The Hague Security Delta

MASTERPLAN

The Hague Security Delta 2013-2014

Rob de Wijk en Joris den Bruinen

Maart 2013

info@thehaguesecuritydelta.com | thehaguesecuritydelta.com | Join us on Twitter: @HSD_NL

INHOUDSOPGAVE

1. SAMENVATTING MASTERPLAN HSD 2013-2014

The Hague Security Delta is een continu groeiend netwerk van bedrijven, overheden en kennisinstellingen in de veiligheidssector, die zich samen sterk maken voor innovatieve veiligheidsoplossingen en economische ontwikkeling. Het is een nationaal veiligheidscluster met een kern in de Haagse regio en verbindingen o.a. met regio Twente, Brainport en Brussel. Het gezamenlijke doel is het verdrievoudigen van omzet, aantal bedrijven, banen en studenten in 2025. Hiermee is HSD de 'security port to Europe'. HSD biedt topkwaliteit aan kennis, producten en diensten voor (verbetering van) veiligheid en veiligheidsbeleving van burgers, bedrijven en de samenleving.

Bescherming van een steeds meer verweven samenleving zal profijt hebben van innovatieve doorbraken op terreinen als voorspellend vermogen, monitoring, informatie-uitwisseling, communicatie, besluitvorming, training en onderwijs door ketens heen, en participatie van bedrijfsleven en burgers. Dit biedt kennisinstellingen en bedrijfsleven internationale positionering en marktperspectief.

In dit plan presenteren we de aanpak voor de eerste jaren om de (langere termijn) doelstellingen te bereiken. HSD neemt regie en verantwoordelijkheid op de landelijke innovatie agenda veiligheid. Allereerst via het uitbouwen van het netwerk, het gezamenlijk investeren in projecten ten behoeve van innovatie en kennisontwikkeling en het beter afstemmen van vraag en aanbod. Voorts het realiseren van innovatiehuizen, livinglabs, een HSD-office, HSD-innovatiestimuleringsregeling en en fysieke locatiebundeling. Ook via handelsmissies, communicatie, marketing en acquisitie. Tevens door het vergroten van de beschikbaarheid van gespecialiseerd personeel en aanstormend talent via opleidingen en training en daarbij bovendien onderwijs, onderzoek en valorisatie te koppelen. De innovatiehuizen die afgelopen jaar zijn opgezet zullen onder de paraplu van een Landelijke Innovatie Centrum Veiligheid verder worden uitgebouwd. En tevens fysiek gebundeld op de locatie Beatrixkwartier tot een HSD Campus. Het gaat om de volgende initiatieven:

	Project	Trekker	Consortium-partners	Locatie	Aanvang project	Start op locatie	Budget indicatie
HSD Landelijk Innovatie Centrum Veiligheid							
	Innovatiehuis Nationale Veiligheid						
	Real Time Intelligence Lab	Thales + TNO	Siemens Capgemini HP, TU, Fox-IT Trigion , Sentient Wiseguys, ENAI, HHS, Geodan T-WMC, Croon Gem. DH	Beatrix-kwartier + internat zone	Zodra € rond	Sept 2013	€7,5 mln (voor 3 jaar)
	Serious Gaming Lab	HCSS	Thales/ T-xchange E-Semble Vstep, TU Crisisplan Trigion, Ranj Games Maken Siemens TNO, NFI Twijnstra Gudde C-TWO, Ijsfontijn	Beatrix-kwartier	Zodra € rond	Sept 2013	€600.000

	Crisis simulatiecentrum	Crisisplan		Beatrix-kwartier		Sept 2013	PM
Innovatiehuis Urban Security							
	Living lab Integrale gebieds beveiliging internationale zone Den Haag	Gem. DH	IO's, Politie, NCTv, e.a. Siemens, Trigion, Thales, Fox-IT + MKB	Beatrix-kwartier + internat zone			PM
	Living Lab Sociale Veiligheid II	TNO	TG, PSIC, HHS, Verwey-Jonker	Op locatie, later Beatrix	Reeds gestart		PM
Innovatiehuis Vitale infrastructuur / Cyber Security							
	ENCS	Alliander	KPN KEMA TNO Univ N'mgn	Beatrix-kwartier	Reeds gestart	Jan 2013	nvt (eigen business case)
Innovatiehuis Cyber Security							
	Cyber Security Academy	Gem. DH Dhr. Van Middelkoop	TU Delft UL/DH HHS, ENCS KPN, Fox-IT, NCTv/NCSC Europol, TNO Min. Def	Beatrix-kwartier	Werk groep gestart	Sept 2013 fase 1. Fase 2 medio 2014	Initieel €500.000 Overig PM
	Cyber Incident Experience Centre	Fox-IT + TNO	NCSC KPN NFI	Eerst TNO waalsdorp daarna Beatrix-kwartier	Zodra € rond	Voor zomer 2013	€800.000
	HSD cyber security traineeship	Fox-IT + KPN, Cap	NCSC, Europol e.a.	Beatrix-kwartier	Werk-groep gestart	Sept 2013	€100.000
Innovatiehuis Forensics							
	CSI The Hague II	NFI	TNO, Philips Thales, TU Delft E-semble AMC, e.a.	NFI fieldlab	nu reeds doorstart/ Jan 2013	2013-2016	€5 mln (voor 3 jaar)
Overige faciliteiten							
	Incubator faciliteiten	Gem. DH	M.b.v. Fakton + HSD-office	Beatrix-kwartier		Nov 2013	PM
	Bedrijfsverzamel gebouw	Gem. DH	M.b.v. Fakton + HSD-office	Beatrix-kwartier		Nov 2013	PM
	HSD office incl HSD MKB desk	HSD-Office	M.b.v. Fakton + gemeente DH	Beatrix-kwartier		Nov 2013	PM

De kern van de governance is dat er een sturings- en verantwoordingsmodel wordt opgezet om zaken te realiseren en de juiste beweging van HSD in gang te zetten, opdat we de gezamenlijk ambities binnen bereik gaan krijgen. Daartoe wordt een stiching The Hague Security Delta opgericht. Met een HSD-board die de strategische koers bepaald, HSD executive committee als uitvoeringsorgaan en de HSD-directie i.s.m. HSD-office als dagelijks uitvoerder.

Gezamenlijk dragen HSD-partners de basisfinanciering van de stichting HSD en het uitvoerings-orgaan HSD-Office. Daarnaast wordt een HSD-innovatiestimuleringsregeling opgezet als financieringsvehikel om projecten en het landelijk innovatiecentrum veiligheid van de grond te krijgen.

2. INLEIDING

In dit plan wordt aangegeven wat The Hague Security Delta wil bereiken en waar we gezamenlijk als eerste op gaan inzetten in 2013 en 2014.

Missie (waarom HSD bestaat)

Het vergroten van de economische ontwikkeling binnen de regio Den Haag en BV NL en het bijdragen aan de (inter-)nationale veiligheid.

Visie (wat wil HSD zijn)

HSD is een internationaal gerenommeerd security-cluster 'Security Port to Europe', waarin vanuit de *triple helix* gedachte partijen uit overheid, bedrijfsleven en kennisinstellingen samenwerken, middelen bundelen om innovatieve producten en diensten rond grote (internationale) veiligheidsvraagstukken te ontwikkelen en vermarkten. Door de netwerken van de verschillende HSD partners te koppelen, kan de internationale footprint van alle HSD organisaties worden vergroot.

