Meerjarenstrategie

Vooruitblik

2026 30

HSD
securitydelta.nl



LEESWIJZER
De structuur van de meerjarenstrategie is opgebouwd vanuit een combinatie van inhoud, rollen en financiering van en voor Security Delta (HSD). Er zijn drie pijlers geformuleerd met een aantal focuspunten, die de basis zijn voor al onze activiteiten.



Colofon
Coördinatie: Chantal de Niet
Illustratie: Visuele verbinders
Fotografie: Istock, HSD, Livedrop
Grafisch ontwerp: Daphne van Langen / raza

© 2025
Niets uit deze uitgave mag worden verveelvoudigd of openbaar gemaakt worden in enige vorm of op enige wijze, zonder voorafgaande schriftelijke toestemming van HSD.

Inhoudsopgave

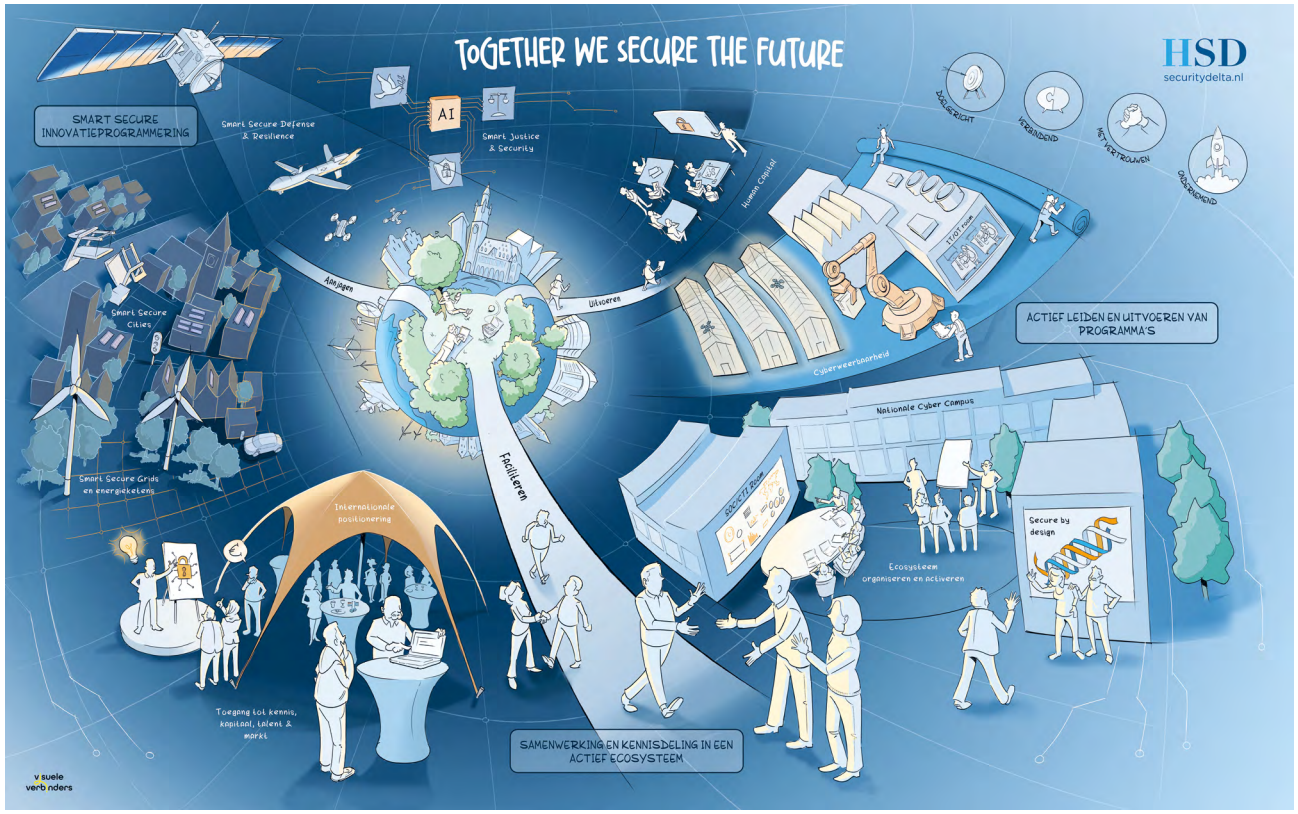
Samenvatting 3
1. Het speelveld en de rol van Security Delta 5
2. De ambitie van Security Delta 7
3. Doelstellingen & Focus 11
3.1 Samenwerking en kennisdeling in een actief ecosysteem 12
3.2 Het actief leiden en uitvoeren van programma's 14
3.3 Smart Secure Innovatieprogrammering 16
4. Aanpak 18
5. Organisatie 22
6. Financiering 25
Bijlage 1 Een klein stukje geschiedenis 26
Bijlage 2 Onze output 28
Bijlage 3 Why-What-How 32

Samenvatting

In de komende vijf jaar levert Security Delta (HSD) een bijdrage aan een veiligere (digitale) wereld en een (cyber) weerbaar & economisch sterker Nederland.

Samen met 300+ triple helix partners werken we binnen verschillende programma's aan verantwoorde inzet van nieuwe technologieën voor veiligheid, kennis-valorisatie en technologietransfer naar andere sectoren. Hierbij houden we de geopolitieke en nationale ontwikkelingen nauw in de gaten, zodat we daar waar wenselijk flexibel op kunnen inspringen. Het is een strategie die leidend is, maar niet in beton gegoten.

We zorgen voor een vruchtbare bodem, zodat we optimaal gebruik maken van een goede kennisbasis, de overheid en eindgebruikers geholpen worden met hun (keten)uitdagingen, kennisinstellingen hun kennis kunnen valideren en waarbij bedrijven binnen het Nederlandse veiligheidscluster kunnen floreren. Wij focussen daarbij op kenniscirculatie, 'endorsen' en strategische toegevoegde waarde leveren voor onze premium partners. Dit doen we met onze 'Toegang Tot' propositie in samenwerking met vele partijen vanuit de HSD Campus in Den Haag en in de toekomst vanuit de Nationale Cyber Campus.



We helpen bij het opzetten en vormgeven van het privaat publieke deel van deze nieuwe Nationale Cyber Campus, waar naast het NCSC ook ruimte komt voor publiek-private samenwerking, ondersteund door HSD. Daarnaast bouwen we onze Cyberweerbaarheid- en Talentprogramma's verder uit.

INNOVATIES

We jagen – in triple helix consortia en vanuit het '**secure by design principe**' – innovaties aan die de veiligheid in een digitaliserende wereld vergroten én die mogelijk tot nieuwe Nederlandse economische verdienmodellen kunnen leiden. Zodat nieuwe dienst- en productiecombinaties kunnen ontstaan. Niet alleen op het gebied van cybersecurity, maar juist ook voor allerhande technische producten en systemen met een digitaal verbonden component. Die vervolgens ingezet kunnen worden in krachtige Nederlandse sectoren zoals defensie & veiligheid, slimme steden, smart grids & energietransitie, tuinbouw, hightech en maakindustrie. Dit levert aantoonbare economische waarde, waarop Nederlandse bedrijven wereldwijd het verschil kunnen maken. De eindgebruiker is binnen deze programma's bepalend en HSD treedt op als facilitator. Hierbij focussen we ons altijd - vanuit onze kracht - op verbinden, coördineren en faciliteren.

DRIE PIJLERS

We werken aan drie pijlers met de volgende focus:



SAMENWERKING EN KENNISDELING IN EEN ACTIEF ECOSYSTEEM

- Community management
- Kenniscirculatie
- Toegang tot financiering & kapitaal, talent en (inter)nationale markt
- Internationale positionering



HET ACTIEF LEIDEN EN UITVOEREN VAN PROGRAMMA'S

- Cyberweerbaarheid
- Human Capital
- Nationale Cyber Campus



SMART SECURE INNOVATIE-PROGRAMMERING

- Smart Secure Cities
- Smart Justice & Security
- Smart Secure Grids & Energy Transition
- Smart Secure Defense & Resilience

1. Het speelveld en de rol van Security Delta

Om de toenemende dreigingen in de wereld het hoofd te bieden en op kansen in te spelen is samenwerking tussen publieke, private en kennispartijen noodzakelijk.

Veiligheidsvraagstukken zijn immers complex en grensoverschrijdend. Geen enkele partij lost deze problemen alleen op. Door samen te werken, komen kennis, capaciteit en middelen bijeen. Samenwerken zorgt ook voor begrip en vertrouwen. Iets wat van groot belang is in het veiligheidsdomein en bij digitaliseringsvraagstukken, met name in situaties met ketenafhankelijkheid en complexe verwevenheden. Bovendien ontstaan op het snijvlak van disciplines de beste innovaties. Als publieke, private en kennispartijen hun krachten bundelen, komen vernieuwende ideeën tot stand die sneller worden vertaald naar toepasbare oplossingen.

DE KRACHT VAN SAMENWERKING

Samenwerking in een sterk ecosysteem leidt tot nieuwe bedrijvigheid, versterking van bestaande organisaties en verhoging van de internationale concurrentiekracht van Nederland. Alleen door samen te werken blijven we veilig en weerbaar. HSD faciliteert en stimuleert deze samenwerkingen.



Focus op dual use tijdens het Securing the Future event

STRATEGISCHE CONTEXT

Geopolitieke spanningen, technologische ontwikkelingen en economische onzekerheid vormen risico's voor de maatschappelijke stabiliteit. Hybride dreigingen en digitale sabotage ondermijnen ons vertrouwen in instituties. Tegelijkertijd groeit het besef dat **digitale autonomie** een cruciale rol speelt bij het versterken van onze weerbaarheid. In een wereld waarin controle over (digitale) infrastructuur, standaarden en data steeds vaker onderwerp is van geopolitieke en economische competitie, is strategische autonomie van groeiend belang voor onze weerbaarheid, continuïteit en concurrentiekracht.

KANSEN ÉN RISICO'S

De snelle ontwikkelingen in technologie, zoals AI, privacy enhancing technologies voor datadeling, unmanned systems, digital twinning en quantum, zorgt voor economische kansen, maar ook voor dreigingen en nieuwe complexe digitale & ethische vraagstukken. Aan de ene kant bevordert verdere digitalisering de efficiëntie en verlaagt het de kosten. Doordat werkzaamheden geautomatiseerd worden en AI voor bepaalde werkzaamheden benut kan worden, kan er met minder mensen sneller en slimmer worden gewerkt. Extra economische kansen zijn er voor de (cyber)securitysector, omdat er een groeiende vraag is naar nieuwe diensten en producten en omdat nieuwe technologieën ingezet kunnen worden voor het vergroten van de veiligheid in zowel het civiele als defensie domein, zogenaamde **dual use** of **omni use** in meerdere sectoren. Hierdoor ontstaat een bredere afzetmarkt.

