ACTIEAGENDA CYBERSECURITY TECHNOLOGIES

DIGITALISERING

DIGITAL HOLLAND
where innovation starts

DIGITALISERING

DIGITAL HOLLAND

where innovation starts

VOORWOORD

Verdienvermogen, weerbaarheid en strategische autonomie zijn van essentieel belang voor onze economie en maatschappij. Toch liggen deze onder vuur. De toenemende impact van cyberaanvallen ondermijnt niet alleen ons verdienvermogen, maar leidt ook tot maatschappelijke ontwrichting. Gijzeling van data, beïnvloeding van verkiezingen, diefstal van intellectueel eigendom en pogingen om vitale infrastructuur aan te vallen zijn in Europa aan de orde van de dag. Het recent verschenen rapport-Wennink noemt het beschermen van de digitale infrastructuur en het versterken van innovatie in cyberveiligheid van groot strategisch belang.

Hier ligt een uitdaging, maar ook een kans voor Nederland.

Als wij in staat zijn onze sterke kennisbasis rondom cybersecurity om te zetten in innovatieve oplossingen om producten en diensten digitaal veilig te maken, slaan we twee vliegen in één klap. Enerzijds beschermen we ons land beter tegen aanvallen. Anderzijds bouwen we een concurrentiekrachtige positie op als land dat cyberveilige producten en diensten levert. Dat gaat echter niet vanzelf, en vraagt om gericht, consistent en langjarig beleid. In deze Actieagenda Cybersecurity Technologies werken we dat uit onder de vlag van de Nationale Technologie Strategie (NTS).

De NTS is een beleidskader van het ministerie van Economische Zaken (EZ). Hierbinnen zijn tien prioriteiten gesteld, waarmee keuzes worden gemaakt voor focus, massa en impact om onze economische slagkracht, nationale veiligheid en maatschappelijke vooruitgang te versterken. Voor elk van deze tien prioritaire sleuteltechnologieën worden actieagenda's ontwikkeld. Dit document betreft de actieagenda Cybersecurity Technologies. Deze actieagenda Cybersecurity Technologies is tot stand gekomen onder regie van Digital Holland (voorheen: Topsector ICT) in de periode najaar 2024 tot eind 2025, in nauwe samenwerking met een brede werkgroep van stakeholders.
De werkgroep stond centraal in het ontwikkelen van een SWOT-analyse, het duiden van het ecosysteem, identificeren van en de grote uitdagingen van vandaag en morgen en het inrichten van een systematiek om deze vraagstukken te adresseren. In dit document vindt u een scherpe analyse maar ook een concreet handelingsperspectief voor activiteiten met impact.

In dit proces zijn organisaties zoals het voormalige dcypher, TNO, NWO, IPN, ACCSS, PRIO en CVNL actief betrokken geweest, naast het kernteam en de adviesraad van de KIA Digitalisering. Er zijn tientallen interviews gehouden en diverse marktconsultaties. Het bureau Technopolis heeft de eerste fase begeleid en bureau Organizational Revolution de tweede fase. De komende periode draait om uitvoering. Dat vraagt om een slagvaardige organisatie, gerichte publiek-private samenwerking en actieve betrokkenheid van stakeholders, regionaal, nationaal en Europees. Alleen samen realiseren we de transitie naar een veilig, concurrerend en technologisch zelfstandig Nederland. Laten we nu aan de slag gaan!

Namens de werkgroep actieagenda Cybersecurity Technologies en bestuur Digital Holland,

Frits Grotenhuis,
Directeur-bestuurder Digital Holland en coördinator KIA Digitalisering

SAMENVATTING

NEDERLAND IN 2035 INTRINSIEK DIGITAAL VEILIG

Dat is de ambitie van deze Actieagenda. Die ambitie is er niet voor niets. De schaal van cyberaanvallen groeit en de schade neemt navenant toe. Met de voortschrijdende digitalisering worden de risico's alleen maar groter. Digitalisering dringt in hoog tempo door in alle sectoren van onze samenleving. Zij vormt het fundament onder energievoorziening, zorg, vitale infrastructuren, transport, productieprocessen, communicatie en innovatie. Die ontwikkeling brengt economische groei en maatschappelijke vooruitgang, maar ze biedt criminelen en statelijke actoren ook nieuwe hackmogelijkheden. De risico's zijn niet alleen financieel: privacy en zelfs de democratie zelf kunnen door cyberaanvallen worden geraakt. Cybersecurity is daarom een urgent vraagstuk.

Nederland is goed gepositioneerd om dat vraagstuk structureel aan te pakken. Wij hebben een sterke kennisbasis die op verschillende gebieden leidend is in de wereld. Dat geeft ons de kans om onze cyberweerbaarheid te vergroten. Daardoor kunnen we effectief op cyberaanvallen reageren. Voorkomen is echter beter dan genezen. De realiteit is dat veel van de technologie waarop we dagelijks vertrouwen, nooit is ontworpen met veiligheid als uitgangspunt. Naast het vergroten van cyberweerbaarheid, zet deze Actieagenda daarom vooral in op 'secure-by-design'. Dat wil zeggen: het ontwikkelen van technologie die zo digitaal veilig mogelijk ontworpen is. Door veiligheid al vanaf het ontwerp van systemen, producten en digitale diensten mee te nemen, kunnen systeem intrinsiek digitaal veilig worden gemaakt.

Om dit te bereiken schetst deze Actieagenda drie actielijnen voor de komende jaren. De eerste is het aanjagen van de sectorale en regionale transitie richting cybersecure-by-design. Daartoe stimuleert de Actieagenda gericht de vorming van publiek-private samenwerking (PPS) rondom intrinsiek veilige oplossingen. Bedrijven, kennisinstellingen en overheden werken samen aan cyberweerbaarheid en aan een transitie van achteraf repareren naar van meet af aan veilig ontwerpen. De tweede lijn betreft de ontwikkeling van nieuwe technologie en methoden. Met name voor cybersecure-by-design en de rol van autonome systemen is nog veel onderzoek en ontwikkeling nodig. Door hierin te investeren kan het Nederlandse bedrijfsleven een nieuwe markt betreden: de technologieën en methoden kunnen worden vertaald in diensten en producten waar wereldwijd vraag naar is. Ten derde roept de Actieagenda op om de randvoorwaarden en de infrastructuur te creëren die de vorige twee lijnen mogelijk maken. Denk hierbij aan menselijk kapitaal en de ontwikkeling van testlabs.

Investeren in technologieontwikkeling en de toepassing daarvan vormt het vertrekpunt van deze Actieagenda. De NTS Cybersecurity Technologies richt zich primair op het ontwikkelen, demonstreren en opschalen van technologieën die digitale veiligheid structureel versterken. Gerichte investeringen zijn nodig om een technologische basis te creëren waarop intrinsiek veilige digitalisering kan worden gebouwd.
De Actieagenda coördineert en versterkt bestaande regionale, nationale en Europese instrumenten zodat zij deze technologieontwikkeling optimaal ondersteunen en toepassing in sectoren en ketens versnellen. Een belangrijk deel van de vooruitgang komt voort uit betere benutting van bestaande kennis, maar structurele technologische doorbraken vergen aanvullende inzet en langdurige investeringen.

INHOUDSOPGAVE

1. INLEIDING: NEDERLAND IN 2035 INTRINSIEK DIGITAAL VEILIG

De aandacht voor cybersecurity groeit snel. Cyber-dreigingen worden steeds vaker werkelijkheid[1] en veroorzaken aanzienlijke maatschappelijke en economische schade. Universiteiten, bedrijven, zorginstellingen en overheden hebben regelmatig te maken met aanvallen op hun digitale systemen. Deze realiteit maakt duidelijk dat digitale veiligheid geen bijzaak meer is, maar een essentiële voorwaarde voor innovatie, verdienvermogen en vertrouwen in de samenleving. Het beschermen van de digitale infrastructuur en het versterken van innovatie in cyberveiligheid is van groot strategisch belang[2].

Tegelijkertijd voltrekt zich een nieuwe fase in de digitale transitie: de opkomst van kunstmatige intelligentie (AI). AI versnelt innovatie, maakt systemen slimmer en helpt dreigingen sneller te detecteren, maar creëert ook nieuwe kwetsbaarheden. Door AI kunnen aanvallen verder worden geautomatiseerd en autonoom uitgevoerd zonder menselijke interventie, maar ook gerichter en moeilijker te herkennen. Daarmee is AI zowel een sleutel tot een veiligere toekomst als een bron van nieuwe risico's.

De vraag is niet óf we willen digitaliseren, maar hoe we dat structureel en intrinsiek veilig doen.

Cybersecurity Technologies zijn daarom onderdeel van de Nationale Technologie Strategie (NTS). De Actieagenda Cybersecurity Technologies (AA CST) geeft uitvoering aan de vraag hoe we veilig kunnen digitaliseren. Zij richt de ambities van Nederland op dit vlak en geeft concrete innovatieroutes en samenwerkingsprogramma's om te komen tot een land dat in 2035 intrinsiek digitaal veilig is.

De urgentie: intrinsiek digitale veiligheid vraagt om technologische ontwikkeling en snellere valorisatie

De urgentie om actie te ondernemen is hoog, zowel op korte als op de lange termijn. Er tekent zich een aantal structurele problemen af:

- Cyberaanvallen nemen toe in frequentie én complexiteit: zowel statelijke als criminele actoren én door de staat gesponsorde criminele actoren zijn actief en maken gebruik van steeds geavanceerdere middelen en tactieken.
- De schade neemt toe: herstelkosten, verstoringen en financiële verliezen stijgen snel. Het aantal digitale producten, processen en diensten neemt toe, waardoor risico's zich steeds vaker door hele ketens en ecosystemen verspreiden.
- Huidige cybersecurity-oplossingen schieten tekort: vooral op ketenniveau en binnen het mkb zijn beveiligingsmaatregelen en technologieën nog onvoldoende ontwikkeld of toegepast om toekomstige dreigingen het hoofd te bieden.
- Nederland is te afhankelijk van buitenlandse leveranciers: de sterke afhankelijkheid van niet-Europese technologie tast onze strategische autonomie aan en beperkt de mogelijkheid om eigen normen en standaarden te bepalen[3].

Deze ontwikkeling vragen om een structurele versterking van de cybersecurity van Nederland. Dat betekent enerzijds het ontwikkelen en toepassen van nieuwe technologieën en anderzijds het vergroten van het bewustzijn in de samenleving over de risico's van digitale producten en diensten. In het publieke debat wordt, naast cybersecurity, momenteel veel gesproken over digitale weerbaarheid. Digitale weerbaarheid benadrukt het vermogen van een organisatie of individu om zich te beschermen tegen digitale risico's, snel te herstellen na een aanval en daarvan te leren om volgende aanvallen te voorkomen. Dit is noodzakelijk, maar niet voldoende. Digitale weerbaarheid vraagt daarbij om een fundamentele verandering in de manier waarop we technologie ontwerpen, gebruiken en vertrouwen. Dat vraagt ook om snellere valorisatie van kennis: het doelbewust creëren van waarde met en voor

1 CBS (2025). Cybersecuritymonitor 2024. IPSOS I&O (2025) Alert Online 2025.
2 P. Wennink (2025) De route naar toekomstige welvaart (p. 95).
3 Ministerie van Defensie (2025) Defensie Cyberstrategie 2025; Europese Commissie (2022). EU strategic dependencies and capacities: second stage of in-depth review.

belanghebbenden. De waarde die cybersecurity creëert, zowel maatschappelijk als financieel, is voor velen nog onvoldoende helder. Het is daarom urgent deze waarde helderder voor het voetlicht te brengen.

De transitie: van reactieve beveiliging naar intrinsiek veilige digitalisering

Cyberdreigingen brengen ook kansen met zich mee: ze versnellen de noodzaak om digitale producten en diensten veilig te maken[4]. In een intrinsiek veilige digitale samenleving worden producten, systemen, componenten en software secure-by-design ontwikkeld: veiligheid is vanaf het begin onderdeel van het ontwerp, niet een toevoeging achteraf[5].

Om dat te bereiken is een vernieuwing nodig die de fundamenten van onze digitale economie opnieuw vormgeeft. Het gaat om technologie die niet langer kwetsbaarheden achteraf repareert, maar veiligheid structureel inbouwt in de onderliggende digitale bouwstenen. Dat betreft zowel de manier waarop systemen worden ontworpen, ontwikkeld en beheerd als de technologieën die aan de basis daarvan staan.

Door deze bouwstenen opnieuw vorm te geven, van hardware tot software, van gegevensbescherming tot intelligente systemen, ontstaat de mogelijkheid om nieuwe generaties digitale producten en diensten te creëren die van nature veilig zijn. Deze transitie maakt het mogelijk om risico's structureel te verminderen en tegelijkertijd de kwaliteit, betrouwbaarheid en innovatiekracht van de digitale economie te versterken.

Deze aanpak leidt niet alleen tot meer veiligheid, maar ook tot nieuwe verdienmodellen en marktkansen. De focus verschuift van 'security producten' die achteraf kwetsbaarheden dichten, naar 'secure producten' die vanaf het begin veilig zijn ontworpen. Cybersecurity wordt zo niet langer een kostenpost, maar een katalysator voor innovatie, vertrouwen en groei.

De opgave: technologieontwikkeling, valorisatie, toepassing en randvoorwaarden

De ambitie Nederland intrinsiek digitaal veilig in 2035 bestaat uit drie samenhangende opgaven, waarin technologieontwikkeling en toepassing centraal staan. De eerste opgave is het versnellen van valorisatie en toepassing van deze technologie in sectoren en waardeketens. Innovatie krijgt pas waarde wanneer zij daadwerkelijk wordt gebruikt. Dat vraagt om het omzetten van kennis in waardevolle ideeën en vervolgens toepassingen.

