Nationale Innovatieagenda Veiligheid 2015

Publiek-privaat innoveren voor veiligheid en welvaart

The Hague Security Delta

Nationale Innovatieagenda Veiligheid 2015

The Hague Security Delta

Nationale Innovatieagenda Veiligheid 2015

Publiek-privaat innoveren voor veiligheid en welvaart

The Hague Security Delta

Voorwoord

Nederland is een aantrekkelijk land om in te wonen, te werken en te investeren. Veiligheid schept daarbij de voorwaarde voor maatschappelijke stabiliteit en economische ontwikkeling. Als Nederland geen veilige en stabiele maatschappij zou zijn, was Amsterdam niet uitgegroeid tot een wereldspeler op het terrein van internet exchange en hadden de mainports Rotterdam en Schiphol nooit hun spilfunctie kunnen vervullen. Den Haag zou niet internationaal erkend zijn als stad van Vrede en Recht en de regio Eindhoven zou niet aangemerkt zijn als een van de meest innovatieve regio's van de wereld. Deze sterke uitgangspositie moeten we behouden in een snel veranderende, steeds competitievere wereld. Daarom is het van belang dat veiligheid als belangrijke economische sector wordt erkend. Innovatie en banen scheppen zijn hier twee zijden van dezelfde medaille. Voorwaarde voor succes is dat het bedrijfsleven, de kennisinstellingen en de overheid zich daar gezamenlijk, ambitieus, wendbaar, met overtuiging en blijvend voor inzetten.

Het nationale veiligheidscluster The Hague Security Delta (HSD), met als voornaamste geografische concentraties Den Haag, Brabant en Twente, heeft hierbij een belangrijke aanjagende, organiserende en coördinerende rol. Dat juist HSD een Nationale Innovatieagenda voor Veiligheid opstelt, is dus geen toeval. De innovatieagenda verbindt de vier o's van *overheid, onderzoek, opleiden en ondernemen*, en steunt zo de ambities van het regeerakkoord. Door deze publiek-private samenwerking komt de door de Wetenschappelijke Raad voor het Regeringsbeleid zo noodzakelijk geachte kennis-circulatie tot wasdom, waardoor meer veiligheid en meer banen ontstaan.

Deze agenda is een bron van inspiratie voor alle partijen die zich willen committeren aan innovatie en economische ontwikkeling. De agenda biedt tegelijk richting en ruimte door een aantal innovatiespeerpunten te benoemen die gezamenlijk in een groeiproces kunnen worden gerealiseerd. Hierdoor zijn overheden, bedrijven en kennisinstellingen beter in staat hun kennisontwikkeling, innovatie-inspanningen en verwervingsbehoeften op elkaar af te stemmen. Voor de behoeftestellers en opdrachtgevers in het veiligheidsdomein resulteert dit in meer waarde voor hun geld; voor de aanbieders ontstaat een robuuste en voorspelbare markt. De agenda biedt zo een fundament voor de ontwikkeling van krachtige, internationaal opererende consortia, zodat Nederland in Europa op het terrein van innovatieve veiligheidsoplossingen een economische speler van formaat blijft. Met deze agenda sluit Nederland naadloos aan op innovatiedoelstellingen van de Europese Commissie, zoals geformuleerd in het onderzoeksprogramma Horizon 2020. Ook in dit programma staat de samenwerking tussen bedrijven, overheden, kennisinstellingen en wetenschap centraal. Deze nationale agenda heeft dus een internationale uitstraling.

Ik ben blij dat er nu een publiek-private agenda ligt die richting geeft aan innovatie en economische ontwikkeling op het gebied van veiligheid. Met dank aan de opstellers en iedereen die aan deze agenda heeft bijgedragen.

Prof. dr. Rob de Wijk
Algemeen Directeur The Hague Security Delta

Inhoudsopgave

‘We moeten hard werken aan inclusieve of integrale innovatie. Daarbij gaat het om vernieuwingen die niet alleen leiden tot economische en maatschappelijke groei, maar tegelijkertijd ook tot méér veiligheid.’[1] Ivo Opstelten

Inleiding en leeswijzer

De Nationale Innovatieagenda Veiligheid 2015 (NIAV) biedt een visie op belangrijke vernieuwingsprojecten voor nationale veiligheid in de komende drie tot vijf jaar, met een doorkijk naar de komende tien jaar. Deze publiek-private agenda richt zich op een combinatie van technologische, sociale en procesinnovaties die een gezamenlijke aanpak vereisen van behoeftestellers, ontwikkelaars en eind-gebruikers. Het doel ervan is om op afzienbare termijn maatschappelijke en economische waarde te creëren.

Door vraag en aanbod te verbinden, voorziet de NIAV in een samenhangend handelingsperspectief voor de centrale en decentrale publieke sector, voor private vragers en aanbieders van innovatieve producten en diensten, en voor kennisinstellingen in het veiligheidsdomein. Bedrijfsleven, overheden en kennisinstellingen, samen wel de *triple helix* genoemd, kunnen zo vroegtijdig de vraag naar innovatieve veiligheidsoplossingen laten aansluiten op de innovatiekracht die ze door een goede samenwerking kunnen ontwikkelen. Daarnaast zorgen zij voor een valide verdienmodel voor de invoering van deze oplossingen.

De NIAV is niet alleen een product, maar ook een proces: de agenda wordt regelmatig bijgesteld op basis van behaalde resultaten en nieuwe inzichten; het gaat er vooral om de innovatiespeerpunten te realiseren. Het nationale veiligheidscluster *The Hague Security Delta* (HSD) stelt de agenda op, beheert deze als product, en ondersteunt de agenda als proces. Onder de merknaam The Hague Security Delta zijn verenigd de triple-helixinitiatieven uit de regio Twente (TS&S, Twente Safety & Security), de regio Brabant (DITSS, Dutch Institute for Technology, Safety & Security) en de regio Den Haag.

Leeswijzer

Hoofdstuk 1 beschrijft doel en positionering van de NIAV, en het proces dat tot de agenda heeft geleid. Hoofdstuk 2 vormt de feitelijke innovatieagenda voor 2015. Dit hoofdstuk is gestructureerd in zes thema's met grote uitdagingen en kansen voor vernieuwing op voorwaarde dat er wordt samengewerkt in triple-helixverband. Per thema richten we de aandacht op enkele specifieke speerpunten die de komende paar jaar tot concrete innovaties kunnen leiden, hiermee krijgt de agenda inhoud en richting. Hoofdstuk 3 richt zich op de realisatie van de agenda. Essentieel is de tabel waarin we de innovatiespeerpunten koppelen aan partijen die de verantwoordelijkheid willen en kunnen nemen om de innovatie te ontwikkelen, toe te passen en op de markt te brengen. Verder leggen we in dit hoofdstuk de verbinding tussen de innovatie-speerpunten en de grote verwervingstrajecten in het veiligheidsdomein. In hoofdstuk 4 verdiepen we de context waarbinnen de NIAV zijn werking krijgt. Dit hoofdstuk is van belang om de wisselwerking te begrijpen tussen een aantal bredere maatschappelijke ontwikkelingen en de NIAV als product en proces. Hoofdstuk 5 ten slotte geeft enkele afsluitende procesoverwegingen.

De lezer die inhoudelijk geïnteresseerd is in de Nationale Innovatieagenda Veiligheid 2015, kan volstaan met hoofdstuk 2. Voor inzicht in hoe de uitwerking van de speerpunten vorm krijgt, is het goed om ook hoofdstuk 3 te lezen.

‘Publiek-private samenwerking op het terrein van veiligheid brengt het beste in alle partijen naar boven. De overheid kan leren van de private sector en omgekeerd. Die vruchtbare wisselwerking leidt tot synergie, een belangrijke meerwaarde waar we allemaal van profiteren.’[2] Ivo Opstelten

1 – Doel en proces Nationale Innovatieagenda Veiligheid

Lokale, regionale en nationale overheden hebben als kerntaak onze veiligheid te garanderen.[3]

1.1 Waarom en wat levert het op?

Nederland investeert de komende jaren miljarden euro's uit de publieke middelen in de veiligheid van de samenleving. Maar ook semipublieke en private instanties en bedrijven investeren in oplossingen die bij veiligheidsdreigingen of -incidenten de continuïteit moeten waarborgen. Bijvoorbeeld in vitale sectoren als energie, telecom, water, transport en financiële infrastructuur. Dit gebeurt in de context van een dynamische samenleving met soms snel veranderende risico's en dreigingen, veiligheidsarrangementen en technologische mogelijkheden. Innovatie is essentieel om deze veranderingen het hoofd te kunnen bieden en ervan te kunnen profiteren.[4] Investeringen in veiligheid moeten een vernieuwend karakter hebben, ook als dat 'vervangingsinvesteringen' zijn. Optimaal gebruikmaken van de innovatiekracht van bedrijven, overheden en kennisinstellingen[5] is vereist.

Een tweede sleutelfactor is de schaalvergroting van veiligheidsvraagstukken door toenemende afhankelijkheden, die het noodzakelijk maakt om over geografische, functionele, hiërarchische en systeemgrenzen heen te kijken. Verbetering is nodig om te komen tot het door alle actoren beoogde effect: meer *waarde voor geld* als resultaat van de investeringen in veiligheid.

Tijdens het congres *Veilig door Innovatie* op 10 oktober 2013 is door vertegenwoordigers van bedrijven, overheden en kennisinstellingen de behoefte geformuleerd om de krachten te bundelen in het gefragmenteerde veld van publieke en private veiligheidspartners. Een gemeenschappelijke innovatieagenda draagt daaraan bij. Het ministerie van Veiligheid en Justitie en The Hague Security Delta (HSD) hebben – namens deze groep – het initiatief genomen deze Nationale Innovatieagenda Veiligheid op te stellen op basis van beschikbaar materiaal, gebaseerd op drie pijlers:

- de vraag- en behoeftestelling van partijen die moeten bijdragen aan maatschappelijke veiligheid;
- aanbodgerichte, technologische of innovatieve ontwikkelingen en trends;
- ruimte voor niet-benoemde initiatieven.

In de periode maart tot en met oktober 2014 hebben we het beschikbare materiaal doorgenomen en veel gesprekken gevoerd met belanghebbenden in het veiligheidscluster. Dit heeft geleid tot deze Nationale Innovatieagenda Veiligheid (NIAV).

