Methodologische verantwoording

IOB Evaluatie van het internationaal cybersecuritybeleid van het ministerie van Buitenlandse Zaken

juni 2021

Dit document geeft informatie over de gebruikte methodologie bij de IOB evaluatie van het Nederlandse internationaal cybersecuritybeleid.

Vier onderzoeks-onderdelen

IOB heeft gebruikgemaakt van vier verschillende onderzoeksmethoden en bronnen:

- Een literatuurstudie
- Interviews met betrokkenen en experts binnen het cybersecuritydomein
- Analyse van interne documenten en correspondentie van het ministerie van Buitenlandse Zaken (BZ)
- Een survey onder medewerkers en experts

In het evaluatierapport zijn de belangrijkste bevindingen uit deze vier onderdelen samengebracht. Daarbij is gebruik gemaakt van bronnentriangulatie: uitspraken in het rapport zijn zoveel mogelijk gebaseerd op bevindingen uit verschillende typen bronnen, om de betrouwbaarheid van bevindingen te verhogen.

De literatuurstudie werd uitgevoerd door een externe partij (zie volgende paragraaf). De interviews en de survey zijn uitgevoerd en geanalyseerd door onderzoekers van IOB, en ook de analyse van de interne documenten is verricht door IOB. Hiervan zijn geen aparte publicaties beschikbaar.

Literatuurstudie

De literatuurstudie is in opdracht van IOB verricht door externe onderzoekers van de Vrije Universiteit Amsterdam. Van de literatuurstudie is een apart rapport gepubliceerd, waarin de methodologische verantwoording en beperkingen van dit onderzoeksonderdeel staan beschreven. De literatuurstudie is te raadplegen via deze link op de website van IOB: www.iob-evaluatie.nl/resultaten/internationaal-cybersecuritybeleid. De literatuurstudie behelst een analyse van de beschikbare academische en grijze literatuur. Bij het vermelden van de bronnen in het hoofdrapport van de evaluatie heeft het IOB-onderzoeksteam verwezen naar de betreffende pagina in het rapport van de literatuurstudie, en niet naar de onderliggende literatuur die wordt aangehaald in de literatuurstudie.

Methodologie interviews met (internationale) experts en betrokkenen bij het cybersecuritybeleid

Een belangrijk onderdeel van het onderzoek was een groot aantal interviews met betrokkenen bij- en experts op het gebied van het internationaal cybersecuritydomein.

Afname interviews
De interviews zijn afgenomen door leden van het onderzoeksteam van IOB. Bij de interviews waren in de regel twee personen aanwezig vanuit IOB: één die het gesprek leidde en de ander die notuleerde. In een enkel geval is hier van afgeweken en is met een opname gewerkt, die later door iemand van het onderzoeksteam werd uitgetypt. In een klein aantal gevallen zijn de aantekeningen niet gemaakt door een IOB-medewerker maar door een professionele notulist. De meeste interviews zijn, in verband met de Covid-19 crisis en het verplicht thuiswerken, maar ook vanwege het feit dat een aanzienlijk aantal respondenten niet in Nederland woont, telefonisch of via videoconferentie verricht. Hiervoor maakte IOB gebruik van verschillende applicaties, zoals – maar niet uitsluitend – Microsoft Teams, Cisco Jabber, Zoom, FaceTime, Skype, Jitsi Meet. Een kleiner aantal interviews vond plaats in persoon op het ministerie van Buitenlandse Zaken of op de werklocatie van geïnterviewden. In alle gevallen heeft IOB in overleg met de respondent de beslissing gemaakt op welke manier het interview het beste plaats kon vinden, waarbij informatieveiligheid en de Covid-19 gezondheidsrisico's en maatregelen de belangrijkste afwegingen waren.

Selectie geïnterviewden
De namen en contactgegevens van de geïnterviewden zijn op verschillende manieren achterhaald. Leden van de referentiegroep van de evaluatie, bestaande uit drie externe experts en twee afgevaardigden van de betrokken beleidsdirecties, hebben namen en waar mogelijk ook contactgegevens aangedragen. Daarnaast heeft het IOB-onderzoeksteam op eigen inzicht namen en contactgegevens opgezocht en potentiele respondenten vervolgens benaderd. Zij kwamen in veel gevallen op in overheidsdocumenten, emailverkeer en (academische) literatuur, maar ook door het toepassen van *snowball-sampling*[1] werd IOB's respondentenlijst uitgebreid.