Doelstelling (wat wil HSD bereiken)

Het creëren van een snel groeiend economisch cluster, een nationaal veiligheidscluster met een kern in de Haagse regio. Die zich richt op een breed gebied van veiligheid, met als inhoudelijke terreinen nationale veiligheid, urban security, cyber security, forensics en bescherming vitale infrastructuur en bordersecurity. En daarnaast thema's die daar dwars doorheen gaan als serious gaming, human capital agenda, big data en CBRN.

Gezamenlijke doelstellingen	Omzet	Banen	Bedrijven	Studenten
2012	€ 1.5 miljard	10.000	300	1.000
2025	€ 4.5 miljard	30.000	900	3.000

Strategie (wat gaan we doen, hoe gaan we dit bereiken)

Allereerst via het uitbouwen van het netwerk, het gezamenlijk investeren in projecten ten behoeve van innovatie en kennisontwikkeling en het beter afstemmen van vraag en aanbod. Voorts het realiseren van innovatiehuizen, livinglabs, een HSD-office, financieringsverhicel en fysieke locatiebundeling. De innovatiehuizen zijn de motor om tot nieuwe (innovatie)projecten en consortia te komen. Voorts ook via handelsmissies, communicatie, marketing en acquisitie. Tevens door het vergroten van de beschikbaarheid van gespecialiseerd personeel en aanstormend talent via opleidingen en training en daarbij bovendien onderwijs, onderzoek en valorisatie koppelen.

Leeswijzer

Hierna volgt allereerst een beschrijving van (2) de context van HSD, zowel vanuit veiligheids, economische als netwerk/cluster optiek. Daarna volgt een beschrijving van (3) het Landelijk Innovatie Centrum Veiligheid opgebouwd aan de hand van de 6 thema's/innovatiehuizen. Vervolgens volgt een uitwerking van de ondersteuning van (4) een HSD-office incl. gebundelde faciliteiten en (5) een HSD-innovatiestimuleringsregeling. Als laatste volgt (6) de HSD-governance over hoe de sturing&verantwoording in elkaar steekt.

3. CONTEXT

Belangrijke uitdaging in Nederland is hoe de effectiviteit van de rechtshandhaving (bijvoorbeeld de pakkans) verhoogd kan worden terwijl we tegelijkertijd de efficiency verhogen. Verder ontstaan er door de verminderde effectiviteit van rampen- en crisisbeheersing politieke risico's, zoals onder andere uit de kwesties Moerdijk en Haren is gebleken.

De helft van alle bedrijven in de defensie- en veiligheidsindustrie in Nederland heeft de afgelopen jaren succesvol nieuwe producten ontwikkeld. De meesten doen dat nu nog alleen, terwijl grotere stappen in het oplossen van integrale complexe veiligheidsvraagstukken kunnen worden gemaakt als zij krachten bundelen: met onderzoeksinstellingen, met de overheid en met elkaar. Zodat innovaties niet alleen technologisch van aard zijn, maar ook ingebed zijn in de gehele organisatie en werkwijze van de afnemende partij, vaak de overheid.

De huidige samenleving en daarmee de veiligheidsomgeving kenmerkt zich door toenemende complexiteit en dynamiek. De relaties tussen publiek en privaat, statelijke en niet-statelijke actoren, oorzaken en effecten, tussen fysieke en digitale wereld en binnen- en buitenland zijn steeds minder eenvoudig en eenduidig in kaart te brengen. Ook is duidelijk dat de overheid niet alleen is in het bieden van veiligheidsoplossingen, zie initiatieven als burgernet of samenwerkingen met private toezichthouders. Voorts, of het nu gaat om fysieke veiligheid, om cyber security of de bescherming van vitale infrastructuur, het is allemaal verweven met elkaar.

Deze ontwikkelingen komen onder meer tot uiting in:

- De complexe verdeling van verantwoordelijkheden voor veiligheid tussen de overheid, bedrijfsleven en burger. Hoewel verantwoordelijkheid voor veiligheid bij de overheid wordt gelegd, is de slagkracht van deze overheid in een genetwerkte wereld steeds minder.
- De grote mate van vermenging van verschillende beleidsdomeinen (veiligheid, duurzaamheid, economie, gezondheid) die in het uitvoeren van en denken over veiligheidstaken tegen elkaar worden afgewogen.
- De samenhang van ontwikkelingen die in het buitenland plaatsvinden met de nationale veiligheidssituatie. De effecten van de Griekse crisis en van de Arabische opstanden zijn goede voorbeelden van deze samenhang.

De Nederlandse overheid heeft tal van trajecten opgezet om met deze factoren te kunnen omgaan.

- Er is meer zicht gekomen op domein overstijgende problemen: de Strategie Nationale Veiligheid overstijgt het perspectief van individuele beleidsterreinen en beoordeelt all-hazard risico's. Er is een Landelijke Operationale Staf (LOS) daar waar het gaat om de bestrijding van nationale crises en rampen. Nieuwe dreigingen zoals cybersecurity worden voortvarend aangepakt.
- Diverse taskforce opgezet rondom bijvoorbeeld overvallen en veiligheid in OV
- Er zijn nieuwe organisatiestructuren doorgevoerd: de wet op de Veiligheidsregio's gaf een nieuwe impuls aan de wijze waarop veiligheid in Nederland is georganiseerd; er bestaat inmiddels een ministerie van Veiligheid; en de lokaal verankerde politie is gereorganiseerd in een Nationale Politie.

- Samenwerking tussen publiek en privaat wordt bevorderd: de vitale infrastructuur wordt door vormen van publiek-private samenwerking (PPS) door overheid en bedrijfsleven beschermd (bv. de publiek-private Cyber Security Raad); de overheid werkt intensiever samen met kennisinstellingen en bedrijven.
- Er vindt op diverse plaatsen uitwisseling van gegevens plaats rondom veiligheid en criminaliteit tussen publieke en private toezichthouders

Ook op Europees niveau worden nieuwe initiatieven opgezet. Zo wil de Europese Commissie haar informatiepositie in tijden van crisis versterken via en Europees Monitoring & Information Centre (EU MIC). Het EU MIC werkt nauw samen met nationale crisiscentra van 32 landen binnen het zogenaamde 'EU mechanisme' (EU 27, Kroatië, de voormalige Joegoslavische republiek Macedonië, IJsland, Liechtenstein en Noorwegen). Daarnaast heeft de EU besloten een nieuwe taakopdracht rondom cyber crime te beleggen bij Europol.

Desondanks blijven er talloze mogelijkheden tot verbetering van de situatie. De pakkans is in NL zeer laag, veel lager dan in andere landen. Dit terwijl de pakkans een zeer belangrijk afschrikwekkend instrument is. Daarnaast bleek uit zeer recente discussies met belanghebbenden in het kader van het project gebiedsbeveiliging internationale zone dat grote noodzaak wordt gevoeld tot het delen van inlichtingen en operationele informatie, gekoppeld aan een heldere verantwoordelijkheidsstructuur op lokaal, regionaal en nationaal niveau. Voorts wordt verder in de vele evaluaties van crises en oefeningen keer op keer geconstateerd dat in Nederland de crisisbeheersing en rampenbestrijding nog niet op orde is: het schort aan de wijze waarop wordt gecommuniceerd; er is sprake van een te ingewikkelde organisatiestructuur; tijdens de responsfase is de aansturing onhelder; en technologische oplossingen zijn voor handen, maar worden onvoldoende benut.

