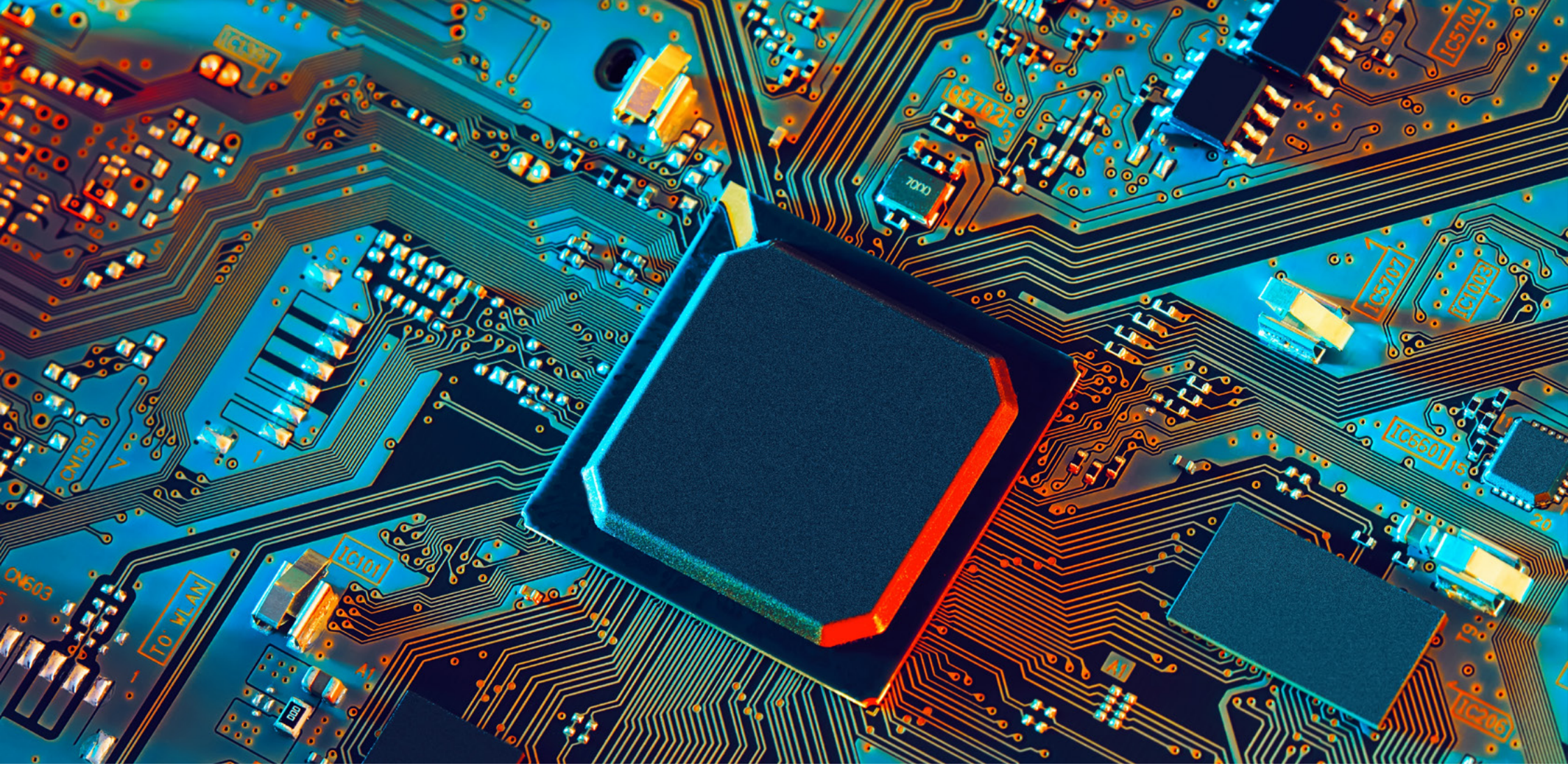

Samenvatting

Verbeter de verbinding

Evaluatie internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken

Achtergrond en belang

Dit document bevat een samenvatting van de belangrijkste bevindingen en aanbevelingen van de IOB-evaluatie van het internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken (BZ).

Toenemende dreigingen

In de evaluatieperiode 2015-2021 zijn cyberdreigingen wereldwijd toegenomen. In binnen- en buitenland vinden dagelijks digitale aanvallen plaats, waarvan een groot deel afkomstig is van staten en aan staten gelieerde actoren. Deze aanvallen halen niet altijd de publiciteit, maar de gevolgen ervan zijn wel steeds vaker merkbaar voor overheden, bedrijven en burgers. Daarnaast is er internationaal een tweedeling ontstaan 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 de vrije toegang tot het internet van burgers willen beknotten. Door de verharde geopolitieke situatie en het toegenomen aantal incidenten, is het moeilijk om mondiaal afspraken te maken over gedragsregels en de toepassing van het internationaal recht in het cyberdomein.

