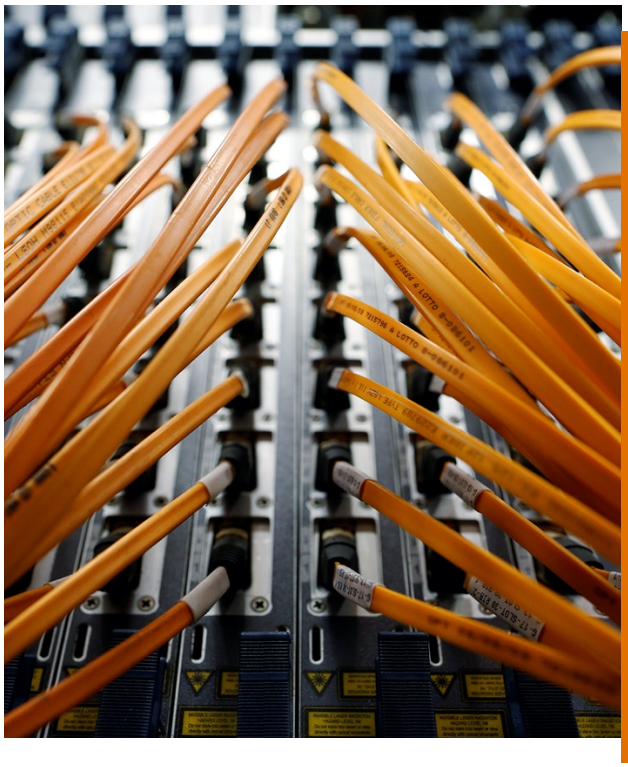
Roadmap Meerjarig Programma Cybersecurity VS 2020 – 2023

DRAFT Update 2022 (v2.4)



"The Netherlands ranks 5th on the global cyber power index. What's more, the long-standing trade relations with the United States […] offers a wealth of opportunities between two countries that have been the home of many of the world's leading innovations. Existing and emerging challenges call for inclusive solutions that we can address together."

Nathalie Jaarsma, Nederlandse ambassadeur voor Security Policy en Cyber

INHOUDSOPGAVE

SAMENVATTING

Deze roadmap is in de loop van 2018-2020 tot stand gekomen in nauwe samenwerking tussen de Nederlandse cyber sector, RVO, het postennet in de VS, en beleidsmakers in Den Haag van verschillende ministeries. Deze update bouwt voort op een aantal lopende initiatieven in de VS en blijft inzetten op een integrale aanpak.

De Verenigde Staten is en blijft een van de grootste spelers in de cybersecurity, zowel qua markt omvang, R&D investeringen, als buitenlandse investeringen. Door de warme relaties tussen Nederland en de VS, bestaan er al vele goede samenwerkingsverbanden. De Roadmap Meerjarig Programma Cybersecurity VS 2020 – 2023 bundelt bestaande activiteiten en vult ze aan met nieuwe. Zo ontstaat er betere coördinatie van activiteiten, met minder fragmentatie en meer focus.

De roadmap heeft als doel om in een samenwerking tussen bedrijfsleven, kennisinstellingen en overheid de Nederlandse cybersecuritysector te versterken.

Op basis van de Nederlandse cyber propositie en een marktverkenning in de VS op de RSA Conference en eerdere missies, is gekozen voor drie thema's in specifieke focus gebieden.
De activiteiten binnen deze roadmap worden vormgegeven en uitgevoerd met Nederlandse publieke en private netwerkpartners in samenwerking met het postennetwerk in de VS.
Het meerjarig committeren van budgetten voor de uitvoering van deze roadmap is noodzakelijk.
Om de algemene ambitie en drie doelstellingen te bereiken worden vier samenhangende strategieën gehanteerd:

***Ambitie**: De algemene ambitie is om de Nederlandse cybersecuritysector op een duurzame wijze te laten groeien en een van de top clusters in de wereld te laten worden.*

