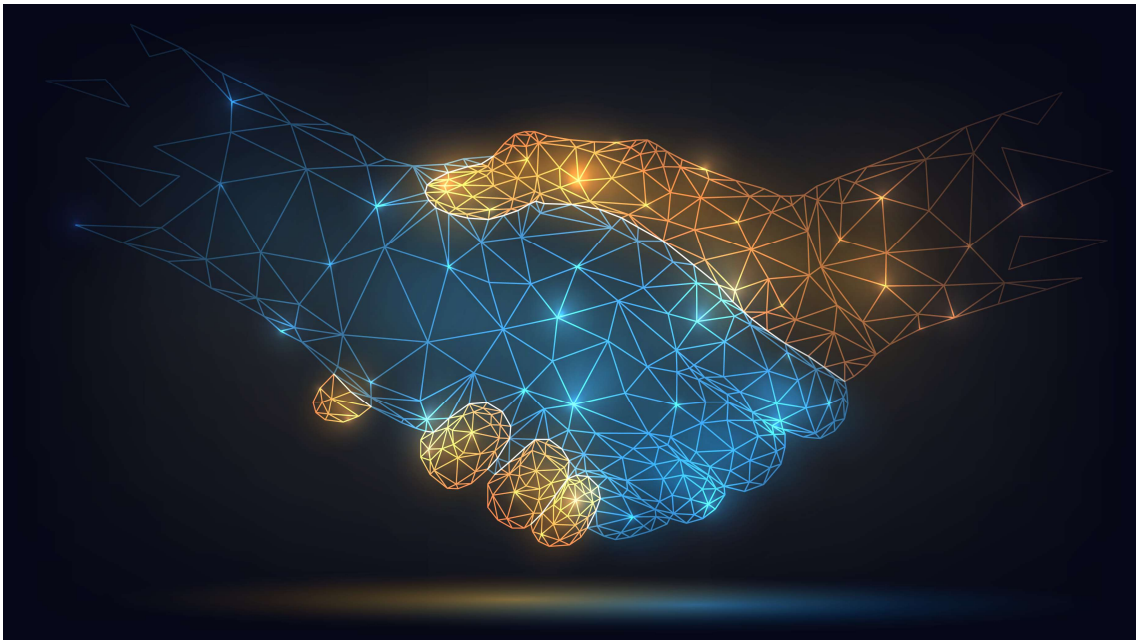
CS4NL

Breed Gedragen Programma Cybersecurity voor de Topsectoren



Versie: 12 oktober 2022[1]

Eddy Boot, dcypher, eddy.boot@dcypher.nl

Patrick de Graaf (kwartiermaker BGP, dcypher, patrick.degraaf@tno.nl)

Frits Grotenhuis, Topsector ICT, frits.grotenhuis@dutchdigitaldelta.nl

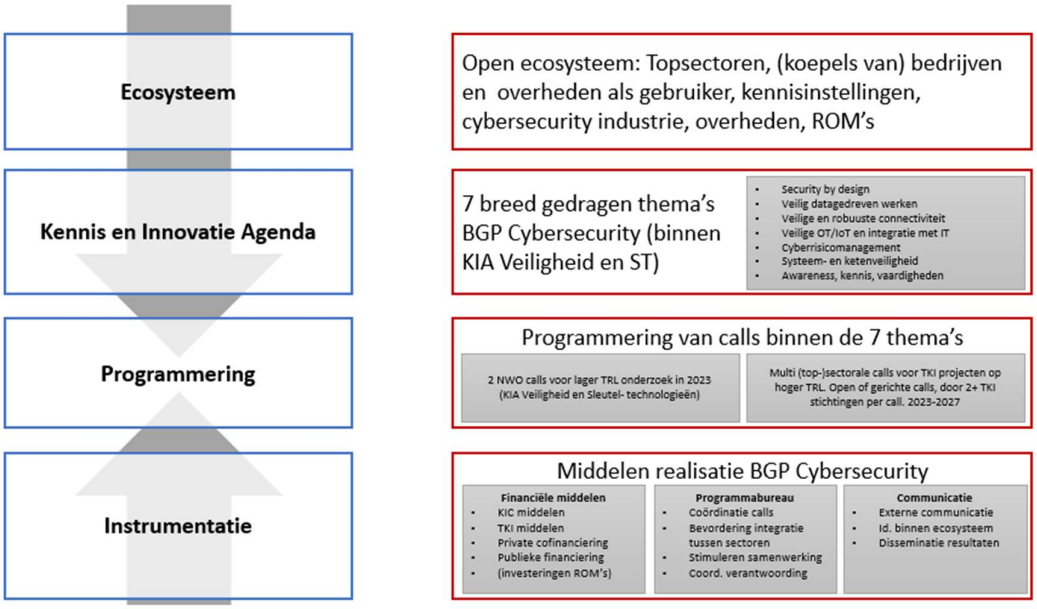
[1] *Disclaimer: Dit voorstel is met grote zorg samengesteld maar betreft werk in uitvoering. Het is dan ook mogelijk dat de informatie in dit voorstel onvolledig is, onjuist is of fouten kan bevatten.*

Managementsamenvatting

Voor u ligt het voorstel voor het Breed Gedragen Programma (BGP) cybersecurity kennis en innovatie voor de Topsectoren. Dit voorstel dat verder gaat onder de naam CyberSecurity voor Nederland (CS4NL) wordt doorontwikkeld naar een convenant tussen de aangesloten partijen, om vanaf 1 januari 2023 te starten, met een daartoe opgezette bestuursstructuur. Het CS4NL zal o.a. NWO-calls en calls op basis van Topsectoren-middelen coördineren, om tot impactvolle projecten te komen. Daarnaast wordt vanuit CS4NL nauw samengewerkt met het coalitieteam dat zich richt op een mogelijk Nationaal Groeifondsvoorstel voor cybersecurity. Het CS4NL biedt een ecosysteem en agenda die als uitgangspunt kunnen dienen voor zo'n voorstel.

Cybersecurity is randvoorwaardelijk voor het veilig en toekomstbestendig functioneren van de Nederlandse samenleving die in rap tempo digitaliseert. Cybersecurity draagt ook bij aan economische groei. Het belang én de urgentie worden inmiddels onderkend. Het onderwerp heeft dan ook een belangrijke plek in het Missiegedreven en Topsectoren en Innovatiebeleid (MTIB). De maatschappelijke transities waar Nederland voor staat, drijven immers veelal op digitalisering en dat kan alleen met de cybersecurity op orde. Soms kan dat met bestaande technologie, soms zijn nieuwe oplossingen nodig. Het belang en impact van digitalisering en de complexiteit van de bijbehorende nieuwe cybersecurity-oplossingen, maken het noodzakelijk dat multidisciplinair, (top-) sectoroverstijgend en in het hele ecosysteem wordt samengewerkt. Om samenwerking te bespoedigen is op initiatief van de Kennis- en Innovatie Agenda (KIA) Sleuteltechnologieën (ST) en in samenwerking met de KIA Veiligheid dit BGP Cybersecurity geschreven. De Topsector ICT en dcypher zijn de penvoerders van dit programma.

Het BGP Cybersecurity beoogt door het bespoedigen van samenwerking via programmering van open en gerichte subsidieoproepen (calls) een substantiële impuls te geven aan cybersecurity-kennis en -innovatie in Nederland. Deze kennis en innovaties dienen bij te dragen aan oplossingen die maatschappelijke transities en de bijbehorende veilige digitale transformaties bespoedigen. Het overkoepelende doel van het BGP cybersecurity is het versterken van de economie. De essentie van het BGP cybersecurity is weergegeven in onderstaande figuur.

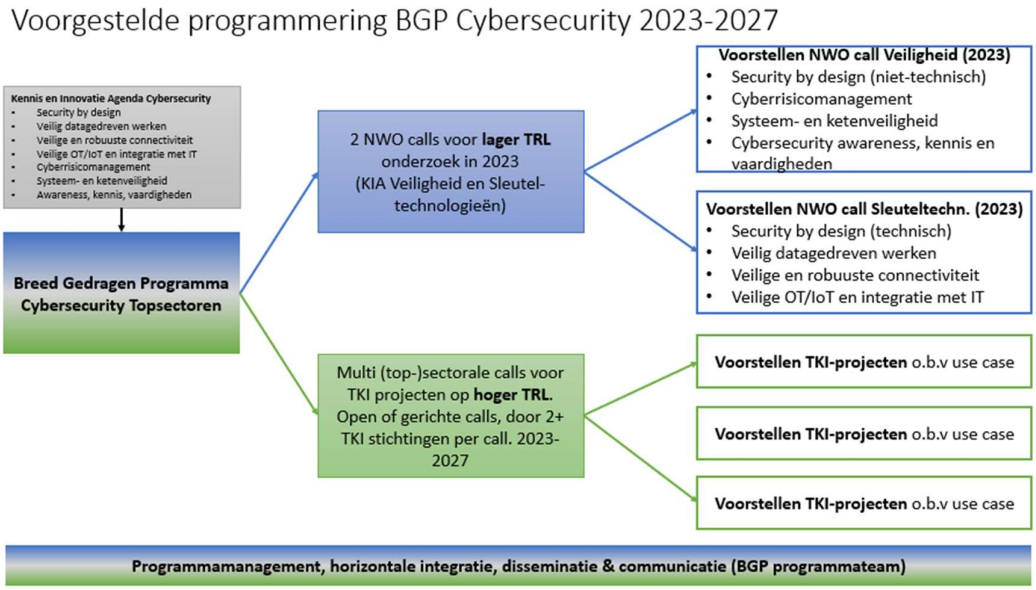


Figuur: overzicht van de kernelementen van het Breed Gedragen Programma Cybersecurity

Het BGP Cybersecurity betrekt de hele innovatieketen: wetenschappelijk en toegepast wetenschappelijk onderzoek, cybersecurity bedrijven, de industrie die cybersecuritytoepassingen in producten verwerkt én de private en publieke eindgebruikers. Aan de basis van het BGP Cybersecurity staat daarom een breed ecosysteem, dat bestaat uit alle topsectoren en organisaties uit hun achterban, de Academic Cyber Security Society (ACCSS), het HBO, NWO, TNO, Cyberveilig Nederland (cyberbedrijfsleven), Regionale Ontwikkelmaatschappijen (via Innovation Quarter) en het ministerie van Defensie. Via de KIA Veiligheid zijn ook de departementen van Economische Zaken en Klimaat (EZK) en Justitie en Veiligheid (JenV) betrokken.

Het BGP Cybersecurity werkt vraaggestuurd, vanuit de cybersecuritybehoeftes die voortvloeien uit de maatschappelijke transities en de bijbehorende digitale transformaties uit het missiegedreven innovatiebeleid. De gedeelde prioriteiten zijn benoemd in een agenda met zeven thema's: 1. Security by design, 2. veilig datagedreven werken, 3. veilige en robuuste connectiviteit, 4. OT/IT security, 5. cyberrisicomanagement, 6. systeem- en ketenveiligheid en 7. Cyber awareness, kennis & vaardigheden (human capital).

De beoogde programmering van het BGP Cybersecurity is vooralsnog vijf jaar, vanaf 2023 t/m 2027 en zal langs 2 sporen verlopen. Ten eerste een spoor voor lagere technologiegereedheidsniveaus (TRL) o.b.v. NWO MISSIE calls. De duur van projecten in dit spoor is tenminste 48 maanden en wordt primair ingevuld door PhD-studenten. Ten tweede een spoor voor hogere TRL met Topconsortia voor Kennis en Innovatie (TKI) (innovatie-)projecten, met variabele duur (vaak kort-cyclischer dan het eerste spoor).



Figuur: overzicht programmering BGP Cybersecurity 2023-2027

Voor het eerste spoor wordt voorgesteld Kennis & Innovatie Convenant (KIC) NWO-middelen in te zetten (v.u. KIA ST en KIA Veiligheid). Voor het tweede spoor worden TKI-middelen ingezet (PPS Toeslag en andere middelen)[2], private cofinanciering vanuit bedrijven die werken 'in cyber' of 'met cyber', publieke cofinanciering (o.a. vanuit Defensie) en eventuele ROM[3]-middelen. Voor dit tweede spoor zet het BGP het mechanisme van de multisectorale of cross-over calls in, waarin tenminste 2

[2] https://www.rvo.nl/subsidies-financiering/pps-toeslag-onderzoek-en-innovatie/voor-tkis
[3] Regionale Ontwikkel Maatschappijen

TKI-stichtingen (en eventueel Defensie) samen projectvoorstellen op gedeelde use cases beoordelen en laten uitvoeren. Net als de thema's zijn de use cases i.s.m. de Topsectoren en hun achterban uitgewerkt (zie de bijlagen). In totaal zijn 12 use cases voorbereid.

Hierna staat een financieel overzicht. De bedragen zijn indicatief, aangezien de definitieve omvang afhankelijk is van besluitvorming elders.

Bron	Totaalbedrag in mio euro (2023-2027)	Waarvan reeds gecommitteerd	Waarvan te mobiliseren
Private middelen	9,4-14,2*	0	9,4-14,2
PPS toeslag, andere Topsectorenmiddelen	3,25	0	3,25
TNO	n.t.b.	0	n.t.b.
NWO	5,5 - 16,5	5,5	5-11
Universiteiten/hogescholen	-	-	-
Regionale middelen (provincie, gemeenten)	-	-	-
Departementale middelen	4-7,25	0	7,25
EU middelen	-	-	-
ROMs	3	0	3
Anders, namelijk…	-	-	-
TOTAAL	**27-44,3**	**5,5**	**21,5-38,8**

* in principe houdt private cofinanciering gelijke tred met de NWO-financiering (30%), PPS toeslag (ca. 50%) en mogelijk ook de publieke cofinanciering

De in dit voorstel genoemde bedragen zijn indicatief. Voor de meeste KIC-partners is het zeker voor het tweede spoor pas mogelijk om commitment af te geven op concrete calls en projectvoorstellen. Voor het eerste spoor (NWO-calls) hebben de Kernteams ST en Veiligheid ook een belangrijke stem in de besluitvorming. Dit hangt samen met de aard van BGP's en de visie binnen de KIA-ST op gezamenlijk programmeren binnen BGP's (zie "*Notitie BGP commitment en governance*", 15 maart 2022): "Het doel van een BGP is te komen tot afstemming tussen KIC-partners over ST-ontwikkeling. Inhoudelijke afstemming moet vervolgens leiden tot synergie in de aanwending van KIC-middelen, zodat de gezamenlijke inzet meer is dan de som der delen." Voor dit BGP Cybersecurity willen we verder gaan dan afstemming en synergie. Het onderwerp cybersecurity is namelijk té urgent gezien de stijgende trend in cybersecurity incidenten en té belangrijk vanwege de toenemende digitalisering van onze maatschappij, om géén substantiële impuls te geven aan kennis en innovatie.

Inhoudsopgave

1 Inleiding

Voor u ligt CS4NL, een voorstel voor een Breed Gedragen Programma (BGP) Cybersecurity voor de Topsectoren, dat in Q4 2022 verder uitgewerkt en omgezet in een convenant tussen de betrokken partijen.

1.1 Waarom een Breed Gedragen Programma op cybersecurity?

Voor een klimaatbestendig, waterrobuust, duurzaam, gezond en veilig Nederland zijn zowel grote als kleine oplossingen nodig. Van de nieuwste wetenschappelijke inzichten en sleuteltechnologieën tot praktische en menselijke oplossingen in design en gebruik. De koppeling van deze maatschappelijke uitdagingen aan het bedrijfsleven en kennisinstellingen heeft geleid tot 25 concrete missies binnen vier thema's (Energietransitie en Duurzaamheid, Landbouw Water, Voedsel, Gezondheid en Zorg en Veiligheid).[4]

De 25 missies zijn de basis voor de Kennis- en Innovatieagenda's (KIA's) die de topsectoren voor elk maatschappelijk thema, sleuteltechnologieën en voor het maatschappelijk verdienvermogen van Nederland hebben gemaakt. Daarbij is ook aandacht voor internationale verdienkansen en menselijk kapitaal.

Om te innoveren op elk van deze missies, is het Kennis- en Innovatie Convenant (KIC)[5] afgesloten. Dit bevat afspraken met ruim 2.200 bedrijven, kennisinstellingen en overheden om gezamenlijk €4,9 miljard euro te investeren in economische kansen van maatschappelijke uitdagingen en sleuteltechnologieën. Van dat bedrag komt €2,05 miljard euro van bedrijven en €2,85 miljard euro uit publieke middelen.

In de Kennis en Innovatie Agenda Sleuteltechnologieën (KIA-ST) verwoorden de Topsectoren gezamenlijk hun ambitie op het gebied van technologieontwikkeling. In principe zijn de sleuteltechnologieën instrumenteel voor de realisatie van de missies van de thematische KIA's. Eén van die sleuteltechnologieën is cybersecurity, of digitale veiligheid. Dit is een randvoorwaardelijk aspect van de realisatie van de maatschappelijke transities achter de 25 missies. Deze zijn namelijk vrijwel allemaal afhankelijke van digitale technologie. Bovendien is cybersecurity in toenemende mate randvoorwaardelijk voor het veilig en toekomstbestendig functioneren van de Nederlandse economie die in zijn geheel in rap tempo digitaliseert. Samenwerking en actie zijn dus essentieel om deze complexe uitdagingen het hoofd te bieden, economische groei mogelijk te maken en voldoende strategische autonomie in het digitale domein te bewerkstelligen. Cyberveiligheid is overigens tevens onderdeel van de KIA-Veiligheid.

De KIA-ST initieerde medio 2021 het traject om te komen tot een Breed Gedragen Programma (BGP) Cybersecurity, waarvan Topsector ICT en dcypher de trekkers zijn. Voor het eerst werken alle 10 Topsectoren samen en dragen bij aan cybersecuritykennis en -innovatie ten behoeve van de grote maatschappelijke uitdagingen waar Nederland voor staat.

Waarom is dit nodig? Ondanks de agendering in diverse strategische documenten, beleidskaders en roadmaps van het bedrijfsleven en de overheid, blijkt het op peil brengen van de weerbaarheid tegen cyberdreigingen en het verzilveren van de kansen een grote opgave. De digitale

[4] https://www.topsectoren.nl/missiesvoordetoekomst

[5] Kamerbrief kennis- en innovatieconvenant 2020-2023 en de roadmap Human Capital Topsectoren 2020-2023, https://www.topsectoren.nl/innovatie/documenten/kamerstukken/2019/november/12-11-19/kamerbrief-kic-2020-2023. En het Kennis- en Innovatieconvenant: https://www.topsectoren.nl/innovatie/documenten/kamerstukken/2019/november/12-11-19/kic-2020-2023

ontwikkelingen volgen elkaar in rap tempo op, evenals nieuwe vormen van cybersecurity-dreigingen. Voor spelers met beperkte kennis, middelen en menskracht is dat niet zelfstandig bij te houden en op in te spelen. Daarnaast vereist het (adequaat) toepassen van maatregelen om weerbaar te zijn, of om kansen te pakken, een stevige kennis- en innovatiebasis van de bedrijven in de Topsectoren. Cybersecurity-kennis is echter nog steeds schaars en cybersecurity innovatie staat zelden centraal. Samenwerking tussen Topsectoren zorgt echter voor meer massa per onderwerp en voorkomt dat 'wielen' worden uitgevonden door (b.v.) kennisdeling en doorverwijzing.

1.2 Wat is een Breed Gedragen Programma?

De KIA-Sleuteltechnologieën (KIA-ST) zet in op de ontwikkeling van sleuteltechnologieën (ST). Nederland doet het goed op het gebied van ST-ontwikkeling, maar kan zonder focus onvoldoende massa creëren in de verdere ontwikkeling en toepassing om concurrerend te zijn en te blijven ten opzichte van andere landen. De KIA-ST heeft daarom de ambitie om keuzes te maken, en kan daar putten uit ongeveer 50 sleuteltechnologieën en een evenzo grote staalkaart aan mogelijke projecten: de Meerjarenprogramma's (MJP's, i.c. MJP-55 Cybersecurity). De KIA-ST kent zelf geen missies aan de hand waarvan keuzes kunnen worden gemaakt. Daarom is bij de start gekozen voor een concrete en pragmatische aanpak waarmee specifieke ST-programma's met breed draagvlak worden ontwikkeld.

Een Breed Gedragen Programma (BGP) is een programma dat een wetenschappelijke basis heeft in een of meerdere ST, met een of meerdere toepassingsgebieden en dus op steun en (financieel) commitment kan rekenen van veel KIC-partners. Het doel van een BGP is te komen tot afstemming tussen KIC-partners over ST-ontwikkeling. Inhoudelijke afstemming moet vervolgens leiden tot synergie in de aanwending van KIC-middelen, zodat de gezamenlijke inzet meer is dan de som der delen.

Alle KIC-partners zijn welkom in de KIA-ST en kunnen het initiatief nemen tot het opwerken van een BGP. Bij voldoende energie en draagvlak wordt een BGP gezamenlijk verder inhoudelijk vormgegeven. Een BGP is daarmee een reflectie van een onderwerp dat voor veel KIC-partners relevant is en dat aansluit bij hun prioriteiten en de belangen van alle bedrijven en maatschappelijke partners die zij vertegenwoordigen.

Breed draagvlak betekent ook meer financiële ondersteuning. Belangrijk onderdeel van het uitwerken en vaststellen van een BGP is daarom het stimuleren van financieel commitment van KIC-partners. Binnen het KIC opereren KIC-partners echter met eigen budget en eigen verantwoordelijkheid. Een vastgesteld BGP kan vanuit dit perspectief worden gezien als een gezamenlijke en gedragen KIA op een specifiek ST-onderwerp (i.c. cybersecurity), waarlangs individuele KIC-partners zelf kunnen programmeren. KIC-partners geven dus aan welke KIC-middelen zij aan een BGP committeren en hoe dit concreet via programmering vorm krijgt. Het BGP (en het programmabureau als uitvoerder ervan) stimuleert synergie tussen de KIC-partners door faciliteren van de processen agenderen & programmeren en community building.

Het vastleggen van financieel commitment voor een BGP is bij eerdere trajecten een lastig proces gebleken, juist omdat KIC-partners elk op hun eigen manier programmeren. Zo kan er beperkte mogelijkheid of bereidheid zijn om (vooraf) een financiële bijdrage aan een BGP toe te zeggen. Commitment voor BGP-voorstellen uit 2021 beperkte zich daarom tot bestaande inhoudelijke speerpunten (technologieën) en lopende projecten/programma's en KIC middelen voor NWO-calls.

In plaats van vooraf financieel commitment te vragen voor een BGP stimuleert KIA-ST inhoudelijke afstemming tussen betrokken KIC-partners, met als doel om in het kader van een BGP gezamenlijk te programmeren. Gezamenlijk programmeren betekent in dit geval dat betrokken KIC-partners:

- Een BGP organiseren op vrijwillige basis en met minimale overhead;
- Zich committeren aan actieve participatie bij de inhoudelijke uitvoering en doorontwikkeling;
- Elkaar op reguliere momenten informeren over inhoudelijke programmering en voortgang;
- Samen ambities bepalen en nieuwe initiatieven (calls, projecten) ontwikkelen.

Deze problematiek speelt ook voor het BGP cybersecurity. We volgen de bovenstaande aanpak, maar voegen daar wel dankzij de inzet van betrokken stakeholders ook additionele financiering aan toe. Het BGP Cybersecurity geeft daarmee een nieuwe impuls aan relevante kennis en innovatie.

1.3 Breed Gedragen: deelnemende partijen

Over de hele breedte van de Topsectoren is participatie in het BGP. Dit toont aan dat cybersecurity leeft in de achterbannen en dat er behoefte is aan kennis en innovatie. Gedeelde innovatie-behoeftes worden samen geagendeerd om zodoende de krachten te bundelen. De tien Topsectoren en overige partners die onderdeel uitmaken van het BGP zijn:

Topsectoren	**KIC partners en overige leden van de stuurgroep**
Topsector Agri & Food	Academic Cyber Security Society (ACCSS)
Topsector Chemie	Cyberveilig Nederland (CVNL, cyberindustrie)
Topsector Creatieve Industrie	dcypher
Topsector Energie	ECP | Platform voor de InformatieSamenleving
Topsector High Tech Systems and Materials	Innovation Quarter (namens de ROM's)
Topsector ICT	Lectorenplatform PRIO (namens HBO)
Topsector Life Sciences and Health	Ministerie van Defensie
Topsector Logistiek	NWO
Topsector Tuinbouw & Uitgangsmaterialen	TNO
Topsector Water & Maritiem	

Via KIA Veiligheid geven de departementen EZK en JenV ondersteuning aan dit BGP. Ook Safety Delta Nederland is aangesloten op het ecosysteem.

Zie voor een uitgebreider overzicht bijlage 1. De kring van betrokken partijen is ruimer, zie bijlage 2. De rationale achter deze samenstelling is de publieke en private sleutelpartijen voor de vraagsturing, de hele innovatieketen voor uitvoering en de financiering samen te laten werken aan de relevante speerpunten.

1.4 Totstandkoming van het BGP Cybersecurity

Voor het BGP Cybersecurity werken het Kernteam KIA ST en Topsectoren vanuit de **vraag** of **behoefte** die voortvloeien uit de maatschappelijke transities en de bijbehorende digitale transformaties uit het missie gedreven innovatiebeleid. De cybersecurity technologie, toepassingen en randvoorwaarden die nodig zijn voor een succesvolle digitale transformatie staan centraal, niet het aanbod aan cybersecurity kennis of producten.