Doelstelling Nationale Innovatieagenda Veiligheid
De Nationale Innovatieagenda Veiligheid is een agenda van publieke en private partijen gericht op het gezamenlijk stimuleren en organiseren van innovaties. De NIAV biedt overzicht en stelt prioriteiten die partijen in de triple helix gezamenlijk kunnen aanpakken. Dit stelt overheden, bedrijven en kennisinstellingen in staat hun innovatie-inspanningen op elkaar af te stemmen, naar synergie te streven en innovaties te verbinden aan toekomstgerichte verwervingstrajecten. Aanbieders van innovatieve producten en diensten zijn zo beter verzekerd van een robuuste en voorspelbare markt. De NIAV biedt zo een samenhangend perspectief om innovaties maatschappelijk en economisch optimaal te laten renderen.

'Kennis en Innovatie is geen doel maar een middel om maatschappelijke en economische impact te bereiken. Open samenwerking tussen overheid, bedrijfsleven en kennisaanbieders staat hier ten dienste aan.'[6] Erik Akerboom

We lopen de belangrijkste elementen van deze doelstelling kort langs.

Collectieve agenda
De NIAV is opgesteld onder de vlag van het nationale veiligheidscluster HSD. In Nederland zijn de afgelopen paar jaar diverse regionale initiatieven ontstaan die werken aan veiligheidsinnovaties in triple-helixverband en zo economische ontwikkeling stimuleren. Het gaat om Twente Safety & Security (TS&S) in de regio Twente, het Dutch Institute for Technology Safety & Security (DITSS) in Noord-Brabant en HSD in Den Haag en omgeving. TS&S, DITSS en HSD hebben in een convenant vastgelegd dat zij intensief samenwerken en dat HSD de gezamenlijke belangen behartigt op nationaal en overkoepelend niveau. DITSS en TS&S maken daartoe deel uit van het bestuur van HSD. Daarmee is feitelijk een nationaal veiligheidscluster ontstaan, met *The Hague Security Delta* als merknaam voor de (inter)nationale positionering van de Nederlandse kennis en kunde op dit gebied.[7]

Oplossingsgerichte innovatie in triple-helixverband
De NIAV heeft een verbindend en systeem-georiënteerd karakter. De agenda richt zich op innovaties die een brede, gezamenlijke aanpak vragen van behoeftestellers, ontwikkelaars en eindgebruikers en die een combinatie vormen van techniek, mensen en organisatie. Inzet van proeftuinen, *living labs*, experimenten en dergelijke is belangrijk om deze combinaties te kunnen maken. Het gaat in de NIAV om toegepaste innovatie met resultaten in de komende drie tot vijf jaar. De NIAV is geen technologieradar of horizonscan gericht op opkomende technologieën die pas op lange termijn tot innovatie leiden.

Overzicht en prioriteit
Er bestaan al vele kennis- en innovatieagenda's in de publieke en private sfeer die de belangen, doelen, behoeften en mogelijkheden van belanghebbenden in het veiligheidsdomein verwoorden. De NIAV bevat geen eigen analyse van de vraag naar of het aanbod van innovatieve veiligheidsoplossingen, maar bouwt juist voort op de inzichten uit deze bestaande visies, agenda's, *roadmaps* en lopende en geplande innovatietrajecten. Wel kent de NIAV een eigen indeling die de dwarsverbanden benadrukt tussen vraag en aanbod en tussen maatschappelijke en economische businesscases. Binnen deze structuur maken we een selectie van speerpunten aan de hand van een toetsingskader.

Hefboomwerking
Een belangrijke functie van de NIAV is het expliciet maken, bundelen en onderschrijven van de vraag door de behoeftestellers.[8] Door verschillende belanghebbenden met hun eigen innovatiebudgetten aan onderwerpen en prioriteiten te koppelen, en vice versa, en door hun innovatie-inspanningen te synchroniseren, wordt de agenda concreet en actiegericht en ontstaat schaalvoordeel en hefboomwerking.

Verbinding met verwervingstrajecten
Essentieel voor de maatschappelijke en economische waardecreatie is de verbinding tussen de NIAV en de verwervingsagenda's van de belangrijkste vragende partijen, zowel overheden als bedrijven met name in de vitale sectoren. Het is immers pas zinvol te investeren in innovatie als er zicht is op mogelijke *return on investment*. Aan de vraagzijde is dit uit te drukken in oplossingen die ook op termijn effectief blijven. Aan de aanbodzijde gaat het erom dat er een gerede kans bestaat dat de investeringen zich vertalen in producten en diensten die op termijn omzet en rendement genereren. Alleen dan zullen zich coalities van partijen vormen die zich willen committeren aan het traject van ontwikkeling en op de markt brengen van de betreffende innovaties.[9]

Handelingsperspectief gericht op maatschappelijk en economisch rendement
Er is sprake van een duidelijk urgentiegevoel rondom het thema veiligheid: zonder gerichte inspanningen zal de overheid immers steeds meer moeite krijgen om burgers en samenleving veiligheid te bieden, verliest Nederland als kennis- en innovatieland aan kracht en zal het bedrijfsleven aan internationale concurrentiekracht en verdienvermogen inboeten.

'De overheid moet helpen te versnellen. Door nieuwe kennis en innovatie in te zetten, kunnen we koploper in de wereld worden en kunnen we de dagelijkse operationele ervaring koppelen aan de ontwikkeling van morgen.'[10] Menno van de Marel

De NIAV vormt een belangrijk instrument om deze druk te vertalen in concrete trajecten die tot tastbare resultaten leiden. De in de NIAV opgenomen speerpunten zijn geselecteerd op hun potentie om zowel maatschappelijke als economische waarde te creëren. Dit doet recht aan de onderscheidende belangen en is de basis voor een vruchtbare samenwerking in triple-helixverband.

1.2 Rollen en verantwoordelijkheden

Het nationale veiligheidscluster HSD is aanjager, opsteller, facilitator en beheerder van de NIAV. Het cluster biedt een open en vertrouwde omgeving waarin samenwerkingsverbanden kunnen worden gevormd rond kennis- en innovatietrajecten. Deze mix van openheid en versterkt onderling vertrouwen is noodzakelijk om de nieuwe samenwerkingsvormen en zakelijke modellen die van belang zijn om de NIAV te realiseren, daadwerkelijk van de grond te krijgen. De partners van het cluster zijn de eerst aangewezenen om de samenwerking rond de in de agenda opgenomen innovatiespeerpunten vorm te geven, zich daaraan te verbinden en te laten zien dat het werkt.

De NIAV stelt zich ook tot doel om de behoefte aan, en vraag naar veiligheidsoplossingen te bundelen. De vraag articuleren en bundelen vanuit de publieke veiligheidspartijen, is gebaat bij regievoering. Het **ministerie van Veiligheid en Justitie** (VenJ) heeft hierin een duidelijke rol. VenJ stimuleert dat overheidspartijen op het terrein van veiligheid gerichte innovatievragen stellen en maakt deze toegankelijk voor geïnteresseerde bedrijven en kennisinstellingen. De regierol van VenJ krijgt momenteel vooral invulling door ondersteuning, ofwel 'lichte regie'. Partijen die er onderling niet uitkomen en behoefte hebben aan een partij die vanuit een overkoepelend perspectief prioriteiten kan stellen, ofwel 'zware regie', kunnen hiervoor ook een beroep doen op VenJ. Tegelijk

heeft VenJ geen systeemverantwoordelijkheid en is hij ook niet politiek aanspreekbaar op de NIAV.
Het **ministerie van Defensie** formuleert welke militaire behoeften de krijgsmacht heeft om de rol van structureel veiligheidspartner te kunnen vervullen. De Versterking Civiel-Militaire Samenwerking (VCMS) richt zich onder meer op gezamenlijke kennisopbouw en innovatie. De NIAV ondersteunt en bouwt voort op VCMS-initiatieven.
Het topsectorenbeleid van het **ministerie van Economische Zaken** schraagt de triple-helixsamenwerking in het nationale veiligheidscluster. Hoewel de nadruk ligt op economische waardecreatie, is in dit beleid ook aandacht voor maatschappelijke waardecreatie. Maatschappelijke veiligheid is voor alle sectoren van belang voor bedrijfscontinuïteit en klantbescherming.

'HSD stimuleert, faciliteert en organiseert samenwerking tussen bedrijven, overheid en kennisinstellingen op het gebied van veiligheidsvraagstukken.'[11] Rob de Wijk

Per innovatiespeerpunt in de NIAV moet een partij uit het nationale veiligheidscluster zich opwerpen als **speerpunttrekker**. Dat houdt in dat die partij de verantwoordelijkheid op zich neemt om een samenwerking op dat speerpunt tot stand te brengen en op gang te houden. Coalitievorming is een belangrijke eerste stap. De feitelijke uitvoering, financiering en borging van de activiteiten van een speerpunt is en blijft een verantwoordelijkheid van de bijdragende partijen zelf.

1.3 Totstandkomingsproces

We hebben de betrokkenen bij het nationale veiligheidscluster benaderd om de agenda tot een gezamenlijk product te maken. Dit is geen eenmalige actie, maar een doorlopende activiteit waarmee we de NIAV periodiek actualiseren. In de periode maart tot november 2014 hebben we het volgende proces doorlopen.

1 Inventarisatie en analyse van een groot aantal kennis- en innovatieagenda's in het veiligheidsdomein.[12] Op basis hiervan hebben we een initiële thematische structuur opgesteld die ordening geeft aan de actuele uitdagingen in het veiligheidsdomein. Dat gebeurde primair redenerend vanuit de vraagzijde, maar zonder de aanbodzijde, de zogenaamde '*technology push*', te veronachtzamen. Binnen deze globale structuur stelden we een *longlist* op van onderwerpen en lopende initiatieven.

2 Deze longlist diende als basis voor een inventarisatieronde, waarin we een grote groep betrokkenen hebben geraadpleegd, zie bijlage 1. We vroegen hen om de belangrijkste innovatiespeerpunten in triple-helixverband zo duidelijk mogelijk weer te geven vanuit hun eigen perspectief.