DOELSTELLINGEN 2023	**STRATEGIEËN 2020 - 2023**
1. Het verbeteren van de toegang voor NL bedrijven tot de Amerikaanse markt en daarbuiten door samenwerking met o.a. in de VS gebaseerde multinationals en financiële instellingen. 2. Het verhogen van het aantal VS partners die zich structureel committeren aan de locatie Nederland als gateway voor cybersecurity in Europa, rekening houdend met de TNO-analyse 2020 t.a.v. strategische behoeftes van NL Cybersector. 3. Het versterken van wetenschappelijke samenwerking met wederzijdse investeringen in publiek-private R&D en innovatietrajecten, voortbouwend op de bestaande assessments van wetenschappelijke expertise clusters en de kennisbehoeftes van het NL bedrijfsleven.	1. Nederlandse propositie: Het bepalen van de sterktes en behoeften van de Nederlandse cybersecurity sector om internationalisering op de VS adequaat uit te voeren. Met name ook met het oog op specifieke uitdagingen en (niche)kansen post-corona voor de Nederlandse cybersecuritysector. 2. Marktverkenning en positionering gericht op cybersecurity kansen in de VS: Het uitvoeren van relevante activiteiten gebaseerd op een aantal gekozen inhoudelijke thema's en geografische focusgebieden in de VS, met het oog op marktontwikkelingen, R&D-samenwerking en het bevorderen van buitenlandse bedrijfsinvesteringen in het Nederlandse ecosysteem. 3. Bilaterale samenwerking, waar nodig gefaciliteerd door het postennetwerk VS en de Nederlandse overheid, gericht op de gezamenlijke aanpak van schadelijke cyberactiviteiten onder meer door publiek-private samenwerking en investeringen in onderzoek en ontwikkeling. 4. Branding & Positionering: Het ontwikkelen van gemeenschappelijke communicatie- en verhaallijnen om Nederlandse sterktes en innovatieve oplossingen te positioneren.

INTRODUCTIE

Deze Roadmap Meerjarig Programma Cybersecurity VS 2020 – 2023 heeft als doel de Nederlandse cybersector op duurzame wijze te laten groeien en de reputatie als Europese toplocatie te versterken. Samenwerking tussen de Nederlandse overheid en Nederlandse publieke en private partijen, afstemming en validatie van vraag en aanbod en de koppeling met het oplossen van maatschappelijke uitdagingen zijn hierbij essentiële uitgangspunten. De roadmap is gebaseerd op de kennis en informatie van nu en wordt als 'living document' ieder kalenderjaar waar nodig 'herijkt' op onderdelen zoals keuze thema's, geografische focusgebieden en/of activiteiten. Deze versie is de 2022 update, mede op basis van het bezoek van de Nederlandse delegatie aan de RSA Conference in juni 2022. Deze grootste Nederlandse cybersecuritydelegatie ooit in het buitenland bestond uit 34 bedrijven, Ministerie van Justitie en Veiligheid (NCSC), Ministerie van Defensie, Topsector ICT, NFIA, postennet, InnovationQuarter en Security Delta (HSD). Ten opzichte van de vorige RSA Conference missie in 2020 was dit een verdubbeling van het aantal partijen. Daarbij was de Nederlandse delegatie de grootste internationale delegatie aanwezig op de RSA Conference in 2022.

Met een publiek-private meerjarige integrale samenwerking wordt ook een betere coördinatie en afstemming van activiteiten bewerkstelligd, met minder fragmentatie en meer focus. Het is van belang om een offensieve aanpak te formuleren, om investeringen in deze activiteiten te kunnen vertalen in zowel een hogere omzet van Nederlandse partners als meer bedrijvigheid in Nederland. Hierbij wordt ingezet op het nieuwe instrumentarium t.b.v. 'strategische acquisitie', waarbij duurzame investeringen in Nederland centraal staan. Op deze wijze verminderen de risico's van mogelijke 'leegloop' van kennis, talent en ondernemingen

De Covid-19 crisis toont aan dat de beschikbaarheid van digitale netwerken cruciaal is. Dit biedt in specifieke sectoren/thema's mogelijk een kans om de cyber security groeisector te benutten en bedrijfscontinuïteit zeker te stellen. Een cyberweerbare economie is een randvoorwaarde voor een bloeiende economie. Cyberweerbaarheid en economisch welbevinden zijn twee kanten van dezelfde medaille.

Een meerjarige roadmap impliceert ook een meerjarige committering budgetten voor het uitvoeren van de activiteiten. Het aansluiten van deze roadmap op de internationaliseringsstrategie Topsector ICT is derhalve noodzakelijk, mede met het oog op aanwijzen van strategische beurzen als de RSA Conference. Ook is het van belang om rekening te blijven houden met de geopolitieke context van de cyber security sector. Beleidsaspecten t.a.v. EU richtlijnen, wereldwijde afspraken over standaarden, of internationale investeringstrends in Nederland kunnen blijven leiden tot aanpassingen van deze roadmap.

