeltjes die nog kleiner zijn dan een atoom. De kwantumcomputer kan veel sneller rekenen dan gewone computers. Hierdoor kan een kwantumcomputer bijvoorbeeld gemakkelijk beveiligingscodes kraken en zijn er in de toekomst daardoor nieuwe manieren van beveiliging nodig.'[20]

Malware (malicious software): 'Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te stelen.'[21]

Nieuwe technologieën: clusternaam voor aan het cyberdomein gerelateerde technologische uitvindingen en ontwikkelingen die impact hebben of kunnen hebben op de maatschappij, zoals, maar niet uitsluitend, artificial intelligence, kwantumcomputers en het 5G-netwerk.

Online mensenrechten: reeds bestaande mensenrechten zoals de vrijheid van meningsuiting en de vrijheid van vergadering die worden toegepast in het cyberdomein.[22]

Publieke kern van het internet (WRR): de gedachte dat 'de centrale protocollen en infrastructuren van het internet als een mondiaal publiek goed beschouwd moeten worden' en dat deze publieke goederen 'gevrijwaard [moeten] blijven van oneigenlijke interventies van staten en andere partijen die schade toebrengen en het vertrouwen in het internet eroderen.'[23]

Ransomware (ransom software): kwaadaardige software waarbij slachtoffers afgeperst worden nadat hun digitale systemen of de bestanden erop met een code op slot zijn gezet.[24]

Sabotage: het opzettelijk, langdurig aantasten van de beschikbaarheid van informatie, informatiesystemen of –diensten, mogelijk leidend tot vernietiging.[25]

Spionage: het kopiëren of wegnemen van informatie door statelijke of daaraan gelieerde actoren.[26]

Swing states: aanduiding voor landen met wisselende of nog ontwikkelende politieke standpunten binnen het internationale cyberdomein, wiens keuzes of stemgedrag binnen internationale fora en politiek van doorslaggevende invloed kunnen zijn.[27]

1 Inleiding en dreigingen

Dit rapport presenteert de hoofdbevindingen van de IOB-evaluatie van het internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken (BZ).

Met 'cybersecurity' wordt hier bedoeld het beschermen van digitale netwerken, gegevens, systemen, infrastructuren, programma's, apparaten en andere hardware tegen aanvallen. Het 'internationaal cybersecuritybeleid' is het beleid gericht op het voorkomen en mitigeren van cyberdreigingen en -aanvallen door staten en aan staten gelieerde actoren, gericht tegen (doelwitten in) andere staten.

Dit is een relatief nieuw beleidsterrein binnen het ministerie van Buitenlandse Zaken (BZ), waarvoor in 2015 de Taskforce Cyber (TFC) is opgericht. Sindsdien is het onderwerp steeds belangrijker geworden, onder andere omdat er een toename heeft plaatsgevonden in cyberdreigingen vanuit staten en aan staten gelieerde actoren. Sinds 2015 is cybersecurity voor het Nederlandse kabinet dan ook uitgegroeid tot prioriteit,[28] en is de aandacht binnen BZ voor internationaal cybersecuritybeleid toegenomen. Het internationaal cybersecuritybeleid is nog niet eerder geëvalueerd. Gezien de verwachting dat cyberdreigingen en –incidenten in hoeveelheid en ernst verder zullen toenemen (zie hieronder), waardoor er verschillende beleidsuitdagingen en strategische vraagstukken voorliggen, is dit een opportuun moment voor deze evaluatie.[a]

Doel en methoden van het onderzoek

Doel en afbakening

Het doel van deze evaluatie is te leren wat goed en minder goed gaat bij het ontwerp en de implementatie van het internationaal cybersecuritybeleid van BZ over de periode 2015-2021,[b] en om aanbevelingen te doen over hoe dit beleid in de toekomst het beste kan worden vormgegeven.

Hierbij moet worden aangetekend dat dit geen impactevaluatie is: vanwege methodologische beperkingen[c] wordt niet geprobeerd vast te stellen in hoeverre verschillende onderdelen van het beleid precies bijgedragen hebben aan de beoogde doelen.

Hoewel de evaluatie met name gericht is op het internationaal cybersecuritybeleid van BZ, bleek gedurende het onderzoek dat een aantal van de belangrijkste uitdagingen en oplossingen breder zijn. Het internationaal cybersecuritybeleid is namelijk verweven met aspecten van het cybersecuritybeleid die bij andere ministeries liggen. Een aantal van de bevindingen en aanbevelingen van deze evaluatie zijn dan ook overheidsbreed.

Meer informatie over de precieze onderzoeksvragen en afbakening is te vinden in de Terms of Reference (ToR) van het onderzoek, die is gepubliceerd op de website van IOB.[d]

[a] Dit evaluatierapport werd eind juni 2021 vastgesteld door de waarnemend directeur van IOB. Ontwikkelingen in het cyberdomein die sindsdien hebben plaatsgevonden, zijn niet meer meegenomen in de evaluatie.

[b] Hierbij is de nadruk komen te liggen op de meest recente jaren, aangezien er in de loop van de jaren veel veranderd is in het beleid, en de evaluatie erop gericht is bruikbare aanbevelingen te doen.

[c] Onder andere omdat andere actoren en ontwikkelingen ook een rol spelen in het al dan niet verwezenlijken van de doelen van het beleid; het feit dat een aantal van de doelen moeilijk te meten is; en er een gebrek is aan betrouwbare, verifieerbare datasets en andere gegevens. Bovendien is het internationaal cybersecuritybeleid een relatief nieuw beleidsterrein, waardoor er weinig tot geen bewijs bestaat over welke benaderingen al dan niet werken voor het behalen van de doelen op langere termijn. Zie ook de Terms of Reference van het onderzoek, gepubliceerd op https://www.iob-evaluatie.nl/in-uitvoering/publicaties/terms-of-reference/2020/05/14/evaluatie-internationaal-cybersecuritybeleid.

[d] Zie voor onder meer de onderzoeksvragen en afbakening de IOB Terms of Reference: https://www.iob-evaluatie.nl/in-uitvoering/publicaties/terms-of-reference/2020/05/14/evaluatie-internationaal-cybersecuritybeleid.

Onderzoeksmethoden

Het onderzoek bestaat uit vier onderdelen:

- interviews met 95 betrokken beleidsmedewerkers, internationale partners en experts;
- analyse van interne documenten en correspondentie van BZ;
- een survey onder betrokkenen en experts;
- een literatuurstudie door de Vrije Universiteit Amsterdam (gepubliceerd op de IOB website: *www.iob-evaluatie.nl/resultaten/internationaal-cybersecuritybeleid*).

Een gedetailleerde beschrijving van de gebruikte onderzoeksmethoden en methodologische beperkingen is als bijlage gepubliceerd op de IOB website: *www.iob-evaluatie.nl/resultaten/internationaal-cybersecuritybeleid*.

Veel van de gebruikte bronnen voor dit onderzoek zijn niet openbaar beschikbaar. Daarom wordt in voetnoten ter illustratie of als verwijzing naar verdere informatie soms ook verwezen naar publiek beschikbare bronnen, zoals (kranten)artikelen of podcasts.

Opzet rapport

De rest van dit inleidende hoofdstuk beschrijft de cyberdreigingen van andere staten waar Nederland mee te maken heeft. In de volgende hoofdstukken worden de bevindingen en aanbevelingen uiteengezet op basis van vier thema's: interdepartementale samenwerking (hoofdstuk 2), strategie en doelstellingen van BZ (hoofdstuk 3), inzet en activiteiten (hoofdstuk 4) en organisatorische opzet (hoofdstuk 5).

Cyberdreigingen richting Nederland

Nationale veiligheid onder druk

Niet iedereen is zich bewust van de hoeveelheid en ernst van cyberdreigingen[e] en –aanvallen die op Nederland afkomen.[f] Zowel in binnen- als buitenland worden dagelijks cyberaanvallen waargenomen, die niet altijd de publiciteit halen.[29] Verscheidene bronnen verschaffen dan ook een verontrustend beeld van de hedendaagse cyberdreigingen, waarvan de reële en potentiële impact op de nationale veiligheid groot is en de schade – zowel fysiek als economisch – hoog op kan lopen.[g] In 2020 schreef de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) dat de toenemende cyberdreiging, met name afkomstig vanuit statelijke en aan staten gelieerde actoren, een probleem voor de nationale veiligheid is. Als reactie daarop bevestigde demissionair minister van Justitie en Veiligheid Grapperhaus dat een geslaagde cyberaanval een enorm ontwrichtend effect op de maatschappij kan hebben, en dat een scenario waarin dergelijke ontwrichting in Nederland plaatsvindt niet langer kan worden uitgesloten.[h] [30]

[e] Zie voor meer achtergronden over de manieren waarop cyberdreigingen tot uiting komen ook de Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB.

[f] Het Nationaal Cyber Security Centrum (NCSC) houdt een overzicht bij van ontwikkelingen, nieuwsfeiten en incidenten op het gebied van digitale veiligheid. Het overzicht bestaat uit openbaar beschikbare informatie en is dus geenszins uitputtend: *https://www.ncsc.nl/actueel/ontwikkelingen-cybersecurity.*

[g] Zie voor een publieke bron bijvoorbeeld De Strateeg podcastaflevering, 'hoe cyberdreiging ons leven kan ontwrichten' (2020), van BNR-Nieuwsradio: *https://www.bnr.nl/podcast/de-strateeg/10415198/hoe-cyberdreiging-ons-leven-kan-ontwrichten.*

[h] Het Cybersecuritybeeld Nederland (CSBN) van juni 2020 is te downloaden via de website van het NCSC: *https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020*; De reactie daarop van demissionair minister Grapperhaus is hier te lezen: *https://www.rijksoverheid.nl/actueel/nieuws/2020/06/29/grapperhaus-ontwikkeling-digitale-dreiging-nederland-is-zorgwekkend.*

Tekstbox 1.1: Voorbeelden publiek bekende cyberaanvallen

In de afgelopen decennia hebben verschillende cyberaanvallen plaatsgevonden die volgens openbare berichtgeving door staten of daaraan gelieerde actoren werden uitgevoerd.[i] Een bekende langlopende cyberaanval werd volgens openbare bronnen tussen omstreeks 2005 en 2010 uitgevoerd door de Verenigde Staten (VS) en Israël, die middels de computerworm Stuxnet het Iraanse nucleaire programma binnendrongen en saboteerden.[j] In 2017 legde de Russische NotPetya malware-aanval op een Oekraïens boekhoudprogramma onder andere gedeeltes van de Rotterdamse haven voor meerdere dagen plat. De aanval raakte ook andere organisaties en bedrijven in Europa, met een financiële schade van honderden miljoenen euro's tot gevolg.[k] Daarnaast gijzelde de Noord-Koreaanse WannaCry *ransomware*-aanval in datzelfde jaar wereldwijd honderd-duizenden Microsoft-computers. *Ransomware* wordt ook door internetcriminelen ingezet voor het gijzelen van targets en het vragen van hoge sommen losgeld.[l] Meer recentelijk werden gegevens van verscheidene overheidsinstanties en bedrijven buitgemaakt door een gecoördineerde hack op het Amerikaanse bedrijf SolarWinds – dat IT-software aanbiedt en onder meer Amerikaanse ministeries, overheidsinstanties en Microsoft als klant heeft – waarvan de precieze omvang op moment van schrijven nog onbekend is.[m]

Economische veiligheid

Niet alleen de nationale veiligheid, maar ook de economische veiligheid[n] en het Nederlands verdienvermogen lijden momenteel onder de toegenomen cyberdreiging. Het stabiel functioneren van het internet is voor Nederland essentieel voor het benutten van maatschappelijke en economische kansen.[31] Met name de hoeveelheid digitale spionage met economisch-technologische motieven[o] maakt het echter moeilijk om belangen van bedrijven en kennisinstellingen te beschermen, wat negatief doorwerkt op de Nederlandse economische veiligheid.[32] Volgens de Algemene Inlichtingen- en Veiligheidsdienst (AIVD)[p] neemt de activiteit op dit gebied alleen maar toe, en kan digitale spionage bovendien een opmaat zijn voor sabotage of beïnvloeding.[33] De ernst van het probleem leidde recentelijk tot een publieke oproep[q] van Nederlandse veiligheidsdiensten tot meer middelen en betere samenwerking om deze economisch-technologische spionage te bestrijden.

Digitale afhankelijkheden en kwetsbaarheden

De bestrijding van cyberaanvallen, zoals spionage, blijkt moeilijk en de activiteit neemt toe. Nederland is op digitaal vlak zeer kwetsbaar doordat zij afhankelijk is van buitenlandse bedrijven en technologieën.[34] De gevolgen van dergelijke afhankelijkheden

[i] De informatie in deze tekstbox over cyberaanvallen en (mogelijke) daders komt uit openbare bronnen en reflecteert niet de zienswijze van het Nederlandse kabinet.

[j] Meer openbare achtergrondinformatie over Stuxnet is onder andere te lezen in dit artikel van de Washington Post uit 2012: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[k] Zie voor meer openbaar beschikbare informatie over de NotPetya-aanval het AD-artikel (2018): https://www.ad.nl/rotterdam/londen-rusland-zat-achter-platleggen-rotterdamse-haven~a32e8bfa/.

[l] Onder andere NRC heeft een omvangrijk online dossier met aanvullende informatie over de Wannacry-aanval en de effecten van ransomware op de samenleving, te raadplegen via: https://www.nrc.nl/dossier/wannacry-virus/

[m] Meer openbaar beschikbare achtergrondinformatie over de SolarWinds-hack is te vinden in het in april 2021 verschenen NPR-artikel (EN): https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack?t=1618831523302.

[n] Economische veiligheid wordt door de NTCV gedefinieerd als 'het ongestoord kunnen functioneren van Nederland als efficiënte en effectieve economie' (Nationale Veiligheid Strategie 2019). Een andere definitie van economische veiligheid die binnen de overheid gebruikt wordt, is het 'vrijhouden van handelsroutes, het tegengaan van cyberspionage en cyberdreigingen, het veiligstellen van de voorzieningszekerheid en het waarborgen van de nationale veiligheid in het kader van buitenlandse investeringen' ('Wereldwijd voor een veilig Nederland' – Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022 (GBVS), 27 maart 2018. Kamerstukken II 2017-2018, 33 694, nr. 12, bijlage 836794, p. 35).

[o] Dergelijke cyberoperaties zijn gericht op het stelen van bedrijfsstrategieën en -plannen, intellectueel eigendom en kostbare onderzoeks- en ontwikkelingsprojecten (zie literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 20).

[p] Het AIVD-jaarverslag van 2020 bevat meer informatie over onder andere spionageactiviteiten van staten richting Nederland en kan worden gelezen via deze website: https://www.aivd.nl/documenten/jaarverslagen/2021/04/29/aivd-jaarverslag-2020.

[q] De oproep werd op 11 februari 2021 gedaan in het Financieel Dagblad: https://fd.nl/economie-politiek/1373125/veiligheidsdiensten-slaan-samen-alarm-om-chinese-cyberdreiging-in-nederland

werden in april 2021 geïllustreerd in een Volkskrant-artikel,[r] waarin het Chinese telecombedrijf Huawei[s] ervan werd beschuldigd jarenlang ongecontroleerde en ongeautoriseerde toegang te hebben gehad tot de gegevens van 6,5 miljoen Nederlandse KPN-klanten. Hierdoor had – en mogelijk heeft[t] – de Chinese staat volgens de krant vermoedelijk toegang tot kritieke bedrijfsinformatie en informatie binnen hogere politieke niveaus. Op moment van schrijven doet het Agentschap Telecom onderzoek bij KPN naar de toedracht en omvang van het incident.[u] Aangezien dit soort gebeurtenissen de kern raken van economische veiligheidsvraagstukken, is de mondiale discussie rondom de toelating van de 5G-netwerken die zijn ontwikkeld door Huawei sterk gepolitiseerd. Verschillende regeringsleiders en experts wijzen erop dat de uitrol van Huawei's 5G-netwerken de Chinese toegang tot de digitale infrastructuur en mogelijkheden voor spionage vergroot.[v]

De Nederlandse maatschappij is daarnaast kwetsbaar voor digitale aanvallen. Processen die voor Nederland vitaal zijn, zoals het betaalverkeer, de waterkeringen en het functioneren van ziekenhuizen, zijn grotendeels afhankelijk van de continuïteit van de digitale infrastructuur en in veel gevallen ontbreekt er een snel inzetbaar analoog alternatief (back-up). Het jaar 2020 kenmerkte zich bovendien door een versnelde – door de COVID-19 pandemie gedwongen – digitalisering, die voor digitaal opererende internationale organisaties, nationale overheden, (vitale) bedrijven, zorginstanties en particulieren veiligheidsrisico's[w] met zich meebracht.[35] Onder meer de plotselinge toename van informatiedeling via onbeveiligde en/of voor kwaadwillende actoren toegankelijke digitale kanalen is een risico gebleken.

Desinformatie

Een andere dreiging die het afgelopen jaar door COVID-19 qua impact en aandacht een vlucht heeft genomen, is de maatschappij-ontwrichtende werking die uitgaat van desinformatie en complottheorieën.[x] Regelmatig wordt dergelijk nepnieuws verspreid door een statelijke of daaraan gelieerde actor, waaronder de Russische 'trollenfabriek'[y] die zich middels het versturen van duizenden tweets mengt in het MH17-proces, het racisme-discriminatiedebat in Nederland en meer recentelijk in de werkbaarheid van COVID-19 vaccins. De verspreiding van desinformatie is geen nieuw fenomeen, maar mede door de gemakkelijke verspreiding ervan dankzij digitale middelen en het grote bereik dat digitale middelen kunnen hebben, wordt de impact vergroot en de ernst van het probleem meer ingezien.[36]

Kwaadwillende actoren en hun motieven

De NCTV wijst statelijke en daaraan gelieerde actoren uit China, Rusland, Iran en Noord-Korea aan als belangrijkste dreigingsactoren voor Nederland. Van deze vier landen zijn volgens geïnterviewden en interne documenten de capaciteiten en activiteiten van China en Rusland het meest bedreigend richting Nederland. China richt zich

[r] Zie voor het bewuste Volkskrant-artikel: https://www.volkskrant.nl/nieuws-achtergrond/huawei-kon-alle-gesprekken-van-mobiele-kpn-klanten-afluisteren-inclusief-die-van-de-premier~bd1aece1/ of voor de reactie van experts het NOS-artikel: https://nos.nl/artikel/2377101-rapport-over-kpn-bevestigt-jarenlange-geruchten-over-spionage-china.html.

[s] Huawei is een Chinees telecombedrijf dat voor een deel in handen is van de Chinese staat.

[t] Verschillende bronnen die door de Volkskrant worden aangehaald, beweren dat de kritieke kern van het KPN 4G-netwerk in 2021 nog wordt beheerd door Huawei: https://www.volkskrant.nl/nieuws-achtergrond/huawei-beheert-nog-steeds-de-kern-van-het-mobiele-netwerk-van-kpn~bbe353c2/.

[u] Een laatste update over het onderzoek werd eind mei 2021 gegeven op de website van het Agentschap Telecom, te raadplegen via: https://www.agentschaptelecom.nl/actueel/nieuws/2021/05/31/update-onderzoek-kpn.

[v] Zie voor een openbare bron over deze kwestie het artikel van Jansen Tham in The Diplomat uit 2018 (EN): https://thediplomat.com/2018/12/why-5g-is-the-next-front-of-us-china-competition/.

[w] In openbare berichtgeving wordt onder meer aandacht besteed aan digitale spionage naar informatie over COVID-vaccins, zie bijvoorbeeld dit artikel uit 2020 van de NOS: https://nos.nl/artikel/2361735-buitenlandse-inlichtingendienst-zat-waarschijnlijk-achter-ema-hack.html.

[x] Zie voor de link tussen COVID-19 en de toename van desinformatie dit essay van de Universiteit Leiden (2020): https://www.universiteitleiden.nl/en/research/research-output/governance-and-global-affairs/tackling-covid-19-disinformation-internal-and-external-challenges-for-the-european-union.