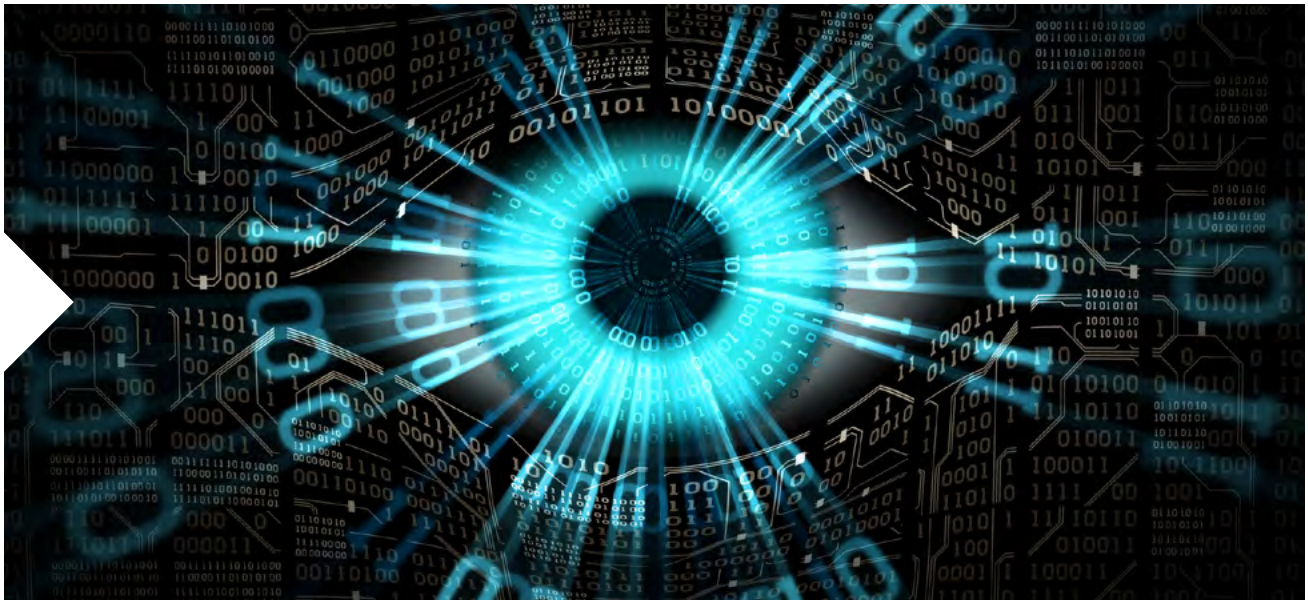
De Actieagenda richt zich daarom op het demonstreren, testen en opschalen van technologie in die domeinen waar de maatschappelijke en economische impact het grootst is. Het mkb krijgt hierbij specifieke aandacht.

De tweede opgave is het versnellen van de ontwikkeling van technologie die digitale veiligheid structureel versterkt. Het gaat hierbij niet om losse oplossingen, maar om een technologische basis die breed inzetbaar is en die de veiligheid van digitale producten, diensten en processen duurzaam verbetert.

De derde opgave is het versterken van de randvoorwaarden die nodig zijn om deze technologische transitie mogelijk te maken. Dat vraagt om voldoende talent, toegankelijke test- en ontwikkelomgevingen, passende ondersteuning en aansluiting op Europese programma's. Deze randvoorwaarden zijn ondersteunend aan het hoofddoel: de totstandkoming van een intrinsiek veilige digitale economie.

Met deze samenhangende opgave definieert de Actieagenda de inhoudelijke scope van het Nederlandse cybersecuritytechnologiebeleid: veiligheid realiseren door technologische ontwikkeling en toepassing in sectoren, ondersteund door doelgerichte randvoorwaarden.

4 Dialogic (2023). De economische kansen van de Nederlandse Cybersecuritysector.
5 De begrippen security-by-design en secure-by-design worden doorgaans door elkaar gebruikt. Het eerste begrip duidt de middelen en maatregelen aan die digitale veiligheid mogelijk maken of onderhouden. Deze Actieagenda gebruikt de tweede definitie omdat deze nadrukkelijk de toestand van beveiligd zijn beschrijft, passend bij de ambitie van de NTS CST (zie Hoofdstuk 3). Ook zonder de toevoeging van het woord 'cyber' betreft secure-by-design in deze Actieagenda altijd digitale veiligheid.



De scope: cybersecurity als fundament van een digitale economie

Cybersecuritytechnologieën zijn bedoeld om digitale risico's te verkleinen en de beschikbaarheid, integriteit en vertrouwelijkheid van systemen en gegevens te waarborgen. Ze zijn gericht op het voorkomen, detecteren en herstellen van cyberincidenten en op het vergroten van het vertrouwen in digitale processen. Wat een aanvaardbaar niveau is, is veelal de uitkomst van een risico-afweging[6]. Het speelveld is daarbij niet beperkt tot de IT-sector. Van smart cities, onderwijs en zorg, tot logistiek, energie, overheid en industrie — in alle domeinen neemt digitalisering sterk toe en is cybersecurity een essentiële randvoorwaarde.

Er moet op verschillende niveaus worden gewerkt aan cybersecurity:

- Als strategische kracht in sectoren en ketens, waarbij veilige bedrijven zich onderscheiden en hun concurrentiepositie versterken.
- Als technologie zoals veilige AI, quantumveilige cryptografie, secure hardware en secure-by-design systemen.
- Als maatschappelijk vermogen, waarbij burgers en professionals digitale risico's begrijpen en adequaat handelen.

Cybersecurity is dus geen ééndimensionale technologie voor één enkele sector, maar een samenspel van technologieën en methodieken die in meerdere sectoren toepasbaar zijn. De aanpak van cybersecurityvraagstukken vereist een multidisciplinaire invalshoek van zowel de verschillende onderzoeksdisciplines (alfa, bèta, gamma) en structurele samenwerking tussen onderzoek, onderwijs, industrie en overheid[7]. Deze Actieagenda zet zich ervoor in om de doorstroming van nieuwe technologie en methodieken naar sectoren aan te jagen en de 'cybersecure-by-design'-transitie te realiseren. Cybersecure-by-design is een proactieve benadering bij het bouwen van digitale producten en systemen, waarbij digitale veiligheid van het begin af aan wordt meegenomen bij het ontwerp, in plaats van achteraf eraan toegevoegd[8/9].

Inhoud

De Actieagenda schetst de ambitie waar Nederland in 2035 wil staan en de route om daar te komen, in de wetenschap dat de uitvoering adaptief moet blijven en ruimte vraagt voor bijsturing. De volgende hoofdstukken bouwen hiervoor verder aan het verhaal:

- Hoofdstuk 2 analyseert de sterkten en zwakten van het Nederlandse ecosysteem.
- Hoofdstuk 3 beschrijft de ambitie en opgaven die daaruit voortvloeien.
- Hoofdstukken 4 tot en met 7 werken deze uit in concrete innovatieprogramma's.
- Hoofdstuk 8 beschrijft de organisatie en governance van de Actieagenda.

6 NTS Cybersecurity Technologies.
7 Nationale Cyber Security Research Agenda IV (2025).
8 https://www.tno.nl/en/digital/cybersecurity/cyber-secure-systems-design/.
9 https://www.cisa.gov/securebydesign.

2. ANALYSE: DE KANSEN VAN CYBERSECURITY TECHNOLOGIES

Om de transitie naar een intrinsiek veilig Nederland in 2035 te realiseren, is inzicht nodig in de sterke en zwakke punten van het Nederlandse ecosysteem, de kansen die daaruit voortvloeien en de internationale positie die Nederland kan innemen. Dit hoofdstuk brengt de bouwstenen van die transitie in kaart: de kracht van het Nederlandse ecosysteem, de strategische kansen en uitdagingen, en de internationale positionering van Nederland als koploper in intrinsiek veilige digitalisering

2.1 KRACHT VAN HET NEDERLANDSE ECOSYSTEEM

Figuur 2.1 geeft een overzicht van de sterkten en zwakten van het Nederlandse ecosysteem. Het canvas laat zien wat de stand van zaken is per bouwsteen van het ecosysteem. Nederland heeft een goede digitale infrastructuur, een hoog innovatievermogen en een sterk ontwikkelde dienstensector rond cybersecurity. De ingrediënten voor een leidende positie zijn aanwezig en omvatten zowel technologische als organisatorische capaciteiten.

Ons land kent internationaal toonaangevende kennis-instellingen die wereldwijd vooroplopen op het gebied van cybersecurityonderzoek en innovatie. Er is een sterke kennisbasis op het vlak van softwareontwikkeling, AI, life cycle security, (post-quantum) cryptografie en cybersecure-by-design methodieken. De recente National Cybersecurity Research Agenda (NCSRA IV) biedt richting aan verdere kennisontwikkeling , waarop deze Actieagenda voortbouwt.

Daarnaast kent Nederland een dynamisch en veel-zijdig cybersecurity bedrijfsleven. Aan de ene kant is er een sterk groeiende groep dienstverleners (adviesbureaus, integrators en security serviceproviders) die organisaties ondersteunen bij risicomanagement, detectie, incidentrespons en compliance. Aan de andere kant ontwikkelt een innovatieve laag van technologieleveranciers geavanceerde cybersecurity-oplossingen, variërend van cryptografische technologie en AI-gedreven detectiesystemen tot beveiligde cloud- en netwerkarchitecturen .

Bovendien bezit Nederland een brede industrie die digitale producten en systemen ontwikkelt, van hightech machines, medische apparatuur en voertuigen tot industriële automatisering. Deze industrie valt onder EU-wetgeving van de komende Cyber Resilience Act (CRA) en moet daarmee aan hoge cybersecurity-eisen voldoen. Bedrijven en toeleveranciers in de maak- en technologiesector worden verplicht om digitale veiligheid structureel in te bouwen in hun ontwerp- en productieprocessen.

De combinatie van dienstverleners, technologiebedrijven en industriële ontwikkelaars vormt een krachtige voedingsbodem voor innovatie en kennisverspreiding. Nederland is daardoor een ideale proeftuin voor de ontwikkeling van secure-by-design oplossingen met brede maatschappelijke en economische impact.

Tenslotte is er een goede publiek-private samenwerking op het gebied van cybersecurity. Nederland is ook goed verbonden met Europese programma's, waardoor kennis en middelen worden gedeeld en Nederlandse expertise internationaal tot waarde komt.

2.2 KANSEN EN UITDAGINGEN

Nederland heeft de juiste ingrediënten in huis om de transitie naar intrinsiek veilige digitale producten en systemen te realiseren. Op basis van Figuur 2.1 komen de volgende drie strategische kansen en bijbehorende uitdagingen naar voren.

10 Dit canvas is ontwikkeld door adviesbureau Wederic.
11 Europese Unie (2024), Digital Decade 2024, https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports.
12 NCSRA IV (2025), Science for a resilient digital ecosystem, juli.
13 Dialogic (2023). De economische kansen van de Nederlandse Cybersecuritysector.
14 https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

TALENT
- Tekort aan talent in bepaalde competenties als linked data en semantiek
- Remote workforce is een kans maar kan ook en risico zijn
- Buitenlandse partijen nemen Nederlandse startups over
- Er zijn verschillende overheidsprogramma's gericht op human capital

NETWERKEN
- Sterk ontwikkeld veld van spelers
- Samenwerking is echter vaak transactioneel niet gericht op transformatie
- Netwerkvorming staat in de kinderschoenen; begin van netwerkvorming rondom EDIHs
- Bedrijfsleven is sterk afhankelijk van buitenlandse technologische oplossingen

INFRASTRUCTUUR
- Onderzoeksinfrastructuur is versnipperd
- Nederland participeert in Europese programma's
- Fysieke infrastructuur voldoet voor bestaande oplossingen maar niet voor de ontwikkeling van AI gedreven modellen
- Europese cloud ontbreekt
- Geen gezamenlijke labs voor risicobeoordeling en schaalvoordeel
- Geen gedeelde infrastructuur om aanvallen en kwetsbaarheden te kunnen delen

WET-EN REGELGEVING
- Europese regelgeving legt verantwoordelijkheid bij producent (met name CRA)
- Eind 2027 moeten producten secure by design zijn
- Regelgeving niet altijd goed afgestemd

DIENSTVERLENERS
- Goed ontwikkelde dienstensector, maar niet exportgericht en niet schaalbaar

LEIDERSCHAP
- Enkele grote bedrijven ontwikkelen toepassingen
- Rondom datadelen is dat echter zeer beperkt; ketendenken is zwak ontwikkeld

CULTUUR
- Meer gericht op incrementele verbetering
- Bewustzijn over risico's neemt toe

FINANCIERING
- Private financiering van startups en scaleups blijft achter
- Publieke innovatie onvoldoende in omvang en vooral gericht op onderzoek, minder op innovatie

KENNIS(OVERDRACHT)
- Sterke kennisbasis in cryptografie, softwareontwikkeling, AI, Postquantum en toepassing in sectoren. Hier ligt een kans
- Academische kennis in lagere TRLs
- Weinig private R&D of kennis wordt niet gedeeld
- Kennisbasis MKB beperkt
- Aansluiting onderwijs op arbeidsmarkt kan beter

MARKTVRAAG
- Cybersecuritysector groeit hard, kans voor Nederland om verdienvermogen te vergroten
- Vraag ligt vooral op bedrijfsniveau en niet op ketenniveau
- Vraag naar beveiliging van producten en diensten blijft achter
- Weinig vraag naar innovatie en security by design

Figuur 2.1 *Overzicht van sterkten en zwakten in het Nederlandse cybersecurity ecosysteem*[15].

Kans 1: Toepassing van technologie in ketens, sectoren en regio's

Nieuwe technologie heeft pas impact wanneer zij wordt toegepast in de praktijk. Die toepassing is geen individuele opgave van afzonderlijke organisaties: digitale veiligheid ontstaat pas wanneer sectoren en waardeketens als geheel nieuwe technologie opnemen. In veel domeinen blijft toepassing versnipperd en worden innovaties onvoldoende meegenomen in ontwerp-, productie- en beheersprocessen.