Verbeterpunten liggen vooral op de volgende gebieden:

- *Voorspellend vermogen:* er is een toenemende urgentie om mogelijk te begane misdaden en crises in een vroegtijdig stadium 'early warning' te onderkennen en gepaste maatregelen te nemen. Hoe kunnen we informatie over voornemens tot criminaliteit en afwijkend gedrag signaleren en ontsluiten om misdaden te voorkomen en hoe kan de voorbereiding op crises beter worden gekoppeld aan mogelijke risico's?
- *Besluitvorming en hulpverlening:* De afgelopen jaren is door velen gewezen op het feit dat crisisbeheersing en rampenbestrijding vooral stoelen op coördinatieprincipes. Het gecoördineerde commando-element in de 'warme fase' door alle lagen heen, met de juiste urgentie voor de operationele effecten is onvoldoende uitgewerkt. Zeker in het licht van de financiële crisis en de instelling van een Nationale Politie is het noodzakelijk om nogmaals te bezien hoe de inzet van capaciteiten op het regionale en lokale niveau efficiënter en doelmatiger kan gebeuren. Vooral het gecoördineerd optreden in 'the golden hour' is daarbij cruciaal.
- *Informatievoorziening en communicatie*: gedeelde en tijdige informatievoorziening -van zowel publieke, incl burgers, als private partijen afkomstig- is van groot belang voor de ontwikkeling van een 'real time' en gemeenschappelijk beeld van een misdaadsituatie en in de crisissituatie. Dit geldt ook voor de koppeling tussen lokaal, regionaal, nationaal en zelf internationaal niveau. En daarna voor het juist communiceren overde situatie en te nemen maatregelen naar een brede groep van politie en hulpdiensten tot bedrijfsleven en burgers.

Op elk van deze terreinen zijn tal van partijen actief die nieuwe kennis, diensten en producten ontwikkelen. Dit gebeurt vaak separaat van elkaar. Door in Den Haag de expertises van bedrijven, kennisinstellingen en overheden bij elkaar te brengen in een omgeving waarin *best practices* floreren, kunnen nieuwe toepassingen worden ontwikkeld. Het bij elkaar brengen van de kennis, activiteiten en capaciteiten van overheid, bedrijfsleven en kennisinstellingen op het gebied van nationale veiligheid, met inbegrip van rampenbestrijding en crisisbeheersing, kan de operationele en bestuurlijke effectiviteit en financiële doelmatigheid van investeringen aanzienlijk vergroten, daarmee de politieke risico's die kleven aan de huidige zwakten binnen het stelsel van rampenbestrijding en crisisbeheersing kleven verminderen, en de economische ontwikkeling van Den Haag, de Zuidvleugel van de Randstad en de BV Nederland een impuls geven.

De bundeling dient daarmee de volgende functies:

- Het versterken van de klantrol van de overheid en in het bijzonder het ministerie van VenJ, o.a. door gebundelde vraagarticulatie
- Het samenbundelen en verdiepen van de conceptuele kennis ten behoeve van nationale veiligheid in brede zin en het creëren van een 'hub' die als kennismakelaar kan dienen voor de in Nederland en internationaal aanwezige kennis op dit gebied.
- Bijeenbrengen, verdiepen en experimenteren van kennis op het gebied van de operationele en technologische aspecten van aanpak criminaliteit en de crisisbeheersing en rampenbestrijding
- Benutten van technologische mogelijkheden om uit grote hoeveelheden informatie de juiste informatie, op het juiste moment bij de juiste persoon/organisatie te krijgen. Dit vergroot de effectiviteit van aanpak criminaliteit en verkleint politiek afbreuk risico bij de gezagdragers en gezagsdragende instanties.
- Het op basis van beschikbare kennis en inzichten opleiden en trainen van voldoende gekwalificeerd personeel ten behoeven van de veiligheidssector
- Het door middel van living labs experimenteren en etaleren van de resultaten van onderzoek en ontwikkeling om een bijdrage te leveren aan de vergroting van de effectiviteit van de aanpak van criminaliteit en de crisisbeheersing/rampenbestrijding en het vermarkten van producten.
- Het creëren van een veiligheidscultuur gebaseerd op het doorbreken van verkokering, het versterken van de gehele veiligheidsketen en het bij elkaar brengen van overheid, bedrijfsleven en kennisinstellingen en het stimuleren van weerbaarheid bij de burger.

Het creëren van een veilige, vertrouwelijke omgeving voor overheden, bedrijven en kennis- en onderwijsinstellingen 'triple helix' waarin kan worden samen gewerkt (kenniswerkers, samen met functionele, operationele gebruikerskennis) is daarbij een belangrijke voorwaarde.

Via co-creatie in een dergelijke omgeving worden betaalbare oplossingen opgeleverd die tegen lagere levensduurkosten op verschillende terreinen kunnen worden ingezet en de effectiviteit en doelmatigheid van investeringen verbeteren. Uiteindelijk moet het centrum niet alleen een nationale, maar ook een internationale zichtbaarheid krijgen waardoor meer bedrijvigheid wordt aangetrokken.

Als onderdeel van het vorige en doorgezet in het huidige kabinetsbeleid vindt er concentratie van onderzoek en ontwikkeling plaats in zo genoemde topsectoren, waaronder de topsector Hightech Systems en Materialen (HTSM). Binnen deze topsector valt ook het cluster veiligheid. Afgelopen periode is daarvoor een HTSM-Security Roadmap ontwikkeld. Onderdeel van deze roadmap is de ontwikkeling van het het boegbeeldproject National Security Monitoring & Information Centre

(NS MIC, hierna het Nationaal Veiligheidsinnovatie Centrum)[1] Dit omvat ook de initiatieven zoals Real Time Intelligence Fieldlab, Cyber Experience Centre, Serious Gaming Lab en de Cyber Security Academy en het reeds opgezette ENCS. Deze worden later in dit stuk nader geduid.

Deze aanpak past binnen de ambitie van de overheid om met gerichte overheidsinvesteringen haar positie van *launching customer* een extra impuls te geven aan de hightech kennisinfrastructuur (het bedrijfsleven en kennisinstituten). In het innovatiecentrum worden alle onderdelen uit de HTSM-Security Roadmap (System of Systems, Cyber Security en Sensoren) samengebracht in een omgeving waar kennis en technologie van wereldklasse zich kunnen ontwikkelen. In het innovatiecentrum worden op innovatieve wijze activiteiten en inzichten van de belanghebbenden geïntegreerd in HTSM-Security, variërend van *first responders tot beveiligers en van* crisismanagers bij de (private) vitale infrastructuur tot de publieke crisismanagers tot op het niveau van de verantwoordelijke minister.

Het Nationaal Veiligheidsinnovatie Centrum is een belangrijke schakel in het doorontwikkelen van het cluster The Hague Security Delta (HSD). Cluster netwerken, zoals HSD, vormen in toenemende mate het ankerpunt voor open innovatie en kennisontwikkeling. Definiëring van een cluster die we hierbij hanteren is: een geografische concentratie van onderling gerelateerde ondernemers, toeleveranciers van ondernemers, onderzoekers/wetenschappers en eindgebruikers, actief in een economisch domein dat van strategisch belang wordt geacht.

