TERMS OF REFERENCE: EVALUATIE INTERNATIONAAL CYBERSECURITYBELEID

IOB, 14 mei 2020

De directie Internationaal Onderzoek en Beleidsevaluatie (IOB) van het ministerie van Buitenlandse Zaken zal een evaluatie uitvoeren van het internationale cybersecuritybeleid van het ministerie.

Dit Terms of Reference (ToR) document beschrijft het hoofddoel en de aanleiding van de evaluatie, de beleidsachtergrond, de afbakening, onderzoeksvragen en onderzoeksmethoden. Tot slot worden een aantal praktische zaken uiteengezet, zoals de tijdsplanning, risico's, en kwaliteitsbewaking.

1. Doel en aanleiding van het onderzoek

Hoofddoel

Het doel van de evaluatie is om te leren wat goed en minder goed gaat bij het ontwerp en de implementatie van het internationale cybersecuritybeleid van het ministerie van Buitenlandse Zaken, om aanbevelingen te doen over hoe dit beleid indien nodig verbeterd kan worden en/of in de toekomst het beste kan worden vormgegeven.

Aanleiding en belang

Er zijn verschillende redenen waarom dit een opportuun moment is voor een evaluatie van het cybersecuritybeleid.

Volgens het Cybersecurity Beeld Nederland 2019 vindt er een groei plaats in de dreiging van statelijke actoren in het digitale domein en zal deze dreiging in 2021 toenemen als gevolg van de huidige geopolitieke ontwikkelingen. De digitale weerbaarheid van Nederland tegen deze dreiging is volgens het Cybersecurity Beeld niet overal op orde. Hierdoor wordt de vraag hoe het huidige beleid verbeterd kan worden om deze dreiging effectief tegen te gaan steeds belangrijker.[i] Daarbij is ook relevant dat tot op heden nog geen evaluatie is uitgevoerd van het Nederlandse internationale cybersecuritybeleid.

IOB zal deze evaluatie als bouwsteen gebruiken voor de Beleidsdoorlichting van artikel 2[1] van de BZ-begroting, een wettelijke verplichting volgens de Regeling Periodiek Evaluatieonderzoek (RPE). Deze beleidsdoorlichting zal in 2022 worden afgerond.

[1] Veiligheid en stabiliteit

Daarnaast speelt ook dat de Comptabiliteitswet een evaluatie van de VNAC (Versterking van de Nationale Aanpak Cybersecurity) middelen verplicht (zie paragraaf 2 hieronder), en heeft de regering de Kamer toegezegd dat de Nederlandse Cybersecurity Agenda (NCSA) in 2021 geëvalueerd zal worden.[ii] De coördinatie van de evaluatie van de NCSA en VNAC middelen ligt bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), en aangezien het internationale cybersecuritybeleid slechts een klein onderdeel van die evaluatie is, zal het daarin geen prominente rol krijgen. Niettemin zal BZ wel gevraagd worden om lessen en andere informatie aan te leveren, en deze IOB evaluatie zal helpen bij het verzamelen van die lessen.

2. Beleidsachtergrond

Achtergrond cybersecurity

In de huidige Nederlandse samenleving is de digitale infrastructuur van levensbelang: bijvoorbeeld voor schoon water uit de kraan, het betalingsverkeer en om droge voeten te houden.[iii] Verregaande digitalisering[2] zorgt ervoor dat het fysieke domein steeds verder vervlochten raakt met het cyberdomein. Daarmee wordt ook cybersecurity (digitale veiligheid) steeds belangrijker voor de nationale veiligheid. Digitale aanvallen kunnen bijvoorbeeld schade toebrengen aan de nationale veiligheid door sabotage aan de waterwerken of het elektriciteitsnet. Ook op een meer indirecte manier kunnen ze de nationale veiligheid in gevaar brengen, omdat ze bijvoorbeeld kunnen zorgen voor schade aan de economie, het ontwrichten democratische processen, en mensenrechtenschendingen, wat kan leiden tot instabiliteit in de samenleving.

Het kabinet definieert cybersecurity als "het geheel aan maatregelen om schade door verstoring, uitval of misbruik te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. De schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie." [iv]

Een van de problemen rondom cybersecurity is het feit dat het attribueren van cyberaanvallen aan bepaalde staten of andere actoren technisch gezien moeilijk is, want online sporen zijn gemakkelijk te wissen. De mogelijkheden van verscheidene staten om een aanval technisch te attribueren zijn de afgelopen jaren toegenomen, maar tegelijkertijd is de complexiteit van cyberaanvallen toegenomen, wat detectie en attributie weer bemoeilijkt.[v] Voor zowel statelijke als niet-statelijke actoren is het uitvoeren van een

[2] Digitalisering is de overgang van informatie naar een digitale vorm zodat het door computers of andere elektronische apparaten gelezen kan worden (Van Dale woordenboek). De term wordt ook gebruikt om de ontwikkelingen in de samenleving aan te duiden die te maken hebben met het toenemend gebruik van digitale informatie en digitale apparaten.

cyberaanval dus onder andere aantrekkelijk omdat de repercussies voor zo'n aanval vaak klein zijn.[vi]

Eén van de bekendste voorbeelden waarbij de cybersecurity niet op orde was is de NotPetya aanval van 27 juni 2017. Hierbij werd via een 'gat' in de beveiliging van een Oekraïens boekhoudprogramma malware (malicious software)[3] geïnstalleerd dat zich verspreidde over de hele wereld. Onder andere de digitale systemen van APM Terminals in Rotterdam raakten geïnfecteerd waardoor de containerterminals negen dagen stil kwamen te liggen. Dit leidde naar schatting tot tientallen miljoenen euro's schade. Ongeveer een half jaar na de aanval beschuldigde het Britse ministerie van Buitenlandse Zaken, met bijval van andere leden van de Five Eyes Community[4], Rusland er openlijk van achter de aanval te zitten, maar Rusland heeft dit altijd ontkend.[vii]

Verschillende soorten cyberdreiging

Er kunnen ten minste vier verschillende soorten cyberdreiging onderscheiden worden (niet gepresenteerd in volgorde van belangrijkheid):

1) Onopzettelijk veroorzaakte cyberdreigingen. Digitale systemen zijn zo complex geworden en in toenemende mate met elkaar verbonden geraakt dat storing of uitval die per ongeluk plaatsvindt een potentieel grote impact heeft.[viii]

2) Cybercriminaliteit. Dit is een grote dreiging voor Nederlandse bedrijven en individuen, en dus voor de Nederlandse economie. Beroepscriminelen, maar ook zogeheten scriptkiddies[5] of cybervandalen kunnen relatief gemakkelijk middelen bemachtigen om digitale aanvallen uit te voeren die het vertrouwen in de digitale samenleving kunnen schaden.[ix]