'Dual Use van technologieën zorgt voor bredere afzetmarkten'

Deze inzet is hard nodig, want de digitale risico's voor Nederland zijn groot en divers en houden ook niet op bij onze landsgrenzen. Terwijl fysieke en digitale omgevingen steeds meer verweven zijn – en daarmee ook IT en OT (operationele technologie) – proberen criminele en statelijke actoren te spioneren, saboteren en beïnvloeden. Cyber criminelen blijven op zoek naar manieren om geld te verdienen. De huidige verschuiving van het versleutelen naar stelen van data om losgeld te eisen zal verder doorzetten. Bovendien versterken toenemende geopolitieke spanningen en nieuwe machtsbalansen de hybride dreigingen en vergroten ze de economische onzekerheid. Daarmee groeit ook het belang van digitaal beleid, strategische autonomie en cybersecurity als fundament voor nationale veiligheid, weerbaarheid, continuïteit en concurrentiekracht.

Maatschappelijke en stedelijke veiligheid is een thema van alle tijden. De afgelopen jaren zien we wel verschuivingen in het type criminaliteit. Enerzijds de digitale component in traditionele criminaliteit, anderzijds een toename van cybercrime zoals hiervoor benoemt. Maar ook is er maatschappelijke aandacht voor thema's zoals demonstraties, straatintimidatie, ondermijnende- en drugscriminaliteit. De vraag naar ingrijpen is hoger dan de beschikbare middelen, daarom wordt er gezocht naar andere en meer efficiënte manieren van voorkomen, beïnvloeden en ingrijpen. Onderzoek, inzet van data & technologieën en experimenteren creëren hiervoor de kansen.

Er is en komt toenemende regelgeving en toezicht op adequate beveiliging, maar nog vaak zonder duidelijke normenkaders en achter-

blijvende uitvoeringskracht. Er is daarnaast een tekort aan divers en multi-disciplinair cybersecurity en technologie talent. Bovendien ontbreekt het over de hele linie aan voldoende digitale en weerbaarheidsvaardigheden om de basis op orde te krijgen.

In een snel veranderende wereld met hybride dreigingen groeit de noodzaak van publiek private samenwerking voor veiligheid. Alleen door te investeren in kennis, samenwerking en innovatie, reageren we niet alleen op gevaren, maar worden we ook weerbaar en wendbaar voor wat komen gaat. Zonder assertief, wendbaar en doordacht gebruik van technologie lopen we achter de feiten aan.

ANDERE MANIER NODIG

Maar technologische oplossingen alleen zijn niet voldoende. Het vraagt om een fundamenteel andere manier van denken en doen: creatief, inclusief en grensverleggend. Succesvolle innovatie in het veiligheidsdomein vereist samenwerking in ecosystemen waarin overheid, bedrijfsleven én kennisinstellingen gelijkwaardig bijdragen. Als we niet innoveren en samenwerken, kunnen we niet beschermen wat ons dierbaar is.

ROL SECURITY DELTA

Publiek-private samenwerking klinkt makkelijk, maar gaat niet vanzelf. Al dertien jaar heeft HSD ervaring met het aanjagen en faciliteren van dit soort samenwerkingen. Niet op papier maar in de praktijk. We hebben gemerkt op zowel de HSD Campus, bij de Cybersecurity Week/ONE Conference als ook in de cyberwarroom tijdens de NAVO summit, dat nabijheid helpt om samen te werken en te werken aan vertrouwen. Iets wat juist in het cybersecurity en digitale veiligheidsdomein belangrijk is. Het vormen van een Nationale Cyber Campus in Den Haag en een federatief stelsel van regionale hubs en labs zal hieraan een belangrijke bijdrage gaan leveren.

‘Als we niet innoveren en samenwerken, kunnen we niet beschermen wat ons dierbaar is’

SECURE BY DESIGN

Een veilige en weerbare samenleving is een randvoorwaarde voor een bloeiende economie en brede welvaart. Daarom zijn economie en veiligheid twee kanten van dezelfde medaille: ‘**secure by design**’ zorgt voor weerbaarheid én voor groei van security bedrijven. Samenwerken en innovatie zijn – zowel technologisch als sociaal – essentieel voor het waarborgen van veiligheid in een snel veranderende wereld. Dit alles vraagt om bewuste keuzes in technologie en digitale autonomie. Hierbij vormen **afsprakenstelsels**, **standaarden**, **interoperabiliteit** en **steward ownership** strategische instrumenten.



2. De ambitie van Security Delta

**Security Delta helpt kansen te benutten en risico's het hoofd te bieden.
Deze ambitie realiseren we door de komende jaren te werken aan 3 pijlers.**



SAMENWERKING EN KENNISDELING IN EEN ACTIEF ECOSYSTEEM

We organiseren en activeren het ecosysteem en zorgen via onze 'toegang tot'- propositie voor een vruchtbare voedingsbodem waar bedrijven, overheden en kennisinstellingen kunnen floreren en groeien. We zorgen voor kennisdeling binnen en buiten het ecosysteem. Daarmee vergroten we het inzicht in de risico's en kansen van verdergaande digitalisering voor de veiligheid van de samenleving. Daarnaast positioneren we het Nederlandse veiligheidscluster internationaal voor het helpen aantrekken van bedrijven en congressen.



HET ACTIEF LEIDEN EN UITVOEREN VAN PROGRAMMA'S

We zorgen dat nieuwe ontwikkelingen van de grond komen en helpen bij de uitvoering ervan. Dit doen we in samenwerking met verschillende partners voor de programma's Cyberweerbaarheid, Human Capital en de Nationale Cyber Campus.



SMART SECURE INNOVATIE-PROGRAMMERING

We 'orkestreren' innovaties en ketendoorbraken die als doel hebben de (digitale) veiligheid te vergroten. Het gaat om valorisatie, crossovers, technologietransfer en het benutten van businesskansen binnen de triple helix. Er is een duidelijke (keten) van eindgebruikers betrokken. Zij bepalen de koers en wij coördineren en programmeren met hen. Dit passen we toe rondom sectoren: Smart Secure Cities, Smart Justice & Security, Smart Secure Grids & Energy Transition, Smart Secure Defense & Resilience.

KRACHTEN BUNDELEN: DOELEN BEREIKEN

Een **bloeiend** en **open ecosysteem** is een voorwaarde om als Security Delta succesvol te kunnen zijn in het delen van kennis en stimuleren van innovatie. Een levendig ecosysteem helpt publieke, private en kennispartijen te floreren. Het creëert een omgeving waarin iedereen inhoudelijke kennis kan halen en brengen. Dit helpt om de nationale versnippering in aanpak tegen te gaan.

Bedrijven worden daarnaast geholpen in hun groei, door hen de weg te wijzen naar talent, samenwerkingspartners, financierings- en internationaliseringsmogelijkheden.

Overheden krijgen toegang tot de nieuwste ideeën, marktkennis en technologieën. Zij kunnen vanuit verschillende invalshoeken input krijgen op publieke veiligheidsvraagstukken. Bovendien kan via het ecosysteem het bereik van beleidsmaatregelen worden vergroot.

De innovatiekracht, efficiency en impact van het werk van **kennispartijen** wordt vergroot door de koppeling te maken met bedrijven en overheden. Het leidt tot meer impact en valorisatie.
In het veiligheidscluster bereiken publieke, private en kennispartners hun **eigen doelstellingen**. Zij zorgen **gezamenlijk** dat kennis en technologie sneller leiden tot oplossingen die de concurrentiekracht van onze samenleving vergroot, niet alleen voor vandaag maar ook voor de toekomst. HSD zorgt voor de randvoorwaarden.

GEZAMENLIJKE STRATEGIE

HSD ziet de toekomst met vertrouwen tegemoet en heeft met vele partners en stakeholders aan deze meerjarenstrategie gewerkt. De RvA, RvT, HSD Office medewerkers, gemeente Den Haag en Provincie Zuid-Holland en Rijksoverheid zijn meegenomen in het proces en ook het partnertevredenheidsonderzoek en evaluatieresultaten van de vorige strategieperiode zijn benut.

We weten dat een strategie niet in beton gegoten kan worden. We groeien mee of veranderen met de realiteit om ons heen. Met flexibiliteit en weerbaarheid kunnen huidige en toekomstige uitdagingen het hoofd worden geboden. Samenwerking ontstaat alleen als het vertrouwen en de basis goed zijn. Dit is een vruchtbare bodem waarop nieuwe ideeën kunnen ontkiemen en tot volle wasdom komen. Het vergde jarenlange voorbereiding, kennis, kapitaal en tomeloze toewijding van het hele veiligheidscluster om deze vruchtbare bodem te laten ontstaan. Maar daardoor kunnen we de komende jaren gezamenlijk werken aan verdere groei van ideeën, kennis, producten, diensten en banen.

LOKALE, REGIONALE EN (INTER)NATIONALE BELEIDSVERBONDENHEID

De HSD-aanpak is verbonden met lokale, regionale, nationale en EU-strategieën, agenda's en beleid. Met Den Haag als internationale stad van Vrede & Recht en het Haagse economie programma en programma 'werken, leren en innoveren' is HSD verbonden. Net als met de Groei Agenda Zuid-Holland en nieuwe versnellingsprogramma daarvan.
En op nationaal niveau met de Nationale Technologie Strategie (Cyber, AI en Quantum), **Wennink Rapport**, Innovatie agenda met de 3% norm, Kennis en Innovatie Agenda Veiligheid, Topsector ICT Internationalisering & talent agenda's, de Nationale Digitalisering Strategie, Nationale Cyber Security Strategie, Defensie Industrie Agenda en Nationale weerbaarheidsinitiatieven.

Deze aanpak is ook slim verbonden aan het **Draghi rapport** en met de EU-prioriteiten op het gebied van zogeheten twin transitions: groen én digitaal, duurzaam én veilig, cyberinitiatieven én defensie. De ambitie: "Een versnelde energietransitie helpt ons om onafhankelijk te worden van Russisch gas en olie uit het Midden-Oosten. Meer investeringen in kunstmatige intelligentie en cybertechnologie vergroten onze weerbaarheid op het gebied van veiligheid en defensie. Beiden kunnen zorgen voor meer autonomie. Kennisinstellingen én bedrijven via ecosystemen spelen samen een grote rol in het onderzoeken van deze mogelijkheden en het doorvertalen naar innovaties." HSD speelt hierin haar rol.



Marktconsultatie

Positionering Security Delta

Security Delta is een **non-profit** organisatie met dertien jaar ervaring. Zo'n driehonderd bedrijven, overheden en kennisinstellingen zijn als partner bij ons aangesloten. Zij delen met ons de overtuiging dat veiligheid in een digitaliserende samenleving alleen wordt vergroot als we krachten bundelen.

De publieke, private en kennisorganisaties die deel uit maken van ons ecosysteem komen uit het hele land. Veiligheid en weerbaarheid zijn nationale thema's. Security Delta heeft dan ook een **nationale focus**. Wel zijn we sterk(er) **verankerd in Zuid-Holland**. Soms starten wij vanuit die verankering vanuit ons ecosysteem in Zuid-Holland, werken we nadrukkelijk samen met andere regio's en schalen we daarna landelijk op. In andere gevallen werken we vanuit onze partners en publieke nationale eindgebruikers aan nationale programmering. Onze fysieke werkplek bevindt zich in en verbindt zich bovendien aan de stad van 'vrede, recht en veiligheid', Den Haag.