CONTEXT CYBERSECURITY NEDERLAND EN VERENIGDE STATEN

Cybersecurity is in korte tijd één van de belangrijkste onderwerpen geworden binnen de ICT, dit is door de huidige COVID-19 crisis en het conflict in Oekraïne verder versterkt. De verwachting is dan ook dat uitgaven aan cybersecuritydiensten en -producten fors zal stijgen. Tegelijkertijd werkt RVO aan een meerjarige internationaliseringsagenda ICT, inclusief cybersecurity. Deze ontwikkelingen bieden de kans om veel meer zichtbaarheid te kunnen geven aan Nederland als toonaangevend cyberspeler – in de VS en daarmee ook mondiaal.

Noord-Amerika is en blijft een van de grootste markten voor cybersecurity, en is goed voor 45% van de 113 miljard dollar wereldwijde omzet. De verwachte globale groei tot 2025 van 10-14% per jaar zal ook in de VS leiden tot meer klanten en investeringen. Dit geldt ook voor innovatie in de sector: Ongeveer 75% van de R&D gelden wereldwijd komen vanuit de VS. De federale overheid speelt zowel als gebruiker als ook financier een belangrijke rol, met jaarlijks 15-20 miljard dollar aan investeringen in cyber-gerelateerde diensten en hardware. De Amerikaanse markt is gekenmerkt door een zeer gevarieerd aanbod – concurrentie is in de meeste sectoren aanzienlijk en internationale marktspelers werken daarom vaak met Amerikaans partners. Maar: de vraag voor cybersecurityoplossingen blijft groot en groeit gestaag. De onderliggende trends in de VS voor investeringen de komende jaren: de opkomst van IoT, nieuwe technologieën zoals AI en machine learning, en de toename van cyberdreigingen (met name potentiele disrupties van

vitale infrastructuur). Ook is er een toenemende vraag in de cybersecuritysector voor defensie en ruimtevaart.

De COVID-19 crisis heeft naast nieuwe uitdagingen voor overheden en bedrijven ook specifieke kansen gebracht in sectoren waar groei in zit en daardoor meer cyberveiligheid behoeven. Het conflict in Oekraïne, waarbij ook cyberaanvallen en hybride dreigingen een grote rol spelen, heeft het belang van samenwerking tussen landen op het gebied van cybersecurity verder onder de aandacht gebracht. Cybercriminelen en andere actoren hebben de afgelopen periode fors meer individuen, bedrijven en publieke instellingen aangevallen voor financieel, politiek en strategisch gewin. Tegelijk is nog duidelijker geworden dat cyberspace een onmisbare schakel is om vitale processen, communicatie en de economie draaiende te houden. De cybersecuritysector is voor beide een essentiële industrie met toenemende wereldwijde vraag, met name ook in de VS, naar nieuwe producten en diensten voor deze nieuwe realiteit. NL heeft met de expertise rond o.a. security- en privacy-by-design, cyber threat intelligence, IoT cybersecurity en kennis rond encryptie een goede uitgangspositie om de vele uitdagingen van de komende jaren te adresseren.

Door de warme relaties tussen Nederland en de VS, bestaan er al vele losse samenwerkingsverbanden. Denk aan G2G samenwerking tussen politie en onderzoeksdiensten, de NAVO, wetenschappelijke samenwerking, bedrijfs-uitwisselprogramma's, investeerders en banden met de US ambassade. Echter, omdat dit losse initiatieven zijn, blijft de zichtbaarheid van de Nederlandse cybersecuritysector – zowel als partner en ook als toplocatie voor investeringen – in de VS beperkt.

Door middel van deze meer gestructureerde roadmap en bundeling van bestaande activiteiten, aangevuld met een aantal strategische nieuwe activiteiten, kunnen we significante stappen zetten in het beter op de kaart zetten van de Nederlandse cybersecuritysector in de VS en het versterken van het Nederlandse ecosysteem. Hierin moeten handelsbevordering, innovatie & kennisdeling, en acquisitie verder samenkomen omdat deze elkaar versterken en de kracht van Nederland maximaal naar voren brengen. Essentieel hierbij is dat de Nederlandse overheid de samenwerking tussen Nederlandse publieke partners en private partijen stimuleert, en samen met deze partijen en het economisch netwerk in de VS, een meerjarige programmering uitrolt om zo ook vraag en aanbod op elkaar af te stemmen en te valideren.