3) Cyberdreigingen door groeperingen of individuen met terroristische motieven. Volgens het Cybersecuritybeeld Nederland is deze dreiging op dit moment laag voor Nederland.[x]

4) Digitale dreigingen door statelijke actoren. Staten zetten digitale middelen in voor spionage-, beïnvloedings- en sabotagedoeleinden om zo militaire, economische of andere geopolitieke belangen te dienen. En zelfs zonder middelen in te zetten kunnen staten invloed uitoefenen op besluitvormingsprocessen in een land, wanneer ze expliciet of impliciet dreigen met verstoring of sabotage. Deze statelijke cyberaanvallen en -dreigingen richten zich bijvoorbeeld op vitale bedrijven, publieke instituties en kritieke infrastructuur.[xi] Maar ook valt te denken aan bijvoorbeeld het online verspreiden van desinformatie om zo

[3] Generieke term voor allerlei soorten computervirussen. (Cybersecuritybeeld Nederland CSBN 2019)
[4] De Five-Eyes community is een samenwerkingsverband op het gebied van inlichtingen tussen de Verenigde Staten, het Verenigd Koninkrijk, Australië, Canada en Nieuw-Zeeland.
[5] Een scriptkiddie is een actor met beperkte kennis die hulpmiddelen gebruik die door anderen zijn bedacht en ontwikkeld, voor digitale aanvallen, om kwetsbaarheden aan te tonen of voor de eigen uitdaging. (Cybersecuritybeeld Nederland CSBN 2019)

spanningen binnen of tussen landen te vergroten, of het eigen land in een gunstiger daglicht te stellen.

Deze evaluatie gaat over het cybersecuritybeleid van het ministerie van Buitenlandse Zaken, dat zich voornamelijk richt op de vierde soort dreiging, van staten en aan staten gelieerde actoren. Dit zal verder uiteengezet worden in de onderstaande paragrafen. Hierbij moet worden aangetekend dat staten het uitvoeren van een cyberaanval en/of het ontwikkelen van een digitaal aanvalsmiddel kunnen uitbesteden aan cybercriminelen, waardoor er niet altijd een eenduidig onderscheid valt te maken tussen een statelijke actor en een criminele actor die activiteiten uitvoert voor een staat.

Nederlandse beleidsachtergrond

Het Nederlandse cybersecuritybeleid wordt in 2011 gepresenteerd in de eerste Nederlandse Cybersecurity Strategie, 'Slagkracht door samenwerking'. In dit beleidsdocument ligt de focus op het verbeteren van de samenwerking tussen nationale actoren, maar wordt ook het belang genoemd van internationale samenwerking voor het tegengaan van cybercrime en het creëren van een "level playing field" voor digitale diensten.[xii]

De tweede Nationale Cybersecurity Strategie, 'Van bewust naar bekwaam,' verschenen in 2013, benadrukt het belang van Europese en bredere internationale samenwerking verder, onder andere op het gebied van internationaal recht en internationale normen en standaarden over hoe te handelen in het cyberdomein. Nederland wil een vooraanstaande rol spelen bij het ontwikkelen van zulke regels, en fungeren als een kennisknooppunt op deze thema's.[xiii]

In februari 2017[6] formuleert het kabinet de eerste *Internationale* Cyber Strategie (ICS), 'Digitaal bruggen slaan,' met zes beleidsprioriteiten: Economische groei en duurzame ontwikkeling van het internet; effectieve internet governance; verdere versterking cybersecurity; effectieve bestrijding cybercrime; internationale vrede, veiligheid en stabiliteit; en rechten en internetvrijheid. [7]

In maart 2018 biedt Minister Blok de Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022 (GBVS) aan de Kamer aan. In deze strategie wordt ingegaan op de hybride mix van middelen (conventionele wapens en moderne beïnvloedingstechnieken zoals verspreiding van desinformatie, spionage en cyberaanvallen) die staten inzetten om hun

[6] In reactie op twee onderzoeksrapporten: het AIV rapport 'Het internet, een wereldwijde vrije ruimte met begrensde staatsmacht' (nov 2014) en het WRR rapport 'De publieke kern van het internet. Naar buitenlands internetbeleid' (maart 2015).
[7] Zie Internationale Cyberstrategie 'Digitaal bruggen slaan', 12 februari 2017, p. 9

strategische doelen te bereiken. Ook staan een aantal activiteiten[8] beschreven die de weerbaarheid van Nederland tegen cyberdreigingen moet verhogen. [xiv]

In april 2018 verschijnt de 'Nederlandse Cybersecurity Agenda; Nederland digitaal veilig' (NCSA). De doelstelling van de NCSA luidt: "Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen."[xv]

Om deze doelstelling te behalen worden zeven ambities geformuleerd, waarvan de tweede ambitie grotendeels bij het ministerie van Buitenlandse Zaken is belegd. Deze ambitie luidt: "Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein".

De ambitie kent drie doelstellingen:[9]

1. Nederland is in staat, al dan niet in coalitieverband, onverwijld en adequaat te reageren bij digitale aanvallen door statelijke actoren en beschikt over offensieve capaciteiten die een bijdrage leveren aan het vermogen tot afschrikking.
2. Nederland bevordert de internationale rechtsorde in het digitale domein, waaronder de waarborging van mensenrechten.
3. Nederland draagt bij aan het mitigeren van cyberdreigingen afkomstig van criminele en statelijke actoren, door te investeren in de capaciteitsopbouw van de mondiale cybersecurity keten.

De figuur hieronder presenteert de doelstellingen van het internationale cybersecuritybeleid waar BZ een belangrijke rol speelt,[10] en een uitwerking van deze doelstellingen.[11]