Op dit moment werken we vanuit de HSD Campus in Den Haag. In de toekomst verhuizen we naar de Nationale Cyber Campus, die eveneens in Den Haag zal worden gevestigd. Deze nieuwe campus wordt niet alleen een fysieke plek met een gesloten overheidsgedeelte en een publiek private actieve community, maar ook een federatief netwerk van samenwerkende hubs en labs. Er wordt daarbij nauw samengewerkt met belangrijke technologiegebieden rond Eindhoven/Brainport en Apeldoorn/Twente.

Zuid-Holland, en met name Den Haag, vormt het centrum van cybersecurity in Nederland. Dankzij de nabijheid van de technologische omgeving van TU Delft en sterke sectoren als maakindustrie, maritieme industrie, energie, tuinbouw en defensie/dual-use, is hier een stevige basis aanwezig voor innovatie en samenwerking.

Daarnaast wordt samengewerkt met technologiehubs in andere regio's, zoals:

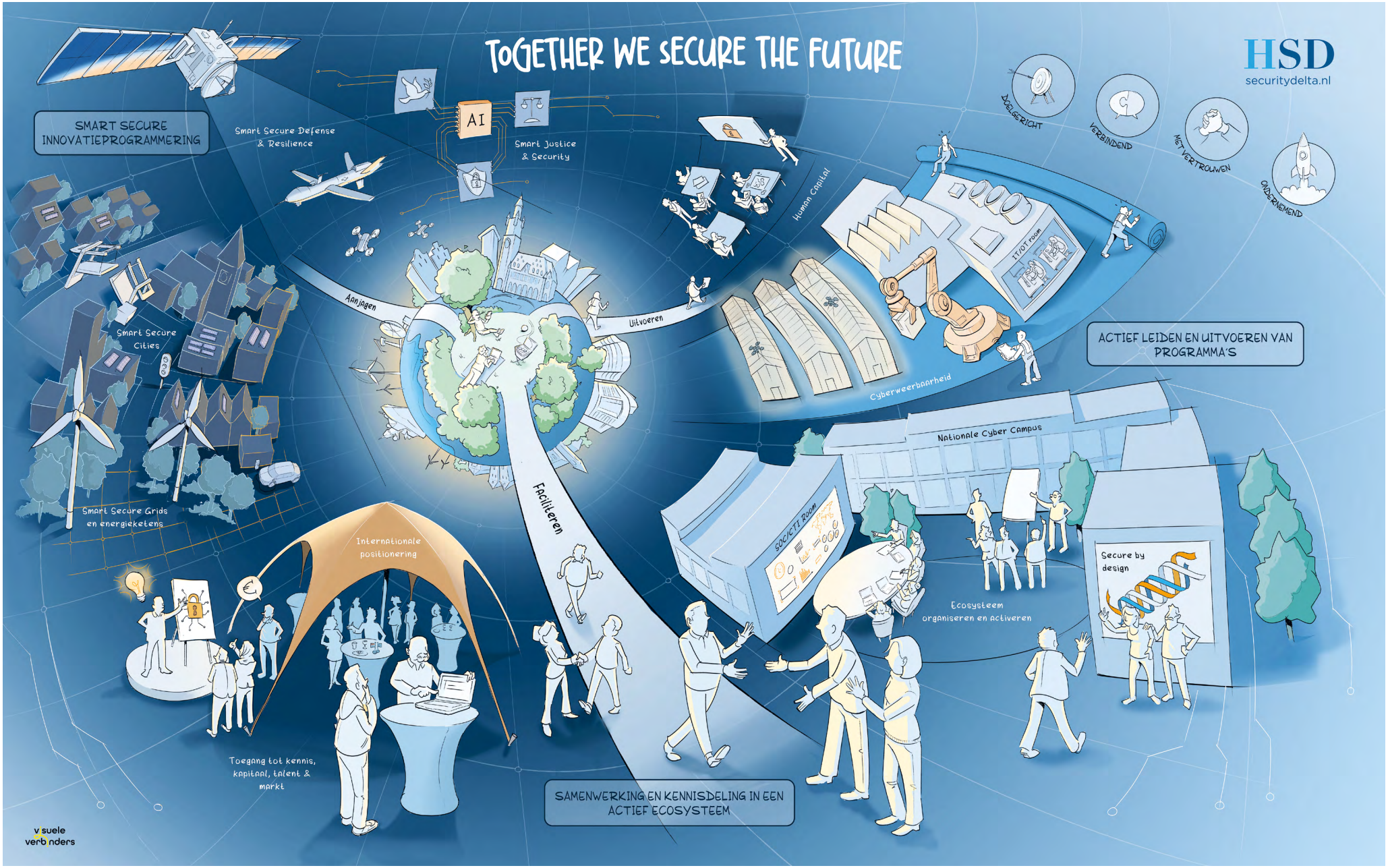
- Eindhoven / Brainport – met onder meer het Cyberweerbaarheidscentrum en het Brabant House of Cyber (in oprichting);
- Apeldoorn / Twente – met het Centrum voor Veiligheid & Digitalisering en diverse onderwijsinstellingen.
- Ook wordt in een nationaal-regionaal stelsel samengewerkt binnen het cyberweerbaarheidsnetwerk met diverse test-, field- en living labs van MBO-HBO- en WO-instellingen die zich bezighouden met (digitale) veiligheid.

HSD is en blijft een neutrale en onafhankelijke organisatie die in staat is om over grenzen heen te denken. Niet alleen over de grenzen van organisaties, sectoren en disciplines, maar ook over politieke en geografische grenzen. We zijn een **verbinder** van verschillende werelden en maken nieuwe combinaties die anders niet ontstaan.

Als relatieve buitenstaander kunnen we vrijer dromen, creëren en experimenteren. We zijn **aanjagers** van innovatie en werken aan **uitvoeringskracht**. Daarin treden we op als onpartijdige **facilitator**, omdat wijzelf niet een direct belang hebben. Zo ontstaan activiteiten, programma's en samenwerkingen die er zonder onze inzet en kennis niet (zo snel) zouden zijn.

Meer over onze rollen en werkzaamheden staat in hoofdstuk 4: 'Aanpak'.




TOGETHER WE SECURE THE FUTURE
HSD
securitydelta.nl
SMART SECURE INNOVATIEPROGRAMMERING
Smart Secure Defense & Resilience
AI
Smart Justice & Security
Human Capital
DOELGERICHT
VERBINDEND
METVERTROUWEN
ONDERNEMEND
Smart Secure Cities
Aanjagen
Uitvoeren
IT/OT room
ACTIEF LEIDEN EN UITVOEREN VAN PROGRAMMA'S
Cyberweerbaarheid
Nationale Cyber Campus
SOC/CT Room
Smart Secure Grids en energieketens
Internationale positionering
Faciliteren
Secure by design
Ecosysteem organiseren en activeren
Toegang tot kennis, kapitaal, talent & markt
SAMENWERKING EN KENNISDELING IN EEN ACTIEF ECOSYSTEEM
v suele verb nders

3. Doelstellingen & Focus

De komende 5 jaar werkt HSD aan drie pijlers met de volgende focus:

1 SAMENWERKING EN KENNISDELING IN EEN ACTIEF ECOSYSTEEM

- Community management
- Kenniscirculatie
- Toegang tot financiering & kapitaal, talent en (inter)nationale markt
- Internationale positionering

2 HET ACTIEF LEIDEN EN UITVOEREN VAN PROGRAMMA'S

- Cyberweerbaarheid
  - Cyberweerbaarheidscentrum Greenport
  - Cyberweerbaarheidscentrum Maakindustrie Zuid-Holland
  - Roadmap cybersecurity Zuid-Holland
  - OT Security (IPCS)
- Human Capital
  - EU/NL talentprogramma CADMUS
  - IT Verband Zuid-Holland
  - Doorontwikkeling SecurityTalent.nl
  - Human Capital Agenda Security
  - International Cybersecurity Summer School
- Nationale Cyber Campus

3 SMART SECURE INNOVATIE-PROGRAMMERING

- Smart Secure Cities
- Smart Justice & Security
- Smart Secure Grids & Energy Transition
- Smart Secure Defense & Resilience

- Deze focus betekent dat we **koers houden**.
- Wel richten we ons meer op **impact maken**.
- Waar we goed in zijn **breiden** we verder **uit** en **schalen** we **op**.
- We **duiden** onze rol per doel en programma's scherper en hebben daarbij oog voor een meerjarige en robuuste financieringsbasis voor deze activiteiten, zodat we ook in de toekomst onze (**gezamenlijke**) **belofte** kunnen blijven **waarmaken**.

Hiena lichten we onze focus en hieraan gekoppelde doelstellingen toe. We geven ook aan wat onze strategische prioriteiten zijn voor de komende jaren. Wat dit betekent voor onze rolinvulling en wat we exact doen, staat beschreven in het volgende hoofdstuk.



Pijler 1

Samenwerking en kennisdeling in een actief ecosysteem

1a. Community Management: Ecosysteem organiseren en activeren
Een actieve bijdrage van de partners in het netwerk zorgt voor duurzamere relaties en vertrouwen, en versterkt het ecosysteem. De ervaring leert dan ook dat betrokken organisaties tevredener zijn. We activeren partijen in het ecosysteem door het organiseren van ontmoetingen, netwerk- & kennisbijeenkomsten en matchmaking. Ook mede-organiseren we de Cybersecurity Week en houden we partners op de hoogte van nieuws, ontwikkelingen en mogelijkheden. Dit doen we vanaf de HSD Campus in Den Haag op basis van de HSD partnerpropositie, zie bijlage 4.

In ons actieve en open ecosysteem is ruimte voor elke professional in het digitale veiligheidsdomein. Organisaties kunnen deelnemen zolang ze een juridische entiteit in Nederland hebben en de Rijksoverheid geen belemmeringen oplegt. Met elkaar maken we het veiligheidscluster HSD en werken we toe naar een Nationale Cyber Campus (zie 2c).

Doelstelling: *Stabiel ecosysteem versterken en activeren: meer partijen zijn actief betrokken in het netwerk en het netwerk bruist.*

1b. Kenniscirculatie
Binnen het ecosysteem van Security Delta zit een schat aan kennis. De nieuwste ontwikkelingen, innovaties en trends op het gebied van veiligheid in een digitaliserende wereld komen van onze partners. Dit gaat onder andere over Cybersecurity technologieën, riskmanagement, AI, GPT.NL, Quantum technologie en post quantumproof Cybersecurity, Secure data sharing, Privacy Enhancing Technologies, eID, data diodes, unmanned systems&drones en dual & omni use technologieën.

Deze kennis willen we bijeenbrengen, ontsluiten en verspreiden. Kennisdeling is immers cruciaal voor betere innovaties en efficiëntere uitvoering. We integreren een fysieke en digitale aanpak. Zo organiseren we thematische kennissessies maar onderhouden we ook een digitaal platform: securityinsight.nl. De inhoud staat altijd centraal.