AMBITIE EN DOELSTELLINGEN (OBJECTIVE & GOALS)

De algemene ambitie is om de Nederlandse cybersecuritysector op een duurzame wijze te laten groeien en een van de top clusters in de wereld te laten worden. In nauw overleg met de NL cyber spelers zijn voor deze meerjarige roadmap een drietal doelstellingen geformuleerd:

1. Het verbeteren van de toegang voor NL bedrijven tot de Amerikaanse markt en daarbuiten door samenwerking met o.a. in de VS gebaseerde multinationals en (financiële) instellingen.
2. Het verhogen van het aantal VS partners die zich structureel committeren aan de locatie Nederland als gateway voor cybersecurity in Europa, rekening houdend met de TNO-analyse 2020 t.a.v. strategische behoeftes van NL Cybersector.
3. Het versterken van wetenschappelijke samenwerking met wederzijdse investeringen in publiek-private R&D en innovatietrajecten, voortbouwend op de bestaande assessments van wetenschappelijke expertise clusters en de kennisbehoeftes van het NL bedrijfsleven.

Deze doelstellingen worden middels een meerjarige integrale aanpak van handelsbevordering, innovatie en kennis en investeringen in de uitvoering versterkt.

STRATEGIEËN – OVERZICHT

Om de genoemde doelstellingen te bereiken zijn de navolgende met elkaar samenhangende strategieën van belang:

Strategie 1

Nederlandse propositie: Het bepalen van de sterktes en behoeften van de Nederlandse cybersecurity sector om internationalisering op de VS adequaat uit te voeren. Met name ook met het oog op specifieke uitdagingen en (niche)kansen post-corona voor de Nederlandse cybersecuritysector.

Strategie 2

Marktverkenning en positionering gericht op cybersecurity kansen in de VS: Het uitvoeren van relevante activiteiten gebaseerd op een aantal gekozen inhoudelijke thema's en geografische focusgebieden in de VS, met het oog op marktontwikkelingen, R&D-samenwerking en het bevorderen van buitenlandse bedrijfsinvesteringen in het Nederlandse ecosysteem.

Strategie 3

Bilaterale samenwerking, waar nodig gefaciliteerd door het postennetwerk VS en de Nederlandse overheid, gericht op de gezamenlijke aanpak van schadelijke cyberactiviteiten onder meer door publiek-private samenwerking en investeringen in onderzoek en ontwikkeling.

Strategie 4

Branding & Positionering: Het ontwikkelen van gemeenschappelijke communicatie- en verhaallijnen om Nederlandse sterktes en innovatieve oplossingen te positioneren.

STRATEGIEËN – UITWERKING

S1: Nederlandse propositie

Tijdens de door RVO georganiseerde innovatiemissies naar de RSA Conference 2019, 2020 en 2022, de grootste cybersecurity conferentie ter wereld die jaarlijks in San Francisco wordt georganiseerd, is door de Nederlandse delegaties gezamenlijk besloten om gezamenlijk op te trekken en de krachten te bundelen om de markt in de VS te bewerken met een herkenbare NL 'brand'.

De *unique selling points* van de Nederlandse cybersecuritysector zijn:

- Nederland heeft sterke niche spelers, die ook door buitenstaanders tot de wereldtop worden gerekend.
- Nederlandse cybersecurityproducten zijn ten opzichte van producten uit andere landen gebruiksvriendelijk en overzichtelijk. Dit hangt nauw samen met dat 'Dutch Design' ten opzichte van andere landen sterk is het creëren en waarborgen van daadwerkelijke integriteit, transparantie en privacy; 'Integrity by Design'. Nederland is groot genoeg om een verschil in de wereld te maken en klein genoeg om niet als dreiging te worden gezien. In het buitenland wordt Nederland gezien als een speler die betrouwbare (trusted) technologie aanbiedt.
- Nederland heeft een lange historie en expertise op het gebied van samenwerking om grote uitdagingen op te lossen. Waar veel andere landen zich puur richten op het verkopen van hun producten en services, focust Nederland op het brengen van kennis en samenwerking om zo tot de juiste oplossingen en innovaties te komen. De publiek-private aanpak —met

daarbij een sterke kenniscomponent d.m.v. het betrekken van universiteiten en onderzoeksinstellingen—waar Nederland zeer sterk in is ontwikkeld, is een belangrijk uithangbord, onder meer in het opzetten van ecosystemen voor innovatie. Dit wordt onder andere uitgedragen tijdens de door MinJenV (NCSC), MinEZK en Gemeente Den Haag jaarlijks georganiseerde One Conference, inhoudelijk een van de meest vooraanstaande internationale conferenties het gebied van cybersecurity.
- Nederland heeft wereldwijd gezien een sterke hackerscommunity, met enkele vooraanstaande partijen die reeds in de VS opereren.