Het internationaal cybersecuritybeleid

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. Binnen BZ is hiervoor in 2015 de Taskforce Cyber (TFC) opgericht, wiens werk grofweg kan worden samengevat als 1) diplomatieke respons en coördinatie bij cyberaanvallen en andere incidenten; 2) diplomatieke inzet ter bevordering van de internationale rechtsorde in het cyberdomein en; 3) financiële inzet voor capaciteitsopbouw op cybersecuritygebied in andere landen.

Belang evaluatie

Gezien de toenemende cyberdreigingen richting Nederland neemt de maatschappelijke en politieke aandacht voor uitdagingen in het cyberdomein toe. Hierdoor is het werk van de TFC urgenter geworden. Het internationaal cybersecuritybeleid, waarbinnen de TFC sinds 2015 opereert, is als relatief jong beleidsterrein echter nog niet eerder geëvalueerd. Uit deze eerste evaluatie blijkt dat sinds 2015 door de TFC vaak goed werk is geleverd en er zaken zijn bereikt, maar er zijn ook uitdagingen en verbeterpunten. Hoewel deze evaluatie gericht was op het internationaal cybersecuritybeleid van BZ, bleek gedurende het onderzoek dat een aantal van de belangrijkste uitdagingen – en oplossingen – overheidsbreed zijn. Gegeven de komst van een nieuw kabinet, is dit dan ook een goed moment voor een blik vooruit en verdere aanscherping van het internationale cybersecuritybeleid, waar deze evaluatie aanbevelingen voor doet.

Het onderzoek

In de evaluatie is onderzocht wat er goed en minder goed gaat bij het ontwerp en de implementatie van het internationaal cybersecuritybeleid van BZ, en welke aanbevelingen op grond hiervan kunnen worden geformuleerd. Het rapport is opgesteld op basis van interviews met 95 betrokkenen en experts, een survey onder 73 betrokkenen en experts, een analyse van interne en externe documenten en een literatuurstudie. Het volledige rapport is hier te vinden: www.iob-evaluatie.nl/resultaten/internationaal-cybersecuritybeleid.

Hoofdbevindingen en aanbevelingen

Interdepartementale samenwerking: deel van probleem en oplossing

Er zijn verschillende ministeries betrokken bij aspecten van het internationaal cybersecuritybeleid. In de evaluatieperiode (2015-2021) zijn er meerdere interdepartementale beleidsdocumenten opgesteld die raken aan het internationaal cybersecuritybeleid en is de samenwerking tussen departementen verbeterd. Niettemin kwamen uit het onderzoek nog steeds afstemmings- en samenwerkingsproblemen naar voren bij het internationaal (en nationaal) cybersecuritybeleid. Zo werken departementen nog te vaak langs elkaar heen, zijn ze niet altijd voldoende op de hoogte van elkaars werk, maken ze niet altijd voldoende gebruik van expertise bij andere departementen, en geven ze niet altijd voldoende medewerking aan elkaar. Hierdoor worden dreigingen en kansen gemist, wordt er inefficiënt gewerkt en is beleid niet altijd coherent (zie hoofdstuk 2). Eén van de belangrijkste oorzaken van de samenwerkingsproblemen is de departementale verkokering van het cybersecuritybeleid in Nederland. Dit komt tot uiting in het feit dat departementen ieder hun eigen prioriteiten stellen, er geen nationale departement-overkoepelende cybersecuritystrategie is, en er geen centrale aansturing van het cybersecuritybeleid bestaat die zo'n strategie op zou kunnen stellen en prioriteiten stelt.

Aanbevelingen

Voor het Nederlandse kabinet:

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

Er is een departement-overstijgende aansturing nodig die zorgt voor het vaststellen van mandaten en taken bij nieuwe vraagstukken en beleidsthema's, het afwegen van verschillende belangen van de betrokken departementen, het bevorderen van de onderlinge afstemming tussen betrokken departementen, en het opstellen, monitoren en wanneer nodig bijstellen van een departement-overstijgende cybersecuritystrategie.

Er zijn verschillende opties om dit te realiseren, die elk hun eigen uitdagingen met zich meebrengen (zie hoofdstuk 2). Er dient onderzocht te worden welke optie het meest geschikt is om de beleidsdoelen te behalen en een oplossing te bieden voor de gesignaleerde problemen.

2. **Creëer een departement-overstijgende cybersecuritystrategie.**

De departement-overstijgende strategie dient een kabinetsvisie te presenteren die duidelijk maakt welke kant Nederland op wil met aan cybersecurity gerelateerde onderwerpen. Het dient geen samenvatting te zijn van zaken die departementen al doen of van plan zijn te doen, zoals de huidige Nederlandse Cybersecurity Agenda (NCSA), maar verbindt de verschillende beleidsthema's door prioriteiten te stellen, eventuele botsende belangen te beslechten, concrete doelstellingen op te nemen en in te gaan op de manieren waarop deze doelen bereikt kunnen worden.