Doelstelling: *We bouwen de kennisprogrammering uit en faciliteren kenniscirculatie. Onze partners en wijzelf staan regelmatig op podia om inhoudelijke kennis te delen.*

1c. Toegang tot financiering & kapitaal, talent en (inter)nationale markt
We versterken en dragen bij aan groei van bedrijven. Organisaties met innovatieve ideeën koppelen we aan en richten we op financieringsbronnen. Startups verbinden we aan accelerators. Startups en scale-ups die op zoek zijn naar kapitaal verbinden we aan investeerders. We helpen organisatie met hun groei door middel van securitytalent.nl via het plaatsen van vacatures, arbeidsmarkt positionering, endorsen van Talent events en verbindingen leggen tussen onderwijsinstellingen, organisaties en arbeidsmarktbemiddelaars. Bedrijven die de internationale markt willen betreden helpen we op weg naar handelsprogramma's en -missies.We organiseren niet langer zelf internationaliseringsprogramma's, maar wijzen wel de weg ernaartoe. Door kennis en kennissen te delen, helpen we met het opschalen van innovaties en het uitvoeren van groeistrategieën.
Het faciliteren van startups, scale-ups en innovatieve mkb'ers in hun (inter)nationale groeiambities, levert uiteindelijk banen op.

Doelstelling: *We communiceren actiever over mogelijkheden op gebied van talent financiering en internationalisering. We organiseren bijeenkomsten waarin kennis wordt gedeeld en vraag & aanbod op dit terrein wordt gekoppeld.*

Een belangrijk deel van de uitvoering op het gebied van financiering en internationalisering ligt bij de economische taakorganisaties: RVO (waaronder NCC-NL) en de ROMs (waaronder InnovationQuarter en The Hague Business Agency).



Pijler 1

Samenwerking en kennisdeling in een actief ecosysteem

1d. Internationale positionering HSD

Een actief ecosysteem met een fysieke plek heeft grote aantrekkingskracht op organisaties die interesse hebben om zich in Nederland te vestigen. Meer bedrijvigheid zorgt voor meer banen en dat trekt weer talent aan. Nationaal en internationaal positioneren we het ecosysteem, door inkomende handelsmissies van bedrijven en overheden te ontvangen. We helpen daarmee Nederland te positioneren en internationale bedrijven en congressen aan te trekken. Zo ondersteunen we regionale ontwikkelingsmaatschappijen (InnovationQuarter en The Hague & Partners in het bijzonder) en de Netherlands Foreign Investment Agency (NFIA) in hun acquisitie-doelstellingen. We voeren niet meer zelf handelsmissies en/of PiB consortia uit. We nemen deel aan internationale handelsmissies als dat een meerwaarde heeft voor de verdere positionering van het ecosysteem. Ook ontvangen we inkomende handelsdelegaties op de HSD Campus en geven we het ECSO cybersecurity made in Europe label uit. We communiceren actief over de partijen in het netwerk en de ambities die we nastreven.

Doelstelling: *De bekendheid en daarmee aantrekkingskracht van het ecosysteem neemt verder toe in het buitenland, zodat de strategische acquisitie partijen hun targets kunnen behalen.*

WAAR LIGT ONZE FOCUS?

De wereld is groot en cybersecurity en digitale veiligheidsrisico's en kansen spelen overal. Wij verbinden onze connecties rondom innovatiesamenwerking, acquisitie-belangen en handelsbevordering voor Nederlandse bedrijven.

De focus van onze werkzaamheden ligt op inhoudelijke en innovatie samenwerking. Voor acquisitie en handelsbevordering verbinden we onze kennis en connecties aan IQ, ROM NL, RVO/NFIA en de handelsposten van Nederlandse ambassades.

Onze internationale inzet is gebaseerd op opgebouwde relaties, strategische afwegingen en de prioriteiten van Digital Holland (voormalig Topsector ICT). Dit resulteert in een gelaagde internationale prioritering, waarmee HSD bij-draagt aan de versterking van de Nederlandse positionering op het gebied van cybersecurity en digitale veiligheid.

FOCUSLANDEN

1. Duitsland, Frankrijk, Zweden, USA, Taiwan en Singapore
2. België, Denemarken, UK, Ierland, Spanje, Tsjechië, Oekraïne, India en Canada
3. Slowakije, Hongarije, Kroatië, Griekenland, Estland, Litouwen, Finland, Polen, Zwitserland, Portugal, Italië, Japan en Korea



Pijler 2

Het actief leiden en uitvoeren van programma's

Op drie belangrijke thema's hebben we als HSD een actieve leidende rol bij het opzetten én de uitvoering van het programma. We identificeren kansen, brengen het potentieel in kaart, smeden nieuwe coalities, helpen programma's ontwikkelen en waar nodig uitvoeren. Onze strategische & inhoudelijke domeinkennis en uitvoeringskracht maken dat we in dit soort processen het verschil kunnen maken. We werken actief mee en staan dus met onze voeten stevig in de klei.



Lancering Cyberweerbaarheidscentrum Maakindustrie Zuid-Holland

2a) Cyberweerbaarheid

We willen de komende jaren doorgroeien naar een belangrijke rol in een landelijk cyberweerbaarheidsnetwerk. De niet vitale maar essentiële sectoren en het mkb zijn in Nederland op het terrein van cybersecurity nog te kwetsbaar. We zijn van mening dat een sectorale aanpak het verschil kan maken, met én voor de sector, startend in de regio om daarna landelijk op te schalen. Thema's en projecten voor de komende jaren:

- Cyberweerbaarheidscentrum Tuinbouwsector
- Cyberweerbaarheidscentrum Maakindustrie Zuid-Holland
- Roadmap cybersecurity Zuid-Holland, waaronder samenwerking met de Europese Digitale Innovatie Hubs (EDIHs)/Digitalzh
- OT-security (IPCS)

Doelstelling: *Onze succesvolle regionale cybersecurity- en weerbaarheidsinitiatieven schalen we landelijk op. (Inter)nationale ontwikkelingen vertalen we in concrete innovatieprogramma's.*

2b) Human Capital

Organisaties in het veiligheidsdomein zijn voor hun groei en succes afhankelijk van de beschikbaarheid van vaardige medewerkers. Het aanbod van securitytalent is en blijft schaars, zelfs in die mate dat het tekort zélf een bedreiging vormt van onze veiligheid. Daarom is het organiseren van toegang tot talent één van onze speerpunten.

We willen onze deskundigheidspositie nationaal en internationaal verder uitbouwen in de komende jaren. Nationaal worden we gezien als de kennispartij op het terrein van security talent. Nieuwe en concrete talentprogramma's worden aan de cyberweerbaarheidscentra en de bredere regionale en nationale ICT Human Capital Agenda's (HCA) gekoppeld. Hiervoor trekken we extra subsidiegelden aan. Daarnaast breiden we onze positie internationaal uit. Er komen nieuwe internationale samenwerkingen tot stand met Europees en nationaal geld. Nederland wordt daarmee internationaal beter op de kaart gezet op het terrein van talent en arbeidsmarkt voor (cyber)security.

Doelstelling: *Het aantal talentprogramma's groeit en daarmee ook de investeringen die we hiervoor organiseren. We schalen bestaande successen op. Securitytalent.nl wordt doorontwikkeld tot hét nationale platform.*

Projecten en programma's waaraan we de komende jaren in ieder geval aan werken:

- IT Verband Zuid Holland (ITVZH) project (€17 miljoen*)
- CADMUS; EU/NL Cybertalent project (€ 6.3 miljoen*)
- Doorontwikkeling van securitytalent.nl als hét Nederlandse talent platform
- Ontwikkelen nieuwe Human Capital Agenda Security 2027-2030
- International Cybersecurity Summer School (ICSS)

**Deze uitgelokte investeringen gaan niet enkel naar HSD als organisatie zelf, maar ook naar de coalitiepartners en helpt om met en via onze partners onze doelstelling te behalen.*


International Cybersecurity Summer School

Pijler 2

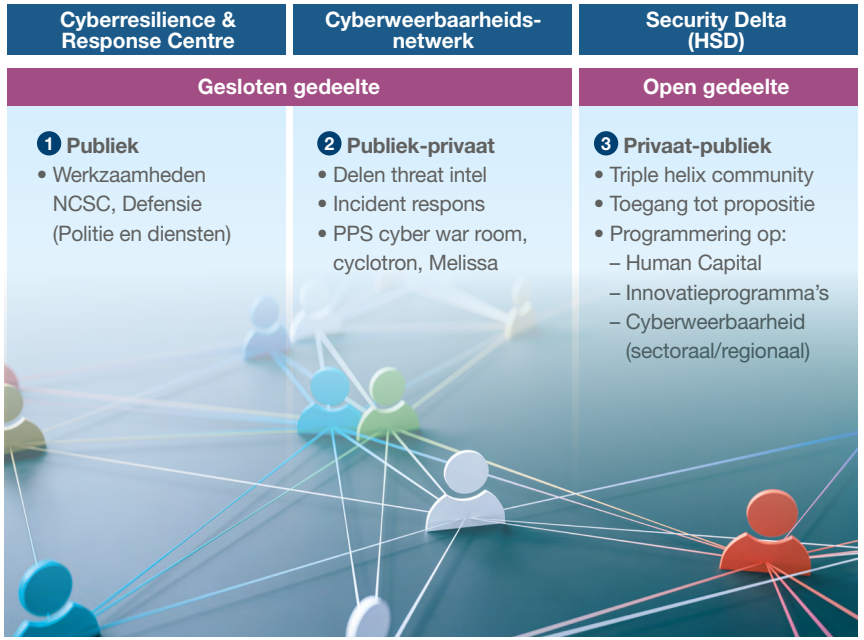
Het actief leiden en uitvoeren van programma's

2c) Nationale Cyber Campus
We hebben als Security Delta zo'n dertien jaar ervaring in het organiseren van een veiligheidsnetwerk. Daarnaast dragen we met de gemeente Den Haag bij aan de HSD Campus. Deze is inmiddels uitgegroeid naar een broedplaats van digitale veiligheidsorganisaties, van startups tot gevestigde spelers, die allemaal de geest van 'veiligheid en samenwerking' delen.
Deze ervaring willen we inzetten op nationaal niveau in een landelijke Cyber Campus ('House of Cyber'). Het Nationaal Cyber Security Center (NCSC) groeit en zal verhuizen. Op de nieuwe locatie in Den Haag wordt ruimte georganiseerd voor publiek private samenwerking. Dit krijgt vorm in een Cyber Campus. Door ook fysiek dicht bij elkaar te zitten, worden drempels voor samenwerking weggenomen.

Het uitwisselen van dreigingsinformatie en de vertaling naar cyberweerbaarheids-toepassingen zal vanuit de kernwerkzaam-heden van het NCSC uitgevoerd worden. Security Delta zal hieromheen het campus-management en de publiek private uitvoering van de 'toegang tot' propositie op zich nemen; kennis, innovatie, kapitaal, talent en markt. Deze Nationale Cyber Campus is de schakel van een federatief stelsel met lokale labs, regionale hubs en campussen. Het opzetten en organiseren van de nieuwe Campus wordt een uitdaging die veel werk vraagt.
We bereiden ons komende jaren voor op de transitie en ontwikkeling van de campus. Als ons te zijner tijd de uitvoeringsrol wordt gegund, nemen we die verantwoordelijkheid op ons. Daarbij zorgen we dat er duidelijke financiële voorwaarden en solide afspraken over risicobeheersing zijn gemaakt met de andere hoofdpartijen.