Om de behoeftes in kaart te brengen, fungeren de Topsectoren (en individuele gebruikersorganisaties) als vertaler. Dit heeft in Q1 2022 geleid tot zeven breed gedragen thema's. Er heeft een toets plaats gevonden met vertegenwoordigers van wetenschap, TO2 en cyberindustrie

of dit wel onderwerpen zijn waarop kennisopbouw en innovatie nodig is. Dat bleek het geval. De thema's fungeren straks rechtstreeks als basis voor NWO-calls voor fundamenteel onderzoek. Samen met de Topsectoren zijn gebruikersorganisaties en andere stakeholders vervolgens in de periode april – juli 2022 aan de slag gegaan om de thema's te verdiepen tot use cases (ofwel probleemstellingen en hun context) die straks aan de basis staan van multisectorale calls voor kort-cyclischer onderzoek. Het BGP-team heeft een aantal Topsectoren die hierin tijd konden en wilden investeren ondersteund (Energie, HTSM, Life Sciences & Health, Logistiek). Deze Topsectoren zijn dus de hofleverancier van de use cases, en andere Topsectoren zijn uitgenodigd om t.z.t. te participeren in de multisectorale calls op deze use cases. Bij de uitwerking zijn talloze experts betrokken van kennisinstellingen, overheden en bedrijfsleven (zie ook bijlage 2).

Op bestuurlijk niveau is gedurende het opstellen van het voorstel contact onderhouden met de KIA ST en Veiligheid, diverse departementen (Defensie, J&V, IenW, EZK) en met het Coalitieteam Nationaal Groeifonds cybersecurity.

Een vroege versie van het voorstel BGP Cybersecurity is in opdracht van de KIA-coördinator Sleuteltechnologieën onafhankelijk beoordeeld door TNO. De resultaten zijn verwerkt in dit voorstel.

1.5 Relatie met andere agenda's en programma's

Het BGP Cybersecurity opereert niet in een *greenfield*. Binnen en buiten het cyberdomein zijn er diverse initiatieven op het gebied van kennis en innovatie voor cybersecurity. Binnen het cyberdomein zien we veel en gevarieerd initiatief, maar tot dusverre beperkt van omvang, niet vraaggestuurd en/of slechts gericht op één sector (i.t.t. het BGP). De insteek van deze initiatieven verschilt onderling sterk: veel push/soms pull, op verschillende sectoren gericht (b.v. water, high tech, energie), allerlei technisch-inhoudelijke accenten, kennis & innovatie als hoofd- of bijzaak, laag vs. hoog volwassenheidsniveau (TRL) etc.

Hier valt nog synergie te behalen door meer regie of op zijn minst stimulering van informatie-uitwisseling. Het samenwerkingsplatform voor kennis en innovatie op cybersecurity, dcypher heeft hier een belangrijke rol in. Het BGP cybersecurity mag zelf niet bijdragen aan vergroting van de complexiteit.

Het onderwerp cyberveiligheid is ook onderdeel van de KIA Veiligheid (MMIP[6] 4). De KIA Veiligheid prioriteert een aantal specifieke onderzoeksgebieden binnen cyberveiligheid, dcypher is hiervan portefeuillehouder. Het Kernteam Veiligheid is ook betrokken bij de totstandkoming van dit BGP-voorstel, juist omdat de inhoudelijke belangen van de KIA's ST en Veiligheid hier dicht op elkaar liggen. Zie bijlage 3 voor de samenhang tussen de BGP-thema's en beide KIA's.

Specifieke aandacht verdient verder het Nationaal Groeifonds (NGF). Tot op heden is het niet gelukt om een voorstel te vormen dat tegemoet komt aan de inhoudelijke behoeftes aan nieuwe oplossingen voor digitale weerbaarheid én de eisen die het NGF stelt aan economisch verdienvermogen. Tijdens het opstellen van dit voorstel is wel voortdurend contact geweest tussen het BGP team en het Coalitieteam NGF Cybersecurity dat zo'n voorstel voorbereidde. Er is dus vooralsnog geen perspectief op een Nationaal Groeifondsprogramma rond cybersecurity, maar mogelijk dat dit in de derde ronde (2023) alsnog wordt gepoogd. Het BGP Cybersecurity biedt dan qua thematiek en ecosysteem een goed fundament.

[6] MMIP is Meerjarige Missiegedreven Innovatieprogramma. Zie voor de KIA Veiligheid: https://www.nwo.nl/sites/nwo/files/assets/KIA%20Veiligheid%20-%2020191015%20definitief_0.pdf

Verder zijn er talrijke programma's, organisaties en andere initiatieven om de dagdagelijkse cyberweerbaarheid te versterken. B.v. door informatiedeling, awareness, delen van good practices of gezamenlijke Computer Emergency Response Teams. Voorbeelden zijn (lang niet uitputtend!): de sectorale Information Sharing & Analysis Centres van het NCSC[7], FERM (haven Rotterdam), INTERSECT, activiteiten vanuit de Economic Board Zuid-Holland, Security Delta (HSD), verzekeraars, Cybersecurity Alliantie (CSA), Platform voor Cyber Security Innovatie (PCSI), Digital Trust Center (DTC, EZK)[8] en aangesloten samenwerkingsverbanden (voor zover hier niet genoemd). Dit zijn voor de hand liggende stakeholders voor de uitvoering van projecten onder het BGP. Internationaal zijn er overigens ook (Europese) samenwerkingsverbanden voor kennis en innovatie, zoals CONCORDIA[9].

Buiten het cyberdomein zijn er verder diverse kennis- en innovatieprogramma's met raakvlakken. Cybersecurity is hierbij ofwel het toepassingsdomein (b.v. bij AI projecten in de NLAIC of post-quantum crypto in Quantum Delta NL) ofwel een randvoorwaarde die wordt meegenomen (b.v. bij het Future Network Services NGF voorstel). Het voert te ver om hier alle initiatieven te inventariseren en te analyseren. Belangrijk is het bewustzijn dat bij de uitwerking van concrete onderwerpen er ook concrete raakvlakken kunnen zijn met andere programma's en domeinen.

1.5.1 Unieke positie BGP Cybersecurity

Het BGP Cybersecurity beoogt een substantiële impuls aan cybersecurity kennis en innovatie, gericht op securityproblemen die we op moeten lossen om meerdere maatschappelijke transities veilig digitaal te kunnen vormgeven en daarmee de economie te versterken. Hierbij is de hele innovatieketen betrokken. Bij voorlopig uitblijven van een NGF cyberprogramma, is het BGP Cybersecurity de belangrijkste vraaggestuurde impuls die we momenteel kunnen geven in Nederland. Dát is de niche en toegevoegde waarde van het BGP.

1.6 Leeswijzer

Dit voorstel gaat in hoofdstuk 2 allereerst in op de maatschappelijke en economische impact, de relatie met strategische autonomie en de sleuteltechnologieën. In hoofdstuk 3 introduceren we de zeven thema's die centraal staan. De 7 gedeelde thema's zijn benoemd voor een veilige digitale transformatie en vormen de Kennis en Innovatieagenda Cyber (KIA Cyber). Informatie over het programma KIA Cyber is opgenomen in hoofdstuk 4 en gaat in op de visie, de structuur, acties en de governance om de projecten tot uitvoering te brengen. Hoofdstuk 5 beschrijft de indicatieve begroting en dekking. Hoofdstuk 6 gaat in op de manier waarop dit programma samenwerkt met haar stakeholders en de communicatie-strategie die hiervoor ontwikkeld is. Hoofdstuk 7 behandelt de risico's en randvoorwaarden en tot slot gaan we in hoofdstuk 8 in op doorontwikkeling.

[7] https://www.ncsc.nl/onderwerpen/start-een-samenwerking/zelf-een-samenwerking-starten/samenwerking-sector
[8] https://www.digitaltrustcenter.nl/overzicht-van-samenwerkingsverbanden
[9] https://www.concordia-h2020.eu/ et al

2 Impact

De meerwaarde van het BGP Cybersecurity zit als eerder opgemerkt in het versterken van de digitale weerbaarheid als maatschappelijke impact (2.1 en 2.2), economisch verdienvermogen (2.3) en strategische autonomie (2.4) van Nederland. Het BGP Cybersecurity pakt daartoe de cyberveiligheidsvraagstukken op die voortkomen uit grote maatschappelijke transities en organiseert hiertoe efficiënte ketens van samenwerking voor kennis en innovatie binnen het kader van de KIA Sleuteltechnologieën (2.5).

2.1 Versterking digitale weerbaarheid

We worden inmiddels regelmatig opgeschrikt door nieuwsberichten over cybersecurity-incidenten. Het gaat ergens fout en de productie ligt enkele dagen stil, gevoelige data of intellectueel eigendom lekt uit naar onbekende en veelal ongrijpbare derden. Geen publieke of private entiteit lijkt gespaard te blijven. Cybersecurity-bedrijven en wetenschappers hanteren inmiddels het dogma '*assume breach*': ga ervan uit dat er ooit een incident bij je plaats vindt. Topsectoren realiseren zich dat nieuwsberichten over cyberincidenten in andere sectoren als waarschuwingen opgevat moeten worden.

De overheid waarschuwt ook al geruime tijd voor de risico's in het digitale domein, o.a. vanuit de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) en de Algemene Inlichtingen en Veiligheidsdiensten (AIVD). Het Cybersecurity Beeld Nederland 2022 (CSBN)[10] beschrijft de uitdaging kernachtig: "*De vraag 'hoe digitaal veilig is Nederland?' is eigenlijk niet te beantwoorden en bovendien bestaat honderd procent veiligheid niet. Digitale processen kunnen altijd uitvallen door technisch of menselijk falen. De digitale ruimte is bovendien hét speelveld van een groeiend aantal staten, waarbij cyberaanvallen het nieuwe normaal zijn. Daarnaast hebben aanvallen door cybercriminelen inmiddels een industriële schaal bereikt. De digitale dreiging is dan ook permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien*."

Naast de veiligheidsdepartementen stuurde ook het ministerie van EZK in 2017 een brief aan de regering met een voorstel om de cybersecurity van het kennisintensieve, niet-vitale deel van het bedrijfsleven te verhogen. In het TNO onderzoek, dat gebruikt is in de brief van het Ministerie, werd constateert dat: "*de [top] sectoren zich (nog) niet voldoende bewust zijn van de risico's die de digitalisering met zich meebrengt […] en dat risicoanalyses voor de sector niet hebben plaatsgevonden*".[11]

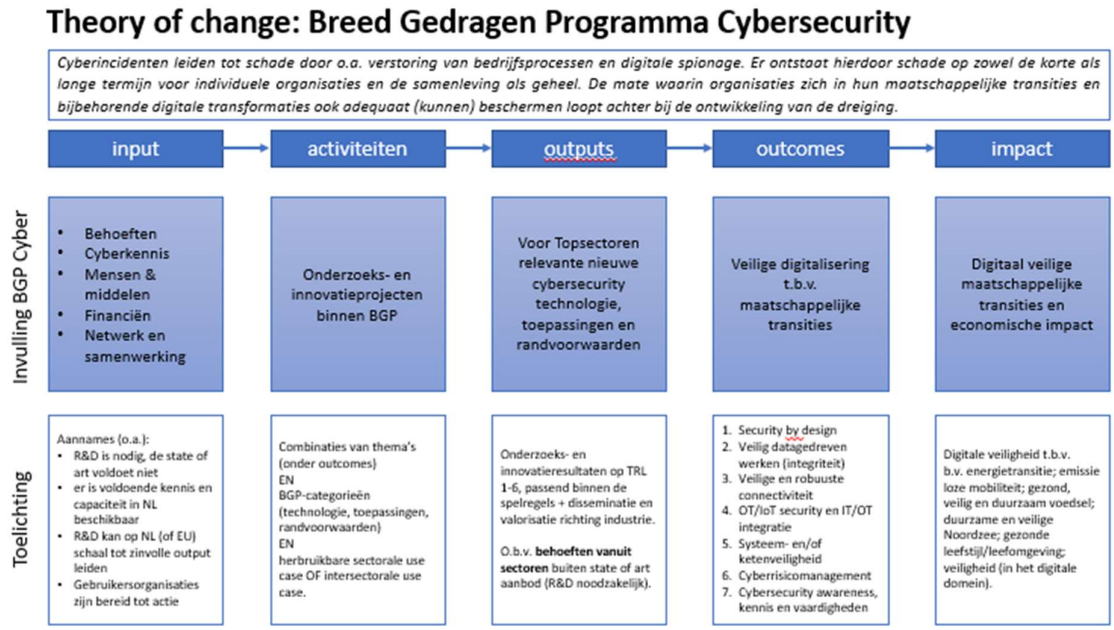
De digitale dreigingen voor Nederlandse organisaties en voor de maatschappelijke transities waarvoor we staan, bestaan op de korte termijn o.a. uit digitale sabotage van IT en OT systemen, cybercrime (b.v. ransomware) en in mindere mate hacktivisme en digitaal vandalisme. Schade op de langere termijn ontstaat door digitale spionage, wanneer economische opponenten (overheden of bedrijven) intellectueel eigendom of andere waardevolle data stelen en inzetten voor versterking van hun eigen concurrentiepositie. Dit zal ten koste gaan van de concurrentiepositie van Nederland. Onze publieke en private investeringen in kennis en innovatie moeten dus ook worden beschermd, willen ze niet voor niets zijn geweest. Verder zijn er steeds meer (internationale) verplichtingen o.b.v. wet- en regelgeving (compliance). Voorbeelden hiervan zijn de GDPR en de Network and

[10] https://www.rijksoverheid.nl/documenten/rapporten/2022/07/04/cybersecuritybeeld-nederland-2022
[11] Kamerstuk st-26643-463, https://zoek.officielebekendmakingen.nl/blg-808966

Information Security (NIS) Directive 2.0[12]. Het ligt in de lijn der verwachting dat de EU en nationale overheid meer zullen gaan reguleren de komende jaren, omdat vrijwillige actie nog niet heeft geleid tot voldoende digitale weerbaarheid.

2.2 Maatschappelijke impact: veilige samenleving en veilige maatschappelijke transities

Om meer grip te krijgen op de maatschappelijke impact van het voorstel, gebruiken we het Theory of Change (ToC) raamwerk. Een ToC raamwerk beschrijft hoe en waarom een interventie (in dit geval het programma) wordt verondersteld te leiden tot een gewenst eindresultaat. De onderdelen van een ToC zijn: input – activiteiten – output – outcomes en impact. Het start met de probleemstelling en context van dit BGP en redeneert als vraaggestuurd terug vanuit maatschappelijke transities (impact) naar digitale transformaties (outcomes) naar outputs van het BGP en verder terug naar activiteiten en input. Een belangrijke fase in een ToC is het ontwikkelen van indicatoren. Deze fase richt zich op de vraag hoe het succes van het programma is vast te stellen. Een stelstel van indicatoren zal door de aangesloten partijen vanaf Q4 in 2022 worden vastgesteld. Een eerste aanzet voor deze indicatoren kan gevonden worden vanaf par. 4.6.



Figuur: Theory of change van het BGP Cybersecurity

Het BGP Cybersecurity draagt (direct of als enabler van digitalisering) bij aan vele Meerjarige Missiegedreven Innovatie Programma's (MMIP's), mede door de zeer brede deelname van de Topsectoren. Die bestempelen cybersecurity als randvoorwaardelijk voor innovaties in verreweg de meeste domeinen. B.v. driekwart voor de roadmaps in de Topsector HTSM geeft b.v. aan dat men zonder (voldoende) cybersecurity niet succesvol kan zijn. En b.v. in de Roadmap Space en Automotive, daarin staat dat cybersecurity randvoorwaardelijk is voor de autonoom rijdende auto van de toekomst en hoe tijdens de productie van space-assets al rekening gehouden moet worden met langdurige weerbare inzet in de ruimte. Vanwege het randvoorwaardelijke karakter voor

[12] Zie o.a. https://magazines.cybersecurityraad.nl/csrmagazine/2022/01/nis2-een-ambitieuze-update-van-de-europese-cybersecurity-richtlijn en https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333. In Nederland is deze richtlijn vertaald in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

digitalisering draagt cybersecurity bij aan zeer veel MMIP's. Het bleek bij opstellen ondoenlijk om álle relaties uitputtend of overzichtelijk te beschrijven. Zie echter hierna wel de analyse in de tussentijdse toets van TNO.

2.2.1 Tussentijdse toets maatschappelijke impact

In opdracht van de KIA-coördinator Sleuteltechnologieën, heeft TNO een vroege versie van het voorstel BGP Cybersecurity beoordeeld. Het BGP-voorstel scoorde hoog op het aspect maatschappelijke impact:[13]

1.1 De bijdrage van het BGP aan het thema Energietransitie en duurzaamheid	64%
1.2 De bijdrage van het BGP aan het thema Landbouw, water en voedsel	33%
1.3 De bijdrage van het BGP aan het thema Veiligheid	94%
1.4 De bijdrage van het BGP aan het thema Gezondheid en zorg	50%

Het initiële voorstel beschrijft volgens TNO al "*een brede scope en heeft een toepassing in meerdere domeinen. Zo zijn bijvoorbeeld alle topsectoren betrokken bij dit voorstel. Om deze reden zijn de scores hoog. De grootste bijdrage wordt verwacht aan het thema Veiligheid (94%). Het percentage 94% is hoog doordat de experts aan zeven van de acht onderliggende missies binnen het thema Veiligheid de score 2 (kern rol) hebben toegekend. (…) Dit komt omdat cyber veiligheid en digitale transformatie een belangrijke rol speelt in deze missies.* "

"*Daarnaast heeft het thema Energietransitie en duurzaamheid een score van 64% gekregen, omdat vier van de zeven missies de score 2 hebben gekregen. De reden hiervoor is dat voor een goedwerkend en veilig energiesysteem cyber security van belang is. Ook gaat MMIP 13 bijvoorbeeld over systeemintegratie, hierbij speelt cyber security ook een belangrijke rol volgens de experts. Tevens heeft het thema Gezondheid en zorg een score van 50% gekregen omdat cyber security een ondersteunende rol kan hebben in deze missies. In het zorgdomein zijn namelijk veel digitale innovaties in ontwikkeling die bijdragen aan het realiseren van een gezonde leefstijl. Tegelijkertijd heeft het zorgdomein te maken met gevoelige persoonsgegevens. Het is dus van belang dat deze gegevens goed worden beschermd en dat de cyber security infrastructuur op orde is. De verwachte bijdrage van het BGP aan het thema Landbouw, water en voedsel heeft een score van 33% gekregen. Dit komt met name door de verwachte bijdrage van het BGP aan de missie beschermde delta omdat daar het MMIP Nederland Digitaal Waterland onder valt. In dit MMIP is het ontwikkelen van digitale systemen die bestand zijn tegen cyber crime opgenomen als één van de doelstellingen.*"

2.3 Economische meerwaarde

Naast versterking digitale weerbaarheid (als maatschappelijke impact) is bevordering van het economisch verdienvermogen een belangrijk argument om te investeren in cybersecurity. Digitale weerbaarheid kost de samenleving onmiskenbaar tijd, geld en capaciteit, maar er zit ook economische meerwaarde in cybersecurity activiteiten voor zowel de aanbiedende partijen[14], als afnemers. Deze paragraaf gaat daar deels kwalitatief, deels kwantitatief op in.

[13] De kleur wit betekent dat er geen tot bijna geen bijdrage is van het BGP aan een maatschappelijk thema. De kleur oranje betekent dat er een beperkte bijdrage wordt verwacht van het BGP aan een thema. De kleur groen betekent dat er een grote bijdrage wordt verwacht van het BGP aan een thema.

[14] Betreft pure players en partial players. Pure players zijn (bedrijven die alleen cybersecurity gerelateerde activiteiten uitvoeren. Partial players bedrijven voor wie cybersecurity niet tot de kern van hun activiteiten behoort. Zie ook TNO 2019 R10769.

Kanttekeningen bij kwantificering economische meerwaarde cybersecurity

Enige kanttekeningen over de informatie en duiding van economische meerwaarde op cybersecurity zijn wel op zijn plaats. Er zijn weinig specifieke kwantitatieve gegevens over cybersecurity in Nederland in algemene zin beschikbaar, laat staan over cyber als economische activiteit.[15] Cybersecurity activiteiten zijn moeilijk te kwantificeren, doordat het vaak een deelverzameling is van, of overlapt met andere economische activiteiten (b.v. ICT). Geijkte databronnen, zoals die van het CBS, zijn daardoor ontoereikend, omdat die geen specifieke classificaties voor cybersecurity bevatten. Voorts zijn de economische effecten van cybersecurity beperkt *direct* en in grote mate ook *indirect*.

Het gebrek aan kwantitatieve gegevens is in 2016 reeds vastgesteld en is tot op heden niet significant verbeterd: “een precieze meting van de waarde van cybersecurity (de uitstralingseffecten van de cybersecurity-sector) voor de economie als geheel blijkt lastig”.[16] Het ministerie van Economische Zaken en Klimaat (Digitale Economie) heeft dit tekort onderkend en zal naar verwachting nader onderzoek laten doen. Dit komt echter te laat voor dit BGP-voorstel.

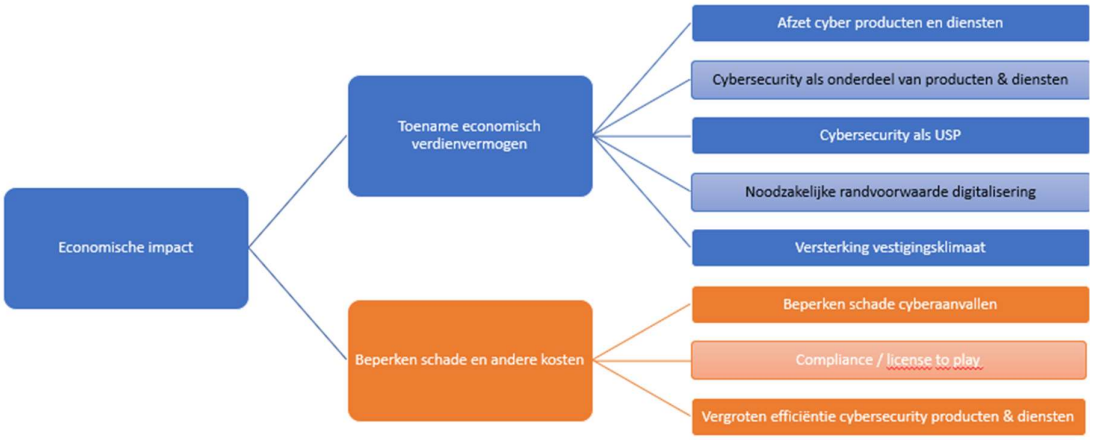
Marktontwikkelingen cybersecurity

Cybersecurity is wereldwijd een groeimarkt. De verwachte groeicijfers van verschillende marktvorsers zitten rond de 8 tot 15% (CAGR 2022-2027), met een wereldwijde omvang van meer dan 130 miljard dollar (2021).[17] Exacte gegevens over de Nederlandse markt ontbreken, maar ING becijfert dat in 2020 tussen de 5 en 7 miljard euro is uitgegeven aan cybersecurity.[18] Dit zou groeien naar 8 tot 11 miljard euro per jaar.

Nederland kent een levendige, hoogwaardige cybersecurity sector, waarvan zich een beperkte groep zich bezig houdt met nieuwe, exporteerbare producten. Het accent ligt op dienstverlening, deels internationaal.[19] Er is de afgelopen jaren sprake van schaalvergroting en consolidatie aan zowel de afnemerskant als aanbodzijde. De trend aan afnemerszijde is dat bedrijven het aantal verschillende in gebruik zijnde cybersecurityproducten wil terugdringen (minder complexiteit, minder kosten). Deze trend zorgt ervoor dat kleine aanbieders verdrongen worden.[20] Aan aanbodzijde is er sprake van consolidatie van leveranciers. Grote techbedrijven nemen cybersecurity bedrijven over (b.v. Mandiant door Google) en grotere cybersecurity bedrijven nemen kleinere cyberbedrijven over (in NL b.v. Fox-IT door NCC (VK) voor 135 miljoen euro en Security Matters door Forescout (VS) voor $113 miljoen). Ook in de cybersecuritysector zijn schaal en kosten relevante economische succesfactoren.

De economische meerwaarde van cybersecurity valt voor Nederland materieel uiteen in 1. toename van het economisch verdienvermogen en 2. het voorkomen of beperken van economische kosten. Beide categorieën hebben zowel directe als indirecte *drivers*.

[15] TNO 2022 R10535
[16] Hendriks, Kocsis et al, SEO Economisch onderzoek en Verdonck Klooster & Associates, Economische Kansen Nederlandse Cybersecurity-Sector, een verkenning, p. 39.
[17] Zie b.v. Mordor Intelligence, Global Cybersecurity Market - Growth, Trends, Covid-19 Impact, And Forecasts (2022 - 2027), 2021. Gartner rapporteert elders in dezelfde orde van grootte. De hierna genoemde cijfers van ING zijn daar tegenover afgezet wel optimistisch.
[18] ING Research, Wat de toenemende cyberdreiging van IT-dienstverleners vraagt, januari 2022.
[19] Zie ter indicatie de leden van Cyberveilig Nederland: https://cyberveilignederland.nl/leden
[20] The European Cybersecurity market - Mapping the opportunities and Route to market for Irish SMEs, Enterprise Ireland, p. 72.