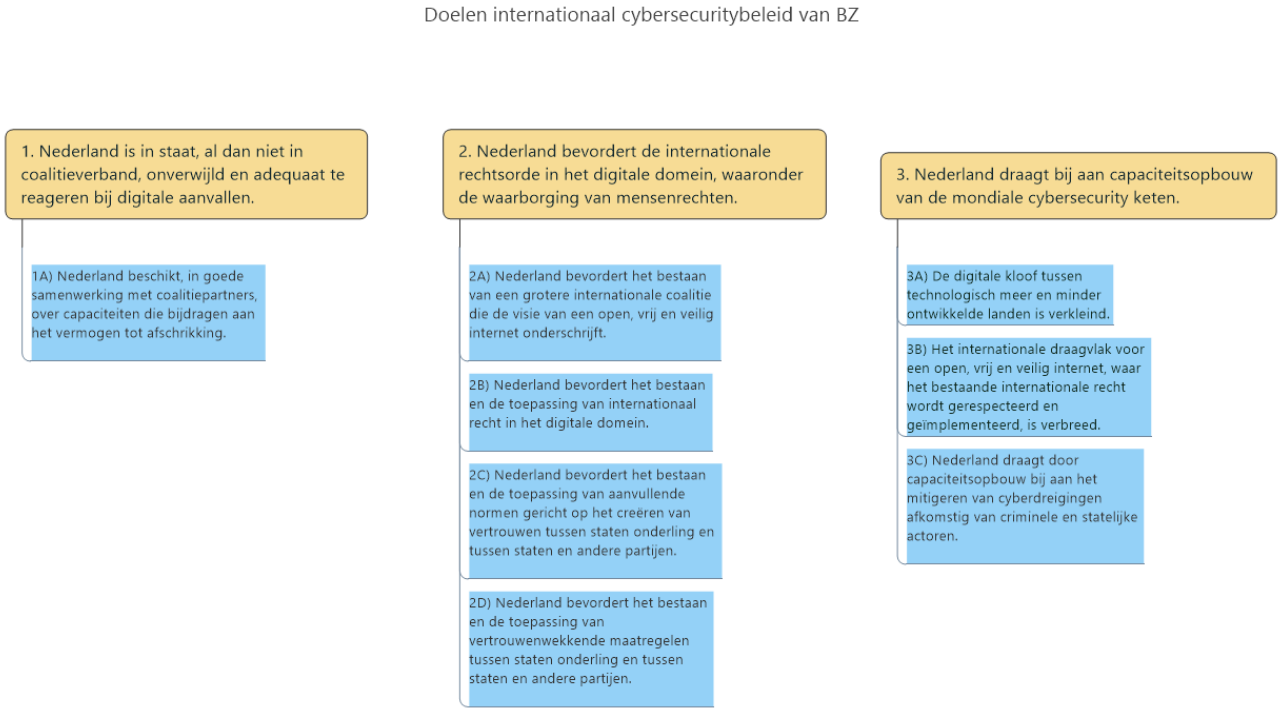
---

[8] Waaronder het investeren in cyberdiplomatie om een internationaal normatief kader voor cyberactiviteiten te ontwikkelen; het investeren in de digitale weerbaarheid van partnerlanden om zo de zwakke schakels in de wereldwijde internetinfrastructuur te versterken; en het investeren in bondgenootschappelijke capaciteiten, zoals binnen de NAVO en de EU, in respons op en ter afschrikking van cyberaanvallen en cyberspionage.

[9] Nederlandse Cybersecurity Agenda, p. 23.

[10] De tweede helft van doelstelling 1, dat Nederland "beschikt over offensieve capaciteiten die een bijdrage leveren aan het vermogen tot afschrikking" valt voornamelijk onder de verantwoordelijkheid van het ministerie van Defensie. In de figuur hieronder is dit daarom weggelaten uit doelstelling 1. Wel noemt de figuur meer algemeen "capaciteiten die bijdragen aan het vermogen tot afschrikking". Hieronder valt de ontwikkeling van nationale en internationale strategische kaders ten behoeve van een respons op digitale aanvallen. In deze kaders zijn verschillende instrumenten opgenomen, waaronder (publieke) attributie, andere diplomatieke en politieke reacties en de inzet van offensieve capaciteiten.

[11] De figuur is gebaseerd op de doelstellingen zoals deze zijn weergegeven in de Nederlandse Cybersecurity Agenda op p.23. Het is mogelijk dat tijdens het onderzoek deze doelstellingen en een uitwerking daarvan verder aangescherpt en gewijzigd zullen worden.



Om de drie doelstellingen te behalen ontplooit Nederland verschillende activiteiten, die grofweg kunnen worden ingedeeld in de volgende categorieën:

- Diplomatie (waaronder de diplomatieke respons bij cyberaanvallen) in multilaterale fora zoals de VN, de OVSE, de EU en de NAVO.
- Diplomatie in multistakeholder fora zoals het Global Forum on Cyber Expertise (GFCE), het Internet Governance Forum (IGF) en de Freedom Online Coalition (FOC).
- Diplomatieke bilaterale relaties en ad-hoc coalities van gelijkgezinde landen, al dan niet ter voorbereiding op discussies in de hiervoor genoemde fora.
- Financiële steun aan (internationale) ngo's en andersoortige multilaterale en multistakeholderinitiatieven, zoals het Global Forum on Cyber Expertise (GFCE) en de Freedom Online Coalition (FOC) en aan projecten zoals de Global Commission on the Stability of Cyberspace (GCSC) en The Hague Norms Project.

Organisatorische opzet cybersecurity binnen het ministerie van Buitenlandse Zaken

Binnen BZ is het eerste aanspreekpunt voor het internationale cybersecuritybeleid de Task Force Cyber (TFC) die onder de Directie Veiligheidsbeleid (DVB) valt. De TFC wordt momenteel uitgebreid van 7,5 fte naar 9,5 fte. Deze personele bezetting is inclusief 2 fte die vanuit de afdeling Mensenrechten en Politiek Juridische VN Zaken van de Directie Multilaterale Organisaties en Mensenrechten (DMM) zijn gedetacheerd aan de Task Force Cyber. Ook is er 1 fte vanuit de Directie Juridische Zaken (DJZ) gedetacheerd aan de TFC.

De Task Force is ingedeeld in drie clusters. De medewerkers werken flexibel voor meerdere clusters en de fte's zijn niet vast aan een cluster gekoppeld.

Hier volgt een overzicht van de drie clusters en hun verantwoordelijkheden, zoals omschreven in het BZ VNAC bestedingsplan dat is goedgekeurd door de managementraad.

1) Internationale veiligheid, respons en internationaal recht. Dit cluster verzorgt de inzet in de eerder genoemde multilaterale en multi-stakeholder fora (zoals EU, VN, IGF) en ad-hoc coalities om het internationaal normatief en juridisch kader voor het digitale domein te versterken, waaronder de bescherming van mensenrechten. Onderdelen daarvan zijn de internationale samenwerking met like-minded landen en capaciteitsopbouw op het vlak van internationaal recht die plaatsvindt in de context van het *Hague Process.* Dit cluster is ook verantwoordelijk voor het ontwikkelen van een diplomatieke respons op verstorende of destructieve cyberoperaties van statelijke actoren, en voor de internationaalpolitieke aspecten van nationale cybersecuritybeleidskwesties (zoals 5G en verbinding economische veiligheid en cybersecurity).

2) Partnerschappen voor een open, veilig en vrij internet. Dit cluster coördineert de inzet van de posten op het terrein van cybersecurity, en richt zich op het creëren van partnerschappen met andere landen om de Nederlandse visie van een open, veilig en vrij internet te verspreiden. Hierbij wordt samengewerkt met DMM. Op iedere post wordt een contactpersoon voor cybersecurity aangewezen. Bij een aantal posten wordt cyberexpertise op een meer structurele manier toegevoegd door 'cyberdiplomaten' die functie-inhoudelijk worden aangestuurd door de TFC.[12]

3) Capaciteitsopbouw. Dit cluster zet zich in om de digitale kloof tussen meer en minder ontwikkelde landen te verkleinen door bijvoorbeeld expertise-uitwisseling. Dit cluster werkt onder andere samen met het Bureau Internationale Samenwerking (BIS) in het kader van de Digitale Agenda voor Buitenlandse Handel en Ontwikkelingssamenwerking.