Het internationaal cybersecuritybeleid binnen het ministerie van Buitenlandse Zaken

Uit het onderzoek blijkt dat de Taskforce Cyber (TFC) van BZ veel goed doet: Nederland profileert zich internationaal sterk en heeft binnen internationale fora bijgedragen aan belangrijke instrumenten zoals de oprichting van de EU Cyber Diplomacy Toolbox en het cybersanctieregime. Daarnaast is de oprichting van het cyberdiplomatennetwerk een sterke zet geweest (zie hoofdstukken 4 en 5).

Er zijn ook een aantal zaken die kunnen worden verbeterd. Zo is er binnen BZ beperkte kennis over aan cybersecurity gerelateerde onderwerpen. Ook is de beschikbare capaciteit binnen de TFC beperkt – net als bij andere onderdelen van de overheid die

over cybersecuritybeleid gaan – gegeven de toename van het aantal cyberincidenten en mondiale uitdagingen, en de tijd die interdepartementale afstemming vergt. Daarnaast ontbreekt het binnen BZ aan een eenduidige en up-to-date strategie, en kaders die duidelijk afbakenen welke thema's wel en niet bij het werk van de TFC horen. Dit maakt het lastiger goed te prioriteren, zorgt ervoor dat sommige strategische vraagstukken onbeantwoord blijven en draagt bij aan de toch al hoge werkdruk.

Aanbevelingen

Voor het ministerie van Buitenlandse Zaken:

3. **Creëer, als onderdeel van- of aansluitend op een nieuwe departement-overstijgende cybersecuritystrategie, ook een nieuwe strategie voor het internationaal cybersecuritybeleid van BZ. Zorg ervoor dat:**

    a. Duidelijke definities en kaders worden opgenomen zodat inzichtelijk is wat al dan niet onder de verantwoordelijkheid van de TFC valt; en uiteengezet wordt wat de korte- middellange- en langetermijndoelstellingen zijn, hoe ze op elkaar aansluiten en hoe beoogd wordt deze te bereiken (zie hoofdstuk 3).
    b. Er antwoord wordt gegeven op strategische vraagstukken die voorliggen als gevolg van toenemende cyberdreigingen, scherpe mondiale tegenstellingen, opkomende technologieën en nieuwe beleidsthema's. Bijvoorbeeld de manier waarop Nederland en gelijkgestemde landen de voor multilaterale onderhandelingen belangrijke *swing states* het beste bij hun invloedssfeer kunnen betrekken, hoe capaciteitsopbouw het beste ingezet kan worden, en de houdbaarheid van de Nederlandse afwijzing van een internationaal cyberverdrag (zie hoofdstuk 4).
    c. Er gegeven de snelle ontwikkelingen in het cyberdomein tijd en capaciteit wordt ingebouwd voor regelmatige strategische reflectie en voor het denken in scenario's over verschillende mogelijke toekomstige ontwikkelingen en dreigingen.
    d. Bij het opstellen van de strategie samengewerkt wordt met andere departementen en stakeholders uit het bedrijfsleven en kennisinstellingen.

4. **Ga na op welke manier er scherper geprioriteerd kan worden in het werk van de TFC om de werkdruk te verlagen.**

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

5. **Zorg ervoor dat BZ beschikt over voldoende capaciteit om invulling te geven aan belangrijke taken binnen het internationaal cybersecuritybeleid. Denk hierbij aan drie zaken:**

    a. **Zorg voor extra menskracht bij de TFC.**
    In het licht van de toenemende dreigingen en incidenten, de mondiale tegenstellingen, opkomende thema's en technologieën, strategische vraagstukken en de daaruit voortkomende (interdepartementale) uitdagingen, is scherpere prioritering alleen niet voldoende en heeft de TFC extra capaciteit nodig.

    b. **Denk na over manieren waarop kennis en expertise over aan cybersecurity gerelateerde onderwerpen ingewonnen en behouden kunnen worden.**
    Zo kunnen medewerkers die ervaring hebben met aan cybersecurity gerelateerde onderwerpen meer gestimuleerd worden om 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. Daarnaast kan actiever kennis van buiten naar binnen gehaald worden, door met meer publiek-private samenwerking kennishiaten binnen BZ op te lossen.

    c. **Investeer in veilige en goed werkende communicatiemiddelen.**
    Naast een investering in menskracht en kennis, is het ook van belang dat BZ, de TFC en voor hen relevante posten gaan beschikken over goed werkende en veilige communicatiemiddelen waarmee vertrouwelijke informatie (beter) gedeeld kan worden (zie hoofdstuk 5).

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