S2: Marktverkenning en positionering gericht op cybersecurity kansen in de VS

De VS is een grote markt en zonder een gefocuste aanpak is de kans klein dat Nederland zich succesvol kan positioneren in de VS. Vandaar dat het belangrijk is om een aantal thema's te definiëren om zo beter in staat te zijn concrete samenwerkingskansen te benutten. Vanuit de innovatiemissies in 2018 en 2019 alsmede de meerdere gezamenlijke reflectiemomenten tijdens en in de aanloop naar de economische missies in 2020 en 2022, tekenen zich drie thema's af waarop Nederland in de VS een significant verschil kan maken. Deze zijn door de bedrijven, kennisinstellingen, MinJenV (NCSC), MinDef, MinBuza, MinEZK, RVO, TNO, TU Eindhoven, Gemeente Den Haag alsmede InnovationQuarter en Security Delta onderschreven. Aan de bedrijvenkant gaat het hierbij om zowel product- als serviceaanbieders, waarbij zowel de defensieve als de offensieve kant van cybersecurity samenkomen. Deze hieronder beschreven drie thema's kunnen tijdens de looptijd van deze roadmap waar nodig verder worden geactualiseerd, aangevuld of vervangen.

Thema 1: Cyber Threat Intelligence (CTI) en Pentesting

De professionele cyberaanvallen van vandaag de dag hebben een nieuw antwoord nodig. Preventie, monitoring en incident respons alleen zijn niet meer voldoende om de schade van een cyberaanval te beperken. Met Cyber Threat Intelligence zijn overheden en bedrijven in staat vroegtijdig te anticiperen op cyberdreigingen en -aanvallen. Hoe eerder een mogelijke cyberdreiging wordt ontdekt, des te minder schade kan er toegebracht worden aan (kritieke) systemen (financiële sector, energie, water, etc.). CTI draait daarom om het verzamelen, analyseren en in context plaatsen van (grote hoeveelheden) cyberdreigingsinformatie. Het snel uitwisselen en delen van deze informatie met relevante stakeholders is echter ook een belangrijke voorwaarde voor het verbeteren van cyberweerbaarheid. Hierin kunnen Nederlandse Cyber een belangrijke rol spelen doordat Nederland een sterke reputatie heeft in cyber en wordt gezien als een (neutrale) partner voor de VS. Aanwijzingen voor acute of opkomende cyberdreigingen stellen een organisatie in staat om proactief maatregelen te treffen, zowel operationeel als voor de lange termijn.[3]

Thema 2: IoT/OT Security

Operational Technology (OT) bevindt zich overwegend in de vitale infrastructuur en de industriële sector. Met de opkomst van technologieën zoals Big Data, Data Analytics en Internet of Things, hebben organisaties steeds meer behoefte om OT met IT-netwerken te integreren via het internet. Denk hierbij ook aan het watermanagement, het beveiligen van sluizen die vaak ook aan het internet verbonden zijn, maar bijvoorbeeld ook infrastructuur van vliegvelden. Echter, dit leidt ook tot cyberrisico's. Internet of Things (IoT) biedt een kerntechnologie voor de digitale wereld. Het biedt grote waarde voor mensen, organisaties en overheden. Maar nog belangrijker, IoT groeit exponentieel. De bredere economie en kritieke infrastructuren worden geconfronteerd met een toenemende dreiging van grootschalige cyberaanvallen die worden gestart vanuit grote aantallen onveilige IoT-apparaten. Vertrouwen kan worden gewaarborgd door robuuste cyberbeveiliging maatregelen te implementeren en pentesting.[4]

Thema 3: Privacy and Data Protection

In navolging van de Algemene Verordening Gegevensbescherming (AVG/GDPR) van de Europese Unie (EU), is in de VS een nieuwe, enigszins vergelijkbare privacywetgeving ingevoerd. De

California Consumer Privacy Act (CCPA), aangenomen op 28 juni 2018, stelt een van de meest uitgebreide regels voor gegevensbescherming in de VS vast. Als zodanig zou het kunnen worden beschouwd als de Amerikaanse tegenhanger van de AVG. Nu deze in werking zijn getreden, zijn organisaties nadrukkelijk verantwoordelijk voor het gebruik van persoonsgegevens. Voor veel organisaties is dit een grote uitdaging, met name organisaties die honderden of zelfs duizenden verschillende gegevensbronnen en systemen gebruiken. Diensten en platforms om privacy en gegevensbescherming te kunnen managen en te kunnen implementeren zijn daarom belangrijk.[5]

Geografische Focusgebieden

Niet alleen inhoudelijk, maar ook geografisch is een focus op een aantal regio's belangrijk om de markt in de VS effectief te kunnen bewerken:

Focus Regio 1: Washington DC, Maryland en Virginia (overheid)

Focus Regio 2: New York City (finance)

Focus Regio 3: Californië (platformen en nieuwe technologieën)

Focus Regio 4: Chicago (manufacturing & automotive)

Potentiele andere regio's om te verbreden: Atlanta (fintech) en mogelijk North-Carolina, Zuidwest VS (Utah, Arizona, Colorado) en San Antonio (Texas), Boston (kennis en health).