De kans ligt in het versnellen van toepassing door sectorale en ketenbrede aanpakken, waarin organisaties gezamenlijk werken aan veilige producten, processen en diensten. Met name in domeinen met grote maatschappelijke en economische betekenis, zoals industrie, energie, zorg, mobiliteit en overheid en telecom, kan grootschalige toepassing structurele verbeteringen in kwaliteit en veiligheid realiseren.

15 Dit overzicht is gebaseerd op KIA Digitalisering, Resultaten Fase 1, waarin alle bestaande rapporten en inzichten zijn samengenomen. Dit is vervolgens gevalideerd in workshops met stakeholders op 26 mei, 13 juni en 19 juni 2025.

Kans 2: Versnellen van technologische ontwikkeling

De tweede kans ligt in het versnellen van de ontwikkeling van nieuwe cybersecuritytechnologieën, omdat het bestaande innovatietempo achterblijft bij de groeiende dreigingscomplexiteit. Nederland beschikt over sterke kennisposities, maar deze moeten sneller en doelgerichter worden doorontwikkeld om relevant te blijven in een digitale omgeving waarin aanvallen autonomer en complexer worden.

Nieuwe technologie is essentieel waar huidige oplossingen tekortschieten. Dit betreft met name quantumveilige cryptografie, veilige hardware-architecturen, verifieerbare softwareketens en AI-gedreven beveiliging. De ontwikkeling hiervan vraagt om meer samenhang en massa in de innovatieketen

Kans 3: Versterking van randvoorwaarden en infrastructuur

De derde kans ligt in het versterken van de randvoorwaarden die nodig zijn voor technologische ontwikkeling en toepassing. Nieuwe Europese wetgeving, waaronder de CRA, Network and Information Security 2 (NIS2)[16] en de AI act[17], vergroot de vraag naar veilige producten processen en diensten, maar er is een tekort aan talent, een versnipperd test- en validatielandschap en onvoldoende gerichte innovatie-instrumenten voor complexe cybervraagstukken.

2.3 INTERNATIONALE POSITIONERING

Momenteel komen de meeste securityproducten van niet-Europese leveranciers[18]. In de maakindustrie ligt dit anders: Nederland is internationaal sterk in het bouwen van complexe machines en digitale infrastructuren, wat kansen biedt voor secure-by-design innovaties. De kleine Nederlandse markt maakt internationale samenwerking en positionering cruciaal voor schaal, afzetvolume en strategische autonomie. Europese programma's en strategische partnerschappen zijn daarvoor essentieel.

2.4 CONCLUSIE: KANSEN VOOR DE TOEKOMST

Nederland beschikt over een sterke basis, maar benut die nog onvoldoende. De drie beschreven kansen vormen de inhoudelijke richting voor de komende jaren:

1. Het versterken van samenwerking in ketens, sectoren en ecosystemen.
2. De ontwikkeling van technologie en methodieken.
3. Invulling van de ontbrekende randvoorwaarden en infrastructuur.

Deze analyse vormt de basis voor de ambitie en opgaven die in Hoofdstuk 3 worden uitgewerkt.

16 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.
17 https://artificialintelligenceact.eu/.
18 Europese Commissie (2022). EU strategic dependencies and capacities: second stage of in-depth review.

3. AMBITIE

Om de transitie naar een intrinsiek cyberveilige wereld vorm te geven, staat de Nederlandse samenleving voor een aantal opgaven. Een opgave om te komen tot sectorale en regionale transitie vraagt om het ontwikkelen van nieuwe technologie en methoden. Daarnaast dienen ook andere randvoorwaarden ingevuld te worden en is er noodzaak tot de ontwikkeling van nieuwe infrastructuur.

3.1 AMBITIE UIT DE NTS CST

De ambitie van deze Actieagenda sluit aan bij de Nationale Technologie Strategie en geeft richting aan de technologische ontwikkeling die nodig is om een digitale economie te realiseren waarin veiligheid structureel is ingebouwd. Deze ambitie vormt de basis voor de opgaven en innovatieprogramma's die in de volgende hoofdstukken worden uitgewerkt. De NTS CST formuleert de volgende ambitie[19]:

> *'In 2035 heeft Nederland een concurrerende cybersecuritymarkt met voldoende talent ontwikkeld, en middels een multidisciplinaire aanpak een internationaal leidende positie in innovatieve cybersecuritytechnologieën verworven.*
>
> *Deze technologieën leveren een essentiële bijdrage aan de beveiliging van infrastructuren en IT- en OT-netwerken, de transitie naar post-quantum cryptografie en meer automatische detectie en verdediging door inzet van AI.*
>
> *Door onderzoek en meer publiek-private samenwerking, op nationaal en internationaal niveau, is de kennispositie versterkt en is kennisvalorisatie toegenomen. Hiermee is cybersecurity een geïntegreerd onderdeel van de Nederlandse sectoren door het toepassen van secure-by-design, secure-by-default, cybersecurity in de toeleveringsketen van organisaties en bedrijfsketens. Dit alles draagt bij aan een digitaal veilig, weerbaar, autonoom en welvarend Nederland'.*

Samengevat:

'Nederland is in 2035 intrinsiek digitaal veilig'.

De economische opgave richt zich op het beschermen en versterken van het Nederlandse verdienvermogen door schade door cyberaanvallen structureel te beperken en door waardecreatie mogelijk te maken door nieuwe cyberveilige producten en diensten op de markt te brengen. De maatschappelijke opgave richt zich op het verkleinen van afhankelijkheden van niet-Europese beveiligingstechnologie, door op kritieke onderdelen eigen, intrinsiek veilige digitale producten en diensten te ontwikkelen.

3.2 SECTORALE EN REGIONALE TRANSITIEOPGAVE

De transitie naar intrinsieke digitale veiligheid begint in de praktijk: binnen sectoren, ketens en regionale ecosystemen. De ambitie is om samenwerkingsverbanden te vormen waarin bedrijven, kennisinstellingen en overheden gezamenlijk werken aan technologieontwikkeling rondom concrete cybersecurityvraagstukken. Alleen door in sectoren en ketens te handelen, kan digitale veiligheid op grote schaal worden bereikt.

In de eerste lijn ligt de focus op het benutten van nieuwe technologie en bestaande kennis door het versterken van bedrijfsoverstijgende samenwerking. Het mkb speelt hierin een belangrijke rol. Veel kleinere bedrijven beschikken nog niet over de kennis of middelen om hun digitale veiligheid structureel te borgen en hebben ondersteuning nodig om veilig(er) te digitaliseren en te voldoen aan toenemende wet- en regelgeving.

In de tweede lijn staat de ontwikkeling van intrinsiek veilige digitale producten en systemen centraal. Hierbij ontstaat een duidelijke supply chain-uitdaging: veel producten bestaan uitonderdelen die door tientallen leveranciers worden geleverd. Als één leverancier onvoldoende beveiligd is, kan dat gevolgen hebben voor het gehele eindproduct en zelfs voor complete sectoren. Daarom is het noodzakelijk dat bedrijven in ketens gezamenlijk optreden om risico's te delen, informatie uitwisselen en afspraken maken over het toepassen van veilige ontwikkel en beheerprocessen.

Grote maakbedrijven spelen hierin een belangrijke rol, omdat hun producten in snel tempo digitale componenten en connectiviteit toevoegen. Ze zijn geen nieuwe toetreder op de cybersecurity-markt maar een nieuw toetreder op de markt van digitaal verbonden producten. Daardoor verschuiven de risico's van individuele producenten en systemen naar complete ketens. De grootste opgave is daarom niet

19 NTS Cybersecurity Technologiest.

het beveiligen van afzonderlijke bedrijven, maar het veilig maken van hele waardeketens waarin bedrijven van elkaar afhankelijk zijn.

Kennisuitwisseling en samenwerking zijn daarbij essentieel. Via initiatieven zoals Europese Digitale Innovatie Hubs (EDIHs), Regionale Ontwikkelingsmaatschappijen (ROM's) en publiek-private consortia kunnen sectoren en regio's leren van elkaar, innovaties sneller toepassen en gezamenlijk nieuwe standaarden ontwikkelen. Start-ups en scale-ups versterken deze beweging door nieuwe technologieën en marktmodellen te introduceren.

De deelambitie: In 2035 passen Nederlandse sectoren en waardeketens veilige technologie breed toe in hun processen en producten. Nederland is internationaal herkenbaar als een land waarin veilige technologie daadwerkelijk wordt gebruikt en waarin intrinsieke veiligheid een onderscheidende factor is in kwaliteit, innovatie en concurrentievermogen.

3.3 TECHNOLOGIE- EN METHODOLOGIE-OPGAVE

Technologische en methodologische opgave vormt de kern van de transitie naar intrinsiek veilige digitalisering. Waar digitale veiligheid nu vaak nog een toevoeging is, moet zij een structureel onderdeel worden van de manier waarop Nederland technologie ontwerpt, bouwt, test en beheert. Dat vraagt om nieuwe kennis, methodieken en technologieën die veiligheid herhaalbaar, aantoonbaar en schaalbaar maken.

Zes thema's geven richting aan deze opgave en vormen samen het technologisch kompas voor de periode 2025–2035:

1. **Secure hardware & embedded systems:** ontwikkeling van veilige, verifieerbare chips, sensoren en controllers als fysieke basis van betrouwbare software en data.
2. **AI & Security:** veilig en uitlegbaar gebruik van AI voor detectie, verdediging en herstel, én bescherming van AI-systemen zelf.
3. **Infrastructuur security:** veiligheid en veerkracht in 6G-, cloud-, edge- en quantum-netwerken als ruggengraat van de digitale economie.
4. **Quantum-veilige cryptografie:** ontwikkeling van Europese cryptografische standaarden, quantum-veilige algoritmen en privacy-bevorderende technologieën.
5. **Secure engineering & productontwikkeling:** integratie van secure-by-design, DevSecOps, formele verificatie en CRA-conforme ontwikkelpraktijken.
6. **System & supply chain assurance:** model-based security, digital twins en assurance-platforms die veiligheid en vertrouwen aantoonbaar borgen op ketenniveau.

De deelambitie: In 2035 beschikt Nederland over een sterke en internationaal erkende basis aan technologie en methodologie voor intrinsiek veilige digitalisering, die breed kan worden toegepast in sectoren en waardeketens.

3.4 RANDVOORWAARDEN EN INFRASTRUCTUUR-OPGAVE

Om technologieontwikkeling en toepassing te kunnen versnellen, zijn sterke en toekomstbestendige randvoorwaarden nodig. De eerste voorwaarde is voldoende en goed opgeleid talent. Dat vraagt om structurele investeringen in onderwijs, bijscholing en praktijkgerichte leeromgevingen, in nauwe samenwerking tussen overheid, onderwijsinstellingen en bedrijfsleven. Daarnaast is een moderne infrastructuur noodzakelijk. Bedrijven moeten toegang hebben tot test-, validatie- en certificeringsfaciliteiten waarin nieuwe technologieën kunnen worden ontwikkeld, getest en gevalideerd volgens Europese standaarden. Gedeelde experimenteerplekken, digitale testomgevingen en gezamenlijke dataverzamelingen versnellen innovatie en toepassing.

Tenslotte houdt het ecosysteem rondom cybersecurity niet op bij de landsgrenzen. Verbinding van het Nederlandse ecosysteem met relevante Europese programma's, investeringslijnen en markten is cruciaal voor het bereiken van schaal, het verbeteren van kennisdeling, hogere afzetvolumes door export en het vergroten van strategische autonomie. Deze verbindingen kunnen helpen de ambitie op het gebied van randvoorwaarden en infrastructuur te realiseren. Daardoor ontstaan ook verbindingen tussen organisaties die ertoe kunnen leiden dat het Nederlandse bedrijfsleven ontwikkelde diensten en producten internationaal kunnen vermarkten.

De deelambitie: In 2035 beschikt Nederland over een robuuste kennis- en innovatie-infrastructuur die technologische ontwikkeling en toepassing van intrinsiek veilige digitalisering mogelijk maakt. Talent, faciliteiten en internationale verbinding zijn structureel georganiseerd en sluiten aan op de technologische behoefte.

4. KADER STRATEGISCHE INNOVATIEPROGRAMMA'S

De Actieagenda Cybersecurity Technologies richt zich op drie samenhangende innovatieprogramma's die de kern vormen van de transitie naar intrinsiek veilige digitalisering in Nederland. Deze programma's versterken elkaar en vormen gezamenlijk de route naar een veilig en toekomstbestendig digitaal ecosysteem.

4.1 VAN VERBINDING NAAR GROEI NAAR CONSOLIDATIE

Dit cybersecuritytechnologieveld is volop in ontwikkeling, maar nog niet volwassen. Er zijn veel waardevolle initiatieven (zie paragraaf 4.2), maar deze zijn vaak nog versnipperd en missen voldoende samenhang. Hierdoor blijft het gezamenlijke innovatievermogen onderbenut. Deze Actieagenda richt zich daarom naast technologieontwikkeling ook op verbinden en afstemmen.
Het doel is om bestaande activiteiten te versterken en de witte vlekken te vullen en een gezamenlijk innovatie ecosysteem te bouwen dat de ambitie 'Nederland is in 2035 intrinsiek digitaal veilig' ondersteunt.
De Actieagenda doorloopt daartoe drie fasen:

1. **Opbouwfase.** Deze fase (jaar 1 – 2) zet sterk in op het verbinden van spelers in het ecosysteem en op het leggen van het technologiefundament onder cybersecurity-by-design. Het eerste is nodig om de versnippering van het ecosysteem te verminderen. De nadruk ligt op gezamenlijke analyses, afstemming van lopende programma's en identificatie van witte vlekken. Het tweede gaat om het ontwikkelen van technologie waarvan nu al duidelijk is dat deze nodig is. Er vormen zich coalities gericht op ontwikkeling van deze technologieën die een kennisfundament leggen om in de latere fasen op door te bouwen.
2. **Groeifase.** In deze periode (jaar 3 – 6) richt de Actieagenda zich op het stimuleren van nieuwe publiek-private consortia, nieuwe technologie- en methodiek innovaties en op het inrichten en versterken van randvoorwaarden en infrastructuren waar het ecosysteem te kort schiet. Naast het doorzetten van de technologische ontwikkeling uit de Opbouwfase, worden ook de in die fase ontdekte witte vlekken ingevuld. Doordat het ecosysteem zich dan gevormd heeft, kan snel massa worden bereikt in de technologieontwikkeling.
3. **Consolidatiefase.** De laatste fase (na jaar 6) richt zich op adoptie en opschaling van ontwikkelde kennis en innovaties in de praktijk. Sectoren en regio's passen de resultaten structureel toe en maken ze onderdeel van hun normale bedrijfsvoering.