3 De uitkomsten van de inventarisatieronde hebben we gebruikt om de initiële thematische structuur aan te passen en speerpunten te selecteren aan de hand van een toetsingskader, zie volgende paragraaf. Daarmee ontstond een *shortlist*. Dit alles is vastgelegd in een conceptversie van de NIAV die is getoetst in het Executive Committee en de HSD-Adviesraad. Een belangrijk element in deze toetsing is het uitzicht op commitment van triple-helixpartijen om daadwerkelijk bij te dragen aan de realisatie van de innovatiespeerpunten.

4 De commentaren en suggesties uit de inventarisatie- en toetsingsronde hebben we verwerkt in een concept van de NIAV 2015. De HSD-Board heeft op 29 september 2014 ingestemd met dit concept. De NIAV 2015 is op 26 november 2014 bekrachtigd door een aantal bestuurders uit het veiligheidsdomein.[13]

Het totstandkomingsproces van de NIAV doorliep niet alleen deze vier stappen, maar was ook ingebed in diverse netwerkactiviteiten binnen het veiligheidscluster. Deze activiteiten hebben bijgedragen aan vorm en inhoud van de agenda. Omgekeerd stimuleert de NIAV, als proces en product, de kenniscirculatie binnen het veiligheidsdomein. Tot slot: de NIAV is een levend document dat we jaarlijks actualiseren. De NIAV 2015 is in die zin een momentopname; tussentijdse nieuwe initiatieven en thema's zijn voortdurend mogelijk.

1.4 Toetsingskader

In het totstandkomingsproces is een toetsingskader gebruikt om de zich ontwikkelende agenda voortdurend toe te spitsen en te ijken. Dat gebeurde aan de hand van deze criteria:

1 Er moet sprake zijn van een **wezenlijke en actuele tekortkoming of behoefte**; de maatschappelijke waarde.

2 Die tekortkoming of behoefte vraagt om een **breed toepasbare en inzetbare oplossing** op systeemniveau,[14] vaak in combinatie met technologische, sociale en procesinnovatie.

3 Daarbij is een **gezamenlijke aanpak** van behoeftestellers, eindgebruikers, innovators en leveranciers van producten en diensten noodzakelijk of ten minste wenselijk, de zogenaamde triple-helixaanpak.

4 Die aanpak leidt tot innovatietrajecten met de potentie van **significante of substantiële marktomzet**, economische waarde en exportpotentieel.

5 Zwaarwegend is dat er aantoonbaar **draagvlak en commitment** bestaat bij een '*coalition of the willing and able*' in triple-helixverband, die de innovatie wil ontwikkelen, toepassen en op de markt wil brengen en wil aansluiten op investeringsagenda's of strategievisies; het proces van totstandkoming van de NIAV moet garanderen dat dit het geval is.[15]

6 De innovatietrajecten kunnen tot **resultaten leiden in de komende drie tot vijf jaar**.[16]

Er is dus geen sprake geweest van een formeel waarderings-proces van alle mogelijkheden om tot een selectie te komen. Dat zou niet alleen een zeer tijdrovend proces zijn, maar waarschijnlijk ook een proces dat zeer lastig op objectieve en inclusieve wijze ingericht zou kunnen worden.

2 – De Nationale Innovatieagenda Veiligheid 2015

Het proces beschreven in paragraaf 1.3 heeft geleid tot een lijst van zestien speerpunten, die we in zes thema's hebben geclusterd. Hoewel vrij breed geformuleerd, weerspiegelen de thema's op zich al de actuele dynamiek in het veiligheidsdomein. Binnen de thema's leggen de innovatiespeerpunten opnieuw specifieke accenten. De speerpunten zijn nader beschreven in de tabel 3.1.

Thema 1 – Samenwerken in netwerken en systemen
Thema 2 – Sociale innovatie voor veiligheid in de samenleving
Thema 3 – Weerbare vitale infrastructuur
Thema 4 – Handelingsgerichte informatievoorziening
Thema 5 – Waarneming met onbemande systemen
Thema 6 – Procesinnovatie in en tussen professionele organisaties

'De Nederlandse Veiligheidsbranche herkent de in de agenda geschetste ontwikkelingen, de opgenomen thema's zijn zeer herkenbaar als thema's waarop innovatie gewenst en mogelijk is.'[18] Laetitia Griffith

Thema 1 – **Samenwerken in netwerken en systemen**

Samenwerken in netwerken en systemen

Het concept *veiligheid* heeft de afgelopen twee decennia een ontwikkeling doorgemaakt van verbreding en vervlechting die voortkomt uit de opkomst van nieuwe en meer omvattende dreigingen.

Bijvoorbeeld: criminaliteit en aanvallen in het cyberdomein, grensoverschrijdende georganiseerde misdaad, mondiale instabiliteit als bedreiging van handel en economische groei, en internationaal terrorisme.

Initieel werd als reactie op deze ontwikkelingen van bedreigingen ook aan de responskant verbreding en vervlechting zichtbaar. In 2007 is de Strategie Nationale Veiligheid opgesteld om integrale risicobeoordelingen en integrale capaciteitsafwegingen mogelijk te maken. Veiligheidspartijen zijn zowel horizontaal als verticaal meer geïntegreerd gaan werken. Een tendens die heeft geleid tot onder meer veiligheidsregio's, versterking van civiel-militaire samenwerking, de instelling van de Nationale Politie, en uitbreiding van procedures voor bovenregionale crisissamenwerking. De integrale aanpak van veiligheid wordt meer en meer ook intrinsiek gedreven. Een adequate aanpak van vraagstukken als stedelijke of digitale veiligheid vereist nauwe afstemming tussen diverse beleidsterreinen en samenwerking van veel partijen, waaronder burgers en bedrijven, zie ook Thema 2: Sociale innovatie voor veiligheid in de samenleving. Maar ook wet- en regelgeving moet zo nodig snel kunnen volgen om niet als rem op noodzakelijke vernieuwing te werken. Verder vormen privacy, ethiek en besturingsvraagstukken belangrijke randvoorwaarden, en soms beperkingen, voor veiligheidsoplossingen.

Veiligheid kortom, is steeds meer een netwerkvraagstuk. Oplossingen moeten bedacht worden in een ecosysteem van allerlei verschillende publieke en private partijen die elkaar, al dan niet geregisseerd, weten te vinden. De netwerkverbanden zijn soms kort en tijdelijk van aard; iets wat met het toegenomen aantal partijen die een rol in veiligheid hebben, waaronder burgers en bedrijven, misschien wel meer en meer het geval is. Dat stelt extra eisen aan de processen, structuren en systemen gericht op snel, ad hoc en tegelijk betrouwbaar, koppelen van actoren in netwerken en ketens. Nieuwe manieren van coalitievorming en samenwerking zijn nodig. Het opzetten van pre-competitieve expirimenteeromgevingen kan daarbij behulpzaam zijn.

Innovatiespeerpunten:

1 Regievoering vraagarticulatie 'één overheid'

De bepalende rol van de overheid in het (publieke) veiligheidsdomein is onmiskenbaar. Meer focus, massa en gezamenlijkheid in vernieuwingstrajecten begint dus bij het beter op elkaar afstemmen en bundelen van de visie op, behoefte aan en feitelijke vraag naar innovatie bij de overheid. Het is van belang dat de publieke veiligheidspartners hun innovatievragen bij overlap bundelen en gecoördineerd uitzetten bij onderzoeksinstituten, bedrijven, nationale innovatiefondsen en het Europese innovatiefonds Horizon 2020. De rem die achterlopende wet- en regelgeving op innovatieve toepassingen kan zetten, moet zowel zorgvuldig als slim en snel worden verminderd. Innovatie in ons veiligheidssysteem vergt een nauwkeurig balanceren tussen rechtszekerheid en zorgvuldigheid versus de gewenste of noodzakelijke snelheid en flexibiliteit van handelen, rekening houdend met de verdeling van rollen, taken en bevoegdheden in ons veiligheidssysteem. Dit laatste is ook van belang als er behoefte is aan, of voordelen of kansen zijn verbonden aan gezamenlijk en/of schaalbaar ontwikkelen en inkopen.

2 Leren van incidenten en oefeningen

De *Staat van de Rampenbestrijding 2013* constateert dat na incidenten en oefeningen nauwelijks wordt geëvalueerd. Praktijklessen worden slecht geleerd, of wel geleerd, maar niet in verbetertrajecten vervat. Het probleem ligt vaak niet binnen organisaties, maar juist in de complexere leerlussen die over het netwerk van veel verschillende organisaties heen liggen. Er is een uitdrukkelijke behoefte om van incidenten te leren. *Serious gaming* kan hier een belangrijke rol spelen, zie ook Thema 6: Procesinnovatie in en tussen professionele organisaties.

3 Waardecreatie in triple-helixinnovatie

Dit is een innovatieopdracht die de partners in het nationale veiligheidscluster zich in belangrijke mate zelf moeten aantrekken. Drie proceselementen staan centraal. Ten eerste de zakelijke kant van innovatie met elementen die geregeld moeten worden, zoals *intellectual property* (IP), resultaten gebruiken in product-marktcombinaties en het proces van innovatie naar aanbesteding. Ten tweede het samenstellen van coalities waarin onderling vertrouwen ontstaat. Ten derde het zorgen voor optimale cross-overs tussen technologieën, tussen en over toepassingsgebieden, en tussen maatschappelijke en economische waardecreatie. Vaak worden verfrissende, ongezochte ideeën geboren in interacties tussen mensen uit verschillende disciplines en vakgebieden – ook wel *clash of disciplines, wildcard*-innovatie genoemd – of tussen ontwikkelaars en eindgebruikers. Kansrijke innovaties ontstaan als partners kiezen voor open innovatie en integraal, intersectoraal, internationaal en inclusief te werk gaan. De thema's die in de agenda zijn opgenomen, worden in hun ontwikkeling zo veel mogelijk geschraagd, verrijkt en getest door *Concept Development & Experimentation*-processen in programma's, projecten, innovatiehuizen, netwerken, *living labs* en operationele experimenten waarin veiligheidsoplossingen worden geconcipieerd, getoetst en/of doorontwikkeld.[19]

Thema 2 – **Sociale innovatie voor veiligheid in de samenleving**

Sociale innovatie voor veiligheid in de samenleving

Bedrijven, maatschappelijke organisaties en burgers zijn steeds vaker onmisbaar voor duurzame oplossingen.[20] Sociale innovatie in veiligheid vertrekt vanuit de betrokkenheid en de bewustwording van burgers, kennisinstellingen, overheden, maatschappelijke organisaties en bedrijven. Deze partijen ontplooien zelf initiatieven die kunnen groeien doordat andere actoren en partijen het belang hiervan inzien. Sociale netwerken en sociale media kunnen daarbij een belangrijke rol spelen, met de overheid in een faciliterende en soms aanjagende functie.