Figuur: directe en indirecte (lichtgekleurde) drivers voor economische waarde van cybersecurity

2.3.1 Toename van het economisch verdienvermogen (value)

a) **Direct: Nationale en internationale afzet van cybersecurity producten en diensten door bedrijven uit Nederland.**
   - Zorgt voor binnenlandse werkgelegenheid (en afzet van product & development)
   - Zorgt voor export.
   - Zorgt voor grotere bedrijven, die in de sector en regio een aanzuigende werking hebben op personeel, startups en investeerders.

b) **Indirect: Afzet producten en diensten waarin cybersecurity componenten zitten**.
   - B.v. ontzorgen van afnemers van (digitale) producten en diensten door óók de beveiliging ervan op te nemen in het (niet-cyber) dienstenpakket. Denk aan medische apparatuur die draadloos is met andere apparaten en die op afstand te besturen zijn.

c) **Direct**: cybersecurity als unique selling point (USP) voor producten en diensten.
   - Dit zien we nog niet veel. Hoe groot is de vraag en hoe groot de mogelijkheden om 'uitmuntende cybersecurity' als USP uit te spelen. Bij banken is het b.v. dat cybersecurity een precompetitief onderwerp is waarop men liever samenwerkt. Het grotere doel is namelijk faciliteren van de digitalisering van financiële processen, waarmee veel kosten worden bespaard (zie hierna bij digitale transformatie). Het is voor klanten (nog) moeilijk controleerbaar of en hoe veilig digitale diensten echt zijn (marktfalen: gebrek aan informatie).
   - Er ligt een economische kans in de juridische macht van Europa. GDPR zorgt voor een vraag naar *privacy enhancing technologies,* zelfstandig (zie 1) of als onderdeel van andere producten en diensten (zie 2). Landen buiten Europa met een grote tech industrie leven in hun thuismarkt onder andere voorwaarden op het gebied van privacy (zie ook bij compliance hieronder). Zodra zij in de Europese markt hun producten af willen zetten levert dit voor Europese (dus ook NL) partijen mogelijk kansen op om de benodigde technologische oplossingen te leveren.
   - Naar verwachting zal de Network and Information Security Directive revisie (NIS 2.0) een boost geven aan de cybersecurity maatregelen die bedrijven moeten nemen. De technologie die nodig is voor deze maatregelen zal kansen opleveren voor bedrijven die (b.v.) monitoring en detectie producten ontwikkelen en aanbieden. Zodra de

wetgeving opgenomen wordt in Nederlandse wetgeving zal de mogelijke economische activiteit als een gevolg hiervan zichtbaar kunnen worden.

d) **Indirect: cybersecurity als noodzakelijke randvoorwaarde voor digitale transformatie**.
   - Arbeidsproductiviteit wordt vergroot door inzet van nieuwe digitale technologie, waarbij cybersecurity nodig is voor een veilige, verantwoorde inzet. B.v. data delen t.b.v. snellere transacties in de fysieke wereld, verhogen van efficiëntie door data of processen gezamenlijk uit te voeren (b.v. cloud), op afstand werken en bedienen van complexe installaties enz. In dit domein zijn ook veel industriële spelers (OEM's) die digitale technologie incorporeren in hun b.v. medische, defensie- of chemische installaties

e) **Indirect: versterking van het vestigingsklimaat** (meer banen naar NL doordat de digitale veiligheid en beschikbaar van de digitale infrastructuur tot de wereldtop behoort).[21]
   - Het is de vraag hoe sterk cybersecurity (en wat dan precies) mee weegt in de besluitvorming van buitenlandse bedrijven om activiteiten naar Nederland te brengen. Factoren die een bijdrage leveren aan een vestigingsklimaat door cybersecurity zijn: een betrouwbare digitale infrastructuur (vooral bandbreedte), beschikking over geografische regionale ecosystemen rondom cybersecurity onderzoek en innovatie en beschikbaarheid van hooggeschoold potentieel (Engelssprekend) personeel.
   - Daarbinnen is het vestigingsklimaat voor cybersecurity bedrijven nog relevant. Nederland heeft internationaal gezien een goede reputatie op kennis en expertise.[22] Op het gebied van productontwikkeling loopt Nederland echter achter, waardoor er afhankelijkheid van het buitenland is ontstaan. Toegang tot kapitaal is daarnaast een knelpunt voor Nederlandse aanbieders om te investeren en op te schalen in cybersecurity.[23] Dit komt mede door de onzekerheid over terugverdienmogelijkheden en een overheid die volgens de sector onvoldoende optreed als *launching customer* en *first mover*.[24] Er is verder een tekort aan cybersecurity professionals om te kunnen voldoen aan de vraag uit het bedrijfsleven.

2.3.2 Voorkomen of beperken van kosten (cost)

a) Direct: beperken van schade als gevolg van cyberaanvallen:
   - Oplossingen die de impact van cyberaanvallen verkleinen, b.v. door aanvallen vroegtijdig te detecteren en af te slaan, of een snellere respons (waardoor er minder (vervolg-)schade ontstaat. Een eerdere schatting van de jaarlijkse schade van cyberaanvallen in Nederland bedraagt volgens Deloitte 10 miljard Euro.[25]

b) **Indirect: compliance aan wet- en regelgeving (license to play).** Primair kost compliance geld, maar vaak is het nodig om 'in business' te blijven of mee te mogen doen in nieuwe marktdomeinen:

[21] Het Verenigd Koninkrijk adresseert het vestigingsklimaat (voor cybersecurity) in zijn cyberstrategie. Zie de National Cyber Strategy 2022, Pioneering a cyber future with the whole of the UK, 2022.
[22] Dialogic, Het Nederlandse investeringsklimaat 2021
[23] Vgl. Cybersprint dat begin 2022 een overnamebod van 47,5 mio euro accepteerde van Darktrace (VK) om verder internationaal te kunnen groeien.
[24] EZK Verdieping Valorisatieketens: Verkenning van het ecosysteem en waardenetwerk Automated Security, TNO 2020 R12224, p. 14-17
[25] Deloitte, Cyber Value at Risk in The Netherlands 2017, 2017

- Regelgeving van overheden (EU, nationaal) of private (internationale) instanties, b.v. de Payment Cards Industrie Compliance Data Security Standard (PCI DSS) voor de financiële wereld. Om aan de standaard te voldoen als marktpartij moeten er kosten gemaakt worden voor cybersecurity. Indien een marktspeler niet compliant is mag deze niet acteren op de markt.
- Verzekeraars stellen voorwaarden voor cyber assurance: zonder compliance moet de organisatie zelf de eventuele schade door cyberaanvallen dekken. Economische meerwaarde is onduidelijk, wel lijkt het erop dat de verzekeraars hier door de toename aan ransomware op aan het toeleggen zijn. De kosten stijgen exponentieel[26] en de voorwaarden voor uitbetaling na een incident zijn nog niet uitgekristalliseerd.[27]
- Compliance aan leveringsvoorwaarden grote afnemers, als license to play om te mogen leveren aan aantrekkelijke klanten. Voorbeelden zijn ABDO[28] Defensie of nieuwe supply chain security initiatieven van het Rijk of industrie. Niet voldoen is geen afzet in dat marktsegment (verlies van omzet). Een ander voorbeeld is de Amerikaanse Executive Order on Improving the Nation's Cybersecurity (mei 2021). Hierin staat dat er een publiekelijk toegankelijke Software Bill of Materials (SBoM) beschikbaar moet zijn voor ieder product.

c) **Direct: vergroten efficiëntie implementatie van cybersecurity maatregelen** beperkt de kosten van cybersecurity zelf en zorgt zo ook indirect voor economische meerwaarde. Als de efficiëntie vergroot wordt zijn er:
   - Minder mensen nodig voor implementatie en/of gebruik (arbeidsproductiviteit van cybersecurity of IT-personeel).
   - Kortere doorlooptijden van implementatie (bespaart menskracht, processen worden korter onderbroken, middelenbeslag en managerial aandacht en kosten).

2.3.3 Marktimperfecties en marktfalen in cybersecurity: noodzaak impuls

Er is in cybersecurity sprake van meerdere vormen van marktfalen, waaronder incentives die op de verkeerde plek liggen, informatie-asymmetrie (tussen aanbieders en klanten) en externe effecten.[29] Cybersecurity wordt bijvoorbeeld ook wel gekenmerkt als een "Lemon Market".[30] Klanten kunnen niet goed beoordelen hoe goed een cybersecurity product is en dus ook niet wat de waarde ervan is.

Ook ENISA constateerde in 2016 dat de Europese interne markt voor cybersecurity imperfect functioneert.[31] Het zijn vooral Amerikaanse bedrijven die de markt domineren en er is meer sprake van een '*supply push*', dan van een '*demand pull'*. Overheidsinterventies blijven daarom nodig, ook

[26] Cyber insurance premiums, costs skyrocket as attacks surge (2021), online: https://www.techtarget.com/searchsecurity/news/252507932/Cyber-insurance-premiums-costs-skyrocket-as-attacks-surge
[27] How the NotPetya attack is reshaping cyber insurance (2021), online: https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/
[28] Algemene Beveiligingseisen voor Defensieopdrachten, deze bevat o.a. diverse voorschriften voor cybersecurity.
[29] Centraal Plan Bureau, Knelpunten op de markt voor cyberveiligheid, 2018. Tyler Moore, Introducing the Economics of Cybersecurity: Principles and Policy Options, International Journal of Critical Infrastructure Protection, 2010
[30] Bruce Schneier, How Security Companies Sucker Us With Lemons, 2007, https://www.wired.com/2007/04/securitymatters-0419/. Debate Security, Cybersecurity Technology Efficacy. Is Cybersecurity Technology the New "Market for Lemons"?, 2020.
[31] ENISA, Cybersecurity as an Economic Enabler, 2016

voor stimulering van onderzoek en ontwikkeling. Nederland investeert echter maar een fractie in cyberveiligheid van wat andere landen (relatief t.o.v. hun bbp) investeren.[32] Minder dan 0,01% bbp, t.o.v. de VS meer dan 0,3% bbp. Dat laatste levert samen met de grote thuismarkt een aanzienlijk schaalvoordeel op, wat Nederland (en Europa met zijn intern verdeelde markt) ontbeert. Producten uit de VS kunnen door hun schaalvoordeel goedkoper zijn én beter. De grotere schaal zorgt namelijk ook voor meer gebruiksdata en meer middelen om te herinvesteren in (verbetering van) producten.

2.3.4 Tussentijdse toets op economische waarde

Ook naar de economische impact is gekeken in het kader van de tussentijdse toets.[33] De economische impact dimensie "*geeft inzicht in hoe de sectoren die gelinkt kunnen worden aan het voorstel zich ontwikkelen op bepaalde economische indicatoren. Dit geeft een beeld van hoe de resultaten van het BGP in potentie kunnen 'landen' (worden geabsorbeerd) in de economie. Daarmee kan (indirect) een beeld worden geschetst van de potentiële economische impact van het voorstel.*"

Het BGP scoort gemiddeld tot hoog op deze dimensie.

2.1 Aantal direct betrokken bedrijfstakken in productie van technologie	5
2.1 Aantal indirect betrokken bedrijfstakken (vanuit opname toepassingen)	23
2.2 Werkgelegenheid bedrijfstakken	
2.2.1 Percentage werkgelegenheid in betrokken bedrijfstakken t.o.v. Nederland totaal	79%
2.2.2 Groei werkgelegenheid in betrokken bedrijfstakken (in %)	1,5%
2.3 Verdienvermogen bedrijfstakken	
2.3.1 Toegevoegde waarde (TW) betrokken bedrijfstakken t.o.v. totaal TW (%)	78%
2.3.2 Gemiddelde groei toegevoegde waarde (TW) 2013-2020 (in %)	1,5%
2.3.3 Groei arbeidsproductiviteit 2013-2020 (in %)	0,3%

"Volgens de experts zijn er bij het produceren van de hiervoor benodigde technologie vijf bedrijfstakken relevant (van de in totaal 39 SBI bedrijfstakken): de elektrotechnische sector, elektrische apparatenindustrie, de machine industrie, telecommunicatiesector en de sector informatietechnologie en informatiediensten.

Cyber security technologieën en innovaties kunnen worden toegepast in vrijwel alle sectoren van de Nederlandse economie. (…) Echter is er wel verschil per bedrijfstak in de mate waarin cyber security technologie wordt toegepast.[34] Volgens de experts zijn er 23 sectoren[35] waar bij cyber security

[32] Rademaker et al. 2016, aangehaald in CPB, 2018. N.b. dit cijfer lijkt wel aan de lage kant, als het wordt afgezet tegen het totaal aantal in cybersecurity werkzame personen en de cijfers die ING Research noemt.
[33] Ook TNO en bij de toets betrokken experts merken op dat het niet mogelijk is "*om de directe impact van de kennis die voortkomt uit het BGP op bijvoorbeeld het bbp te schatten.(…) Er is geen ex-ante evaluatiemethode die de impact van individuele onderzoeksprogramma's kan inschatten.*"
[34] Om deze reden zijn de bedrijfstakken die een rol spelen in de toepassing geselecteerd aan de hand van de volgende criteria: 0 = technologie uit het BGP is standaard onderdeel van de bedrijfsvoering, dit geldt voor iedereen als een bedrijfsrisico. 1 = de technologie wordt breed toegepast door bedrijven actief in deze bedrijfstak. 2 = de bedrijfstak speelt een rol in de productie van de technologie. De 23 genoemde sectoren hebben dus de score 1 gekregen en refereren aan bedrijfstakken waar de BGP technologie breed toegepast wordt door (vrijwel) alle actoren in deze bedrijfstak
[35] Het betreft de sectoren: Landbouw, bosbouw, visserij; Delfstoffenwinning; Voedings-, genotmiddelenindustrie; Grafische industrie; Aardolie-industrie; Chemische industrie; Farmaceutische industrie; Basismetaalindustrie; Metaalproductenindustrie; Auto- en aanhangwagenindustrie; Overige transportmiddelenindustrie; Reparatie en installatie van machines; Energieproductie; Water en afvalbeheer; Groot- en detailhandel; Vervoer en opslag; Filmindustrie, radio en televisie; Financiële diensten; Juridische diensten, accountancy en consultancy; Architecten en ingenieursdiensten; Specialistische en overige zakelijke diensten; zorg en welzijn.

technologie breed in de sector kan worden toegepast.[36]

Doordat cyber security met name in de toepassing impact heeft op een brede set aan sectoren, vertegenwoordigen deze bedrijfstakken een hoog percentage van de Nederlandse werkgelegenheid, namelijk 79%. De werkgelegenheid in deze bedrijfstakken is tussen 2013 en 2020 met 1,5% gegroeid. Dit is hoger dan de gemiddelde groei van de werkgelegenheid in Nederland, die in dezelfde periode 1,3% bedroeg. De toegevoegde waarde van de betrokken sectoren betrof 78% van de totale Nederlandse toegevoegde waarde in 2020. De gemiddelde groei van de toegevoegde waarde van de betrokken sectoren bedroeg 1,5% tussen 2013 en 2020 – net iets onder het landelijk gemiddelde over dezelfde periode. De groei in arbeidsproductiviteit over dezelfde periode bedroeg voor de geselecteerde sectoren 0,3%; een iets hogere score dan het landelijk gemiddelde.

Op basis van bovenstaande kan geconcludeerd worden dat de potentiële impact van dit BGP op de economie zich spreidt over een groot aantal sectoren, met relatief groot percentage betrokken werkgelegenheid en toegevoegde waarde. Met name in de toepassing is er sprake van een grote spreiding van sectoren. De groei van de werkgelegenheid en arbeidsproductiviteit liggen beiden rond het landelijk gemiddelde."

Verder geeft de tussentijdse toets inzicht in de capaciteit van het ecosysteem om het BGP Cybersecurity om te zetten in meer concurrentievermogen. Hoe hoger het percentage in de tweede kolom van de tabel, hoe groter de potentiële impact, en hoe hoger de kans op succes. De score van het BGP Cybersecurity is gemiddeld hoog (groen).

4.1 Concurrentievermogen van bedrijfstakken betrokken in productie	70%
4.2 Innovatievermogen bedrijfstakken	67%
4.3 Sterke technologieën	68%
4.4 Sterke kennisvelden	66%

"Van de vijf bedrijfstakken die betrokken zijn in de productie (zoals geïdentificeerd in de context van Dimensie 2) zijn drie sectoren (erg) concurrerend: Elektrische apparatenindustrie, Machine-industrie en Informatietechnologie en informatiediensten. Dit betekent dat deze sectoren een sterkere groei in toegevoegde waarde en in export vertonen ten opzichte van andere EU15 landen. Nederland kan daarom voor 70% bouwen op sterk concurrerende bedrijfstakken, wat een relatief sterke positie betekent. Hoge niveaus van export en toegevoegde waarde suggereren namelijk een sterke concurrentiepositie, en daarom kan Nederland concurrerend worden in cybersecurity.

De kans dat Nederland in staat is om de innovaties te laten landen in de markt hangt ook af van het innovatievermogen van de sectoren betrokken in de toepassing. Hoe innovatiever een sector is, hoe groter de kans is dat nieuwe technologieën worden opgepakt en toegepast. Van de 23 sectoren die de technologie moeten toepassen (zie Dimensie 2) zijn met name de Chemische industrie en daarnaast ook de Voedings-, genotmiddelenindustrie, Aardolie-industrie, Farmaceutische industrie, Basismetaalindustrie en de Auto- en aanhangwagenindustrie innovatief. De andere sectoren zijn gemiddeld of minder innovatief en de kans is minder groot dat innovaties goed in deze markten zullen landen. Wanneer de verhouding van sterke sectoren wordt doorgerekend is 67% hier innovatief. Dit geeft Nederland een gemiddeld sterke uitgangspositie voor Cyber Security.

2.4 Strategische autonomie cybersecurity

Strategische autonomie is de derde strategische overweging om te investeren in kennis en innovatie in cybersecurity. Strategische autonomie is geen einddoel, maar een manier om meer

[36] De impact wordt bepaald op de som van alle sectoren – zowel in productie als toepassing.

handelingsperspectief te creëren ter bevordering van de eigen positie (van Nederland). Het beschermen van Nederlandse economische- en veiligheidsbelangen hangt mede af van de innovatiekracht van de Topsectoren en de capaciteit om hun missies voor de toekomst veilig vorm te geven.[37] Het ontwikkelen en toepassen van innovatieve cybersecurity oplossingen draagt bij aan de maatschappelijke transities waar de Topsectoren naartoe werken. Daarnaast levert het slagkracht op om belangrijke cybersecurity thema's gecoördineerd aan te pakken. Kennis wordt meerjarig opgebouwd en vervolgens geborgd in de Nederlandse maatschappij.

2.5 Rol van sleuteltechnologieën en kennisvelden

Aan de 'input' kant van het theory of change model staan o.a. de sleuteltechnologieën en kennis die we in Nederland kunnen mobiliseren. Cybersecurity is een sterk multidisciplinair terrein.[38] Dat is terug te zien in de vele kruisverbanden per sector en wetenschappelijke disciplines. In onderstaande tabel zijn de domeinen en thema's met de wetenschappelijke disciplines verwerkt (Alpha (α) Beta (β) en Gamma (ɣ)):

Sleuteltechnologieën	High performance & grid computing	Sensoren (incl quantum)	Artificial intelligence	Data analytics	Encryption	Robotics	Quantum
Transport		β/ɣ	α/β/ɣ				β
Energie	α/β/ɣ						β
Water & Maritiem		β	α/β/ɣ	β	β		
HTSM	β		α/β/ɣ			β	β
Agri & Food		β/ɣ	α/β/ɣ	α/β/ɣ		α/β/ɣ	
T&U		β	α/β/ɣ	β		β	
LSH	α/β/ɣ	α/β/ɣ	α/β/ɣ	α/β/ɣ	α/β/ɣ	α/β	β
Creatieve industrie					α/β/ɣ		
Human Capital				α/β/ɣ	α/β/ɣ		
Publieke sector				α/β/ɣ	α/β/ɣ		β
Samenleving			α/β/ɣ	α/β/ɣ	α/β/ɣ	α/β/ɣ	β

Sleuteltechnologieën worden op twee manieren geadresseerd in het BGP Cybersecurity: als *enabler* van cybersecurity technologie (geel), als toepassingsgebied voor cybersecurity technologie (**niet** gearceerd) of beide (groen). Onderstaande tabel laat zien welke wetenschappelijke disciplines relevant zijn, gebruik makend van de CWTS[39], geplot op alfa, Bèta en Gamma:

Alfa	**Bèta**	**Gamma**
Social Sciences & Humanities Filosofie, Communicatie wetenschappen Sociologie Psychologie Politicologie Ethiek	Computer Science/ICT Mathematics	Rechtswetenschappen Criminologie Bedrijfskunde Economie/econometrie

[37] Veenendaal, M.A., Schie, T.C.C. van, Rademaker, M., & Faesen, L. (2021), *Soevereiniteit en Digitale Autonomie, online:* https://hcss.nl/report/soevereiniteit-en-digitale-autonomie/

[38] Suggestie van ACCSS: het door aangereikte BGP format is puur technisch ingestoken, begrijpelijk omdat het afgeleid is van het topsectoren beleid en de KIA Sleutel Technologieën. ACCSS zou niet technische aspecten zoals "transitie naar een veilige digitale samenleving", "digitale soevereiniteit", "security & sociale media" en "privacy" ook een plek in het format willen geven.

[39] Centre for Science and Technology Studies

De vraaggestuurde cyberthema's (zie hoofdstuk 3) behoeven vrijwel allemaal onderzoek en innovatie over de hele TRL ladder heen. Dit verschilt uiteraard per specifiek onderwerp binnen een thema. Fundamenteel onderzoek, toegepast onderzoek, product-/dienstontwikkeling zijn allen in scope. Implementatie en feitelijke toepassing formeel niet, maar hier zullen wel inhoudelijke randvoorwaarden voor worden geschapen.

2.5.1 Tussentijdse toets over sleuteltechnologieën

De tussentijdse toets heeft ook de relatie onderzocht tussen het BGP Cybersecurity en de sleuteltechnologieën. Niet verrassend is de hoge score op digitale technologieën (Topsector ICT is één van de trekker), quantum technologie en de cross-overs tussen alfa, beta en gamma.

3. 1 De bijdrage van Advanced materials	0%
3. 2 De bijdrage van Quantum technologies	83%
3.3 De bijdrage van Photonics & light technologies	0%
3.4 De bijdrage van Digital technologies	100%
3.5 De bijdrage van Nanotechnologies	0%
3.6 De bijdrage van Chemical technologies	0%
3.7 De bijdrage van Life sciences technologies	0%
3.8 De bijdrage van Engineering & fabrication technologies	42%
3.9 Crossovers: bijdrage van alpha, beta en gamma	2

"Cyber security is een systeemaspect en is ondersteunend aan veel sectoren, cyber security is daarmee ingebed in de gehele keten. De experts verwachten daarnaast dat het BGP specifiek relevant is voor enkele sleuteltechnologieclusters. De grootste bijdrage wordt verwacht in het cluster Digital Technologies, waar de experts verwachten dat het BGP een substantiële bijdrage (kern rol) zal leveren aan alle zes de onderliggende sleuteltechnologieën. Ook verwachten de experts dat het BGP een grote bijdrage zal leveren aan het sleuteltechnologiecluster Quantum Technologies. In twee van de drie onderliggende sleuteltechnologieën (Quantum computing; Quantum communication) speelt het BGP volgens de experts een kern rol en de derde onderliggende sleuteltechnologie (Quantum sensors and metrology) speelt het BGP een ondersteunende rol. Daarnaast is het BGP volgens de experts relevant voor drie van de zes onderliggende sleuteltechnologieën in het cluster Engineering & fabrication technologies: Sensors & Actuators, Cyber physical/embedded systems (in beide een kern rol) en Robotics (ondersteunende rol)."

"Volgens de experts zijn er vijf kennisvelden die een kern rol spelen bij de ontwikkeling van cyber security; hiervan hebben er twee een sterke positie (Informatie- en communicatie wetenschappen en sociale en gedragswetenschappen) en drie een gemiddeld sterke (computerwetenschappen, electro-techniek) of zwakke positie (wiskunde). Tevens zijn er vijf kennisvelden die een ondersteunende rol spelen. Deze zijn over het algemeen relatief sterk tot sterk: economische wetenschappen; geschiedenis, filosofie en religie; Politieke wetenschappen; Psychologische wetenschappen; Rechten en criminologie; Sociologie en antropologie. Hierdoor komt de totale score uit op 66%."

3 Kennis en Innovatie Agenda Cybersecurity

Het BGP Cybersecurity bestaat uit een ecosysteem van partijen, een agenda en programmering. Dit hoofdstuk gaat in op de agenda.

3.1 Kennis- en Innovatie Agenda met zeven thema's

In workshops met experts uit de betrokken Topsectoren, aanvullende gesprekken en deskresearch zijn de volgende zeven gedeelde cybersecurity thema's geïdentificeerd voor kennis en innovatie, en ingedeeld langs Technologie, Toepassing en Randvoorwaarden:

	Technologie/kennis	Toepassing	Randvoorwaarde
Security by design			
Veilig datagedreven werken			
Veilige en robuuste connectiviteit			
Veilige OT/IoT en integratie met IT			
Cyberrisicomanagement			
Systeem- of ketenveiligheid			
Awareness, kennis en vaardigheden			

Deze thema's weerspiegelen gezamenlijke cybersecurity probleemgebieden, die moeten worden opgelost om de maatschappelijke transities digitaal veilig te kunnen doorvoeren. De thema's zijn relatief hoog-over, om de gemene deler te blijven beschrijven, en in lijn met de NLCS in wording, alsmede de nieuwe i-Strategie. Dat vergde een scherpe inhoudelijke discussie tussen Topsectorvertegenwoordigers en experts, zowel over de maatschappelijke context, als over cybersecurity technologie (mens, organisatie, techniek). Wat is het securityprobleem precies? Is daar al geen oplossing voor? Is het probleem van de ene Topsector niet vanuit cybersecurity perspectief hetzelfde, of juist verschillend? Is er al een oplossing op de markt, of moeten we iets nieuws gaan verzinnen?!

De thema's zijn inhoudelijke input voor NWO Missie calls en zijn later in het totstandkomingsproces vertaald naar use cases, waarin concretere probleemstellingen in een bepaalde context zijn geprioriteerd. Deze vormen de basis voor de multisectorale TKI-calls (zie H4).