Aan het eind van de verbindingsfase is duidelijk waar de grootste lacunes liggen, waarna gerichte investeringen en programmatische keuzes gemaakt kunnen worden. Het merendeel van de nieuwe activiteiten zal daarom gedurende de looptijd ontstaan. Het tempo en de omvang hiervan hangen van de gezamenlijke inzet van publieke- en private middelen in de komende jaren.

4.2 PROGRAMMASTRUCTUUR

De Actieagenda Cybersecurity Technologies richt zich op de coördinatie van drie onderling versterkende Innovatieprogramma's, die direct aansluiten op de drie opgaven uit Hoofdstuk 3 (zie Figuur 4.1):

1. **Sectorale & regionale transities:**
   Praktijkgerichte publiek-private consortia die cybersecurity in ketens, ecosystemen en sectoren structureel versterken, technologische innovatie aanjagen en toepassing versnellen. Deze consortia pakken rechtstreeks de bestaande lacunes in de markt en in de voortgang van de transitie in cybersecurity aan, door daarvoor technologische oplossingen te verzinnen.

   Bedrijven hebben vaak onvoldoende individuele prikkels om te investeren in collectieve cyberveiligheid, terwijl de baten publiek of ketenbreed zijn. Tegelijk verloopt de overgang naar intrinsiek veilige digitalisering te traag door een gebrek aan samenwerkingsstructuren, leerprocessen en gedeelde richting. Dit geldt met name voor het mkb dat in sectorale en regionale ecosystemen een belangrijke rol vervult, maar vaak achterblijft op het gebied van cybersecurity.

   Door consortia te vormen bouwen organisaties handelingsvermogen op en ontstaat de schaal om de technologische transitie te versnellen en verankeren. Bij de keuze voor sectoren zoekt

deze Actieagenda in eerste instantie zoveel mogelijk aansluiting bij de prioriteiten uit de Industriebrief[20].

2. **Technologie & Methodologie:**
   Het Innovatieprogramma Technologie & Methodologie vormt het hart van deze Actieagenda. Het richt zich op het ontwikkelen en verbeteren van technologie die digitale veiligheid structureel versterkt. Het programma stimuleert onderzoek, experimentatie en opschaling van technologische en methodologische bouwstenen die veiligheid vanaf het ontwerp borgen en breed toepasbaar zijn.

   Het programma werkt 'whole of TRL', dus van fundamenteel onderzoek tot marktintrede, met bijzonder aandacht voor de 'valleys of death'. Dat betekent ruimte voor nieuwsgierigheid gedreven onderzoek op lage Technology Readiness Levels (TRLs) en voor markgerichte keuzen op hogere TRLs. Naast producten en diensten is er ook aandacht voor innovatie in productieprocessen en -middelen.

   Dit programma vormt de bron waaruit nieuwe veilige producten, diensten en processen kunnen voortkomen. Het ondersteunt de andere programma's door technologie en methodologie beschikbaar te maken voor toepassing en opschaling.

3. **Randvoorwaarden & infrastructuur:**
   Dit programma richt zich op de condities die nodig zijn om de transitie mogelijk te maken. Innovaties stranden vaak op een tekort aan talent, een versnipperde infrastructuur, niet passende innovatie-instrumenten en onduidelijke of belemmerende regelgeving.
   Zonder structurele randvoorwaarden lopen zelfs goede initiatieven vast. Technologische innovatie landt niet zonder sociale innovatie. Daarom richt dit programma zich op verbetering van condities rondom talent, testlabs, financiering, regelgeving en innovatie instrumenten.

Onder elk van deze Innovatieprogramma's verbindt de Actieagenda publiek-private samenwerkingsverbanden (uitgewerkt in hoofdstuk 5 t/m 7). Nieuwe consortia kunnen worden toegevoegd Innovatieprogramma's op basis van opkomende behoeften en kansen.

Op basis daarvan kunnen nieuwe producten en diensten worden ontwikkeld die internationaal vermarkt kunnen worden. De Actieagenda stimuleert ons verdienvermogen doordat:

- producten uit de maakindustrie vaker als secure products worden verkocht.
- nieuwe bedrijvigheid ontstaat rond security products (technologieën die secure-by-design, life-cycle security en autonome cybersecurity mogelijk maken) secure-by-design.

SECTORALE & REGIONALE TRANSITIES	**BHoC**	**FLECS**	**Cyberveilige Energie transitie**	**PCSI**	**...**	**...**
TECHNOLOGIE & METHODOLOGIE	**Security by design**	**PQC**	**Autonome Cybersecurity Systemen**	**...**	**...**	**...**
RANDVOORWAARDEN & INFRASTRUCTUUR	**Standaarden**	**Talent**	**Start-ups**	**Experimenteer-ruimtes**	**...**	**...**

Figuur 4.1 *De drie innovatieprogramma's van de Actieagenda Cybersecurity Technologies*

20 Minister van Economische Zaken (2025), Brief aan de Tweede Kamer betreffende Industriebeleid met focus, 17 oktober.

4.3 TRANSITIE-AANPAK

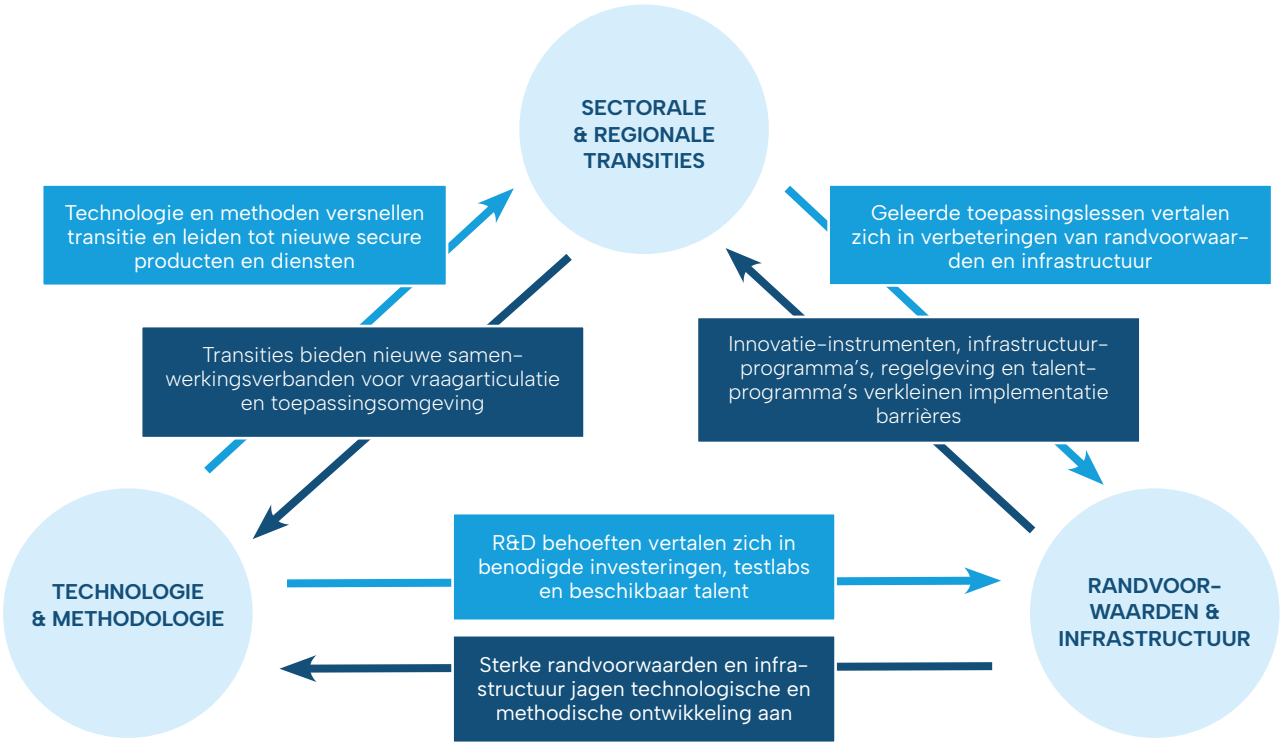
De transitie-aanpak om de ambitie te realiseren is gebaseerd op het idee dat de drie innovatieprogramma's elkaar continu versterken (Figuur 4.2).

De Actieagenda zoekt actief naar het verbinden van de drie innovatieprogramma's zodat zij elkaar zoveel mogelijk versterken. Essentieel voor het slagen van de Actieagenda is dat actief wordt gezocht naar overlap, complementariteit en synergie. Zo ontstaat een dynamische cyclus waarin versnippering wordt teruggedrongen, valorisatie toeneemt en innovatie en impact worden vergroot. Dit alles versterkt het lerend vermogen van het ecosysteem. De driehoek in Figuur 4.2 is daarbij de leidraad om te komen tot een permanente, duurzaam lerende en sturende structuur. De organisatie van de Actieagenda dient deze integrale transitie-aanpak te ondersteunen.

4.4 HUMAN CAPITAL, VALORISATIE, INTERNATIONALISERING

Om dit samenspel werkend te krijgen dient ook een aantal andere randvoorwaarden te zijn ingevuld. De beschikbaarheid van voldoende talent en een groter maatschappelijk bewustzijn rondom cybersecurity 'zijn voorbeelden van cruciale randvoorwaarden. De agenda zoekt daarom verbinding met Human Capital Agenda Digitalisering. Een tweede voorwaarde is het aanjagen van valorisatie en marktcreatie, met name in het mkb, waar verbetering van valorisatie nog mogelijk is. Brabant House of Cyber (zie Tabel 5.1) is een activiteit die daaraan bijdraagt. De Actieagenda zet zich ervoor in dit initiatief nationaal op te schalen.

Ten derde is internationalisering essentieel. De Nederlandse markt is beperkt van omvang en veel cybersecurity-oplossingen worden in samenwerking met buitenlandse partijen ontwikkeld. Door slim gebruik te maken van elders opgedane kennis en beschikbare middelen kan het effect van de inzet van Nederlandse middelen sterk worden vergroot. Verbinding van de NTS aan de Europese strategieën rondom cybersecurity is daarom noodzakelijk. De agenda sluit dan ook aan bij en bouwt voort op internationale samenwerkingsverbanden, marktbewerking, onderzoeksprojecten en kaders. Kennis uit het buitenland wordt in Nederland toegepast en Nederlandse oplossingen worden ook over de grenzen verkocht.



Figuur 4.2 *Samenhang tussen programma's*

4.5 AANSLUITING OP BESTAANDE INSTRUMENTEN: REGIONAAL, NATIONAAL, INTERNATIONAAL

Binnen het werkveld van de Actieagenda zijn al veel bestaande activiteiten en ook bestaande financieringsinstrumenten. Het doel van de Actieagenda is niet om deze te vervangen maar vooral om hierop voort te bouwen, te verbeteren waar nodig en om de inzet beter op elkaar te laten aansluiten. Waar het lopende activiteiten betreft, gaat het bijvoorbeeld om kennisontwikkeling vanuit NWO-programma's, toegepast onderzoek bij TNO, EU-gefinancierde programma's (gestimuleerd door NCC-NL[21]) startup-activiteiten, overheidsprogramma's (o.a. bij de innovatieonderdelen van Defensie[22]) en bedrijfsmatige R&D. De kennis die daarbij is en wordt opgedaan vormt een waardevolle basis voor deze Actieagenda en de Actieagenda heeft onder meer tot doel te coördineren dat op deze bestaande kennisbasis wordt voortgebouwd.

Ten aanzien van instrumenten geldt dat de Actieagenda voor de eerste fase (zie Hoofdstuk 4.1) gefinancierd kan worden uit bestaand instrumentarium (Tabel 4.2). Dit instrumentarium is te vinden op regionaal, nationaal en internationaal niveau. Op regionaal niveau zijn bijvoorbeeld middelen van de ROM's van belang. De ROM's hebben in opdracht van het ministerie van Economische Zaken gewerkt aan Regionale Versterkingplannen NTS[23]. Aansluiting bij Europees Consortium voor digitale infrastructuur (EDIC)- en EDIH-initiatieven op regionaal niveau geeft eveneens mogelijkheden om de Actieagenda te realiseren. Op nationaal niveau gaat het om middelen bij Topsectoren, NWO, RVO en TNO. Maar ook de Human Capital Agenda ICT, InvestNL, het Cybersecurity Innovation Fund (CIF) en Techleap hebben middelen beschikbaar of bieden hulp bij toegang tot middelen. Ook zijn gezamenlijke projecten en programma's met andere departementen dan het ministerie van Economische Zaken mogelijk. Cybersecurityvraagstukken doen zich immers ook voor rondom onder andere gezondheid, logistiek of defensie.

Op internationaal niveau zijn bijvoorbeeld Europese fondsen als, Horizon Digital, Digital Europe Program (DEP) en European Defence Fund (EDF) belangrijk, evenals middelen van de NATO en vanuit nationale budgetten van Europese lidstaten in het kader van Important Project of Common European Interest (IPCEIs). Het internationale niveau is in het bijzonder van belang omdat de Nederlandse markt beperkt van omvang is en omdat veel technologische ontwikkeling ook in andere landen plaatsvindt. Door slim gebruik te maken van de daar opgedane kennis en middelen, kan het effect van de inzet van Nederlandse middelen sterk worden vergroot. Verbinding van de NTS met het Europese innovatie- en industriebeleid is daarom noodzakelijk om ook deze financieringsmogelijkheden te benutten.