Tevens is een ambassadeur voor Veiligheid en Cyber (AMAD,[13] die rechtstreeks onder de SG valt) actief in het onderhouden van partnerschappen en betrokken bij de inbreng in de verschillende fora genoemd onder 1).

Andere betrokken departementen

Een belangrijke speler bij het Nederlandse cybersecuritybeleid is het ministerie van Justitie en Veiligheid (J&V) waarvan de Nationaal Coördinator voor Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC) de belangrijkste betrokken organisaties zijn. Zij houden zich bijvoorbeeld bezig met nationale regelgeving ten aanzien van cybercriminaliteit en (de bevoegdheden van) opsporings- en veiligheidsdiensten, en het coördineren van de aanpak van cyberincidenten.

[12] Er zijn cyberdiplomaten actief op de volgende posten: Washington, New York, Geneve, Brussel (NAVO/EU), Moskou, Peking en Singapore
[13] Ambassadeur in Algemene Dienst

Het ministerie van Economische Zaken en Klimaat (EZK) zet zich in om de economische kansen die digitalisering en nieuwe technologieën bieden te verzilveren, maar houdt zich ook bezig met veiligheidsaspecten, zoals veiligheidseisen waaraan software en hardware (bijvoorbeeld servers en modems) moeten voldoen.

Het ministerie van Defensie draagt bij aan de digitale veiligheid door cyberaanvallen te verstoren of af te schrikken, en is verantwoordelijk voor de digitale verdediging tegen geavanceerde digitale dreiging in het geval van een militair conflict. Defensie heeft verschillende cyberstrategieën gepubliceerd[14] die ten doel hebben de cybercapaciteiten te vergroten. Zo is er een Defensie Cyber Commando opgericht en is het Defensie Computer Emergency Response Team[15] (DefCERT) versterkt.

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD), onderdeel van het ministerie van Defensie, speelt samen met de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), die valt onder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), een rol in technische attributie; het vaststellen wie de actor achter een cyberaanval is.

Budget

De toegenomen dreiging van statelijke en criminele actoren in het digitale domein zorgde er de afgelopen jaren voor dat er bij het kabinet meer aandacht kwam voor het nationale en internationale cybersecuritybeleid. Hiertoe heeft het kabinet in het regeerakkoord van 2017 in totaal 95 miljoen euro beschikbaar gesteld, de zogeheten VNAC-middelen (Versterking van de Nationale Aanpak Cybersecurity).[xvi] Het beleid dat verbonden is aan de besteding van deze financiële middelen staat beschreven in de eerder genoemde NCSA.

Een (relatief klein) deel van de implementatie van de NCSA en van de VNAC-middelen ligt bij BZ: BZ ontvangt in deze kabinetsperiode EUR 1 miljoen in 2019 en structureel EUR 2 miljoen.

Naast de VNAC-middelen is er ook geld gereserveerd voor cybersecurity onder artikel 2.2. van de BZ-begroting ('Bestrijding en terugdringen van internationaal terrorisme en andere vormen van internationale criminaliteit.') Het is momenteel nog onduidelijk hoeveel middelen er exact zijn besteed aan het cybersecuritybeleid van BZ in de afgelopen 5 jaar; dit zal nader worden onderzocht.

[14] Defensie Cyber Strategie 2018, Kamerbrief Actualisering Defensie Cyber Strategie 23 feb 2015

[15] Het team moet ervoor zorgen dat militaire operaties geen hinder ondervinden en de informatiesystemen van Defensie betrouwbaar zijn. Hiervoor moet DefCERT cyberdreigingen op tijd zien; onderzoeken hoe groot de dreiging is; en zorgen dat de dreiging vermindert of verdwijnt. Daarnaast kan DefCERT ook civiele autoriteiten ondersteunen bij de coördinatie van cyberdreigingen. (bron: Defensie)

3. Afbakening

Hieronder staat meer informatie over wat wel en niet binnen de reikwijdte van het onderzoek valt. Hierbij moet worden aangetekend dat, net als bij elk IOB-onderzoek, het mogelijk is dat gedurende het onderzoek de afbakening ietwat aangepast dient te worden omdat gaandeweg naar voren komt dat een onderwerp toch meer (of minder) relevant blijkt voor het beantwoorden van de onderzoeksvragen dan van tevoren voorzien.

1. **Internationaal beleid:** De evaluatie gaat over het Nederlandse *internationale* cybersecuritybeleid, en niet over de vele andere aspecten van het Nederlandse cybersecuritybeleid. Het internationale en nationale cybersecuritybeleid zijn echter in de praktijk met elkaar verweven, dus waar relevant zullen ook nationale cybersecurity aspecten worden meegenomen.

2. **Dreiging van statelijke actoren:** de evaluatie gaat primair over het cybersecuritybeleid gericht tegen dreiging van staten en aan staten gelieerde actoren. De evaluatie kan echter ook aspecten van het beleid gericht op dreigingen van terroristische of private criminele actoren meenemen indien deze raken aan het cybersecuritybeleid van BZ.

3. **Relatie cybersecuritybeleid BZ met andere aspecten beleid:** De evaluatie richt zich op het internationale cybersecuritybeleid voor zover dat valt onder de verantwoordelijkheid van het ministerie van Buitenlandse Zaken, en niet op aspecten van het internationale cybersecuritybeleid die primair onder de verantwoordelijkheid van andere ministeries liggen, zoals de Nederlandse operationele offensieve en defensieve cybercapaciteiten. Waar relevant zal de relatie tussen BZ en andere aspecten van het internationale cybersecuritybeleid echter wel worden meegenomen in dit onderzoek, evenals de wisselwerking met andere ministeries. Hieronder wordt de afbakening ten opzichte van enkele aspecten van het internationale cybersecurity beleidsterrein verder toegelicht:
    a. <u>Economische aspecten:</u> Het benutten van de economische kansen die digitalisering biedt valt grotendeels onder de verantwoordelijkheid van het ministerie van EZK en zal niet meegenomen worden in de evaluatie. Echter, bij veiligheidsaspecten van economische dossiers die een internationale dimensie hebben (denk bijv. aan het 5G dossier) kan de rol die BZ hierin vervult wel meegenomen worden.
    b. <u>Mensenrechten:</u> De eerste doelstelling van ambitie twee van de NCSA is dat Nederland de internationale rechtsorde in het digitale domein bevordert, waaronder de waarborging van mensenrechten (p. 23). Het gaat hierbij met name om mensenrechten als vrijheid van meningsuiting en vrijheid van vergadering, die aansluiten bij het Nederlandse streven naar een open en vrij internet. Dit is niet alleen een streven an sich, maar hangt ook samen met veiligheid omdat het inperken van de vrijheid van mensen online gevolgen kan hebben voor de stabiliteit van landen. Dit omdat het internet een middel is voor sociale mobilisatie,

en andersom gebruikt kan worden door staten als een repressiemiddel. Daarnaast kan het inperken van de vrijheid online gevolgen hebben voor het goed functioneren van het internet, wat van belang is voor de bredere stabiliteit van de Nederlandse samenleving. De doelstelling omtrent het waarborgen van mensenrechten online en het streven naar een open en vrij internet zal daarom worden meegenomen in de evaluatie.