Het IOB-onderzoeksteam heeft bij de selectie van de uiteindelijk geïnterviewden gewaarborgd dat recht werd gedaan aan de breedte van het beleidsterrein. Zodoende heeft IOB gesproken met professionals in het cybersecuritydomein uit binnen- en buitenland, zoals: medewerkers van BZ, medewerkers van andere Nederlandse ministeries, experts van kennisinstellingen en het bedrijfsleven, medewerkers van door BZ gefinancierde uitvoerende organisaties, en andere internationale partners van BZ.

Een methodologische beperking van het onderzoek is dat er voornamelijk is gesproken met respondenten uit Nederland en uit landen die als bondgenoot van Nederland kunnen worden

[1] *Snowball-sampling* is een manier om de selectielijst van potentiele interviewrespondenten uit te breiden door tijdens interviews te vragen naar de namen van andere personen of organisaties die relevant kunnen zijn voor het onderzoek.

beschouwd, waardoor mogelijk invalshoeken van respondenten uit niet-gelijkgestemde landen zijn gemist. Hiervoor is gekozen op basis van overwegingen van informatieveiligheid, logistiek en mogelijke (diplomatieke) afbreukrisico's.

In totaal zijn 95 personen geïnterviewd.

Vertrouwelijkheid
Deelname aan een interview geschiedde op geheel vrijwillige basis. Het IOB-onderzoeksteam beloofde de geïnterviewden vertrouwelijk om te gaan met hetgeen dat gezegd werd en met de interviewverslagen. Dit betekent onder meer dat de namen van de respondenten niet in het rapport staan, dat er geen bevindingen herleidbaar naar personen zijn opgeschreven en dat er geen gebruik is gemaakt van quotes of andere (bijna) letterlijke bewoordingen van de respondent. Enkel algemene bevindingen zijn opgeschreven, gebaseerd op meerdere bronnen. De interviewverslagen werden, overeenkomstig met de gemaakte afspraken met de geïnterviewden over vertrouwelijkheid, op een veilige plaats bewaard en niet gedeeld met personen buiten het IOB-onderzoeksteam. Bovendien werden alle geïnterviewden gewezen op het recht te allen tijde hun deelname te kunnen terugtrekken. Dit is in geen enkel geval gebeurd.

Twee interviewrondes
De interviews vonden plaats in twee rondes. De eerste ronde liep van juni tot en met november 2020 en bevatte het merendeel van de interviews. Deze ronde ging vooraf aan het analyseren van de resultaten en het schrijven van de eerste versie van het rapport. De tweede interviewronde vond plaats in februari en maart 2021, en had voornamelijk als doel nog onzekere informatie te verifiëren en ontbrekende informatie in te winnen. In een paar gevallen hebben de IOB-onderzoekers een respondent uit de eerste ronde, ook in de tweede ronde bevraagd.

Semigestructureerde, kwalitatieve interviews
De interviews duurden doorgaans 1-1.5 uur en waren semigestructureerd. Dit betekent dat het IOB-onderzoeksteam voorafgaand aan elk interview een lijst met onderwerpen en vragen had opgesteld, maar dat de precieze inhoud van de uiteindelijke gesprekken afhing van de ervaring en expertise van de respondent – waar in veel gevallen tijdens het interview meer duidelijkheid over ontstond. Het IOB-onderzoeksteam stelde meestal open vragen naar de ervaringen met- en zienswijzen op het internationaal cybersecuritybeleid, dreigingen en uitdagingen. In de tweede ronde waren de interviews vaak wat korter en werden minder open vragen gesteld.

Het IOB-onderzoeksteam stelde niet dezelfde vragen aan alle geïnterviewden. Om die reden kunnen de interviews niet gebruikt worden om kwantitatieve uitspraken te doen zoals "75% van de geïnterviewden vond X". In het rapport is dan ook niet aangegeven hoeveel geïnterviewden een bepaalde uitspraak deden, aangezien het misleidend zou zijn om te vermelden dat bijvoorbeeld twintig van de 95 mensen een bepaald antwoord hebben gegeven, terwijl niet alle geïnterviewden dezelfde vraag kregen voorgelegd. Wel is middels de bronvermelding (in eindnoten) een beschrijving gegeven van de rol van geïnterviewden die een bepaalde bevinding onderbouwden, zoals 'beleidsmedewerkers en diplomaten van Buitenlandse Zaken en externe experts'. Uiteraard is het onderzoeksteam daarbij zorgvuldig omgesprongen met de beloofde vertrouwelijkheid en is te alle tijden gewaarborgd dat een bevinding niet herleidbaar zou zijn naar personen.