3.1.1 Security by design

Het verhogen van de cyberweerbaarheid door security by design (of 'by default') is een stip op de horizon die door alle Topsectoren benoemd is. Een selectieve maatregel kan voldoende bescherming bieden voor een select proces, maar houdt geen rekening met of biedt onvoldoende bescherming met de andere (operationele) processen. Cybersecurity dreigingen richten zich op de hele organisatie en netwerken. Daarom uiten de Topsectoren de behoefte aan normen en een referentiearchitectuur voor te ontwikkelen hardware en software. Een afsprakenstelsel voor minimale eisen van hard- en software en de werking ervan (denk aan identificatie, authenticatie en autorisatie van datastromen). Door een security by design aanpak willen de Topsectoren ervoor zorgen dat processen en apparaten veiliger worden én dat de uitval ervan minder schade teweegbrengt in de organisatie.[40] Ook de governance binnen en tussen organisaties hoort bij dit

[40] Inspiratie o.a. bij NCSC UK cyberstrategie voor 2030, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049345/cyber-security-strategy-2022.pdf

vraagstuk: hoe worden de normen of afspraken toegepast en geborgd gedurende de levenscyclus van systemen en hun bijbehorende fysieke platforms?! Technologie en toepassing.

3.1.2 Veilig datagedreven werken

Dit is een vaak genoemd thema. De maatschappelijke transities van de Topsectoren worden namelijk in hoge mate ondersteund door het gebruik van data science en AI. Data staat centraal. Daarom zijn er kennis- en innovatievragen over het gebruik en totstandkoming ervan en is men benieuwd naar de mogelijke risico's. Topsectoren zijn op zoek naar manieren om geautomatiseerd data te delen en analyseren en deze data op te werken naar bedrijfs- en sectorspecifieke voorspellingen. Men is onvoldoende op de hoogte en geëquipeerd om veilig data uit te wisselen tussen bedrijven en tussen bedrijven en publieke instellingen. Daarnaast is onvoldoende bekend hoe de betrouwbaarheid en veiligheid van datastromen die input leveren aan cruciale modellen en systemen gegarandeerd kunnen worden (authenticiteit en betrouwbaarheid van de bron, integriteit en vertrouwelijkheid van data gedurende opslag, transport en verwerking). Samenwerking, digitalisering en lange bewaartermijnen stellen speciale eisen aan cybersecurity, aan digitaal data delen en aan borging van intellectueel eigendom en kroonjuwelen. Er moeten toekomstbestendige afspraken (technische) gemaakt worden over wie wel of niet bij welke data en modellen mogen komen, digitaal gezekerd is, zonder dat dit een efficiënte samenwerking in de weg staat.

Het is een onderwerp dat speelt in vrijwel alle Topsectoren, bijvoorbeeld bij het veilig aansturen en monitoren van industriële controlesystemen op afstand, maar ook bij het vertrouwen van sensordata van open (GPS- en weerdata) en gesloten (bedrijfsinterne) bronnen. De authenticiteit van (digitale)media is b.v. ook een punt van zorg. Welke bronnen zijn nog te vertrouwen en zijn daar technologische waarborgen voor te ontwikkelen? Ook spelen juridische ethische vraagstukken een rol in de maatschappelijke uitdagingen van de Topsectoren. Men vraagt zich af of de huidige manier van dataeigenaarschap en dataverzameling nog wel mag en moet. Welke Privacy Enhancing Technologies (PET) moeten (door)ontwikkeld worden om klaar te zijn voor de toekomst? Vernieuwende toepassingen worden op dit moment ondersteund door technieken zoals Federated Learning en multi-party computation. Cryptografie (quantum-safe) als hulpmiddel voor authenticatie, integriteit en vertrouwelijkheid is eveneens een ondersteunende technologie. Idem automatisch kunnen labelen van (gevoelige) data. Is Nederland in staat om een afsprakenstelsel te ontwikkelen of beïnvloeden dat als blauwdruk kan dienen voor meerdere sectoren? Hoe werkt een dergelijke technologie in samenwerking met bestaande diverse groepen van actoren en andere afsprakenstelsels? Een voorbeeld hiervan is een blauwdruk die de transportsector kan gebruiken voor zowel leveranciers, als met de bloemenveilig Flora Holland, en de digitale systemen van de douane in binnen- en buitenland. Technologie en toepassing.

3.1.3 Veilige en robuuste connectiviteit

Een toekomstbestendig innoverend Nederland is afhankelijk van een veilige digitale infrastructuur. Datagedreven werken valt of staat met connectiviteit. Dat wil zeggen; vertrouwen in de draadloze en bekabelde verbindingen, én in de protocollen en standaarden die de functionaliteit, beschikbaarheid en veiligheid van verbindingen waarborgen. De vraag naar (veilige) connectiviteit blijft groeien, mede door de aanstaande breed uit te rollen technieken zoals 5G en 6G. Topsectoren zijn benieuwd naar de beveiliging van de fysieke infrastructuur maar ook naar het afsprakenstelsel dat daar een cruciale rol in speelt. Welke rol gaat het kwantuminternet spelen, hoe blijven netwerken van de toekomst synchroon (synchronisatie van atoomklokken)?Gezamenlijk optrekken voorkomt dat elke sector een eigen wiel gaat uitvinden, waardoor connectiviteit tussen systemen en data uit verschillende sectoren geborgd wordt op de lange termijn. Cross-sectorale samenwerkingen

zijn vereist voor de volgende stadia van de ontwikkelingen; mobiliteit van de toekomst vereist bijvoorbeeld dat stedenbouwkundigen en de telecomindustrie met elkaar ontwikkelen. Connectiviteit maakt gegevensoverdracht, gegevensopslag en gegevensuitwisseling mogelijk als onderdeel van de voortgaande digitalisering.

3.1.4 Veilige OT en IoT en integratie met IT

De verwevenheid van IT en OT neemt in toenemende mate toe bij kritische (productie)processen. Apparaten en systemen praten met elkaar, lezen sensoren uit en worden door externen onderhouden en gemonitord. Topsectoren hebben onvoldoende grip op de risico's en dreigingen die deze integratie oplevert. Daarnaast is er onvoldoende begrip van beschikbare en inzicht in te ontwikkelen beheersmaatregelen. De verwevenheid van IT en OT is organisaties veelal ingeslopen vanuit het oogpunt van efficiëntie en functionaliteit. Topsectoren hebben behoefte aan kennis over deze integratie. Bij de uitwerking van use cases is dit o.a. verder verdiept naar het goed in kaart kunnen brengen van de risico's in complexe IT/OT omgevingen, modeleren en simuleren van dit soort omgevingen. Er liggen ook raakvlakken met de thema's cyberrisicomanagement en systeem- en ketenveiligheid.

3.1.5 Cyberrisicomanagement

Meerdere Topsectoren hebben aangegeven grote behoefte te zien voor innovatie op effectief en adequaat cyberrisicomanagement. Om te weten welke risico's van toepassing zijn is er meer kennis en toepassing nodig van (IT) asset management. Tevens zijn data en modellen nodig over de impact van cybersecurity dreigingen, de beschikbare maatregelen en de afhankelijkheid van ketens (b.v. de supply chain).[41] Het gaat hierbij om intern risicomanagement. Voor de nabije toekomst zou innovatie een rol kunnen spelen om real-time data te gebruiken voor risicomanagement (in tegenstelling tot statische gegevens). Een grote uitdaging is dat risico indicatoren en maatregelen niet kwantificeerbaar zijn, waardoor het profijt van investeringen ondermaats ingeschat wordt. De onderschatting leidt tot onvoldoende beschermingsmaatregelen. Onderdeel van cyberrisicomanagement is het inrichten van en oefenen met crisisorganisatie. Met name in geval van keten- of systeemaanvallen is snelle en effectieve coördinatie over individuele organisaties essentieel om aanvallen af te wenden of (economische en/of maatschappelijke) schade te beperken.

3.1.6 Systeem- en ketenveiligheid

Topsectoren hebben ook de behoefte geuit voor bedrijfsoverstijgend mitigeren van risico's. Digitale weerbaarheid van ketens of van een systeem van componenten (of organisaties) is door de soms eenvoudige verspreiding van cyberdreigingen noodzakelijk. Kunnen cascade-effecten of grote geaccumuleerde schade worden voorkomen!? Het gaat dan bijvoorbeeld om het hacken van leveranciers van een bedrijf dat hoogtechnologische beveiligingsapparatuur ontwikkelt en dan daar tot digitale spionage of sabotage leidt. Of om het tegelijkertijd verstoren van meerdere sluizen in de grote waterwegen van Nederland.

Systeem- of ketenveiligheid omvat supply chain security als specifieke verschijningsvorm. Dat organisaties onderdeel zijn van lange en complexe, tijdkritieke supply chains is voor velen een gegeven. Er is aanvullende kennis nodig om de cyberrisico's in complexe supply chains inzichtelijker te maken en te mitigeren. De effecten van incidenten of verstoring in de keten zorgen voor effecten waar bedrijven niet op voorbereid zijn. Een ander soort risico betreft hier niet de bedrijfsvoering,

[41] Voorbeeld van een model is breder toegankelijkere versie van de Algemene Beveiligingseisen Defensieopdrachten 2019 (ABDO).

maar digitale componenten die verderop in de keten worden geassembleerd in een groter product. Een specifieke categorie hierbinnen is software. Grote applicaties bevatten vele componenten en componenten van componenten, die bij elke update weer veranderen in samenstelling.[42] Op basis van een modern cyberrisicomanagement moeten de juiste beheersmaatregelen gekozen en geïmplementeerd worden. De behoefte hieraan is op dit moment al groot en de verwachting is dat dit de komende jaren enkel in belang toeneemt.

3.1.7 Cybersecurity awareness, kennis en vaardigheden

Misschien wel het belangrijkste gemeenschappelijke knelpunt en zeker randvoorwaarde voor succes van cybersecurity is het kunnen beschikken over voldoende kennis en vaardigheden en tijdig en voldoende prioriteren van het onderwerp. Bedrijven hebben het onderwerp cybersecurity echter niet of onvoldoende op de agenda staan,[43] omdat b.v. bestuurders onvoldoende op de hoogte van de dreigingen en/of het onderwerp onvoldoende (concreet) agenderen. Bedrijven hebben daarnaast beperkt zicht op de wet- en regelgeving. Een van de gevolgen daarvan is dat lagere managementniveaus geen capaciteit hebben om de organisatie te beschermen of te voldoen aan wet- en regelgeving (compliance). Bestuurders moeten in staat gesteld worden om de risico's te besturen en de verantwoording te nemen.

Daarnaast is het personeelsvraagstuk breed onderkend. Ook al krijgt het onderwerp voldoende prioriteit, het tekort aan gekwalificeerd cyberpersoneel en voldoende kennis bij niet-cyberpersoneel is alsnog een belemmering. Bedrijven en overheden kunnen de cybersecurity-vacatures niet vullen door een gebrek aan geschoold personeel en de hoge doorloopsnelheid van werknemers. Capaciteit wordt extern ingehuurd over langere perioden met als gevolg een zwakke eigen kennispositie en beperkte interne cultuur van cybersecurity-personeel. Er zijn wel meerdere initiatieven gestart.[44] Zo is de Human Capital Agenda ICT samen met haar partners bezig met de uitvoering van een plan om meer ICT-professionals op te leiden doormiddel van omscholing.

Medewerkers zijn onvoldoende op de hoogte van wat veilig (digitaal) gedrag is, of weten dat wel maar voeren dat gedrag niet uit. In samenwerking met bestuurders moet getoond worden wat de kosten en impact van verstoringen zijn. Daarnaast moet het 'digitale veiligheidsdenken' aangeleerd worden en veilig gedrag moet de norm worden; het is een randvoorwaarde voor toekomstbestendige innoverende en digitaliserende organisaties. Hier kan een rol voor HCA liggen in de vorm van bewustwording en vaardigheden bij brengen bij het personeel. Ook de creatieve industrie kan bijdragen aan innovatieve vormen van kennisoverdracht, bewustwording en de vertaling naar handelingsperspectief.

[42] Log4J is hier een goed voorbeeld van. Deze Java component zit in talloze applicaties overal ter wereld, zonder dat beheerders zich daar altijd bewust van zijn.
[43] Zie b.v. eindrapportage Cybervolwassenheidsonderzoek (2021), DCMR Milieudienst Rijnmond, online: https://www.dcmr.nl/sites/default/files/2021-10/Eindrapportage%20Cybervolwassenheidsonderzoek%20DCMR%20v1.1.pdf
[44] Andere initiatieven komen o.a. van EZK, Security Delta (HSD) en Centrum voor Veiligheid en Digitalisering

4 Programma

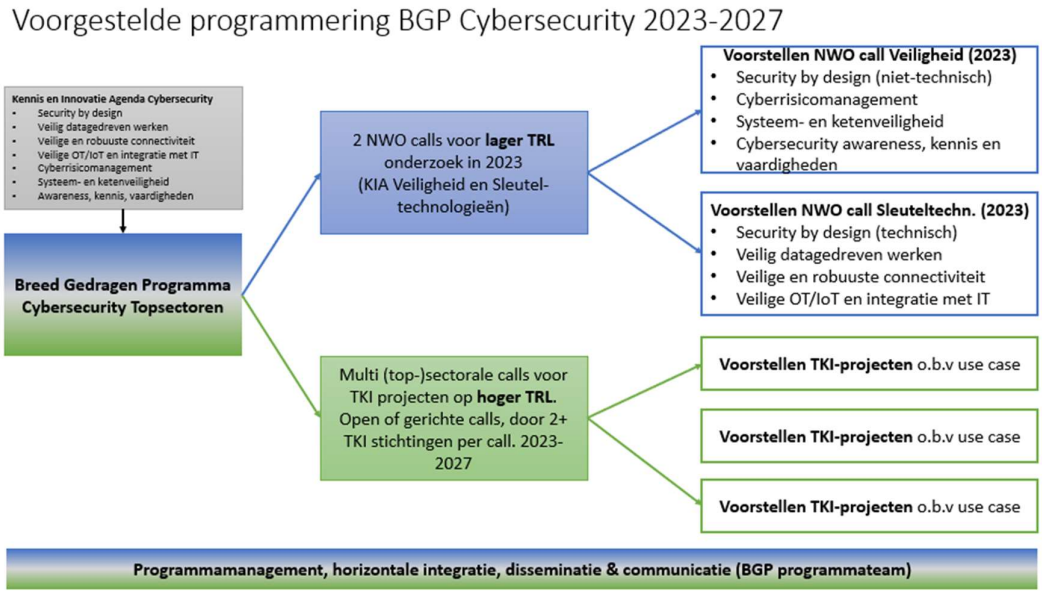
Het BGP Cybersecurity bestaat uit een ecosysteem van partijen, een agenda en programmering. Dit hoofdstuk gaat in op de twee sporen in de programmering. Uitgangspunt bij de programmastructuur was het vermijden van nieuwe instrumenten en juist de beoogde activiteiten in te vlechten in bestaande mechanismen en structuren.

4.1 Programmastructuur

Tijdens de programmavorming voor het Breed Gedragen Programma (BGP) Cybersecurity is een brede groep opgebouwd, die zich heeft geschaard achter een kennis- en innovatieagenda van 7 cybersecurity thema's. Het doel is vanaf 2023 ook daadwerkelijk samen te gaan programmeren en onderzoeks- en innovatieprojecten te laten starten. Dit langs twee sporen:

- Ten eerste een lager TRL spoor o.b.v. NWO Missie calls, de duur van projecten hier is 48+ maanden (i.v.m. duur PhD's).
- Ten tweede een hoger TRL spoor met TKI (innovatie-)projecten, met variabele duur en omvang.

Voor het eerste spoor is het voorstel KIC NWO-middelen in te zetten (vanuit de KIA ST[45] en KIA Veiligheid, evt. i.c.m. private cofinanciering, afhankelijk van de call-condities van NWO). Dit hangt als gezegd af van de besluitvorming binnen beide Kernteams en uitwerking i.s.m. NWO en de Kernteams. Voor het tweede spoor is het beoogd doel TKI-middelen in te zetten (PPS Toeslag)[46], private cofinanciering, publieke cofinanciering (Defensie) en ROM[47]-middelen. De TKI-stichtingen bepalen wanneer en in welke mate dat gebeurd.



Figuur: overzicht programmering BGP Cybersecurity 2023-2027

[45] Bij schrijven nog niet besloten in de KIA ST. Voor de KIA Veiligheid ligt er wel een besluit om volgend jaar cybersecurity te programmeren. De BGP-thema's worden o.b.v. inhoud over beide NWO Missie calls verdeeld.
[46] https://www.rvo.nl/subsidies-financiering/pps-toeslag-onderzoek-en-innovatie/voor-tkis
[47] Regionale Ontwikkel Maatschappijen. Ook deze zijn inmiddels betrokken bij de uitwerking van dit voorstel.

Het zwaartepunt van het BGP cybersecurity programma ligt op de twee inhoudelijke sporen. Er is daarnaast ter ondersteuning van het hele programma een programmabureau, waarin activiteiten als initiatie van call processen, communicatie, disseminatie en horizontale integratie plaats vinden (zie ook hierna).

4.2 Spoor NWO Missie calls

Het BGP-voorstel voorziet in een spoor fundamenteel onderzoek, met beoogde financiering vanuit de KIC-middelen. Doelgroepen voor uitvoering zijn (o.a.) WO en HBO. Het onderwerp cybersecurity of -veiligheid komt zowel in de Kennis en Innovatie Agenda (KIA) Sleuteltechnologieën (ST, MJP-55) als Veiligheid (MMIP-4) terug. De noodzaak en urgentie om te acteren is groot, de ruimte beperkt. Een combinatie van KIC calls uit beide KIA's is aanbevelenswaardig. De vraag is, hoe de thema's te verdelen over beide KIC-calls. Daarvoor is gekeken naar de inhoudelijke ambities van beide KIA's. Hiervoor is gekeken naar de beoogde omvang van de beschikbare KIC middelen en de inhoudelijke accenten.

De **KIA ST** zet in op sleuteltechnologieën, voor toekomstige economische kansen, en om vanuit de topsectoren gericht technologische bijdragen te laten leveren aan het oplossen van maatschappelijke uitdagingen. Cybersecurity valt in de KIA ST binnen Digital Technologies, Team Dutch Digital Delta. Het Meerjarenprogramma (MJP) 55 Cyber bouwt inhoudelijk voort op de Nationale Cyber Security Research Agenda III (NCSRA, 2018) en houdt een brede inhoudelijke scope aan.

KIA Cyberveiligheid: Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren. Hiervoor zijn vijf *deelprogramma's* geïdentificeerd: Bestrijden cybercrime, Bevorderen ontwikkeling cybercompetenties, Defensieve cybertechnologie, Offensieve cybertechnologie, Ketenweerbaarheid en governance. Ook de KIA Veiligheid bouwt voort op de NCSRA III.

Na overleg met NWO en bespreking in de stuurgroep BGP is de onderstaande verdeling van BGP thema's over de twee beoogde KIC calls het uitgangpunt voor uitwerking in Q4 2022 (N.B. beide Kernteams worden vanuit hun rol betrokken bij de verdere uitwerking!):

KIA Sleuteltechnologieën: technologie gedreven cybersecurity onderwerpen binnen de 7 BGP thema's	**KIA Veiligheid: niet-technologie gedreven en sterk multidisciplinaire onderwerpen (m.n. ook 'softe' disciplines) binnen de 7 BGP thema's**
• Security by design • Veilig datagedreven werken • Veilige en robuuste connectiviteit • Veilige OT/IoT en integratie met IT	• Security by design (niet technisch) • Cyberrisicomanagement • Systeem- of ketenveiligheid (incl. supply chain security) • Cybersecurity awareness, kennis en vaardigheden

NWO voorziet de volgende aanpak voor concretisering van beide calls:

T.a.v. de Missie Veiligheid call: Doel openstelling call is Q1 2023. Regie over het proces ligt bij NWO. Het kwartiermakersteam BGP Cybersecurity ondersteunt waar nodig. Daarvoor moet vooral in Q4 2022 werk verricht worden door een klankbordgroep. Streven is om via Click.NL ook het perspectief van sleutelmethodologieën te betrekken in de houtskoolschets.

Na openstelling call zal nog ondersteuning door klankbord groep plaatsvinden. Het 'ecosysteem' incl. eindgebruikers wordt betrokken middels klankgroepsessies. Leden voor de klankbordgroep worden aangezocht uit Kernteam Veiligheid, NWO, HBO, cyberindustrie, departementen en dcypher.

T.a.v. Missie ST call: hier moet nog goedkeuring vanuit de KIA zelf komen (oktober 2022), incl. definitieve bepaling van de omvang. De interne goedkeuring bij NWO volgt daarna. Daarmee loopt deze call ongeveer 2 maanden achter op de KIA Veiligheid call. Doel openstelling is dan ook iets later, Q2 2023. Verder zelfde procesgang als KIA Veiligheid.

N.B. deze werkwijze vindt plaats binnen de governancestructuur van beide KIA's.

4.3 Spoor multisectorale TKI-calls

Het TKI-spoor wordt opgebouwd vanuit multisectorale use cases, die Topsectoren en partijen uit die Topsectoren met het kwartiermakersteam BGP hebben uitgewerkt in de voorbereidingsfase. Ook later in het traject kunnen nieuwe use cases worden toegevoegd. Het programmabureau faciliteert dit proces.

In de BGP stuurgroep[48] is een voorkeur uitgesproken voor het mechanisme van de multisectorale calls. Dit mechanisme is al in enkele Topsectoren toegepast en op die ervaring kunnen we voortbouwen. Een voorbeeld is het Synergia project van de Topsectoren Agro & Food, Tuinbouw en Uitgangsmaterialen en HTSM. Ook bij LSH is ervaring op gedaan met deze vorm van samenwerking. Vanuit de KIA Water, Voedsel call zijn meerdere cross-overs calls (geweest);[49] het gaat daarbij voor TKI LSH om de cross-over met TKI T&U en TKI AF.[50] Verder is er ervaring opgedaan met cross-over projecten i.s.m. HTSM voor het IMAGINE project.[51]

Het past ook goed bij de visie binnen de KIA-ST op gezamenlijk programmeren binnen BGP's: "*Het doel van een BGP is te komen tot afstemming tussen KIC-partners over ST-ontwikkeling. Inhoudelijke afstemming moet vervolgens leiden tot synergie in de aanwending van KIC-middelen, zodat de gezamenlijke inzet meer is dan de som der delen*."[52]

"**In plaats van vooraf financieel commitment te vragen voor een BGP stimuleren we als KIA-coördinator inhoudelijke afstemming tussen betrokken KIC-partners, met als doel om in het kader van een BGP gezamenlijk te programmeren.** " (opmaak tekst uit aangehaalde notitie)

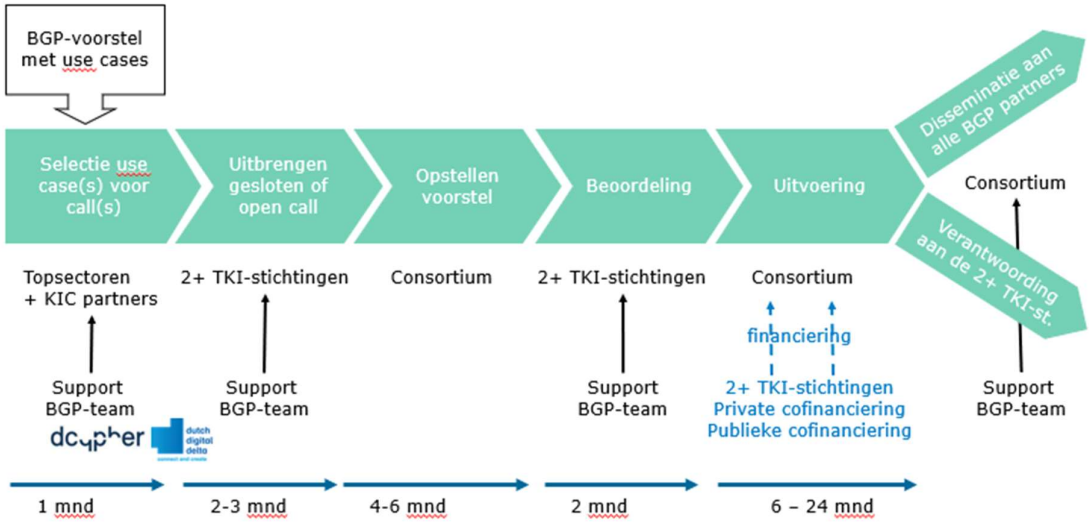
Het BGP Cybersecurity volgt deze lijn en gaat verder dan alleen gezamenlijke speerpunten en inventariseren van lopende projecten/programma's. Het onderwerp cybersecurity is té urgent gezien alle dreigingen en té belangrijk vanwege de toenemende digitalisering voor onze maatschappij, om géén impuls te geven aan kennis en innovatie. Op korte termijn komt die impuls ook niet uit andere hoeken.[53] We zullen pragmatisch door moeten pakken met een agenda en concrete programmering.

[48] 9 juni 2022 en na uitwerking van het proces via een *silent procedure* op 1 juli bekrachtigd.
[49] De PPS calls 2021 en 2022 hiervan zijn beschikbaar als inspiratiemateriaal.
[50] Zie voor een eerder voorbeeld van een cross-over project ook https://www.health-holland.com/project/2022/2021/intestine-chip-integrated-immune-and-microbiota-compartments
[51] Initieel ingediend onder een TKI Agri & Food call (dus tripartite). https://www.health-holland.com/project/2021/2021/innovations-manufacturing-and-marketing-fully-personalised-food-products
[52] KIA ST, "*Notitie BGP commitment en governance*", 15 maart 2022
[53] Zo is er b.v. nog geen investeringsvoorstel in de maak voor het Nationaal Groeifonds.