c. Desinformatie: Het tegengaan van digitale beïnvloedingstechnieken die staten inzetten om hun geopolitieke doelen in het buitenland na te streven, zoals het verspreiden van desinformatie en 'deep fakes'[16], valt onder de Nederlandse doelstelling de internationale rechtsorde in het digitale domein te bevorderen en wordt meegenomen in deze evaluatie. Ook op dit beleidsdossier vindt veel samenwerking plaats met andere departementen zoals BZK en VenJ, en zal de evaluatie zich primair richten op de rol van BZ op dit beleidsterrein.

d. Capaciteitsopbouw: Zoals hierboven is aangegeven gaat de derde doelstelling van ambitie twee van de NCSA over capaciteitsopbouw: het helpen van andere landen om hun cyberveiligheid op orde te krijgen. Deze doelstelling zal worden meegenomen in de evaluatie. Echter, BZ (met name vanuit de directies DSH en DMM) financiert ook andere cybergerelateerde projecten die als 'capaciteitsopbouw' kunnen worden bestempeld, maar die niet direct te maken hebben met cybersecurity, zoals het vergroten van de toegang van de bevolking tot het internet in ontwikkelingslanden. Dit soort projecten worden niet meegenomen in de evaluatie.

4. **Niet de cybersecurity van het ministerie zelf**: hoewel het versterken van de digitale veiligheid van de Rijksoverheid een speerpunt van het beleid is (bijvoorbeeld verwoord in de tweede Nationale Cybersecurity Strategie (NCSS 2) zal de evaluatie niet ingaan op de cybersecurity van het ministerie van BZ zelf.

2015 - 2020: De evaluatie neemt 2015 als startpunt, toen de Task Force Cyber werd opgericht na de Global Conference on Cyber Space (GCCS). Eerder was er ook al aandacht voor internationaal cyberbeleid (zie paragraaf 2) maar na de GCCS en de oprichting van de Task Force Cyber is er veel veranderd.

Geen impactevaluatie

De evaluatie zal *niet* proberen de impact van het beleid te meten, omdat het niet mogelijk is precies vast te stellen in hoeverre het Nederlandse internationale cybersecuritybeleid bijdraagt aan het verwezenlijken van de drie doelen: het bevorderen van de internationale rechtsorde in het digitale domein, het vermogen adequaat te reageren bij digitale aanvallen, en capaciteitsopbouw van de mondiale cybersecurity keten. Dit is onder andere omdat internationale ontwikkelingen en acties van andere staten, bedrijven en andere actoren ook een rol spelen in het al dan niet verwezenlijken van deze doelen, en het niet mogelijk is om de huidige situatie te vergelijken met hoe de situatie zou zijn geweest zonder de Nederlandse inspanningen. Daarnaast zijn een aantal van de doelen moeilijk te

[16] Het manipuleren van audio en/of video. (CSBN 2019)

meten,[17] en is er een gebrek aan betrouwbare, verifieerbare datasets en andere gegevens.[xvii]

Een evaluatie kan in een dergelijke situatie beter beogen een uitspraak te doen over de waarschijnlijkheid dat het beleid bijdraagt aan het verwezenlijken van de doelstellingen door te kijken naar alle stappen in de 'beleidstheorie' van het beleid (het plan van hoe het beleid de gestelde doelen zal behalen) en over wat er goed of minder goed gaat in de organisatie en uitvoering van dit plan. De volgende paragraaf beschrijft de onderzoeksvragen die hiervoor zijn opgesteld.

4. Onderzoeksvragen

Hoofdvraag

Wat gaat er goed en minder goed bij het ontwerp en de implementatie van het internationale cybersecuritybeleid van het ministerie van Buitenlandse Zaken over de periode 2015-2020, en welke aanbevelingen kunnen op grond hiervan worden geformuleerd over hoe dit beleid verbeterd kan worden en/of in de toekomst het beste kan worden vormgegeven?

Deelvragen

a) Context en probleemschets

1. Wat zijn de belangrijkste ontwikkelingen in de afgelopen jaren op het gebied van de digitale dreiging van statelijke en daaraan gelieerde actoren, in het bijzonder richting Nederland?
2. Wat zijn de belangrijkste ontwikkelingen in de afgelopen jaren op het gebied van internationaal cybersecuritybeleid gericht tegen de dreiging van statelijke en daaraan gelieerde actoren? (voor zover direct relevant voor Nederland)
3. Wat zijn de verwachte ontwikkelingen op het gebied van de dreiging van statelijke en daaraan gelieerde actoren in de komende vijf jaar?

b) Hoe ziet het beleid er uit?

4. Hoe ziet het internationale cybersecuritybeleid van BZ gericht op het tegengaan van de digitale dreiging van statelijke en daaraan gelieerde actoren eruit?
    a. Wat is het ultieme doel en wat zijn de hier van afgeleide beleidsdoelstellingen?
    b. Wat zijn de belangrijkste activiteiten die zijn gepland en worden uitgevoerd om deze beleidsdoelstellingen te bereiken?

[17] Men weet bijvoorbeeld pas in hoeverre een land daadwerkelijk in staat is adequaat te reageren op een digitale aanval als er een aanval is geweest, en men zich bewust is van deze aanval, terwijl cyberaanvallen vaak heimelijk zijn.

c. Wat zijn de middelen en de organisatorische opzet binnen BZ om deze activiteiten uit te voeren?

c) Logica beleidstheorie

5. In hoeverre kan (volgens betrokkenen, experts en beschikbare literatuur) logischerwijs verwacht worden dat de organisatorische opzet en ontplooide activiteiten bij zullen dragen aan het behalen van het beoogde ultieme doel en de hier van afgeleide beleidsdoelstellingen van BZ?
   a. In hoeverre en waarom kan verwacht worden dat de beoogde beleidsdoelstellingen bij zullen dragen aan het ultieme doel?