Voor het Nederlandse instrumentarium geldt dat de Actieagenda richting kan geven aan de investeringen in cybersecurity technologieën. Voor al het instrumentarium geldt dat de Actieagenda een belangrijke rol kan spelen bij het afstemmen, coördineren en synergie creëren tussen de instrumenten en tussen de verschillende regionale, nationale en internationale niveaus. Verbinding van de NTS aan de Europese strategieën rondom cybersecurity is daarom noodzakelijk.

ACTIVITEITEN/ MIDDELEN	INSTRUMENTARIUM SECTORALE & REGIONALE TRANSITIES	INSTRUMENTARIUM TECHNOLOGIE & METHODOLOGIE	INSTRUMENTARIUM RANDVOORWAARDEN & INFRASTRUCTUUR
BESTAAND/BESTAAND	35	70	15
NIEUW/BESTAAND	205	30	35
NIEUW/NIEUW	-	100	70
PRIVAAT	245	175	120
TOTAAL	**485**	**375**	**240**

***Tabel 4.2** Overzicht projectie instrumentarium (mln. €; 2026-2035)*

21 https://english.rvo.nl/topics/ncc-nl.
22 https://www.defensie.nl/onderwerpen/innovatie/downloads/beleidsnota-s/2025/04/04/defensie-strategie-voor-industrie-en-innovatie-2025-2029.
23 https://www.rom-nederland.nl/trots-op-het-regionaal-versterkingsplan-nts-samen-verder-bouwen-aan-sterke-waardeketens/.

4.6 KPI'S

De KPI's richten zich op de realisatie van de drie Innovatieprogramma's. De bijbehorende KPI's zijn in 2035:

Innovatieprogramma Sectorale & Regionale Transities:

- Voldoen 100% van de nieuwe digitale producten en processen van Nederlandse producenten aantoonbaar aan secure-by-design-principes.
- Is de Nederlandse industrie en vitale infrastructuur post-quantum beveiligd.
- Zijn ten minste 10 sectorale of regionale cybersecurity innovatie consortia actief die marktfalen en transitiefalen structureel hebben doorbroken.

Innovatieprogramma Technologie & Methodologie:

- Zijn inzichten en breed bruikbare componenten, technologie en methodieken van eigen bodem beschikbaar voor alle organisaties, voor zover private partijen daar geen intellectuele eigendomsrechten op hebben. 80% van de bedrijven maakt gebruik daarvan.
- Zit Nederland in de wereldwijde top 5 waar het adoptie van secure-by-design technologie en methodieken betreft.
- Is er een jaarlijks overzicht van de nieuwste beschikbaar gekomen technieken dat toegankelijk is voor iedereen. 80% van de bedrijven gebruikt dat overzicht.

Randvoorwaarden & Infrastructuur:

- Behoort de kennisinfrastructuur op cybersecuritygebied tot de top 5 in de wereld.
- Heeft Nederland de experimentele infrastructuur passend bij de technologische en methodologische innovatie op cybersecurity.
- Zijn aanbod van en vraag naar cybersecuritytalent met elkaar in evenwicht.

4.7 VERBINDING MET ANDERE ACTIEAGENDA'S

Elk technologiedomein digitaliseert in snel toenemende mate. De Actieagenda Cybersecurity Technologies kent daarom logische verbindingen met de technologieontwikkeling in andere Actieagenda's (zie Tabel 4.3 voor een overzicht). Zo zullen producten en diensten die voortkomen uit die technologieontwikkeling en een digitale component hebben, per 2027 moeten voldoen aan EU- regelgeving inzake digitale productveiligheid. Ook zullen de ecosystemen waarin die technologieontwikkeling plaatsvindt hun ketenweerbaarheid op orde moeten hebben om verstoringen in ontwerp, productie en vermarkting te voorkomen. Tot slot geldt voor elke speler in dat ecosysteem dat het de eigen digitale weerbaarheid op orde heeft, zodat ICT- en productiesystemen niet verstoord worden.

Voor de Actieagenda's Quantum, AI & Data en Semicon is de Actieagenda CST relevant op productniveau. Waar het technologieontwikkeling betreft die geen digitale componenten heeft, zal het ecosysteem waarin die ontwikkeling plaatsvindt wel digitaal veilig moeten zijn en is de Actieagenda CST dus ook relevant voor de andere Actieagenda's. Hiermee is intrinsieke digitale veiligheid voorwaardelijk voor het succes van alle Actieagenda's. Daarom kijken we uit naar brede en stevige aansluiting met die Actieagenda's.

ACTIEAGENDA	CROSSOVER
OPTICAL SYSTEMS AND INTEGRATED PHOTONICS	Producten, productie- en processystemen voor onderzoek, ontwikkeling, productie en vermarkting intrinsiek digitaal veilig maken door nieuwe generaties 'security products' en 'secure products'.
QUANTUM TECHNOLOGIES	Versnelling van post-quantum cryptografie (PQC) en integratie van quantumveilige toepassingen in (vitale) sectoren zijn crossovers met de quantum agenda.
PROCESS TECHNOLOGY, INCLUDING PROCESS INTENSIFICATION	Producten, productie- en processystemen voor onderzoek, ontwikkeling, productie en vermarkting intrinsiek digitaal veilig maken door nieuwe generaties 'security products' en 'secure products'.
BIOMOLECULAR AND CELL TECHNOLOGIES	Producten, productie- en processystemen voor onderzoek, ontwikkeling, productie en vermarkting intrinsiek digitaal veilig maken door nieuwe generaties 'security products' en 'secure products'.
IMAGING TECHNOLOGIES	Producten, Productie- en processystemen voor onderzoek, ontwikkeling, productie en vermarkting intrinsiek digitaal veilig maken door nieuwe generaties 'security products' en 'secure products'.
MECHATRONICS AND OPTOMECHATRONICS	Gebruik van robots vereist toegang tot veel data van hoge kwaliteit. Daarnaast genereert gebruik van robotica ook data die persoonlijk of commercieel gevoelig kan zijn. Cybersecurity is daarom relevant ter ondersteuning van producten ontwikkeld in het innovatieprogramma Robotica.
ENERGY MATERIALS	Producten, Productie- en processystemen voor onderzoek, ontwikkeling, productie en vermarkting intrinsiek digitaal veilig maken door nieuwe generaties 'security products' en 'secure products'.
SEMICONDUCTOR TECHNOLOGIES	De ontwikkeling van cybersecure chips is een cross-over met Semiconductor technologies, waarover afstemming plaatsvindt. Relevant is verder dat cybersecurity binnen de semicon-productieketen binnen de Actieagenda Cybersecurity Technologies aandacht krijgt.
AI & DATA	Ten aanzien van AI & Data vindt samenwerking plaats op twee vlakken. Allereerst kan AI worden ingezet ter voorkoming en bestrijding van cyberaanvallen. Dit valt in principe onder de Actieagenda Cybersecurity. Ten tweede kan cybersecurity worden ingezet bij de ontwikkeling van AI, Data en cloudoplossingen. Dit valt in principe on der Actieagenda AI & Data. De werkelijkheid zal grijze gebieden kennen. De twee Actieagenda's stemmen daarover af en zetten gezamenlijke activiteiten op waar nodig.

Tabel 4.3 *Samenhang met andere Actieagenda's vanuit de NTS.*

5. INNOVATIEPROGRAMMA SECTORALE EN REGIONALE TRANSITIES

5.1 ALGEMENE BESCHRIJVING

Het Innovatieprogramma Sectorale en regionale transities heeft als ambitie om sectoren en regionale ecosystemen in 2035 intrinsiek digitaal veilig te maken en nieuwe bedrijvigheid te creëren. Dat betekent dat cybersecurity niet langer als kostenpost of nabrander wordt gezien, maar als integraal onderdeel van bedrijfsvoering en als onderscheidende factor voor Nederlandse producten en diensten om zo meer vermarkting te bewerkstelligen. Daarbij verschuift de aandacht van producten en diensten voor veiligheid naar intrinsiek digitaal veilige producten. Daarvoor zijn duurzame ecosystemen nodig. Dit geldt niet alleen voor het grootbedrijf, maar juist ook voor het mkb. Een dynamisch ecosysteem waarin allerlei partijen elkaar inspireren en scherp houden is het middel om in 2035 intrinsiek veilig te zijn.

Kennisvragen die daarbij een rol spelen zijn onder meer:

- Welke samenwerkingsvormen geven de beste garantie voor kennis- en informatie-uitwisseling?
- Hoe richten we het ecosysteem zodanig in dat 'valleys of death' worden voorkomen?
- Hoe zetten we effectieve waardeketens en business cases op om innovatie tot toepassing en valorisatie te laten leiden?
- Hoe verbinden we regionale ecosystemen landelijk?
- Welke dwarsverbanden zijn er sectoraal te maken vanuit secure-by-design?

De beantwoording van deze vragen heeft een belangrijke impact op het verdienvermogen van de Nederlandse economie. De economisch grootste impact is zonder meer de bescherming van het bestaande verdienvermogen van alle sectoren tegen cyberaanvallen. Cyberaanvallen ondermijnen de economie en de bestrijding ervan raakt aan alle maatschappelijke activiteit. Een tweede vorm van impact betreft de vergroting van de autonomie van Nederland en de Europese Unie door vermindering van de afhankelijkheid van niet-EU partijen.

Door Europese alternatieven te ontwikkelen voor bestaande technologie wordt de EU minder afhankelijk van buitenlandse leveranciers. De derde vorm van impact is de ontwikkeling van nieuwe producten waarmee een wereldmarkt kan worden bediend. Het gaat hier dus om het tot stand brengen van nieuw verdienvermogen.

Overheidsinterventie is hier op de plaats omdat cybersecurity investeringen de afgelopen jaren onvoldoende van de grond zijn gekomen in de markt. De oorzaak daarvan is dat cybersecurity investeringen op het niveau van waardeketens en ecosystemen alleen collectief zinvol zijn. Individuele partijen wachten op elkaar. Om dat patroon te doorbreken is een PPS-aanpak een nuttig instrument.

5.2 PLAN VAN AANPAK

De Actieagenda coördineert en stimuleert publiek-private samenwerkingsverbanden in sectoren en regio's De Actieagenda stuurt op kennisuitwisseling tussen bestaande en nog te vormen consortia en het organiseren van impulsen tot vernieuwing in de praktijk vanuit onderzoek. Daarbij zijn de PPS'en zelf verantwoordelijk voor de inzet van hun middelen. De Actieagenda stimuleert dat publieke- en private fondsen beschikbaar komen die die investeringen versterken en helpt de PPS'en hun doelstellingen te realiseren door coördinatie tussen PPS'en. Daarbij probeert de Actieagenda ook te stimuleren dat in verschillende PPS'en de diverse lijnen van sectorale & regionale transitie, technologie & methodologie en randvoorwaarden & infrastructuur met elkaar verbonden worden.

De Actieagenda verzorgt de afstemming tussen de reeds bestaande PPS'en die zelfstandig blijven opereren. Daarnaast ondersteunt de Actieagenda de vorming van nieuwe consortia. Gedurende de tienjarige looptijd van de Actieagenda kunnen nieuwe sectoren of regio's aanhaken en profiteren van de geleerde lessen. Daarmee groeit het programma van enkele toonaangevende consortia uit tot een breed ecosysteem van intrinsieke digitale veiligheid in de Nederlandse economie. Om een concreet beeld te vormen geeft Tabel 5.1 vier bestaande en zich ontwikkelende consortia weer. Dit geringe aantal is tekenend voor het jonge veld van cybersecurity en

CONSORTIUM	OMSCHRIJVING
BRABANT HOUSE OF CYBER (BHOC)	Ontwikkeling van veilige digitale producten, componenten en systemen voor de hightechindustrie
FIELDLAB ENERGY CYBER SECURITY (FLECS)	Vergroten van de cyberweerbaarheid van de offshore wind-infrastructuur door technologieontwikkeling
INNOVATIECOALITIE CYBER-VEILIGE ENERGIETRANSITIE	Versterking van veilige en toekomstbestendige digitalisering van energiesystemen
PARTNERSHIP FOR CYBER SECURITY INNOVATION (PCSI)	Ontwikkeling van innovatieve cybersecurityoplossingen in de financiële sector

Tabel 5.1 *Lopende consortia en consortia in ontwikkeling*

benadrukt de noodzaak van dit Innovatieprogramma. Deze voorbeelden raken ook de drie verschillende soorten impact hierboven. Hoewel het zwaartepunt van deze consortia ligt op sectorale of regionale transitie investeren zij ook in de technologie & methodologie laag en de infrastructuur laag. Vanuit de praktijk worden vragen geformuleerd aan kennisinstellingen over technologie maar bijvoorbeeld ook opleiding.

Brabant House of Cyber

Dit richt zich op het aanpakken van marktfalen op het gebied van product security en ketenweerbaarheid in de hightechsector. De ambitie is de ontwikkeling van veilige digitale producten, componenten en systemen voor de hightechindustrie. Op deze manier wil Brabant House of Cyber digitale producten intrinsiek veilig te maken, zoals vereist onder de Cyber Resilience Act, en tegelijk de weerbaarheid van het hightech-ecosysteem te versterken. Dit consortium zet in op kennisontwikkeling rond full-stack product security, zelfbeschermende systemen en AI-toepassingen in cybersecurity.

Concrete activiteiten concentreren zich rondom drie themalijnen: cyber-innovatie (nieuwe technologieën en methoden), cyber-talent (ontwikkelen opleidingsmogelijkheden) en cyber-weerbaarheid (opbouw van het vermogen om met aanvallen om te gaan). Driekwart van het beoogde budget wordt besteed aan het creëren van veilige producten.