Volgens de netwerktheorie zijn de verschillen in succes van clusters in belangrijke mate te verklaren aan de hand van de coördinatie/regie en de integratie van fysieke, sociale en technische elementen van het netwerk. Basiselement van een dergelijke infrastructuur is allereerst een fysieke plek als een onmisbare grondslag voor identificatie en ontmoeting. Daarnaast vormen online communities en communitietechnologieën een belangrijke aanvulling om kennisdeling en samenwerking mogelijk te maken. Bovendien zijn netwerkhub-diensten zoals samenwerking tussen regionale en nationale belanghebbenden (bv met regio's Eindhoven en Twente, G4, veiligheidsregio's en ministeries), (inter)nationale samenwerking o.g.v. onderwijs en onderzoek (bv met KUN en Universiteit van Dublin), strategische verbanden (zoals met brainport en Security Cluster Ottowa) en mondiale zichtbaarheid een noodzakelijke component voor internationaal concurrerende sociale infrastructuur.

Samenvattend, gezien de complexiteit van hedendaagse veiligheidsuitdagingen, dienen het bedrijfsleven, overheid en kennisinstellingen nauw met elkaar samen te werken. Dit biedt via netwerk/clustervorming tevens economische kansen. Nieuwe risico's, een krimpende arbeidsmarkt en een dynamische economie, vragen om nieuwe, technologie gedreven, veiligheidsantwoorden. Ingebed in een stevige juridische basis en gesteund door publieke opinie. Alleen met elkaar in de 'triple helix' kunnen de grote ambities en gezamenlijke doelstellingen met wederzijdse opbrengsten verwezenlijkt worden.

[1] Wij stellen voor om afscheid te nemen van de naam NS MIC. In tegenstelling tot het EU MIC gaat het hier niet om een centrum met operationele taken, maar om een publiek-privaat innovatiecentrum.

4. LANDELIJK INNOVATIECENTRUM VEILIGHEID

Het Landelijk Innovatiecentrum Veiligheid is geen eigenstandig institutie.[2] Het is een samenwerkingsverband waarbinnen partijen gezamenlijk rond een bepaald (deel)onderwerp conceptueel en operationeel-gerichte activiteiten ondernemen, waaronder, ideevormen, testen, *experience*, training & opleiding. Dat samenwerken kan op locatie maar levert meer op als het fysiek gebundeld plaats vindt. Men moet elkaar kunnen ontmoeten en wederzijds bevruchten. Het is een faciliteit en het is tevens een etalage om nieuwe innovaties zichtbaar te maken.

Bij de fysieke bundeling wordt rekening gehouden en een balans gevonden in de fysieke vormgeving voor wat betreft 'uiterst vertrouwde en beveiligde omgeving' en 'open innovatie en etalage ruimte'.

Het Innovatiecentrum vervult als best practice een (inter)nationaal rolmodel in het bereiken van effectiviteit en innovatieve samenwerking tussen overheden, kennisinstellingen en bedrijven rond netwerkcentrische veiligheidsconcepten, kennis en innovatie en het intrinsiek veilig ontwerp van steden en bescherming vitale infrastructuur.

De innovatiehuizen van het HSD PID project, de netwerken/denktanks waar diverse projecten en livinglabs uit voort zijn gevloeid met CSI The Hague en Living Lab Sociale Veiligheid als goede voorbeelden, worden ten behoeve van de continuïteit geïntegreerd en geïncorporeerd in het Nationaal innovatiecentrum Veiligheid. Hieronder volgt per inhoudelijke thema/HSD-innovatiehuis een uitwerking.

4.1 Innovatiehuis Nationale Veiligheid

4.1.1. Integratie lopende en afgeronde PID projecten

In 2007 heeft het Kabinet de Strategie Nationale Veiligheid aan de Tweede Kamer aangeboden. Zoals aangegeven is deze strategie all-hazard en snijdt de strategie dwars door alle beleidsterreinen. Mede door dit verbindende karakter dient het gedachtengoed van deze strategie als uitgangspunt voor het Innovatiehuis. Het Innovatiehuis kan daarmee (ontwikkelde en nog te ontwikkelen) innovatieve oplossingen aandragen voor de knelpunten die bij de verdere ontwikkeling en uitvoering van de strategie worden ervaren, zowel bij de overheid, het bedrijfsleven en in de wetenschap. Daarbij richt het zich voornamelijk op twee aspecten:

- het ontwikkelen van nieuwe kennis en inzichten op dit terrein:
    - Het versterken van het voorspellend vermogen
    - Het versnellen van de besluitvorming en hulpverlening
    - Het verbinden van informatievoorziening en communicatie
- Voorstudies uitgevoerd voor landelijk innovatiecentrum veiligheid

2 Het CSI Lab bij het NFI in Den Haag is als voorbeeld en inspiratiebron voor het Innovatiecentrum genomen voor de succesvolle samenwerking tussen overheid, bedrijven en kennisinstellingen om baan brekende, inhoudelijke maar ook economisch waardevolle doorbraken te realiseren.

4.1.2 Nieuwe initiatieven en living labs

Real time intelligence field lab

In het real time intelligence field lab worden door open innovatie en co-creatie door overheid, bedrijven en kennisinstellingen de concepten, technieken en innovaties bedacht, getest en beproeft ten behoeve van actuele en toekomstige veiligheids- en crisismanagementvraagstukken. Hiermee ook in opmaat naar de meldkamer van de toekomst. Op dit moment komen informatiestromen al vanuit vele kanalen en in de meldkamer van de toekomst wordt niet langer slechts reactief gestuurd door telefonische 112-meldingen van incidenten maar stuurt daarnaast proactief informatie gestuurd ook zelf op preventie, handhaving en opsporing. Hiermee wordt ook de koppeling gelegd tussen fysieke beveiliging en cyber security. Naast de voice meldingen speelt ook het monitoren van sociale media, het internet, burgernet, Amber Alert enz. in toenemende mate een rol. Informatie push en pull en het slimmer absorberen van menselijke informatie. Maar denk ook aan de informatie afkomstig van de veelheid aan diverse sensoren (cameratoezicht, alarminstallaties, brandmelders, verkeerslussen, etc.). Daarenboven is er ook reeds veel informatie beschikbaar in bestaande authentieke registers en bestanden. Er schuilt een enorm potentieel in het bewust en actief koppelen van deze diverse informatiebronnen (system-of-systems). Maar dat moet wel veilig en met respect voor de privacy kunnen gebeuren. Technisch en organisatorisch gesproken is dat koppelen overigens makkelijker gezegd dan gedaan. De verschillende (informatie)systemen hebben allemaal hun eigen herkomst, ontstaansgeschiedenis, technologiebasis, en doelstellingen. Er is specifieke technologie benodigd om deze bronnen te ontsluiten en interoperabel te maken.

De focus ligt op het vormgeven van netcentrisch werken, het opbouwen van een actueel open gedeeld situationeel beeld (lokaal, regionaal en landelijk), informatiesturing en het creëren van voorspellend vermogen. Onderzoek naar de maatschappelijke effecten van de toepassing (privacy, acceptatie bij burgers) en/of gebruikerseffecten zal een vast onderdeel zijn.