S3: Bilaterale samenwerking

Nederland heeft als bondgenoot een sterke band met de VS op het gebied van veiligheid. Tegenwoordig richt zich dat niet alleen op de meer traditionele vormen van defensie- en veiligheidssamenwerking, maar ook nieuwe vormen, zoals cybersecurity en het bevorderen van verantwoord gedrag in cyberspace. Dit is bevestigd door het in mei 2019 gezamenlijke statement van de overheden van de VS en Nederland, naar aanleiding van hun inaugurele cyberdialoog. Hierin onderstreepten zij het belang van samenwerking tussen de twee landen in cyberspace.

De cyberdialoog en andere bilaterale relaties, beleidsmatig en operationeel, bieden goede mogelijkheden voor strategische discussie over G2G samenwerking die potentieel impact kunnen hebben op het bedrijfsleven maar ook om specifieke punten of initiatieven uit de sector onder de aandacht te brengen. Sterke G2G samenwerking door middel van economic diplomacy, maar ook bilaterale R&D trajecten, openen deuren voor zowel Nederlandse als Amerikaanse bedrijven. Een aantal prioriteiten waar de Nederlandse cybersecuritysector een actieve(re) en constructieve rol kan spelen t.a.v. Amerikaanse partners zijn bijv.:

- Gezamenlijke onderzoek naar cybersecurity van opkomende technologieën zoals AI, quantum en 5G. Inclusief gez. Inzet bij standaardontwikkeling in relevante internationale *standards bodies*;
- Tegengaan (en verantwoordelijk houden) van cybercriminaliteit en ondermijnende cyberoperaties (APT) waar verregaande samenwerking met de cybersecuritysector rond o.a. CTI een speerpunt is;
- Versterken van de ICT supply chain security, ook in COVID-19 verband, ten behoeve van de weerbaarheid van (internationaal) vitale sectoren en economische functies zoals telecom, financiële en medische sectoren;
- Inzet op cybersecurity capaciteitsopbouw in ontwikkelingslanden om daarmee deze landen te laten profiteren van de digitale economie en tegelijk vrijheden die cybercriminelen daar hebben weg te nemen;
- Inzet op het beschermen van mensenrechten online en tegengaan van ongewenste digital surveillance van kwetsbare (politieke) groeperingen en individuen.

S4: Branding en positionering

Door middel van een gemeenschappelijke, publiek-privaat-ontwikkelde branding kunnen we de sterktes van de Nederlandse cybersecuritysector optimaal presenteren aan Amerikaanse counterparts. De gemeenschappelijke communicatie- en verhaallijnen zijn essentieel om marktbewerkingsactiviteiten op te schalen. Deze kunnen door de betrokken partijen worden gebruikt en versterkt. Daarnaast zullen media/communicatie uitingen van de individuele partijen, maar ook van presentaties van bijvoorbeeld bewindspersonen, breder gedeeld worden zodat boodschappen versterkt kunnen worden zoals bijvoorbeeld tijdens de RSA Conference. De Nederlandse unique selling points, zoals beschreven in 'S1 Nederlandse propositie', samengevat in de slogan '*NL cyber – Integrity by Design*', vormen in dit alles de basis.

De door de RVO en partners ontwikkelde '*Netherlands: The (Secure) Digital Gateway to Europe*' propositie, waarin het Nederlandse veiligheidscluster reeds meerdere jaren nadrukkelijk naar voren wordt gebracht, zal verder worden versterkt. De Nederlandse cybersecurityorganisaties die meegenomen worden op handelsmissie en/of naar een paviljoen op een beurs vormen de bewijslast voor de propositie die gericht is om buitenlandse bedrijven aan te trekken. Dit leidt tot kansen voor de NFIA (waaronder InnovationQuarter) en RVO/IRIS om verbindingen te leggen en dit actief te benutten.