Analyse
De gespreksnotulen werden geüpload naar het kwalitatieve analyseprogramma MaxQDA. Dat programma is gebruikt voor het coderen van de interviews binnen een door het onderzoeksteam opgesteld codeerschema – waarin handmatig unieke labels aan de specifieke antwoorden van

respondenten werden gehangen. Dit gecodeerde bestand heeft vervolgens gediend als één van de vier belangrijke databronnen op basis waarvan het IOB-onderzoeksteam het rapport heeft geschreven.

Methodologie analyse van (interne) documenten en correspondentie

Een ander belangrijk onderdeel van het onderzoek was een analyse van een groot aantal (interne) documenten en correspondentie van BZ. Dit gebeurde net als bij de interviews met het analyseprogramma MaxQDA.

Alle geraadpleegde documenten zijn door IOB-onderzoekers geselecteerd op basis van relevantie voor het onderzoek. De documenten stammen nagenoeg allemaal uit de onderzochte periode van 2015-2021, waarbij enigszins de nadruk lag op de laatste helft van deze onderzochte periode. Waar relevant zijn enkele documenten van voor 2015 meegenomen in de analyse. Gedurende het onderzoek zijn ook nieuw verschenen documenten verzameld en geanalyseerd zodat het onderzoek zoveel mogelijk de actualiteit mee zou blijven nemen.

Hieronder staat een beschrijving van het soort documenten dat is meegenomen in de analyse.

Interne documenten van het ministerie van Buitenlandse Zaken
De interne documentatie bevat voornamelijk (concept)nota's, berichtenverkeer, emailverkeer, interne rapportages en interne evaluaties. Het IOB-onderzoeksteam had gedurende de onderzoeksperiode toegang tot een interne samenwerkingsruimte van de Taskforce Cyber en vulde deze documenten aan met berichtenverkeer en bestanden uit BZ-archieven. Deze documenten geven een beeld van de interne besluitvorming, de manier waarop BZ omgaat met internationale ontwikkelingen, de voortgang van activiteiten en de onderlinge verhoudingen tussen BZ en relevante samenwerkingspartners.

Daarnaast is door de Taskforce Cyber ook toegang verleend tot een aantal hoger gerubriceerde interne documenten, en correspondentie daaromtrent, die door IOB-onderzoekers zijn ingezien binnen een beveiligde omgeving.

Kamerstukken en officiële beleidsstukken
Deze openbare bronnen geven voornamelijk inzicht in de kabinetsdoelstellingen op het gebied van cybersecurity en van de gerapporteerde voortgang in bijvoorbeeld de multilaterale overleggen of op het gebied van desinformatie. Dit betreft bijvoorbeeld Kamerbrieven, maar ook het Cybersecuritybeeld Nederland (CSBN) van de NCTV, de Nederlandse Cybersecurity Agenda (NCSA), de Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS) en de Internationale Cybersecuritystrategie 'Digitaal Bruggen Slaan' van het ministerie van Buitenlandse Zaken.

Openbare documenten van (buitenlandse) ngo's, organisaties en overheden
Het internationaal cybersecuritydomein is per definitie grensoverschrijdend en veelomvattend. Derhalve hebben IOB-onderzoekers, afhankelijk van beschikbaarheid en relevantie, openbare documenten van verscheidene binnen het cyberdomein opererende ngo's, organisaties en overheden geanalyseerd.

Internationale academische literatuur
De hierboven besproken literatuurstudie die IOB door de Vrije Universiteit Amsterdam heeft laten

uitvoeren dekt het grootste gedeelte van de beschikbare literatuur over het internationaal cyberbeleid, zoals omschreven in de methodologische verantwoording in de literatuurstudie. Desalniettemin hebben de IOB-onderzoekers in het voortraject maar ook gedurende de studie openbare literatuur geraadpleegd, bijvoorbeeld om te helpen de interviewvragen vorm te geven. Dit betrof, in tegenstelling tot de literatuurstudie van de Vrije Universiteit, geen uitgebreide analyse.