➔ Het opzetten van een experimentele faciliteit voor het delen van inlichtingen en operationele informatie is onderdeel van het real time intelligence field lab. Naar aanleiding van de discussies met belanghebbenden in de internationale zone van Den Haag zal HSD dit field lab koppelen aan het *project gebiedsbeveiliging internationale zône*. Hiermee krijgt het field lab focus, is de internationale zone gediend en wordt concreet een bijdrage geleverd aan het verminderen van de kwetsbaarheid van de internationale zone en het verbeteren van de response in geval van calamiteit.

Serious gaming Lab

In The Hague Security Delta is de afgelopen jaren veel kennis en ervaring opgedaan met serious gaming voor veiligheidsvraagstukken. Op deze basis wil HSD een serious gaming omgeving ontwikkelen waarin rondom visie- en conceptontwikkeling en ramp- en crisismanagement het mogelijk wordt vier dominante situaties rond om de veiligheidsvraagstukken bij elkaar te brengen:

- Publiekprivate samenwerking
- Lokale en regionale samenwerking
- Regionale en bovenregionale samenwerking
- Nationale en internationale samenwerking

Deze serious security gaming en experimenteeromgeving wordt aanpalend en deels geïntegreerd met de andere faciliteiten van het landelijk innovatiecentrum en is daarmee tevens de omgeving

waarin test- en experimenteercapaciteit voor de mensen die in de vier situaties moeten samenwerken. Het snijdt bovendien door alle vijf de innovatiehuizen heen.

Een breed scala aan partijen die betrokken zijn bij the Hague Security Delta beschikken over onderdelen van serious gaming faciliteiten. Het gaat daarbij om simulatieomgevingen, Group Facility technologieën, geschoolde experts in serious gaming methoden en technieken etc. De doelstelling van dit project is om deze faciliteiten bijeen te brengen, daar waar nodig en mogelijk te integreren en zo een hoger kennis- en expertiseplatform te bieden waarin de bovengenoemde doelen nationaal en internationaal kunnen worden aangeboden en vermarkt.

➔ Het HCSS is in de lead. Er is geïnventariseerd welke gaming faciliteiten op de nieuwe locatie van Beatrixkwartier gebundeld ondergebracht worden. Vanuit de gedachte dat dit de zichtbaarheid van de deel faciliteiten verhoogt, aanloop genereert, exploitatie kosten kan drukken en synergie met andere onderdelen van nationaal veiligheidsinnovatie centrum vergroot. 15 mrt 2013 presenteren alvast drie consortia hun respectievelijke projectplannen en business case voor onderwerpen die op de HSD serious gaming dag van 30-11-2012 naar boven kwamen.

Crisis simulatiecentrum

Het crisissimulatiecentrum heeft als doel bedrijven en (semi)publieke organisaties de gelegenheid te bieden te trainen op strategisch, tactisch en/of operationeel niveau met behulp van de state of the art technologie die ingezet wordt op het terrein van het ondersteunen van besluitvorming, het ontwikkelen van handelingsperspectieven, het duiden van informatie, communicatie, het analyseren van mediaberichtgeving en het visualiseren van deze data.

Het crisissimulatiecentrum kent de onderstaande functionaliteiten:

- Het verhuurt de crisissimulatieruimte aan bedrijven en organisaties die zelf niet over een crisisruimte beschikken (zowel om te oefenen als het bieden van ruimte van waaruit de crisis wordt gemanaged indien een organisatie wordt geconfronteerd met een daadwerkelijke crisissituatie of incident);
- Het is de state of the art crisisruimte waarin bedrijven hun nieuwste technologieën kunnen testen op functionaliteit en effectiviteit, deze met behulp van simulaties kunnen testen op crisisteams of deze kunnen presenteren ten behoeve van verkoop;
- Het crisissimulatiecentrum kan - als kennisknooppunt voor universiteiten, hogescholen en het bedrijfsleven - eveneens gebruikt worden voor het observeren en analyseren van besluitvormers, crisismanagers en teams voor wetenschappelijk onderzoek of ten behoeve van assessments;
- Het crisissimulatiecentrum kan ook gebruik worden voor opleiden van functionarissen of het ontwikkelen van competenties die een rol spelen binnen crisisbeheersing.
- Het mogelijk ook dienen als fall back voor NCC

➔ Crisisplan BV. biedt een garantie aan afname van trainingsdagen. De locatie zal dus ingericht moeten worden om dit te faciliteren; dit kan van start als financiering voor inrichting van de locatie georganiseerd is.

4.2 Innovatiehuis Urban Security

4.2.1. Integratie lopende en afgeronde PID projecten

De afgelopen periode zijn de volgende initiatieven ontplooit:

- Living Lab Sociale Veiligheid: een proeftuin voor innovatieve producten, diensten en concepten op het gebied van sociale veiligheid
- De Integrale Veiligheidsmonitor (Ivm): een jaarlijks terugkerend bevolkingsonderzoek naar veiligheid, leefbaarheid en slachtofferschap
- Showcase Veilig Nederland: d.m.v. serious gaming de gevolgen op de omgeving van bouw- en ruimtelijke plannen weergeven
- Secure Haven: heeft als doel voor Den Haag een veilige, aantrekkelijke en duurzame leefomgeving te ontwikkelen, was een aanzet voor project integrale gebiedsbeveiliging
- BeWare project: innovatieve besluitvormingssupport systeem voor de controle en meldkamers door het stroomlijnen van bewakingssignalen door alleen dan de operator te melden/alarmeren als er een risico of bedreiging zich voordoet.
- Vitruv Project: laat stadsontwikkelaars nadenken over veiligheidsvraagstukken

4.2.2. Nieuwe initiatieven en living labs

Integrale gebiedsbeveiliging Internationale Zone

Er zijn in Den Haag 131 internationale instellingen met circa 14.000 medewerkers. Veel daarvan zijn gevestigd in de Internationale Zone. Onder andere Europol en het Joegoslavië tribunaal. In de toekomst wordt hier ook EuroJust gehuisvest. Ook vinden er internationale congressen plaats, met regeringsleiders uit de hele wereld. Om het gebied steeds aantrekkelijker te maken voor organisaties en bewoners, investeert gemeente Den Haag onder meer veel in veiligheid. Dit gaat tot noch toe voor elk gebouw en voor elk event gepaard met eigen fysieke veiligheidsmaatregelen (cameratoezicht, bufferzônes, hekken, bewakers). Met de huidige stand van de technologie kan dit efficiënter én met minder overlast voor de omgeving.

HSD maakt zich er daarom sterk voor de Internationale Zone in te zetten als ‘living lab’ voor integrale gebiedsbeveiliging. Dat houdt in dat er bewezen technologische oplossingen worden geïmplementeerd voor de integrale beveiliging van het hele gebied. Partijen in The Hague Security Delta zijn hierover momenteel met elkaar in gesprek.

➔ Als eerste stap wordt het reeds bestaande Netherlands International Security Forum gevraagd alle partijen/stakeholders rondom de internationale zone Den Haag op te nemen in dit forum. Voorts organiseert de gemeente Den Haag in nauwe afstemming met HSD-office een kleine werkgroep van directe spelers in de m2 rondom World Forum gebouw die de problematiek verder in kaart brengt. De resultaten van deze werkgroep worden gebruikt om de experimenteerfaciliteit van het real time intelligence lab verder vorm te geven. De Nuclear Summit van 2014 en de aanstaande bouw van Eurojust bieden een volgende uitgelezen kans om het real time intelligence field lab verder vorm te geven.