[y] Trollen zijn Twitter-accounts die erop uit zijn om onwaarheden te verspreiden, zie voor openbare berichtgeving hierover het artikel uit 2018 in de Groene Amsterdammer: https://www.groene.nl/artikel/hoe-russische-trollen-inspelen-op-westerse-angsten.

voornamelijk op (economische) spionage, terwijl de Russische tactieken zijn gericht op het ontregelen van westerse samenlevingen, onder andere middels de verspreiding van desinformatie.[37] Ook de VS dragen volgens sommigen bij aan de toegenomen onveiligheid in het cyberdomein.[38] Zij dringen middels de *Defense Forward*-agenda[z] preventief digitale systemen van mogelijke aanvallers binnen die ze vervolgens kunnen saboteren. Hoewel hiermee activiteiten van kwaadwillende actoren richting de VS kunnen worden voorkomen, kan de agenda een reactie uitlokken van tegenstanders waardoor deze bij kan dragen aan escalatie in het cyberdomein.[39] Daarnaast is het aantal landen dat beschikt over offensieve cybercapaciteiten de afgelopen jaren toegenomen en wordt verwacht dat deze ontwikkeling de komende jaren verder zal doorzetten.[40] Dit zal de komende jaren leiden tot een breder speelveld van actoren waar dreiging vanuit gaat – ook richting Nederland.

Staten opteren in veel gevallen voor een cyberoperatie omdat cyberhandelingen relatief onzichtbaar zijn.[41] Zo kunnen staten hun capaciteiten en handelingen beter verborgen houden dan het geval is bij de ontwikkeling en inzet van conventioneel militair materieel, wat bijvoorbeeld dankzij de inzet van satellieten wel zichtbaar is. Mede door deze onzichtbaarheid blijkt het voor slachtoffers vaak een uitdaging tijdig te ontdekken door wie zij werden aangevallen, of op te merken dat er überhaupt een cyberaanval aan de gang is. Bovendien maken staten vaak gebruik van aan hen gelieerde actoren, zogeheten cyberproxies,[aa] waardoor het in veel gevallen moeilijk is voldoende juridisch bewijs te vergaren om een statelijke actor aan te wijzen als dader of medeplichtige.[ab][42]

Om deze redenen kunnen staten hun verantwoordelijkheid voor cyberaanvallen afschuiven of blijvend ontkennen. Daarnaast zijn cyberoperaties, in tegenstelling tot traditionele manieren van sabotage, spionage of verspreiden van desinformatie, relatief laag in kosten en hoog in effectiviteit.[43]

Vrijheden en mensenrechten online

Het Nederlandse kabinet is van mening dat mensenrechten ook online van toepassing zijn, wat onder meer zou moeten waarborgen dat burgers online vrij hun mening kunnen uiten, online vrij kunnen vergaderen en erop kunnen vertrouwen dat hun online privacy wordt gerespecteerd. Hoewel 180 staten in 2003 bevestigden dat de Universele Verklaring van de Rechten van de Mens (UVRM) volledig toepasbaar is online, is er nog geen consensus over de manier waarop en staan deze mensenrechten wereldwijd door toedoen van zowel nationale overheden als private actoren onder druk.[44] Technologische ontwikkelingen maken het bovendien gemakkelijker voor overheden om inbreuk te maken op de mensenrechten van burgers.[45] Zo verzamelt de Chinese staat via een mobiele app op grote schaal gegevens die het gebruikt ter onderdrukking van de Oeigoerse moslimminderheid in de provincie Xinjiang.[ac] En ook in niet-autoritaire regimes bestaat een spanningsveld tussen de privacy van burgers en de inzet van technologie voor nationale veiligheidsdoeleinden. De Amerikaanse overheid houdt bijvoorbeeld door middel van *algorithmic surveillance* online communicatie van Amerikaanse burgers op grote schaal in de gaten.[ad]

[z] De tactiek van *Defend Forward* houdt in dat mogelijke cyberoperaties proactief worden geobserveerd, gevolgd, en tegengegaan om kwaadwillende cyberoperaties te verstoren en te verslaan, waarbij alle daarvoor nodig geachte instrumenten worden ingezet. Het doel ervan is om de kosten van cyberoperaties te verhogen en een versterkend normerend effect te bewerkstelligen. Informatie afkomstig van Lawfare (EN): https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior.

[aa] Een cyberproxy is een tussenpersoon die een offensieve cyberoperatie uitvoert, of er direct aan bijdraagt, die bewust mogelijk wordt gemaakt door een begunstigde (literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8). Zo schrijft de VS de eerder genoemde SolarWinds-hack toe aan het Russische hackerscollectief APT29, ook bekend als Cozy Bear, dat volgens de Amerikaanse lezing direct verbonden is aan de Russische buitenlandse inlichtingendienst (SVR), zie (EN): https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[ab] Het aanwijzen van een of meerdere daders van een cyberaanval, wordt ook wel attributie genoemd.

[ac] Lees voor openbare berichtgeving hierover bijvoorbeeld het BBC-artikel '*China's Xinjiang citizens monitored with police app, says rights group*' uit 2019 (EN): https://www.bbc.com/news/world-asia-china-48130048.

[ad] Zie voor openbaar beschikbare informatie over mogelijke doorwerkingen van de toepassing van nieuwe technologieën op mensenrechten de rapporten van Amnesty International (EN): https://www.amnesty.nl/actueel/new-technologies-and-their-impact-on-the-promotion-and-protection-of-human-rights-in-the-context-of-assemblies-submission-to-the-un-high-commissioner-for-human-rights en Human Rights Watch (EN): https://www.hrw.org/topic/technology-and-rights.

Overheden en private actoren staan bovendien voor lastige dilemma's: enerzijds is de vrijheid van meningsuiting online een groot goed in veel democratische landen, anderzijds gaan er stemmen op om gevaarlijke uitingen zoals de verspreiding van complottheorieën en desinformatie actiever tegen te spreken of offline[ae] te halen.[af][46] Regeringen van landen met een meer controlerende overheid streven er al enkele jaren naar om hun nationale soevereiniteit online te versterken, en derhalve het internet(verkeer) en online communicatie te controleren, reguleren en soms (deels) te beknotten.[ag] Het mondiale internet raakt door dergelijke tendensen in toenemende mate gefragmenteerd[ah] of versplinterd.[47]

De combinatie van de nationale en economische veiligheid die in het geding zijn, de activiteiten in het cyberdomein van grootmachten als China, Rusland en de Verenigde Staten, de toenemende offensieve cybercapaciteiten van meerdere landen en de mensenrechten die online worden beknot, maakt het werk van BZ, en andere onderdelen van de Nederlandse overheid, divers en urgent. Verschillende Nederlandse vakdepartementen en overheidsinstanties zetten zich in ter versterking van de Nederlandse en mondiale cyberveiligheid. Welke ministeries dat zijn, wat ze doen en hoe dat gaat, wordt in het volgende hoofdstuk besproken.

[ae] Zo haalde Twitter begin 2021 het account van voormalig Amerikaans president Donald Trump offline, nadat hij herhaaldelijk ongefundeerde uitspraken deed over de verloren verkiezingen. Het sociale mediabedrijf publiceerde daarover het volgende statement (EN): *https://blog.twitter.com/en_us/topics/company/2020/suspension.html.*

[af] Zoals in het advies van de AIV over de regulering van online content (2020): *https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2020/06/24/regulering-van-online-content.*

[ag] Van staten als China en Rusland is bekend dat zij bijvoorbeeld het zoekgedrag van hun inwoners controleren, censuur toepassen en bepaalde gedeeltes van het internet afsluiten. Ook een dreigement van voormalig Amerikaans president Trump om de mobiele app TikTok te verbieden in de VS wanneer deze niet van eigenaar zou veranderen, kan worden gezien als een actie die leidt tot inperking van (delen van) het vrije internet.

[ah] Fragmentatie of versplintering van het internet (het 'splinternet') behelst het geleidelijke proces waarin staten het internet op basis van nationale belangen inrichten en waarbij sommige staten ervoor kiezen (de toegang tot) het internet voor hun burgers in te perken of te beknotten.

2 Interdepartementale samenwerking

Het internationaal cybersecuritybeleid is het beleid gericht op het voorkomen en mitigeren van cyberdreigingen en -aanvallen door staten en aan staten gelieerde actoren, zoals beschreven in het vorige hoofdstuk. Hoewel deze evaluatie gaat over het internationaal cybersecuritybeleid zoals belegd bij het ministerie van Buitenlandse Zaken (BZ), spelen andere ministeries en overheidsorganisaties ook een belangrijke rol bij onderdelen van dit beleid.

Het ministerie van Defensie is bijvoorbeeld verantwoordelijk voor taken van de krijgsmacht in het digitale domein en daarmee voor de Nederlandse offensieve en defensieve cybercapaciteiten. Daarnaast is dit ministerie – samen met BZ – verantwoordelijk voor samenwerking binnen de Noord-Atlantische Verdragsorganisatie (NAVO). Het ministerie van Justitie en Veiligheid (JenV) is onder andere verantwoordelijk voor internationale samenwerking tegen cybercriminaliteit; de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) onder meer voor inlichtingen op het gebied van digitale spionage en sabotage; het ministerie van Economische Zaken en Klimaat (EZK) met name voor digitalisering en het promoten van Nederlandse cybersecurity bedrijven in het buitenland en het Nationaal Cyber Security Centrum (NCSC) voor onder andere internationale samenwerkingsverbanden met andere Cyber Security Incident Response Teams (CSIRTs). En hoewel BZ een coördinerende rol heeft voor internationale vrede en veiligheid in het cyberdomein,[48] heeft de NCTV een coördinerende rol voor nationale cybersecurity; en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) voor het thema desinformatie, dat een sterk internationaal karakter heeft.[49]

Interdepartementaal zijn er verschillende beleidsstukken van kracht die het internationaal cybersecuritybeleid uiteenzetten. In 2018 is de overheidsbrede 'Nederlandse Cybersecurity Agenda: Nederland digitaal veilig' (NCSA) opgesteld. Hierin zijn zeven ambities voor de gehele overheid opgesteld over verschillende aspecten van cybersecurity, waarbij de tweede ambitie[ai] gaat over het internationaal cybersecuritybeleid. Andere interdepartementale beleidsdocumenten als de 'Internationale Cyberstrategie: Digitaal bruggen slaan' (ICS) uit 2017 en de 'Geïntegreerde Buitenland- en Veiligheidsstrategie: Wereldwijd voor een veilig Nederland' (GBVS) uit 2018 gaan deels ook over het internationaal cybersecuritybeleid.[aj]

Medewerkers van de verschillende ministeries werken regelmatig op ad-hoc basis of op informele manieren samen op het gebied van internationaal cybersecuritybeleid. Er zijn ook een aantal geïnstitutionaliseerde interdepartementale overlegorganen, zoals het Interdepartementaal Overleg Cybersecurity (IOCS)[ak] en het Interdepartementaal Overleg Internationale Cybersecurity (IOIC).[al] Ook wordt er samengewerkt in inter-

[ai] De tweede ambitie luidt: "Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein." Nederlandse Cybersecurity Agenda (NCSA), 20 april 2018. Kamerstukken II 2017-2018, 26 643, nr. 536, bijlage 839986, p. 7.

[aj] De Internationale Cyberstrategie gaat naast cybersecurity bijvoorbeeld ook over economische kansen in het digitale domein en digitalisering als ontwikkelingssamenwerkingsonderwerp. De Geïntegreerde Buitenland- en Veiligheidsstrategie stipt (internationaal) cybersecuritybeleid aan als een van meerdere veiligheidsbeleidsonderwerpen.

[ak] De NCTV zit het IOCS voor, andere deelnemende ministeries zijn BZ, Defensie, EZK, JenV, de NCTV, het NCSC, BZK, de AIVD en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), het ministerie van Infrastructuur en Waterstaat (IenW), het ministerie van Financiën (Financiën), het ministerie van Onderwijs, Cultuur en Wetenschap (OCW), het ministerie van Volksgezondheid, Welzijn en Sport (VWS), het ministerie van Sociale Zaken en Werkgelegenheid (SZW), de Nationale Politie en het Openbaar Ministerie (OM). Hierin wordt onder andere gesproken over de coördinatie van de NCSA, strategie en beleidsvorming over cybersecurity in het algemeen, het uitwisselen van relevante ervaringen, en nationale incidenten. Internationale cybersecurity en digitale veiligheid komen hierbij ook aan bod.

[al] Het IOIC wordt voorgezeten door BZ, dat met de NCTV, het NCSC, EZK, AIVD, MIVD, BZK en Defensie spreekt over onder andere de Nederlandse inzet in internationale fora en capaciteitsopbouw.

departementale werkgroepen over specifieke thema's, zoals het diplomatiek responsoverleg,[am] de Taskforce Economische Veiligheid (TFEV)[an] en de werkgroep desinformatie.[ao]

Verbeterde samenwerking

De samenwerking op het terrein van (internationaal) cybersecuritybeleid tussen departementen gaat in veel gevallen goed.[50] Zo wordt door veel respondenten positief gesproken over de onderlinge communicatie, de persoonlijke relaties en het feit dat verschillende departementen elkaar vaak goed kunnen vinden.[51] Tijdens de evaluatieperiode (2015-2021) is de aandacht voor cybersecuritybeleid gegroeid binnen de gehele overheid. Dit komt niet alleen tot uiting in de toename van beschikbare middelen voor departementen middels de Versterking van de Nationale Aanpak Cybersecurity (VNAC)-gelden[ap] uit het regeerakkoord van 2017 en de daaraan gekoppelde creatie van de NCSA in 2018, maar ook in de intensivering en formalisering van samenwerking tussen departementen door het ontstaan van een aantal nieuwe werkgroepen en overlegstructuren.[aq] Een aantal geïnterviewden geeft dan ook aan dat de interdepartementale samenwerking over de afgelopen jaren verbeterd is,[52] en dat bij opkomende cyber-gerelateerde onderwerpen, zoals desinformatie en economische veiligheid, de samenwerking in de loop van de tijd vaak verbetert.[53]

Een voorbeeld van een geformaliseerde overlegstructuur waarin de samenwerking zich positief heeft ontwikkeld, is het door BZ voorgezeten diplomatiek responsoverleg. In dit overleg wordt met andere departementen aan de hand van nationale en internationale cybersecurity incidenten gesproken over welke diplomatieke responsopties[ar] er worden ingezet, en waarin steunverzoeken[as] van andere landen voor respons in coalitieverband op cyberincidenten worden behandeld (zie hoofdstuk 4 voor meer informatie over het diplomatiek responskader en -overleg). Hoewel het overleg van betrokkenen van verschillende departementen enige kritiek krijgt,[at54] hebben het herhaaldelijk gebruik van de overlegstructuur, informatie-uitwisselingen en 'successen' als de gecoördineerde respons na de hack op de Organisatie voor het Verbod op Chemische Wapens in Den Haag (de OPCW-casus) en de uitrol van het cybersanctieregime van de Europese Unie (zie hoofdstuk 4) gezorgd voor meer wederzijds begrip, verduidelijking van de onderlinge rollen, en zo tot een betere samenwerking.[55]

[am] Het diplomatiek responsoverleg geeft advies op hoog-ambtelijk of politiek niveau over de Nederlandse reactie op cyberaanvallen. BZ zit dit overleg voor, andere deelnemers van het diplomatiek responsoverleg zijn Defensie, de AIVD, de MIVD, de NCTV, JenV, en op ad hoc basis de Nationale Politie.

[an] De TFEV behandelt economische veiligheidsvraagstukken (zoals de discussie rondom de uitrol van het 5G- netwerk) en bestaat naast de NCTV en BZ uit het ministerie van Algemene Zaken (AZ), BZK, de AIVD en MIVD, Defensie, EZK, IenW, Financiën en de Nationale Politie.

[ao] Bij de werkgroep desinformatie zijn BZK en BZ, alsmede de NCTV, Defensie, OCW, EZK, AIVD, MIVD, en VWS betrokken.

[ap] In het regeerakkoord van 2017 werd 95 miljoen euro gereserveerd voor de Versterking van de Nationale Aanpak Cybersecurity, ook bekend als de VNAC-gelden. BZ ontving daarvan structureel 2 miljoen euro. Voor meer informatie en budgetverdeling, zie het regeerakkoord 'Vertrouwen in de toekomst' (p. 3 en p. 57), beschikbaar via: https://www.rijksoverheid.nl/documenten/publicaties/2017/10/10/regeerakkoord-2017-vertrouwen-in-de-toekomst.

[aq] Zoals het eerdergenoemde IOCS, IOIC, het diplomatiek responsoverleg, de TFEV en de werkgroep desinformatie.

[ar] Diplomatieke respons is een diplomatieke reactie op een cyberaanval door of onder verantwoordelijkheid van een andere staat, zoals het – al dan niet publiekelijk en gezamenlijk met andere landen – aanwijzen van een dader (attributie) en het opleggen van sancties tegen de veronderstelde dader. Hoewel technische bewijsvoering bij diplomatieke respons wel een rol speelt, wordt niet per se beoogd – en is het ook niet altijd mogelijk – tot strafrechtelijke vervolging over te gaan.

[as] Een steunverzoek wordt uitgezet door een land dat in de meeste gevallen zelf slachtoffer is geworden van een cyberaanval, waarbij het zoekt naar een bredere coalitie van landen om gezamenlijk een (diplomatiek) signaal af te geven richting de aanvallers.

[at] Een uitdaging binnen het responsoverleg ontstaat bijvoorbeeld wanneer een steunverzoek van een ander land naar Nederland uitgaat om een cyberaanval gezamenlijk of in coalitieverband te attribueren. BZ wil daar vanuit diplomatieke overwegingen soms sneller op reageren dan voor andere deelnemers aan het responsoverleg wenselijk is, omdat onderzoek en afwegingen van de Nederlandse veiligheidsdiensten ook meegenomen moeten worden en dit soms meer tijd kost.

Uitdagingen

Hoewel interdepartementale samenwerking voor het cybersecuritybeleid in de afgelopen zes jaar is verbeterd, is het ook een van de onderwerpen waarover interviewrespondenten van alle betrokken ministeries en overheidsorganisaties en externe experts en belanghebbenden het meest kritisch zijn,[56] en waarover ook in interne documenten en openbare literatuur[au][57] kritisch wordt gesproken. In deze evaluatie werd aanvankelijk specifiek gekeken naar het internationaal cybersecuritybeleid en focuste op het werk van BZ, maar uit het onderzoek bleek dat de problemen in de samenwerking het internationaal cybersecuritybeleid overstijgen en ook over cybersecuritybeleid in het algemeen gaat. Hieronder worden de belangrijkste uitdagingen en oorzaken hiervan genoemd.

Samenwerkings- en afstemmingsproblemen

Geïnterviewden van alle betrokken departementen en organisaties geven aan dat – ondanks de bestaande overlegstructuren en verbeteringen over de laatste jaren – ministeries nog te vaak langs elkaar heen werken, niet altijd voldoende op de hoogte zijn van elkaars werk, niet altijd voldoende gebruik maken van expertise bij andere departementen, niet altijd voldoende medewerking geven aan elkaar en niet altijd goed met elkaar afstemmen.[58] Een gevolg van deze samenwerkings- en afstemmingsproblemen is dat er inefficiënt wordt gewerkt en beleid niet altijd coherent is.

In interviews met medewerkers van verschillende ministeries komen veel voorbeelden naar voren van zulke samenwerkings- en afstemmingsproblemen en de gevolgen daarvan.[59] Bijvoorbeeld dat medewerkers van betrokken departementen te laat of niet voldoende in een afstemmingsproces betrokken worden of betrokkenheid tonen, en daardoor standpunten op het laatste moment moeten worden aangepast; of dat bij internationale fora een medewerker van een ministerie een collega van een ander ministerie treft, en deze collega andere instructies van zijn of haar departement heeft meegekregen. Ook worden kansen gemist doordat vertegenwoordigers van ministeries die met andere (internationale) organisaties of landen spreken, niet voldoende zicht hebben op welke andere relevante zaken er spelen bij andere ministeries en daardoor niet elkaars belang of het nationale belang behartigen.[60] Zie bijvoorbeeld hoofdstuk 4, waar wordt beschreven hoe diplomatieke ontwikkelingen in internationale standaardenfora[av] werden gemist omdat ze waren belegd bij afgevaardigden van vakdepartementen, en er geen diplomaten van BZ aan deelnamen.