Veiligheid in en van de samenleving is pas echt ingebakken als zij van het begin af aan wordt meegenomen in het ontwerp van allerlei maatschappelijke functies, zoals wonen, werken, bewegen en recreëren en de bijbehorende infrastructuur. Eerdere initiatieven laten zien dat burgers, bedrijven en maatschappelijke organisaties geïnteresseerd zijn om hierin een actieve rol te spelen, zoals bij zorgen voor veiligheid rondom het spoor, bij agressie tegengaan in het openbaar vervoer, bij gezamenlijk voor meer veiligheid zorgen in wijken en buurten, bij uitgaansgeweld tegengaan of zorgen voor collectieve veiligheid op industrieterreinen. Dit vergt nieuwe manieren van organiseren, over professionele grenzen heen durven denken, herdefiniëren van traditionele rollen en verantwoordelijkheden. De huidige nadruk op *onveiligheid bestrijden* gaat plaatsmaken voor *veiligheid ontwerpen*.
Op terreinen zoals zorg, onderwijs en gezondheid worden maatoplossingen meer en meer toegesneden op de individuele behoefte. Dat gaat ook gebeuren voor veiligheid. Van een situatie waarin professionals bepalen wat er gebeurt, eventueel met ondersteuning van de burgers, gaan we op termijn naar een situatie waarin vaak het omgekeerde geldt. Burgers – 7,5 miljoen huishoudens in bijna 12.000 buurten – bepalen, professionals ondersteunen. De overheid houdt de regie over externe en fysieke veiligheid, is verantwoordelijk voor wet- en regelgeving en dwingt die af als grenzen overtreden worden.

Innovatiespeerpunten:

4 Sociale innovatie en zelforganiserend vermogen

De maatschappelijke weerbaarheid en zelfredzaamheid moet worden versterkt.[21] Dit kan door gebruik te maken van het zelforganiserend vermogen van de samenleving, met de overheid in een stimulerende en regisserende rol. Belangrijke opgaven zijn nieuwe, passende vormen van zelforganiserend vermogen vinden en bieden, en maatschappelijke krachten ontsluiten en organiseren. Burgers kunnen een eigen informatiepositie opbouwen die ze perspectief geeft en in staat stelt om actief te participeren in veiligheidsdiscussies die hen direct raken. Sociale media, mobiele applicaties, domotica, het *internet of things* en het semantische web kunnen daarbij een belangrijke rol spelen.

5 Bewustwording: perceptie versus realiteit

In een complexe, dynamische samenleving komen er voortdurend risico´s bij, terwijl andere risico´s afnemen of wegvallen. Weten dat er gevaren zijn en bewust zijn van deze risico's is van belang om de juiste maatregelen te nemen.[22] Het is vaak moeilijk in te schatten of, wanneer en in welke omvang en vorm mogelijke gevaren actueel kunnen worden. Er heerst vaak een gevoel van – toenemende – onveiligheid waar de cijfers anders uitwijzen. Voortdurend de realiteit duidelijk overbrengen aan de samenleving is van groot belang om passende handelingsperspectieven te geven. Hier kunnen open data en een opendatasamenleving een belangrijke rol spelen.

6 *Security by design* in stedelijke voorzieningen en bij evenementen

Het voorkomt onnodige kosten achteraf als vanaf de start-, ontwerp- of gunningsfase veiligheidsimplicaties – met de nadruk op sociale veiligheid – worden meegenomen als een belangrijke factor naast andere ontwerpparameters, zoals privacy, architectuur, schoonheid of verdienmodellen. Veilige en aantrekkelijke evenementen blijken verder een aanwijsbaar economisch effect te hebben op de omgeving waarin zij plaatsvinden. Inmiddels laten diverse proeven zien dat voor veilige en aantrekkelijke evenementen innovatieve technologieën, bijvoorbeeld *Sensing*[23], belangrijke bijdragen kunnen leveren. Het naar de markt brengen van sociale innovaties gaat maar langzaam.
Er is sterke behoefte aan hoogwaardige systeemintegratoren die deeloplossingen aan elkaar verbinden om tot integrale en vernieuwende oplossingen te komen, ook als businessmodel. Dat laatste vereist onder meer dat de – lokale – overheden ruimte voor vernieuwing bieden en hun vergunningenbeleid harmoniseren.

Thema 3 – **Weerbare vitale infrastructuur**

Weerbare vitale infrastructuur

We spreken van vitale infrastructuur, opgedeeld in vitale sectoren, als het gaat om producten, diensten en onderliggende processen die, als zij uitvallen, maatschappelijke ontwrichting kunnen veroorzaken. Dat kan zijn omdat er sprake is van veel slachtoffers en grote economische schade, of als het herstel heel lang duurt en er geen reële alternatieven zijn, terwijl we deze producten en diensten niet kunnen missen.[24] De vitale infrastructuur is dus cruciaal voor het goed functioneren van de Nederlandse maatschappij.

Een aantal vitale sectoren is in de handen van de overheid, zoals keren en beheren oppervlaktewater; met onder andere de dijken; en openbare orde en veiligheid; brandweer, politie en geneeskundige hulpverlening bij rampen en crisis. Ongeveer tachtig procent van de vitale infrastructuur is in handen van bedrijven waarbij de overheid in veel gevallen met wet- en regelgeving en toezicht een stevige invloed heeft. Enkele recente gevallen van buitenlandse investeringen in Nederland – bijvoorbeeld de mogelijke overname van KPN en het voornemen om internationale aandelenruil voor Gasunie en Tennet mogelijk te maken – hebben de vraag actueel gemaakt in hoeverre dergelijke investeringen gevolgen kunnen hebben voor de nationale veiligheid. Het gaat tot nu toe om een beperkt aantal gevallen, maar potentieel om grote belangen, zowel in economische als veiligheidszin.[25]
Dit roept vragen op over de afbakening van de vitale infrastructuur, ook in wettelijke zin, over de rolverdeling tussen de overheid en de betrokken bedrijven zelf en over het instrumentarium dat civiele en private partijen ter beschikking staat om de vitale infrastructuur te beschermen tegen operationele en strategische dreigingen.

Een belangrijke ontwikkeling is dat alle sectoren, vitaal en niet-vitaal, aan elkaar gekoppeld worden zonder precies te weten welke kwetsbaarheden dat met zich mee brengt. Als alles met alles verweven en verbonden raakt, is de vraag gerechtvaardigd of het huidige onderscheid tussen vitale en niet-vitale sectoren op termijn wel houdbaar is. Een veilig gedachte sector kan opeens massaal getroffen worden, ook omdat het cyberdomein veel kopieergedrag kent en kennis eenvoudig te distribueren is.

Hoewel in algemene zin het bewustzijn van de gevaren de laatste jaren is toegenomen, zijn er grote verschillen in de mate waarin verschillende sectoren ook echt actie ondernemen. Dat heeft onder meer te maken met de ‘businesscase’ van hackers en met feitelijke incidenten, de omvang en beschikbare budgetten van bedrijven in de sector en de organisatiegraad van de sector. Zo zijn banken al jaren doelwit, werken ook daarom nauw samen en organiseren collectief de inlichtingen; zij hebben bijvoorbeeld afgesproken om niet te concurreren op veiligheid. In de sectoren energie en water is wel veel aandacht voor fysieke veiligheid, maar nog relatief weinig voor cyberveiligheid.

Innovatiespeerpunten:

7 Kenmerken en afbakening vitaal
Onze vitale infrastructuur is cruciaal voor onze maatschappij en economie. De definitie en afbakening van *vitaal* zijn voortdurend onderwerp van aandacht. Belangrijke vraagstukken daarbinnen zijn hoe de verbinding tussen beleidsmakers en uitvoerders vorm te geven? Welke nu nog niet geïdentificeerde of nieuwe processen zouden tot de vitale infrastructuur gerekend moeten worden?
Hoe kunnen we handhaven dat vitale processen ongestoord verlopen, gegeven de toenemende onderlinge afhankelijkheid van processen? Kunnen we op basis van gemeenschappelijke kenmerken het instrumentarium en de effectiviteit van generieke en specifieke beschermings- en responsmaatregelen verbeteren? Hoe kan slimme modularisering (bijvoorbeeld in *smart grids*) en decentralisatie van vitale functies (keten)kwetsbaarheden verminderen?

8 Cyber security ‘Internet of Things’
Het gaat in dit speerpunt om de *cyber resilience* te verbeteren van allerlei besturings-, controle- en informatiesystemen en apparaten die in een *internet of things*-omgeving gegevens verzamelen – thuis, op straat, in publieke ruimtes, in bedrijven, inclusief ICS/SCADA-systemen enzovoort – en onderling communiceren zonder menselijke tussenkomst. Niet in de laatste plaats gaat het om de systemen die veiligheidsorganisaties zelf gebruiken.

9 Ketenbenadering cyber security
Enerzijds is de uitdaging om informatiebeveiliging te integreren in alles wat we doen; *security by design* en *cyber resilience* niet alleen in technische zin, maar verweven in alle processen en structuren. Anderzijds gaat het om het op orde brengen en houden van de samenhangende stappen: intentie, inlichtingen, detectie en respons. Onderzoek naar en vergelijking van *best practices* is nodig, op bedrijfs, sector en generiek niveau.