Living Lab Sociale Veiligheid

Living Lab Veiligheid is een nieuw instrument om innovatie in de sociale veiligheid in te zetten om problemen op te lossen. Op de locatie in de openbare ruimte waar het probleem zich manifesteert is een testomgeving gecreëerd voor experimentele maatregelen ter verbetering van veiligheid en leefbaarheid. Onderzoekers kunnen de effectiviteit toetsen en de maatregelen verfijnen voordat invoering op grote schaal plaatsvindt. Een testperiode voorkomt kostbare bijstellingen achteraf en neemt onnodige angsten voor bijeffecten weg. Het is een project van Twynstra Gudde, TNO, de Haagse Hogeschool, het Verwey-Jonker Instituut en het Public Security Innovation Centre. Concreet voorbeeld van een opdracht die is uitgevoerd door het living lab sociale veililgheid is: Het Haagse Parnassia, instelling voor geestelijke gezondheidszorg, heeft een opdracht verstrekt om te onderzoeken en testen hoe de integrale veiligheid incl. andere noodzakelijke wensen rondom een centrum ingericht, gewaarborgd en verbeterd kan worden. Deze opdracht wordt momenteel uitgevoerd. Andere voorbeelden zijn dat er op het terrein van een studentenhuisvesting wordt geëxperimenteerd met cameratoezicht en er een lerend netwerk m.b.t. woninginbraken is opgezet.

➔ Er wordt op dit moment doorgestart. Waarbij weer aangesloten wordt op concrete vragen uit de markt.

4.3 Innovatiehuis Cyber Security

4.3.1. Integratie lopende en afgeronde projecten

De afgelopen periode zijn de volgende initiatieven ontplooit:

- De National Cyber Security Research Agenda (IIP VV)
- Privacy Indentity Lab
- Het voorbereiden van HSD Cyber Security Academy en traineeship
- Het mede opzetten van European Network for Cyber Security (ENCS)

4.3.2. Nieuwe initiatieven en living labs

Cyber incident experience

De Cyber Incident Experience is een setting waarbij operationele ervaring van hedendaagse dreigingen en incidenten binnen enkele weken inzichtelijk wordt gemaakt, zodat hier direct lessen uit kunnen worden getrokken. De verantwoordelijke personen (met name directie en management) van betrokken organisaties worden geconfronteerd met de werkelijke situatie, relevante gerelateerde data en gevolgen van het incident. Op die manier kunnen de juiste vragen gesteld worden om het volledige en ongekleurde inzicht in de situatie te krijgen. Vervolgens kan de juiste expertise ingeschakeld worden om vanuit dat inzicht en met die kennis prioriteiten te stellen, actielijnen uit te zetten en oplossingen aan te dragen.

De belangrijkste aandachtspunten zijn:

- Beleving. Beleving van datgene wat werkelijk is gebeurd, hoe het zo ver heeft kunnen komen en hoe de organisatie er mee om is gegaan. Technisch, organisatorisch en in de media.
- Vertrouwelijkheid. Het incident moet volledig betrouwbaar afgeschermd kunnen worden van de buitenwereld.

- Snelheid. Een kopie van het incident moet zeer kort (maximaal enkele weken) na een incident beschikbaar zijn.
- Expertise. Expertise van de situatie bij de getroffen organisatie en cyberexpertise van het incident en de incident response.
- Oplossingen. Gerealiseerde innovaties gelieerd aan de problematiek van het incident.

Denk bijvoorbeeld aan een vertrouwelijke omgeving waarbij d “Diginotar hack” inzichtelijk wordt gemaakt met zowel de technische details als de organisatorische aspecten voor een select gezelschap van direct betrokkenen (de organisatie zelf, de overheid en andere betrokken instanties) . Daarnaast zou een variant beschikbaar gemaakt kunnen worden waarbij de focus ligt op de hack in combinatie met oplossingen om dit soort zaken tijdig te signaleren en daar optimaal op te reageren. Hierbij komen dan ook de maatschappelijke, internationale en juridische aspecten aan bod.

➔ Met Fox-IT in de lead is een eerste inventarisatie naar marktbehoefte gedaan en concept businesscase opgesteld. Er blijkt behoefte en partijen zijn bereid te betalen voor zo’n experience. Als het consortium en de financiering rond is kan gestart worden met het inrichten van de locatie incl. hard/software en beeldschermen e.d. en wordt het portfolio opgebouwd door twee concrete experiences uit het recente verleden uit te werken.

ENCS

Het in oktober 2012 opgerichte European Network for Cyber Security (ENCS) door KPN, Alliander, DNV KEMA,TNO en Radboud Universiteit is een nieuw kenniscentrum gericht op onderzoek, testen, kennisdelen en training op het gebied van cyber security voor vitale infrastructuren. Deze organisatie is reeds gevestigd op de plek waar ook de andere onderdelen van het nationaal veiligheidsinnovatie centrum bijeen gebracht zullen worden. Dit is een crossover tussen innovatiehuis cyber en bescherming vitale infrastructuur.

Cyber Security Academy

Doel is een brede Cyber Security Academy met een internationale hoogstaande reputatie, die zijn kracht ontleent aan een intensieve ‘Triple Helix’ van overheid, bedrijfsleven en kennisinstellingen samenwerking in Cyber Security. De term ‘Academy’ staat overigens nadrukkelijk niet voor een opleiding volgens een enge definitie met specifieke accreditatie, niveau, bekostiging en dientengevolge een uitsluiting van allerlei andere denkbare vormen van opleiding, onderzoek en kennisvergaring. Academy staat hier voor een ‘joint effort’; een gemeenschappelijk dak waaronder Delft, Leiden, HHS en de cruciale actoren in Cyber Security hun krachten bundelen en ieder hun specifieke expertise, kennis en ervaring inbrengen.

In de bijlage is opgenomen de volledige opdrachtformulering voor het opstellen van een businesscase die uiteindelijk zal moeten leiden tot de oprichting van de Academy met een kick start door bestaande opleidingen en onderzoeksgroepen van TU Delft, Universiteit Leiden en Haagse Hogeschool gezamenlijk onder te brengen.

➔ Een werkgroep onder leiding van Dhr. Eimert van Middelkoop (oud minister van Defensie) en met het HEC als secretaris is aan de slag gegaan met het opstellen van een business case. In eerste aanzet wordt bekeken welke onderdelen van TU Delft, Universiteit Leiden/campus Den Haag en HHS samengebracht worden om vanaf sept 2013 te starten. Medio januari wordt de business case opgeleverd ten behoeve van besluitvorming.

HSD cyber security traineeship

Het doel van het opzetten van een HSD cyber security traineeship is het op korte termijn opleveren van cyber security specialisten. Het is een traineeship dat zowel een publiek (NCSC/Europol) als privaat (Fox-IT, KPN en ..) onderdeel kent. Het biedt ook de mogelijkheid om een gezamenlijke arbeidsmarkt en wervingscampagne onder de vlag van HSD te organiseren.

➔ Op dit moment is een klein werkgroepje gevormd uit het innovatiehuis cyber security met Fox-IT/KPN in de lead en in nauwe afstemming met de HSD-office een businesscase aan het opstellen. Bovendien wordt het gesprek gevoerd met partijen die de uitvoering/traineecoördindatie op zich nemen.