   Bij vraag 5a zal ook worden verkend of BZ een rol zou moeten spelen ten aanzien van beleidsdoelstellingen die niet in de huidige beleidstheorie zijn opgenomen, maar mogelijkerwijs wel instrumenteel zijn voor het behalen van het ultieme doel (mogelijke blinde vlekken).

   b. In hoeverre en waarom kan verwacht worden dat de ontplooide activiteiten bij zullen dragen aan de beoogde beleidsdoelstellingen?
   c. In hoeverre en waarom kan verwacht worden dat de organisatorische opzet bij zal dragen aan de beoogde beleidsdoelstellingen?

d) Evaluatie van activiteiten

6. In hoeverre behalen de activiteiten gericht op beleidsontwikkeling, beleidsbepaling en beleidsimplementatie hun beoogde resultaten? Waarom worden deze beoogde resultaten al dan niet behaald?

   Bij vraag 6 is het zoals eerder gesteld niet mogelijk om de impact ten aanzien van de beleidsdoelstellingen te meten, maar is het wellicht wel mogelijk om inzicht te verschaffen in kleine resultaten van activiteiten gericht op beleidsimplementatie. Indien ook dit niet mogelijk blijkt, zal dat in de methodologische verantwoording van het rapport worden aangegeven.

7. In aanvulling op vraag 6: Zijn er andere zaken die goed en minder goed gaan bij het uitvoeren en organiseren van de activiteiten waaruit lessen kunnen worden getrokken voor de toekomst?

Bij vraag 7 zal in ieder geval worden gekeken naar de interdepartementale afstemming; de afstemming in beleid met en tussen verschillende internationale actoren; de samenwerking tussen BZ en de private sector en nationale organisaties; in hoeverre er duidelijkheid is bij betrokkenen over de te behalen doelen en de strategie om deze doelen te bereiken; in hoeverre BZ goed is uitgerust voor het formuleren van beleid in een dynamische omgeving met snelle technologische ontwikkelingen; in hoeverre BZ goed is uitgerust om adequaat te reageren op toekomstige beleidsthema's waarvan het op dit moment waarschijnlijk is dat deze bij het ministerie belegd zullen gaan worden.

Bij vraag 6 en 7 zullen we in het onderzoek niet per definitie in evenveel detail kijken naar alle activiteiten. Dit zal afhangen van welke er tijdens het onderzoek naar voren komen als de meest relevante voor het formuleren van lessen, op basis van onder andere wat

geïnterviewden aandragen als voorbeelden van succesvolle of juist niet succesvolle inzet, beleidsmatige prioriteiten, en de relatieve financiële en personele inzet.[18]

e) Aanbevelingen

8. Welke aanbevelingen volgen voor het toekomstige cybersecuritybeleid van BZ?

5. Onderzoeksmethoden

Voor het beantwoorden van de onderzoeksvragen zal zoveel mogelijk gebruik worden gemaakt van triangulatie: het gebruiken van verschillende typen bronnen voor het beantwoorden van een onderzoeksvraag om vast te stellen of bevindingen hieruit overeenkomen, en daarmee hun betrouwbaarheid te verhogen. De volgende methoden en bronnen zullen gebruikt worden voor het onderzoek:

Interviews

Interviews met betrokkenen, zoals:

Medewerkers van het ministerie van Buitenlandse Zaken:

- Task Force Cyber (TFC)
- Directie Veiligheidsbeleid (DVB)
- Directie Multilaterale Organisaties en Mensenrechten (DMM)
- Bureau Internationale Samenwerking (BIS)
- Directie Integratie Europa (DIE)
- Directie Juridische Zaken (DJZ)
- Directie Internationale Marktordening en Handelspolitiek (IMH)
- Relevante regiodirecties
- Relevante ambassades

Medewerkers van andere departementen:

- Ministerie van Justitie en Veiligheid (JenV): NCTV - Nationaal Cyber Security Centre, DG Rechtspleging en Rechtshandhaving
- Ministerie van Economische Zaken en Klimaat (EZK): Task Force Economische veiligheid, Directie Kennis en Innovatie
- Ministerie van Binnenlandse Zaken (BZK): AIVD
- Ministerie van Defensie (DEF): Cyber Commando, MIVD, DefCERT

[18] Uit verkennende gesprekken kwamen vooralsnog de suggesties naar voren dat extra aandacht in het onderzoek in ieder geval besteed zou moeten worden aan de EU cybersecurity toolbox, waaronder EU cybersanctieregime, ad-hoc coalities en VN diplomatieke bijdragen (GGE en UN open-ended working group) en het Global Forum on Cyber Expertise (GFCE).

Betrokkenen bij door Nederland gesponsorde of mede-opgerichte organisaties en raden, zoals:

- Global Forum on Cyber Expertise (GFCE)
- Cyber Security Raad (CSR)
- Freedom Online Coalition (FOC)
- Digital Defenders Partnership (DDP)
- Organization of American States (OAS)

Betrokkenen uit andere landen bij diplomatieke fora en internationale organisaties die een rol spelen in het Nederlandse internationale cybersecuritybeleid, zoals:

- VN: UN Group of Governmental Experts GGE on the Developments in the Field of Information and Telecommunications in the Context of International Security, Internet Governance Forum en de UN Open Ended Working Group.
- NAVO: The NATO Cooperative Cyber Defence Centre of Excellence
- International Telecommunication Union (ITU).
- EU: EDEO
- OVSE
- Andere partnerlanden: de Verenigde Staten, Groot-Brittannië, Duitsland, Estland

Overige experts

- Zoals uit de wetenschap, denktanks, bedrijfsleven en ngo's

Documentanalyse

Openbare overheidsdocumenten
Analyse van openbare overheids- en beleidsdocumenten, zoals kamerstukken en beleidsbeschrijvingen.

Interne documenten
Interne documenten van de Task Force Cyber en andere relevante directies binnen het ministerie van Buitenlandse Zaken, zoals interne (concept) beleidsdocumenten, communicatie, procedurevoorschriften en andere stukken van regelende aard, verslagen van overleg- en stuurgroepen, interne evaluatierapporten, interne werkafspraken, ambassaderapporten, rapporten van projectleiders, etc. (zie paragraaf 6 hieronder)

Literatuuronderzoek

Naast analyse van interne documenten zal publiekelijk beschikbare secundaire literatuur, waaronder wetenschappelijke literatuur, worden bestudeerd. Afhankelijk van de omvang van de beschikbare wetenschappelijke literatuur zal deze studie worden uitbesteed aan een externe onderzoeker of door een IOB-onderzoeker worden gedaan.

6. Toegang tot documenten en omgang met gerubriceerde informatie

Conform het besluit van de Minister van Buitenlandse Zaken van 27 mei 2019, nr. MinBuZa.2019.3926-31, dient IOB volledig en ongehinderd toegang te ontvangen tot alle gegevens waarover de beleidsdirecties en uitvoeringsorganisaties beschikken.