Verschillende belangen

Het probleem is niet alleen dat ministeries soms langs elkaar heen werken, maar ook dat er tegenstrijdige belangen bij ministeries bestaan.[61] Een voorbeeld is dat BZ nationaal en internationaal het kabinetsstandpunt[aw] benadrukt dat de mogelijkheid tot encryptie[ax] belangrijk is voor vrije en veilige communicatie van bijvoorbeeld burgers en journalisten. Tegelijkertijd hebben het Openbaar Ministerie (OM), de Nationale Politie en veiligheidsdiensten er belang bij om opsporing via digitale middelen beter mogelijk te maken, wat door encryptie bemoeilijkt wordt. En hoewel ook de minister van JenV tegen de Tweede Kamer benadrukte achter het encryptiestandpunt te staan, blijkt uit interviews

au Zoals bijvoorbeeld gesteld in Financieel Dagblad, 'Het is tijd voor een Deltaplan Cybersecurity' (2020): https://fd.nl/opinie/1316434/het-is-tijd-voor-een-deltaplan-cybersecurity, het adviesrapport van de Cyber Security Raad (2021): https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid en de op het moment van schrijven nog niet gepubliceerde evaluatie van de NCSA.

av Met standaardenfora worden internationale fora bedoeld waar standaarden voor digitale technologieën worden opgesteld, om de kwaliteit en veiligheid ervan te waarborgen. Voorbeelden hiervan zijn het ITU (standaarden voor nieuwe technologieën) en ICANN (internetstandaarden).

aw Het standpunt van het Nederlandse kabinet over encryptie werd in 2016 in een brief van de ministers van Justitie en Veiligheid en Economische Zaken aan de Tweede Kamer uiteengezet (Kamerstuk 26 643, nr. 383), die te downloaden is via: https://zoek.officielebekendmakingen.nl/kst-26643-383.html.

ax Encryptie is de versleuteling van (gevoelige) informatie, zoals bijvoorbeeld bij berichten in de berichtendienst WhatsApp.

met betrokken beleidsmedewerkers[62] en openbare berichtgeving[ay] dat de wens om encryptie te kunnen omzeilen voor opsporingsdoeleinden wel bestaat bij medewerkers van de opsporings- en veiligheidsdiensten. Een ander voorbeeld is dat economische belangen, die veelal door EZK worden behartigd, kunnen botsen met veiligheids- en geopolitieke belangen die met name door andere ministeries worden behartigd.[63] Dit komt bijvoorbeeld tot uiting op het 5G-dossier dat in hoofdstuk 1 is genoemd, waarbij telecombedrijven vanuit commercieel perspectief gebruik willen maken van het 5G-netwerk van Huawei, terwijl er ook veiligheidsrisico's aanzitten en geopolitieke overwegingen meespelen.[az]

Oorzaken

Beperkte capaciteit

Een oorzaak van problemen in de interdepartementale samenwerking is beperkte capaciteit.[64] Niet alleen bij BZ (zie hoofdstuk 5), maar ook bij andere betrokken ministeries zijn medewerkers druk met eigen specifieke taken en het reageren op de vele ontwikkelingen en urgente dreigingen zoals omschreven in hoofdstuk 1. Hierdoor is er vaak minder tijd voor overleg met anderen, het op de hoogte houden van anderen, of het bijdragen aan de doelen van andere ministeries.[65] Hierbij speelt ook mee dat er een grote hoeveelheid departementen en overheidsorganisaties betrokken is bij het internationaal cybersecuritybeleid, en dat veel beleidsthema's aan elkaar raken. Dit zorgt ervoor dat adequaat afstemmen veel tijd vergt.[66]

Organisatorische verkokering

Een meer structurele oorzaak is de organisatorische verkokering van het Nederlandse cybersecuritybeleid.[67] De verantwoordelijkheid over verschillende beleidsthema's die aan internationaal cybersecuritybeleid raken, is verdeeld over verschillende ministeries (zie ook de eerste paragraaf van dit hoofdstuk), terwijl de problemen en dreigingen zoals omschreven in hoofdstuk 1 over departementale scheidingen heen gaan en niet precies in de departementale categorieën kunnen worden opgedeeld. Onderwerpen als spionage, cybercriminaliteit, economische kansen, economische veiligheid, nieuwe technologieën, en desinformatie zijn met elkaar verweven; de rol van staten, criminelen en bedrijven is met elkaar verweven; en nationale en internationale dreigingen en veiligheid zijn met elkaar verweven. Dit alles betekent dat er beleidsthematische overlap is die de traditionele departementale verdeling van onderwerpen overstijgt.

Een voorbeeld van die verwevenheid is het beleidsthema cybercriminaliteit.[ba] De verantwoordelijkheid voor opsporing en het tegengaan van cybercriminaliteit ligt bij diverse instanties van JenV, zoals het Directoraat-Generaal Rechtspleging en Rechtshandhaving (DGRR), het OM, de Nationale Politie en het NCSC. Ook internationale samenwerking omtrent opsporing, zoals met Europol en Interpol, valt onder de verantwoordelijkheid van JenV. Tegelijkertijd is cybercriminaliteit binnen de Verenigde Naties (VN) een thema geworden dat door toedoen van Rusland sterk wordt gelinkt aan diplomatieke inzet (zie hoofdstuk 4), waardoor cybercriminaliteit als thema niet los van cyberdiplomatie kan worden behandeld. Bovendien is het niet altijd mogelijk vast te stellen of een statelijke, een daaraan gelieerde, of een criminele actor bij een cyberaanval betrokken is (zoals uitgelegd in hoofdstuk 1). Dit maakt het lastig om te bepalen binnen welk gremium het incident wordt behandeld en welke ministeries daarbij betrokken worden.

[ay] Zie: antwoord op vragen van het lid Verhoeven over het verzwakken van encryptie door de minister van Justitie en Veiligheid (2021), beschikbaar via: https://zoek.officielebekendmakingen.nl/ah-tk-20202021-1959.html. Voor andere publiek beschikbare informatie over de discussie rondom encryptie, zie bijvoorbeeld het 2021 NOS-artikel: https://nos.nl/artikel/2371134-overheid-werkt-aan-plan-voor-afzwakken-encryptie-taak-voor-nieuw-kabinet.html en het RTL-artikel: https://www.rtlnieuws.nl/tech/artikel/5219525/grapperhaus-minister-justitie-veiligheid-encryptie-versleuteling-whatsapp.

[az] Geopolitieke overwegingen en veiligheidsrisico's zijn belangrijk voor bijvoorbeeld de NCTV en de veiligheidsdiensten (AIVD en MIVD). De veiligheidsdiensten sloegen in 2021 in het Financieel Dagblad dan ook alarm over Chinese cyberdreigingen in Nederland: https://fd.nl/economie-politiek/1373125/veiligheidsdiensten-slaan-samen-alarm-om-chinese-cyberdreiging-in-nederland. Voor een andere openbare bron die naast de veiligheidsbelangen ook de economische belangen rondom het 5G-netwerk uiteenzet, zie bijvoorbeeld dit artikel in Trouw uit 2020: https://www.trouw.nl/economie/het-chinese-huawei-in-het-hart-van-ons-internet-is-dat-wel-zo-verstandig~bbe8ce14/.

[ba] Cybercriminaliteit wijst in brede zin naar activiteiten die uitgevoerd worden met ICT-middelen voor criminele doeleinden. Zie de informatiepagina van de politie (https://www.politie.nl/onderwerpen/cybercrime.html) voor meer informatie.

In de literatuur, interviews, en de survey wordt dan ook gepleit dat er voor de aanpak van cyberdreigingen een *whole-of-government* aanpak[bb] nodig is, of in ieder geval voor een organisatorische opzet waarin de huidige departementale verkokering wordt tegengegaan.[bc68]

Gebrek aan overkoepelende strategie en aansturing

De organisatorische verkokering van het Nederlandse cybersecuritybeleid komt onder andere tot uiting in het feit dat er geen departementaal-overkoepelende cybersecuritystrategie is. De betrokken ministeries hebben ieder hun eigen focus en stellen ieder hun eigen prioriteiten, ook bij bijvoorbeeld de inzet van de VNAC-gelden.[69] Zoals eerder genoemd is er wel de NCSA, maar dit is feitelijk een samenvatting van de verschillende prioriteiten van ministeries. Het is niet een departementaal-overstijgende coherente nationale cybersecuritystrategie waarin mogelijk botsende belangen worden beslecht, prioriteiten worden gesteld, en gezamenlijke ministeriele keuzes worden gemaakt over de kant die Nederland op wil met cybervraagstukken.[bd70] Ook is er geen centrale aansturing van het cybersecuritybeleid die zo'n strategie op zou kunnen stellen, prioriteiten stelt, en een koers uitstippelt. De NCTV heeft binnen de overheid wel een coördinerende rol op het gebied van nationale cybersecurity, maar dit omvat niet alle cyber(security)gerelateerde onderwerpen.[be] De NCTV heeft geen aansturende rol, en de NCTV staat niet boven de ministeries maar valt onder de verantwoordelijkheid van de minister van JenV.

Aanbevelingen

Hoewel deze evaluatie specifiek over het internationaal cybersecuritybeleid van BZ gaat, blijken de in dit hoofdstuk gesignaleerde uitdagingen breder, en vereisen ze departementaal-overkoepelende oplossingen. De departementale verkokering van het Nederlandse cybersecuritybeleid dient te worden tegengegaan om (samenwerking in) het beleid te verbeteren, en daarmee sneller, efficiënter en beter te kunnen reageren op dreigingen en mogelijkheden in het digitale domein. Hieronder staan twee specifieke aanbevelingen hiervoor.

Voor het Nederlandse kabinet:

Creëer een departement-overstijgende cybersecuritystrategie

Creëer een departement-overstijgende cybersecuritystrategie, die:

- Een kabinetsvisie presenteert van de kant die Nederland op wil met aan cybersecurity gerelateerde onderwerpen.
- Mandaten, taken en verantwoordelijkheden van betrokken departementen en organisaties vastlegt.
- Geen samenvatting is van zaken die departementen al doen of van plan zijn te doen, maar verbinding aanbrengt tussen de verschillende beleidsthema's door prioriteiten te stellen, eventuele botsende belangen te beslechten, concrete doelstellingen op te nemen en in te gaan op hoe deze doelen bereikt kunnen worden.

[bb] De *whole-of-government* aanpak is een aanpak waarbij 'gebruik wordt gemaakt van de unieke expertise, middelen en autoriteiten van elk ministerie, en van elk middel, of elke combinatie van middelen, die het meest effectief is om een bepaalde dreiging te verstoren.' (Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 3 en p. 70).

[bc] Zie voor een andere publiek beschikbare bron waarin dit wordt bepleit de BNR-Nieuwsradio podcastaflevering van 12 juli 2020, 'Hoe cyberdreiging ons leven kan ontwrichten', met Jaya Baloo, CISO van Avast en cybersecurity-journalist Brenno de Winter, terug te luisteren via https://www.bnr.nl/podcast/de-strateeg/10415198/hoe-cyberdreiging-ons-leven-kan-ontwrichten.

[bd] Hetzelfde geldt voor de Internationale Cyberstrategie, wat leest als een samenvatting van verschillende beleidsthema's en prioriteiten waarvan cybersecuritybeleid een onderdeel is, zoals eerder omschreven. In de Geïntegreerde Buitenland- en Veiligheidsstrategie, dat weliswaar van geïntegreerd veiligheidsbeleid spreekt, is cybersecuritybeleid en digitale veiligheid slechts een van meerdere veiligheidsonderdelen. Deze documenten kunnen dus niet worden geoormerkt als departementaal-overkoepelende cybersecuritystrategieën.

[be] Zoals, bijvoorbeeld, het thema internationale vrede en veiligheid waar BZ de coördinerende rol in heeft. Zie Brief van de minister van Justitie en Veiligheid, 20 april 2018. Kamerstukken II 2017-2018, 26 643, nr. 536, p. 2.

Bij het opstellen van de nationale cybersecuritystrategie kan geleerd worden van andere landen, zoals Australië, de VS en het Verenigd Koninkrijk (VK),[bf] en van experts uit het bedrijfsleven en kennisinstellingen (zie ook hoofdstuk 5).

Onderzoek op welke manier departement-overstijgende aansturing van cybersecurityzaken het beste kan worden vormgegeven, en realiseer dit.

Een overkoepelende strategie alleen is niet genoeg, onder andere omdat er – zeker gegeven de snelle ontwikkelingen en vele onderlinge verbanden in het cyberdomein – altijd zaken zullen opkomen waar de strategie geen antwoord op geeft. Er is ook departement-overstijgende aansturing nodig, die zorgt voor het vaststellen van mandaten en taken bij nieuwe vraagstukken, het afwegen van verschillende belangen en het opstellen, monitoren en wanneer nodig bijstellen van de eerdergenoemde strategie, en meer algemeen het verbinden van de verschillende beleidsterreinen en bevorderen van onderlinge afstemming. Hierbij dient goed nagedacht te worden over de beste vorm.

- Er zijn verschillende opties,[71] zoals een departement-overkoepelende stuurgroep, een ministeriele onderraad[bg] of een andere ministerieel overleg- en besluitvormingsorgaan; een orgaan naar model van de nationale veiligheidsraad, zoals bestaat in de VS;[bh] of een minister(ie) van Digitale Zaken.[bi72]
- De verschillende opties zullen elk hun eigen uitdagingen met zich meebrengen, mede gezien het feit dat de expertise voor de verschillende aspecten van cybersecuritybeleid bij de vakdepartementen ligt. Zo zou een ministerie van Digitale Zaken onder andere het risico met zich meebrengen dat er meer afstemmingsproblemen komen in plaats van minder, omdat het werk van zo'n ministerie zal raken aan het werk van alle vakdepartementen.[73]
- Een organisatorische verandering van de aansturing van cybersecuritybeleid moet dan ook geen doel op zich zijn. Er dient daarom onderzocht te worden welke optie het meest geschikt is om de beleidsdoelen te behalen en een mogelijke oplossing biedt voor de in dit hoofdstuk gesignaleerde problemen.

[bf] Australië heeft zowel een nationale cybersecurity strategie (beschikbaar via (EN): https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf) als een internationale cyber engagement strategie waarin verschillende internationale beleidsthema's die aan cybersecurity raken, zijn samengevoegd (beschikbaar via (EN): https://www.internationalcybertech.gov.au/our-work. De nationale cybersecurity strategie van het VK wordt in 2021 vernieuwd, voor de strategie van 2016-2021, zie (EN): https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. In de VS is in 2019 de *Cyberspace Solarium Commission* opgezet, die in 2020 een rapport uitbracht met aanbevelingen voor de strategie en organisatorische opzet voor afschrikking in het cyberdomein, zie (EN): https://www.solarium.gov/. Voor een vergelijkend perspectief van 22 nationale cybersecurity strategieën, zie het artikel van de Britse denktank RUSI (2021, EN): https://rusi.org/explore-our-research/publications/occasional-papers/exploring-national-cyber-security-strategies-policy-approaches-and-implications.

[bg] Zoals ook aanbevolen in het advies van de Cyber Security Raad van april 2021: https://www.cybersecurityraad.nl/actueel/nieuws/2021/04/06/csr-adviseert-%E2%82%AC833-miljoen-voor-een-integrale-aanpak-voor-cyberweerbaarheid.

[bh] Meer informatie over de Nationale Veiligheidsraad van de VS is te vinden via (EN): https://www.whitehouse.gov/nsc/.

[bi] Een ministerie van Digitale Zaken is eerder voorgesteld in partijprogramma's van de 2021 Tweede Kamer verkiezingen: zo werd bijvoorbeeld in het Volt verkiezingsprogramma (https://voltnederland.org/standpunten) en het verkiezingsprogramma van de Piratenpartij (https://wiki.piratenpartij.nl/tk2021:partijprogramma:thema#minister_van_digitale_zaken) een ministerie van Digitale Zaken genoemd. In het verkiezingsprogramma van D66 (https://d66.nl/verkiezingsprogramma/) werd gepleit voor een minister van Digitalisering.

3 Strategie en doelstellingen internationaal cybersecuritybeleid BZ

Doelen internationaal cybersecuritybeleid BZ

Zoals in de vorige hoofdstukken beschreven, is het internationaal cybersecuritybeleid binnen BZ in 2015 belegd bij de speciaal daarvoor opgerichte Taskforce Cyber, en zijn er sindsdien verschillende (interdepartementale) beleidsdocumenten opgesteld die aan het internationaal cybersecuritybeleid raken.[bj] Hiervan zijn de Internationale Cyberstrategie (ICS), de Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS) en de Nederlandse Cybersecurity Agenda (NCSA) het meest leidend voor BZ.

De doelstellingen van BZ voor het internationaal cybersecuritybeleid zijn deels in de ICS, GVBS en NCSA, en deels in Kamerbrieven omschreven. Op basis van analyse van deze stukken, interne beleidsdocumenten en interviews kunnen deze doelstellingen als volgt worden samengevat:[74]

1. Het coördineren en formuleren van adequate diplomatieke en politieke respons bij digitale aanvallen.[75]

2. Het bevorderen van de internationale rechtsorde (het tegengaan van straffeloosheid, het vergroten van accountability en het beschermen van mensenrechten online, waarbij de universele toepassing van het bestaand internationaal recht en vrijwillige, niet-bindende gedragsnormen de uitgangspunten voor het normatief kader vormen).[76]

3. Het versterken van internationale samenwerking door het vormen van partnerschappen en verbreden van internationale coalities, onder andere[bk] door middel van (kennis)capaciteitsopbouw in derde landen.[77]

Naast bovenstaande drie doelen wordt in Kamerbrieven,[78] beleidstukken,[79] en Nederlandse inbreng in internationale fora[80][bl] ook vaak het streven genoemd van een 'open, vrij en veilig internet'.

Doelen internationaal cybersecuritybeleid BZ?

Wat uit bovenstaande beschrijving blijkt, is dat er niet één plek is waar de doelen voor het internationaal cybersecuritybeleid van BZ vastliggen en worden uitgewerkt. Betrokken medewerkers van BZ geven dan ook aan verschillende documenten aan te houden als leidraad voor hun werk:[81] de NCSA, de ICS, de GBVS, en Kamerbrieven.

[bj] Strategieën die raken aan het internationaal cybersecuritybeleid zijn bijvoorbeeld: de Digitale Agenda voor Buitenlandse Handel en Ontwikkelingssamenwerking (2019), de Defensie Cyber Strategie (2018), de Defensienota 2018 en de Defensievisie 2035 (2020), de Nederlandse Digitaliseringsstrategie 2020 (p. 15, p. 22, p. 41), en de eerdergenoemde Internationale Cyberstrategie (2017), Geïntegreerde Buitenland- en Veiligheidsstrategie (2018) en de Nederlandse Cybersecurity Agenda (2018).

[bk] Andere manieren waarop BZ internationale samenwerking op het gebied van cybersecurity probeert te versterken is via bilaterale cyberdialogen, zoals de Indonesië-Nederland dialoog, of via regionale dialogen, zoals de cyberdialoog met de Westelijke Balkan. Voor openbare informatie over de Indonesië-Nederland dialoog, zie: https://www.rijksoverheid.nl/documenten/diplomatieke-verklaringen/2021/01/21/eerste-indonesie-nederland-dialoog-over-internationaal-cyberbeleid-gezamenlijke-verklaring (21 januari 2021); voor de dialoog met de Westelijke Balkan, zie: https://magazines.rijksoverheid.nl/bz/veiligheidsdiplomaat/2021/03/03 (april 2021).

[bl] Zoals in papers, spreekpunten en speeches van TFC-leden binnen internationale organisaties, zoals de Europese Unie en de Verenigde Naties, en bij optredens op internationale conferenties.

Deze documenten hanteren niet allemaal dezelfde omschrijving van de doelen en zijn niet allemaal even recent. Betrokken BZ-medewerkers geven dan ook verschillende omschrijvingen en interpretaties van de doelen,[82] en niet iedereen beschrijft ze zoals eerder in dit hoofdstuk samengevat. De gevolgen hiervan worden later in dit hoofdstuk omschreven.