Impact: versterking van de internationale concurrentie-positie van de Nederlandse hightechindustrie, verhoging van de nationale cyberweerbaarheid, structurele bijdrage aan talentontwikkeling en regionale innovatiekracht. Partners: Naast een groot aantal mkb-bedrijven zijn dit ASML, Neways, NTS, Provincie Noord-Brabant, BOM, TNO, TU/e, Avans, Brainport Development.

FLECS

Een publiek-privaat partnerschap met als doel de cyberweerbaarheid van de offshore wind-infrastructuur in de Nederlandse Exclusieve Economische Zone te vergroten. FLECS ontwikkelt een onderzoeks- en innovatieprogramma rond drie thema's: samenwerking in de keten, cybersecuritytechnologieën en menselijk gedrag.

Voorbeelden van technologieontwikkeling zijn onder meer technologiegebaseerde diensten (bijvoorbeeld via vulnerability assessments, supply chain oefeningen); research en innovatie (bijvoorbeeld het gebruik van een digital twin om supply chain samenwerking of menselijk gedrag rondom cyberaanvallen te bestuderen), investeringen in menselijk kapitaal (bijv. traineeships, kennisoverdracht).

Impact: versterking van de veiligheid van de energietransitie op de Noordzee, internationale positionering van Nederland als koploper in cybersecure offshore-infrastructuur, en een blauwdruk voor andere vitale sectoren.

Partners: naast initiatiefnemers TKI Offshore Energy, het ministerie van Klimaatbeleid en Groene Groei, het ministerie van Economische Zaken en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) zijn er netbeheerders, windparkexploitanten en cybersecuritybedrijven betrokken bij FLECS.

Innovatiecoalitie Cyberveilige Energietransitie

Richt zich op de veilige en toekomstbestendige digitalisering van energiesystemen. Het consortium werkt aan cyberinnovaties voor slimme energie-netwerken, digitale platforms voor vraag- en aanbod-sturing, en gedistribueerde energieopslag.

Onderscheidend is de ketenaanpak, gericht op het terugdringen van versnippering en het vergroten van de gezamenlijke impact.

Impact: versnelling van de energietransitie, hogere cyberweerbaarheid van gedigitaliseerde netwerken, en versterkte samenwerking tussen energiebedrijven, technologieaanbieders en beleidsmakers

Partners: Economic Board Zuid-Holland, TNO, TU Delft, KPN, Stedin, Batenburg Techniek, Technolution, the Green Village, Provincie Zuid-Holland, InnovationQuarter en Security Delta (HSD) in samenwerking met Havenbedrijf Rotterdam, Westland infra, Dutch Institute for Vulnerability Disclosure (DIVD), European Network for Cyber Security (ENCS), Greenport West-Holland, Topsector ICT, gemeente Den Haag, TU PowerWeb Institute, Living Lab Scheveningen, Campus@Sea, Duurzaamheidsfabriek en Hi Delta.

PCSI (Partnership for Cyber Security Innovation)

Een meerjarig publiek-privaat programma dat zich richt op de financiële sector en grote organisaties. Binnen PCSI werken banken, verzekeraars, kennisinstellingen en technologiepartners samen aan de ontwikkeling van innovatieve cybersecurityoplossingen. De focus ligt op het vergroten van digitale weerbaarheid tegen geavanceerde dreigingen, onder meer door gezamenlijke R&D-projecten, testomgevingen en kennisuitwisseling.

Impact: versterking van de stabiliteit en betrouwbaarheid van de financiële sector, ontwikkeling van generieke oplossingen die ook in andere sectoren toepasbaar zijn, en stimulering van samenwerking en technologie-ontwikkeling tussen grote ondernemingen en kennis-partners.

Partners: ABN-AMRO, Achmea, Belastingdienst, ING, Shell en TNO zijn de kernpartners, daarnaast zijn nog vele publieke- en private partijen aangesloten als liaisonpartners.

5.3 FINANCIËLE BREAKDOWN

In 2026 werkt de Actieagenda samen met de vier genoemde consortia om samenwerking op te bouwen, activiteiten elkaar te laten versterken en geleerde lessen uit te wisselen. De projectie is dat per consortium van €20-35 miljoen aan investeringen nodig is voor de komende 5 jaar, verdeeld over overheid, kennisinstel-lingen en bedrijven (zie Tabel 5.2). Voor de looptijd van de Actieagenda richt de Actieagenda zich op het ondersteunen van 2 additionele consortia per jaar na 2026 zodat uiteindelijk in 2035 20 consortia zijn gestart. Uiteindelijk leidt dit tot een totale publiek-private investering over tien jaar van €400-€500 mln. Daarbij bouwt dit programma voort op de al bestaande, sterke positie van Nederland op het vlak van cybersecurity, en zoekt de aansluiting bij Europese projecten.

Daarbij komt ruim 51% uit private middelen. Dit percen-tage neemt in de loop van de tijd procentueel toe terwijl de publieke bijdrage in de loop van de tijd vermindert. De rationale hiervan is dat in de beginjaren nog veel nieuwe processen en aanpakken moeten worden ontwikkeld, terwijl in latere jaren op bestaande kennis kan worden voortgebouwd en worden opgeschaald op basis van deelnemers die zelf (meer) inleggen.

	BEOOGDE FINANCIERING (MEUR)									
	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Bestaande activiteiten/ bestaande middelen	4	4	4	4	4	4	3	3	3	2
Nieuwe activiteiten/ bestaande middelen	6	6	11	16	21	26	32	32	27	28
Nieuwe activiteiten/ nieuwe middelen	-	-	-	-	-	-	-	-	-	-
Privaat	5	5	10	20	25	30	35	40	45	30
TOTAAL	**15**	**15**	**25**	**40**	**50**	**60**	**70**	**75**	**75**	**60**

Tabel 5.2 *Projecties financiering Innovatieprogramma Sectorale en regionale transities*

6. INNOVATIEPROGRAMMA TECHNOLOGIE EN METHODOLOGIE

6.1 ALGEMENE BESCHRIJVING

Het Innovatieprogramma Technologie & Methodologie ontwikkelt de technologieën én methodieken die nodig zijn voor veilige producten, betrouwbare data, gecontroleerde ketens en strategische autonomie. Om brede toepassing te borgen, vormt het de methodische brug tussen ontwerp, verificatie, validatie en certificering: secure-by-design-frameworks, formele verificatie en conformity-assessment-tools maken veiligheid herhaalbaar en aantoonbaar. Zo versnelt dit programma de overgang van reactieve beveiliging naar intrinsiek veilige producten, ketens en ecosystemen – de basis voor een intrinsiek digitaal veilig Nederland in 2035.

De zes thema's in dit programma fungeren als technologisch kompas voor 2025–2035. Tabel 6.1 geeft de thema's weer (Appendix A geeft meer detail). Ze maken het mogelijk om gericht innovatieonderwerpen te agenderen, prioriteren en op te schalen in lijn met technologische ontwikkelingen en dreigingsbeelden. De thema's sluiten aan bij CRA, AI Act, NIS2 en Chips Act en dragen bij aan een autonome en betrouwbare Europese digitale economie. Ook sluiten deze thema's aan bij de NCSRA-IV[24] die de bestaande Nederlandse positie op deze gebieden wil uitbouwen. Tot slot, deze thema's bouwen voort op huidige generaties cybersecurity-producten en diensten als Security Operations Centers (SOCs) inclusief SIEM (Security Information and Event Management) en EDR (Endpoint Detection and Response) technologieën, Threat Intelligence Platforms, Network Security Tools en gereedschappen voor (post-quantum) cryptografie en tools voor pentesting, red teaming en Security Orchestration, Automation and Response (SOAR).

De benoemde technologieën lenen zich bij uitstek voor de ontwikkeling van producten en diensten waarmee het bedrijfsleven een marktpositie kan opbouwen. Het bedrijfsleven kan dit doen door fysieke producten te produceren en te verkopen (bijv. chips, sensoren, satellietnetwerken) of door dienstverlening te ontwikkelen en te verkopen (bijv. implementatie van Privacy Enhanching Technologies (PETs) of het bouwen van digital twins). Hier ligt een sterke basis voor toekomstig verdienvermogen van Nederlandse bedrijven.

THEMA	INNOVATIE ZWAARTEPUNT	NIVEAU	INNOVATIELIJNEN
Secure Hardware & Embedded Systems	Technologie	Fysieke laag	Veilige chips, sensoren, controllers, embedded security
AI & Security	Technologie	Intelligentie & adaptiviteit	AI for security & security of AI, explainable en verifieerbare AI
Infrastructuur security	Technologie	Netwerken & Cloud	6G, quantum- en satellietnetwerken, secure cloud & edge
Quantum Veilige cryptografie	Technologie	Data & identiteit	Europese cryptografie, quantumveilige algoritmen, PETs, datalifecycle security
Secure Engineering & Product Development	Methodologie	Ontwerp & software	Secure-by-design, veilige ontwikkelketens, CRA-conformiteit, formele verificatie
System & Supply Chain Assurance	Methodologie	Integratie & ecosysteem	Model-based security, digital twins, assurance, ketenvertrouwen

Tabel 6.1 *Thema's voor het Innovatieprogramma Technologie en Methodologie*[25]

24 NCSRA IV (2025), Science for a resilient digital ecosystem.
25 Deze tabel is apart gevalideerd in enkele expertsessies.

6.2 PLAN VAN AANPAK

De Actieagenda werkt in de beginfase samen met een aantal lopende activiteiten en er wordt een aantal calls en programma's opgezet (met nieuwe middelen). Dat leidt tot de activiteiten in Tabel 6.2.

Richten met technologie en methodiekagenda

Dit innovatieprogramma richt zich in de eerste fase op verdere uitwering van de technologie en methodologie agenda uit Tabel 6.1, inhoudelijke prioritering van onderwerpen en eerste richtinggevende activiteiten. Daarvoor wordt een koplopersgroep van 'thought leaders' in cybersecurity, secure-by-design, autonome cybersecurity en product security aangesteld. Dit houdt in dat voor elk van de thema's een roadmap wordt ontwikkeld en bestaande initiatieven worden gebundeld. Dat leidt tot een prioritering van vervolgstappen waaromheen middelen kunnen worden gezocht. In de loop van de tijd wordt dit uitgebreid en opgeschaald vanuit bestaande en nieuwe middelen en programmering.

Intrinsiek weerbare digitale ecosystemen

Deze programma, te starten vanuit een NWA-call in voorbereiding, gaat de vraag beantwoorden hoe digitale ecosystemen door innovatie intrinsiek veiliger en weerbaarder kunnen worden gemaakt en hoe zij hun aanpassingsvermogen kunnen vergroten. Zij is met name gericht op netwerken van organisaties die via digitale technologieën samenwerken om gezamenlijke waarde te creëren. Dit kunnen bijvoorbeeld toeleveringsketens zijn, digitale informatienetwerken, logistieke ketens of kennisecosystemen. Het gaat hierbij zowel om verticale ketensamenwerking (leveranciers of klanten) als om horizontale ketensamenwerking (samenwerking tussen organisaties van hetzelfde niveau). In elk van deze ecosystemen is cybersecurity op het niveau van het ecosysteem van minstens zo groot belang als de cybersecurity van de individuele organisaties daarin.

Het programma richt zich op het intrinsiek digitaal weerbaarder maken van ecosystemen door middel van nieuwe samenwerkingsvormen en innovatieve technologieontwikkeling. Met name digitale ecosystemen in de (rijks)overheid en vitale sectoren verdienen extra aandacht vanwege de hoge impact die verstoringen door cyberaanvallen daar kunnen hebben. Daarbij moet antwoord worden gegeven op zowel organisatorische als technologische vragen. Organisatorische vraagstukken betreffen hoe organisaties beter kunnen samenwerken bij het uitwisselen van dreigingsinformatie, hoe toezicht hierop kan worden verbeterd op ecosysteemniveau en welke risicomanagementmodellen op ecosysteemniveau nodig zijn. Technische vraagstukken betreffen de inzet van innovatieve technologie om verouderde systemen te beschermen en hoe kan technologie worden ingezet om informatie over cyberdreigingen zo snel mogelijk op de juiste plek te krijgen. Publieke partners hierin zijn AIVD, ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Justitie en Veiligheid en Infrastructuur en Waterstaat. Bij de uitvoering van het programma zal een brede vertegenwoordiging van afnemend- en toeleverend bedrijfsleven (inclusief de cybersecurity-industrie) betrokken worden.

ACTIVITEIT	OMSCHRIJVING	BRON
Richting geven met de technologie en methodologie agenda	Inrichten koplopersgroep die inhoudelijk eigenaarschap wil en kan nemen op de agenda, vertalen naar acties en programmering.	TKI ICT
Intrinsiek weerbare digitale ecosystemen	Intrinsiek veiliger en weerbaarder maken van digitale ecosystemen en vergroten van hun aanpassingsvermogen	NWA Lijn 2 call
Hapkido	Onderzoek naar de wijze waarop de overgang naar een quantumveilige publieke sleutelinfrastructuur kan worden gerealiseerd	NWO call Cybersecurity
Veilige chips	Ontwikkelen innovatieve, hardware-gebaseerde benaderingen voor chipbeveiliging	O.a. TNO
Secure Engineering & Product Development	Methodologie	Ontwerp & software
System & Supply Chain Assurance	Methodologie	Integratie & ecosysteem

Tabel 6.2 *Voorbeeld van activiteiten*

HAPKIDO

Hapkido onderzoekt hoe de overgang naar een quantumveilige publieke sleutelinfrastructuur (Public Key Infrastructure, PKI) kan worden gerealiseerd. De mogelijke komst van quantum computers maakt traditionele beveiligingsmechanismen achterhaald. Er is al veel kennis ontwikkeld over quantumveiligheid. Deze kennis kan worden omgezet in toepassingen en daarmee ook in nieuwe bedrijvigheid.