Het prioriteren en plannen van use cases, de daadwerkelijke programmering, gebeurt in de Stuurgroep, ondersteund door het Programmabureau. Deze laatste stemt per jaar met de TKI-stichtingen en Defensie (en later eventuele andere financiers en behoeftestellers) af welke use cases omgezet kunnen worden in een TKI-call. Hierbij zijn zowel de doelen en KPI's van de betrokken Topsectoren als het BGP bij van belang. Een bijbehorende vraag is welke TKI-stichting het best geëquipeerd is om als trekker op te treden voor de gekozen use case.

4.4 Uitwerking multisectorale calls voor het BGP Cybersecurity

Schematisch ziet de werking het mechanisme van multisectorale cybersecurity TKI-calls er als volgt uit:



Figuur: schematische weergave werkwijze multisectorale TKI-calls (tijdlijn is indicatief[54])

Dit proces zal als volgt verlopen:

- Het programmabureau BGP initieert het programmeringsproces bij de aangesloten TKI-stichtingen en legt de beschikbare use cases voor.
- 2+ Topsectoren (en partijen uit hun achterban en waar opportuun Defensie[55]) onderschrijven dezelfde cybersecurity use case(s) en willen daar op inzetten (uiteraard mits er een goed voorstel komt op de call).
    - N.B.1 Een eerste set use cases maakt onderdeel uit het BGP voorstel. Zie bijlagen van dit voorstel. Later kunnen er nieuwe use cases worden toegevoegd (het is een dynamisch veld!).
    - N.B.2 Bij minder dan 2 Topsectoren is een sectoraal initiatief een beter instrument en valt het uit het BGP (onnodige overhead voorkomen).
- Het programmabureau faciliteert de Topsectoren in de selectie van op te pakken use cases. Welke zijn er? Hoe verhouden die zich tot de thema's en MTIB doelstellingen? Waar liggen kansen voor kruisbestuiving en massa maken?

[54] De werkelijke doorlooptijden zullen (o.a.) sterk afhangen van de besluitvormingsprocedures binnen de diverse te betrekken fora. Het BGP-team kan een aanjagende rol vervullen.
[55] Waar hier verder in deze paragraaf wordt gesproken over TKI-stichtingen als financier en beoordelaar, wordt ook bedoeld het ministerie van Defensie, voor die use cases waarin zij willen participeren en meefinancieren.

- De TKI-stichtingen van de betrokken Topsectoren stellen samen een call-tekst op voor de door hen samen gekozen use case(s). Het programmateam BGP kan hierbij inhoudelijk ondersteunen.
- Vóór het uitbrengen van deze call stemmen de TKI-stichtingen hun procedures op elkaar af. Er zijn namelijk (kleine) verschillen in het besluitvormingsproces, die kunnen leiden tot b.v. een verschillend tempo of andere cofinancieringseisen. Pragmatiek is hier leidend: wat is werkbaar voor de beoogde call met de beoogde partijen?
    - N.B. de procedures blijven intact, het gaat hier om afstemming binnen de bestaande kaders!
    - N.B. 2 afstemming RVO vooraf is noodzakelijk om te zorgen dat de gezamenlijke calls ook zonder problemen administratief kunnen worden verwerkt.
- Onderdeel van de afstemming is het reserveren van TKI-middelen per Topsector.
    - N.B. op moment van schrijven kunnen meerdere Topsectoren in principe middelen beschikbaar maken. Indien er niet voldoende middelen zijn, is een call (op die use case) niet zinvol. Het proces stopt dan helaas.
- De gezamenlijke (“Breed Gedragen”) call kan “gesloten” (er is al een consortium in beeld) of “open” (er is nog geen consortium of er zijn er meerdere) zijn. Deze call wordt opengesteld door een TKI-stichting, mede namens alle betrokken TKI-stichtingen en eventueel andere (publieke) co-financiers.
- Eén of meer consortia stellen een TKI-projectvoorstel op, binnen een te bepalen looptijd, en dienen dat in bij alle TKI-stichtingen. Het voorstel moet voldoen aan de gezamenlijke spelregels van alle TKI-stichtingen (m.a.w. elke stichting moet het goed kunnen keuren). Het voorstel heeft b.v. voldoende private cofinanciering om de gehele gezamenlijke inleg van de Topsectoren te matchen.
    - N.B.1 een consortium kan zelf sectoroverstijgend zijn, of juist bestaan uit partijen binnen het ecosysteem van één Topsector. In het eerste geval is kruisbestuiving al besloten in het consortium. In het tweede is er aanvullende inspanning nodig om resultaten breder beschikbaar te maken voor toepassing in andere Topsectoren. We noemen dat binnen het BGP Cybersecurity ‘horizontale integratie’ en dit is één van de beoogde activiteiten van het programmateam BGP.
- Alle betrokken TKI-stichtingen doorlopen hun besluitvormingsprocedure. Het programmateam BGP monitort de voortgang, opdat er één gezamenlijk en gelijkluidend besluit komt.
    - N.B.1 Er zijn spelregels nodig voor de situatie dat TKI-stichtingen tot verschillende besluiten komen. Uit te werken in de convenantfase van het BGP (Q4 2022).
    - N.B. 2 Idem voor de situatie dat meerdere consortia indienen en hun voorstellen het beschikbare budget overschrijden.
- De TKI-stichtingen kennen elk voor hun deel het consortium subsidie toe. Er zijn bij een aantal Topsectoren ook modellen beschikbaar voor o.a. een passende consortium agreement, AVG verwerkersovereenkomsten.
- Vervolgens voert het consortium het innovatieproject uit. Een innovatieproject kan zich richten op één of meerdere sectorale toepassingen. In het eerste geval zijn er zeker activiteiten voor horizontale integratie (toepassing in andere sectoren) nodig. B.v. door vertegenwoordigers van andere sectoren op te nemen in een klankbordgroep.
- In alle gevallen zullen de resultaten breed worden gedeeld over de KIC partners en hun achterban. Het programmabureau BGP heeft disseminatie als één van de hoofdactiviteiten staan. Deze activiteiten passen ook goed bij de natuurlijk rol van dcypher voor het cybersecurity kennis en innovatie ecosysteem.

- Het consortium heeft dus ook meerdere partijen om verantwoording aan af te leggen. Dat kan echter met één en dezelfde rapportage en/of accountantsverklaring (bij grote bedragen) voor het gehele innovatieproject.

Het programmabureau BGP Cybersecurity initieert en faciliteert het benodigde afstemmingsproces, maar treedt niet in de plaats van de TKI-stichtingen of andere actoren. De bestaande financieringsinstrumenten blijven intact.

4.4.1 Samenloop met participatie Defensie

Defensie prioriteert haar R&D in het Kennisplan Cyber. Defensie heeft specifieke behoeftes, maar op veel onderwerpen is de basis hetzelfde als die voor Topsectoren. Aangezien het ministerie van Defensie het voornemen heeft substantieel te participeren, gaan we ervan uit dat zij deelneemt aan use cases die matchen met dit Kennisplan. In de praktijk zal dit betekenen dat Defensie in eniger mate betrokken wil zijn bij het uitbrengen van subsidievoorstellen, het toetsingsproces van voorstellen, cofinanciering en ook de beschikking krijgt over projectresultaten. De vorm van de Defensie-cofinanciering is in de loop van Q4 2022 nog te bepalen met het Ministerie. Meest waarschijnlijk is de vorm van een subsidie. Aandachtspunt: deze geldt dan ook als te matchen publieke cofinanciering, tenzij er met Defensie een andere financieringsconstructie wordt afgesproken tijdens het programma. Die bewegingsvrijheid is aan te bevelen.

4.5 Use cases voor de multisectorale calls

Bij de voorbereiding van dit voorstel zijn in samenspraak met de meest actieve topsectoren en hun achterban de use cases opgesteld. Deze use cases zijn bedoeld als input voor multisectorale TKI-calls:

Topsector (TS) / Use Cases	Thema	Energie	Logistiek	Holland High Tech	Health Holland	Chemie	Agro & Food	Dutch Digital Delta	Water & Maritiem	Creatieve Industrie	Tuinbouw & Uitgangsmaterialen	Ministerie van Defensie
1. Security assessments in complexe systemen	4, 5	**X**				X		X	X		X	
2. Veilige sensoren voor automatisch inspecteren en detecteren	2	**X**	X			X		X	X	X	X	
3. Cyber threat intelligence Sharing and Threat Modelling	4, 6	**X**						X				X
4. Systemisch inzicht in toenemende complexe IT en OT systemen	4, 6	**X**		X				X			X	X
5. Innovatie op intrusion detection	3, 6	**X**						X				X
6. Digital Twin for Supply Chain Security	6		X	**X**				X			X	
7. Supply Chain Security Tool – inzicht in supply chain	6		X	**X**	X	X		X				X
8. Modeleren & Simuleren van complexe (IT/)OT systemen, digital twin	4, 6	X	X	**X**	X			X			X	X

9. Veilige apparatuur en applicaties in thuisomgeving	1, 3, 4, 5	X			**X**		X	X	X			
10. Veilig datagedreven werken	2, 1, 7	X			**X**			X			X	
11. Systeem/Ketenveiligheid	6			X	**X**			X			X	
12. Cyberweerbaarheid in de logistieke sector	7		**X**				X	X	X			

Legenda Thema's BGP	1. Security by design 2. Veilig datagedreven werken 3. Veilige en robuuste connectiviteit 4. Veilige OT/IoT en integratie met IT 5. Cyberrisicomanagement 6. Systeem- of ketenveiligheid 7. Cybersecurity awareness, kennis en vaardigheden

Tabel: overzicht van use cases en aangegeven toepasbaarheid per Topsector en voor Defensie.[56]

De in de bijlagen opgenomen use cases zijn alle bewust nog "concept". Pas bij het opstellen van daadwerkelijke calls is het nodig om de cases definitief te maken. Dat biedt het BGP ook de ruimte om onderzoeksvragen te dimensioneren t.o.v. het dan beschikbare budget en de relatieve prioriteit op dat moment van elk van de use cases.

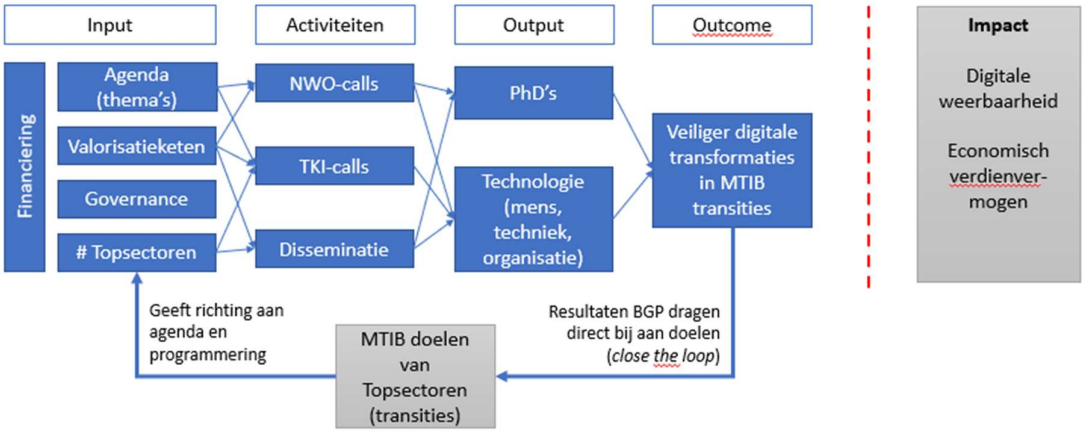
4.6 Governance: sturen op resultaat

Het strategische doel van BGP is dat cybersecurity als sleuteltechnologie de digitaal veilige transformatie mogelijk maakt die nodig is voor grote maatschappelijke transities (*outcome*). Dit heeft impact op digitale weerbaarheid van onze samenleving en economisch verdienvermogen.[57]

Het BGP levert als output (projectresultaten) voor dat kerndoel vraaggestuurde kennis- en innovatie op 7 thema's, toegepast op maatschappelijke transities. Om dat mogelijk te maken organiseert het BGP Cybersecurity in eerste instantie NWO en TKI calls, bedoeld om de hele cybersecurity valorisatieketen te mobiliseren. Daarnaast zullen meer mogelijkheden ontgonnen worden.

In hoofdstuk 1 werd de implementatie van de Theory of Change voor het BGP Cybersecurity al op hoofdlijnen beschreven. In deze paragraaf werken we dat uit naar KPI's. Het is expliciet de bedoeling om dit in de volgende fase in overleg met de Stuurgroep verder vorm te geven. Het betreft hier een eerste schootsrichting.

[56] In sommige gevallen loopt de afstemming nog bij schrijven, i.v.m. de vakantieperiode. Dat geldt b.v. voor Defensie voor een deel van de use case.
[57] Impact valt buiten de directe invloed en accountability van het BGP Cybersecurity zelf, maar is wel de leidraad.



Omgezet naar een (eerste worp voor) KPI's ter monitoring en aansturing van het BGP Cybersecurity:

Input	Activiteiten	Outputs	Outcomes	Impact
Financiële omvang BGP # deelnemende Topsectoren Mate van betrok-kenheid hele valorisatieketen Agenda Governance Doelen uit MTIB (TS)	# NWO en TKI calls (en projecten) Mate van dekking thema's in programma uit agenda (# thema's)? # disseminatie activiteiten	# PhD's # Technologische resultaten (mens, techniek en organisatie)	# adoptie van resultaten in maatschappelijke transities Of Veiliger digitale transformaties in MTIB	Relatieve afname van # cyber-incidenten Toename BBP (buiten accountability van BGP)

Het BGP Cybersecurity beweegt zich op een matrix van 7 cyberthema's en een veelvoud aan MTIB doelen. Primair is het BGP vraaggestuurd, dus zijn de MTIB doelen leidend. Voor cybersecurity als sleuteltechnologie zijn daarnaast eigen milestones op de cyberthema's ook noodzakelijk. De verwachte omvang van het programma zal echter niet voldoende zijn om voor alle 7 thema's een sluitend geheel aan milestones te programmeren. Daarom is substantiële doorontwikkeling van het BGP, b.v. naar een Groeifondsvoorstel, zeer wenselijk.

4.7 Bewerkstelligen van synergie: horizontale integratie, disseminatie, communicatie

Bij uitvoering zullen betrokken partijen (uitvoerders, gebruikers) een balans moeten vinden tussen inbedding van cybersecurity in de digitalisering en bovenliggende maatschappelijke transities van het MMIP enerzijds (verticale integratie) en breed gebruik van de onderzoeksresultaten anderzijds (horizontale integratie).

Verticale integratie gebeurt bij sterke voorkeur binnen de uitvoering van het kennis-/ innovatieproject o.b.v. de thema's en use cases. Dit geldt zeker voor het TKI-spoor, maar is ook relevant voor het NWO-spoor. Het projectvoorstellen beschrijven daarom straks hoe de cybersecurity activiteiten inpassen in de grotere context van digitalisering en MMIP. Dit is zinvol voor een goede bruikbaarheid in de betreffende Topsector en voorkomt dat er binnen de MMIP weer een nieuw initiatief opstart. Maximale synergie is hier het doel.

Horizontale integratie bevordert dat trajecten niet blijven steken in één toepassingsgebied, maar breder toepasbaar zijn (het is een breed gedragen programma!). Het plan en uitvoering zullen dus rekening moeten houden met de relevantie voor andere betrokken Topsectoren en i.s.m. het programmabureau BGG Cybersecurity voor disseminatie en horizontale integratie moeten zorgen. Horizontale integratie zal o.a. via de volgende wegen worden bereikt:

- Meerdere toepassingsgebieden uitwerken per project;
- Deelname van vertegenwoordigers van andere sectoren dan alleen het toepassingsgebied, b.v. via klankbordgroepen of uitvoering;
- Gerichte én brede verspreiding van onderzoeks(tussen-)resultaten (disseminatie).

Disseminatie

Gerichte én brede verspreiding van onderzoeks-(tussen-)resultaten is randvoorwaardelijk voor het succes van het BGP Cybersecurity. De eerste verantwoordelijkheid hiervoor ligt bij de uitvoerende onderzoeksteams, het programmabureau BGP zal hier een faciliterende rol in vervullen met mensen en middelen (zie ook H6). Kanalen zijn o.a. wetenschappelijke publicaties, publicatie van (tussen-)resultaten via de website van het BGP Cybersecurity (via dcypher en Topsector ICT), presentaties aan een brede groep belanghebbenden en andere events. Zie ook het communicatieplan in H6.

5 Looptijd, indicatieve begroting en dekking

5.1 Looptijd 2023-2027

De beoogde **looptijd** van het BGP Cybersecurity is 2023 – 2027. Hiermee volgt het BGP de looptijd van het huidige Kennis en Innovatie Convenant (KIC) en het hierop volgende KIC. De stuurgroep BGP kan besluiten het programma langer door te laten lopen na 2027.

5.2 Begroting en dekking

<NB alle genoemde bedragen zijn indicatief op dit moment, want afhankelijk van besluitvorming elders (b.v. KIA ST, Defensie)>

De indicatieve **begroting** van het BGP Cybersecurity kent in de uitvoeringsfase drie bestemmingen:

1. voor de KIC / Missie calls (uit NWO-gelden voor de KIA's ST en Veiligheid);
2. voor de multisectorale TKI-calls (uit PPS Toeslag of andere Topsectorenmiddelen, private en publieke cofinanciering);
3. voor de noodzakelijke programmakosten.

Begrotingsstromen	Bedrag 2023-2027 (mio Euro)
Programmering Missie calls NWO	13,7-21,5m (incl. cofinanciering)
Programmering TKI calls	12,5-21,5 (incl. cofinanciering)
Programmakosten	1-1,25
Totaal	**27-44,3**

De omvang van de twee programmeerstromen groeit mee met de beschikbare middelen. De omvang van de Missie calls is b.v. afhankelijk van de middelen die de KIA ST ter beschikking stelt. De multisectorale TKI calls kunnen qua omvang groeien als Topsectoren meer middelen reserveren (b.v. in de volgende KIC periode, of er middelen vanuit ROM's beschikbaar komen).

Voor de **dekking** is het goed om op te merken dat binnen het KIC de KIC partners opereren met eigen budget en eigen verantwoordelijkheid. Daarmee kan een BGP worden gezien als een gezamenlijke en gedragen KIA op een specifiek ST onderwerp. De KIC partners bepalen zelf waarop en hoeveel ze inleggen. Ook maken we gebruik van bestaande instrumenten. De in dit BGP additioneel georganiseerde dekking voor de BGP programmering komt uit de volgende bronnen:

Bron	Totaalbedrag in mio euro (2023-2027)	Waarvan reeds gecommitteerd	Waarvan te mobiliseren
Private middelen	9,4-14,2	0	9,4-14,2
PPS toeslag, andere Topsectorenmiddelen	3,25	0	3,25
TNO	n.t.b.	0	n.t.b.
NWO	5,5 - 16,5	5,5	5-11
Universiteiten/hogescholen	-	-	-
Regionale middelen (provincie, gemeenten)	-	-	-
Departementale middelen	4-7,25	0	7,25
EU middelen	-	-	-
ROMs	3	0	3
Anders, namelijk…	-	-	-
TOTAAL	**27-44,3**	**5,5**	**21,5-38,8**

* in principe houdt private cofinanciering gelijke tred met de NWO-financiering (30%), PPS toeslag (ca. 50%) en mogelijk ook de publieke cofinanciering

Topsector HTSM programmeert reeds cybersecurity innovatie (1,6M/jr excl. private cofinanciering). Dit is niet meegenomen in bovenstaand dekkingsstaatje. De Topsectoren Energie, Life Sciences & Health en Logistiek hebben indicaties voor commitment afgegeven van totaal 3,25 M Euro (excl. private cofinanciering van gelijke ordegrootte). Deze en andere Topsectoren kunnen pas concreet commitment afgeven bij het daadwerkelijk programmeren van de multisectorale calls! Dit is onlosmakelijk verbonden aan de in te zetten instrumenten.

Voor **TNO**-middelen (totaal 6 mio Euro, reeds geprogrammeerd op cybersecurity onderwerpen) zal ruimte worden gezocht om de programmering beter te richten op geprioriteerde BGP thema's. Ook dit is nog niet opgenomen in het dekkingsstaatje Het **ministerie van Defensie** heeft een reservering van een meerjarige, oplopende reeks gemaakt die zowel nog geformaliseerd moet worden in de Defensie begroting. Daarnaast dienen ook de use cases voldoende overlap te hebben met de Defensie onderzoeks- en ontwikkelbehoefte. Afstemming hierover loopt nog bij schrijven.

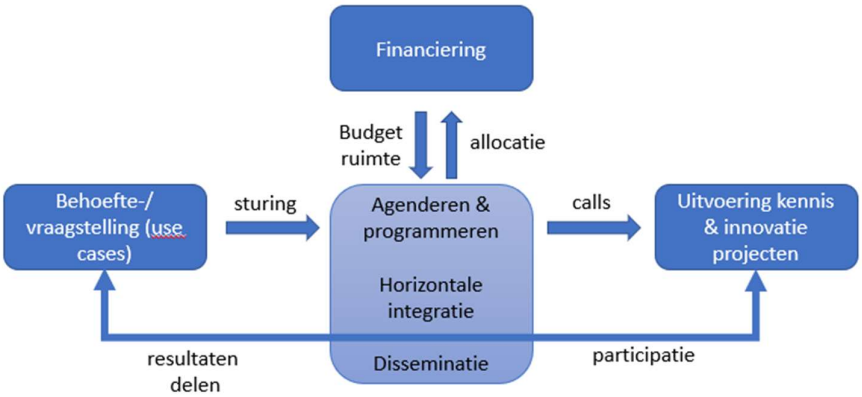
Deze middelen in principe geheel ingezet voor dekking van de kennis- en innovatieprogrammering. Voor de programmakosten onderzoeken we de mogelijkheid een beroep te doen op generieke Topsectoren middelen bij EZK. Indien dat niet mogelijk blijkt te zijn, zal een deel van het programmeringsbudget worden gereserveerd voor programmakosten.

6 Samenwerking en organisatie

6.1 Samenwerking met stakeholders van het BGP Cybersecurity

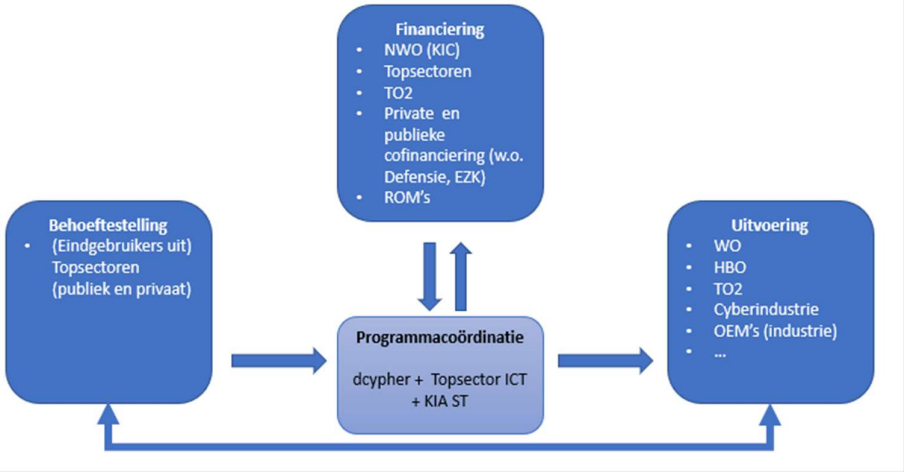
Aan de totstandkoming van de agenda en programmalijnen heeft een brede groep aan stakeholders deelgenomen. Belangrijk is deze groep belanghebbenden betrokken te houden gedurende de fase van uitrol van calls en andere instrumenten. Dit is van belang voor de uitvoering van de beoogde kennis- en innovatieprojecten, financiering en toekomstig gebruik van resultaten.

De stakeholders binnen het BGP Cybersecurity kunnen worden onderverdeeld in vraagstellers (vaak eindgebruikers, of intermediaire organisaties), uitvoerders van kennis en innovatie en financiers. Samen werken zij aan agendering en programmering in het BGP, gefaciliteerd door een programmabureau. Dat programmabureau faciliteert ook de horizontale integratie (tussen en disseminatie van resultaten en community management.



Figuur: samenwerking binnen het BGP Cybersecurity

Buiten de direct bij het BGP betrokken partijen zijn ook andere belanghebbenden te onderkennen. Dat zijn o.a. potentiële toetreders in alle categorieën (het BGP is open), niet direct aangesloten beleidsdepartementen en de media.