Andere punten die in de positionering naar voren zullen worden gebracht zijn:

- Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein en is toonaangevend op het gebied van cybersecurity, kennisontwikkeling en bevorderen van digitale veilige hard- en software;
- Nederland is aantrekkelijk voor buitenlandse cybersecuritybedrijven, vanwege de vooraanstaande kennis op het gebied van smartgrids en SCADA (een type industrieel controlesysteem) en beveiliging van vitale infrastructuren (water, energie, bruggen etc.);
- Het Nederlandse onderzoek op het terrein van cybersecurity is internationaal van hoog niveau.

BIJLAGE: ACTIVITEITEN OVERZICHT 2022-2023

De geplande en te plannen activiteiten voor het uitvoeren van de roadmap op basis van de gekozen strategieën staan in deze bijlage opgenomen.

De algemene afstemming/coördinatie tussen de verschillende activiteiten staan niet in het overzicht opgenomen. Coördinatie van activiteiten is van groot belang om te bewerkstelligen dat deze elkaar in de uitvoering kunnen versterken. De trekkers van de roadmap activiteiten zullen elk kwartaal bij elkaar komen om de voortgang en nieuwe kansen te bespreken.

OMSCHRIJVING ACTIVITEIT	**Handel**	**Acquisitie**	**Innovatie & Kennisdeling**
1. Jaarlijks een NL-paviljoen op de RSA Conferentie in San Francisco organiseren, dé internationale conferentie in de VS waar de cybersecurity-community uit de hele wereld samenkomt en de ideale kans om Nederland op het wereldtoneel te positioneren en nieuwe relaties op te bouwen. Daarnaast jaarlijks een missie (ntb: economisch, handels, of innovatie) naar de RSA Conferentie in San Francisco. De RSA Conference wordt daarbij ondergebracht in het Strategische Beurzenprogramma. *Trekker: IQ, RVO, DIO*	x	x	x
2. Ontwikkelen en waar nodig aanpassen van gezamenlijke PR/communicatieboodschap en aanpak. Uitvoering daarvan, o.a. op basis van middelen die hiervoor beschikbaar zijn, zoals publieksdiplomatie middelen. Hiermee positioneren we de Nederlandse cybersecuritysector gedurende het jaar in de VS, ook buiten de grote activiteiten zoals de RSA Conference. Dit doen we o.a. op basis van 'verhalen' uit de Nederlandse sector gekoppeld aan uitdagingen die spelen in de VS en waarbij Nederland oplossingen kan bieden. Alle betrokken partijen kunnen meeliften op deze communicatielijnen en deze, door middel van hun eigen communicatie, ook weer verder helpen te versterken. We kijken hoe de branding explicieter kunnen maken, zoals bijvoorbeeld de Duitsers met 'made in Germany'. *Trekker: RVO, Amb. Washington, IQ, HSD*	x	x	x
3. Partners for International Business (PIB) programma (in 2022 gestart) uitrollen en het consortium positioneren onder begeleiding van een lokale liaison.(**X**[1]) *Trekker: HSD, IQ*	x		
4. Inzetten van marktverkenningsmiddelen die bij postennet beschikbaar zijn voor individuele bedrijven om de markt voor hun product/service bij klantgroepen te verkennen maar ook hulp bij juridische checks van producten, belastingconstructies, diensten en contracten. Daarnaast ook de in 2021 gemaakte marktanalyse DC-area verder benutten. *Trekker: Postennet VS, RVO*	x		
5. Organiseren van verkennende meetings en missies naar de VS om de thema's verder te ontwikkelen (o.a. IMTS in Chicago). Hierbij organiseren van ronde tafels op de inhoudelijke thema's met key stakeholders uit de VS. Mogelijkheden voor aanhaken bij (mogelijke) PIB Ruimtevaart, maakindustrie programmering, Agrifood roadmap en LSH roadmap onderzoeken.	x	x	x