Doelstelling: *Helpen opzetten en vormgeven van de Nationale Cyber Campus. We voeren te zijner tijd het campus community management uit en coördineren de logistieke en facilitaire zaken die daarbij komen kijken.*

Opzet Nationale Cyber Campus





Pijler 3

Smart Secure Innovatieprogrammering

We ‘orkestreren’ innovaties en ketendoorbraken die bijdragen aan het vergroten van (digitale) veiligheid. Dit gebeurt op basis van een sterke kennisbasis, met als doel het bevorderen van kennisvalorisatie en technologie transfer, én het creëren van nieuwe businesscases. Daarbij onderzoeken we mogelijke cross-overs naar andere sectoren en zoeken we naar financieringsmogelijkheden.

Systeem en ketendoorbraken
De inzet van technologie voor systeem- en ketendoorbraken is ons uitgangspunt. Er vallen programma’s binnen die gericht zijn op de inzet van nieuwe technologie voor veiligheid, zoals AI, quantum en drones en dan in een specifiek toepassingsdomein. Er is een duidelijke (keten) van eindgebruikers betrokken. Zij bepalen de koers en wij coördineren en programmeren met hen.

We werken aan de volgende programma’s:
- Smart Secure Cities (steden en politie)
- Smart Justice & Security (JenV en strafrechtketen, Politie, NFI, OM)
- Smart Secure Grids en energieketens (Innovatiecoalitie Cyberveilige Energietransitie)
- Smart Secure Defense & Resilience (Defensie/dual use)

3a) Smart Secure Cities (steden en politie)
We willen de komende jaren doorgroeien Met 6 gemeenten (Den Haag, Rotterdam, Amsterdam, Almere, Apeldoorn en Eindhoven), VNG, Politie -zowel vanuit de regio als nationaal niveau- voeren we het meerjarig programma van de Impact Coalitie Safety & Security uit via onze rol. Meer dan 100 betrokken partijen werken aan jaarlijks aan 15-20 innovatieprojecten. De programma’s richten zich op de inzet van data en nieuwe technologieën voor de openbare orde en (digitale) veiligheid in steden. Thema’s die hierbinnen aan bod komen zijn onder andere crowd management, cameratoezicht en geluidssensoren, inzet en bestrijding van drones, veilig data delen en de ethische, sociaal maatschappelijke en privacyvraagstukken in slimme veilige steden.

Ook is er samen met diverse kennisinstellingen een uitvoeringsprogramma rondom een onderzoeksagenda en neemt het ELSA (Ethical, Legal, Social, Aspect) lab deze kennis mee bij de ontwikkeling van veilige slimme steden.

3b) Smart Justice & Security (JenV en strafrechtketen, Politie, NFI, OM)
Het programma Smart Justice & Security is een voortzetting van het triple helix AI-programma met bijhorende sub eco-systeem in opdracht van het ministerie van Justitie en Veiligheid (programma directies AI en X rondom kennis&innovatie&strategie) en afzonderlijke acties op verzoek van de politie, het OM en Nederlands Forensisch Instituut (NFI). Zoals bijvoorbeeld voor het OM bezien of een Cybersecurity Schadefonds zinvol en haalbaar is.

We pakken onze rol vanuit de werkgroep Vrede, Veiligheid en Recht verder op. Zo’n 110 betrokken professionals vormen deze werkgroep waarbij om de 6 weken een bijeenkomst is waarbij kennis, vragen en mogelijkheden rondom events en financieringen gedeeld worden. Met als doel het samenbrengen van relevante Nederlandse spelers om effectieve, veilige en verantwoorde AI-toepassingen te ontwikkelen en in te zetten voor veiligheid, vrede en een goed functionerend rechtssysteem. De basis hiervoor en focus daarbij is het rapport ‘AI-toepassingen voor veiligheid, vrede en recht’ dat HSD destijds samen met NLAIC in opdracht van J&V heeft geschreven.

Belangrijke thema’s hierbij zijn:
- Privacy bestendig data delen
- AI, data en intelligence voor beslisondersteuning
- AI voor cybersecurity en (cyber)security van AI
- Gebruik van taal- en spraaktechnologie





Pijler 3

Smart Secure Innovatieprogrammering

3c) Smart Secure Grids & Energy Transition
Een nieuw programma dat is opgestart gaat in op de ontwikkeling van veilige technologie: 'secure by design'. Het programma is geïnitieerd door de Innovatiecoalitie Cyber-veilige Energietransitie, bestaande uit 10+ partijen. De gezamenlijke ambitie is dat Zuid-Holland de voortrekkersrol pakt in een energievoorziening die vanaf het ontwerp veilig, betrouwbaar én interoperabel is: *secure by design*. Zodat dit daarna in Nederland opgeschaald kan worden.

Digitalisering, nieuwe innovatieve producten in de keten en decentrale energiesystemen zijn een oplossing voor die transitie en bijvoorbeeld ook voor netcongestie, maar creëren ketenuitdagingen en cyberrisico's. Met dit programma willen we de weerbaarheid van het digitale energie-ecosysteem verhogen en de energietransitie versnellen.

De coalitie is opgericht door Economic Board Zuid-Holland, TNO, TU Delft, KPN, Stedin, Batenburg Techniek, Technolution, the Green Village, Provincie Zuid-Holland, IQ en HSD in samenwerking met Havenbedrijf Rotterdam, Westland infra, DIVD, ENCS, Greenport West-Holland, Topsectoren ICT en energie, gemeente Den Haag, TU PowerWeb Institute, Living Lab Scheveningen, Campus@Sea, Duurzaamheidsfabriek en Hi-Delta.

3d) Smart Secure Defense & Resilience (Defensie/dual use)
Vanuit Europa komt niet alleen veranderende regelgeving maar ook een groeiend besef voor de noodzaak van publiek-private samenwerking voor complexe nationale veiligheidsopgaven. De defensie-uitgaven van de lidstaten gaan omhoog en daarmee de investeringen in oplossingen die een dubbele inzetbaarheid hebben voor zowel veiligheid als samenleving. We onderzoeken hoe wij hierin een rol kunnen spelen en pakken een rol als dit een meerwaarde vervuld en impact maakt.

Een potentieel programma gaat over dual use en omni use technologieën. We werken het bestaande partnership met het Ministerie van Defensie (Cyber innovation hub en FRONT) samen met de contacten van COMMIT en Mindbase uit tot een programma. Naast de rol die defensie gaat spelen in Nationale Cyber Campus. We sluiten aan bij Provincie Zuid-Holland/Economic Board Zuid-Holland, InnovationQuarter, ROMs Nederland en NIDV, zodat we kunnen werken aan een deelecosysteem waarin technologie, ondernemerschap en strategische autonomie samenkomen. Met initiatieven zoals het SecFund, MindBase, ODIN, Yes!Delft, SeaSEC en NATO Diana ondersteunen we innovatieve mkb's, startups en scaleups die werken aan dual use technologieën en innovaties die zowel in civiele als militaire domein inzetbaar zijn. Ook leveren een bijdrage bij de organisatie van het 'Securing the Future event' in Den Haag. Dit alles doen we in nauwe verbondenheid met de regio's Brabant en Oost-Nederland.

Doelstelling: *We starten nieuwe programma's die gericht zijn op veiligere technologie en de verantwoorde inzet van technologie voor veiligheid in de praktijk en (ketens) van toepassingsgebieden. We schalen bestaande succesvolle programma's en oplossingen op.*

Randvoorwaarden voor realisatie
Om de nieuwe ambities en meerjarendoelstellingen uit dit plan te kunnen realiseren, is meer menskracht en dus meer geld nodig. Wij zien mogelijkheden rondom de nieuwe programma's en een rol ten behoeve van het campusmanagement.

Doelstelling: *Meer financiering regelen waarmee extra capaciteit wordt aangetrokken voor HSD Office voor het behalen van deze strategische doelen en de uitvoering van de programma's.*



4. Aanpak

Een overzicht van onze rollen en werkzaamheden per pijler.

1 Samenwerking en kennisdeling in een actief ecosysteem

Doelstellingen	Onze rollen en werkzaamheden
1a. Community management Stabiel ecosysteem versterken en activeren: meer partijen zijn actief betrokken in het netwerk en het netwerk bruist.	We **onderhouden contacte**n met onze triple helix partners binnen het ecosysteem, houden hen op de hoogte van mogelijkheden en organiseren netwerkactiviteiten. We **maken matches** tussen organisaties waaruit nieuwe samenwerkingen voortkomen. We voeren persoonlijke gesprekken, versturen thematische mails en nieuwsbrieven, organiseren inhoudelijke bijeenkomsten en onderhouden een digitaal platform voor en over het ecosysteem. Om ons werk goed te kunnen blijven doen, brengen we de behoeften binnen het ecosysteem in kaart en spelen we daarop in. Met (potentiële) nieuwe partners voeren we gesprekken en geven we uitleg over het doel en de werkwijze van het ecosysteem. We zorgen dat nieuwe organisaties een onboarding krijgen, gekoppeld worden aan alle activiteiten en geïntroduceerd worden binnen de community, bijvoorbeeld tijdens de netwerkevents en/of via nieuwsbrieven en artikelen. De **HSD Campus** is de fysieke ontmoetingsplek voor het ecosysteem. De levendigheid op de Campus trekt organisaties aan, het inspireert en verbindt.
1b. Kenniscirculatie We bouwen de kennisprogrammering uit en faciliteren kenniscirculatie. Onze partners en wijzelf staan regelmatig op podia om inhoudelijke kennis te delen.	Onze partners en wijzelf geven inhoudelijke presentaties op uiteenlopende podia. Ook organiseren we **kennissessies** en verbinden ons als e*ndorsing partner* aan interessante bijeenkomsten die we promoten in ons netwerk. We houden ons digitale kennisplatform **securityinsight.nl** up-to-date. Het is een platform voor ons netwerk om expertise te etaleren en kennis te delen. Daarnaast organiseren we **marktconsultaties**, waarin publieke, private en kennispartijen samen nadenken over oplossingen voor veiligheidsvraagstukken.