Daarnaast is de rol van een 'open, vrij en veilig internet' niet duidelijk. Zo omschrijven sommige betrokkenen en documenten het als een ultiem doel waar de andere doelen tot moeten leiden; anderen als een visie of streven die naast de andere doelen staat; anderen als de boodschap die wordt uitgedragen in diplomatieke fora, en anderen als een combinatie van deze elementen.[bm][83]

Ook is er geen duidelijk vastgelegde,[bn] breed gedeelde[84] definitie van wat een open, vrij en veilig internet omhelst. 'Open' en 'vrij' worden door elkaar heen gebruikt om te verwijzen naar het niet blokkeren van delen van het internet voor inwoners door overheden; het niet afschermen van toegang tot internetgebruikers door andere landen; vrijheid van meningsuiting online; en bescherming tegen surveillance van internetgebruikers door de overheid. 'Veilig' wordt gebruikt om te duiden op de bescherming tegen aanvallen van staten of criminelen, maar ook de bescherming tegen surveillance van internetgebruikers en het schenden van de vrijheid van meningsuiting door overheden.[85]

Los van verschillen in interpretatie denken departementen ook verschillend over welk aspect prioriteit heeft, bijvoorbeeld over 'vrij' (geïnterpreteerd als vrij van surveillance door de overheid) versus 'veilig' (geïnterpreteerd als beschermd tegen criminaliteit) zoals bij het encryptievraagstuk dat in het vorige hoofdstuk beschreven is. Wat hierbij ook meespeelt, is dat er een verschuiving heeft plaatsgevonden in het denken over het open, vrij en veilige internet gedurende de evaluatieperiode.[86] Die verandering komt onder andere door de in hoofdstuk 1 omschreven toename van incidenten, fragmentatie van het internet, het onder druk staan van de internationale rechtsorde en de groeiende zorgen over online desinformatie. Zo formuleert het Nederlandse kabinet op het moment van schrijven een reactie op een advies van de Adviesraad Internationale Vraagstukken (AIV). Het advies pleit ervoor keuzes te maken voor de veiligheid van het internet, ten koste van het grensoverschrijdende, open karakter van het internet.[bo]

Een vergelijkbare onzekerheid bestaat over hoe capaciteitsopbouw in derde landen (zie de derde doelstelling hierboven) samenhangt met de andere doelen. Capaciteitsopbouw betekent in dit kader 'financiële ondersteuning voor projecten die de cybercapaciteiten van lage inkomenslanden proberen te verbeteren, waarbij de focus voornamelijk ligt op kennisopbouw' (zie hoofdstuk 4).

[bm] Het open, vrij en veilig internet wordt omschreven als 'doel' waarnaar de drie doelstellingen toewerken (Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, pp. 2-3) of waartoe de 'drie sporen van de Nederlandse beleidsinzet in het internationale cyberdomein' dienen (Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, p.8); als 'streven' dat Nederland uitdraagt in 'globale fora' om andere landen te overtuigen zich daarvoor in te zetten (Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62, p. 10) of 'Nederlandse waarden' die geëxporteerd worden (NCSA p. 10); of als 'visie' (NCSA p. 23; 'Digitaal bruggen slaan' – Internationale Cyberstrategie: naar een geïntegreerd internationaal cyberbeleid (ICS), 12 februari 2017. Kamerstuk II 2016-2017, 26 643, nr. 447, bijlage 80029, p. 8).

[bn] In de NCSA is geen expliciete definitie opgenomen van het open, vrij en veilig internet, maar wordt het omschreven als waarden van Nederland: "[Digitale autonomie] bevordert bovendien de export van Nederlandse waarden als een open, vrij en veilig internet" (p. 10). Ook wordt het open, vrij en veilig internet genoemd als 'maatregelen' bij de tweede ambitie: het bevorderen van een "internationale coalitie die de visie van een open, vrij en veilig internet onderschrijft" (p. 23) en een "intensieve bijdrage aan een vrij, open en veilig internet" te leveren (p.24). In de ICS wordt gesproken van het open, vrij en veilig internet als 'visie' (p. 8) en 'belangen' (pp. 2-3), met uitleg: het 'open' internet wordt gezien als "ongefragmenteerd Internet, waarin informatie vrij kan bewegen" en waardoor het internet met "effectieve zelforganisatie en zelfregulering [kon] uitgroeien tot een wereldwijd gedeelde en voor iedereen toegankelijke infrastructuur" (p. 2). 'Veilig' en 'vrij' worden samen uitgelegd om de onderlinge complementariteit te onderstrepen: "een veilige samenleving is een samenleving waarin de fundamentele rechten en vrijheden van het individu worden beschermd." (p.3). In de GBVS wordt de term niet gedefinieerd, maar wordt kort gesteld: "Nederland is met zijn open en geglobaliseerde economie en vrije samenleving gebaat bij een vrij, open en veilig internet." (p.7).

[bo] Het AIV-adviesrapport 'Regulering van online content. Naar een herijking van het Nederlandse internetbeleid' (2020) is beschikbaar via: https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2020/06/24/regulering-van-online-content.

Volgens sommige geïnterviewden[87] en de ICS[bp] is capaciteitsopbouw een vorm van ontwikkelingssamenwerking, met als doel het helpen van andere landen. Een meer gangbare opvatting onder betrokkenen is echter dat capaciteitsopbouw geen doel op zich is, maar een middel voor het bereiken van een strategisch doel. Een deel van de betrokkenen,[88] de NCSA en GBVS[bq] beschrijven capaciteitsopbouw hierbij als een middel om te helpen cyberdreigingen te mitigeren, met het argument dat 'de mondiale cybersecurityketen zo sterk is als de zwakste schakel' - dit betekent dat Nederland onveiliger wordt wanneer derde landen een zwakke cybersecurity hebben. Volgens andere betrokkenen[89] en Kamerstukken[br] is capaciteitsopbouw voornamelijk een middel om coalities te creëren voor de Nederlandse visie op de internationale rechtsorde en (diplomatieke) respons, door zogeheten *swing states*[bs] te overtuigen van deze visie en dat uit te dragen in internationale fora (zie hoofdstuk 4).[90] Deze verschillende interpretaties hoeven elkaar niet tegen te spreken – capaciteitsopbouw zou in principe meerdere doelen tegelijk kunnen hebben. Maar welk doel voornamelijk wordt nagestreefd met capaciteitsopbouw, heeft invloed op hoe het in de praktijk het beste ingezet kan worden. Dit wordt verder besproken in hoofdstuk 4.

Strategie en strategische reflectie

Beperkte definities, strategie en strategische reflectie

Naast dat de doelen van BZ niet op één duidelijke plek vastliggen, zijn de doelen (zoals 'het bevorderen van de internationale rechtsorde') vrij abstract. Dit is omdat ze niet altijd gelinkt zijn aan definities en uitwerkingen van relevante termen zoals 'bevorderen van de internationale rechtsorde', 'mensenrechten online', 'cybersecurity' en 'cyberbeleid', waardoor niet altijd duidelijk is wat men precies wil bereiken.[91] Op de tweede plaats zijn er niet voor elk hoofddoel subdoelen geformuleerd over wat men bijvoorbeeld binnen één, twee en vijf jaar zou willen bereiken, en ontbreekt er een eenduidige strategie voor hoe dit bereikt zou moeten worden.[92] Dit maakt het lastig om te bepalen of en wanneer een doel al dan niet bereikt is.

Het ontbreken van gedetailleerde doelstellingen is tot op zekere hoogte begrijpelijk, omdat cybersecurity een beleidsterrein is waarin ontwikkelingen elkaar snel opvolgen en waarin het al dan niet behalen van doelen afhangt van veel andere actoren en onzekere factoren. Een zeer gedetailleerde strategie waarin precies staat wat BZ de komende tien jaar gaat doen, zou daarom waarschijnlijk snel achterhaald zijn.

Niettemin zijn vaak gehoorde kritiekpunten[93] op het internationaal cybersecuritybeleid van BZ het gebrek aan een eenduidige, duidelijke en up-to-date strategie en dat er onvoldoende voor de langeretermijn strategisch wordt nagedacht en gepland. Deze kritiek

[bp] De ICS stelt bijvoorbeeld: "Het is van belang de internationale digitale kloof tussen technologisch meer en minder ontwikkelde landen te dichten, zodat derde landen kunnen profiteren van de kansen die wereldwijde digitalisering biedt. Capaciteitsopbouw binnen het cyberdomein is dan ook van groot belang." (ICS p. 8).

[bq] De GBVS stelt bijvoorbeeld: "Nederland investeert in de digitale weerbaarheid van partnerlanden om hen te helpen hun kennis- en expertiseniveau naar een zo hoog mogelijk niveau te brengen en zo de zwakke schakels in de wereldwijde internetinfrastructuur te versterken." (p. 26), en de NCSA: "Nederland versterkt de mondiale cybersecurityketen door het cybersecurityniveau van derde landen te verhogen." (p. 24).

[br] Zoals de Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60: "Nederland ondersteunt bovendien activiteiten die bijdragen aan de capaciteitsopbouw in derde landen, niet in de laatste plaats in landen die we in VN-verband nodig hebben (G-77 landen) voor een brede coalitie ter bevordering van verantwoordelijk gedrag in het cyberdomein", en de ICS stelt "Op langere termijn helpen investeringen van Nederland in capaciteitsopbouw om strategische allianties op te bouwen gericht op het ondersteunen van een vrij, open en veilig internet en aanverwante Nederlandse beleidsdoelstellingen." (p. 8).

[bs] *Swing states* is een aanduiding voor landen met wisselende of nog ontwikkelende politieke standpunten binnen het internationale cyberdomein, wiens keuzes of stemgedrag binnen internationale fora en politiek van doorslaggevende invloed kunnen zijn. Zie voor een uitleg het paper van Chatham House en de Global Commission on Internet Governance uit 2014 (EN): https://www.cigionline.org/sites/default/files/gcig_paper_no2.pdf) en de literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 86.

gaat enerzijds over (een gebrek aan) strategie in het algemeen, zoals dat er wel wordt nagedacht over hoe te reageren op huidige dreigingen, maar niet genoeg over hoe er in de toekomst gehandeld kan worden bij verschillende scenario's die kunnen ontstaan in de wereld – wat juist bij een beleidsonderwerp met snelle veranderingen waardevol is. Anderzijds is deze kritiek meer specifiek, zoals dat strategieën ontbreken voor hoe capaciteitsopbouw en cyberdiplomaten het beste ingezet kunnen worden (zie ook hoofdstukken 4 en 5).

Medewerkers van de Taskforce Cyber (TFC) zijn druk met reageren op urgente dreigingen (omschreven in hoofdstuk 1), en voor strategische reflectie en het opstellen van een up-to-date strategie wordt onvoldoende tijd genomen (zie ook hoofdstuk 5).[94] Het in het vorige hoofdstuk beschreven gebrek aan een coherente, overkoepelende interdepartementale cybersecuritystrategie waarin prioriteiten worden gesteld, speelt ook mee in het ontbreken van een eenduidige, duidelijke en up-to-date strategie voor het internationaal cybersecuritybeleid. Het verder uitwerken van concrete stappen, scenario's en definities voor BZ en de TFC zou onderdeel moeten zijn van een overkoepelende interdepartementale cybersecuritystrategie, of daaruit moeten volgen.

Gevolgen

Het ontbreken van een up-to-date, eenduidige strategie en definities betekent dat er geen duidelijke kaders bestaan voor afwegingen over wat wel en niet onder internationaal cybersecuritybeleid valt. Daarmee is onduidelijk wat wel en niet onder de verantwoordelijkheid van de TFC of andere directies binnen BZ valt.[95] De TFC houdt zich deels bezig met zaken die direct te maken hebben met het voorkomen en mitigeren van cyberdreigingen en -aanvallen gericht op Nederland, zoals (diplomatieke) respons tegen cyberaanvallen en internationale normen en recht over cyberaanvallen. Daarnaast houdt de TFC zich bezig met beleidsthema's die alleen indirect te maken hebben met de cybersecurity van Nederland, zoals de bevordering van online mensenrechten in andere landen en capaciteitsopbouw in derde landen. Door het ontbreken van duidelijke kaders van wat wel en niet bij het internationaal cybersecuritybeleid hoort is nu niet helemaal duidelijk[96] op basis waarvan de organisatorische knip is gemaakt tussen deze laatste beleidsthema's en bijvoorbeeld cybersecurity en handelsbevordering, dat bij de Directie Internationaal Ondernemen (DIO) ligt; de Digitale Agenda voor Buitenlandse Handel en Ontwikkelingssamenwerking,[bt] dat onder meer bij de Directie Sociaal Ondernemen (DSO) ligt; *dual-use*[bu] exportcontrole, dat bij Directie Internationale Marktordening en Handelspolitiek (IMH) ligt; en het algehele mensenrechtenbeleid, dat bij de Directie Multilaterale Instellingen en Mensenrechten (DMM) ligt. Er wordt zelfs verschillend gedacht over de vraag of de TFC alleen verantwoordelijk is voor het internationaal cybersecuritybeleid, zoals gesteld door sommige betrokkenen, of voor het bredere internationaal cyberbeleid, zoals gesteld door anderen.[97]

Het ontbreken van kaders en definities zorgt met name voor uitdagingen bij het organisatorisch onderbrengen van nieuwe beleidsthema's, die zoals beschreven regelmatig opkomen.[98] Zo zijn gedurende de evaluatieperiode beleidsthema's als *Artificial Intelligence*, kwantumtechnologie, economische veiligheid, desinformatie en regulering van online content in belang toegenomen.[99] Dergelijke thema's raken aan cybersecurity, en daarmee aan het werk van verschillende ministeries, verschillende afdelingen binnen BZ, zoals de hierboven genoemde directies, en bijvoorbeeld ook aan verschillende afdelingen binnen de Directie Veiligheidsbeleid (DVB).

Dit heeft als risico dat niemand zich voldoende verantwoordelijk voelt en zaken niet goed of niet tijdig worden opgepakt, of dat er niet optimaal wordt geanticipeerd op nieuwe thema's en dreigingen.[100] Daarnaast worden nu soms zaken belegd bij de persoon, afdeling of beleidsdirectie die er capaciteit voor heeft, in plaats van dat gekeken wordt waar het onderwerp het beste behandeld zou kunnen worden.[101]

[bt] Zie de Digitale Agenda voor Buitenlandse Handel en Ontwikkelingssamenwerking (2018), te raadplegen via: https://www.rijksoverheid.nl/ministeries/ministerie-van-buitenlandse-zaken/documenten/rapporten/2019/06/03/rapprt-digitale-agenda-voor-buitenlandse-handel-en-ontwikkelingssamenwerking.

[bu] Dual-use goederen zijn goederen die voor zowel militaire als civiele doelen kunnen worden gebruikt. In het geval van cybersecurity duidt het op dat dezelfde digitale (genetwerkte) technologie gebruikt kan worden voor zowel militaire als civiele doelen.

Binnen het werk van de TFC maakt het ontbreken van beleidskaders met korte, middellange- en langetermijndoelen het moeilijker om te bepalen wat prioriteit zou moeten hebben binnen het werk van de TFC en waar nee tegen gezegd kan worden. Naar welke internationale fora gaan we wel en niet? Aan welke landen en organisaties geven we financiële ondersteuning voor capaciteitsopbouw? Met welke landen gaan we de dialoog aan? Op welke verzoeken van organisaties, andere departementen en andere landen gaan we wel en niet in? Over dit soort vragen wordt uiteraard nagedacht, en er wordt gewerkt met een jaarplan. Niettemin zorgt het ontbreken van een duidelijkere strategie ervoor dat er soms teveel ad-hoc gewerkt wordt op basis van welke dreigingen, verzoeken, internationale bijeenkomsten, overleggen, en andere acute zaken er op de TFC afkomen, in plaats van dat er prioriteiten worden gesteld op basis van wat men denkt dat op de langere termijn het meeste effect heeft op het behalen van de doelen.[102] Dit alles zorgt voor een extra aanslag op de capaciteit, zoals in hoofdstuk 5 aan bod komt.

Aanbevelingen

Voor het ministerie van Buitenlandse Zaken:

Creëer, als onderdeel van of aansluitend op de nieuwe interdepartementale cybersecuritystrategie (zie hoofdstuk 2), ook een nieuwe strategie voor het internationaal cybersecuritybeleid van BZ.

Zorg er hierbij voor dat:

- Duidelijke definities en kaders worden opgenomen zodat inzichtelijk is wat al dan niet onder de verantwoordelijkheid van de TFC valt.
- Duidelijk uiteengezet wordt wat de korte-, middellange- en langetermijndoelen zijn, hoe deze op elkaar aansluiten en hoe beoogd wordt deze te bereiken.
- Bij het opstellen van de strategie samengewerkt wordt met andere departementen (zie hoofdstuk 2) en stakeholders uit het bedrijfsleven en kennisinstellingen (zie hoofdstuk 5).

Bouw tijd en capaciteit in voor regelmatige reflectie op beleid en het denken in scenario's.

Gegeven de snelle ontwikkelingen in het cyberdomein dient er tijd en capaciteit ingebouwd te worden voor regelmatige strategische reflectie en herbezinning op het beleid, het denken in scenario's over verschillende mogelijke toekomstige ontwikkelingen en dreigingen, en waar nodig actualisering van de strategie.

Het opvolgen van deze aanbevelingen kost tijd en capaciteit. Voor de aanbevelingen omtrent de capaciteit voor het internationaal cybersecuritybeleid, zie hoofdstuk 5.

4 Inzet en activiteiten

Het ministerie van Buitenlandse Zaken (BZ) onderneemt verschillende activiteiten om bij te dragen aan het behalen van de in het vorige hoofdstuk beschreven doelen. Zoals in hoofdstuk 2 omschreven, heeft BZ binnen Nederland een coördinerende rol op het gebied van internationale vrede en veiligheid. In de praktijk betekent dit dat BZ voor de eerste doelstelling, adequate respons bij digitale aanvallen en incidenten, nationaal het diplomatiek responsoverleg coördineert en zich hiervoor inzet in coalitieverband en in de Europese Unie (EU) en de Noord-Atlantische Verdragsorganisatie (NAVO). Een groot deel van de inzet voor het tweede doel, de bevordering van de internationale rechtsorde, bestaat uit diplomatieke activiteiten in verschillende multilaterale fora zoals de Verenigde Naties (VN), de EU, de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) en de NAVO. Tevens zet BZ zich in bilateraal verband in om zowel met gelijkgestemde als niet-gelijkgestemde landen dialoog te voeren.[bv] Daarnaast geeft BZ financiële steun aan organisaties die helpen met cybercapaciteitsopbouw en kennisdeling in derde landen, zoals aan Cyber Law International (CLI) voor trainingen over internationaal recht, het Global Forum on Cyber Expertise (GFCE) voor kennisdeling over internationale capaciteitsopbouw en aan organisaties als Global Partners Digital (GPD) en Access Now ter bevordering van mensenrechten online. Dit hoofdstuk bevat meer informatie over de verschillende soorten inzet van Nederland, en de successen en uitdagingen die hierbij komen kijken.

Respons

Zoals in hoofdstuk 1 besproken, vinden er dagelijks digitale aanvallen plaats waar Nederland en zijn bondgenoten mee te maken hebben. Discussies over het al dan niet (collectief) reageren op dergelijke aanvallen en binnengekomen steunverzoeken van andere landen, vinden regelmatig plaats en worden gevoerd in het in hoofdstuk 2 geïntroduceerde interdepartementaal diplomatiek responsoverleg. In bepaalde gevallen wordt door de betrokken partijen een gecoördineerde diplomatieke respons jegens de aanvaller voorgesteld, of wordt steun verleend aan een verzoek van een land of coalitie. Bekende output van dit responsoverleg is de OPCW-casus, waarbij in coalitieverband uiteindelijk sancties werden opgelegd aan de Russen die verantwoordelijk worden gehouden voor de hack op de OPCW in Den Haag in 2018.[bw] Het eerste doel van de inzet voor attributie en diplomatieke respons is om de kosten op slecht gedrag te verhogen en om zo de besluitvorming van statelijke actoren te beïnvloeden, waarbij het blootleggen van een schadelijke cyberactiviteit reputatieschade voor de agressor kan opleveren of een opmaat kan zijn voor sancties en/of tegenmaatregelen.[103] Een ander doel is met attributie en diplomatieke respons een normerend effect te bewerkstelligen, doordat normoverschrijdend gedrag door een staat of daaraan gelieerde actor in het cyberdomein wordt aangekaart en afgekeurd.[104] Voor het Nederlandse kabinet is een responscoalitie met gelijkgestemde landen belangrijk, waar het onder meer in EU-verband aan bouwt.[105]

Belangrijke instrumenten in het kader van responsactiviteiten zijn de EU *Cyber Diplomacy Toolbox* en het EU cybersanctieregime, dat volgens betrokkenen en interne documenten instrumenten zijn waar Nederland een sterke bijdrage aan heeft geleverd.[106] De toolbox – het beleidskader dat diplomatieke handvatten biedt om als EU bij incidenten en aanvallen te reageren – is tijdens het Nederlands voorzitterschap van de EU in 2016

[bv] Gelijkgestemde landen zijn landen met vergelijkbare politieke standpunten binnen het internationale cyberdomein.