Thema 4 – **Handelingsgerichte informatievoorziening**

Handelingsgerichte informatievoorziening

De snelheid en het gemak waarmee we communiceren en informatie delen, noodzaakt tot nieuwe manieren van organiseren en samenwerken. In de militaire wereld wordt al decennia geëxperimenteerd met informatiegestuurd genetwerkt optreden. Gestart vanuit een sterke technische focus is in toenemende mate ook de menselijke component, de wijze van gebruik en de feitelijke waarde van genetwerkt optreden betrokken in de afwegingen. Ook andere veiligheidspartijen, onder meer de politie, hebben de afgelopen jaren ervaren hoe zij hun informatiepositie kunnen verbeteren en beter benutten door genetwerkt op te treden. Een recente ontwikkeling is om met grote hoeveelheden data een omgevingsbeeld op te bouwen en daarop handelingen te baseren. We genereren met internet, sociale media, databases en allerlei sensoren, inclusief smartphones, exponentieel meer data dan enige jaren terug. Dit is de Web 2.0-ontwikkeling.
Om die data nuttig te kunnen toepassen zijn geautomatiseerde processen nodig die deze data structureren, controleren, schiften, combineren en van betekenis voorzien. Dit is de stap naar het semantische Web 3.0 dat op kennis is gericht – met onderliggend het grote belang van open linked data als basis. Algoritmen voor patroonherkenning moeten verder ontwikkeld worden. Technologie stelt ons hiertoe in staat en is ook een belangrijke drijfveer, maar dient zorgvuldig toegepast te worden, met interoperabiliteit als belangrijke voorwaarde.

In de – als we niet uitkijken onontwarbare en niet gevalideerde – brij van gegevens wordt het steeds belangrijker om de identiteit en authenticiteit van personen, instanties, dingen en informatie vast te stellen. Zijn mensen wie ze zeggen te zijn, bijvoorbeeld bij grenspassage of op sociale media? Het achterhalen van identiteiten van individuen, soms gekoppeld aan zicht op hun intenties, is van groot belang voor openbare orde en veiligheid, opsporing, handhaving, toezicht, contraterrorisme en forensisch onderzoek. In september 2011 wees DigiNotar ons op de gevaren van een gecompromitteerde identiteit van instanties en/of hun producten en diensten.
De pendant in het *internet of things* is of systemen of digitale agents betrouwbaar genoeg zijn om informatie aan te verstrekken of om gevraagde acties voor uit te voeren. Het meest ingewikkeld lijkt de situatie waarbij digitale informatie wordt gelezen, verrijkt, veranderd, gedupliceerd en mogelijk weer teruggeplaatst zonder een spoor van deze stappen achter te laten. In alle gevallen gaat het om toegangscontrole, fysiek en virtueel; en dan niet alleen om de toegang zelf, maar ook om registratie van pogingen tot toegang en van de genomen acties na toegang. Punt van aandacht is ook de vraag naar het eigenaarschap en gebruiksrecht van informatie. In een beheerste informatiewereld worden gegevens gevalideerd, ordentelijk opgeslagen en vernietigd wanneer dat wettelijk verplicht is. In de gedistribueerde informatiewereld met zijn ongebreidelde duplicatie van gegevens is de vraag naar het eigenaarschap en vernietiging van informatie een goeddeels onbeantwoorde kwestie.

Innovatiespeerpunten:

10 Genetwerkte informatie op knooppunten

Hier zien we twee typen knooppunten. Ten eerste meld- en regiekamers en commandoposten van leger, politie en in steden; fysieke locaties dus, mogelijk mobiel. Ten tweede digitaal ondersteunde eerstelijns veiligheidsprofessionals die, situationeel gedreven en taak- of missiespecifiek, als knooppunt kunnen fungeren. Kritische factoren zijn onder meer informatie-uitwisseling tussen publieke en private veiligheidspartijen,[26] de betrouwbaarheid en actualiteit van de informatiestroom, het organiseren van de toegang tot informatie – zie ook speerpunt 12 – maar vooral de wijze waarop informatiestromen worden gebruikt om de informatiepositie te verbeteren en een hoogwaardig omgevingsbeeld op te bouwen. De basis voor de informatiehuishouding op elk domein is begrippen eenduidig definiëren. Zeker in de ontwikkeling richting Web 3.0-toepassingen op de langere termijn, is het werken aan realtime, interoperabele en gestructureerde data een essentieel onderdeel van de speerpunten 10, 11 en 12.

11 Herkennen en voorspellen van afwijkend gedrag

We willen beter in staat zijn gedrag van individuen en groepen of ontwikkelingen te herkennen en te voorspellen. Dit speerpunt is gericht op het gebruik van big data- en datamining-technieken om afwijkend, ongewenst en/of ongeoorloofd gedrag te herkennen en het op basis hiervan voorspellen van toekomstig crimineel of vijandig gedrag. Deze kennis vormt zo weer een grondslag om ongewenst en ongeoorloofd gedrag te voorkomen, dan wel om vroegtijdig te kunnen ingrijpen om escalatie te voorkomen.
Deze specifieke vorm van patroonherkenning in menselijk gedrag gebeurt steeds meer op grond van realtime multisensorinformatie, in combinatie met informatie uit open, eigen en andermans informatiesystemen en databases.
Er lopen al diverse proeftrajecten in lokale field labs.
In winkel- en uitgaanscentra en bij evenementen detecteren en signaleren toezichthouders afwijkende bewegingen van de publiekstromen, waarna zij daar hun acties gericht op kunnen afstemmen.

12 Vaststellen en garanderen van – digitale – identiteit

Van personen: koppeling van digitale en fysieke identiteitsherkenning, tegengaan van fraude en diefstal van identiteit – inclusief digitale en financiële data – op internet.
Van instanties en hun producten en diensten: toezicht, transparantie, toetsing, wet- en regelgeving. Van ‘dingen’: authenticatie van afzender en ontvanger in automatische processen. Van belangrijke informatie: hiervoor is een model nodig om de wijze waarop een oorspronkelijk stukje informatie successievelijk wordt verrijkt, veranderd, gebruikt enzovoort – kortom: de levenscyclus van de betreffende informatie – te kunnen vastleggen of achterhalen.

Thema 5 – **Waarneming met onbemande systemen**

Waarneming met onbemande systemen

Verdergaande automatisering en robotisering helpt de effectiviteit te verhogen en de kosten te beheersen van langdurige of permanente routinetaken. Dit thema richt zich op een breed assortiment aan monitoring, surveillance en detectietaken met onbemande systemen, van langdurig, over grote afstanden en eventueel *stand-off*; tot realtime, dichtbij en kortdurend. Civiel-militaire samenwerking is hier geboden.

Militaire *unmanned arial vehicles* (UAV's) worden al ingezet voor civiele taken, zoals zorgen voor luchtzicht in gevaarlijke situaties, zoals rampen en grote branden, bij het in kaart brengen van grote plaatsen delict of in specifieke observatie-situaties. Zoals voor veel van de samenwerkingsmogelijkheden geldt als belangrijke drijfveer dat door bundeling van inspanningen schaalvoordeel kan worden behaald; zowel efficiëntie- als kwaliteitswinst. Dit voordeel is denkbaar in de hele keten: visievorming, regelgeving, behoeftestelling, ontwikkeling en testen, verwerving, infrastructuur, instandhouding en feitelijke inzet van onbemande vliegende systemen. Bestaande samenwerking is recent verder verdiept in het kader van de voorbereiding van de NSS2014, waarbij de detectie en interventiemogelijkheden zijn onderzocht. Een pragmatische reden voor de aansluiting van de politie bij defensie is dat er wel militaire, maar nog geen civiele regelgeving is die de inzet van UAV's afdoende regelt.

Veiligheidsorganisaties zullen maximaal willen en moeten meeliften met commerciële ontwikkelingen op het gebied van onbemande vliegende platformen en systemen. Onder druk van wet- en regelgeving zal de betrouwbaarheid en veiligheid van op de markt verkrijgbare UAV's zich snel ontwikkelen.[27] Defensie zal hier op bepaalde aspecten als 'slimme specificeerder', en eventueel 'slimme ontwikkelaar' willen vooruitlopen. Het gaat dan bijvoorbeeld om beveiliging van de communicatie met de platformen en om de integratie van hoogwaardige *sensor payloads* en verwerking en interpretatie van de multisensorinformatie in de gerichte opbouw van een omgevingsbeeld. De politie zal ontwikkelingen op dit gebied kunnen stimuleren door in haar verwervingsprojecten innovatieve componenten op te nemen. In beide gevallen is kennis van de snel ontwikkelende markt in relatie tot de eigen behoefte noodzakelijk: 'slimme koper'. Beide partijen hebben verder interesse in UAV's als dreiging. Het gaat dan om zowel crimineel en vijandig gebruik als de veiligheidsaspecten van hobbyisme.

Innovatiespeerpunten:

13 Visie- en conceptontwikkeling voor operaties met onbemande sensorplatformen
Dit betreft de ontwikkeling van al dan niet gezamenlijke inzetscenario's, doctrinevorming enzovoort. Hieruit volgen eisen voor innovatie, niet alleen gericht op platformen en systemen, maar ook op de feitelijke toepassing van de sensorinformatie. Met dit laatste raakt dit onderwerp aan Thema 4: Handelingsgerichte informatievoorziening.
Een belangrijk punt van aandacht is de relatie dan wel integratie van bemande en onbemande luchtvaart.

14 Operationele autonomie UAV's
Zeker voor langdurige observatie geldt het streven naar maximale autonomie van vliegende onbemande platformen. Niet alleen van enkelvoudige platformen, maar ook in het overdragen, in tijd en/of ruimte, van platformen en systemen.

Thema 6 – **Procesinnovatie in en tussen professionele organisaties**

Procesinnovatie in en tussen professionele organisaties

De veiligheidsprofessional wordt op verschillende manieren geconfronteerd met een wereld in verandering en een dynamische, complexe omgeving waarin hij moet optreden. Zijn taakuitvoering kent enerzijds steeds meer randvoorwaarden en anderzijds steeds meer mogelijkheden door het gebruik van technische hulpmiddelen. Ten slotte zijn in zijn werkwijze steeds meer netwerkafhankelijkheden ingebouwd.

Dit heeft consequenties voor alle humanresourcesaspecten: voor competentieprofielen, werving en selectie, opleiding, training en oefening, fysieke en mentale inzetbaarheid, opwerkingsprocessen naar een taak of missie, teamsamenstellingen enzovoort. Deze dynamiek vraagt bovenal een operationele mindset van organisaties en professionals: het optimaal presteren in feitelijke operaties moet de primaire leidraad voor de inrichting van processen en structuren zijn.