1 Samenwerking en kennisdeling in een actief ecosysteem

Doelstellingen	Onze rollen en werkzaamheden
1c. Toegang tot financiering & kapitaal, talent en (inter) nationale markt We communiceren actiever over mogelijkheden op gebied van talent, financiering en internationalisering. We organiseren bijeenkomsten waarin kennis wordt gedeeld en vraag en aanbod op dit terrein wordt gekoppeld.	We brengen **subsidiemogelijkheden** over het voetlicht, in individuele gesprekken met organisaties en in algemene mailings en nieuwsberichten. We beantwoorden vragen over financieringsmogelijkheden en koppelen organisaties aan NCC NL. Samen met anderen organiseren we kennissessie over financiering en kapitaal en investeerderssessies. We helpen mee om startups te verbinden aan accelerator programma's. En we brengen bedrijven in contact met investeerders. Met partners die op zoek zijn naar **internationale samenwerkingen** voeren we gesprekken. We informeren en communiceren over de internationaliseringsprogramma's, congressen en handelsmissies. Geïnteresseerde partijen verwijzen we naar werkzaamheden van de regionale ontwikkelingsmaatschappijen en RVO. Op verzoek stellen we roadmaps en **marktverkenningen** op waarin we bestaande of nieuwe verkenningen uitvoeren. We peilen daarin de behoefte van de markt, en de mogelijkheden van Nederland om business te doen in een specifieke internationale markt. We ontsluiten via het talentplatform SecurityTalent.nl vacatures, trainingen en opleidingen. Via dit platform bieden we ook een carrière navigator. Partners kunnen hun vacatures en trainingen uploaden en zichtbaar maken. Daarnaast helpen we partners met hun groei via arbeidsmarkt positionering, *endorsen* van Talent events en het leggen van **verbindingen** tussen onderwijsinstellingen, organisaties en arbeidsmarktbemiddelaars.
1d. Internationale positionering De bekendheid en daarmee aantrekkingskracht van het ecosysteem neemt verder toe in het buitenland.	We ontvangen inkomende **handelsmissies**, stellen daarvoor programma's op en geven uitleg over het doel en de werkwijze van het ecosysteem. We koppelen internationale bedrijven aan de regionale ontwikkelingsmaatschappijen (ROM) als ze interesse hebben zich in Nederland te vestigen. Op verzoek van de ROM's spreken we met bedrijven die in Nederland willen landen. We bezoeken internationale congressen en reizen mee met handelsmissies om het ecosysteem te vertegenwoordigen en promoten. Aan internationale samenwerkingsverbanden nemen we deel met eenzelfde doel. We geven interviews en schrijven artikelen over het veiligheidscluster, zodat we de Nederlandse propositie op gebied van cybersecurity helpen **promoten** in binnen- en buitenland.

❷ Het actief leiden en uitvoeren van programma's

Doelstellingen	Onze rollen en werkzaamheden
2a. Cyberweerbaarheid Onze succesvolle regionale cyberweerbaarheidsinitiatieven schalen we landelijk op. (Inter)nationale ontwikkelingen vertalen we naar concrete innovatieprogramma's.	We zetten **sectorale cyberweerbaarheidsprogramma's** op en voeren deze ook uit. We optimaliseren onze bestaande cyberweerbaarheidscentra Greenport en Maakindustrie Zuid-Holland en delen de lessons learned met andere regio's of schalen landelijk op in verbinding met de nieuwe nationale Cyber Campus en het landelijk dekkend stelsel. Binnen de cyberweerbaarheidscentra voeren we het programmamanagement en regelen alles dat hierbij komt kijken. We organiseren **kennissessies**, CISO-sessies, workshops en delen threatintel via Connect2Trust. We maken praktische instrumenten, zoals toolboxen. Met mkb'ers voeren we gesprekken over hun kennis van en behoefte aan cybersecurity. Daarmee helpen we ze om digitaal veiliger te worden. Aan de cyberweerbaarheidscentra zijn websites gekoppeld en die onderhouden we. We zorgen voor **nieuwe content** en voldoende bezoekers om awareness en handelingsperspectief te vergroten. Hiervoor schrijven we sectorgerichte artikelen, nieuwsbrieven en LinkedIn berichten.
2b. Human Capital Het aantal talentprogramma's groeit en daarmee ook de investeringen die we hiervoor organiseren. We schalen bestaande successen op. Securitytalent.nl wordt doorontwikkeld tot hét nationale platform.	We voeren verschillende **talentprogramma's** uit, op Europees, nationaal en regionaal niveau. Hierin pakken we een leidende en coördinerende rol, als we deze positie gegund krijgen. Dit doen we al voor het Europese CADMUS programma en via IT Verband Zuid-Holland. We voeren inhoudelijke analyses en onderzoeken uit én rapporteren daarover. Ook schrijven we meerjarenprogramma's, zo verschijnt elke vier jaar een nieuwe Human Capital Agenda Security. Deze agenda is de basis voor onze activiteiten. Aan deze programma's zijn ook websites gekoppeld, die we onderhouden. Voorbeelden hiervan zijn: **securitytalent.nl**, **cybersecuritywerkt.nl** en **summerschoolcybersecurity.org**. Op Security Talent zijn de vacatures en opleidingen in het securitydomein gebundeld en kun je competentie-gericht je eigen ontwikkelplan vormgeven. Deze ontwikkelen we verder door. Daarnaast organiseren we al meer dan 10 jaar de International Cybersecurity Summer School samen met Europol, NCIA, Univeriteit Leiden en diverse premium partners.
2c. Nationale Cyber Campus Helpen opzetten en vormgeven van de Nationale Cyber Campus. We voeren te zijner tijd het campus community management uit en coördineren de logistieke en facilitaire zaken die daarbij komen kijken.	We helpen mee bij het vormgeven van de **Nationale Cyber Campus** en bereiden ons voor op het uitvoeren van het campusmanagement, bestaande uit de ecosysteem rol alsmede de verhuur, beheer en facilitaire zaken rondom zo'n campus. Het kan ook zijn dat wij hiervoor verantwoordelijkheid nemen, maar de uitvoering uitbesteden. Deze campusrol lijkt ons nu gegund te worden. Er zal wel financiering voor deze uitvoerende rol beschikbaar dienen te komen. Hierover zijn we in gesprek met betrokken partijen. Met deze mogelijke nieuwe rol in de Nationale Cyber Campus krijgen we ook nieuwe taken. We zorgen voor het **community management** rondom de campus en we gaan bezien hoe we het beheer kunnen organiseren (uitbesteden). Daarbij valt te denken aan het bemensen van de receptie, het regelen van ontvangst van gasten, de verhuur van zalen en kantoren en het organiseren van het facilitair management in het gebouw. Omdat een levendige campus meer is dan alleen logistiek, vallen hieronder ook werkzaamheden die zorgen dat Campus bewoners meerwaarde halen uit hun werkomgeving. Er worden periodieke gesprekken gevoerd zodat verbindingen kunnen worden gelegd.

3 Smart Secure Innovatieprogrammering

Doelstellingen	Onze rollen en werkzaamheden
3a. Innovatieprogrammering We starten nieuwe programma's die gericht zijn op veiligere technologie en de verantwoorde inzet van technologie voor veiligheid in de praktijk en (ketens) van toepassingsgebieden. We schalen bestaande succesvolle programma's en oplossingen op.	We voeren **innovatieverkenningen** uit. We praten met organisaties, brengen de mogelijkheden en beperkingen in kaart en schrijven dit op in een bondig rapport. We organiseren rondetafels rondom innovatiethema's (en op basis van verkenningen). We brengen partijen bijeen om samen een innovatie-idee uit te werken, een programma op te stellen, een consortium op te zetten of een subsidieaanvraag in te dienen. We steunen coalities door mee te denken, inhoudelijke feedback te geven of actieve participatie. Met dit werk schrijven we (mee) aan subsidie-aanvragen en zorgen we dat meer geld terechtkomt bij zinvolle innovatieprogramma's. We leveren ook een bijdrage aan nationale strategie en innovatie agenda's. Op het terrein van innovatie zorgen wij dat publieke en private partijen samen werken aan concrete innovatieprogramma's. We zorgen dat bestaande programma's uitgebreid worden en nieuwe programma's worden opgezet. Onze werkzaamheden bestaan uit het voeren van gesprekken zodat nieuwe experts aansluiten op de programma's, het organiseren en voorzitten van overleggen, het voeren van programmamanagement en het uitvoeren van onderzoeken om een programma verder te helpen. Soms bestaat onze rol in een programma meer uit het bepalen van de strategie en soms organiseren we de hele uitvoering. We **coördineren** en **programmeren**, waarbij de (keten van) eindgebruikers bepalend c.q in de lead zijn. Dit doen we op de volgende thema's: • Smart Secure Cities (steden en politie) • Smart Justice & Security (JenV/strafrechtketen Politie, NFI, OM) • Smart Secure Grids & Energy Transition (Innovatiecoalitie Cyberveilige Energietransitie) • Smart Secure Defense (dual use/Defensie)
3b. Extra funding Meer financiering regelen waarmee extra capaciteit wordt aangetrokken voor het behalen van de doelen	Voor deze programma's zoeken we **passende financiering**, zodat we onze gestelde doelen kunnen realiseren.

5. Organisatie

Om bruggen te kunnen bouwen tussen organisaties is vertrouwen in ons team nodig.

HSD is daarbij onafhankelijk en we maken als team samen met onze partners waar wat we beloven. We zijn in staat verbindingen te zien en te maken, snel te schakelen en ideeën om te zetten naar concrete actie, naar resultaat en impact.

De organisatie van Security Delta is '*lean* en *mean*'. Er is weinig overhead en we werken efficiënt en kosteneffectief. Het kleine en toegewijde team heeft veel slagkracht. We combineren inhoudelijke kennis (niet als expert) met procesvaardigen, inzicht in het netwerk en stakeholdermanagement, verbindings-kwaliteiten en verandermanagement skills. Het team biedt de gewenste kwaliteiten als basis voor de strategische ambities, mits we daarbovenop nieuwe financiering en vacatures zouden weten in te vullen.
Het team groeit daarom mee met de ambities van HSD en ontwikkelt zich professioneel door, passend bij de nieuwe fase waarin HSD zich bevindt. Zonder dat hiervoor een wijziging van de organisatiestructuur nodig is. We blijven een platte organisatie met korte lijnen, waarbij verbinding, programmaregie & -orkestratie en community management centraal staat. We continueren onze succesvolle stagiairs/ medewerkers combinatie en de pool van ZZP-ers en mogelijk detacheringen als flexibele schil.

'Het team groeit mee met HSD ambities'



Teamfoto HSD Office

We blijven een lerende organisatie met veel aandacht voor lessons learned en verbinding tussen (programma)inhoud en community/ partnermanagement. We werken continue aan het invullen van 'goed werkgeverschap' en bouwen daarbij voort op ons succesvolle HR-beleid en ons uitgebreide personeelshandboek.

KERNWAARDEN

Onze visie en aanpak komt terug in onze kernwaarden:

- **Verbinden**: Samen komen we verder, door het delen van kennis helpen we elkaar. De successen die we boeken behalen we als team.
- **Doelgericht**: We hebben een helder doel voor ogen, zetten tijd en middelen efficiënt in en houden elkaar scherp. In de resultaten die we boeken staan onze partners centraal.
- **Vertrouwen**: in een veilige omgeving kunnen we leren van fouten en staan we open voor feedback. We werken samen en nemen onze verantwoordelijkheid.
- **Ondernemend**: We pakken op ethisch verantwoorde wijze onze kansen. Bevlogen en gedreven pakken we werk met beide handen aan en zetten waar nodig die extra stap.

We hebben aantoonbare aandacht voor deze kernwaarden en onze professionele en gezonde bedrijfscultuur.

GOVERNANCE

De governance van onze organisatie is goed geregeld. De Raad van Toezicht heeft een formele toezichtstaak. Daarnaast staat zij, in samenwerking met de Raad van Advies, de bestuurder met raad en daad bij. De samenstelling van de leden van de RvT en RvA is divers en representeert het triple helix ecosysteem. Dit bevordert een open en multidisciplinaire blik die gericht is op de toekomst. Twee leden van de RvT zullen na het aflopen van hun 2x4-jarige benoemingstermijn, conform de 'good governance code' vervangen worden.