Dit geldt ook voor staatsgeheime of anderszins gerubriceerde documenten, mits de betrokken onderzoekers de benodigde veiligheidsscreening hebben ondergaan. De aan dit onderzoek toegewezen IOB-onderzoekers hebben allen een veiligheidsonderzoek ondergaan voor toegang tot informatie op het niveau NATO COSMIC TOP SECRET / EU TOP SECRET.

Gerubriceerde geschreven bronnen zullen waar nodig alleen op stand-alone computers of in een beveiligde omgeving binnen het ministerie ingezien worden. Staatsgeheime bronnen zullen niet met naam en toenaam geciteerd worden in het onderzoeksrapport. Bovendien zal aan de vertegenwoordigers van de betrokken beleidsdirecties in de referentiegroep worden gevraagd de onderzoekers te attenderen op mogelijk uit veiligheidsoverwegingen gevoelige verwijzingen in het conceptrapport.

7. Onderzoeksethische en andere risico's

Risico's	Mitigerende acties
1. Toegang tot documenten: cybersecurity is een beleidsgebied waarin veel documenten gerubriceerd zijn.	• De betrokken onderzoekers hebben een veiligheidsscreening ondergaan waardoor zij toegang hebben tot gerubriceerd materiaal op het niveau NATO COSMIC TOP SECRET / EU TOP SECRET.
2. Vanwege de gevoelige aard van het onderwerp is het mogelijk dat geïnterviewden, bijvoorbeeld medewerkers van BZ of internationale partners, zich niet vrij voelen om eerlijk en open informatie met de onderzoekers te delen.	• Alle interviews zullen volledig vertrouwelijk worden afgenomen, en geïnterviewden kunnen anoniem aan de interviews meedoen. • Mensen die vanuit verschillende achtergronden en posities bij het beleid betrokken zijn zullen worden geïnterviewd, zodat vragen van veel verschillende kanten kunnen worden belicht. • Bevindingen uit interviews zullen worden vergeleken met bevindingen uit andere soorten bronnen.
3. Veel beleidsontwikkeling zal niet in detail vastgelegd zijn in documenten. Dit maakt het moeilijker om bevindingen uit interviews te vergelijken met bevindingen uit andere soorten bronnen.	• IOB zal dit als beperkende factor meenemen in de methodologische verantwoording in het rapport. • Tevens zal het daarom wellicht nodig zijn om meer mensen met verschillende achtergronden te interviewen om zo de betrouwbaarheid van de bevindingen die volgen uit interviews te verhogen.

4. Het is mogelijk dat onderzoekers achter bevindingen komen waarvan publicatie de veiligheid of de goede werking van het cybersecuritybeleid in de weg zal staan.	• In de eerste plaats zullen de onderzoekers alleen informatie publiceren die daadwerkelijk relevant is voor het beantwoorden van de onderzoeksvragen, niet toevallige ontdekkingen die ook interessant zijn. • Daarnaast zullen medewerkers van de Task Force cyber die deelnemen in de referentiegroep de mogelijkheid krijgen om aan te geven of bepaalde bevindingen of verwijzingen naar bepaalde bronnen een gevaar vormen voor de staatsveiligheid. • Indien noodzakelijk voor de staatsveiligheid kunnen de onderzoekers in overleg besluiten om bepaalde risicovolle bevindingen niet te publiceren en alleen in een mondelinge technische briefing achter gesloten deuren aan leden van de Tweede Kamer toe te lichten.
5. Cyberbeleid en -diplomatie is een relatief nieuw beleidsterrein. Dit betekent dat de beschikbare wetenschappelijke literatuur beperkt zal zijn, en er niet bijvoorbeeld al veel afgeronde systematische reviews beschikbaar zijn over wat al dan niet werkt in internationaal cybersecuritybeleid.	• Het onderzoek zal om deze reden ook afgaan op interviews met experts • Waar mogelijk kunnen parallellen getrokken worden met andere veiligheidsterreinen, zoals non-proliferatie. • Indien nodig zal geaccepteerd moeten worden dat bepaalde onderzoeksvragen niet onomstotelijk beantwoord kunnen worden met de beschikbare kennis, en zal dit aangegeven worden in het rapport.
6. De NCTV heeft toegezegd om een evaluatie van de NCSA te laten uitvoeren en in 2021 af te ronden. Het WODC is gevraagd hiervoor een methodologie te ontwikkelen. Ook is er een evaluatie van de VNAC middelen toegezegd. Het is mogelijk dat de IOB-cybersecurityevaluatie ongeveer tegelijkertijd klaar is als de evaluatie van de NCSA/VNAC, wat tot verwarring kan leiden.	• Gesprekken met betrokkenen bij de NCSA/VNAC evaluatie tonen bovendien aan dat het erg onwaarschijnlijk is dat het internationale aspect veel aandacht zal krijgen in die evaluatie, omdat BZ slechts een klein deel van de VNAC middelen krijgt en een relatief kleine rol speelt in de NCSA. • Niettemin zullen IOB-onderzoekers tussentijds contact onderhouden met het WODC en een eventuele andere partij aan wie de evaluatie van de NCSA zou kunnen worden uitbesteed, om duplicatie in de focus van de twee onderzoeken te voorkomen. • De IOB-evaluatie biedt dan ook niet alleen een risico maar ook kansen aan de TFC/BZ: - IOB streeft ernaar dat de evaluatiebevindingen door de TFC gebruikt kunnen worden om te voldoen aan informatieverzoeken voor de NCSA/VNAC evaluatie. - IOB is een onafhankelijke partij die evaluaties opstelt op basis van wetenschappelijke methoden. BZ is daardoor in staat hoogwaardige en betrouwbare input te leveren voor de NCSA/VNAC-evaluatie over lessen, en wat er nodig is voor toekomstig beleid. - De inspanningen van BZ zullen in de nationaal georiënteerde evaluatie van de NCSA/VNAC waarschijnlijk minder sterk naar voren komen; de IOB-evaluatie zal hier een goede aanvulling op zijn.

7. Gezien de uitbraak van Covid-19 en de daarbij horende maatregelen kunnen de interviews waarschijnlijk niet gedurende de hele onderzoeksperiode fysiek worden afgenomen. Gezien de vertrouwelijke aard van het onderwerp, zou dit een probleem op kunnen leveren voor de openheid waarmee respondenten de interviewvragen zullen beantwoorden tijdens een virtueel gesprek.	• Waar mogelijk worden interviews waarvan te verwachten is dat deze minder waardevolle informatie opleveren indien die virtueel worden afgenomen uitgesteld. • We zullen werken met maatwerkinterviews waarbij we per respondent bekijken waar hij/zij zich comfortabel bij voelt. • We hopen binnen afzienbare tijd beschikking te hebben over een veilig virtueel communicatiemiddel. • Wanneer de Covid-19 crisis negatieve gevolgen heeft voor het onderzoek, zullen we dit expliciet benoemen als limitatie in de methodologische verantwoording van het rapport.