[bw] Zie voor openbare berichtgeving over de OPCW-casus bijvoorbeeld het artikel op NU.nl (2020): https://www.nu.nl/tech/6067694/eu-legt-vier-russen-sancties-op-voor-hackaanval-op-opcw-in-den-haag.html.

opgezet, in 2017 operationeel geworden, en in 2019 uitgebreid met een inmiddels operationeel cybersanctieregime.[bx] Het cybersanctieregime wordt zowel in documenten als door geïnterviewden omschreven als een belangrijke stap in het verbreden van de Europese wens voor gecoördineerde diplomatieke respons.[107] Deze eerste stap maakt het mogelijk om aanvallen publiekelijk te veroordelen en vervolgens consequenties aan grensoverschrijdend gedrag in het cyberdomein te verbinden.[108] Hoewel overgaan tot attributie en diplomatieke respons een belangrijk signaal af kan geven, twijfelen sommige geïnterviewden aan de verwachting dat het op termijn het gedrag van aanvallers positief zal beïnvloeden, omdat zij bijvoorbeeld vermoeden dat het nauwelijks een afschrikkende werking zal hebben voor belangrijke cyberagressors als Rusland en China.[109] Deze twijfel bestond al onder vertegenwoordigers van sommige ministeries toen dit EU-instrumentarium werd opgezet,[by] en blijkt bij sommigen dus nog steeds te bestaan. De *Toolbox* en met name het cybersanctieregime, zijn echter relatief nieuw, en nog niet vaak genoeg ingezet om de doorwerking ervan te evalueren. Veelvuldig gebruik van het regime en diplomatieke responsopties in het algemeen zullen in de toekomst moeten uitwijzen wat het normerend effect van attributie en verschillende vormen van respons is, en in hoeverre dit van invloed is op de aanvallen van tegenstanders. Geïnterviewden zien het huidige EU-instrumentarium dan ook niet als compleet, maar als een beginpunt dat nog verder uitgebouwd kan worden.[110]

Diplomatieke inzet ter bevordering van de internationale rechtsorde

Nederland profileert zich in diplomatiek opzicht

Nederland bokst internationaal boven zijn gewicht in de cyberdiplomatie en capaciteitsopbouw, en profileert zich in diplomatiek opzicht nadrukkelijk.[111] Dat geldt voor zowel de VN-discussies, als voor de Nederlandse inbreng in EU- en OVSE-verband. Uit interviews, de survey en documentanalyse komt naar voren dat Nederland over het algemeen een constructieve inbreng heeft in deze multilaterale discussies, waaraan de BZ-diplomaten actief deelnemen en bovendien een duidelijk en over de tijd consistent geluid verkondigen.[112] Naast de eerder besproken bijdrage aan de EU *Cyber Diplomacy Toolbox* en het cybersanctieregime, heeft het Nederlandse kabinet als één van de weinige landen invulling gegeven aan de manier waarop het internationaal recht volgens hen van toepassing is op het cyberdomein, waarmee het de internationale discussies daaromtrent kan voeden.[113] Inhoudelijke voorbeelden van de positieve inzet zijn de standpunten op het gebied van mensenrechten die BZ internationaal gezien[bz] consistent ter tafel brengt;[114] de ingebrachte norm ter bescherming van de publieke kern van het internet[ca] die in maart 2021 en mei 2021 werden opgenomen in twee VN-consensusrapporten (zie tekstbox 4.1);[115] en de in dezelfde rapporten overgenomen norm tegen digitale aanvallen op gezondheidsinstellingen, waarover BZ aan het begin van de COVID-crisis harde noten kraakte[cb] in VN-verband.[116] Daarnaast wordt Nederland in OVSE-verband gewaardeerd voor zijn inzet voor vertrouwenwekkende maatregelen[cc] en de aangeboden hulp aan andere landen deze maatregelen te implementeren.[117]

[bx] Zie voor een publieke bron over de *Toolbox* en het cybersanctieregime: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/ en https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/.

[by] Bij dit dossier betrokken ambtenaren geven aan dat vertegenwoordigers van ministeries in EU-verband ten tijde van de totstandkoming niet altijd met één mond spraken. In hoofdstuk 2 behandelde samenwerkings- en afstemmingsproblemen en botsende belangen worden aangedragen als redenen voor deze issues.

[bz] Nationaal is er tussen ministeries wel enige onenigheid over de internationale positionering van Nederland op het gebied van mensenrechten online, zoals duidelijk wordt in de voortdurende discussie over het nationale standpunt encryptie (zie hoofdstuk 2).

[ca] De norm van de publieke kern van het internet stamt uit het gelijknamige 2015 WRR-rapport, en is de gedachte dat "de centrale protocollen en infrastructuren van het internet als een mondiaal publiek goed beschouwd moeten worden" en dat deze publieke goederen "gevrijwaard [moet] blijven van oneigenlijke interventies van staten en andere partijen die schade toebrengen en het vertrouwen in het internet eroderen." (Synopsis van het WRR-rapport, De publieke kern van het internet (2015), p. 7).

[cb] Daar werd destijds in een blog van het Amerikaanse Council on Foreign Relations aandacht aan besteed (EN): https://www.cfr.org/blog/amid-covid-related-cyber-threats-netherlands-leads-un-efforts.

[cc] Vertrouwenwekkende maatregelen faciliteren directe communicatie en informatie-uitwisseling tussen staten en beogen de risico's op cyberconflict te verminderen. Voor meer informatie hierover, zie (EN): https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/.

Botsende visies

De positieve inzet van Nederland ten spijt, de realiteit is dat er een situatie van permanente spanning in het mondiale cyberdomein is ontstaan, waarbij het cyberdomein een belangrijke arena is geworden voor het aangaan van geopolitieke confrontaties.[118] Geïnterviewden wijzen er op dat cyberoperaties door verschillende landen – Nederland volgens sommigen incluis[119] – de bereidheid te komen tot mondiale afspraken over gedragsregels en normen in het cyberdomein compliceren.[120] Aangezien de hoeveelheid en ernst van cyberoperaties door kwaadwillende staten of daaraan gelieerde actoren blijft toenemen (zoals besproken in hoofdstuk 1), is de multilaterale dialoog een lastig gesprek geworden.[121] Vooral de tweedeling tussen overwegend westerse landen (waaronder Nederland) die over het algemeen een mondiaal open, vrij en veilig internet nastreven en landen – zoals Rusland en China – die nationale internetsoevereiniteit bij de inrichting van het internet vooropstellen,[cd] zorgt voor frictie.[122] De kampen hebben conflicterende meningen over met name de toepasbaarheid van het internationaal recht in het digitale domein en de status van internationale normen voor (on)gewenst gedrag in het cyberdomein. Bovendien liggen de visies ver uit elkaar over de vraag op welke manier mensenrechten als vrijheid van meningsuiting, vrijheid van vergadering en bescherming van privacy ook online gelden.[123] Recente ontwikkelingen confronteren Nederland met prangende vraagstukken en strategische dilemma's, onder meer op het gebied van de wenselijkheid van een bindend internationaal cyberverdrag, de scherpe tegenstellingen in multilaterale fora als de VN en ITU, de mondiale strijd om de stem van opkomende cybermachten en de rol van capaciteitsopbouw en bilaterale dialoog daarbij. Deze vraagstukken worden in de volgende paragrafen uiteengezet.

Geen bindend cyberverdrag

Een groep landen die nationale internetsoevereiniteit nastreeft,[ce] beargumenteert dat het bestaand internationaal recht niet goed toepasbaar is op het cyberdomein en streeft daarom naar nieuwe, bindende rechts- en gedragsregels – bij voorkeur in de vorm van een nieuw cyberverdrag.[124] Behalve landen mengen ook grote bedrijven zich in het debat.[125] Zo deden zowel Microsoft als Siemens voorstellen om te komen tot nieuwe bindende internationale afspraken, waarbij het voorstel van Microsoft met name opviel doordat deze oproep ook aan staten gericht was. [cf][126] De facto verschilt hun kritiek op de toepasbaarheid van het bestaand internationaal recht in het cyberdomein – en de oproep voor nieuwe bindende regels in het cyberdomein – niet veel van datgene waar de Russen en Chinezen zich voor inzetten.[127]

Volgens de Nederlandse lezing zouden door een dergelijk cyberverdrag, met daarin de waarborging van nationale internetsoevereiniteit, vrijheden op het internet beknot kunnen worden en mensenrechten online verder onder druk komen te staan.[128] Nederland en de coalitie van gelijkgestemden zijn daarnaast huiverig toe te geven aan het openen van verdragsonderhandelingen, aangezien het momentum niet in het voordeel van de open, vrije en veilige visie van het internet is.[129] De coalitie zet zich in plaats daarvan in voor het uitleggen van de toepasbaarheid van internationaal recht in het cyberdomein en het implementeren van eerder gemaakte normafspraken.[130] Nederland probeert derhalve andere landen te laten kennismaken met hoe het huidige pakket aan rechts- en gedragsregels wél werkt en ze ervan te overtuigen dat nieuwe bindende regels onnodig zijn[cg] – om zo weg te blijven van ongewenste onderhandelingen over een nieuw cyberverdrag.

[cd] Internetsoevereiniteit is een term die werd geïntroduceerd door de Chinese overheid. Het behelst het recht op complete controle over het cyberdomein binnen staatsgrenzen (literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8). Volgens de lezing van Nederland en gelijkgestemde landen leidt dit in de praktijk tot onder meer de inperking van internetvrijheden en een 'splinternet' – zie hoofdstuk 1.

[ce] Naast Rusland en China worden in ieder geval Cuba, Iran, Nicaragua, Syrië, Venezuela en Zimbabwe tot deze groep landen gerekend.

[cf] Zie voor de openbaar verschenen tekst van de Digital Geneva Convention (EN): *https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/*.

[cg] Nederland zet in multi- en bilateraal verband breed in op het uitleggen van de toepasbaarheid van het internationaal recht. Onder meer bilaterale cyberdialogen, projecten in het kader van capaciteitsopbouw en de implementatie van vertrouwenwekkende maatregelen in OVSE-verband worden hiervoor gebruikt.

Scherpe tegenstellingen in VN-processen

De VN biedt een belangrijk podium voor de multilaterale dialoog over internationaal recht en de status van normen in het cyberdomein. Sinds 2015 is er echter weinig vooruitgang geboekt in VN-verband.[ch][131] In 2015 besloot de VN *Group of Governmental Experts* (GGE), een groep cyberexperts uit twintig VN-landen, dat het internationaal recht toepasbaar is op het cyberdomein en werd er een pakket van elf niet-bindende gedragsnormen aangenomen. In de daaropvolgende sessie,[ci] die eindigde in 2017, kon de GGE voor het eerst niet tot een consensusrapport komen en werd het proces van deze groep als mislukt beschouwd.[132] Sindsdien lijken de standpunten van deelnemende landen eerder verder uit- dan dichter bij elkaar komen te liggen.[133] Geboren uit kritiek op de exclusiviteit van de GGE,[cj] is op Russisch initiatief sinds 2018 de VN *Open-Ended Working Group* (OEWG) actief.[ck] Hierdoor hebben meer landen, inclusief de *swing states*, invloed verworven in de discussies over internationale normen voor gewenst gedrag in het cyberdomein en zijn er binnen de VN twee parallel lopende processen actief. De GGE en OEWG houden elkaar in een greep, waardoor het bereiken van consensus tot recentelijk onwaarschijnlijk werd geacht.[134]

Aanvankelijk was de Russische oproep voor de OEWG dan ook tegen het zere been van de VS en andere gelijkgestemde landen, en stemde Nederland tegen de totstandkoming van deze OEWG – mede uit vrees voor onderhandelingen voor een cyberverdrag.[135] Nederland en gelijkgestemde landen opteren bovendien voor een VN-agenda die zich richt op implementatie in plaats van discussie, waarin de afspraak uit 2015 dat het internationaal recht toepasbaar is op het cyberdomein als startpunt wordt genomen en het pakket van elf niet-bindende gedragsnormen zou worden geïmplementeerd.[136] Daarnaast zou de focus volgens hen moeten liggen op het formuleren van antwoorden op vragen hoe het internationaal recht van toepassing is. Hoewel de inwerkingtreding van de OEWG volgens Nederlandse betrokkenen onwenselijk was,[137] nam Nederland samen met gelijkgestemde landen wel zitting in de OEWG en probeerde er een succes van te maken – hopende dat de OEWG zou kunnen worden afgesloten en opgevolgd met een proces dat zich zou richten op de implementatie van gedragsnormen.[138] Eind november 2020 stemde de Eerste Commissie van de Algemene Vergadering van de VN (AVVN) echter voor een door Rusland ingediende resolutie ter voortzetting van de OEWG voor een periode van vijf jaar vanaf medio-2021 – wederom een onwenselijke ontwikkeling voor Nederland en gelijkgestemde landen. Bovendien is de bij de eerste OEWG opgenomen voorwaarde dat het proces met een consensus diende te worden besloten, door inzet van Rusland komen te vervallen en vervangen door een meerderheidsstemming.[139] Het reële risico is, mede door het invoeren van meerderheidsstemmingen, dat in deze nieuwe OEWG onderhandeld gaat worden over een cyberverdrag.

Tot veler verrassing kwam de eerste OEWG in maart 2021 tot een consensusrapport (zie tekstbox 4.1), met als winst voor Nederland dat het rapport de afspraken uit 2015 over de toepasbaarheid van het internationaal recht op het cyberdomein herbevestigt – nu onderschreven door alle VN-lidstaten.[cl] Vervolgens bereikte eind mei 2021 ook de VN GGE (2019-2021) consensus (zie ook tekstbox 4,1), waarin onder andere inhoudelijke richtlijnen zijn toegevoegd aan de reeds bestaande gedragsnormen.[cm]

[ch] Voor een openbare beschouwing hierover, luister bijvoorbeeld naar de Podcast 'Cyberhelden' van Ronald Prins, aflevering 4, met Sico van der Meer (28 januari 2021), beschikbaar via https://www.cyberhelden.nl/episodes/episode-4/.

[ci] Er zijn in totaal zes GGEs (geweest): in 2004/2005 (A/RES/58/32), 2009/2010 (A/RES/60/45), 2012/2013 (A/RES/66/24), 2014/2015 (A/RES/68/243), 2016/2017 (A/RES/70/237), en de huidige GGE, in 2019/2021 (A/RES/73/266).

[cj] Aan de GGE neemt een select aantal cyberexperts uit verschillende landen deel. Van 2019-2021 namen experts uit 25 landen deel.

[ck] In de OEWG zijn alle VN-lidstaten uitgenodigd om mee te doen. Zie voor de oprichting van de eerste OEWG de AVVN resolutie 73/27 uit 2018.

[cl] Het rapport is openbaar beschikbaar en te openen via de VN-website (EN): https://www.un.org/disarmament/open-ended-working-group/.

[cm] Op het moment van schrijven is het door de 25 experts overeengekomen consensusrapport net uit, en is enkel een *advance copy* beschikbaar (EN): https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

Tekstbox 4.1: Consensusrapporten OEWG en GGE

Open-Ended Working Group

In maart 2021 concludeerde de OEWG met een consensusrapport waaraan alle 193 VN-lidstaten konden bijdragen. Nederland zette zich samen met gelijkgestemde landen in voor het herbevestigen van de in 2015 in VN GGE-verband gemaakte afspraken over de toepasbaarheid van het internationaal recht op het cyberdomein – en zag die inzet uiteindelijk gereflecteerd worden in het consensusrapport. De voor Nederlandse vertegenwoordigers[cn] gewenste vooruitgang werd geboekt met de verwijzing naar het VN-Handvest voor vreedzame geschillenbeslechting en met de opname van de bescherming van de publieke kern van het internet, gezondheidsinstellingen en electorale processen als aanvullende richtlijnen voor gedragsnormen.[140] De herbevestiging van in 2015 gemaakte afspraken door alle VN-lidstaten en de opname van aanvullende richtlijnen voor gedragsnormen bieden voor Nederland welkome handvatten om op te kunnen treden bij normoverschrijdend gedrag van staten en aan staten gelieerde actoren in het cyberdomein.[141]

Commentatoren[co] en betrokkenen[142] plaatsen echter ook kritische noten bij het consensusrapport. Het herbevestigen van afspraken die zes jaar daarvoor zijn gemaakt, lijkt immers meer een stap zijwaarts dan een stap vooruit, temeer omdat een belangrijk vraagstuk – namelijk de manier waarop het internationaal recht van toepassing is in het cyberdomein – onvoldoende wordt beantwoord.[143] De tegenstellingen tussen landen waren te scherp om vooruitgang te boeken op de toepasbaarheid van het internationaal recht. Daarnaast verwijst het rapport nauwelijks naar mensenrechten en de online toepasbaarheid daarvan – wat voor Nederland een belangrijk onderdeel van de inzet was. De vermelding van een juridisch-bindend instrument, in de laatste paragraaf van het rapport, geeft bovendien een voor Nederland ongewenste hint naar het cyberverdrag waar de nieuwe OEWG – zeker als het aan Rusland en China ligt – voor een deel over zal gaan.

Group of Governmental Experts

Het consensusrapport waarmee de GGE in mei 2021 concludeerde, biedt vergeleken met het OEWG-rapport en in lijn met de Nederlandse inzet meer inhoudelijke passages over de toepasbaarheid van het internationaal recht in het cyberdomein[cp] en richtlijnen met meer uitleg over de niet-bindende gedragsnormen.[144] Daarnaast worden staten in het GGE-rapport uitgenodigd hun nationale posities over het internationaal recht in het cyberdomein uiteen te zetten en publiekelijk beschikbaar te maken,[145] wat het Nederlandse kabinet al in 2019 deed[cq] en waar bijvoorbeeld het VK in juni 2021 gehoor aan gaf.[cr] De inzet die Nederland en gelijkgestemde landen al dan niet gereflecteerd zagen in het consensusrapport loopt verder qua inhoud redelijk langs de lijnen van het zojuist behandelde OEWG-rapport.[146]

Blik vooruit

De impact van beide rapporten op het internationale cyberdomein is nog ongewis. Dat heeft mede te maken met verschillen in de totstandkoming en inhoud van de rapporten. Kortgezegd is een belangrijk verschil tussen beide rapporten dat het OEWG-rapport tot stand kwam na onderhandelingen waaraan alle VN-lidstaten mochten deelnemen, waardoor het draagvlak breed is maar de inhoud enigszins oppervlakkig blijft. Het GGE-rapport daarentegen gaat wel meer in op de toepasbaarheid van

[cn] De namens BZ bij dit proces betrokken medewerkers schreven erover in de Veiligheidsdiplomaat: https://magazines.rijksoverheid.nl/bz/veiligheidsdiplomaat/2021/02/02.

[co] Zie bijvoorbeeld voor opbouwende kritiek het World Politics Review-artikel van Emily Taylor, 'A Breakthrough for UN Governance of Cyberspace' (2021), beschikbaar via: https://www.worldpoliticsreview.com/articles/29496/a-breakthrough-for-global-cyber-governance, en de stevigere kritiek die op Twitter werd geuit door Stefan Soesanto (@iiyonite) van het Center for Strategic Studies (CSS) en door prof. Jack Goldsmith (@jacklgoldsmith) van Harvard Law School.

[cp] Zo wordt voor het eerst bevestigd dat het Internationaal Humanitair Recht (IHL) van toepassing is op cyberoperaties tijdens een gewapend conflict, zie (EN): Michael Schmitt, 'The sixth United Nations GGE and international law in cyberspace' (2021), beschikbaar via: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

[cq] De standpunten van het Nederlandse kabinet over de toepasbaarheid van het internationaal recht op het cyberdomein zijn beschikbaar via: https://zoek.officielebekendmakingen.nl/kst-33694-47.html.