We optimaliseren onze backoffice en administratie processen. Zowel ten behoeve van ons partnermanagement met behulp van ons CRM-systeem als in voorbereiding tot een uitvoeringsrol bij de nieuwe Nationale Cyber Campus. We stellen AI-beleid en handleiding op om intern duidelijkheid te verschaffen over de kaders waarin we AI benutten voor ons werk. Met specifieke aandacht over het gebruik van AI rondom ons talentplatform. We blijven continue werken aan verbeteracties op het gebied van cybersecurity en privacy beleidsuitvoering. We continueren ons financiële beleidsuitvoering en risico-management, en werken zo naar een jaarlijkse schone accountantsverklaring op het jaarverslag en jaarrekening alsmede op de programma- en projectverantwoordingen.

STRATEGISCHE SAMENWERKINGSPARTNERS

Niet alleen binnen het ecosysteem wordt samengewerkt, ook in het behalen van de doelstellingen werkt Security Delta nauw samen met een breed scala aan organisaties. Om het ecosysteem heen, zit een brede schil van organisaties die samen met het team van Security Delta meewerken aan de uitvoering. Ons werk is geen soloklus. We kunnen het niet alleen, én dat willen we ook niet.

Onze strategische samenwerkingspartners zijn onder meer: de gemeente Den Haag, Provincie Zuid-Holland, Economic Board Zuid-Holland, de G5 -waaronder Amsterdam en Rotterdam,- VNG, Digital Holland (voormalig Topsecor ICT), ministerie JenV, EZ, DEF, BZK, OM, de Nationale Politie, NFI, Europol en NCIA, Centrum voor Veiligheid & Digitalisering (CVD), Cyberweerbaarheidscentrum Brainport, Oost en Noord NL, FERM/haven Rotterdam, Greenport, HiDelta, Droneport, Campus@ Sea, Green Village, Living Lab Scheveningen, InnovationQuater, BOM, ROM-NL, The Hague & Partners, The Hague Convention Bureau, Connect2Trust, AIC4NL, NCC NL, Yes!Delft, Quantum Delta, Cyberveilig Nederland, CISO community Nederland en al onze 300+ partners.

VERBINDEN AAN HET ECOSYSTEEM: PARTNERSCHAP

HSD is een open ecosysteem, iedere professional in het security domein kan bij ons kennis halen en delen. We hebben op organisatieniveau een partnerschapsmodel. Elke securityorganisatie met een Nederlandse entiteit kan zich bij het veiligheidscluster aansluiten als HSD partner. Door partner te worden wordt het werk van Security Delta ondersteund en werken we aan wederkerige waarde.

Er zijn twee soorten betaalde partnerschappen: **Premium** en **Netwerk**. Premium partners willen een actieve bijdrage leveren en netwerk-partners zijn ‘vrienden van’ Security Delta. Voor de eerste groep is het accountmanagement actief, voor de tweede passief. Het Alliance partnership is onbetaald en wordt gebruikt
voor samenwerkingen met andere netwerkorganisaties en kennisplatformen zonder winstoogmerk.

Daarnaast hebben we programmapartners. Een programmapartner doet mee aan een inhoudelijk innovatieprogramma, bijvoorbeeld door lid te worden van een cyberweerbaarheidscentrum.





Rollen triple helix partners

1 MINISTERIE(S) EN ANDERE ORGANISATIES IN HET VEILIGHEIDS- EN ECONOMISCHE DOMEIN

- Richten zich op het behalen van maatschappelijk rendement.
- Bepalen behoeften en voeren regie op gezamenlijke vraagarticulatie bij de publieke veiligheidspartners, voor zover behorend tot haar taakveld.
- Regisseren de Nederlandse maatschappelijke en economische belangen voor de agenda richting Europa (zoals HorizonEurope).
- Regisseren/coördineren de 'Kennis- en Innovatie Agenda's' en Innovatie Inkoop.
- Financieren (mede) concrete programma's waarvoor zij HSD benut.
- Richten eigen investeringen en financieringsinstrumentarium zoveel mogelijk in lijn met de nationale agenda's in.

2 BEDRIJVEN

- Richten zich op economisch rendement met maatschappelijke waarde
- Pakken een actieve rol in de clusterontwikkeling, vanuit gezamenlijk én eigen belang.
- (Mede) initiëren vanuit en investeren in concrete R&D innovatieprojecten.
- Zijn actief in pre-competitieve samenwerking in de triple helix op de themagebieden van HSD.
- Dragen bij aan kenniscreatie, kenniscirculatie en de uitvoering van de Human Capital Agenda.
- Helpen actief andere HSD partners om de internationale foodprint te vergroten.
- Stellen R&D kennis beschikbaar en richten zich binnen de triple helix op open innovatie.

3 KENNIS- EN ONDERWIJSINSTELLINGEN

- Richten zich op maatschappelijk én economisch rendement.
- Pakken een actieve rol in de clusterontwikkeling.
- Stimuleren kenniscirculatie en valorisatie, zoveel mogelijk in lijn met de nationale agenda's.
- Activeren verbindingen van fundamenteel en toegepast onderzoek aan innovatieprojecten.
- Helpen actief andere HSD partners om de internationale foodprint te vergroten.

6. Financiering

Het vanuit de inhoud faciliteren van een ecosysteem en zorgen voor kennisdeling en innovatie, kan niet zonder voldoende financiële middelen en investeringen.

Hiervoor zullen combinaties van publieke en private financieringen aangeboord worden: exploitatiesubsidie, programma-financiering en projectinvesteringen.
De publieke partijen investeren in de basisfinanciering van Security Delta en private partijen en kennisinstellingen geven commitment via partnerfees.

De uitgelokte investeringen op concrete innovatieprojecten komen uit de publieke vraagpartij, aangevuld met private middelen, onderzoeksgelden vanuit de kennisinstellingen en beschikbare cofinancieringsinstrumenten. De ambities in deze strategie hangen wel samen met structurele duurzame basis-inkomsten (basis exploitatie/ programma-financiering en partner fees). Deze inkomsten zullen moeten doorgroeien van de huidige €2,5 miljoen naar zo'n €3,5 miljoen tot €4 miljoen per jaar.

De financiering van de Nationale Cyber Campus is een apart deel. Zonder goede afspraken over opslag voor community management en logistiek/facilitaire zaken boven op de kale m2 prijs kan HSD deze rol niet op zich nemen. Ook gaat HSD in gesprek met de gemeente Den Haag om de financiële duurzaamheids- en reserves positie van de stichting te verbeteren om te risico's die gemoeid zijn bij de campus en een rol van HSD af te dekken.

Met de huidige middelen (partnerfees en exploitatiesubsidie gemeente DH) is het onze ambitie om vijf miljoen per jaar aan uitgelokte investeringen binnen te halen als outcomewaarde in de programmering.



Bijlage 1 Een stukje geschiedenis

Bij de start van deze meerjarenstrategie bestaat Security Delta (HSD) dertien jaar. In deze periode heeft de organisatie een ontwikkeling doorgemaakt op verschillende fronten.

Van een vooral lokale, Haagse focus, naar regionaal en landelijk. Van een kleine groep van betrokken organisaties naar ruim 300 grote en kleine bedrijven, overheidsorganisaties en kennisinstellingen. We werken vanuit de HSD Campus, waar publieke, private en kennispartijen gevestigd zijn en elkaar ontmoeten.

CONCLUSIES TERUGBLIK STRATEGIE 2021 – 2025

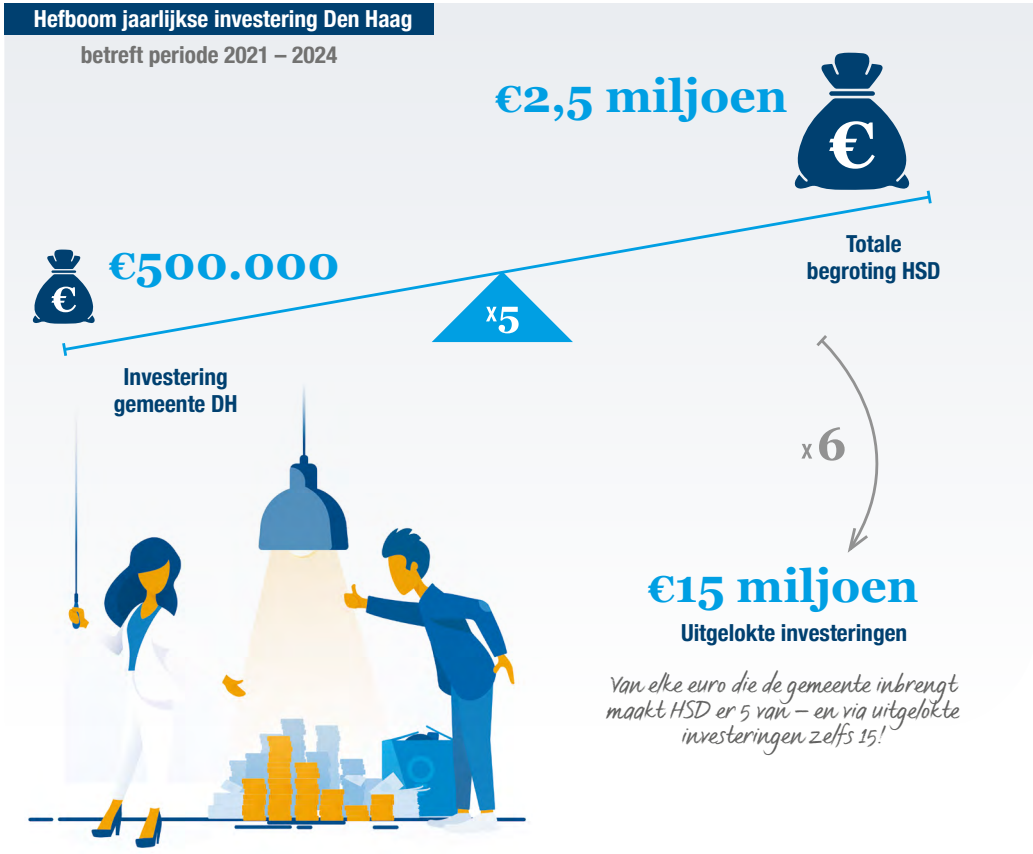
De afgelopen jaren heeft Security Delta zich ingezet voor het versterken van de samenwerking binnen het digitale veiligheidsdomein. De ambities uit de meerjarenstrategie 2021 –2025 waren hiervoor de basis. Samen met onze partners hebben we maatschappelijke én economische waarde gecreëerd via vele verschillende activiteiten. Terugkijkend kunnen we met trots concluderen dat we onze ambities hebben gerealiseerd. Security Delta levert. Samen met onze partners hebben we de gestelde KPI's gehaald en op diverse punten zelfs overgepresteerd. Naast dat we duurzamer gefinancierd en georganiseerd worden, worden we door stakeholders meer en meer gezien en ervaren als een 'trusted' en onafhankelijke verbinder. De werk-zaamheden van Security Delta spelen in op de behoefte van de partners en wensen vanuit de programma's, zoals gebleken uit ons partnertevredenheids-onderzoek. In 2025 werd een 7,5 als waardering gegeven voor onze dienst-verlening.