'De gebeurtenissen van elke dag, nationaal en internationaal, bewijzen dat een blijvende ontwikkeling en innovatie op het gebied van veiligheid noodzakelijk is.'[28] Laetitia Griffith

Een belangrijk subthema is het efficiënter en effectiever trainen en oefenen van samenwerkende veiligheidsprofessionals uit de blauwe, rode, witte, oranje en groene zuilen, zo nodig samen met private beveiligingsbedrijven. Het gaat daarbij om complexe situaties die noodzaken tot multidisciplinair en *multilevel* samenwerken. Complicerende factoren kunnen aspecten zijn als geweld en geweldsescalatie, toepassing van nieuwe technieken, procedures en doctrines of dilemma's tussen ethiek en effect. Veel relevante scenario's kunnen slecht in de praktijk worden getest en moeten in een of andere vorm gesimuleerd worden. *Serious/applied gaming*-technieken en middelen kunnen uitkomst bieden – mits voldoende gevalideerd. Het kan gaan om organieke training en oefening in min of meer standaardsituaties, maar ook om specifieke missievoorbereiding. Buiten de opleidingscontext kan ook worden gedacht aan het gebruik van *gaming*-technieken om inzichten te krijgen in de verantwoordelijkheidsverdeling bij incidenten. Het is bijvoorbeeld goed denkbaar om de thema's of scenario's uit de jaarlijkse Nationale Risicobeoordeling juist op dit aspect te '*gamen*'.

Innovatiespeerpunten:

15 Geïntegreerd optreden met heterogene teams
Hier komen menselijke competenties en technologische ondersteuning samen. Het gaat om structurele organieke samenwerking en om incidentele intermenselijke verbanden tussen professionals onderling en tussen professionals en burgers. Dat alles speelt zich af in acute operationele situaties of in langdurige zaken, en veelal met hoogtechnologische hulpmiddelen, soms onder primitieve omstandigheden. Vaak zit er druk op en stress in. Diezelfde professional maakt het allemaal mee in de loop van zijn carrière, in een specifieke functie en soms zelfs in een tijdsbestek van enkele weken. Welke innovaties kunnen op het niveau van het individu, van het team en van de ondersteunende omgeving bijdragen aan een beter teamresultaat? Het '*teamen*' van mens en (intelligente) machine wordt belangrijk, met wederzijds vertrouwen als basis. Hoe krijgt dit gestalte?

16 Koppeling actuele werkelijkheid-virtuele omgeving
Zeker in het geval van een missievoorbereiding is het van belang de deelnemers in een *serious game* een virtuele omgeving voor te schotelen die recht doet aan de werkelijkheid. Natuurlijk moet de techniek de didactische doelstellingen volgen, maar in veel gevallen is een hoog realisme gewenst. Afhankelijk van het niveau van de game kan dit bijvoorbeeld betekenen dat een fysieke situatie – bijvoorbeeld de indeling van een gebouw – snel in 3D gevisualiseerd moet kunnen worden, dat de feitelijke profielen van de bij een zaak betrokken personen direct beschikbaar zijn enzovoort. Hier ligt een relatie naar speerpunt 2. Validatie is belangrijk.

‘Het ministerie van Veiligheid en Justitie vindt innovatie heel belangrijk. Op het terrein van veiligheid zien we steeds meer voorbeelden van nieuwe producten die voortkomen uit de samenwerking tussen bedrijven, overheden en universiteiten.’[29] Ivo Opstelten

3 – Investeringen en opbrengsten van innovatie

De Nationale Innovatieagenda Veiligheid (NIAV) komt tot stand in een proces van interactie met de belangrijkste belanghebbenden in het veiligheidsdomein. Als logisch uitvloeisel van deze interactie en het commitment dat hiermee verbonden is, koppelen de betreffende partijen de eigen innovatieagenda's aan de nationale agenda. Dit is de crux van de NIAV: er moeten zich consortia van triple-helixpartijen in het nationale veiligheidscluster vormen om gezamenlijk de in de agenda opgenomen innovaties te realiseren met een hefboomeffect op de afzonderlijke bijdragen. De tabel in paragraaf 3.1 geeft een aanzet tot deze coalitievorming.

Investeringen in innovatie worden gedaan met het oog op toekomstige baten. Daar zit altijd een risico in: niet alle investeringen brengen hun geld op. Partijen zijn eerder bereid dit risico te dragen als er ook echt een markt is voor de producten en diensten die het resultaat zijn van de innovatie. Dit is de reden waarom de NIAV nadruk legt op het articuleren, bundelen en onderschrijven van de vraag van de behoefte-stellers. Een belangrijke stap hierbij is het leggen van de verbinding tussen de NIAV en de verwervingsagenda's van de belangrijkste vragende partijen in het veiligheidsdomein.

Paragraaf 3.2 geeft daartoe een eerste aanzet. The Hague Security Delta ondersteunt de ontwikkeling van een nationale verwervingsagenda die in 2016 naast de NIAV sturing aan het proces van innovatie en economische ontwikkeling gaat geven.

3.1 Innovatie-investeringen in coalitieverband

De tabel op pagina 28 is een cruciaal element in de overgang van een papieren innovatieagenda naar een agenda die leeft, werkt en ertoe doet. De tabel verbindt innovatiespeerpunten met partijen die samen willen investeren om die speerpunten te verwezenlijken. In de meeste gevallen gaat het om een combinatie van vragers en aanbieders. De partijen die in de tabel staan voelen zich verantwoordelijk om het betreffende innovatiespeerpunt te realiseren. Daarbij brengen ze ook eigen middelen in, zoals budget, capaciteit, kennis, toegangen, netwerken en testfunctionaliteiten. In afzonderlijke plannen van aanpak, die per innovatiespeerpunt verschillen, werken partijen uit hoe dat gebeurt. Het is zaak om bij de start van een innovatietraject vast te stellen welke partij wat, wanneer, waarom en hoe bijdraagt, hoe regie op ontwikkeling en resultaat wordt vormgegeven en welke clausules daarbij gelden. Vragende partijen bijvoorbeeld, kunnen zich committeren door expliciet uit te spreken dat de geleerde lessen in het innovatieproces – bijvoorbeeld door toetsing in proeftuinen e.d. – meewegen in het opstellen van specificaties in relevante verwervingstrajecten. Er is dan geen sprake van gedwongen winkelnering, maar wel van het door alle betrokken partijen nuttig gebruikmaken van inzichten die zijn opgedaan in het innovatietraject. Aanbiedende partijen committeren zich aan risicodragende investeringen, maar bijvoorbeeld ook aan een vorm van technologie- en kennisdeling met de andere partijen in de coalitie, met aandacht voor afspraken over bijvoorbeeld intellectueel eigendom.

'Hoewel innovatie de corebusiness is van bedrijven en onderwijsinstellingen, is een aanjagende rol van de overheid cruciaal.'[30] Kees Verhoeven

De ervaring leert dat het vormen van een effectieve coalitie die is gericht op het ontwikkelen, toepassen en op de markt brengen van innovaties sterk afhangt van een leidende partij. In de tabel heeft bijna ieder innovatiespeerpunt ten minste één trekker die het voortouw neemt voor het op gang brengen van de coalitievormingen en de ontwikkeling van een plan van aanpak, en die de regie voert over de samenwerking. Idealiter wordt per speerpunt een triple-helixstructuur gevormd met ten minste één sponsor of opdrachtgever uit de publieke sector en een triple helix begeleidingsgroep (*community of practice*).

In het proces van coalitievorming en uitwerking van een plan van aanpak zal het innovatiespeerpunt een kleuring en nadruk krijgen die de specifieke interesses, belangen en sterktes van de coalitiepartners weerspiegelt. Bovendien is het goed mogelijk dat een speerpunt meer opvolgingstrajecten krijgt. Dit is onvermijdelijk en goed te billijken. De NIAV is eerder een katalysator dan een voorschrift, en in die zin net zo goed volgend op initiatieven als richtinggevend. Het doel: maat-schappelijke en economische waardecreatie staat voorop.

Innovatiespeerpunten

	Innovatiespeerpunt	Trekkers[31]	(Mogelijke) partners	Lopende initiatieven en overige overwegingen
1	**Regievoering vraagarticulatie 'één overheid'**	NCTV (programma Veilig [door] innovatie)	*Reguliere partners voor de NCTV op dit speerpunt:* Algemene Inlichtingen- en Veiligheidsdienst Ministerie van Defensie (MIVD en Koninklijke Marechaussee) Nationale Politie Politieacademie Instituut Fysieke Veiligheid Veiligheidsregio's Nederlands Forensisch Instituut Rijks Instituut voor Volksgezondheid en Milieu (RIVM) Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR) Openbaar Ministerie Ministerie van Financiën (Belastingdienst, FIOD, Douane, Algemene Inspectiedienst) Ministerie van Sociale Zaken (SIOD) Ministerie van Infrastructuur en Milieu (ILT) *Andere partners:* Gemeenten (G4/ G32) DITSS TS&S	• De ontwikkeling van het nationale veiligheidscluster HSD fungeert hierin als belangrijke pijler en basis • Lopende NCTV-initiatieven: Het financieren van 10-15 projecten bij en door de veiligheidspartners, bij voorkeur in samenwerking met bedrijven en kennisinstituten. Het gecoördineerd aanleveren van input voor het Werkprogramma Horizon 2020 Secure Societies voor 2016, en het faciliteren van consortiavorming voor indieners op het werkprogramma 2015. Het uitvoeren en financieren van het *Small Business Innovation Research*-programma 'bescherming tegen onbemande systemen, detectie en interceptie van drones. Het organiseren en financieren van de Veiligheid Innovatie Competitie 2015. Het inventariseren van nieuwe vraagstukken onder de veiligheidspartners en deze informatie inbrengen in NIAV 2015. • Articulatie van veiligheidsvragen van in dit overzicht niet genoemde organisaties en de vitale infrastructuur (zoals de transportsector met secure lane), veiligheidsexpertise centra (zoals CCV/EVPT) moeten aandacht krijgen in dit speerpunt. De ontwikkeling van kennis op dit terrein is nodig, Safety Valley i.s.m. Nyenrode is ook bereid mee te werken. De methode veiligheidsatelier zoals toegepast bij DITSS is binnen dit thema goed toepasbaar.
2	**Leren van incidenten en oefeningen**	Veiligheidsregio Haaglanden	Politieacademie Ministerie van Defensie Veiligheidsregio Haaglanden Haagse Hogeschool RIVM TNO Twijnstra en Gudde DITSS TS&S	• Het Instituut Fysieke Veiligheid (IFV) werkt vanuit zijn wettelijke taak, in het kader van de Strategische Agenda van het Veiligheidsberaad, samen met de Nationale Academie Crisisbeheersing aan de ontwikkeling van opleidingen voor medewerkers in de veiligheidsregio's op terreinen van crisisbeheersing. • 7e Kaderprogramma, demonstratieproject crisismanagement DRIVER (Driving Innovation in Crisismanagement for European Resilience, een samenwerking tussen Veiligheidsregio Haaglanden, TNO en E-Semble in een breed Europees consortium. • RIVM wil graag vanuit zijn kennispositie (gezondheid) en rol een (co)trekkende en ondersteunende rol vervullen. • RIVM ontwikkelt een beoordelingskader meetstrategie chemische incidenten in de vorm van een app. voor adviseurs gevaarlijke stoffen. RIVM start in 2015, met betrokkenheid van IFV, Veiligheidsregio's en GHOR, een Root Cause Analysis om beter en dieper inzicht te verkrijgen in "wat niet goed gaat bij incidenten, en hoe daarvan te leren". • Project realtime information voor Veiligheidsregio Midden-West-Brabant. • Roadmap Smart Cities.