Het programma HAPKIDO voert een onderzoeks- en ontwikkelingsproject uit dat zich richt op de overgang naar quantumveilige Public Key Infrastructures. Het programma omvat het ontwikkelen van cryptografische technieken, migratie-architecturen en governance-modellen om organisaties te helpen hun digitale communicatie te beveiligen tegen de bedreigingen van quantumcomputers. Belangrijkste activiteiten zijn onder meer het ontwerpen en testen van hybride quantum-veilige PKI-systemen die nog compatibel zijn met bestaande encryptiemethoden, het opstellen van een routekaart voor de migratie naar quantumveilige infrastructuren en het ondersteunen van organisaties bij deze transitie. Daarnaast is fundamenteel cryptografisch onderzoek nodig, onder meer naar beveiligingsbewijzen en combinaties van cryptografische schemata om de veiligheid tijdens de overgang te waarborgen. Partners zijn onder andere TU Delft, CWI, KPN, Microsoft en Logius.

Veilige chips

Chips vormen een cruciaal onderdeel van de technologische infrastructuur. Hun beveiliging is nu nog grotendeels gebaseerd op conventionele methoden, zoals softwarematige cryptografie en sleutelopslag. Diverse Nederlandse partijen, waaronder NXP, Sandgrain en Fortaegis, ontwikkelen innovatieve, hardware-gebaseerde benaderingen voor chipbeveiliging. Zo kunnen chips worden uitgerust met Secure Processing Units (SPU's), elk voorzien van een uniek authenticatiemechanisme. Hierdoor worden ze vrijwel onkraakbaar, zelfs voor toekomstige kwantumcomputers. Onderzoek naar dit type technologie maakt het mogelijk cryptografische sleutels niet langer centraal op te slaan of tussen apparaten uit te wisselen, waarmee traditionele kwetsbaarheden worden geëlimineerd. Deze geavanceerde chips zijn breed inzetbaar in uiteenlopende sectoren, zowel nationaal als internationaal. Daarmee ontstaat een flink economisch potentieel. Het innovatieprogramma Technologie en Methodologie kijkt wat dit onderwerp en dit soort bedrijven nodig hebben om de kloof tussen onderzoek naar dergelijke chips en hun toepassing in de praktijk te helpen overbruggen. Mogelijke partners zijn TNO, NXP, Sandgrain en Fortaegis.

6.3 FINANCIËLE BREAKDOWN

Tabel 6.3 geeft een projectie van de financiering en laat zien dat voor de activiteiten onder deze agenda de private financiering bijna 50% is van het totaal. Op basis van ervaringscijfers is de gemiddelde omvang van consortia ongeveer €5 miljoen publieke bijdrage. Hierbij zit ook een belangrijk deel waar nieuwe middelen voor nodig zijn. In Tabel 6.3 is gerekend met de ontwikkeling van 20 tot 40 consortia over de gehele tienjarige looptijd van de Actieagenda.

	BEOOGDE FINANCIERING (MEUR)									
	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Bestaande activiteiten/ bestaande middelen	10	10	10	10	5	5	5	5	5	5
Nieuwe activiteiten/ bestaande middelen	-	-	-	-	5	5	5	5	5	5
Nieuwe activiteiten/ nieuwe middelen	10	10	10	10	10	10	10	10	10	10
Privaat	15	15	15	15	15	20	20	20	20	20
TOTAAL	**35**	**35**	**35**	**35**	**35**	**40**	**40**	**40**	**40**	**40**

Tabel 6.3 *Projecties financiering Innovatieprogramma Technologie en Methodologie*

7. INNOVATIEPROGRAMMA RANDVOORWAARDEN EN INFRASTRUCTUUR

7.1 ALGEMENE BESCHRIJVING

Het Innovatieprogramma op dit gebied richt zich op de randvoorwaarden en infrastructuur die nodig zijn om de benodigde transitie te realiseren. De ambitie is om een speelveld te creëren dat de andere twee Innovatieprogramma's ondersteunt en dat internationaal tot de top behoort. Dit kan via talentprogramma's, testlabs, regelgeving, financiering en ondersteuning van startups en scale-ups. Het invullen van randvoorwaarden en infrastructuur gaat op een aantal punten de Nederlandse schaal te boven. Afstemming met Europese kaders (NIS2, CRA, AI Act) en internationale samenwerking zijn nodig om dit Innovatieprogramma te realiseren. Uiteindelijk is in 2035 voldoende talent beschikbaar, floreren er startups en zijn er testlabs actief.

Kennisvragen die daarbij van belang zijn, zijn:

- Hoe creëren we vanuit het 'by design' paradigma voldoende urgentie, belang en de goede mindset op innovatie, vraagsturing, ondernemerschap, samenwerking en internationalisering?
- Welke nieuwe en aangepaste bestaande innovatie-instrumenten zijn nodig om ze beter toepasbaar en impactvol te laten zijn?
- Hoe komen we aan voldoende talent voor onderzoek, ontwikkeling en toepassing van cybersecurity by design Hoe sturen we op strategische inkoop van de overheid en grootbedrijf die innovatie bevorderd?
- Hoe zetten we een innovatie-infrastructuur op van testlabs, fieldlabs, digital twins en regulatory sandboxes?
- Hoe zorgen we dat regelgeving niet voor belemmering maar voor meer veiligheid, innovatie en verdienvermogen zorgt?
- Hoe creëren we toegang tot EU-financiering en markt?

De impact op het verdienvermogen van dit innovatie-programma is groot. Zo is de aanwezigheid van voldoende talent en cybersecurityprofessionals een sine qua non voor het ontstaan van een Nederlandse cybersecurity-industrie. Zonder dit talent en deze professionals zijn de andere twee innovatieprogramma's moeilijk te realiseren.

7.2 PLAN VAN AANPAK

Voor de beantwoording van de kennisvragen, sluit de Actieagenda aan bij bestaande initiatieven, maar stimuleert zij ook de ontwikkeling van een aantal nieuwe activiteiten (zie Tabel 7.1). De kennisvragen weerspiegelen de versnippering van het veld.
Op veel plekken zijn partijen nog zoekende. Dit Innovatieprogramma richt zich in de eerste fase dan ook vooral op activiteiten die verbinding tot stand brengen.

Verbindingsactiviteiten

Gelet op het feit dat rondom cybersecurity eerst een Opbouwfase (zie 4.1) nodig is, start de Actieagenda

ACTIVITEIT	OMSCHRIJVING
Verbindingsactiviteiten	Activiteiten gericht op het leggen van verbindingen in het ecosysteem zodat versnippering vermindert
HCA ICT Taskfore Cybersecurity	Vergroten van zowel het aantal als de kwaliteit van cyberprofessionals in Nederland.
Secure Alliance	Beveiliging van autonome en adaptieve cybersecurityoplossingen die digitale systemen levenslang beveiligen tegen steeds veranderende en geavanceerde dreigingen. Daartoe zet dit programma Industry Innovation Labs op en stimuleert het wetenschappelijke onderzoek.

Tabel 7.1 *Mogelijke activiteiten*

met een aantal laagdrempelige activiteiten. Deze zijn erop gericht het ecosysteem rondom cybersecurity te verstevigen en witte plekken in het ecosysteem of de kennis te identificeren. Aansluitend bij de NTS zijn dit bijvoorbeeld:

- Dialoogsessies met investeerders over de mogelijkheden van nieuwe technologieën die ontwikkeld worden in het Innovatieprogramma Technologie & Methodologie;
- Dialoogsessies met de onderwijssector om te komen tot een analyse van kansen en barrières rondom cybersecurity-onderwijs;
- Een serie events rondom thema's als quantumbeveiliging voor het mkb;
- Dialoogsessies met dienstverleners en producenten van cybersecurityproducten de behoefte aan testlabs, fieldlabs en regulatory sandboxes beter in kaart te brengen;
- Dialoogsessies met verantwoordelijken voor cybersecuritybeleid en -handhaving over innovatieversterkende regelgeving, conformiteit en standaardisatie.

De investeringen in deze sessies beperkt. Het gaat om kleinschalige sessies waarbij de diepte in wordt gegaan om een goed beeld te krijgen van de behoeften van de deelnemers. Daarbij is in deze sessie in het bijzonder aandacht voor verknoping met de andere twee Innovatieprogamma's, Sectorale & regionale transitie en Technologie & methodologie.

Human Capital Agenda

De Human Capital Agenda Taskforce Cybersecurity werkt aan het vergroten van zowel het aantal als de kwaliteit van cyberprofessionals in Nederland. Daartoe volgt het een publiek-private aanpak waarin overheid, onderwijs en bedrijfsleven samenwerken. De taakgroep reageert op de groeiende vraag naar cybersecurity-talent, zoals vastgesteld in landelijke rapportages en arbeidsmarktanalyses.

Daarbij richt de taskforce zich onder andere op:

- Het bepalen van de strategische koers voor cyberonderwijs, arbeidsmarkt en talentontwikkeling.
- Initiëren van actieplannen gericht op instroom, doorstroom en behoud van cybersecurityprofessionals.
- Opzetten van vier 'werktafels' voor 2026 die zich richten op essentiële thema's zoals educatie, samenwerking met werkgevers, ontwikkeling van het docentberoep en betere arbeidsmarkttoeleiding.
- Bevordering van multidisciplinaire samenwerking tussen kennisinstellingen, bedrijven en publieke organisaties om skills en kennis rond digitale veiligheid breed toegankelijk te maken.
- Uitvoeren van initiatieven die knelpunten (tekorten, mismatch skills) in de cybersecuritysector aanpakken en talent effectiever inzetten op nationaal niveau.

Partners: Het ministerie van Economische Zaken is opdrachtgever en Platform Talent voor Technologie (PTvT) en NCC-NL zijn uitvoerders.

Infrastructuur: SECURE Alliance

De Self-Evolving Cybersecurity for Unyielding REsilience (SECURE) Alliance stimuleert samenwerking rondom nieuwe infrastructuur. De SECURE Alliance heeft als hoofdvraag hoe autonome en adaptieve cybersecurityoplossingen ontwikkeld kunnen worden die digitale systemen levenslang beveiligen tegen steeds veranderende en geavanceerde dreigingen, waaronder de impact van quantumtechnologieën en AI.

Om dit te bereiken versterkt de SECURE Alliance de infrastructuur door de opzet van Industry Innovation Labs. Dit zijn langdurige samenwerkingen tussen bedrijven en kennisinstituten voor het oplossen van complexe sectorale cybersecurity-uitdagingen, gericht op TRL 2-6. Daarnaast ondersteunt het SECURE Science Program fundamenteel onderzoek (TRL 2-4) naar onderwerpen zoals secure-by-design, zelfbeschermende intelligentie, voorbereiding op quantumveiligheid en robuust levenscyclusbeheer. Onder de titel NextGen Cyber Ecosystems realiseert het ook impact door brede adoptie, ontwikkeling van menselijk kapitaal, beleidsafstemming en opschaling van innovaties, inclusief certificering en ondersteuning van startups.

De initiatiefnemer van de SECURE Alliance, TU Delft, werkt toe naar indiening van een voorstel bij NWO in 2026 om de Alliance te versterken middels meerjarige financiering, parallel aan de looptijd van de Actieagenda (10 jaar).

7.3 FINANCIËLE BREAKDOWN

De investeringsprojecties in infrastructuur zoals labs en in de Human Capital Agenda zijn weergegeven in Tabel 7.2. Een deel van de middelen is uit bestaand instrumentarium te financieren zoals uit TNO en NWO-middelen. Voor Industry Innovation Labs zijn echter nieuwe middelen nodig.

	BEOOGDE FINANCIERING (MEUR)									
	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Bestaande activiteiten/ bestaande middelen	5	5	5	–	–	–	–	–	–	–
Nieuwe activiteiten/ bestaande middelen	-	-	-	5	5	5	5	5	5	5
Nieuwe activiteiten/ nieuwe middelen	5	5	10	10	10	10	5	5	5	5
Privaat	10	10	10	10	15	15	15	15	10	10
TOTAAL	**10**	**10**	**15**	**15**	**15**	**15**	**10**	**10**	**10**	**10**

Tabel 7.2 Projecties financiering Innovatieprogramma Randvoorwaarden en Infrastructuur

8. ORGANISATIE

De hoofdtaak van de Actieagenda CST is focus aan te brengen in innovatieactiviteiten en investeringen op het gebied van Cybersecurity Technologies. Door het afstemmen en verbinden van de beschikbare (en mogelijk nieuwe) instrumenten werkt de Actieagenda aan de realisatie van gezamenlijke doelen. Daarbij draagt iedere organisatie vanuit eigen kracht en eigen verantwoordelijkheid bij aan de Actieagenda.

Daaruit volgt dat de structuur en governance van de agenda de volgende activiteiten dient te ondersteunen:

- Verbinden van publieke partijen om hun instrumentarium op de Actieagenda te richten (op regionaal, nationaal en internationaal niveau)
- Verbinden van private met publieke partijen rondom de Actieagenda
- Vergroten van de bekendheid van de Actieagenda bij de verschillende spelers in het veld, zowel privaat als publiek
- Monitoring van de voortgang van de Actieagenda
- Aanpassen van de Actieagenda aan nieuwe (technologische) ontwikkelingen
- Identificeren van synergie tussen de Innovatie-programma's en de overige Actieagenda's die onder de NTS vallen

De governance van de Actieagenda CST wordt geborgd vanuit de KIA Digitalisering in nauwe samenwerking met de KIA ST, waar Digital Holland als agenda-lid themateam deel van uitmaakt. De KIA Digitalisering werkt daarbij samen met de coalities die onderdeel uitmaken van de actieagenda, het ministerie van Economische Zaken (de Directies Innovatie en Digitale Economie), alsmede key stakeholders zoals TNO, NWO, de ROM's, IPN (WO), PRIO (HBO) en het NCC-NL (RvO). Digital Holland (voorheen Topsector ICT) fungeert als coördinerend projectbureau voor de Actieagenda CST en werkt in nauwe afstemming met het ministerie van Economische Zaken, coalities en andere stakeholders.