In vier jaar tijd zijn mooie concrete resultaten geboekt. We hebben impact gemaakt met onze inhoudelijke programmalijnen, samen met en voor onze partners. Met verschillende consortia hebben we €63,1 miljoen aan uitgelokte investeringen opgehaald, ruim boven onze doelstelling van €30 miljoen. Deze uitgelokte investeringen gaan niet rechtstreeks naar de organisatie zelf, maar helpen wel om - met en via onze partners - onze doelstellingen te behalen.

Terugblik meerjarenstrategie '21-'25



DOWNLOAD



Bijlage 1 Een stukje geschiedenis

Terugkijkend op de vorige meerjarenperiode zijn de volgende 10 conclusies te trekken.

1 **HSD heeft alle KPI's gekoppeld aan de doelstellingen behaald**. Op diverse punten is er zelfs over-prestatie. Via de correlatie van onze output resultaten' creëren wij met onze partners outcome waarden. Zowel direct als indirect leveren we impact en rendeert de investering in HSD.

2 De HSD i**nhoudelijke programmering** en 'toegang tot …' propositie zijn succesvol.

3 Er is blijvende zo niet **grotere behoefte aan verbindende kracht** en triple helix samenwerking in het veiligheidsdomein. Met de dubbele doelstelling veiligheid in een digitaliserende wereld en daarnaast economische waarde en groei van banen dragen we bij aan brede welvaart in Nederland, Zuid-Holland en Den Haag. Kortom: HSD heeft bestaansrecht.

4 **HSD wordt meer en meer (h)erkend als eco-systeem** dat toegevoegde waarde levert. Zonder HSD Office als aanjager, verbinder, facilitator, 'communicator' en 'regisseur vanuit een inhoudelijk verbindende rol' is er beperkt(er) resultaat en rendement om uitvoeringskracht te realiseren.

5 Er ligt een **meerjarig financieel fundament** onder HSD en daarmee is HSD Office stabiel(er), maar nog niet optimaal.

6 We hebben **koers gehouden en focus/verdieping aan-gebracht**. We zijn flexibel genoeg geweest om met veranderende omgeving mee te bewegen, zonder met de wind mee te waaien. Dit was succesvol.

7 Er is op het gebied van cybersecurity nog steeds sprake van een **versplinterd veld** en de nationale rol HSD ogv Cybersecurity is nog niet echt ingevuld.

8 De cyberweerbaarheidsaanpak start sectoraal/regionaal, kost veel werk om uit te bouwen en is **nog niet duurzaam gefinancierd**.

9 De financiële basis HSD (veelal gekoppeld aan KPI's) **vergt veel van het team**

10 **Het voorwerk en de voorinvestering is relatief hoog**



Bijlage 2 Onze output

1 Samenwerking en kennisdeling in een actief ecosysteem

Doelstellingen	Output 5 jaar	
1a. Community management Stabiel ecosysteem versterken en activeren: meer partijen zijn actief betrokken in het netwerk en het netwerk bruist.	**1** stabiel ecosysteem **200** gesprekken met potentiële nieuwe partners **25** berichten over nieuwe partners **1** evaluatie ecosysteem **700** matches **10** netwerkbijeenkomsten **10** overleggen Raad van Advies	**300** accountgesprekken met premium partners **5** bijeenkomsten 'ontwikkelingen in het veld' voor premium partners **15** HSD premium partners update mailings **5** haal meer uit HSD partnership mailings **3** kanalen voor delen ontwikkelingen binnen ecosysteem: securitydelta.nl & HSD LinkedIn kanaal & nieuwsbrieven **5** bijdrages aan Cybersecurity Week
1b. Kenniscirculatie We bouwen de kennisprogrammering uit en faciliteren kenniscirculatie. Onze partners en wijzelf staan regelmatig op podia om inhoudelijke kennis te delen.	**20** HSD Cafés **10** marktconsultaties **50** presentaties op podia **50** endorsing bijeenkomsten	**1** digitaal platform: Security Insight **20** Security Insight nieuwsbrieven
1c. Toegang tot financiering & kapitaal, talent en (inter)nationale markt We communiceren actiever over mogelijkheden op gebied van talent, financiering en internationalisering. We organiseren bijeenkomsten waarin kennis wordt gedeeld en vraag en aanbod op dit terrein wordt gekoppeld.	Financiering & Kapitaal: **10** bijeenkomsten financiering en kapitaal **25** bedrijven matchen aan investeerders **25** startups koppelen aan accelerator **5** thema nieuwsbrieven **25** nieuwsberichten	Talent: **2** platforms: securitytalent.nl & cybersecuritywerkt.nl **25** nieuwsberichten **10** endorsing partner van Talent events (Inter)nationale markt: **12** koppelingen maken tussen internationale programma's en geïnteresseerden **2** marktverkenningen nieuwe internationale markten opstellen **5** themanieuwsbrieven over internationale missies **25** nieuwsberichten over handelsmissies
1d. Internationale positionering HSD De bekendheid en daarmee aantrekkingskracht van het ecosysteem neemt verder toe in het buitenland.	**35** bedrijven landen in NL (indirecte bijdrage) **25** congressen landen in NL (indirecte bijdrage) **10** deelnames aan internationale handelsmissies **25** inkomende handelsdelegaties ontvangen	**15** ECSO cybersecurity made in Europe labels uitgegeven **1.000** vermeldingen in online media **15** interviews geven

Bijlage 2 Onze output

❷ Het actief leiden en uitvoeren van programma's

Doelstellingen	Output 4 jaar	
2a. Cyberweerbaarheid Succesvolle regionale cyberweerbaarheids-initiatieven schalen we landelijk op. (Inter) nationale ontwikkelingen vertalen we naar concrete innovatieprogramma's.	**4** programma's **60** coalitiebijeenkomsten **25** kennissessies, workshops en rondetafels **3** digitale platforms: cwgreenport.nl, cwmaakindustrie.nl, ikhebcyberkracht.nl	**25** nieuwsbrieven **35** nieuwsberichten
2b. Human Capital Het aantal talentprogramma's groeit en daar-mee ook de investeringen die we hiervoor organiseren. We schalen bestaande successen op. Securitytalent.nl wordt doorontwikkeld en groeit.	**2** talent programma's uitvoeren (CADMUS, ITVZH) **2** nieuwe talent programma's opgezet **10** coalitiebijeenkomsten en kennissessies **1** nieuwe Human Capital Agenda Security 2027-2030	**1** analyse Nederlandse arbeids- & opleidingenmarkt **5** internationale cybersecurity summer schools **2** digitale platforms: Securitytalent.nl en Cybersecuritywerkt.nl **1** doorontwikkeling Securitytalent.nl met competentietool & uitbreiding **450.000** bezoeken, **5.000** vacatures en **600** opleidingen op securitytalent.nl
2c. Nationale Cyber Campus Helpen opzetten en vormgeven van de Nationale Cyber Campus. We voeren te zijner tijd het campus community management uit en coördineren de logistieke en facilitaire zaken die daarbij komen kijken.	**1** visie & strategie Nationale Cyber Campus Cyber Campus community management: invulling pas bekend na verdere uitwerking planvorming	

Bijlage 2 Onze output

3 Smart Secure Grids & Energy Transition

Doelstellingen	Output 4 jaar
3a. Innovatieprogrammering We starten nieuwe programma's die gericht zijn op veiligheid, veiligere technologie en haar verantwoorde inzet in verschillende toepassingsgebieden. We schalen bestaande succesvolle programma's en oplossingen op.	**4** programmalijnen ontwikkeld en in uitvoering: Smart secure Cities, Justice & Security, Smart Secure Grids & Energy Transition en Defense **5** verkenningen en (duidings)onderzoeken **5** nieuwe coalities bouwen inclusief financiering voor de uitvoering daarvan **25** coalitiebijeenkomsten, kennissessies en workshops **20** landelijke overleggen bijwonen **1** digitaal inhoudelijk platform: veiligesmartcities.nl **25** nieuwsberichten **5** bijdrages aan jaarlijkse Securing the Future event
3b. Extra funding Meer financiering regelen waarmee extra capaciteit wordt aangetrokken voor het behalen van de doelen.	**20** financieringsaanvragen met als outcome waarde **€50** miljoen aan uitgelokte investeringen voor innovatie-programma's

Bijlage 2 Onze output

Interne organisatie en bedrijfsvoering

Doelstellingen	Output 4 jaar
• Doorontwikkelen **propositie HSD en huisstijl** op basis van meerjarenstrategie en HSD-rol Nationale Cyber Campus	**1** up to date HSD propositie & huisstijl
• Schrijven **jaarplannen** en **jaarverslag**	**5** jaarplannen en jaarverslagen **1** terugblik meerjarenstrategie **1** nieuwe meerjarenstrategie 2031-2035
• Eigen **cybersecurity**, **privacy** en **AI-beleid** in uitvoering: 3,5 op schaal van 5 als score	**1** cybersecurity en AVG beleid in uitvoering met continue verbeteracties per jaar **1** formele cyber audit voor score volwassenheidsniveau **1** AI beleid geformuleerd en in praktijk gebracht
• **Personeelstevredenheid** hoog, zodat medewerkers lang(er) bij HSD Office blijven	Goed werkgeverschap in praktijk Lage uitstroom en extra instroom voor groei van **5–10** personen in het team
• **Financiën**: backoffice processen geoptimaliseerd, schone control verklaringen van de accountant, meer financiering aantrekken voor uitbreiding eigen omzet en aantrekken van extra personeel	**1** risicomanagementbeleid **1** CRM up to date Jaarlijks **€1mln – €1,5 mln** extra voor aantrekken personeel voor programmering en campusmanagement

Bijlage 3 Why – How – What

Wat is Security Delta (HSD)

HSD
securitydelta.nl

Security Delta is het Nederlandse veiligheidscluster met HSD Office als onafhankelijke aanjager, verbinder en facilitator.



Why

Samenwerken en samen innoveren voor een veiligere (digitale) wereld en brede welvaart. Together we Secure the Future!



What

Wij bieden als onafhankelijke non-profit organisatie toegang tot kennis, innovatie, (inter)nationale markt, talent en financiering & kapitaal.



How

Door middel van ons (inter)nationale netwerk en onze rol als aanjager, verbinder, facilitator en programmacoördinator/ orkestrator.



Inhoudelijke focus:

- Cyberweerbaarheid
- Human Capital
- Nationale Cyber Campus
- Smart Secure Cities
- Smart Secure Grids & Energy Transition
- Smart Secure Defense & Resilience
- Smart Justice & Security

Triple helix & ecosysteem partners

HSD partners zijn overheden & publieke partijen, onderwijs & kennisinstellingen en bedrijven uit heel Nederland. Van startups tot scale-ups, innovatieve mkb's, vitale infrastructuurorganisaties, industrie tot grote corporates. En van ROM's, NFIA, RVO, ambassades, accelerators, investeerders, NCC-NL, trainingsbureaus tot gespecialiseerde dienstverleners.



Together we Secure the Future

Security Delta (HSD)
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
+31(0)70 2045180

info@securitydelta.nl
www.securitydelta.nl

HSD
securitydelta.nl