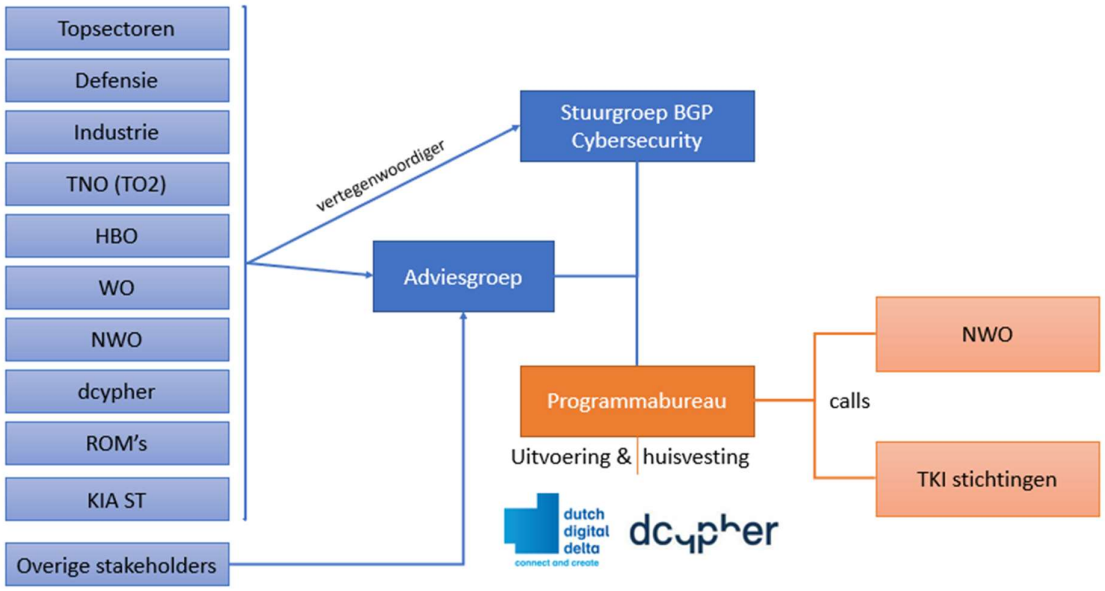
Figuur: rolverdeling van partijen binnen de uitvoering van het BGP Cybersecurity

Op het niveau van individuele projecten binnen de NWO- en TKI-calls stellen vraagstellers, uitvoerders en financiers vast: welke partijen deelnemen aan het consortium, welke omvang en duur het project kan hebben en de inhoud ervan. Het BGP Cybersecurity faciliteert dit proces, maar er is a priori geen *grand design* tussen de partijen om alle voorstellen in onderlinge samenhang te vormen. Indien er meerdere TKI use cases en delen van NWO-calls of andere middelen in gang worden gezet op hetzelfde thema, kan dcypher diens Roadmap methodologie inzetten om de samenhang en doorontwikkeling te bewerkstelligen. Zoals in H4.6 opgemerkt, zijn meer middelen nodig dan nu in kaart gebracht, om een sluitende set aan milestones te realiseren op alle thema's voor alle Topsectoren. Doorontwikkeling naar b.v. een Groeifondsprogramma is wenselijk.

Verder merken we op dat rollen ook niet zwart-wit zijn, het gaat primair om de beweging en het effect. Zo kan b.v. een ROM adviseren over een interessante use case, of een uitvoeringspartner de brug zijn naar deelname aan een Europese financieringsinstrument. Enzovoort. Het beoogd effect (outcome) en impact staan voorop.

6.2 Programma-organisatie

Het BGP Cybersecurity organiseert een ecosysteem rond een inhoudelijke agenda en twee programmeringsstromen. Om dit te kunnen doen (en de relatie met de buitenwereld te blijven leggen), wordt een bescheiden organisatie ingericht. De overhead wordt zo laag mogelijk gehouden. Tegelijkertijd: zonder inspanning geen synergie. Er is daarom een slagvaardige stuurgroep, een brede adviesgroep en een klein, faciliterend programmabureau voorzien.



Figuur: organisatie van het BGP Cybersecurity

6.2.1 Stuurgroep als strategieteam

De Stuurgroep geeft al sinds november 2021 in samenwerking met de TKI-directeuren sturing aan de ontwikkeling van het BGP en heeft draagvlak verkregen vanuit de Topsectoren en de andere actoren. De hele valorisatieketen is in de Stuurgroep vertegenwoordigd. Voor de uitvoeringsfase willen we de stuurgroep doorontwikkelen, om doeltreffend en doelmatig strategie, proces en draagvlak te besturen en bewaken. De exacte vormgeving zal met de Stuurgroep nog worden besproken en daar besloten (Q4 2022).

De beoogde stap is dat de Stuurgroep zich omvormt tot een strategieteam van beperkte omvang, om zodoende het nieuw te vormen Programmabureau strategisch aan te kunnen sturen en de uitvoering en doorontwikkeling van het BGP Cybersecurity op hoofdlijnen te kunnen monitoren. Het strategieteam bestaat idealiter uit representatieve bestuurlijke vertegenwoordigers uit de hele valorisatieketen (vraagstellers, uitvoerders en financiers), uit onderzoek en onderwijs, overheid, bedrijfsleven (groot, klein, startup, 'in cyber' en 'met cyber'), (cybersecurity)-eindgebruikers en maatschappij, de KIA ST en Topsectoren. Deze vertegenwoordigers worden gekozen op hun functie of rol en hebben de juiste positie en voldoende mandaat in hun organisaties of netwerk om strategisch sturing te geven aan de uitvoering en doorontwikkeling van het BGP.

Verantwoordelijkheden stuurgroep:

> Ziet erop toe dat de inhoudelijke agenda wordt gevolgd en programmering plaats vindt.
> Stuurt de programmamanager functioneel aan en beslist over escalatiepunten.
> Evalueert jaarlijks de voortgang en besluit over eventuele bijstelling.
> Bevordert draagvlak voor uitvoering en doorontwikkeling van het BGP Cybersecurity en schakelt daarvoor (politiek)bestuurlijk met de hiervoor relevante partijen in Nederland.

6.2.2 Adviesgroep voor kennis en draagvlak

Bij het opstellen van het BGP Cybersecurity heeft zich een ruime groep met bestuurders en experts gevormd. Wanneer de Stuurgroep zich door ontwikkelt tot een strategieteam van kleinere omvang, zou het een verlies zijn als de kennis en relaties van deze groep uit beeld raken. Het is voor deze belanghebbenden ook van belang op de hoogte te blijven van de voortgang, relaties te kunnen leggen met eigen activiteiten en invloed uit te oefenen op de uitrol van het programma. We stellen daarom een brede Adviesgroep voor die halfjaarlijks of vaker als nodig bijeen komt en wordt uitgenodigd voor BGP cybersecurity events.

De rol van de Adviesgroep is - zoals de naam al zegt - advies geven aan de programmamanager en de Stuurgroep. Dat advies kan gaan over inhoudelijke zaken (interessante nieuwe use cases b.v., later in het traject evaluatie van de agenda) of procesmatig (hoe laten we de call-instrumenten goed werken?!). Ook is het de plek waar praktijkervaringen kunnen bespreken om het uitvoeringsproces te verbeteren. Een andere belangrijke taak van de adviesgroep is 'inventariseren en agenderen': signaleren wat er speelt in het veld en waar daarom nodig is aan nieuwe kennis en innovatie

6.2.3 Faciliterend Programmabureau

Het BGP-programmateam heeft onder leiding van de kwartiermaker tot dusverre vorm en inhoud gegeven aan besluiten en acties vanuit de stuurgroep. Hierin trekken medewerkers van dcypher en Topsector ICT samen op en overleggen wekelijks om acties uit te zetten en op te volgen. Het team blijft als Programmabureau ook vanaf 2023 idealiter de inhoudelijke en organisatorische motor van het BGP Cybersecurity. Een aan te stellen programmamanager BGP Cybersecurity stuurt een klein programmabureau aan, waaronder een secretaris. Het voorstel is deze rol bij dcypher onder te brengen, dat is immers het publiek-private samenwerkingsplatform voor cybersecurity kennis en innovatie. Daar ligt ook synergie met andere community building activiteiten in het cyberdomein. De programmamanager BGP kan gebruik maken van de capaciteit, organisatie en activiteiten van dcypher zodat de overhead minimaal kan blijven.

De programmamanager is het gezicht van het BGP Cybersecurity en is verantwoordelijk voor:

- Coördinatie, inhoudelijke en procesmatige ondersteuning voor het programmeringsdeel van het BGP Cybersecurity, i.s.m. de trekkers/voorzitters van de op te zetten kennis- en

innovatie calls via NWO en TKI-stichtingen. De Programmamanager bewaakt hierbij de BGP-agenda en verstrekt inhoudelijke voeding aan de opstellers van calls. NWO en TKI-stichtingen voeren hun reguliere proces uit. De programmamanager ondersteunt de stroomlijning van verschillende TKI-processen om te komen tot succesvolle multisectorale calls, zonder in de verantwoordelijkheid van de TKI-stichtingen te treden.

- Ondersteuning van de Stuurgroep, w.o. secretarisschap van de Stuurgroep. Doet een onderbouwd voorstel voor prioritering van use cases voor TKI-calls. Monitort inhoudelijke en financiële voortgang, signaleert knelpunten en groeikansen, escaleert strategische punten tijdig naar de Stuurgroep. Minimaal een jaarlijkse rapportage en evaluatie in de Stuurgroep.
- Ondersteuning en inschakeling van de Adviesgroep voor inhoudelijke of procesmatige consultatie op reguliere basis en vaker indien nodig.
- Aansturen van de doorontwikkeling van het BGP, met nieuwe partners, nieuwe financieringsstromen, nieuwe use cases en nieuwe uitvoerders. Nationaal en internationaal waar zinvol. Dit i.s.m. de Stuurgroep en Adviesgroep (zie verder H8).
- Bevorderen samenwerking tussen partijen en horizontale integratie. Houdt de relatie van het BGP met andere cybersecurity kennis- en innovatieprogramma's (incl. HCA ICT) in de gaten en zoekt indien zinvol de samenwerking op. Ook wordt hier de verbinding gelegd met andere stakeholders die zich op een ander TRL niveau bevinden, zoals diverse initiatieven in cyber weerbaarheid en awareness. Ook binnen andere sectoren is al ervaring opgedaan, ook soms buiten de Topsectoren, met diverse use cases binnen de 7 thema's welke nuttig zijn om binnen onderzoeksgroepen te presenteren.
- Aansturing van communicatie en bevorderen van disseminatie van resultaten, om valorisatie van de kennis en innovatie te versterken. Maakt waar mogelijk gebruik van de bestaande kanalen van dcypher, Topsector ICT en KIA ST.
- Inregeling en operationele aansturing van het programmateam.

Het Programmabureau neemt zelf geen deel aan projecten van kennis- en innovatieconsortia. De consortia en het Programmabureau werken wel samen om horizontale integratie (hergebruik in andere sectoren) en disseminatie van projectresultaten te bereiken. Consortia zullen dus informatie over voortgang en resultaten moeten verschaffen aan het Programmabureau. Het bureau verschaft op diens beurt disseminatiekanalen en kan bemiddelen in samenwerking met andere partijen (netwerkrol). Ook kan het bureau eventuele doublures of overlap met lopende (of voorgenomen) kennis- en innovatietrajecten signaleren en partijen verbinden. Dit sluit goed aan op de rol die dcypher al heeft.

6.3 Communicatie

Het Programmabureau ondersteunt de deelnemende partijen met interne (binnen het BGP) en externe communicatie-activiteiten. Hiertoe zal een strategisch communicatieplan worden gemaakt. Het BGP maakt zoveel mogelijk gebruik van de reeds voor handen zijnde kanalen en middelen van dcypher en de Topsector ICT.

6.3.1 Doelen en doelgroepen (binnen en buiten het BGP)

Informeren over de kennis en innovatie waaraan sectoroverstijgend wordt gewerkt binnen het BGP Cybersecurity en het activeren van partijen die daar een waardevolle bijdrage aan kunnen leveren. Met als doel om samenwerking te stimuleren tussen de belangrijkste actoren in de kennis- en innovatieketen van cybersecurity, uitmondend in actieve participatie in een van de projecten in het BGP.

Doelgroepen: Topsectoren en hun achterban (w.o. hun experts, bedrijven enz.) en de andere genoemde cybersecurity innovatie initiatieven en agenda's, onderzoeks- en onderwijsinstellingen, ROM's, cybersecurity industrie, industrie die als gebruiker of assembleur van cybersecurity interesse heeft, betrokken departementen, maatschappelijke organisaties, media en potentiële nieuwe deelnemers.

6.3.2 Middelen en activiteiten op hoofdlijnen

Het is van belang eenduidige boodschappen te gebruiken als kapstok voor alle verdere mediacommunicatie. Deze kernboodschappen zijn:

Het BGP Cybersecurity versterkt de soevereine cyberveiligheid met kennis en innovatie, waarmee ook toepassing en het verdienvermogen van Nederland toeneemt.

Het BGP Cybersecurity pakt de cyberveiligheidsvraagstukken op die voortkomen uit grote maatschappelijke transities en organiseert hiertoe efficiënte ketens van publiek-private samenwerking.

Het BGP Cybersecurity constateert dat het urgent en belangrijk is gericht te investeren in Nederlandse cybersecuritykennis en -innovatie en dat in nauwe samenwerking te doen, gezien de schaarse middelen en mensen.

7 Risico's, mitigatie en randvoorwaarden

7.1 Risico's en mitigatie

Tijdens het afronden van het BGP-voorstel (Q4 2022) en uitvoering (2023-2027) kunnen zich risico's manifesteren. Het programmabureau voert het risicomanagement uit namens de stuurgroep.

Risico	Mitigatie
Private deelnemers dragen onvoldoende bij aan cofinanciering van NWO of TKI calls (NB dit wordt een groter risico indien Defensiemiddelen als publieke financiering worden ingezet en dus ook moeten worden gematcht)	Incentive ligt bij indienende consortia, die de slagkracht en reikwijdte van het BGP vergroten. Awareness bij eindgebruikers vergroten en koepelorganisaties inschakelen om die gebruikers meer te betrekken. Inperken van omvang van calls als last resort.
Defensie prioriteert anders in Najaarsnota, bijdrage BGP omlaag. B.v. omdat er onvoldoende overlap is in de use cases en behoeftes Defensie.	Voortzetten van afstemming met het Cyber Warfare & Training Center van Defensie. Zo nodig inperken van omvang van TKI-calls
BGP brengt als geheel een te kleine impuls aan kennis en innovatie	Aanwas extra middelen en activiteiten in BGP (sneeuwbal, zie H8) Doorontwikkelen naar Groeifonds (zie H8)
Doorlooptijd voor afstemming van calls lang, zodat partijen afhaken.	Programmabureau faciliteert proactief besluitvorming. Plant meetings, denkt mee over inhoud en proces. Communicatieactiviteiten vanuit BGP om aandacht te houden (zie H6)
Formele besluitvorming rond KIC-middelen van NWO nog niet rond (op inhoud en omvang). Kan tot wijziging van scope en/of omvang leiden.	Bespreking in Kernteams ST en Veiligheid. Zo nodig inperken van calls.
Geen capaciteit beschikbaar voor uitvoering kennis- en innovatieprojecten	Publiciteit rond BGP en afzonderlijke calls. Gebruik van bestaande en bekende kanalen NWO en TKI-calls. Inhoudelijke en commerciële waarde van beoogde projecten verhogen door breder toepassingsgebied (multisectoraal).

7.2 Randvoorwaarden

Voor het slagen van het BGP zien we een aantal randvoorwaarden c.q. kritieke succesfactoren.

Uitvoering: Voldoende, gekwalificeerde mensen om projecten voor te stellen en uit te voeren bij de verschillende uitvoerende organisaties (WO, HBO, TO2, bedrijfsleven, eindgebruikers).

Financiering: bereidheid van publieke en private financiers om binnen de bestaande instrumenten voldoende mee te investeren. Het Programmabureau stimuleert inzet van deze middelen en strijkt de plooien glad waar nodig. Zie H5. Voor eindgebruikers geldt dat zij voldoende urgentie en belang moeten onderkennen om in kind of in cash te participeren.

Programmabureau: beschikbaarheid van financiële middelen voor instandhouding van het programmabureau (250k/jr) gedurende het programma. Toegang tot bestaande communicatiekanalen Topsector ICT en dcypher. Ondersteuning van dcypher en Topsector ICT staf.

8 Doorontwikkeling: structurele beweging op gang brengen

8.1 BGP als sneeuwbal

Van meet af aan is het BGP Cybersecurity bedoeld als 'sneeuwbal', als groeiprogramma. We leggen met dit ecosysteem, agenda en programmering een fundament, dat langs verschillende assen moet gaan doorgroeien. Dat kan langs meerdere assen:

- Nieuwe multisectorale use cases binnen de 7 cyberthema's, om meer kennisgaten te dichten.
- Uitbreiding van financiering (b.v. TKI-middelen t.b.v. nieuwe use cases, of additionele publieke of private partijen (incl. ROM's) die bij willen dragen). Dit kan expliciet ook aan de orde zijn bij de nieuwe KIC-periode en allocatie van middelen voor die periode.
- Uitbreiding van het ecosysteem met nieuwe partijen voor b.v. die financiering of uitvoering of gebruik. Het BGP Cybersecurity is een open ecosysteem, nieuwe toetreders zijn welkom.
- Verlenging van de looptijd na 2027.

De uitbreiding kan ook internationaal zijn, richting EU b.v. voor financiering of desgewenst met internationale partners voor uitvoering.

Buiten het programma zelf kan het BGP zich ook door (laten) ontwikkelen. Het ligt voor de hand om te participeren (of zelfs te initiëren) wanneer er een nieuw Nationaal Groeifondsvoorstel komt. Het BGP brengt een goed ecosysteem en een vraaggestuurde agenda mee. De doorontwikkeling naar een eventueel Groeifondsvoorstel vanuit het BGP zal ook van invloed zijn op de inrichting van governance en uitvoering. Hoe verhouden BGP-organisatie en NGF-organisatie zich dan tot elkaar?

Een andere mogelijkheid is dat technologische ontwikkelingen binnen het BGP een dermate omvang krijgen, dat het instrument van de dcypher routekaart kan worden ingezet om valorisatie te bevorderen. De Stuurgroep besluit over majeure groeistappen van het BGP.

8.2 Korte termijn: afronding BGP voorstel en opstart programma

Voordat we over doorontwikkelen kunnen praten, zal eerst het BGP voorstel afgerond en goedgekeurd moeten worden. Bij positieve besluitvorming in stuurgroep BGP, Kernteam ST en Thematеam ST, zal in Q4 2022 de voorstelfase worden afgerond met de volgende acties:

- Begeleiden convenantproces voor het BGP, tussen alle aangesloten KIC partners.
- Met NWO voorbereiden van de NWO-calls op cyberveiligheid/-security 2023.
- Fine-tuning van de use cases waar nodig en (nogmaals) toetsen op welke use cases de verschillende topsectoren in willen zetten.
- Voorbereiden multisectorale calls met de TKI-stichtingen, m.n. programmeren van eerste calls (welke use cases eerst!?) en synchroniseren van besluitvormings- en verantwoordingsprocessen.
- Inrichting governance voor uitvoeringsfase.
- Inrichten, dekking en opstarten programmabureau BGP.
- Afronden en opstart uitvoering communicatieplan BGP.

Het bouwen en onderhouden van het ecosysteem is daarnaast een continu proces.

Bijlage 1: overzicht huidige deelnemende KIC partners

Topsectoren	Contactpersoon	Contact cyberexpertise
Agri & Food	Kees de Gooijer, Directeur TKI Agri & Food	-
Chemie	Oscar van den Brink, Directeur TKI Chemie	Johan van Middelaar (Safety Delta NL)
Creatieve industrie	Bart Ahsmann, Directeur TKI Creatieve Industrie	Frank Visser
Energie	Harold Veldkamp, Directeur Digitalisering voor TKI Energie	Claire Groosman
HTSM	Leo Warmerdam, Directeur TKI HTSM	Johan de Heer, Dimitri Hehanussa, Jasper de Graaf
ICT	Frits Grotenhuis, Directeur Topsector ICT	Team ddd, ACCSS, TNO, René Montenarie
Life Sciences & Health	Nico van Meeteren, Directeur TKI LS&H	Martina Bartelink, Christiaan Piek
Logistiek	Liesbeth Brügemann, programmamanager TKI Dinalog	Liesbeth Brügemann
T&U	Jose Vogelezang, Directeur TKI T&U	Colinda de Beer
Water en Maritiem	Herry Nijhuis / Jantienne van der Meij-Kranendonk, Directeur TKI Watertechnologie	Chris Karman (DigiShape)
Wetenschap		
ICT	Inald Lagendijk, Wetenschappelijk Boegbeeld ICT	Id.
ACCSS	Aiko Pras, vice-voorzitter bestuur	Jan Piet Barthel
Kennisinstelling / TO2		
TNO	Berry Vetjens, Marktdirecteur Unit ICT	Id.
Overig		
NWO	Christiane Klöditz, Hoofd Wiskunde en Informatica bij het domein Exacte en Natuurwetenschappen en Topsector ICT - team ddd, KIA Veiligheid.	Mario van der Linden, Ruben Sharpe
Awareness en cyberweerbaarheid	Marjolijn Bonthuis, Programmadirecteur Cyber cluster ECP	div.
dcypher	Eddy Boot, directeur dcypher	Tom van Schie, Rick van der Kleij, Patrick de Graaf, Lisa Soldaat, Roos-Marie van Gerven
Cyberveilig Nederland	Liesbeth Holterman, strategisch adviseur	Id.
Lectorenplatform PRIO	Ben Kokkeler, AVANS	Id.
Innovation Quarter, namens ROM's	Philip Meijer, senior Account Manager Cybersecurity	Id.
Ministerie van Defensie	Auke Venema, strategisch adviseur Kennis & Innovatie	Cyber Warfare & Training Center

Bijlage 2: overige geconsulteerde personen

Naast de in bijlage 1 genoemde organisaties, is met een groot aantal instanties gesproken in interviews en workshops over het BGP. Mede dankzij hun input staat er nu een programmavoorstel.

- Cisco
- Elaad.NL
- Energy Coöperatie Betuwe
- Erasmus School of Health Policy and management
- FERM
- FME
- HAN
- Health Holland
- Health-RI
- HSD
- Invest NL
- INTERSECT
- kenniscentrum veilige digitale samenleving
- MIND Platform
- Ministerie van EZK
- Ministerie van IenW
- Ministerie van J&V
- Ministerie van VWS
- Neuro Control
- NL Digital
- Radboud Universiteit
- Rotterdam School of Management, Erasmus Universiteit Rotterdam
- Safety Delta NL
- Security Delta (HSD)
- Thales
- TU Delft
- TU Eindhoven
- Volker
- Vrije Universiteit
- Windfarm Services
- Wageningen University & Research
- ZonMw

Bijlage 3: samenhang cybersecurity thema's BGP met KIA's ST en Veiligheid en NCSRA III

BGP thema's (expertgroep)	MJP 55 Cybersecurity – Digitale Veiligheid en Privacy (KIA ST)	KIA Veiligheid-Cyberveiligheid	Nationale Cyber Security Research Agenda III (2018)
Security by Design	Ontwerpen en ontwikkelen van veilige systemen en software	defensieve cybertechnologie: security by design	Design (alles)
Veilig datagedreven werken (incl. authenticatie bronnen, veilig data delen, integriteit)	Behalve Encryption technologies/digital scrutiny, zijdelings geadresseerd in MJP 55.	defensieve cybertechnologie: cryptografie en automated security	Design en Defence (vrijwel alles in deze categorieën) Attacks (crypto)
Robuuste, veilige infrastructuur	Zijdelings geadresseerd in MJP 55. Buiten MJP Cyber: Quantum communication	defensieve cybertechnologie: cryptografie	Design (e.g. crypto)
OT security + IT/OT integratie	Onveilige Internet of Things (IoT) systemen. Buiten MJP Cyber in KIA ST: cyberphysical systems	Defensieve cybertechnologie: automatische detectie binnen industriële omgevingen zoals bijvoorbeeld in industriële ICS-SCADA systemen	Design en Defence (voor zover toepasbaar op OT/IoT)
Systeem- en ketenveiligheid	Via verwijzing naar NCSRA III	Ketenweerbaarheid en governance	Governance
Cyberrisicomanagement	Via verwijzing naar NCSRA III	Ketenweerbaarheid en governance: risicomgt, business case Defensieve cybertechnologie: Het automatiseren van detecteren of organisaties compliant zijn aan wetgeving, (eigen gestelde) standaarden.	Defence (b.v. dynamic risk management, cost/benefit analysis). Governance
Awareness (breed) + Human Capital Agenda	Via verwijzing naar NCSRA III	Bevorderen ontwikkeling cybercompetenties	Defence (awareness)
		Offensieve cybertechnologie	Attack (technologie voor offensieve toepassingen)
	Encryption technologies/digital scrutiny		Privacy
	Kwetsbaarheden automatisch te detecteren en repareren	Automated Vulnerability Research	Attacks: Automated Vulnerability Research.
		Bestrijden cybercrime	

Bijlage 4: use cases voor multisectorale TKI-calls

De onderstaande use cases zijn opgesteld i.o.m. experts vanuit de (achterban van) de deelnemende Topsectoren. De use cases zijn bedoeld om richting te geven aan de multisectorale TKI-calls in het kader van het BGP Cybersecurity. Verdere uitwerking van de use cases is nog mogelijk tot aan het opstellen van die calls door de TKI-stichtingen. In de fase van beantwoording van deze calls worden publiek-private consortia gevormd voor de uitvoering van projecten.