OMSCHRIJVING ACTIVITEIT	**Handel**	**Acquisitie**	**Innovatie & Kennisdeling**
Daarnaast kijken we naar aansluiting met activiteiten van Holland Fintech. *Trekker: RVO, Postennet VS, IQ, BOM, HSD*			
6. Samenwerking tussen Amerikaanse en Nederlandse veiligheidsclusters binnen Global EPIC en soft-landing programma's. We versterken de relaties met o.a. de Amerikaanse veiligheidsclusters in Maryland, Georgia en Fairfax en kijken daarbij naar mogelijkheden voor gezamenlijke activiteiten ter versterking van de relaties. *Trekker: HSD, IQ*	x	x	x
7. Organiseren netwerksessies/seminars/webinars, uitsturen nieuwsbrieven en communicatie via o.a. social media in Nederland voor uitbreiden van het aantal betrokken Nederlandse bedrijven, kennisinstituten, en publieke en private partners om zo het netwerk en de impact van de roadmap te vergroten. We brengen op meerdere momenten in het jaar de betrokken organisaties bij elkaar zodat zij kunnen netwerk, kennis kunnen uitwisselen en mogelijkheden kunnen verkennen tot samenwerking in Nederland en de VS. Deze behoefte werd nadrukkelijk uitgesproken vanuit de delegatie naar de RSA Conference 2022. *Trekker: RVO, HSD, IQ*	x		x
8. Uit laten zoeken hoe Nederlandse cybersecuritybedrijven zaken kunnen doen met de Amerikaanse overheid. Vanwege de gevoeligheden rondom veiligheid is dit soms lastiger dan in andere sectoren. Tijdens de RSA Conference 2022 kwam naar voren dat er behoefte is aan een duidelijke uitleg over de verschillende voorwaarden waaraan moet worden voldaan en de mogelijkheden om hiermee om te gaan. Naast de Amerikaanse veiligheidsdiensten (o.a. CISA en NSA) gaat het om ook lower-level overheden. *Trekker: Ambassade Washington (IA)*	x		
9. Voor de betrokken bedrijven wordt een pitching course georganiseerd. Effectief kunnen pitchen en presenteren is cruciaal om succesvol te zijn en blijven in de VS. Tijdens de RSA Conference 2022 missie kwam uit de delegatie dat hier behoefte aan was. *Trekker: RVO, Postennet, ism de PIB*	x		
10. De NFIA (en ROMs) richten zich op het acquireren van bedrijven uit de VS die Nederland specifiek wil aantrekken. Ze koppelen dit, waar mogelijk, aan de andere activiteiten waarbij de Nederlandse bedrijven een sterk uithangbord zijn. *Trekker: NFIA, IQ*		x	

OMSCHRIJVING ACTIVITEIT	**Handel**	**Acquisitie**	**Innovatie & Kennisdeling**
11. Vanuit min OCW en het postennet in de VS wordt het 'Dutch Network for Academics in the US' opgericht, een netwerk gericht op academische samenwerking binnen de US. Dit programma wordt samen met Min OCW ontwikkeld en vanaf september 2022 uitgerold. Het onderwerp cybersecurity zal in de programmering worden meegenomen. Er wordt vanuit de TU Delft en MIT gekeken wat de wensen voor samenwerking zijn en of hiervoor een werkgroep opgezet moet worden. *Trekker: Consulaat SF, Min OCW, TU Delft en MIT*			x
12. Reguliere afstemming van relevante overheidsinstellingen (o.a. MinJenV (NCSC), Ministerie Defensie en Ministerie Buitenlandse Zaken) met hun counterparts in de VS om synergiën te creëren ihkv lopende G2G samenwerking en het promoten van een stabiel internet en aansprakelijkheid van landen (o.a. vanuit inzet Ambassador at Large Security Policy and Cyber). Koppeling van kansen/mogelijkheden die ontstaan vanuit deze gesprekken en beleidsnotities aan de andere roadmap activiteiten. Zodoende worden de betrokken overheidspartijen beter op de roadmap aangesloten. Vanuit de Ambassade in Washington wordt een Influentials Missie vanuit de VS naar Nederland voorbereid. *Trekker: Amb. Washington, MinBuza, MinJenV*	x		x
13. Jaarlijks organiseren van de One Conference in Den Haag + inkomende VS-delegatie, eventueel met gezamenlijke kennissessies (i.s.m. de US Embassy). Tijdens de One Conference B2B matchmaking tussen NLse en US bedrijven. *Trekker: MinJenV (NCSC) i.s.m. MinEZK, Gem.DH (organisatie). Kennissessies i.s.m. US Embassy The Hague, HSD.*	x	x	x
14. Opzetten van studenten uitwisselingsprogramma's tussen Nederlandse en Amerikaanse universiteiten/hogescholen en het laten deelnemen van studenten aan cybersecurity summer schools (waaronder de Cybersecurity Summer School). *Trekker: Postennet VS*			x
15. Jaarlijks (eind kalenderjaar) monitoren en rapportage voortgang van de doelen en indicatoren achter de roadmap. Evt. 'herijking' van gekozen thema's, focusgebieden, en aanvulling KPI's. *Trekker: RVO i.s.m. alle partners*	x	x	x

(x^1) – Financering PIB vanuit het Partners for International Business budget en valt buiten de begroting financiering activiteiten van deze roadmap.
Let op: 'Trekker' betekent niet dat andere partijen/partners geen bijdrage aan de resp. activiteit leveren.