4.4 Innovatiehuis Bescherming Vitale Infrastructuur

4.4.1. Integratie lopende en afgeronde PID projecten

De afgelopen periode zijn de volgende zaken ontwikkeld:

- Interdependency study for ICT en voor Electricity
- Alert System Counter Terrorism
- Strategic Platform for Critical Infrastructure
- Studies on preparation continuity Critical infrastructure during Flu pandemic en evacuation and Critical Infrastructure
- RECIPE: een handboek voor de beveiliging van vitale infrastructuur

4.4.2. Nieuwe initiatieven en living labs

ENCS

Het in oktober 2012 opgerichte European Network for Cyber Security (ENCS) door KPN, Alliander, DNV KEMA,TNO en Radboud Universiteit is een nieuw kenniscentrum gericht op onderzoek, testen, kennisdelen en training op het gebied van cyber security voor vitale infrastructuren. Deze organisatie is reeds gevestigd op de plek waar ook de andere onderdelen van het nationaal veiligheidsinnovatie centrum bijeen gebracht zullen worden. Dit is een crossover tussen innovatiehuis cyber en bescherming vitale infrastructuur.

Daarnaast is het voor de komende periode van belang om concrete casussen te vinden die in een marktomgeving kunnen worden opgepakt.

4.5 Innovatiehuis Forensics

4.5.1. Integratie lopende en afgeronde PID projecten

De afgelopen periode zijn de volgende initiatieven ontplooit:

•CSI The Hague: een demonstratie- en trainingsfaciliteit om virtueel een plaats delict te onderzoeken met 3D scans van de werkelijke plaats delict.

•CBRNe Programme: Het programma van de NFI om CBRNe aanvallen en rampen te voorkomen en te bestrijden.

•NFI Field Lab: Het NFI Field Lab bestaat uit een grote hal waar de plaats delict op schaal gerecreëerd kan worden door middel van gaming technologie.

•NFI Academy: De NFI Academy verzorgt als onderdeel van het Nederlands Forensisch Instituut (NFI) forensische cursussen voor uiteenlopende doelgroepen.

4.5.2. Nieuwe initiatieven en living labs

CSI Lab The Hague

Het NFI heeft in 2011 een revolutionair CSI Lab in gebruik genomen. Het is een demonstratie- en trainingsfaciliteit om virtueel een plaats delict te onderzoeken. Daarvoor leggen forensisch onderzoekers eerst de werkelijke misdaadlocatie vast met 3D-scans, exact zoals de politie de situatie heeft aangetroffen. Later kan men alle gegevens virtueel opnieuw onderzoeken in het CSI Lab. Dat maakt het mogelijk om zelfs jaren later nieuwe hypotheses over de toedracht te toetsen.

CSI Lab The Hague gebruikt bestaande technieken uit vakgebieden als de luchtvaart, medische wetenschap en de game-industrie. In samenwerking met het Amsterdam Medisch Centrum (AMC) wordt een camera ontwikkeld om minutieus bloed- en warmtesporen te traceren en vast te stellen hoe oud ze zijn. Verder krijgen forensisch rechercheurs in het lab met behulp van serious gaming training om sporen te verzamelen. Dit trekt uit de hele wereld forensisch onderzoekers die in het CSI The Hague getraind worden. Het NFI is de projectleider en werkt samen met onder andere Philips, Thales, AMC, TNO, Cap Gemini, TU Delft en Haagse Hogeschool. De eerste fase is afgerond en heeft geleid tot 1 start up bedrijfje en ca. 10 spin off projecten.

➔ Er wordt op dit moment doorgestart. NFI is in de lead en daarbij in overleg met de i.i.g. de huidige consortium partners voor het vervolg. In de volgende fase zullen de resultaten moeten worden doorontwikkeld tot marketable products and services. Het zal hierbij primair gaan om het volgende:

- Tools om microscopische sporenpatronen te vinden, veiligstellen en mogelijkerwijs terplekke te bestuderen.
- Tools om de plaats delict razendsnel 3D te visualiseren en vastleggen, inclusief integrale sporenpatronen.
- Portable tools om razendsnel op de plaats delict richtinggevend forensisch onderzoek te verrichten
- Ontwikkelen digitale forensische technieken
- Tools om CBRNE situaties mee te kunnen onderzoeken.
- Infrastructuur om serious gaming in te doen, met het oog op training van politiepersoneel, mede ook in CBRNE scenario's. Dit zal ook moeten leiden tot geteste best practice protocollen.

Deze toepassingen zullen - mits succesvol - een wereldwijd toepassingsgebied hebben binnen politie, inlichtingendiensten en defensie. Daarnaast ook o.g.v. border security. Een potentieel grote afzetmarkt dus.

5. HSD-OFFICE + OVERIGE HSD-CAMPUS FACILITEITEN

Ten behoeve van de facilitering aan HSD, wordt er een professioneel 'lean en mean' HSD-office met een bepaalde kritische massa van minimaal 5,5 fte opgebouwd.

De werkzaamheden die HSD- office ontplooit zijn onder te brengen in vier functionaliteiten:

1. Netwerkbeheer&facilitering
2. Project(financierings)ondersteuning & kwaliteitsbewaking
3. Communicatie en Public Affairs
4. Internationale business development activiteiten en Acquisitie

Voorlopig is de HSD-office gevestigd aan de Sophialaan 10 als inwoner in het pand van het The Hague Institute of Global Justice. Deze ruimte biedt naast een kantoor met 3 werkplekken, een ontvangst mogelijkheid voor 1 op 1 gesprekken, ook 2 fysieke vergaderplekken en een conferentie capaciteit tot 100 personen. Dit is de plek waar op dit moment de programma directie, projectmedewerkers, innovatiehuisbetrokkenen bijeen komen en waar HSD vergaderingen, brainstorm sessies, thema- en netwerk bijeenkomsten plaats vinden. Op termijn verhuist dit HSD-office naar het Beatrixkwartier, alwaar de fysieke bundeling van HSD gaat plaats vinden.

Communicatie & Public Affairs

Hier omtrent wordt verwezen naar het aparte stuk "HSD alignment- en communicatieplan". Kern hiervan is dat HSD bouwt aan duurzame relaties van HSD-partners voor gezamenlijke belangen en doelstellingen. Communicatie levert bovendien bestaansrecht aan en energie op voor het gezamenlijk doorontwikkelen van het cluster. We vertellen het grotere verhaal, door concrete, praktische en zichtbare zaken en successen van bijvoorbeeld de living labs en nieuwe innovaties uit te venten. Er wordt gewerkt aan een fysieke en digitale community en we zetten met elkaar de agenda in het veiligheidsdomein. We proberen zoveel mogelijk 'free publicity' te generen. Met betrekking tot Public Affairs werken we aan het bij elkaar brengen en uitnutten van de triple helix gedachte en de overheid te bewegen naar het zijn van launching customer voor innovatieve veiligheidsoplossingen. Ook zorgen we ervoor dat alle 'haakjes' in stukken ten behoeve van financieringsbronnen goed staan ten behoeve van HSD en haar partners.

MKB desk

De HSD MKB Desk staat ondernemers bij met praktische hulp en advies, met name op bedrijfskundig en financieel vlak en bij innovatie-trajecten. Adviseurs zoeken samen met ondernemers naar de beste oplossing en begeleiden hen bij de zoektocht naar kapitaal. Ook treden ze op als matchmaker tussen MKB en grote (overheids-)partijen: ze koppelen ideeën, ondernemers en bedrijven en bevorderen onderlinge samenwerking. Tenslotte biedt de HSD MKB Desk onafhankelijk advies bij het vinden van een bedrijfslocatie of zakelijk netwerk.