Case 1: Security assessments in complexe systemen

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ✓ **Topsector Energie** ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ✓ **Topsector Tuinbouw & Uitgangsmaterialen** ✓ **Topsector Water & Maritiem** ✓ **Topsector Chemie** Andere partners en bedrijven: Safety Delta Nederland (SDN) e.a.
Thema BGP	○ Veilige OT en OT/IT integratie ○ Cyberrisicomanagement
Relatie met MTIB	Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.
Doel en nut van de beoogde pre-competitieve innovatie	Er komt steeds meer (Europese) regelgeving die eisen stelt aan cybersecurity van (kritieke) infrastructuren (bijv. NIST2.0). Ook stellen bedrijven zelf meer security eisen. Om deze groeiende compliance-behoefte te ondersteunen, zijn methodieken nodig om te toetsen waar maatregelen nodig zijn en/of er aan de eisen wordt voldaan. Het gaat hier niet om standaard IT systemen, maar om IoT/OT (embedded) systemen die (al dan niet) met IT systemen verbonden zijn.
Use case en link met (organisaties uit) topsectoren	Om de veiligheid van IoT/OT (embedded) systemen (die (al dan niet) met IT-systemen verbonden zijn) te verzekeren en waarborgen, zijn methodieken nodig om te toetsen waar maatregelen nodig zijn en/of er aan de gestelde security eisen wordt voldaan.
Scope en onderzoeksvragen op hoofdlijnen	Kennis/innovatie vragen:

	- Hoe ziet een generiek security assessment methodiek eruit voor connected IT/IoT/OT systemen (al dan niet embedded)? - Zijn er verschillen in toepassingen in verschillende maatschappelijke sectoren (Energie, Water)? o Hoe is deze methodiek toepasbaar te maken op ketens van systemen?
Ingeschatte duur en omvang van verwachte projecten	Verwachte duur: 1-2jr Verwachte omvang: <500K

Case 2: Veilige sensoren voor automatisch inspecteren en detecteren

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ✓ **Topsector Energie** ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	☐ Topsector Agri & Food ✓ **Topsector Creatieve Industrie** ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** Topsector Life Sciences and Health ✓ **Topsector Logistiek** ✓ **Topsector Tuinbouw & Uitgangsmaterialen** ✓ **Topsector Water & Maritiem** ✓ **Topsector Chemie** Andere partners en bedrijven: o Safety Delta Nederland (SDN) , TUD e.a.
Thema BGP	Veilig datagedreven werken
Relatie met MTIB	Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.
Doel en nut van de beoogde pre-competitieve innovatie	*To do*
Use case en link met (organisaties uit) topsectoren	o Bij (o.a.) alternatieve energieopwekking (denk Wind op Zee) is veilige bediening en onderhoud nodig (i.c. onder en boven water). Sensoren geven automatisch data af die bepalen of het veilig genoeg is. B.v. winddata om windmolens tijdig in vaanstand te zetten. De data uit sensoren moet betrouwbaar zijn: zeker afkomstig van de bron en data onderweg niet gemanipuleerd. Deze problematiek speelt bij Water & Maritiem ook in b.v. inspectie riolering en drinkwater.

	○ Door ontwikkeling van kennis op de ontwikkelingen die er zijn op het gebied van datamanipulatie en innovatie om die manipulatie te voorkomen en te detecteren wanneer het gebeurt, kunnen we als Nederland de operatie van onze kritieke infrastructuren veilig stellen
Scope en onderzoeksvragen op hoofdlijnen	Kennis/innovatie vragen: ○ Hoe kan de authenticiteit van cruciale databronnen voor inspectie en detectie van problemen in fysieke infrastructuur worden gewaarborgd? ○ Idem de integriteit van datastromen, zoals bescherming tegen spoofing?
Ingeschatte duur en omvang van verwachte projecten	Verwachte duur: 1-2jr Verwachte omvang: 500K – 1mln

Case 3: Cyber Threat Intelligence Sharing and Threat Modelling

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ✓ **Topsector Energie** ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Thema BGP	✓ Veilige OT en OT/IT integratie ✓ Cyberrisicomanagement ✓ Systeem- en ketenveiligheid
Relatie met MTIB	Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.
Doel en nut van de beoogde pre-competitieve innovatie	○ Er wordt in Nederland en wellicht ook in Europese context onvoldoende samengewerkt op het gebied van strategische en tactische uitwisseling van kennis en ervaringen op het gebied van cyberveiligheid ○ Op het moment dat we echt een op een veilige wijze de economische en maatschappelijke kansen van digitalisering willen verzilveren, dan zal er samengewerkt

	moeten worden om ongewenste digitale activiteit buiten de deur te houden, dit kan alleen samen, want alleen is een partij te klein om echt weerbaar te zijn
Use case en link met (organisaties uit) topsectoren	Binnen de Nederlandse energiesector en tussen verschillende sectoren wordt er onvoldoende kennis- en ervaringsdeling toegepast als het gaat om cyber dreigingen en risico inventarisatie. Dit zorgt ervoor dat kennis over cyberdreigingen binnen partijen in de sectoren blijven, daar waar het delen kan zorgen voor een bredere oplossingscapaciteit
Scope en onderzoeksvragen op hoofdlijnen	Kennis/innovatievragen: o Kunnen we d.m.v. Threat Modelling templates op onconventionele systemen (d.w.z. systemen als bv laadpalen, windmolens en zonnepanelen binnen de energiesector) aanzienlijk slagkracht ontwikkelen om onze digitale weerbaarheid te vergroten? o Kunnen we d.m.v. het delen van cyber kennis de algemene bewustwording binnen diverse sectoren vergroten? o Kunnen we door het actief delen van ervaring en met cyber threat situaties, collectief tot een bredere cyber weerbaarheid komen?
Ingeschatte duur en omvang van verwachte projecten	Verwachte duur: <1jr (doorlopende beheer buiten scope) Verwachte omvang: 500K

Case 4: Systemisch inzicht in toenemende complexe IT en OT systemen

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ✓ **Topsector Energie** ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ✓ **Topsector High Tech Systems and Materials** ✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ✓ **Topsector Tuinbouw & Uitgangsmaterialen** ☐ Topsector Water & Maritiem ☐ Topsector Chemie Andere partners en bedrijven: NCSC, Defensie
Thema BGP	✓ **Systeem- en ketenveiligheid**

Relatie met MTIB	Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.
Doel en nut van de beoogde pre-competitieve innovatie	Moderne softwaresystemen omvatten steeds complexere en dynamischere toeleveringsketens. Gebrek aan systemisch inzicht in de samenstelling en functionaliteit van deze systemen draagt aanzienlijk bij aan het cyberbeveiligingsrisico.
Use case en link met (organisaties uit) topsectoren	Er is een gebrek aan systemisch inzicht in de samenstelling en functionaliteit van IT/OT systemen.
Scope en onderzoeksvragen op hoofdlijnen	Kennis/innovatie vragen: ○ Hoe beïnvloeden IoT en IT/OT systemen kritieke infrastructuur netten? ○ Kunnen bestaande SBOM analyses nog de risico voor die effecten signaleren?
Ingeschatte duur en omvang van verwachte projecten	Verwachte duur: 2-4jr (NWO) -> overhevelen naar spoor 1, NWO KIC-calls Verwachte omvang: 1mln +

Case 5: Innovatie op intrusion detection

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ✓ **Topsector Energie** ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie ** Dit is mogelijk op alle topsectoren een issue en mogelijkheid tot innovatie* Andere partners en bedrijven: • Defensie
Thema BGP	✓ Robuuste en veilige connectiviteit ✓ Systeem- en ketenveiligheid

Relatie met MTIB	Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.
Doel en nut van de beoogde pre-competitieve innovatie	○ Steeds meer apparaten zijn/worden slim en steeds meer van die slimme apparaten zijn op de een of andere manier gekoppeld aan kritieke infrastructuur (binnen de energiesector bv aan het elektriciteitsnet) ○ Inzicht en kennis over hoe om te gaan met indringers buitenaf (intrusion detection) ○ Nieuwe IoT systemen zijn bij consumenten (zoals Home Energy Management systemen) in gevallen ook gekoppeld met private laadpunten, Vehicle-2-Grid ontwikkelingen maken de versmelting tussen energie- en mobiliteitssystemen nog nauwer
Use case en link met (organisaties uit) topsectoren	Hoe kunnen we zorgen voor vernieuwing op het gebied van 'intrusion detection' door voorspellen en monitoring van systeemprestaties, met gekoppelde nieuwe apparaten (bv aan het elektriciteitsnet) en versmelting van verschillende systemen die voorheen ontkoppeld waren?
Scope en onderzoeksvragen op hoofdlijnen	Kennis/innovatie vragen: ○ Welke nieuwe IoT systemen zorgen voor welke mogelijke nieuwe dreigingen? ○ Hoe zijn systemen aan elkaar gekoppeld door introductie van nieuwe apparaten? ○ Welke vernieuwing is er nodig om intrusion detection geschikt te maken voor deze meer gekoppelde en complexe systemen?
Ingeschatte duur en omvang van verwachte projecten	○ Verwachte duur: 1-2jr ○ Verwachte omvang: 500K – 1 mln

Case 6: Supply Chain Security

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ✓ **Topsector High Tech Systems and Materials** ☐ Topsector ICT ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	*Zo concreet mogelijk (als geen namen van bedrijven of instellingen, dan in elk geval beoogde categorie, b.v. "telecom", "netbeheerders" of "procesindustrie")* ☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ✓ **Topsector Logistiek** ✓ **Topsector Tuinbouw & Uitgangsmaterialen** ☐ Topsector Water & Maritiem

	☐ Topsector Chemie Andere partners en bedrijven: • Defensie
Thema BGP	✓ Systeem- en ketenveiligheid
Relatie met MTIB	KIA Veiligheid: Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.
Doel en nut van de beoogde pre-competitieve innovatie	De verwevenheid van productie- en dienstenketens is groot. Steeds meer van deze verwevenheid is digitaal. In het digitale domein is ook sprake van een grote supplier afhankelijkheid en verwevenheid. Systemen draaien op andere systemen (system-of systems), bevatten onderdelen van leveranciers die ook weer onderdelen van andere leveranciers nodig hebben (Tier 1, 2, 3,…) waarbij sprake is van een global supply network. Hiermee is zowel bij aanschaf als bij updaten het risico op aanwezigheid van kwetsbaarheden, ingebouwde achterdeuren en malware. Met een verstoring of een hack van een onderdeel in de keten kan de hele keten verstoord worden. Door dit globale supply network is het zicht op de supply chain risico's onduidelijk. Anderzijds kan de reikwijdte van hacks erg groot zijn, omdat bij bijvoorbeeld software-updates na een hack malware exponentieel verspreid kan worden. De meest risicovolle momenten betreffen aanschaf van software en/of componenten die opgenomen worden in het netwerk en de momenten van updates van in het netwerk draaiende applicaties en systemen, waarbij malware binnengehaald wordt. Om de problemen het hoofd te bieden is het essentieel om in te zetten op: 1. ontwikkelen van mitigerende maatregelen 2. validatie en beveiliging van de ontwikkelde maatregelen 3. beslisondersteunende tooling op basis van toetsing en mitigerende mogelijkheden om betere inschatting van risico's te nemen 4. dynamische inzichten in afhankelijkheden in volledige productie- en dienstenketens 5. trainomgeving voor medewerkers zodat bij het voordoen van supply chain incidenten de juiste maatregelen en acties genomen worden 6. Detectie van gerichte aanvallen op onze vitale processen (denk aan het hacken van alle gemalen in een regio)
Use case en link met (organisaties uit) topsectoren	Om het complexe brede probleem van supply chain te scopen zal in dit BGP in eerste instantie gefocust worden op het ontwikkelen van een digital twin ten behoeve van supply chain security. De digital twin zal een omgeving kunnen bieden waarbinnen mitigerende maatregelen, het valideren en beveiligen van de ontwikkelde maatregelen en het ontwikkelen van beslisondersteunende tooling op basis van toetsing en mitigerende mogelijkheden om betere inschatting van risico's te nemen bieden. De digital twin zal vanuit zowel defensieve als offensieve testing kunnen worden ingezet. Het zal tevens dienen als een digitale trainomgeving voor medewerkers zodat bij het voordoen van supply chain incidenten de juiste maatregelen en acties genomen worden en door detectie van gerichte aanvallen op gehele keten.

Scope en onderzoeksvragen op hoofdlijnen	• De hoofd-onderzoeksvraag is: *Hoe kan de ketenafhankelijkheid beheersbaar gemaakt worden*? Hierbij wordt ingezet op het ontwikkelen van digital twin van dynamische afhankelijkheden waarop risico's in een gehele productie- en/of dienstverleningsketen getest en getraind kunnen worden. Deze use case modelleert en simuleert een flow binnen een leverancierskeketen De onderstaande onderzoeksvragen zullen ondersteund worden door de hierboven beschreven digital twin: • Hoe kan een gewogen risico inschatting gemaakt worden bij aanschaf van onderdelen (componenten en/of applicaties) die met het ICT-netwerk verbonden worden? • Ontwikkelen van beslisondersteuningstooling die inzicht geeft in de diverse aspecten aan risico's (o.a. geopolitieke status, kwaliteit, certificering, leveringszekerheid) in combinatie met inzicht in mitigerende maatregelen (door automatische modelering van de dynamische architectuuromgeving en mitigerende mogelijkheden). Deze beslisondersteuning vormgegeven met inachtneming van diverse functies/rollen en organisatorische processen waarlangs beslissingen genomen worden.
Ingeschatte duur en omvang van verwachte projecten	Ketenafhankelijkheden & ontwikkeling digital twin - Dynamische ketenafhankelijkheden modelleren - Ontwikkeling digital twin voor supply chain security - Detectie van ketenbrede gerichte aanvallen - Beslisondersteuningstool (2 jaar)

Case 7: Supply Chain Security Tool

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ✓ **Topsector High Tech Systems and Materials** ☐ Topsector ICT ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	*Zo concreet mogelijk (als geen namen van bedrijven of instellingen, dan in elk geval beoogde categorie, b.v. "telecom", "netbeheerders" of "procesindustrie")* ☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ✓ **Topsector Life Sciences and Health** ✓ **Topsector Logistiek** ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ✓ **Topsector Chemie**

	Andere partners en bedrijven: • Defensie
Thema BGP	✓ Systeem- en ketenveiligheid
Relatie met MTIB	• Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.
Doel en nut van de beoogde pre-competitieve innovatie	Naarmate bedrijven groter worden en meer met elkaar verbonden zijn, zijn ze voor de uitvoering van hun bedrijfsactiviteiten steeds meer afhankelijk van leveranciers. Naarmate het technologische landschap zich verder ontwikkelt, kan deze afhankelijkheid, indien niet goed beveiligd, een kwetsbaarheid worden. In de afgelopen jaren is gebleken dat toeleveringsketens een van de belangrijkste zwakke plekken in de beveiliging van organisaties zijn. Ze creëren onbedoeld een achterdeur naar de privacy gevoelige data en activiteiten van nietsvermoedende bedrijven. Hoewel beveiliging binnen de muren van het bedrijf hoog in het vaandel mag staan, bent je slechts zo sterk als je meest kwetsbare leverancier. Het is verontrustend dat je risicoprofiel afhangt van de waakzaamheid van anderen, maar door de juiste stappen te nemen door je toeleveringsketen te beoordelen, te beveiligen en te bewaken, kan je de controle weer terug krijgen. Het beoordelen van je rol binnen de supply chain en je eigen cybersecurity maturiteit is complex. Daarnaast zijn er op het moment geen helder toepasbare oplossingen om de zogenaamde whitespots, de zwakke plekken in je supply chain inzichtelijk te krijgen.
Use case en link met (organisaties uit) topsectoren	Deze use case richt zich op de ontwikkeling van een tool, die toepasbaar is voor bedrijven en organisaties om een eerste inzicht te krijgen in de supply chain waar je zelf onderdeel van uit maakt, in de zwakke punten in de keten en je cyber security maturiteit. Dit inzicht geeft je hiermee input in de meest efficiënte maatregelen die je kan nemen om de keten als geheel, en jezelf als bedrijf of organisatie naar een hogere cyber security maturiteit te brengen.
Scope en onderzoeksvragen op hoofdlijnen	De hoofd-onderzoeksvraag is: Hoe kan je de supply chain in kaart brengen vanuit het oogpunt van cybersecurity en waar zitten de zwakke punten ? Deze use case heeft een concrete deliverable: een toepasbare tool.Het is tevens een bewustwordingsinstrument. Het richt zich niet alleen op de supply chain als geheel maar ook de rol die het bedrijf of de organisatie zelf kan nemen om de supply chain en haar eigen cybersecurity situatie te optimaliseren. De onderzoeksvragen gekoppeld aan deze use case zijn: • Welke methodieken zijn er reeds aanwezig bij de kennisinstellingen om supply chains te mappen en welke kennis ontbreekt nog? • Hoe kunnen we de kennis en methodieken convergeren naar een toepasbare tool • Welke bronnen met cybersecurity dreigingsinformatie kunnen worden ingezet. Kunnen hier dreigingen uit worden geïdentificeerd die voor een bepaalde sector extra aandacht vereist? • Hoe identificeer je de whitespots in een supply chain, Welke kennis is hierover reeds beschikbaar en welke moet worden ontwikkeld? • Hoe zorgen we ervoor dat de tool ook bewustwording creeert bij partijen die zich nu nog niet bewust zijn van de risico's bij een cyberaanval op een supply chain?

Ingeschatte duur en omvang van verwachte projecten	• 1,5 jaar

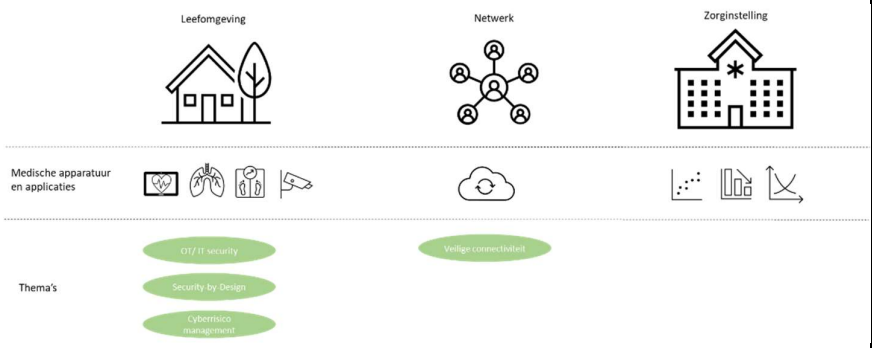
Case 8: Modelleren en simuleren van complexe OT/IT systemen

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ✓ **Topsector High Tech Systems and Materials** ☐ Topsector ICT ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	*Zo concreet mogelijk (als geen namen van bedrijven of instellingen, dan in elk geval beoogde categorie, b.v. "telecom", "netbeheerders" of "procesindustrie")* ☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ✓ **Topsector Energie** ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ✓ **Topsector Life Sciences and Health** ✓ **Topsector Logistiek** ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie Andere partners en bedrijven: • N.t.b.
Thema BGP	✓ Veilige OT en OT/IT integratie
Relatie met MTIB	*Thema Veiligheid:* • Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.
Doel en nut van de beoogde pre-competitieve innovatie	ICS en converged IT/OT (inclusief de IoT en IIOT) omgevingen worden steeds meer verbonden aan de intranetten en het internet waardoor deze steeds kwetsbaarder worden voor aanvallen. Een aanval kan grote impact hebben, niet alleen op de getroffen organisatie maar ook op zowel de economie als de maatschappij. Er is op dit moment weinig zicht op wat er werkelijk gebeurt binnen de OT infrastructuur van deze bedrijven. Er is daarnaast ook nog weinig zicht op de impact van een aanval en een eventuele mitigerende actie. Een goede Test and Experimentation Facility waarin systemen volwaardig en nauwkeurig kunnen worden gemodelleerd en gesimuleerd en waarbij verschillende soorten aanvallers, verschillende soorten aanvallen, kunnen worden gemodelleerd en gesimuleerd is een oplossingsrichting voor de bovenstaande uitdagingen gezien de beperkte beschikbaarheid en (terechte) vrees voor negatieve effecten op de OT systemen. Een digital twin als testomgeving is een door alle deelnemende partijen geschikt middel om courses of actions te kunnen bepalen voor de werkelijke omgeving. Het opzetten van een digital twin is complex. Het gaat hier om het modelleren en simuleren van systemen én de infrastructuren van de omgevingen, welke daarom eerst goed begrepen zullen moeten worden Met een digital twin kan de attack surface kunnen worden gesimuleerd en de security issues zullen hier goed naar voren moeten kunnen komen. Voor defensie kan

	het gebruik van digital twins naast deze defensieve aspecten ook relevant zijn vanuit een offensief perspectief. De hoofdvraag van deze use case is dan ook bepaald als volgt: *Hoe kunnen systeem & infrastructuur adequaat worden gemodelleerd /gesimuleerd, allereerst gelet op het oogpunt van cybersecurity?*
Use case en link met (organisaties uit) topsectoren	Een digital twin als testomgeving is een door alle deelnemende partijen geschikt middel om courses of actions te kunnen bepalen voor de werkelijke omgeving. Het opzetten van een digital twin is complex. Het gaat hier om het modelleren en simuleren van systemen én de infrastructuren van de omgevingen, welke daarom eerst goed begrepen zullen moeten worden Met een digital twin kan de attack surface kunnen worden gesimuleerd en de security issues zullen hier goed naar voren moeten kunnen komen. Voor defensie kan het gebruik van digital twins naast deze defensieve aspecten ook relevant zijn vanuit een offensief perspectief. De hoofdvraag van deze use case is dan ook bepaald als volgt: *Hoe kunnen systeem & infrastructuur adequaat worden gemodelleerd /gesimuleerd, allereerst gelet op het oogpunt van cybersecurity?*
Scope en onderzoeksvragen op hoofdlijnen	• Wat zouden de eigenschappen van deze soort Digital Twin moeten zijn? Het bepalen van het aggregatieniveau van een digital twin is een onderzoeksvraag. Tot welk niveau is modellering nodig? Bij welk aggregatieniveau is het kosteneffectief betekenisvol? Op welke manier kan de digital twin als een twin multi-inzetbare testomgeving voor IT/OT worden vorm worden gegeven? De technologie/oplossingen die worden ontwikkeld zullen voor meerdere sectoren moeten kunnen worden ingezet. • Hoe kan het gebruik van de digital twin, naast de inzet vanuit defensieve aspecten ook worden ingezet vanuit een offensieve simulering? Bovenstaande onderzoeksvragen richten zich op het modelleren en simuleren van systeem & infrastructuur. Vervolgonderzoekvragen richten zich op de inzet van de digital twin. Hoe kunnen de juiste courses of actions (COA's) worden bepaald met de digital twin. • Hoe kan je inzichtelijk maken **hoe aanvallen goed kunnen worden waargenomen**. Hierbij is het belangrijk dat het normale gedrag binnen de complexe infrastructuur goed gemodelleerd kan worden. Dit is de basis voor het detecteren van anomalieën (vreemde activiteiten of gedragingen binnen de infrastructuur die een signaal kunnen zijn van een aanval) van groot belang. De vraag hierbij is welke (combinatie van) (anomalie)detectietechnieken geschikt zijn voor converged IT/OT omgevingen. • De haalbaarheid en toepasbaarheid van **(anomalie)detectie toetsen**. Vragen hierbij zijn hoe netwerk data en sensor data slim gecombineerd kunnen worden, hoe alerts actionable gemaakt kunnen worden en hoe false positives gereduceerd kunnen worden. Het doel is om een **prototype** voor security monitoring en detectie te realiseren. Het prototype kan worden gevalideerd binnen een digital twin en/of operationele context.
Ingeschatte duur en omvang van verwachte projecten	4 jaar.

Case 9: Veilige apparatuur en applicaties in thuisomgeving

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ✓ **Topsector Life Sciences and Health** ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	✓ **Topsector Agri & Food** ☐ Topsector Creatieve Industrie ✓ **Topsector Energie** ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ✓ **Topsector Tuinbouw & Uitgangsmaterialen** ✓ **Topsector Water & Maritiem** ☐ Topsector Chemie Andere partners en bedrijven: • N.t.b.
Thema BGP	• Security by design • Robuuste en veilige connectiviteit • Veilige OT en OT/IT integratie • Cyberrisicomanagement
Relatie met MTIB	• **Centrale missie:** CM In 2040 leven alle Nederlanders tenminste vijf jaar langer in goede gezondheid en zijn de gezondheids-verschillen tussen de laagste en hoogste sociaal-economische groepen met 30% afgenomen. • **Missies:** I. In 2040 is de ziektelast als gevolg van een ongezonde leefstijl en ongezonde leefomgeving met 30% afgenomen. II. In 2030 wordt zorg 50% meer (of vaker) in de eigen leefomgeving (in plaats van in zorginstellingen) georganiseerd, samen met het netwerk rond mensen. III. In 2030 is van de mensen met een chronische ziekte of levenslange beperking het deel dat naar wens en vermogen kan meedoen in de samenleving met 25% toegenomen. IV. In 2030 is de kwaliteit van leven van mensen met dementie met 25% toegenomen.
Doel en nut van de beoogde pre-competitieve innovatie	• De zorgsector is bij uitstek een sector waar digitalisering -in versnelling geraakt door de coronacrisis- een enorme vlucht heeft genomen. Denk hierbij aan het gebruik van elektronische patiënt dossiers, de inzet van sensors en apps om patiënten op afstand te monitoren, het toepassen van kunstmatige intelligentie/ machine learning voor diagnosestelling en behandeling, en het beschikbare stellen van informatie aan patiënten en cliënten via portalen en persoonlijke gezondheids-omgevingen.