	Innovatiespeerpunt	Trekkers[31]	(Mogelijke) partners	Lopende initiatieven en overige overwegingen
3	**Waardecreatie in triple-helixinnovatie**	Nationaal veiligheidscluster HSD Gemeente Den Haag	Alle betrokken partners RIVM Haagse Hogeschool TNO	Alle betrokken HSD-partners hechten grote waarde aan dit thema, voorbeelden van initiatieven: • *Living labs* in Haagse regio, bijvoorbeeld Internationale zone, CSI The Hague, testbeds ENCS en de HSD-innovatiehuizen. • Initiatieven en projecten bij TS&S (bijvoorbeeld Safety Field lab) en bij DITSS (bijvoorbeeld Stratumseind Eindhoven). • RIVM wil graag supporter zijn, maar kan niet financieel bijdragen. • De ontwikkeling van de internationale dimensie van HSD wordt als zeer belangrijk ervaren, TNO wil daar expliciet aan bijdragen ook in de EU-netwerken waar TNO in acteert.
4	**Sociale innovatie en zelforganiserend vermogen**	TS&S DITSS Gemeente Den Haag	Nationale Politie Veiligheidsregio Rotterdam-Rijnmond en Zeeland Haagse Hogeschool RIVM TNO TU Eindhoven Tilburg University	• Een niet limitatieve opsomming van initiatieven en ontwikkelingen: Burgernet Amber Alert en SOS Alarm (burgers) en Live View (bedrijven, private beveiligers), samenwerking in de buurt 'ken uw buren', projectidee BART (Burger Alert Real Time) in het kader van de Road Map Smart City Den Haag. project Cyber Community Protection Network – CyCopNet (in conceptfase), Resilient Delta's in Zeeland, coöperatie Safety Valley. Bij DITSS: Openbaar Meld Systeem Challenge 'terugdringen onnodige brandmeldingen'. Social design; gaming voor veilig internetgebruik, licht voor gedragsbeïnvloeding, veiligheidsbeleving in tunnels. Risk Factory bij TS&S. • RIVM is geïnteresseerd in het vraagstuk van burgers die bij rampen en incidenten zelf met eigen apparatuur, zoals smartphones, metingen verrichten en de betekenis van die data voor first responders; snelle detectie van agentia, interpretatie en validatie van die data en communicatie. De ontwikkeling van data en nepdata kan behulpzaam zijn bij oefeningen.
5	**Bewustwording: perceptie versus realiteit**	TS&S	Nationale Politie Haagse Hogeschool Universiteit Twente TNO	• Den Haag Showcase Veilig Nederland (een consortium van HCSS, T-Xchange, TNO, Capgemini). • Siemens heeft in coproductie met de Haagse Hogeschool een 3D geprinte brug ontwikkeld waarmee de gevolgen van een hack in de besturing van een brug of de beveiliging daarvan kunnen worden getoond. Deze brug zal op de HSD-Campus een plek krijgen.
6	***Security by design* in stedelijke voorzieningen en bij evenementen**	DITSS Gemeente Den Haag	Technische Universiteit Eindhoven Trigion TNO Tilburg University InnovationQuarter Gemeenten (G4/G32)	• Een niet-limitatieve opsomming van ontwikkelingen: Integrale gebiedsbeveiliging Internationale Zone, fase 1 (TNO, Thales). Designing out crime (Stratumseind Eindhoven), Fastlane, anomalie detectie, Businespark Loven Tilburg, safety and community (IC3Media, VCS) Civil sensed city, burger betrokkenheid (DITSS). Philips is actief op dit gebied als het gaat om de invloed van licht, geluid en geur op (de perceptie van) veiligheid (betrekken via DITSS). • Nodig in dit speerpunt is de betrokkenheid van een system integrator, bijvoorbeeld diensten evenementenveiligheid van gemeenten. Future Events wil hier als landelijk publiek-privaat evenementenplatform een rol in vervullen.

	Innovatiespeerpunt	Trekkers[31]	(Mogelijke) partners	Lopende initiatieven en overige overwegingen
7	**Kenmerken en afbakening vitaal**	KPN	TNO Siemens Universiteit Twente	• KPN ervaart hier een belangrijk vraagstuk voor de verbinding tussen beleidsmaker en uitvoerders in de vitale infrastructuur en de ontwikkeling van een gemeenschappelijk perspectief op het cybervraagstuk binnen de vitale infrastructuur.
8	**Cybersecurity *'Internet of Things'***	Siemens KPN	NCTV Cyber Security Raad (NCSC) Capgemini TNO ENCS[32] Universiteit Twente DITSS FOX-IT	• Een niet limitatieve opsomming van ontwikkelingen: Testbed energie infrastructuur en smart grids. Testbed watersector en andere sectoren, planvormingsfase (ENCS). Trainingen voor Industrial Control Systems Security, Project Cyber Attack Detector (TNO, Fox-IT). Vraaggestuurd programma Cyber Security Topsectoren HTSM kijkt naar security by design voor ICT-gebaseerde vitale infrastructuur. Het project Peseta betreft de digitale uitwisseling van bankafschriftgegevens, betrokken actoren zijn Inspectie SZW, FIOD, Inspectie Leefomgeving en Transport, NVWA, Koninklijke Marechaussee en Rijksrecherche. • Een belangrijk kwestie voor KPN is hier de ontwikkeling van secure networks en monitoring (sensing/scada). • De NCTV (Cyber Security Raad en het Nationaal Cyber Security Center) dragen aan dit thema bij met kennis en advies, als dit thema geconcretiseerd wordt in zijn uitwerking. Te denken valt daarbij aan een innovatiecase waarin technologische detectiemogelijkheden om falen en sabotage van, zonder menselijke tussenkomst, communicerende systemen te verminderen, ook wel kill-switches genoemd.
9	**Ketenbenadering cyber security**	Fox-IT Thales Capgemini KPN Haagse Hogeschool	NCTV/NCSC Cyber Security Academy Haagse Hogeschool TNO DITSS Siemens InnovationQuarter	• Een niet limitatieve opsomming van voorzieningen en ontwikkelingen: Cyber Security Lab TNO, Nationaal Cyber Security Centrum (NCSC). Vraaggestuurd programma Veilige Maatschappij – topic cyber security (TNO) en Vraaggestuurd programma Cyber Security (TNO). Hulp voor veilig online thuis en mobiel, waaronder internetbankieren, weerbaarheid pesten – ook door – gaming. bijvoorbeeld Sweety (Dutch design award 2014). Topsectoren HTSM beziet hoe de cybersecuritystatus van de Nederlandse vitale infrastructuur op uniforme wijze inzichtelijk gemaakt kan worden (DeMoS: Detectie, Monitoring en Situational Awareness). Er is een diversiteit aan SCADA- en ICS-vraagstukken op te lossen. • Op basis van een gemeenschappelijk te ontwikkelen plan van aanpak is de Haagse Hogeschool eventueel bereid vanuit een trekkende positie deel te nemen aan de realisatie van dit speerpunt. • NCTV heeft warme belangstelling voor dit thema en ziet hierin ook aanzienlijke mogelijkheden voor bedrijven (bijvoorbeeld. Shell en Tennet). NCTV moedigt op dit thema het particulier initiatief op veiligheidsinnovatie actief aan.