Business to business ondernemers kunnen bij de HSD MKB Desk terecht als zij (van plan zijn te) innoveren in technologieën en oplossingen voor complexe veiligheidsvraagstukken. Ook starters in het veiligheidscluster zijn welkom. In alle gevallen geldt dat de dienstverlening van het bedrijf aantoonbaar verband moet houden met de belangrijkste thema's van The Hague Security Delta. Alle vragen worden vertrouwelijk behandeld. Een intake gesprek bij de MKB Desk is gratis. Voor leden van The Hague Security Delta is ook het vervolgtraject zonder kosten.

De HSD MKB desk is onderdeel van het HSD-office i.s.m. Syntens, die ook de MKB desk verzorgt voor de gehele topsector HTMS. De adviesgroep bestaat verder uit professionals van Syntens, gemeente Den Haag, TNO MKB en Kamer van Koophandel Den Haag. De adviseurs hebben een goed inzicht in de security sector, het regionale bedrijfsleven en (financiële) regelingen op zowel Europees als regionaal en lokaal niveau. Afhankelijk van de vraag kunnen ondernemers worden doorverwezen naar externe adviseurs en specialisten.

Internationale activiteiten/acquisitie

Partners in The Hague Security Delta ondernemen gezamenlijke initiatieven om het veiligheidscluster internationaal op de kaart te zetten. Op hoofdlijnen gaat het om het:

- het positioneren van Den Haag als dé plek voor internationale veiligheid business;
- initiëren van en deelnemen aan inkomende en uitgaande handelsmissies;
- het onderzoeken en (laten) wegnemen van belemmeringen voor de vestiging van buitenlandse ondernemingen;
- het werven van relevante conferenties en beurzen voor de regio
- het vinden van business development opportunities
- het verkrijgen van leads t.b.v. het acquireren van bedrijven en instituties

➔ Tot medio 1e kwartaal 2013 wordt door de gemeente Den Haag, HSD-office en WFIA/NFIA gewerkt aan een acquisitie en handelsmissie agenda. Hierin wordt vanuit de inhoud en met het oog op logische lijnen en toekomstige kansen bekeken hoe dit te gaan aanpakken en welke inzet we waar op gaan zetten. Ook wordt de samenwerking bezien met o.a. NIDV, PSIC, ROM en het Border Security Innovation Center.

Voor wat betreft internationale promotie van het cluster sluit The Hague Security Delta aan bij de campagne ‘Doing Business First Class” van gemeente Den Haag. Daarin wordt de stad neergezet als aantrekkelijk vestigingsgebied voor veiligheidsbedrijven en –organisaties, hun medewerkers en gezinsleden. Het gunstige internationale ondernemersklimaat en belastingstelsel worden uitgelicht, evenals de aanwezigheid van partners in het veiligheidscluster, gezamenlijke innovatie-initiatieven, de hoogopgeleide internationaal georiënteerde beroepsbevolking en aangename leefomgeving. Daarnaast wordt zoveel mogelijk inhoudelijk aangesloten bij communicatiekanalen van (internationaal georiënteerde) HSD partners en organisaties die Nederland in het buitenland promoten. Met als kernboodschap: “The Hague Security Delta: security port to Europe.” Met als onderbouwing de succesvolle exportpositie van de Nederlandse veiligheidsindustrie en de sterke banden met andere clusters in Nederland en daarbuiten.

Incubator faciliteiten

Het nationaal innovatiecentrum biedt ook een incubatieomgeving waarin ook kleine innovatieve partijen, zich gemakkelijk kunnen aansluiten, dan wel vestigen. Diensten en technologische deeloplossingen kunnen ontwikkelen en testen, in een omgeving waar ook de eindgebruiker aanwezig is, zorgt voor een verbeterde aansluiting tussen vraag(articulatie) en aanbod. Tevens zal advies en coaching verzorgt worden via HSD en het partner netwerk.

Bedrijfsverzamelgebouw (startups en MKB)

De aansluitende gebouwen/faciliteiten van het nationaal innovatiecentrum bieden (voldoende) ruimte om een HSD bedrijfsverzamelgebouw te ontwikkelen. Hierin kunnen startups en MKB bedrijven die relatie hebben tot de veiligheidssector zich vestigen. Door de aanzuigende werking van het nationaal veiligheidsinnovatie centrum en de Cyber Security Academy is het de verwachting dat meerdere bestaande organisaties/bedrijven zich op dezelfde plek willen vestigen.

6. HSD-DEVELOPMENT

Er wordt door HSD aansluiting georganiseerd met de Regionale Ontwikkelingsmaatschappij. Bovendien zorgt gemeente Den Haag in nauwe samenwerking met HSD directie voor een eigen financieringsvehikel om projecten van de grond te krijgen. HSD-innovatie stimuleringsregeling naar model van Brainport development. De gemeente Den Haag heeft reeds toegezegd zich hiervoor in te spannen en financieel bij te dragen. Er is een goedkeuring op de voorlopige aanvraag voor een subsidie in het kader van ‘Kansen voor West/EFRO gelden’ ten behoeve van gezamenlijke huisvesting, fysieke inrichting en bijdrage in de exploitatie van het landelijk innovatiecentrum veiligheid. De definitieve aanvraag is ingediend en 15 mei volgt een formeel akkoord. Met het ministerie van V&J zijn vergevorderde gesprekken over samenwerking. Ook met het ministerie van EZ worden afspraken gemaakt over toegang tot seedsfunds en het financieringsinstrumenten zoals bv de groeifaciliteit.

7. HSD-GOVERNANCE EN BASISFINANCIERING

De kern van de governance is dat er een sturings- en verantwoordingsmodel nodig is om zaken te realiseren en de juiste beweging van HSD in gang te zetten, opdat we de gezamenlijk ambities binnen bereik gaan krijgen. Daartoe wordt een stiching The Hague Security Delta opgericht. Met een HSD-board die de strategische koers bepaald, HSD executive committee als uitvoeringsorgaan en de directie i.s.m. HSD-office als dagelijks uitvoerder. De ‘gouden driehoek’ is vertegenwoordigd in de HSD-board en een bestuurder van de gemeente Den Haag is onafhankelijk voorzitter. Een belangrijk aandachtspunt is de balans tussen de HSD-board en overige aangesloten partijen. Door de geformaliseerde positie van de HSD-partner jaarvergadering, met een toezichthoudende rol, is de juiste balans gevonden tussen de HSD-board partijen en de andere aangeslotenen. De bijdragen van HSD partners wordt bepaald aan de hand pakketten in de partnership. Een premium pakket afhankelijk van de grote van de organisatie met een speciale plek ogv marketing&communicatie en in aanmerking komend voor projecten en consortia, en een regular pakket van overige partners met een beperktere voorzieningen. Er is een matrix opgesteld die aangeeft wat men van HSD mag verwachten per vorm van partnership.

The Hague Security Delta

Sophialaan 10
2514 JR The Hague
The Netherlands

2508 CP The Hague,
The Netherlands
T +31(0)70 302818

info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
Join us on Twitter: @HSD_NL