	• Digitalisering is van strategisch belang geworden om de gezondheidszorg in Nederland toegankelijk, betaalbaar en van goede kwaliteit te houden. De betaalbaarheid staat onder druk en krapte op de arbeidsmarkt noodzaakt tot anders organiseren en anders (samen)werken in de zorg. Zorgdigitalisering is een maatschappelijk vraagstuk geworden en van belang voor burgers, overheid, bedrijfsleven, zorgverzekeraars, belangenorganisaties/ koepels en zorginstellingen. • Digitale informatie speelt een cruciale rol in de zorgdienstverlening waarbij de beschikbaarheid, integriteit en vertrouwelijkheid hiervan (aantoonbaar) dient te zijn gewaarborgd. Betrokken partijen voelen en hebben hierin een publiek-private verantwoordelijkheid en het beschermen van informatie en de privacy van patiënten zou voor de zorgsector een vanzelfsprekendheid moeten zijn. Een en ander wordt versterkt door toenemende wet- en regelgeving, zoals de NEN7510, AVG voor privacy, MDR voor medische devices en de WEGIZ voor gegevensuitwisseling. • Met de toenemende digitalisering nemen ook de veiligheidsrisico's toe. [voorbeeld] In februari 2020 bracht de Onderzoeksraad voor Veiligheid een rapport uit waarin werd gewezen op de risico's van patiëntveiligheid bij IT-uitval in ziekenhuizen. Regelmatig halen diverse geslaagde cyber(ransomware) aanvallen op zorginstellingen in het buitenland en ernstige kwetsbaarheden in veel gebruikte systemen en datalekken bij Nederlandse zorginstellingen het nieuws. Ook de WRR bracht een rapport uit over de afhankelijkheid van IT en de risico's op digitale ontwrichting. Zij hebben onder meer een evaluatie gedaan naar de Citrix kwetsbaarheid van begin 2020. Deze kwetsbaarheid heeft ook een forse impact gehad op de zorgsector. • De 2e VWS-missie luidt dat in 2030 minimaal 50% van de zorg in de eigen leefomgeving (ipv in zorginstellingen) wordt georganiseerd, samen met het netwerk rond mensen. • De verplaatsing van zorg naar de thuissituatie is reeds in volle gang waarbij gebruik wordt gemaakt van medische apparatuur en applicaties. Het strategisch belang van cybersecurity gecombineerd met de 2e VWS-missie heeft geleid tot de (titel van de) projectkaart 'cyberveilig gebruik van medische apparatuur en applicaties in de eigen leefomgeving'. In onderstaand figuur is de relatie gevisualiseerd tussen bovenstaande missie, de betreffende BGP Cybersecurity thema's en de projectkaart. 
Inhoudelijke hoofdlijn	• Zorginstellingen werken steeds meer samen in de (zorg)keten en gedragen zich steeds meer als netwerkorganisaties. Door de verplaatsing van zorg naar de thuissituatie wordt de thuis-/ leefomgeving ook onderdeel van de zorgketen. • In de thuissituatie wordt ook vaak gebruik gemaakt van medische technologie; in combinaties van medische apparatuur, wearables (sensors en apps) en (cloud)applicaties (niet meer weg te denken). Specifiek is in de thuissituatie sprake van een combinatie van (gecontroleerde) apparatuur van zorginstellingen en niet-gecontroleerde sensors/ apps en netwerkverbindingen van de consument. • Een beroep wordt gedaan op patiënten/ mantelzorgers in het gebruik en bediening van de apparatuur en applicaties waarvoor ze niet zijn opgeleid (itt tot zorgprofessionals). Dit stelt

	eisen aan de gebruiksvriendelijkheid, rekening houdend met de vaardigheden van vaak kwetsbare groepen. Ook in de thuisomgeving moet sprake zijn van een veilige en gebruiksvriendelijke toepassing hiervan. Zowel zorgverleners als consumenten (patiënten) zouden zo weinig mogelijk hoeven na te denken over de veiligheid van het gebruik van medische apparaten en applicaties. Deze moeten vanzelfsprekend veilig zijn en blijven, wat begint bij de ontwerpfase. • Sinds 26 mei 2021 geldt nieuwe Europese regelgeving voor medische hulpmiddelen (Medical Device Regulation - MDR). Dit kan betekenen dat een product in een andere risicoklasse valt dan voorheen en daarom moet voldoen aan strengere veiligheids- en kwaliteitseisen. De MDR kan een belangrijke bijdrage aan security-by-design leveren (zie 1e thema). • Niet alleen worden hoge eisen gesteld aan de apparatuur zelf maar ook aan de netwerkinfrastructuur om gegevens en medische toepassingen in de keten gezamenlijk en veilig te kunnen gebruiken (zie 3e thema). • Specifiek aandachtspunt is dat de levenscyclus van medische apparatuur vaak langer is dan de IT-component die onderdeel uitmaakt van het apparaat. Wijzigingen hierop moeten aan strikte voorwaarden voldoen en voor het opsporen van kwetsbaarheden is specifieke technologie benodigd (zie 4e thema). • Bij alle wet- en regelgeving in de zorg (onder meer NEN 7510, AVG, MDR, ISO27001, WGBO, WKKGZ en convenant medische technologie) staat risicomanagement centraal. Dit geldt ook voor de thuissituatie (zie 5e thema). Het adequaat beveiligen van medische technologie in professionele zorgomgevingen kent al diverse uitdagingen en hier worden in de thuisomgeving extra uitdagingen aan toegevoegd.
Use case en link met (organisaties uit) topsectoren	Om medische apparatuur en applicaties in een thuisomgeving van patiënten adequaat te kunnen beveiligen en veilig te kunnen gebruiken is een samenhangend stelsel van organisatorische, procedurele en technische maatregelen nodig, rekening houdend met de specifieke kenmerken van deze omgeving (zie ook observaties hierboven). Dit begint bij de ontwerpfase (denk aan gebruiksvriendelijkheid) (zie thema 1) en geldt niet alleen voor de apparatuur en applicaties (zie thema 4), maar ook voor de netwerkinfrastructuur (zie thema 3) waaraan het apparaat is gekoppeld en de IT-omgeving van de zorginstelling om de patiënt op afstand zorg te kunnen bieden (zie ook figuur). Een verstoring (bv stroomuitval, verkeerd gebruik apparatuur door patiënt, netwerkuitval, etc) of een hack kan de patiëntveiligheid in gevaar brengen. De mate waarin is afhankelijk van de kwetsbaarheid van de patiënt en de zorg die met het medische apparatuur/ applicatie wordt geleverd (zie thema 5). De diversiteit aan systemen (en hierin gebruikte technologieën die weer van andere leveranciers kunnen zijn) en onderlinge connectiviteit is groot en volledig gedigitaliseerd (zie thema 6). Mede gelet op de specifieke kenmerken die samenhangen met de thuissituatie (cyberveiligheid is afhankelijk van de zwakste schakel) is het krijgen van een volledig overzicht en inzicht op risico's veelal niet mogelijk (sprake van een bepaalde mate van onzekerheid). Om hier meer grip op te krijgen is het noodzakelijk om in te zetten op: 1. Definiëren van voor de eigen leefomgeving specifieke zorgprofielen in combinatie met medische apparatuur en applicaties (op basis van een 'archetype zorgprofiel leefomgeving'). 2. Gegeven het archetype, het ontwikkelen van een risicomethodiek waarbij patiëntveiligheid centraal staat, en het op basis hiervan uitwerken van risicoprofiel per zorgprofiel. 3. Op basis van de eisen die de MDR stelt aan 'medical devices', in combinatie met (inter)nationale normenkaders (ISO27xxx), het ontwikkelen van concrete richtlijnen en handvatten (mitigerende maatregelen) voor de hele levenscyclus. De richtlijnen zijn niet alleen technisch van aard, maar ook organisatorisch en procedureel. De risicomethodiek wordt gerelateerd aan de maatregelen. 4. Valideren van de verschillende zorgprofielen (samen met het risicoprofiel en bijbehorende mitigerende maatregelen) aan de hand van praktijkcases. De opgedane praktijkervaring wordt verwerkt in zowel de risicomethodiek als de richtlijnen.

	5. Ontwerpen en ontwikkelen van een 'platform' waarmee zorgprofielen kunnen worden gemodelleerd ('digital twin'), risico en maatregelen kunnen worden gesimuleerd om in de praktijk tot veiligere omgevingen te komen. Vanwege de complexiteit en diversiteit van het voorliggende vraagstuk worden drie fasen voorgesteld. In de eerste fase wordt een strategische verkenning uitgevoerd voor nadere verdieping en probleemvalidatie. Hiertoe wordt gesproken met 'veel' verschillende partijen en relevante documentatie bestudeerd. De bevindingen uit de gesprekken en documentatie worden verwerkt in een rapportage en gepubliceerd. In een aparte notitie wordt de aanpak en de planning van fase twee en drie gemaakt. De tweede fase omvat de ontwikkeling van de zorgprofielen, de risicomethodiek en de richtlijnen. En daarnaast de validatie hiervan. De derde fase betreft het platform waarmee risico's en maatregelen kunnen gesimuleerd.
Scope en onderzoeksvragen op hoofdlijnen	De hoofdonderzoeksvraag luidt: wat zijn de barrières (cyberrisico's), maar ook de drijfveren voor succes (maatregelen), om elk individu cyberveilige, gebruiksvriendelijke zorgoplossingen (medische apparatuur en applicaties) te bieden en te gebruiken in zijn of haar eigen leef- (of werk-) omgeving? De onderliggende/ ondersteunende onderzoeksvragen zijn: • Voor welke typen zorg en voor welke patiëntgroepen kan zorg in de thuissituatie worden geleverd? Welke voorwaarden gelden er, bv vaardigheden patient icm bediening apparatuur, IT thuis, (denk aan de zwakste schakel) etc ? • Welke risicomethodieken bestaan er en worden gebruikt voor het uitvoeren van een risicoanalyse? Wat zijn de ervaringen (voor- en nadelen) met de methodieken, in hoeverre zijn de methodieken praktisch toepasbaar, etc • Welke eisen stelt de MDR aan cybersecurity? In hoeverre zijn deze eisen concreet toepasbaar (blijft het apparaat of de app gebruiksvriendelijk per doelgroep?), hoe verhouden de eisen zich tot (inter)nationale standaarden, etc • Hoe worden de verschillende methodieken en de MDR-eisen in de praktijk toegepast door leveranciers, zorginstellingen en toezichthouders Afbakening t.o.v. in NLAIC lopende onderzoeken zal ook nog plaats moeten vinden.
Ingeschatte duur en omvang van verwachte projecten	Verwachte duur: 2 tot 4 jaar. Verwachte omvang: 1-5 mio

Case 10: Veilig datagedreven werken

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ✓ **Topsector Energie** ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ✓ **Topsector Life Sciences and Health** ☐ Topsector Logistiek ✓ **Topsector Tuinbouw & Uitgangsmaterialen** ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials

	✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie Andere partners en bedrijven: • N.t.b.
Thema BGP	• Veilig datagedreven werken
Relatie met MTIB	• **Centrale missie:** CM In 2040 leven alle Nederlanders tenminste vijf jaar langer in goede gezondheid en zijn de gezondheids-verschillen tussen de laagste en hoogste sociaal-economische groepen met 30% afgenomen. • **Missies:** I. In 2040 is de ziektelast als gevolg van een ongezonde leefstijl en ongezonde leefomgeving met 30% afgenomen. II. In 2030 wordt zorg 50% meer (of vaker) in de eigen leefomgeving (in plaats van in zorginstellingen) georganiseerd, samen met het netwerk rond mensen. III. In 2030 is van de mensen met een chronische ziekte of levenslange beperking het deel dat naar wens en vermogen kan meedoen in de samenleving met 25% toegenomen. IV. In 2030 is de kwaliteit van leven van mensen met dementie met 25% toegenomen.
Doel en nut van de beoogde pre-competitieve innovatie	• Met de toenemende digitalisering neemt ook de hoeveelheid digitale gegevens toe. Des te meer als gegevens worden samengevoegd tot (zeer) grote gegevensverzamelingen afkomstig van meerdere zorginstellingen. Algoritmen zijn hierbij gebaat, en biedt veel mogelijkheden om ML/AI toepassingen te ontwikkelen. Binnen zorginstellingen (met name beeld- en gegevensintensieve omgevingen) staat ML/AI volop in de belangstelling. Niet alleen binnen de instelling zelf, maar ook bij samenwerkingsverbanden en leveranciers. Nu (nog) als ondersteunend middel voor de zorgverlener, maar mogelijk in de toekomst als vervanger
Use case en link met (organisaties uit) topsectoren	• Toegepast onderzoek is nodig naar mogelijkheden om kwaliteit van data in bronsystemen te kunnen verbeteren, evenals een betrouwbare transformatie van data naar bruikbare datasets t.b.v. onderzoek en toepassing in zorginstellingen. • Prioriteit zou liggen op de transformatie van data en de algoritmen, en in 2e instantie de kwaliteit van brondata. • Samenwerkingsverband die op structurele basis zorgdata verzamelt, de data transformeert en beschikbaar stelt voor onderzoek en toepassingen.
Scope en onderzoeksvragen op hoofdlijnen	• ML/AI toepassingen dienen aantoonbaar betrouwbaar te werken: • Algoritmen vereisen voor een goede werking (aantoonbare) integere data, veelal afkomstig uit bronsystemen. Hoe weet je dat data kwalitatief op orde is, en onderweg niet is gemanipuleerd? • Algoritmen dienen (aantoonbaar) betrouwbaar te werken (en dus betrouwbaar ontworpen -> secure-by-design). Hoe weet je dat algoritmen niet zijn gecompromitteerd?

	• Algoritmen dienen (aantoonbaar) betrouwbare informatie te genereren. Hoe weet je dat de data vanaf de bron t/m de grafiek/ tabel betrouwbaar is verwerkt (data-lineage)? • NB: vraagstukken rondom het anonimiseren van gegevens en verkrijgen van toestemming tbv onderzoek is buiten scope. Afbakening t.o.v. in NLAIC lopende onderzoeken zal ook nog plaats moeten vinden.
Ingeschatte duur en omvang van verwachte projecten	Verwachte duur: 2 tot 4 jaar. Verwachte omvang: 1-5 mio

Case 11: Systeem/Ketenveiligheid

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ✓ **Topsector Life Sciences and Health** ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	✓ **Topsector Agri & Food** ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ✓ **Topsector Water & Maritiem** ☐ Topsector Chemie
Thema BGP	• Systeem- en ketenveiligheid
Relatie met MTIB	

	• **Centrale missie:** CM In 2040 leven alle Nederlanders tenminste vijf jaar langer in goede gezondheid en zijn de gezondheids-verschillen tussen de laagste en hoogste sociaal-economische groepen met 30% afgenomen. • **Missies:** I. In 2040 is de ziektelast als gevolg van een ongezonde leefstijl en ongezonde leefomgeving met 30% afgenomen. II. In 2030 wordt zorg 50% meer (of vaker) in de eigen leefomgeving (in plaats van in zorginstellingen) georganiseerd, samen met het netwerk rond mensen. III. In 2030 is van de mensen met een chronische ziekte of levenslange beperking het deel dat naar wens en vermogen kan meedoen in de samenleving met 25% toegenomen. IV. In 2030 is de kwaliteit van leven van mensen met dementie met 25% toegenomen.
Doel en nut van de beoogde pre-competitieve innovatie	• Zorgsector ontwikkelt zich steeds meer richting ketens van zorg waarbinnen publieke en private partijen samenwerken en producten en (zorg)diensten worden geleverd. Niet alleen voor wat betreft nutsvoorzieningen en IT maar ook (kritieke) toeleveringsketens zoals medicatie, bloed en medische disposables. Voor deze ketens zijn vaak geen directe alternatieven voorhanden en/of kunnen in beperkte mate voorraden worden aangelegd. Bij zorginstellingen bestaat vaak geen inzicht in cyberrisico's en weerbaarheid van dergelijke . • In de VS zijn hier de afgelopen jaren via CISA al flinke stappen in gezet (zie link), in NL moet dit nog van de grond komen. Zie https://www.cisa.gov/national-critical-functions
Use case en link met (organisaties uit) topsectoren	• Voorbeelden van ketens met een grote afhankelijkheid zijn: medicatie, medische disposables, veiligheidsketen, etc. • Voorgesteld wordt om één keten te selecteren en met betrokken partijen de vraagstelling uit te werken.
Scope en onderzoeksvragen op hoofdlijnen	Onderzoek nodig naar risicomanagement in de supply chain van zorginstellingen. Patiëntveiligheid kan in het geding komen bij de zwakste schakel in de keten. • Wat zijn de belangrijkste toeleveringsketens in de zorg? • Welke cybergerelateerde risico's kunnen worden onderkend binnen deze ketens? • Welke mitigerende maatregelen zijn nodig om de cyberrelateerde risico's te kunnen beheersen? • Welke instrumenten zijn voorhanden voor borging en opvolging, en welke dienen nog te worden ontwikkeld?
Ingeschatte duur en omvang van verwachte projecten	Verwachte duur: 1-1,5 jaar (m.n. i.v.m. consulteren van ketenpartijen) Verwachte omvang: < 1 mio Euro

Case 12: Cyberweerbaarheid in de logistieke sector

Initiatief nemende topsector	☐ Topsector Agri & Food ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ☐ Topsector ICT ☐ Topsector Life Sciences and Health ✓ **Topsector Logistiek** ☐ Topsector Tuinbouw & Uitgangsmaterialen ☐ Topsector Water & Maritiem ☐ Topsector Chemie
Andere deelnemende Topsectoren, KIC-partners en bedrijven	*Zo concreet mogelijk (als geen namen van bedrijven of instellingen, dan in elk geval beoogde categorie, b.v. "telecom", "netbeheerders" of "procesindustrie")* ✓ **Topsector Agri & Food** ☐ Topsector Creatieve Industrie ☐ Topsector Energie ☐ Topsector High Tech Systems and Materials ✓ **Topsector ICT** ☐ Topsector Life Sciences and Health ☐ Topsector Logistiek ☐ Topsector Tuinbouw & Uitgangsmaterialen ✓ **Topsector Water & Maritiem** ☐ Topsector Chemie Andere partners en bedrijven: • N.t.b.
Thema BGP	✓ Awareness, kennis en vaardigheden
Relatie met MTIB	*Zie: https://www.topsectoren.nl/missiesvoordetoekomst* Centrale missie: Cyberveiligheid. Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren. Overige relevante missies: Vraag en aanbod worden sneller bij elkaar gebracht om kort cyclisch succesvolle innovaties te implementeren. Het vak van veiligheidsprofessional behoort in 2030 tot de top 10 van meest aantrekkelijke beroepen in Nederland. Relatie met missie logistiek: De transitie naar duurzame, concurrerende en veilige logistieke ketens en goederenvervoer als onderdeel van de Gezamenlijke Ambitie, Logistiek en goederenvervoer in 2050: concurrerend, duurzaam en veilig.
Doel en nut van de beoogde pre-competitieve innovatie	Nederland is toonaangevend in de logistiek met haar diverse mainports zoals de Haven van Rotterdam en Schiphol. Dit zorgt ervoor dat Nederland een aantrekkelijke vestigingslocatie is voor ondernemers. De logistieke sector draagt steeds meer bij aan de Nederlandse economie. Logistiek is bovendien onmisbaar voor andere sectoren zoals de voedsel en maakindustrie. Dit maakt logistiek een belangrijke economische sector. Om de toonaangevende positie in de

	logistiek te behouden wordt er geïnvesteerd in innovatie waaronder digitalisering van de sector. Om toonaangevend te blijven in de logistiek worden bedrijfsprocessen continue vernieuwd en worden er samenwerkingen in de logistieke keten aangegaan. Informatie in en tussen bedrijven, opdrachtgevers en opdrachtnemers (zoals klantgegevens en voertuigposities) wordt steeds meer via internet gedeeld. Het digitaal delen van informatie ten behoeve van het logistieke proces is eenvoudiger, sneller en efficiënter, maar dit maakt ondernemingen in deze sector ook kwetsbaar voor cyber security risico's. De logistieke sector bestaat uit goederenvervoer en personenvervoer. Transport vindt plaats over de weg, het spoor, het water en de lucht. Hierbij wordt gebruik gemaakt van een logistieke keten. Het betreft de gehele organisatie, planning en uitvoering van de stroom van producten en diensten. Informatievoorziening is cruciaal voor het beheersingsproces van personen- en goederenbewegingen. Deze is doorgaans gedigitaliseerd. Belangrijke schakels in de logistieke keten ten aanzien van goederenvervoer zijn de aanvoer, productie, opslag, overslag en distributie. Er is zodoende sprake van een ketenafhankelijkheid van de verschillende bedrijven die actief zijn in de logistieke keten. Dit betekent dat wanneer er ergens in de keten een (cyber security) incident plaatsvindt, dit aanzienlijke gevolgen kan hebben voor de gehele keten. Dit betekent dat cyberweerbaarheid niet alleen betrekking heeft op afzonderlijke bedrijven, maar op gehele logistieke processen en ketens. Bedrijven in de logistieke sector lopen een niet gering risico om slachtoffer te worden van cybercriminaliteit door de aard van hun bedrijfsactiviteiten, de producten en diensten die ze vervoeren voor derden en/of de mogelijke buit die er bij hun te halen is. De mate van cyberweerbaarheid van ondernemers in de logistieke sector verschilt sterk. Een belangrijke oorzaak hiervan is dat een deel van de ondernemers zich onvoldoende bewust is van de kans op slachtofferschap van cybercriminaliteit en de mogelijke impact daarvan op hun bedrijfsvoering. Een andere oorzaak is dat het bij een deel van de ondernemers ontbreekt aan kennis, capaciteit en/of middelen om hun cyberweerbaarheid daadwerkelijk te bevorderen. Hierdoor worden er (met name door de kleinere bedrijven) niet altijd de benodigde (beleidsmatige, technische en/of personele) maatregelen genomen om de cyberweerbaarheid te bevorderen. Tot slot worden door medewerkers al dan niet bewust (bijvoorbeeld uit efficiëntie overwegingen) basisregels van het cyber security beleid genegeerd wat de kans op insider threats verhoogd. Dat hangt nauw samen met een gebrek aan medewerkers binnen de sector die op het gebied van cybersecurity tijdig dreigingen kunnen signaleren en verhelpen. Er doen zich drie barrières voor die ervoor zorgen dat het verhogen van de cyberweerbaarheid van ondernemers (nog) niet optimaal verloopt. De eerste barrière vormt het überhaupt bereiken van de ondernemers om hen te informeren over cyber security dreigingen. De tweede barrière vormt het gedrag van ondernemers. Ondernemers laten zich niet zomaar aanzetten om te investeren in cyber security maatregelen. Dit komt mede doordat ondernemers het risico op slachtofferschap van cybercriminaliteit en de mogelijke gevolgen daarvan onderschatten en/of omdat ze onvoldoende kennis hebben om hun cyberweerbaarheid daadwerkelijk te bevorderen. De derde barrière betreft de gebrekkige samenwerking en informatiedeling door ondernemers in de logistieke sector ten aanzien van cyber security. Het merendeel van bedrijven actief in de logistieke sector werkt samen met tientallen andere bedrijven. Veelal wordt er in ieder onderdeel van het gehele operationele proces samengewerkt en informatie gedeeld met een of meerdere ketenpartners. Bedrijven in de logistieke sector zijn zich bewust van de ketenafhankelijkheid. Zij onderkennen dat de cyberweerbaarheid niet alleen afhankelijk is van de inspanningen van hun eigen organisatie, maar ook (in toenemende mate) van die van hun samenwerkingspartners in de keten. Desondanks wordt er tussen bedrijven in de logistieke sector nog niet of nauwelijks samengewerkt en informatie gedeeld op het terrein van cyber security. Dit is een gemiste kans omdat door informatie over kwetsbaarheden, dreigingen, (bijna) incidenten, best practices en lessons learned te delen de cyberweerbaarheid van afzonderlijke bedrijven en daarmee van de gehele logistieke keten kan worden bevorderd.

Use case en link met (organisaties uit) topsectoren	De (digitale) processen, toegepaste technologieën, (potentiële) kwetsbaarheden en daaruit voortkomende cyber security risico's kunnen verschillen bij ondernemers in de logistieke sector (mede afhankelijk van de aard van hun activiteiten en te vervoeren producten en diensten). Tegelijkertijd zijn er overeenkomsten wat betreft de barrières om de cyberweerbaarheid te bevorderen. Rekening houdend met de verschillen en overeenkomsten kan er worden afgebakend door een specifiek onderzoeksgebied aan te wijzen. Het voorstel hiervoor is de haven van Rotterdam, een belangrijke mainport. Deze use case wordt ingebracht door de Security Delta, het nationale veiligheidscluster, in samenwerking met FERM, een stichting die zich inzet voor de cyberweerbaarheid van ondernemers in het Rotterdamse havengebied.
Scope en onderzoeksvragen op hoofdlijnen	Wat is de aard, omvang en wat zijn de verschijningsvormen van cybercriminaliteit ten aanzien van ondernemers in de logistieke sector? In welke mate zijn ondernemers in de logistieke sector cyberweerbaar? Hoe kan cyberweerbaarheid van (grootte, middelgrote en kleine) ondernemers in de logistieke sector worden bevorderd en/of de ketenafhankelijkheid worden gereduceerd met behulp van technologische en sociale innovatie? Op welke manier kunnen (grootte, middelgrote en kleine) ondernemers in de logistieke sector worden geïnformeerd en geactiveerd om hun cyberweerbaarheid te bevorderen en/of hun ketenafhankelijkheid te reduceren om de kans op en de impact van een mogelijk cyber security incident (in de keten) te beperken? Hoe kunnen medewerkers werkzaam in de logistieke sector door middel van opleiden, trainen en oefenen cyberweerbaar worden gemaakt? Op welke manier kunnen cyber security experts uit andere sectoren worden verleid om te (gaan) werken in de logistieke sector om de cyberweerbaarheid van afzonderlijke ondernemers en/of de gehele keten te bevorderen? Wat kan worden geleerd van technologische en sociale innovaties uit andere sectoren om de cyberweerbaarheid van ondernemers in de logistieke sector te bevorderen?
Ingeschatte duur en omvang van verwachte projecten	De geschatte duur betreft 1 tot 3 jaar en de geschatte investering betreft 100.000 euro. De Security Delta heeft recent in opdracht van de Metropool Regio Rotterdam Den Haag een onderzoek uitgevoerd naar de cyberweerbaarheid van ondernemers in ondermeer de logistieke en maritieme sector in de Provincie Zuid-Holland. In het kader van het onderzoek is gesproken met tientallen functionarissen van bedrijven in de logistieke sector, branche organisaties, publiek private samenwerkingsverbanden, lokale, regionale en nationale overheden. Een aanzienlijk deel hiervan is ook graag bereid mee te werken aan een volgend onderzoek. Daarnaast beschikt FERM over een groot netwerk van bedrijven actief in het Rotterdams havengebied waarvan de verwachting is dat tenminste een deel hiervan desgewenst ook zal participeren aan het te verrichten onderzoek. Tot slot wordt door de Security Delta (mede naar aanleiding van het eerdere onderzoek) momenteel gewerkt aan de oprichting van een cyberweerbaarheidscentrum voor de logistieke sector. Verschillende relevante organisaties hebben hun medewerking hieraan reeds toegezegd. Zij zijn zodoende ook te benaderen voor het te verrichten onderzoek.