[cr] Het *policy paper* uit naam van de Britse regering is online openbaar beschikbaar (EN): https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

internationaal recht en manieren waarop gedragsnormen geïmplementeerd kunnen worden, maar is tot stand gekomen op basis van discussies tussen experts uit 25 VN-lidstaten. De doorwerking van het GGE-rapport op het internationale cyberdomein kan dus pas worden bezien wanneer er meer duidelijkheid is over de ontvangst van de inhoud van het rapport bij overige VN-lidstaten en de manieren waarop het rapport al dan niet naar de praktijk vertaald gaat worden.[147]

De komende tijd moet blijken op welke manier VN-lidstaten bereid en in staat zijn erop door te pakken.[148] De hoop van Nederland en gelijkgestemde landen richt zich op het Programme of Action (PoA), een VN-voorstel van Egypte en Frankrijk, om de overeengekomen afspraken en normen uit de consensusrapporten te implementeren.[149] Of en op welke manier het PoA uiteindelijk wordt vormgegeven, is op moment van schrijven nog ongewis. Het al dan niet doorgaan van het PoA is voor Nederland en gelijkgestemde landen belangrijk, omdat het zonder PoA lastig lijkt de beide consensusrapporten te implementeren. De verwachting die uit interviews, de documentanalyse en de literatuurstudie naar voren komt, is hoe dan ook dat de mondiale tegenstellingen hun weerslag zullen blijven hebben op de discussies over cybersecurity in de VN.[150]

Uitwijken naar andere VN-fora

Mede vanwege de scherpe tegenstellingen en de patstelling van de afgelopen jaren is de tendens ontstaan dat er regelmatig uitgeweken wordt naar andere VN-fora, waarin de coalitie van landen rondom Rusland en China momenteel nationale belangen probeert te behartigen.[151]

- Met name Rusland tracht in de Derde Commissie van de AVVN, die onder andere de bestrijding van cybercriminaliteit bediscussieert, te komen tot een nieuw mondiaal cybercrimeverdrag dat de reeds bestaande Budapest Conventie[cs] kan ondermijnen. Dat wordt door Nederlandse betrokkenen beschouwd als een tactiek om de impasse in de andere twee VN-fora te doorbreken en toe te werken naar bindende rechtsregels waarbij de waarborging van mensenrechten uit de Budapest Conventie wordt afgezwakt, en de nationale internetsoevereiniteit binnen het thema cybercriminaliteit wordt verstevigd.[152]
- China heeft door de jaren heen een sterke positie verworven in onder andere de International Telecommunications Union (ITU),[ct] waardoor het grote invloed heeft op de standaarden die afgesproken worden rondom het gebruik van nieuwe technologieën.[153] Dit is belangrijk omdat dergelijke standaarden van invloed zijn op voor de publieke en private sector toegestane en verboden toepassingen van (nieuwe) technologieën. De grote invloed van China op internationale discussies over standaardenregimes levert het land derhalve zowel politieke als economische voordelen op, omdat zij hierdoor de kans krijgen hun nationale belangen over te laten nemen in mondiaal geldende standaarden.[cu] Hierbij treedt er een mogelijk negatieve doorwerking van technologie op mensenrechten op.[154]

[cs] De Budapest Conventie stelt internationale standaarden voor de omgang met cybercriminaliteit en elektronisch bewijs. Op moment van schrijven zijn 65 landen lid van de conventie, waaronder Nederland. Voor een volledige lijst, zie (EN): https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[ct] De International Telecommunications Union is een in 1865 opgerichte VN-organisatie die gespecialiseerd is in Informatie en Communicatie Technologie (ICT) en als doel heeft mensen op de wereld te verbinden. Cybersecurity, nieuwe technologieën en de inrichting van het internet vallen allemaal onder het mandaat van de ITU. Zie ook hun website (EN): https://www.itu.int/en/about/Pages/default.aspx.

[cu] Lees voor een openbare bron over de Chinese motieven voor het winnen van invloed in standaardendiscussies (“those who set the standards win the world”) het rapport van Rush Doshi voor Brookings (EN): https://www.brookings.edu/research/china-as-a-cyber-great-power-beijings-two-voices-in-telecommunications/.

BZ laat blijken deze ontwikkelingen inmiddels op het netvlies te hebben,[155] maar geïnterviewden uiten kritiek op dat BZ pas laat aansloot bij deze overleggen. Ze wijzen erop dat op enkele cruciale momenten de gewenste (geo)politieke antenne van BZ ontbrak, waardoor het Nederlandse kabinet in eerste instantie de toenemende politisering van cybercrime- en standaardenfora gemist lijkt te hebben.[156] Zowel discussies in de Derde Commissie over cybercriminaliteit als de technische fora waarin standaarden voor nieuwe technologieën worden afgesproken, zijn dus voor langere tijd niet goed belegd geweest binnen de Nederlandse overheid en ook anno 2021 verloopt de interdepartementale coördinatie en afstemming soms moeizaam.[157] De in hoofdstuk 2 besproken departementale verkokering en daardoor stroef lopende samenwerking is hier een belangrijke oorzaak van. Daarnaast hebben tekorten aan strategie, strategische reflectie en het vermogen om tijdig na te denken over de inzet bij nieuwe thema's binnen BZ (zie hoofdstuk 3), deels voortkomend uit een breder spelend capaciteitsgebrek (zie hoofdstuk 5), bijgedragen aan de te geringe betrokkenheid van BZ bij deze belangrijke thema's.[158]

Toenemend belang opkomende cybermachten

Een volgend strategisch vraagstuk gaat over de houdbaarheid van de inzet van Nederland en gelijkgestemde landen in VN-verband, nu een grote groep *swing states* door hun toetreding tot de OEWG een doorslaggevende stem hebben verworven in VN-onderhandelingen.[159] Waar Nederland en gelijkgestemde landen zich inzetten om onderhandelingen over een nieuw cyberverdrag en een verdere beknotting van het internet te voorkomen, zijn niet alle *swing states* daarvan overtuigd. Voor veel van deze landen geldt dat zij amper inspraak hadden in de voor 2018 afgesproken normen en leidraden over de toepasbaarheid van het internationaal recht, waardoor deze landen – bijvoorbeeld Zuid-Afrika, India en Indonesië – open lijken te staan voor gesprekken over nieuwe, bindende regels in het cyberdomein.[160] De argumentatielijn om tot een radicalere oplossing te komen voor de problemen binnen het cyberdomein is voor velen beter uit te leggen dan het narratief van Nederland en gelijkgestemde landen – die zich inzetten voor het behoud van de status quo.[161] Hierdoor ziet een aantal *swing states* hun voorkeur voor een multilaterale dialoog over juridisch-bindende gedragsregels momenteel beter vertegenwoordigd binnen het Rusland-China kamp.[162] Hoewel de processen aan snelle veranderingen onderhevig zijn en de toekomst moeilijk te voorspellen valt, is al wel bekend dat de nieuwe OEWG een looptijd heeft tot en met 2025. Lukt het Nederland en gelijkgestemde landen wellicht met een meer positieve agenda de *swing states* bij hun invloedsfeer te betrekken? In hoeverre zijn Nederland en gelijkgestemde landen bereid concessies te doen aan *swing states* en zijn zij bijvoorbeeld bereid mee te doen aan discussies over nieuwe gedragsnormen en bindende gedragsregels? Volgens experts en betrokkenen hebben Nederland en gelijkgestemde landen bij behoud van de huidige inzet in ieder geval een meer solide verhaal nodig om hun blijvende afwijzing van juridisch-bindende regels te ondersteunen.[163]

Capaciteitsopbouw

De strijd om het winnende narratief

Naast activiteiten voor de diplomatieke respons bij cyberaanvallen en inzet in diplomatieke fora over internationaal recht in het cyberdomein, is capaciteitsopbouw één van de belangrijke activiteiten voor de TFC. 'Capaciteitsopbouw' betekent hier het verstrekken van financiële en andere ondersteuning voor het helpen opbouwen van aan cybersecurity gerelateerde capaciteiten van derde landen. Zo richtte Nederland tijdens de Global Conference on Cyber Space (GCCS) in Den Haag in 2015 het GFCE[cv] op, dat sindsdien als multistakeholderforum internationale kennisdeling over capaciteitsopbouw faciliteert. Daarnaast financiert BZ cursussen over de toepassing van het internationaal recht in het cyberdomein, die wereldwijd worden uitgevoerd door Cyber Law International. De TFC ondersteunt ook activiteiten om mensenrechten online wereldwijd te bevorderen, zoals via projecten van Access Now, HIVOS[cw] en het Global Network Initiative (GNI). Onder meer via de Freedom Online Coalition (FOC)[cx] voert Global Partners Digital (GPD) activiteiten uit ter bevordering van een open, vrij en veilig internet met een focus op inclusievere (online) samenlevingen.[164]

[cv] Het GFCE is een initiatief van BZ en opereert sinds 2020 als onafhankelijk stichting. Het is een multistakeholder- en kennisplatform met een divers ledenbestand van landen, organisaties en bedrijven. Zie ook hun website: https://thegfce.org/about-the-gfce/.

[cw] Voluit het Humanistisch Instituut voor Ontwikkelingssamenwerking.

[cx] Nederland is één van de initiatiefnemers van de Freedom Online Coalition (FOC), die in 2011 werd opgericht en focust op een open en vrij internet. Momenteel zijn 32 landen lid van de FOC.

Zoals in hoofdstuk 3 besproken, worden in verschillende beleidsdocumenten en door verschillende respondenten uiteenlopende motieven genoemd voor cybercapaciteitsopbouw. Voor sommigen is capaciteitsopbouw een vorm van ontwikkelingssamenwerking, die misschien niet onder het internationaal cybersecuritybeleid bij de TFC – binnen de Directie Veiligheidsbeleid (DBV) – hoort te vallen.[165] Volgens sommige beleidsstukken[166] en geïnterviewden is de nationale veiligheid echter een belangrijk motief voor capaciteitsopbouw, wat verklaart dat de TFC zich bezighoudt met capaciteitsopbouw.[167] Desondanks is de directe link tussen de nationale veiligheid en capaciteitsopbouw in derde landen volgens technisch experts te ver gezocht: het bestaan van een mondiale cybersecurityketen die zo 'zwak is als de zwakste schakel' die moet worden versterkt in het belang van de nationale veiligheid (zie hoofdstuk 3), wordt vanuit een technisch oogpunt in twijfel getrokken.

Uit de analyse blijkt dat de inzet voor capaciteitsopbouw in de praktijk voor een groot deel gericht is op het vergroten van de Nederlandse invloedsfeer ten behoeve van multilaterale processen – en dan met name in VN-verband; het doel de internationale rechtsorde te bevorderen en de coalitie voor een open, vrij en veilig internet te verbreden.[168] Derhalve kan capaciteitsopbouw worden beschouwd als een strategisch middel, dat tezamen met de bilaterale dialoog door Nederland kan worden ingezet *swing states* te overtuigen van onder andere de toepasbaarheid van het internationaal recht en de implementatie van normen en vertrouwenwekkende maatregelen. Capaciteitsopbouw biedt dus kansen om de coalitie van gelijkgestemde landen uit te breiden.[169] Dit motief voor capaciteitsopbouw wordt weliswaar weinig benadrukt in belangrijke beleidsdocumenten zoals de NCSA, maar uit de documentanalyse en interviews wordt duidelijk dat onderliggende, strategische motieven steeds meer doorwerken in de inzet van de TFC voor capaciteitsopbouw. De TFC maakt bijvoorbeeld sinds kort gebruik van stemmingsuitslagen in VN-verband en eventuele lidmaatschappen bij andere internationale organisaties voor cybersecurityzaken van VN-lidstaten, om zo de focuslanden en inzet te bepalen.[170] Zo verzorgde CLI recentelijk cursussen aan diplomaten uit landen in Zuidoost-Azië, wat gerelateerd is aan een bredere inzet van Nederland en gelijkgestemde landen, zoals Australië en de VS, om tegenwicht te bieden aan de sterke invloed van China in de regio.[171]

Geïnterviewden wijzen er desalniettemin op dat de TFC in de afgelopen jaren nog te weinig heeft uitgedacht hoe het capaciteitsopbouwactiviteiten en de keuze voor uitvoeringsorganisaties in lijn kan brengen met dit strategisch motief.[172] Zo kan capaciteitsopbouw nog beter worden gekoppeld aan bilaterale inzet en een mogelijke inbreng van het postennet hierbij, en kan capaciteitsopbouw qua activiteiten en budget nog beter worden gekoppeld aan hetgeen andere ministeries en directies binnen BZ ondernemen – die zich vanuit hulp en handel bezighouden met digitalisering in andere landen.[173] Daarnaast zou Nederland zich nog meer kunnen richten op het in gezamenlijkheid optrekken met gelijkgestemde landen, zoals dit al deels gebeurt in EU- en OVSE-verband, om zo een sterkere coalitie te vormen waarin bestaande verschillen tussen landen in aanpak en boodschap worden opgelost.[174] Er moet immers opgebokst worden tegen een grootmacht als China – dat met de *Digital Silk Road* (DSR) een langetermijnstrategie met veel financiële middelen[cy] ter beschikking heeft voor lageinkomenslanden met groeiende cybercapaciteiten.[175] Hierdoor lijken Nederland en gelijkgestemde landen de strijd in deze landen te verliezen en ontstaat het risico dat de focuslanden van China's DSR een op Chinese normen en waarden gestoeld traject van digitalisering doorlopen.[cz] Een consequentie daarvan kan zijn dat deze landen hun nationale belangen beter vertegenwoordigd zien in de inzet voor meer internetsoevereiniteit van China en Rusland. Dit zal waarschijnlijk het stemgedrag van deze landen in de OEWG beïnvloeden, en kan daarmee negatief doorwerken op de manier waarop bijvoorbeeld mensenrechten online gewaarborgd worden.

[cy] Binnen het Chinese Belt & Road Initiative, met een totale waarde van circa USD 1 biljoen, wordt geschat dat de DSR tot in 2019 ongeveer USD 79 miljard had bijgedragen aan digitale ontwikkeling en capaciteitsopbouwprojecten over de hele wereld. Zie voor de schattingen het rapport (2018) van de Organisatie voor Economische ontwikkeling en Samenwerking (OECD), te downloaden via hun website (EN): *https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf,* en het Bloomberg-artikel (EN): *https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain.*

[cz] De literatuurstudie deelt deze bevinding en voorziet in aanbevelingen om de effectiviteit van capaciteitsopbouwactiviteiten te verbeteren, zie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 81, 83-87.

Conclusie/Aanbevelingen

In hoofdstuk 2 en 3 is gepleit voor een nieuwe interdepartementale cybersecuritystrategie, met als onderdeel ervan of aanvulling erop een internationale cybersecuritystrategie en meer strategische reflectie. Dit hoofdstuk werpt een aantal belangrijke strategische dilemma's en vraagstukken op.

Voor het ministerie van Buitenlandse Zaken:

Geef in een nieuwe internationale cybersecuritystrategie in ieder geval invulling aan de volgende vragen:

- Welke langetermijnvisie formuleert het Nederlandse kabinet als reactie op de toenemende cyberdreigingen, scherpe mondiale tegenstellingen en de wensen van *swing states* met ontwikkelende cybercapaciteiten? Wat betekent deze langetermijnvisie voor de Nederlandse inzet in de voortkomende VN-processen, zoals de nieuwe OEWG en het PoA?
- Op welke manier kan Nederland, al dan niet in coalitieverband, de in recente OEWG- en GGE-consensusrapporten overeengekomen gedragsnormen het beste inzetten voor attributie en diplomatieke respons bij normoverschrijdend gedrag van andere staten in het cyberdomein?
- Op welke manier kan het Nederlandse kabinet de invloed van Nederland en gelijkgestemde landen vergroten in multilaterale discussies omtrent de omgang met nieuwe technologieën en cybercriminaliteit? En op welke manier waarborgt het kabinet dat het toekomstige belangrijke discussies over nieuwe thema's binnen het cyberdomein zoveel mogelijk vanaf het begin en op de juiste manier aanvliegt?
- Wat is het hoofddoel achter de inzet voor capaciteitsopbouw? Als het hoofddoel inderdaad coalitievorming ten behoeve van de multilaterale onderhandelingen over internationaal recht in het cyberdomein is, op welke manier kunnen de projecten en keuzes voor uitvoeringsorganisaties dan zo goed mogelijk aansluiten op dit soort strategische doelen?

5 Organisatorische opzet

Bij het ministerie van Buitenlandse Zaken (BZ) is met name de Taskforce Cyber (TFC) verantwoordelijk voor het internationaal cybersecuritybeleid. De TFC valt onder de Directie Veiligheidsbeleid (DVB) en is sinds de oprichting in 2015 in omvang gegroeid – in de zomer van 2020 met een laatste uitbreiding van twee extra fte.[da] Op dit moment werkt de TFC met 11,5 fte,[176] inclusief 0,5 fte van de Directie Multilaterale Instellingen en Mensenrechten (DMM) en één fte van de Directie Juridische Zaken (DJZ). Daarnaast is een Ambassadeur in Algemene Dienst voor veiligheidsbeleid en cyber (AMAD) betrokken bij het werk van de TFC.

De TFC stuurt ook een netwerk aan van 'cyberdiplomaten' en 'cyberaanspreekpunten'.[db] Dit netwerk startte in 2019 vanuit de wens op bepaalde Nederlandse posten een cyberdiplomaat te hebben en is nog in ontwikkeling (zie tekstbox 5.1).

De TFC is binnen het departement niet de enige die zich met cybersecuritybeleid en daaraan gerelateerde onderwerpen bezighoudt (zie hoofdstuk 3). Relevante directies en (mogelijke) samenwerkingspartners zijn naast DMM en DJZ het Bureau Internationale Samenwerking (BIS), de Directie Integratie Europa (DIE), de Directie Sociale Ontwikkeling (DSO) en de Directie Internationale Marktordening en Handelspolitiek (IMH). De TFC is niet verantwoordelijk voor de cybersecurityhuishouding van het ministerie; dat is met name belegd bij de Security-afdeling van de Directie Bedrijfsvoering (DBV-Security).

Naast samenwerkingspartners binnen BZ heeft de TFC ook veel externe samenwerkingspartners, waaronder andere ministeries (zie hoofdstuk 2) en een brede groep andere stakeholders, zoals bedrijven, kennisinstellingen en maatschappelijke organisaties.[dc]

Positief beeld

Over het algemeen is in deze evaluatie een positief beeld ontstaan over het werk van de TFC. Dit wordt mede bevestigd door een aantal samenwerkingspartners die zich positief uitlaten over de inzet van de TFC en het gewicht dat de TFC internationaal in de schaal weet te leggen.[177] Onder meer vanwege de inhoudelijke focus en overtuigingskracht is de TFC volgens geïnterviewden in staat een herkenbaar geluid in internationale fora te laten horen (zie hoofdstuk 4). De deskundigheid die de TFC in huis heeft gehaald door middel van parttime ondersteuning van DMM en DJZ, wat kennis op het gebied van respectievelijk mensenrechten en internationaal recht toevoegt aan de TFC, wordt als een goede zet gezien. Hetzelfde geldt voor de samenwerking die de TFC opzoekt met kennisinstellingen en (semi-)private instellingen, zoals middels aanbestedingen bij de Universiteit Leiden en de Global Commission for Stability of Cyberspace (GCSC), die de kennis en deskundigheid van de TFC aanvullen.[178] De leden van de TFC worden bovendien beschouwd als gedegen en constructieve samenwerkingspartners – zowel door nationale als internationale partners – die veel werk weten te verzetten.[179]

[da] Sommige geïnterviewden geven aan niet goed te begrijpen waarom de TFC formeel nog een werkgroep heet, aangezien de TFC de afgelopen vijf jaar een onmisbare positie heeft ingenomen binnen het departement en grotendeels functioneert als een directie of afdeling. Om niet in een semantische discussie over naamgeving te vervallen, laat IOB dit vraagstuk buiten beschouwing.