8. Betrokkenen

Onderzoeksteam

IOB heeft de penvoering en is eindverantwoordelijk voor de vaststelling van de tekst van het rapport. De hoofdmedewerker vanuit IOB voor het onderzoek is Wendy van der Neut. Ook zullen een externe consultant, Gijs van Loon, en een stagiaire, Anouk Pietersen, meewerken aan het onderzoek. Indien nodig kunnen er andere onderzoekers aangetrokken worden voor het onderzoek. Alle onderzoekers binnen IOB die deel uit zullen maken van het onderzoeksteam, inclusief de bovengenoemde externe consultant en stagiaire, zullen een veiligheidsonderzoek ondergaan.

Referentiegroep

De referentiegroep heeft als doel de kwaliteit van het onderzoek en het gevoel voor de (beleids)context te bewaken, en bestaat uit medewerkers van de betrokken beleidsdirectie en externe experts. Zij adviseren over de ToR, uitvoering van het onderzoek en concept-conclusies en -aanbevelingen. Tevens kunnen de referentiegroepleden vanuit hun expertise over cybersecurity de onderzoekers bijstaan met meer praktische adviezen, en wijzen op goede informatiebronnen.

In de referentiegroep nemen deel, als vertegenwoordigers van de betrokken beleidsafdeling:

- Jan-Jaap Gerards, Sr beleidsmedewerker van de Task Force Cyber
- Guus van Zwoll, Sr beleidsmedewerker van de Task Force Cyber

Daarnaast nemen er drie externe onafhankelijke wetenschappelijke adviseurs plaats in de referentiegroep:

- Prof. dr. Bibi van den Berg, Universiteit Leiden
- Prof. dr. Terry Gill, Universiteit van Amsterdam
- Drs. Sico van der Meer, Instituut Clingendael en Technische Universiteit Eindhoven

Interne klankbordgroep

Naast de referentiegroep is er ook een klankbordgroep, met een aantal IOB-onderzoekers die niet direct betrokken zijn bij het onderzoek. De klankbordgroep komt elke zes weken (digitaal) bijeen en geeft feedback op en suggesties voor de onderzoeksaanpak, voortgang, dilemma's, concept teksten, etcetera. De leden zijn Anne Bakker, Kirsten Lucas en Paul Westerhof.

De referentiegroep en klankbordgroep worden beide voorgezeten door Arjan Schuthof van IOB.

9. Tijdsplanning

Hieronder staat een concept-tijdsplanning. De precieze tijdsplanning zal afhankelijk zijn van een aantal factoren, waaronder coronamaatregelen, personele bezetting, de snelheid waarmee toegang tot de benodigde documenten kan worden gekregen, en de beschikbaarheid van interviewrespondenten in de zomermaanden.

Datum	Wat?
Februari 2020	• Schrijven ToR • Eind februari ToR bespreken met TFC • Onderzoeksplanning opstellen
Maart 2020	• 5 maart ToR voorleggen aan klankbordgroep • Toegang krijgen tot documenten TFC
April 2020	• ToR voorleggen aan referentiegroep • Presentatie onderzoek bij stafoverleg TFC • Begin analyse interne documenten
Mei 2020	• Vaststelling ToR • Interviews, documentanalyse
Juni-juli 2020	• Interviews, documentanalyse en literatuuronderzoek
Augustus-september 2020	• Interviews, documentanalyse en literatuuronderzoek
Oktober 2020	• Beginnen met bevindingen schrijven • Aanbesteding externe onderzoeker voor aanscherpen aanbevelingen
November-December 2020	• Bevindingen schrijven • Onderzoek aanscherpen aanbevelingen

Januari-februari 2021	• Onderzoek aanscherpen aanbevelingen
Maart 2021	• Eerste versie rapport af (bevindingen over aanbevelingen toevoegen)
April 2021	• Klankbordgroep en referentiegroepbijeenkomst over eerste versie rapport
Mei 2021	• Herschrijven rapport
Juni-juli 2021	• Onvoorziene uitloop

10. Rapport

Het rapport zal in de Nederlandse taal worden geschreven. Mocht het noodzakelijk zijn met het oog op de nationale veiligheid, kunnen de onderzoekers in overleg besluiten bepaalde risicovolle bevindingen niet te publiceren en alleen intern te delen en in een mondelinge technische briefing achter gesloten deuren aan leden van de Tweede Kamer toe te lichten.

11. Budget

IOB zal de kosten van het onderzoek dragen. Een begroting zal worden opgemaakt zodra de onderzoeksvragen zijn vastgesteld, en daarmee ook de onderzoeksmethoden kunnen worden bepaald.

[i] Cybersecuritybeeld Nederland CSBN 2019
[ii] Aanbieding Nederlandse Cybersecurity Agenda (NCSA), kenmerk 2253565, 20 april 2018
[iii] Website Nationaal Cyber Security Centrum https://www.ncsc.nl/
[iv] Cybersecuritybeeld Nederland CSBN 2019
[v] Cybersecuritybeeld Nederland, p. 7/8, 11/12
[vi] Internationale Cyberstrategie 'Digitaal bruggen slaan', 12 februari 2017
[vii] Boek: 'Het is oorlog maar niemand die het ziet'. Thomas Rueb; verscheidene nieuwsberichten, waaronder: https://nos.nl/artikel/2181380-gijzelvirus-waarschijnlijk-onderdeel-van-spionage-operatie.html, www.ad.nl/rotterdam/londen-rusland-zat-achter-platleggen-rotterdamse-haven~a32e8bfa/, www.infosecuritymagazine.nl/nieuws/apm-terminals-had-beveiliging-niet-op-orde www.ad.nl/rotterdam/londen-rusland-zat-achter-platleggen-rotterdamse-haven~a32e8bfa/ www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ www.infosecurity-magazine.com/news/five-eyes-united-blaming-russia/
[viii] Cybersecuritybeeld Nederland CSBN 2019
[ix] Cybersecuritybeeld Nederland CSBN 2019
[x] Cybersecuritybeeld Nederland CSBN 2019
[xi] Cybersecuritybeeld Nederland CSBN 2019, Internationale Cyberstrategie 'Digitaal bruggen slaan', 12 februari 2017
[xii] Nederlandse Cybersecurity Strategie (NCSS) 1, Slagkracht door samenwerking, juni 2011
[xiii] Nederlandse Cybersecurity Strategie (NCSS) 2, Van bewust naar bekwaam, 28 oktober 2013
[xiv] Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022 (GBVS), p. 16, 19
[xv] Nederlandse Cybersecurity Agenda, 2018, p. 7
[xvi] Regeerakkoord 2017-2021 'Vertrouwen in de toekomst', 10 oktober 2017, p. 3
[xvii] Zie e.g. Silfversten e.a., 'Cybersecurity: A State of the Art Review', 2019, pp. 30-31