Binnen de governancestructuur van KIA Digitalisering worden een thematean en een programmaraad ingericht, in nauwe afstemming met de directie Digitale Economie. Het thematean heeft daarbij het overzicht over het totale veld en legt de verbinding tussen industriebeleid en innovatiebeleid. Het speelt een rol bij het verbinden van partijen, sturen op nieuwe middelen en programma's en het vergroten van de bekendheid van de Actieagenda. De programmaraad overziet de verschillende innovatieprogramma's, signaleert waar witte vlekken zitten, onderzoekt waar Actieagenda's elkaar kunnen versterken en doet voorstellen voor het updaten van de Actieagenda aan het thematean. Het levert bovendien de informatie aan om de programmavoortgang van de Actieagenda te monitoren. Tevens wordt circa twee keer per jaar een event georganiseerd met alle spelers op de Actieagenda om kennis en ervaring uit te wisselen, maar vooral ook voort te bouwen op elkaar en synergie te realiseren tussen de verschillende Innovatieprogramma's.

COLOFON

De Actieagenda is ontwikkeld onder regie van Digital Holland (Voorheen Topsector ICT) en het kader van de KIA Digitalisering. Dit is gedaan in nauwe afstemming met KIA Sleuteltechnologie, het ministerie van Economische Zaken en een breed pallet aan stakeholders. Aan de totstandkoming van deze Actieagenda heeft een uitgebreid proces ten grondslag gelegen waarbij met een groot aantal partijen is samengewerkt. In een eerste fase is een verkenning gedaan van het vraagstuk, een SWOT gemaakt rondom Cybersecurity in Nederland. Er is ook een inventarisatie gemaakt van regelingen, projecten, ideeën, ervaringen op dit vlak, zowel regionaal, nationaal als internationaal. Deze veelheid aan informatie is in een tweede fase omgezet in de voorliggende Actieagenda. Dat is gebeurd in samenwerking met het veld. Een werkgroep heeft voorstellen en ideeën ontwikkeld die vervolgens in nauwe afstemming met partijen in het veld verder zijn gevalideerd, aangescherpt en soms ook verworpen. Dat heeft geleid tot een document dat de weerslag gaf van de verschillende discussies. Dit document is in een uitgebreide reviewronde met een aantal partijen verder aangescherpt en verbeterd.

De Actieagenda is tot stand gekomen met behulp van een groot aantal individuen en partijen. Wij zijn in het bijzonder dank verschuldigd aan:

- Een dynamisch samengestelde werkgroep met in de kern het voormalige dcypher, TNO-ICT, Digital Holland in nauwe afstemming met ministerie van Economische Zaken, directie Digitale Economie en NWO.
- Kernspelers binnen digitale veiligheid uit bedrijfsleven, overheid en wetenschap met wie wij tientallen interviews hielden.
- Collega-topsectoren, ROM's en Topinstituten van wier kennis we gebruik mochten maken en die hun netwerken hebben ingezet om op diverse momenten informatie aan te leveren.
- Deelnemers in vijf marktconsultaties met in totaal zo'n ruim vijftig deelnemers uit bedrijfsleven, onderzoek en beleid.
- Feedback en reviews uit de netwerken van KIA-Digitalisering, de Adviesraad KIA-Digitalisering, het voormalige dcypher, ROM's, TNO, NWO, IPN, PRIO, RVO, opstellers van de National Cybersecurity Research Agenda, het ministerie van Economische Zaken, 4TU.
- Vertegenwoordigers van de verschillende consortia en programma's die deel gaan uitmaken van de Actieagenda.
- Het ministerie van Economische Zaken directie Innovatie en directie Digitale Economie.
- Organisaties betrokken bij de expertvalidatie van Innovatieprogramma Technologie en Methodologie waaronder TNO, TU's, Maakindustrie en de Cyberindustrie.

DIGITALISERING

DIGITAL HOLLAND
where innovation starts

APPENDIX A:
TECHNOLOGISCHE EN METHODOLOGISCHE R&D-AGENDA

1. SECURE HARDWARE & EMBEDDED SYSTEMS (TECHNOLOGIE)

Noodzaak:
De veiligheid van digitale systemen begint bij hardware. Europa is nog sterk afhankelijk van niet-Europese chip- en embedded-securitytechnologie. Veilige, verifieerbare hardware is een voorwaarde voor intrinsiek veilige digitale producten.

Innovatielijnen:
- Trusted Execution Environments (TEE's) en hardware roots of trust.
- Physical Unclonable Functions (PUF's) en secure identity modules.
- Embedded secure-by-design in sensoren, controllers en edge-devices.
- Security-extensies van processoren voor ingebouwde beveiliging (FHE, confidential computing, side-channel-resistance, secure enclaves).
- Ontwikkeling van Europese secure SoC's en microcontrollers met formele verificatie.
- Hardware-integriteitstesten, validatie en supply-chain-assurance

Voorbeelden van concrete producten en diensten:
- Secure System-on-Chip (SoC) voor industriële, medische en defensietoepassingen
- Processorarchitecturen met ingebouwde FHE- en cryptografische extensies.
- PUF-gebaseerde identity modules voor IoT en robotica
- Secure controllers en firmware-gebaseerde trusted-boot-systemen
- Isolatie technologie malware / ransomware aanvallen, met name door 'user clicks' op onbetrouwbare bestanden en browsers, alsmede credential diefstal, te voorkomen
- Vinden, vergrendelen en wissen van devices op afstand (bijvoorbeeld bij gestolen devices)
- Beheer en monitoren van security hygiëne van devices alsmede remote herstel in geval van incidenten
- Sensoren die fysieke tampering van devices detecteren
- Hardware-assurance-labs en certificeringsdiensten voor Europese leveranciers

Impact doel:
Versterking van de Europese soevereiniteit in halfgeleider- en processortechnologie en borging van fysieke betrouwbaarheid als basis voor veilige en betaalbare software, data en AI

2. AI & SECURITY (TECHNOLOGIE)

Noodzaak:
AI is een sleuteltechnologie voor innovatie, maar brengt ook nieuwe risico's: manipulatie, bias en misbruik. Zonder ingebouwde waarborgen ontstaan kwetsbaarheden; met de juiste principes kan AI juist digitale veiligheid en autonomie versterken.

Innovatie lijnen:
- AI for Security: AI voor cyberverdediging in alle 5 van de fases Identify, Protect, Detect, Respond, Recover
- Security of AI: bescherming tegen adversarial attacks, data-poisoning, backdoor, input/evasion, model stealing, membership inference en model-misbruik (allen softwarematig) en side channel analyse (hardware matig)
- Explainable & Verifiable AI in lijn met AI Act en CRA.
- Formele assurance- en governance-methodieken voor betrouwbare AI.
- Integratie van AI met human-in-the-loop voor transparante besluitvorming

Kenmerkende voorbeelden:
- Autonome red-teaming-agents voor kwetsbaarheidsanalyse.
- AI-gedreven intrusion-detection-platforms met self-healing.
- Explainable AI-dashboards en assurance-frameworks

Nederland is in staat om veilige, betaalbare, veerkrachtige, soevereine uitlegbare en verifieerbare AI-systemen te produceren die cyberweerbaarheid versterken ('autonome cybersystemen') in lijn met Europese waarden van betrouwbaarheid en controle.

3. INFRASTRUCTUUR SECURITY (TECHNOLOGIE)

Noodzaak:
Communicatienetwerken en digitale infrastructuren — zoals 6G-, quantum- en satellietnetwerken, datacenters en edge-clouds — vormen de ruggengraat van de digitale samenleving.

Om continuïteit van vitale processen te waarborgen, moeten deze infrastructuren vanaf het ontwerp veilig, veerkrachtig en controleerbaar zijn, met hardware-verankerde beveiliging en Europese alternatieven voor cloud- en communicatiediensten.

Voorbeeld innovatielijnen:
- Veilige 6G-architecturen en protocollen met end-to-end trust-layers.
- Quantum Key Distribution (QKD) en hybride quantum-klassieke netwerken.
- Beveiliging van quantum communicatie netwerken
- Secure cloud & edge-infrastructuren met confidential computing en TEE's.
- Processor security-extensies in infrastructuurcomponenten (secure enclaves, FHE, memory isolation).
- Resilient networking: zelfherstellend en adaptief bij storingen of aanvallen.
- Secure orchestration & monitoring: realtime detectie en attestatie van workloads via hardware-trust.

Voorbeeld producten:
- 6G Secure Core Network Architectures met geïntegreerde trust-lagen.
- QKD-testbed-infrastructuren en secure connectivity gateways.
- Confidential edge-cloud servers met enclaves en FHE-ondersteuning.
- Resilient communication-frameworks voor vitale sectoren

Impact doel:
Veilige, betaalbare, veerkrachtige en soevereine endpoint devices, netwerk- en cloudinfrastructuren vormen de basis van Europa's digitale autonomie en garanderen continuïteit voor vitale diensten.

4. QUANTUM-VEILIGE CRYPTOGRAFIE (TECHNOLOGIE)

Noodzaak:
De vertrouwelijkheid, beschikbaarheid en integriteit van data staan onder druk door de opkomst van quantumcomputers en afhankelijkheid van niet-Europese cryptografische technologie. Digitale soevereiniteit vereist een Europese, quantum-veilige cryptografische basis en krachtige privacybevorderende methoden.

Voorbeeld innovatielijnen:
- Post-Quantum Cryptografie (PQC) en hybride cryptosystemen voor veilige transitie.
- Quantum-veilige identiteiten en sleuteluitwisseling binnen Identity Access Management (IAM) en federatieve trustmodellen.

- Privacy-Enhancing Technologies (PETs), inclusief Fully Homomorphic Encryption (FHE), Secure Multiparty Computation (MPC) en Zero-Knowledge Proofs (ZKP).
- Data lifecycle security (bescherming van data in creatie, gebruik, opslag en verwijdering)
- Integratie van cryptografie in hardware en IoT-systemen Trusted Execution Environments (TEEs), Secure Elements, accelerators)

Voorbeeld producten:
- Quantum-safe crypto-libraries en SDK's voor software, IoT en cloud.
- Europese key-management-frameworks en hybride PKI's.
- PET-platforms met FHE/MPC/ZKP voor privacy-preserving data-analyse.
- Crypto accelerators en secure elements in hardware

Impact doel:
Een soevereine, betaalbare en toekomstbestendige cryptografische infrastructuur beschermt vertrouwelijkheid en integriteit van data, voorkomt quantumdreigingen en verkleint de Europese afhankelijkheid van buitenlandse cryptotechnologie.

5. SECURE ENGINEERING & PRODUCT DEVELOPMENT (METHODOLOGIE)

Noodzaak:
De meeste software en digitale producten zijn niet vanaf het ontwerp veilig ontwikkeld. Bedrijven zoeken naar herhaalbare en aantoonbare secure engineering-praktijken en naar manieren om veiligheid structureel te integreren in hun ontwikkelketens.

Innovatielijnen:
- Secure-by-design pipelines (DevSecOps, secure coding, veilige softwarearchitecturen).
- Usable security & secure UX: ontwerprichtlijnen, pattern libraries en design-systemen die veilig en intuïtief gebruik bevorderen
- AI-assisted & AI-generated secure software
- Software Bills of Materials (SBOMs) voor transparantie en kwetsbaarheidsbeheer.
- Formele verificatiemethoden voor software en hardware in het ontwerp- en ontwikkelproces.
- Autonome validatie en self-healing systems met continue monitoring.
- CRA-conforme frameworks en compliance tooling (evidence by design).

Kenmerkende voorbeelden:
- Secure Software Factories met geïntegreerde DevSecOps en formele checks.
- SBOM-verificatie- en complianceplatforms voor leveranciers en afnemers.
- Usable security kits (UX-richtlijnen, componenten, configuratiewizards).
- Policy-constrained AI-codegen pipelines (LLM-guardrails, SAST/DAST + verificatie).
- Self-healing frameworks die afwijkingen automatisch mitigeren

Impact doel:
Cybersecurity wordt een structurele kwaliteits- én soevereiniteitsnorm in productontwikkeling, waardoor Nederland veilige, betaalbare en betrouwbare software autonoom kan produceren.

6. SYSTEM & SUPPLY CHAIN ASSURANCE (METHODOLOGIE)

Noodzaak:
Digitale waardeketens zijn complex en grensoverschrijdend. Organisaties missen inzicht in risico's, afhankelijkheden en compliance. Nieuwe methodieken zijn nodig om traceerbaarheid, veiligheid en vertrouwen structureel te borgen.

Voorbeeld Innovatielijnen
- Cybersecure-by-design op ketenniveau met standaardkaders en verificatie (teneinde aan te tonen dat originele componenten niet gemanipuleerd worden tussen de fabriek en gebruiker en tijdens de levenscyclus van de technologie).
- Model-based security & risk-engineering voor complexe ecosystemen.
- Digital twins voor simulatie, stress-testing en incident-respons.
- Monitoring- en transparantieplatforms met realtime risico-inzicht.
- SBOM/GUBOM voor gestandaardiseerde componentregistratie.
- Assurance-as-a-Service en certificeringsmethodieken conform CRA, NIS2 en AI Act.
- Voorkomen of detecteren van spyware / firmware / malware / hardware aanvallen.

Voorbeeld producten:
- Ketenveiligheidsdashboards met realtime inzicht in risico's en afhankelijkheden.
- Digital twin-modellen van kritieke ketens voor simulatie en stress testing.
- Trust & transparency platforms voor ketenpartners en leveranciers.
- Assurance-as-a-Service voor compliance en risicobeheersing.
- Keurmerk voor supply chain assurance en product assurance (bijv voor CRA-niveaus).
- Cryptografische verificatie om aan te tonen dat componenten niet worden gemanipuleerd.

Impact doel:
Veilige, transparante en soevereine digitale ketens waarin risico's beheersbaar zijn en vertrouwen aantoonbaar is verankerd, van component tot ecosysteem.

DIGITALISERING

DIGITAL HOLLAND

where innovation starts