[db] Op het moment van schrijven bestaan er zes posten die op de politieke afdeling een fulltime cyberdiplomaat hebben, te weten: Washington; Peking; Singapore; de Permanente Vertegenwoordiging Verenigde Naties New York; de Permanente Vertegenwoordiging Verenigde Naties en andere internationale organisaties Genève; en de Permanente Vertegenwoordiging EU Brussel/NAVO Brussel. Overige posten zijn gevraagd een aanspreekpunt voor cyberzaken aan te wijzen. Zij zijn, in tegenstelling tot cyberdiplomaten, niet fulltime met cybersecurity gerelateerde zaken bezig en werken, vaak binnen de politieke afdeling van ambassades, ook aan andere dossiers.

[dc] Doordat de overheid, het bedrijfsleven, maatschappelijke organisaties en kennisinstellingen allemaal een rol spelen in het digitaal veilig houden van Nederland, wordt voor het cybersecuritybeleid ook wel gesproken van een 'multistakeholder model'.

Capaciteitsgebrek

Niettemin kampt de TFC met een gebrek aan capaciteit.[180] Hoewel de TFC door de jaren heen in omvang is gegroeid, mede dankzij de in 2020 benutte aanvullende middelen voor cybersecurity,[181] loopt de stijging in menskracht onvoldoende synchroon met de toename in werkzaamheden.[182] Het tekort aan menskracht[dd] wordt door een brede groep geïnterviewden gezien als een belangrijk facet van het capaciteitsgebrek.[183] De werkdruk op de TFC is groot, en lijkt eerder toe- dan af te nemen.[184] In de afgelopen jaren heeft met name het veranderende dreigingsbeeld ervoor gezorgd dat TFC-leden meer tijd kwijt zijn aan responszaken, en dan voornamelijk aan interdepartementale en internationale afstemmingsprocessen.[185] Daarnaast vragen nieuwe thema's, zoals desinformatie, economische veiligheid en nieuwe technologieën aandacht en tijd van de TFC (zie ook hoofdstukken 3 en 4).

Hoewel de flexibele opzet van de TFC ruimte biedt mensen vrij te maken voor nieuwe, prangende thema's en cyberincidenten,[186] ontstaat er in zulke situaties personele krapte op andere thema's. De gevolgen hiervan zijn meerledig. Besluitvorming over het al dan niet oppakken van nieuwe thema's of activiteiten gebeurt te veel op basis van capaciteitsoverwegingen, in plaats van op basis van inhoudelijke gronden.[187] Belangrijke strategische discussies – over bijvoorbeeld de koers van het internationaal cybersecuritybeleid op de langere termijn, of op activiteitniveau over het strategischer inzetten van capaciteitsopbouw, cyberdiplomaten en bilaterale partnerschappen (zie hoofdstukken 3 en 4) – kunnen door permanente drukte onvoldoende worden gevoerd.[188] Zaken worden daardoor op de lange baan geschoven als ze niet direct belangrijk zijn. Daarnaast zijn volgens geïnterviewden de negatieve gevolgen van het gebrek aan capaciteit op organisatorisch niveau merkbaar. De TFC heeft te weinig tijd en capaciteit voor de optimalisering en gedegen aansturing van het netwerk van cyberdiplomaten en –aanspreekpunten (zie tekstbox 5.1).[189] Daarnaast is er te weinig tijd voor het benutten van de samenwerkingsverbanden met andere directies binnen BZ en andere betrokken departementen die bezig zijn met het onderwerp.[190]

Het door geïnterviewden geconstateerde tekort aan tijd en aandacht bij de TFC voor bepaalde belangrijke taken[191] lijkt echter niet enkel te verklaren door het gebrek aan menskracht. Geïnterviewden vertellen dat ook meespeelt dat er te weinig keuzes worden gemaakt om meer focus aan te brengen in het werk van de TFC. Dit wordt mede veroorzaakt door het gebrek aan up-to-date en eenduidige strategische doelstellingen, definities en kaders voor prioriteitstelling (zoals in hoofdstuk 3 besproken werd).[192] De TFC neemt deel aan veel initiatieven en activiteiten waarbij het belang van de deelname niet altijd duidelijk is.[193] Hier gaat in sommige gevallen capaciteit verloren die mogelijkerwijs beter besteed had kunnen worden. Mogelijk is er winst te behalen door in overleg met andere departementen en BZ-directies na te denken over het achterwege laten of herbeleggen van taken en verantwoordelijkheden – bijvoorbeeld naar het cyberdiplomatennetwerk (zie tekstbox 5.1).

[dd] Het probleem van te weinig menskracht komt mede door een - door geïnterviewden geïdentificeerd -algemeen tekort aan mensen en middelen voor aan cybersecurity gerelateerde zaken binnen de gehele overheid.

Tekstbox 5.1: Netwerk cyberdiplomaten en -aanspreekpunten

De meerwaarde van het netwerk cyberdiplomaten en –aanspreekpunten wordt door menig geïnterviewde binnen en buiten BZ erkend – terwijl het netwerk relatief nieuw en nog in opbouw is.[194] De meerwaarde zit hem momenteel voornamelijk in de lokale contacten met *counterparts*, aanwezigheid bij bijeenkomsten en de informatie die eruit voortkomt.[195] De door de COVID-19 pandemie ingestelde reisbeperkingen onderstrepen het belang van het diplomatieke postennet. Om bijvoorbeeld de meer gevoelige responszaken met andere landen af te stemmen, zijn de vooruitgeschoven diplomaten op de posten en bij de permanente vertegenwoordigingen (PVs) essentieel gebleken.[196] Dankzij de lokale contacten, aanwezigheid en informatiestroom kan de TFC zich beter voorbereiden op bijvoorbeeld multilaterale discussies, en beter geïnformeerde beslissingen nemen over mogelijke internationale responsopties bij incidenten. Naast de TFC , maken ook andere directies binnen BZ en andere departementen soms dankbaar gebruik van de cyberdiplomaten.[197]

Niettemin liggen er met meer tijd en aandacht vanuit de TFC mogelijkheden om de werking van het netwerk verder te verbeteren en er meer uit te halen. Hoewel de behoefte hieraan per diplomaat of aanspreekpunt verschilt, is er volgens geïnterviewden te weinig aansturing vanuit de TFC naar de posten en ontbreekt voor een deel van de cyberposten een strategisch plan.[198] Hierdoor is nog niet duidelijk gecommuniceerd wat er op de posten van de diplomaten en aanspreekpunten verwacht wordt, en heeft men in de TFC voor delen van het netwerk nog onvoldoende uitgedacht hoe ze er het maximale uit kunnen halen. Zowel vanuit Den Haag als tussen de cyberdiplomaten onderling is er volgens geïnterviewden te weinig contact en wordt nog niet zo vaak als zou kunnen relevante informatie gedeeld.[199]

In potentie zou het netwerk een deel van de oplossing kunnen zijn voor het capaciteitsprobleem bij de TFC, door bepaalde taken en verantwoordelijkheden naar hen te delegeren. De paradox wil nu dat, om die extra stap te maken, er juist meer tijdsinvesteringen nodig zijn, waardoor er de facto extra capaciteit van de TFC gevraagd wordt.

Verouderde middelen

Voor heel BZ geldt dat het werken vanuit huis gedurende de COVID-19 pandemie uitdagingen met zich meebrengt, onder meer in de vorm van goed werkende en veilige communicatiemiddelen. De TFC verwerkt daarbij regelmatig hoger gerubriceerde – waaronder staatsgeheime – informatie en is gezien de reisrestricties veelal aangewezen op digitale communicatie. Voor vertrouwelijke afstemmingsprocessen, met andere ministeries of andere landen, blijken de communicatiemiddelen die de TFC en de posten ter beschikking hebben gedateerd en niet veilig genoeg – of ontbreken ze in sommige gevallen volledig.[200] Zo zijn er voor de TFC relevante posten die niet over geschikte communicatiemiddelen beschikken om bepaalde documenten te ontvangen of versturen, wat er onder meer toe leidde dat belangrijke informatie land X wel op tijd bereikte, terwijl de informatie in land Y niet of pas na omzwervingen aankwam.

Verkrijgen en behouden van kennis

Een laatste, relatief vaak genoemde, organisatorische uitdaging voor BZ betreft het verkrijgen en behouden van de juiste kennis en expertise. Geïnterviewden wijzen erop dat specifieke kennis en expertise over cybersecurity binnen de hele Nederlandse overheid, en dus ook bij BZ, schaars is.[201] Voor BZ geldt dat cybersecurity een niche binnen het diplomatenambt is, waar specialistische kennis voor nodig is.[202] Dit staat enigszins haaks op het beleid dat de meeste Nederlandse diplomaten worden geworven als generalist. Hoewel sommige geïnterviewden beargumenteren dat diplomatieke kennis en ervaring belangrijker zijn in het werk voor de TFC dan technische kennis over cybersecurity,[203] geven met name mensen bij andere ministeries en mensen uit het veld aan dat het gemis aan meer technische expertise soms nadelig doorwerkt in de onderlinge communicatie.[204]

In lijn met het roulatiesysteem van BZ werken diplomaten en beleidsmedewerkers bovendien slechts enkele jaren voor de TFC en vertrekken ze vervolgens naar een andere directie of post – waarna in sommige gevallen de opgedane specifieke cyberkennis niet meer wordt benut. Het roulatiesysteem van BZ wordt door geïnterviewden dan ook als nadelig ervaren voor het behoud van kennis over cybersecurity en daaraan gerelateerde thema's.[205] Het gebrek aan kennis en expertise op het gebied van cybersecurity binnen BZ wordt ook veroorzaakt door de relatieve onbekendheid met het thema. Geïnterviewden geven aan dat het lastig is het belang van cybersecurity en het internationaal cybersecuritybeleid uit te leggen aan collega's binnen BZ, die er in hun dagelijkse werkzaamheden niet of nauwelijks mee bezig zijn.[206] In dat kader noemen geïnterviewden het feit dat BZ

regelmatig negatief in het nieuws komt over hun eigen informatiehuishouding en gebrek aan voldoende cybersecurity[de] zowel exemplarisch voor-, als een negatief uitvloeisel van het gebrek aan kennis en expertise op dit gebied.[207] Zoals in de Terms of Reference vermeld, heeft IOB geen onderzoek verricht naar de cybersecurityhuishouding van het ministerie.

Aanbevelingen

Voor de Taskforce Cyber:

Ga na op welke manier er scherper geprioriteerd kan worden in het werk van de TFC.

Grijp bij het prioriteren de nieuwe strategie (hoofdstuk 3) aan om duidelijk te maken bij welke activiteiten en op welke dossiers welke inzet van de TFC gerechtvaardigd is en welke activiteiten of dossiers – in overleg met andere departementen en directies binnen BZ – mogelijkerwijs beter elders belegd kunnen worden.

Echter, in het licht van de toenemende dreigingen en incidenten, de geopolitieke verharding, opkomende thema's en technologieën, strategische vraagstukken en de daaruit voortkomende (interdepartementale) uitdagingen, is scherpere prioritering alleen niet voldoende, en is het capaciteitsgebrek bij BZ (net als bij andere onderdelen van de Nederlandse overheid) op het gebied van cybersecuritybeleid zorgelijk. De TFC heeft de komende jaren meer capaciteit nodig om de toenemende werklast te kunnen dragen, waarbij het gebaat zou zijn bij een sterkere inrichting van het waarborgen van cyberkennis en –expertise binnen BZ.

Voor het ministerie van Buitenlandse Zaken:

Zorg ervoor dat BZ beschikt over voldoende capaciteit, kennis en communicatiemiddelen om invulling te geven aan belangrijke taken binnen het internationaal cybersecuritybeleid.[208] Denk hierbij aan drie zaken:

1. Zorg voor extra menskracht bij de TFC, zodat voldoende invulling kan worden gegeven aan de volgende belangrijke taken:
   - Responszaken, diplomatieke inzet en de aansturing van het cyberdiplomatennetwerk – waarbij de werklast de afgelopen jaren is toegenomen en waarschijnlijk zal blijven toenemen.
   - Interdepartementale samenwerking en strategische reflectie. Het samenwerken met andere departementen (zie hoofdstuk 2) en herformuleren van een duidelijke internationale cybersecuritystrategie (zie hoofdstuk 3) vraagt tijd, capaciteit en aandacht. Dit geldt ook voor de gewenste regelmatige strategische reflectie over de koers en inzet van het internationaal cybersecuritybeleid.
2. Denk na over manieren waarop kennis en expertise over aan cybersecurity gerelateerde onderwerpen bij BZ kan worden ingewonnen en behouden.
   - Beleidsmedewerkers die ervaring hebben met een aan cybersecurity gerelateerde onderwerp dienen gestimuleerd te worden binnen het roulatiesysteem door te schuiven naar een voor het thema relevante nieuwe rol. Hierbij kunnen de initiatieven van de Werkgroep Vervullen Vacatures ter verbetering van de in- en doorstroom bij BZ aangegrepen worden.
   - Haal actiever kennis van buiten het ministerie naar binnen. Hierbij kan worden voortgebouwd op de ervaringen met onder meer de Universiteit Leiden en Instituut Clingendael. De juiste kennis en expertise kan worden vastgelegd door cyberexperts te werven voor een rol bij BZ, maar gezien de krappe arbeidsmarkt (waar ook andere departementen hinder van ondervinden) dient ook onderzocht te worden op welke manier meer publiek-private samenwerking kennishiaten bij BZ kan oplossen.
3. Investeer in veilige en goed werkende communicatiemiddelen.
   - Naast een investering in menskracht en kennis, is het ook van belang dat BZ, de TFC en de voor hen relevante posten gaan beschikken over goed werkende en veilige communicatiemiddelen waarmee vertrouwelijke informatie (beter) gedeeld kan worden.

[de] Zoals bijvoorbeeld in de Volkskrant (2020): https://www.volkskrant.nl/nieuws-achtergrond/we-vertrouwen-elkaar-toch-hoe-buitenlandse-zaken-staatsgeheimen-al-jaren-niet-goed-beveiligt~b4b8c3b6/ of in het rapport van de Algemene Rekenkamer (2020): https://www.rekenkamer.nl/actueel/nieuws/2020/05/20/beveiliging-informatie-geen-prioriteit-bij-ministerie-van-buitenlandse-zaken.

Eindnoten

1 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
2 Cybersecurity Woordenboek van Cybersecurity Alliantie Nederland, beschikbaar via: https://www.cybersecurityalliantie.nl/documenten/publicaties/2019/09/30/cybersecurity-woordenboek.
3 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
4 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 50.
5 Cybersecurity Woordenboek van Cybersecurity Alliantie Nederland, beschikbaar via: https://www.cybersecurityalliantie.nl/documenten/publicaties/2019/09/30/cybersecurity-woordenboek.
6 Cybersecurity Woordenboek van Cybersecurity Alliantie Nederland en de informatiepagina van de Nationale Politie: https://www.politie.nl/onderwerpen/cybercrime.html.
7 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
8 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
9 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
10 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
11 Informatie via Expertisecentrum Europees Recht: https://ecer.minbuza.nl/-/een-eu-cybersanctieregime-stap-voor-meer-veiligheid-in-cyberspace.
12 Informatie via Lawfare (EN): https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior.
13 Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, 18 oktober 2019. Kamerstukken II 2019-2020, 30 821, nr. 91, p. 3.
14 Zoals uitgelegd op https://www.encyclo.nl/lokaal/10046.
15 Cybersecurity Woordenboek van Cybersecurity Alliantie Nederland.
16 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 20.
17 Cybersecurity Woordenboek van Cybersecurity Alliantie Nederland.
18 Gebaseerd op uitleg uit ProDemos 'Wat is internationaal recht?' (2015), beschikbaar via: https://reserveren.prodemos.nl/uploads/media_items/wat-is-internationaal-recht-1.original.pdf, en Rijksoverheid, 'Internationale rechtsorde', beschikbaar via: https://www.rijksoverheid.nl/onderwerpen/internationale-vrede-en-veiligheid/internationale-rechtsorde.
19 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
20 Cybersecurity Woordenboek van Cybersecurity Alliantie Nederland.
21 Cybersecurity Woordenboek van Cybersecurity Alliantie Nederland.
22 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
23 Synopsis van het WRR rapport 'De publieke kern van het internet' (2015), p. 7.
24 Cybersecurity Woordenboek van Cybersecurity Alliantie Nederland.
25 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
26 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 6-8.
27 Gebaseerd op de definitie van Maurer en Morgus, 'Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate' (2014), p. 6.
28 Nederlandse Cybersecurity Agenda (NCSA), 20 april 2018. Kamerstukken II 2017-2018, 26 643, nr. 536, bijlage 839986, p. 1.
29 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 17-18; Cybersecuritybeeld Nederland 2020, 29 juni 2020. Kamerstukken II 2019-2020, 26 643, nr. 695, bijlage 942250; Interviews medewerkers BZ en andere ministeries.
30 Cybersecuritybeeld Nederland 2020, 29 juni 2020. Kamerstukken II 2019-2020, 26 643, nr. 695, bijlage 942250, p. 7; Brief van de minister van Justitie en Veiligheid, 29 juni 2020. Kamerstukken II 2019-2020, 26 643, nr. 695.
31 Nederlandse Cybersecurity Agenda (NCSA), 20 april 2018. Kamerstukken II 2017-2018, 26 643, nr. 536, bijlage 839986, pp. 7, 23.
32 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; interne documenten BZ; Podcast 'Cyberhelden' van Ronald Prins, aflevering 4, met Sico van der Meer (28 januari 2021), beschikbaar via https://www.cyberhelden.nl/episodes/episode-4/; Brief van de minister van Justitie en Veiligheid, 18 april 2019. Kamerstukken II 2018-2019, 30 821, nr. 72; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 20-21.
33 AIVD jaarverslag 2020 (2021), p. 8-9.
34 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; interne documenten BZ; Brief van de minister van Justitie en Veiligheid, 18 april 2019. Kamerstukken II 2018-2019, 30 821, nr. 72; Brief van de minister van Justitie en Veiligheid en staatssecretaris van Economische Zaken en Klimaat, 1 juli 2019. Kamerstukken II, 2018-2019, 30 821, nr. 92; Clingendael Webinar, 'Europe's Digital Decade & China's Digital Silk Road', met Brigitte Dekker, David Ringrose, Reinhard Bütikofer en Maaike Okano-Heijmans (3 december 2020), beschikbaar via: https://www.clingendael.org/event/webinar-europes-digital-decade-chinas-digital-silk-road.

The Hague Program for Cyber Norms (Universiteit Leiden), 2020 Conference, panel 4, 'Digital and cyber sovereignty at crossroads', 11 november 2020. Meer informatie via: https://www.thehaguecybernorms.nl/conference-2020/conference-2020-program-overview; Staalduinen and Joshi (TNO), 'The IoT Security Landscape: Adoption and Harmonisation of Security Solutions for the Internet of Things' (2019), beschikbaar via: https://www.tno.nl/en/about-tno/news/2019/10/the-internet-of-things-security-landscape-study-gives-recommendations-for-cybersecurity/.
35 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen.
36 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; interne documenten BZ; Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, 13 mei 2020. Kamerstukken II 2019-2020, 30 821, nr. 112; Brief van de minister van Justitie en Veiligheid, 18 april 2019. Kamerstukken II 2018-2019, 30 821, nr. 72.
37 Interviews experts van kennisinstellingen en uit het bedrijfsleven, medewerkers BZ en andere ministeries, internationale partners; interne documenten BZ; Financieel Dagblad, 'Veiligheidsdiensten slaan samen alarm om Chinese cyberdreiging in Nederland' (2021), beschikbaar via: https://fd.nl/economie-politiek/1373125/veiligheidsdiensten-slaan-samen-alarm-om-chinese-cyberdreiging-in-nederland; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 20-25; AIVD jaarverslag van 2020 (2021), p. 8.

38 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, interne documenten BZ; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 21, 23, 89-90.

39 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. Beschikbaar via: *https://www.rathenau.nl/nl/digitale-samenleving/cyberspace-zonder-conflict.*

40 AIVD jaarverslag 2020 (2021); Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 23; interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen.

41 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; interne documenten BZ.

42 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven; interne documenten BZ; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 25.

43 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen; interne documenten BZ; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 18, pp. 26-27.

44 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 27-30 en pp. 42-43; interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; interne documenten BZ.