Webinars
IOB-onderzoekers hebben gedurende de onderzoeksperiode diverse online Webinars over actuele cybersecurityvraagstukken, van onder andere de Universiteit Leiden en Instituut Clingendael, bijgewoond. Aantekeningen van voor het evaluatieonderzoek relevante uitspraken en bevindingen zijn door de IOB-onderzoekers meegenomen in de documentanalyse.

Cybernieuws
Het cybersecuritydomein kenmerkt zich doordat het continu in beweging is waardoor ontwikkelingen elkaar in rap tempo opvolgen. Gedurende de onderzoeksperiode hebben de IOB-onderzoekers elkaar op de hoogte gehouden van voor het evaluatieonderzoek relevante gebeurtenissen en nieuwsfeiten. Voor een lange periode deden de onderzoekers dit bijna wekelijks. Voor het onderzoek relevante verslagleggingen van dergelijke gebeurtenissen en nieuwsfeiten zijn door de IOB-onderzoekers meegenomen in de documentanalyse.

Methodologie survey ter aanscherping van de aanbevelingen

In maart 2021 is door de IOB-onderzoekers een korte survey opgesteld als onderdeel van een aanvullende onderzoeksronde waarin het eerste conceptrapport verder werd verbeterd en aangescherpt. De survey was specifiek gericht op het verder concretiseren en aanscherpen van de concept aanbevelingen.

De survey behandelde vier thema's: interdepartementale samenwerking; strategie en doelstellingen; capaciteit bij BZ; en kennis en expertise. De survey bestond uit voornamelijk multiple-choice vragen, enkele open vragen en aanvullende velden voor toelichting.

Respondenten
De aanbevelingensurvey werd uitgestuurd naar een groep ter grootte van 73 personen, waarvan de overgrote meerderheid in een eerder stadium geïnterviewd was. Er is gekozen om internationale experts en partners die waren geïnterviewd niet uit te nodigen voor de survey, omdat de onderwerpen van de surveyvragen niet goed zouden aansluiten bij hun kennis.

Uiteindelijk vulden 45 respondenten de volledige survey in, wat neerkomt op een responspercentage van 62%. Onder de respondenten waren mensen met verschillende rollen (medewerkers bij BZ in Den Haag, ambassademedewerkers, medewerkers van andere ministeries, externe experts en externe partners van BZ) vertegenwoordigd. Er is geen onderscheid gemaakt in de thema's en vragen die de verschillende respondenten te zien kregen. De respondenten werden geïnstrueerd vragen over te slaan wanneer ze de vragen niet goed konden of wilden beantwoorden. Derhalve was geen enkele vraag aangemerkt als 'verplicht' en was er bij alle meerkeuzevragen een 'weet niet / geen mening' optie toegevoegd. De respondenten werden in de uitnodigingsmail uitgenodigd ook aandacht te geven aan de open velden voor verdere toelichting bij een antwoord, waaraan veelal gehoor werd gegeven.

Anoniem en vertrouwelijk

De survey was anoniem. De antwoorden worden vertrouwelijk behandeld, zijn enkel toegankelijk voor het IOB-onderzoeksteam en worden niet gedeeld werden met derden. De surveyresultaten staan op een afgeschermde plek, en worden tot maximaal een jaar na de publicatie van het rapport bewaard. IOB vroeg in de survey niet naar (bijzondere) persoonsgegevens, en noemde zelf geen vertrouwelijke informatie. De survey werd uitgezet via een enquêtetool. In het geval dat respondenten de survey liever per mail wilden invullen, of mondeling antwoorden wilden terugkoppelen, kon dat ook. Deze optie werd hen aangeboden in de uitnodigingsmail, tezamen met een Word-versie van de survey, die respondenten konden terugmailen als ze van de optie gebruikmaakten. Zeven respondenten kozen voor deze optie.

Net als bij de interviews zijn de surveyresultaten alleen gebruikt als bron voor algemene bevindingen in evaluatierapport. Er wordt in het rapport nimmer verwezen naar de surveyantwoorden van specifieke personen en antwoorden zijn niet letterlijk geciteerd.