45 Interviews medewerkers BZ en andere ministeries, internationale partners; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 28-29.

46 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen.

47 Brief van de minister van Justitie en Veiligheid, 18 april 2019. Kamerstukken II 2018-2019, 30 821, nr. 72; Accenten van de aanpak statelijke dreigingen, 18 april 2019. Kamerstukken II 2018-2019, 30 821, nr. 72, bijlage 880665; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60; interne documenten BZ; interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners.

48 Brief van de minister van Justitie en Veiligheid, 20 april 2018. Kamerstukken II 2017-2018, 26 643, nr. 536, p. 2.

49 Interne documenten.

50 Interviews medewerkers BZ en andere ministeries.

51 Interviews medewerkers BZ en andere ministeries en uitvoerende organisaties.

52 Interviews medewerkers BZ en andere ministeries.

53 Interviews medewerkers BZ en andere ministeries.

54 Interview medewerkers BZ en andere ministeries.

55 Interviews medewerkers BZ en andere ministeries.

56 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, uitvoerende organisaties, medewerkers internationale organisaties.

57 Interne documenten BZ.

58 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners.

59 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen.

60 Interviews medewerkers BZ en internationale partners.

61 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven.

62 Interviews medewerkers BZ en andere ministeries, experts uit het bedrijfsleven, internationale partners.

63 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven.

64 Interviews medewerkers BZ en andere ministeries, medewerkers internationale organisaties.

65 Interviews medewerkers BZ en andere ministeries, medewerkers internationale organisaties.

66 Interviews medewerkers BZ en andere ministeries.

67 Interviews experts van kennisinstellingen, internationale partners, medewerkers van verschillende betrokken ministeries; aanbevelingensurvey IOB.

68 Interviews experts van kennisinstellingen, internationale partners, medewerkers van verschillende betrokken ministeries; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 3, p. 70.

69 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven.

70 Interviews medewerkers BZ en andere ministeries; evaluatie NCSA (nog niet gepubliceerd).

71 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven; aanbevelingensurvey IOB.

72 Aanbevelingensurvey IOB.

73 Interviews medewerkers BZ en andere ministeries; aanbevelingensurvey IOB.

74 Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, pp. 2-8; Brief van de minister van Buitenlandse Zaken, 17 april 2020. Kamerstukken II 2019-2020, 33 694, nr. 57, p. 5; Voortgang Nederlandse Cybersecurity Agenda, 12 juni 2019. Kamerstukken II 2018-2019, 26 643, nr. 614, bijlage 887547, p. 2; Brief van de minister voor Buitenlandse Handel en Ontwikkelingssamenwerking, 22 maart 2021. Kamerstukken II 2020-2021, 34 952, nr. 129; Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, p. 2; Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62, p. 2.

75 Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, p. 2.

76 Brief van de minister van Buitenlandse Zaken, 17 april 2020. Kamerstukken II 2019-2020, 33 694, nr. 57, p. 5.

Voortgang Nederlandse Cybersecurity Agenda, 12 juni 2019. Kamerstukken II 2018-2019, 26 643, nr. 614, bijlage 887547, p. 2; Brief van de minister voor Buitenlandse Handel en Ontwikkelingssamenwerking, 22 maart 2021. Kamerstukken II 2020-2021, 34 952, nr. 129; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, p. 2.

77 Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, p. 2; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, p. 5 en p. 8; Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62, p. 2.

78 Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, p. 3; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, p. 8.

79 Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, pp. 2-3; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, p. 8; Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62, p. 10; Nederlandse Cybersecurity Agenda (NCSA), 20 april 2018. Kamerstukken II 2017-2018, 26 643, nr. 536, bijlage 839986, p. 10, pp. 23-24; 'Digitaal bruggen slaan' – Internationale Cyberstrategie: naar een geïntegreerd internationaal cyberbeleid (ICS), 12 februari 2017. Kamerstukken II 2016-2017, 26 643, nr. 447, bijlage 80029, pp. 2-3, p. 8; 'Wereldwijd voor een veilig Nederland' – Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022 (GBVS), 27 maart 2018. Kamerstukken II 2017-2018, 33 694, nr. 12, bijlage 836794, p. 7.

80 Interne documenten BZ.

81 Interviews medewerkers TFC en andere BZ-directies.

82 Interviews medewerkers TFC en andere BZ-directies.

83 Interviews medewerkers TFC en andere BZ-directies, experts van kennisinstellingen.

84 Interviews medewerkers BZ, experts van kennisinstellingen, internationale partners.

85 Interviews medewerkers BZ, experts van kennisinstellingen, internationale partners.

86 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen, internationale partners.

87 Interviews experts van kennisinstellingen en uit het bedrijfsleven, internationale partners.

88 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen, internationale partners.

89 Interviews medewerkers BZ en uitvoerende organisaties.

90 Nederlandse Cybersecurity Agenda (NCSA), 20 april 2018. Kamerstukken II 2017-2018, 26 643, nr. 536, bijlage 839986, pp. 23-24; Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62, p. 2.

91 Op moment van schrijven nog niet gepubliceerde evaluatie van de NCSA; interviews medewerkers BZ, experts van kennisinstellingen, medewerkers internationale organisaties.

92 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven.

93 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, uitvoerende organisaties en medewerkers internationale organisaties.

94 Interviews medewerkers TFC en andere ministeries, experts van kennisinstellingen.

95 Interviews medewerkers TFC en andere BZ-directies, experts van kennisinstellingen, internationale partners.

96 Interviews medewerkers TFC en andere BZ-directies, internationale partners.

97 Interviews medewerkers TFC en andere BZ-directies.

98 Interviews medewerkers TFC.

99 Brief van de minister van Buitenlandse Zaken, 17 april 2020. Kamerstukken II 2019-2020, 33 694, nr. 57, p. 2.

100 Interviews medewerkers TFC en andere BZ-directies.

101 Interviews medewerkers TFC en andere BZ-directies.

102 Interviews medewerkers TFC en andere BZ-directies, internationale partners.

103 Interne documenten BZ; interviews medewerkers BZ.

104 Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, pp. 2 en 8.

105 Interviews medewerkers BZ; interne documenten BZ; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, p. 4.

106 Interviews medewerkers internationale organisaties, experts uit het bedrijfsleven, medewerkers BZ en andere ministeries; interne documenten BZ.

107 Interne documenten BZ; interviews medewerkers BZ, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners.

108 Interviews medewerkers BZ, experts van kennisinstellingen, internationale partners.

109 Interviews experts van kennisinstellingen en uit het bedrijfsleven, medewerkers verschillende betrokken ministeries.

110 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62, p. 5.

111 Interviews medewerkers internationale organisaties en uitvoerende organisaties, experts van kennisinstellingen en uit het bedrijfsleven, medewerkers BZ en andere ministeries; interne documenten BZ.

112 Interviews medewerkers internationale organisaties en uitvoerende organisaties, experts uit het bedrijfsleven en van kennisinstellingen, medewerkers BZ en andere ministeries; aanbevelingensurvey IOB.

113 Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60; interviews internationale partners, medewerkers BZ.

114 Interviews internationale partners, experts van kennisinstellingen, medewerkers BZ en andere ministeries; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 62.

115 Interviews medewerkers BZ, experts van kennisinstellingen, uitvoerende organisaties.

116 Interviews internationale partners, medewerkers BZ en andere ministeries.

117 Interviews beleidsmedewerkers BZ en andere ministeries, internationale partners; Interne documenten BZ.

118 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 20-21.

119 Interviews medewerkers BZ, internationale partners, experts van kennisinstellingen en uit het bedrijfsleven.

120 Interviews medewerkers BZ en andere ministeries, internationale partners, experts van kennisinstellingen en uit het bedrijfsleven.

121 Interne documenten BZ; interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; Brief van de minister van Justitie en Veiligheid, 18 april 2019. Kamerstukken II 2018-2019, 30 821, nr. 72; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60; Clingendael Webinar, 'Europe's Digital Decade & China's Digital Silk Road', met Brigitte Dekker, David Ringrose, Reinhard Bütikofer en Maaike Okano-Heijmans (3 december 2020), beschikbaar via: https://www.clingendael.org/event/webinar-europes-digital-decade-chinas-digital-silk-road.

122 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 77-78; interne documenten BZ.

123 Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60; interne documenten BZ; interviews medewerkers BZ en andere ministeries, internationale partners.

124 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 35 en pp. 60-61; interne documenten BZ; interviews experts van kennisinstellingen, medewerkers BZ.

125 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 63-64.

126 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 63; Gorwa & Peez, 'Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord' (p. 263) in Broeders & Van den Berg, 'Governing Cyberspace: Behavior, Power, and Diplomacy' (2020), beschikbaar via: https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf.

127 Interne documenten BZ; The Hague Program for Cyber Norms (Universiteit Leiden), 2020 Conference, panel 4, 'Digital and cyber sovereignty at crossroads', 11 november 2020. Meer informatie is beschikbaar via: https://www.thehaguecybernorms.nl/conference-2020/conference-2020-program-overview; interviews medewerkers BZ.

128 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 35, 60-61; interne documenten BZ.

129 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 35 en pp. 60-61.

130 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen; interne documenten BZ; Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60.

131 Interne documenten BZ.

132 Interne documenten BZ; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 77-78.

133 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners; interne documenten BZ; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 77-78.

134 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 78; Interviews medewerkers BZ, experts van kennisinstellingen, internationale partners.

135 Interviews medewerkers BZ, internationale partners; interne documenten BZ; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 77-78.

136 Brief van de minister van Buitenlandse Zaken, 5 juli 2019. Kamerstukken II 2018-2019, 33 694, nr. 47, Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60; interne documenten BZ.

137 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 77-78; interne documenten BZ.

138 Interne documenten BZ; interviews medewerkers BZ.

139 Interne documenten BZ.

140 Interne documenten BZ; interviews medewerkers BZ.

141 Interne documenten BZ; interviews medewerkers BZ.

142 Interviews medewerkers BZ; interne documenten BZ.

143 Interviews medewerkers BZ; interne documenten BZ.

144 Interview medewerker BZ; Interne documenten BZ; Michael Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace' (2021), beschikbaar via: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

145 VN, 'Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security, advance copy' 28 mei 2021, p.14.

146 VN, 'Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security, advance copy' 28 mei 2021; interview medewerker BZ; interne documenten BZ.

147 Interview medewerker BZ; interne documenten BZ; Michael Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace' (2021), beschikbaar via: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/; Andrijana Gavrilovic, 'What's new with cyber negotiations? The UN GGE 2021 report' (2021), beschikbaar via: https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-gge-2021-report.

148 Interviews medewerkers BZ; interne documenten BZ; The Cyberpeace Institute, 'The UN GGE final report: a milestone in cyber diplomacy, but where is the accountability?' (2021), beschikbaar via: https://cyberpeaceinstitute.org/news/the-un-gge-final-report-a-milestone-in-cyber-diplomacy-but-where-is-the-accountability.

149 Interviews medewerkers BZ; interne documenten BZ.

150 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 78; Interviews medewerkers BZ, experts van kennisinstellingen, internationale partners; Interne documenten BZ.

151 Interviews medewerkers BZ en andere ministeries; interne documenten BZ; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60; Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62; Clingendael Webinar, 'Europe's Digital Decade & China's Digital Silk Road', met Brigitte Dekker, David Ringrose, Reinhard Bütikofer en Maaike Okano-Heijmans (3 december 2020), beschikbaar via: https://www.clingendael.org/event/webinar-europes-digital-decade-chinas-digital-silk-road.

152 Interne documenten BZ; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60; interviews medewerkers BZ en andere ministeries.

153 Interviews medewerkers BZ en andere ministeries, internationale partners, experts van kennisinstellingen en uit het bedrijfsleven; interne documenten BZ; Clingendael Webinar, 'Europe's Digital Decade & China's Digital Silk Road', met Brigitte Dekker, David Ringrose, Reinhard Bütikofer en Maaike Okano-Heijmans (3 december 2020), terug te kijken via: https://www.clingendael.org/event/webinar-europes-digital-decade-chinas-digital-silk-road; Staalduinen and Joshi (TNO), 'The IoT Security Landscape: Adoption and Harmonisation of Security Solutions for the Internet Of Things' (2019), beschikbaar via: https://www.tno.nl/en/about-tno/news/2019/10/the-internet-of-things-security-landscape-study-gives-recommendations-for-cybersecurity/; Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62, p. 9.

154 Interne documenten BZ; interviews medewerkers BZ.

155 Interne documenten BZ; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60; interviews medewerkers BZ.

156 Interviews internationale partners, experts van kennisinstellingen, medewerkers BZ en andere ministeries.

157 Interviews medewerkers BZ en andere ministeries.

158 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven.

159 The Hague Program for Cyber Norms (Universiteit Leiden), 2020 Conference, panel 6, 'Toward inclusion: the global governance of cyber norms', 12 november 2020. Meer informatie is beschikbaar via: https://www.thehaguecybernorms.nl/conference-2020/conference-2020-program-overview; interne documenten BZ.

160 Interviews internationale partners en medewerkers BZ; interne documenten BZ.

161 Interne documenten BZ; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 61; Interviews internationale partners, experts van kennisinstellingen, medewerkers BZ.

162 Interviews internationale partners, experts van kennisinstellingen, medewerkers BZ en andere ministeries; interne documenten BZ.

163 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 61; interviews internationale partners, experts van kennisinstellingen, medewerkers BZ.

164 Interne documenten BZ.

165 Interviews medewerkers BZ, uitvoerende organisaties.

166 Nederlandse Cybersecurity Agenda (NCSA), 20 april 2018. Kamerstukken II 2017-2018, 26 643, nr. 536, bijlage 839986; 'Wereldwijd voor een veilig Nederland' – Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022 (GBVS), 27 maart 2018. Kamerstukken II 2017-2018, 33 694, nr. 12, bijlage 836794.

167 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen, internationale partners.

168 Interviews medewerkers BZ en andere ministeries, medewerkers bij uitvoerende organisaties; Verslag van een schriftelijk overleg, 11 februari 2021. Kamerstukken II 2020-2021, 33 694, nr. 62; Verslag van een schriftelijk overleg, 23 juni 2017. Kamerstukken II 2016-2017, 26 643, nr. 475; Brief van de minister van Buitenlandse Zaken, 16 november 2020. Kamerstukken II 2019-2020, 33 694, nr. 60, 'Digitaal bruggen slaan' – Internationale Cyberstrategie: naar een geïntegreerd internationaal cyberbeleid (ICS), 12 februari 2017. Kamerstukken II 2016-2017, 26 643, nr. 447, bijlage 80029, p. 8; interne documenten BZ.

169 Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, pp. 84-85.

170 Interne documenten BZ; interviews medewerkers TFC.

171 Interne documenten BZ.

172 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen.

173 Interviews medewerkers BZ, experts van kennisinstellingen.

174 Interviews experts van kennisinstellingen en uit het bedrijfsleven, medewerkers BZ; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 85.

175 Interviews medewerkers BZ, experts van kennisinstellingen; Clingendael Webinar, 'Europe's Digital Decade & China's Digital Silk Road', met Brigitte Dekker, David Ringrose, Reinhard Bütikofer en Maaike Okano-Heijmans (3 december 2020), beschikbaar via: https://www.clingendael.org/event/webinar-europes-digital-decade-chinas-digital-silk-road; Literatuurstudie Van Douwen, Gjaltema (Vrije Universiteit), in opdracht van IOB, p. 84; interne documenten BZ.

176 Interne document BZ.

177 Interviews medewerkers internationale organisaties, experts van kennisinstellingen, medewerkers verschillende betrokken BZ-directies en verschillende betrokken ministeries.

178 Interviews medewerkers internationale organisaties, experts van kennisinstellingen, medewerkers betrokken BZ-directies en verschillende betrokken ministeries.

179 Interviews medewerkers andere BZ-directies en andere ministeries, experts van kennisinstellingen, medewerkers internationale organisaties.

180 Interviews medewerkers TFC en andere BZ-directies, andere ministeries, experts van kennisinstellingen, medewerkers uitvoerende organisaties.

181 Brief van de minister van Justitie en Veiligheid, 12 juni 2019. Kamerstukken II 2018-2019, 26 643, nr. 614, p.1.

182 Brief van de minister van Justitie en Veiligheid, 27 juni 2018. Kamerstukken II 2017-2018, 26 643, nr. 544; Brief van de minister van Justitie en Veiligheid, 12 juni 2019. Kamerstukken II 2018-2019, 26 643, nr. 614; Brief van de minister van Justitie en Veiligheid, 12 juni 2019. Kamerstukken II 2018-2019, 28 684, nr. 564; interviews medewerkers TFC en andere BZ-directies, medewerkers verschillende betrokken ministeries; aanbevelingensurvey IOB.

183 Interviews medewerkers TFC, medewerkers verschillende betrokken ministeries; aanbevelingensurvey IOB

184 Interviews medewerkers TFC, experts van kennisinstellingen, medewerkers uitvoerende organisaties.

185 Interviews medewerkers TFC.

186 Interviews medewerkers TFC.

187 Interviews medewerkers TFC; aanbevelingensurvey IOB.

188 Interviews medewerkers TFC; aanbevelingensurvey IOB.

189 Interviews cyberdiplomaten en –aanspreekpunten, medewerkers TFC, experts van kennisinstellingen en uit het bedrijfsleven.

190 Interviews cyberdiplomaten en –aanspreekpunten, medewerkers TFC en andere BZ-directies, medewerkers uitvoerende organisaties; aanbevelingensurvey IOB.

191 Interviews cyberdiplomaten en –aanspreekpunten, medewerkers TFC, experts van kennisinstellingen, medewerkers uitvoerende organisaties.

192 Interviews medewerkers TFC.

193 Interviews medewerkers TFC en internationale partners.

194 Interviews cyberdiplomaten en –aanspreekpunten, medewerkers TFC en andere BZ-directies, andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven, internationale partners.

195 Interviews cyberdiplomaten en –aanspreekpunten, medewerkers TFC en andere BZ-directies, andere ministeries, experts van kennisinstellingen, internationale partners.

196 Interne documenten BZ; Interviews medewerkers BZ.

197 Interviews cyberdiplomaten en –aanspreekpunten, medewerkers TFC en andere BZ-directies, andere ministeries, experts uit het bedrijfsleven.

198 Interviews cyberdiplomaten en –aanspreekpunten, medewerkers TFC.

199 Interviews cyberdiplomaten en –aanspreekpunten, medewerkers TFC.

200 Interviews medewerkers BZ; interne documenten BZ.

201 Interviews medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven; Podcast 'Cyberhelden' van Ronald Prins, aflevering 4 met Sico van der Meer (28 januari 2021), beschikbaar via https://www.cyberhelden.nl/episodes/episode-4/; aanbevelingensurvey IOB.

202 Interviews medewerkers TFC, andere BZ-directies en andere ministeries, experts uit het bedrijfsleven; aanbevelingensurvey IOB.

203 Interviews medewerkers verschillende betrokken ministeries, internationale organisaties en experts uit het bedrijfsleven; aanbevelingensurvey IOB.

204 Interviews cyberdiplomaten- en aanspreekpunten, medewerkers andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven.

205 Interviews met medewerkers BZ, experts van kennisinstellingen, internationale partners; aanbevelingensurvey IOB.

206 Interviews met medewerkers TFC, andere directies BZ, cyberdiplomaten en –aanspreekpunten, medewerkers van andere ministeries.

207 Interviews met medewerkers BZ en andere ministeries, experts van kennisinstellingen en uit het bedrijfsleven.

208 Aanbevelingensurvey IOB.

Verbeter de verbinding | IOB Evaluatie | Verbeter de verbinding | IOB Evaluatie | Verbeter de verbinding | IOB Evaluatie | Verbeter de verbinding | IOB Evaluatie | Verbeter de verbinding | IOB Evaluatie | Verbeter de verbinding | IOB Evaluatie

Uitgebracht door: Ministerie van Buitenlandse Zaken
Directie Internationaal Onderzoek en Beleidsevaluatie (IOB)
Postbus 20061 | 2500 EB Den Haag

www.iob-evaluatie.nl
www.rijksoverheid.nl/bz-evaluaties
www.twitter.com/IOBevaluatie

ISBN: 978-90-5146-068-1

Opmaak: Today | Utrecht

Foto voorpagina: Shutterstock