	Innovatiespeerpunt	Trekkers[31]	(Mogelijke) partners	Lopende initiatieven en overige overwegingen
10	**Genetwerkte informatie op knooppunten**	KPN iCOPP ENAI	Nationale Politie Thales Capgemini TS&S DITSS Siemens TNO Axis-communications Conseillers en Gestion et Informatique (CGI) Gemeente Den Haag	• Een niet limitatieve opsomming van ontwikkelingen en initiatieven: De Regionale Toezicht Ruimte Zuid-Oost-Brabant. samenwerking in TS&Sverband; Twente Experimental Command, Control and Communication Centre for Secure Environments (Tech4se), Universiteit Twente/Center for Telematics and Information, het concept van de meldkamer van de toekomst (CO24). Internationale Zone (Den Haag), common-operational picture (iCOPP, ENAI). • Belangrijke aspecten voor KPN binnen dit thema zijn: monitoring en secure networks. • Het opzetten van pre-competitieve experimenteeromgevingen, bijvoorbeeld op terreinen van realtime intelligence, cyber en meldkamers is aangewezen, TNO wil zich daar sterk voor maken. • TNO is actief op het thema realtime intelligence en werkt aan tools en concepten voor intelligencetaken.
11	**Herkennen en voorspellen van afwijkend gedrag**	Capgemini KPN DITSS	TNO NFI TS&S Universiteit Twente InnovationQuarter Nationale Politie	• Een kritieke factor als het gaat om herkennen van afwijkend gedrag is het zoveel mogelijk beperken van “valse negatieven’ en ‘valse positieven’. Privacy, ethische en juridische aspecten spelen in dit thema een belangrijke rol. • Een niet limitatieve opsomming van initiatieven: Automatische videoanalyse (TNO). Videocontentanalyse (DITSS). Digitaal sporenonderzoek in the cloud (nationale politie, NFI). Digitale forensische accountancy (ACM, AFM, DNB). Ontwikkelingen in Twente (TS&S, Tec4se en CO24). PiD project Beware (Trigion). Anomaliedetectie (DITSS). KPN is zeer geïnteresseerd in aspecten van situational awareness.
12	**Vaststellen en garanderen van – digitale – identiteit**	Authasas KPN	TNO Fox-IT TU Delft TU Eindhoven NFI TS&S DITSS Universiteit Twente InnovationQuarter	• Een belangrijk facet binnen dit speerpunt is het ontwerpen van vertrouwen, privacy en beveiliging in de meervoudig publiek-privaat gekoppelde informatiestromen van de internetwereld. • Een niet limitatieve opsomming van initiatieven en ontwikkelingen: Encryptietechnieken, Leiden-Delft-Erasmus Center for Safety and Security. Een variëteit aan initiatieven bij TS&S en DITSS (NXP, FIDO, Tec4se, CO24, BRP-project, VX company forensics recognition & individualisation. • NCTV ziet online-identiteitsmanagement als belangrijke uitdaging waarin veel economisch potentieel aanwezig is voor innovaties. In dit thema zou het consumen-tenperspectief nadrukkelijk kunnen worden betrokken; betrouwbare transacties op internet, veilige websites.

	Innovatiespeerpunt	Trekkers[31]	(Mogelijke) partners	Lopende initiatieven en overige overwegingen
13	**Visie- en concept-ontwikkeling voor operaties met onbemande sensorplatformen**	Ministerie van Defensie	TNO Nationale Politie Nationaal Lucht- en Ruimtevaartlaboratorium (NLR) Brandweer Nederland RIVM Universiteit Twente TS&S	• Een niet limitatieve opsomming van initiatieven en ontwikkelingen: PiD project RAEBELL (feasibility study of low-level airspace surveillance). Meten van stoffen in rookpluimen en radioactieve wolken met onbemande vliegtuigjes (RIVM samen met NCTV).Trainen, testen en experimenteren met onbemande vliegtuigen (TS&S).
14	**Operationele autonomie UAV's**	Aerialtronics	TU Delft Ministerie van Defensie Nationale Politie Thales Nederland Business Line Above Water Systems NLR TNO Universiteit Twente	• NCTV hecht belangstelling aan deze thematiek en zal, na concretisering van dit thema in aanpak, doelen en resultaten, zijn betrokkenheid op dit thema bepalen.
15	**Geïntegreerd optreden met heterogene teams**		Nationale Politie Twijnstra Gudde TNO TS&S	• Een niet limitatieve opsomming van initiatieven, ontwikkelingen en voorzieningen: Rollenspel Secure Haven (TNO, Universiteit van Leiden, Cap Gemini). TNO is actief op het terrein van grootschalig (civiel-militair) samenwerken bij rampen en crises. PiD project Stepping Stones for Safety and Security: doorlopende leerlijnen veiligheidsopleidingen (ROC Mondriaan, HHS, Trigion). TS&S heeft de ambitie om het European Safety & Security Center in te richten op het voormalige Vliegveld Twente. TS&S is actief op terrein van technology enhanced learning/virtual training. Troned[33] en de Riskfactory bieden een variëteit aan (fysieke en virtuele) infrastructuren voor OTOTEL (Onderwijs, training, oefening, testen, evalueren en leren). Het TS&S Safety Field lab biedt locatie en (praktijk)expertise voor ontwikkeling en testen van het functioneren van heterogene teams en virtuele/mixed reality training. Deze voorzieningen zijn ook inzetbaar bij speerpunt 16.
16	**Koppeling actuele werkelijkheid – virtuele omgeving**	Thales/T-Xchange TS&S KPN	Nationale Politie TNO Trigion E-Semble DITSS Gemeente Den Haag	• T-Xchange (Thales) is betrokken bij vier projectvoorstellen binnen Horizon 2020 en de Veiligheidsregio Twente bij twee calls (waaronder FCT-7-2014, law enforcement capabilities, pan European platform for serious gaming and training). • KPN is zeer geïnteresseerd in aspecten van situational awareness. • De gemeente Den Haag wil op dit speerpunt een faciliterende rol vervullen. • Een niet limitatieve opsomming van serious gaming initiatieven: Gebiedsontwikkeling Twente (Thales), Den Haag Showcase Veilig Nederland (HCSS, T-Xchange, TNO, Capgemini), PiD project Close Protection Serious Gaming (TU-Delft, E-semble), Burgemeestersgame IFV (T-Xchange), Veilig internetgebruik thuis en mobiel (DITSS), Cyber Incident Experience (TNO/Fox-IT).

3.2 Koppeling NIAV aan verwervingsagenda's

De verbinding tussen de NIAV en de verwervingsagenda's van de belangrijkste vragende partijen is essentieel voor de maatschappelijke en economische waardecreatie. In de horizontaal en verticaal gelaagde veiligheidsstructuren is dat vaak een complexe uitdaging. De publieke investeringen in veiligheid komen op alle overheidsniveaus tot stand, binnen departementen en tussen departementen, en soms in publiek-private samenwerkingen. Daarnaast staan de investeringen die, soms buiten het zicht van de overheid, plaatsvinden in private bedrijven, vooral in de vitale sectoren.

'Goed veiligheidsbeleid moet integraal, kostenbewust en modern zijn en gebaseerd op een korte-, middellange- en langetermijnvisie. In de huidige financiële situatie zijn we verplicht om met elkaar samen te werken, als departementen, maar ook binnen de 'gouden driehoek' van overheid, bedrijfsleven en kennisinstituten.'[34] Ivo Opstelten

De economische waarde van de investeringen die in het verlengde liggen van de NIAV, schatten we op drie tot vijf miljard euro voor de komende tien jaar, als we uitgaan van een materieelvernieuwingsquote van 3 tot 5 procent van de overheidsbestedingen. Deze investeringen moeten maatschappelijk renderen – Nederland veilig tegen aanvaardbare kosten – maar ook zorgen voor economisch opbrengsten door het exportpotentieel van de geïmplementeerde oplossingen te benutten. Dit kan vooral succesvol zijn als investeringen in innovatie en in producten en diensten op elkaar zijn afgestemd.

Zoals we in deze NIAV rekening houden met de toekomstige verwervingsagenda, zo moeten de verwervingstrajecten rekenschap geven en gebruikmaken van de praktijkervaring en het ontwikkelde inzicht in oplossingen die zijn opgedaan in een innovatiegericht voortraject, en die ook in de toekomst standhouden (zie ook paragraaf 4.2).

Verdichtingspunten[35] voor veiligheidsinvesteringen	Grote geplande en te verwachten investerings- en verwervings-programma's
Mobiele communicatie (C2000-opvolger)	Van secure speech en data naar breedband (streaming video, cloud-functies), benutten LTE , Informatiegestuurd Optreden 2.0. Benodigde investeringen > € 100 miljoen.
Voertuig C3I	Verbetering situational awareness OVD, programma Sight, Informatiegestuurd Optreden 2.0, 'digitaal motorkapoverleg'. Benodigde investeringen > € 100 miljoen.
Situational awareness 'officier van dienst'	Mobiel, gekoppeld, realtime. Benodigde investeringen € 25-100 miljoen.
Meldkamers	Van 25 naar 10 (11), meldkamer van de toekomst, LCMS 2.0, koppeling IBO-EBO, koppeling DCC'n, Shared Security Operations Centre Internationale Zone Den Haag. Benodigde investeringen € 25-100 miljoen.
Nood- en crisisnetwerken	Vernieuwing en capaciteitsuitbreiding Noodnet, NAFIN, LCMS 2.0. Benodigde investeringen € 25-100 miljoen.
Drones	Operationele inzet van robots, controle lage en microluchtruim. Benodigde investeringen € 5-25 miljoen. Follow-up PiDproject Raebell.
Cyber	Preventieve, actieve defensieve en offensieve capaciteiten. Testfaciliteit 2.0 (in oprichting). Benodigde investeringen € 25-100 miljoen.
Uitrusting first responders	Smart functional uniforms, non lethal weapons, Informatiegestuurd. Optreden 2.0, LCMS 2.0. Benodigde investeringen > € 100 miljoen.
Stedelijke voorzieningen	Smart City-programma's. Benodigde investeringen > € 100 miljoen.
HSD als landelijke innovatiefaciliteit	Incubator faciliteren voor landelijk innovatiecluster veiligheid – op basis van speerpunten in de agenda – in de geografische kernen Den Haag, Twente en Brabant.

‘Veiligheid kent veel aspecten die in samenhang beschouwd moeten worden. De Nederlandse veiligheidssector kan hier nog veel meer op inzetten dan nu wordt gedaan. Daar valt nog veel winst te boeken in geld en resultaat.’[17] Henk Geveke

4 – De NIAV in breder perspectief

We plaatsen de NIAV uitdrukkelijk in het perspectief van maatschappelijke en economische uitdagingen, met innovatie als belangrijkste middel om deze uitdagingen aan te gaan. De aspecten en ontwikkelingen die we in dit hoofdstuk beschrijven, geven nadere invulling aan dit gecombineerde perspectief. Dat kan helpen om de feitelijke agenda in hoofdstuk 2 en de koppeling daarvan aan investeringen in hoofdstuk 3 beter in de context te plaatsen.

4.1 Werkwijze Nationale Veiligheid

De NIAV past goed in de werkwijze Nationale Veiligheid zoals die interdepartementaal is ontwikkeld onder regie van het ministerie van Veiligheid en Justitie, voorheen berustte deze verantwoordelijkheid bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, zie Figuur 1. De NIAV is een instrument om invulling te geven aan het derde procesblok: Opvolging, door innovatieve oplossingen te ontwikkelen voor de Capaciteitenbehoefte.

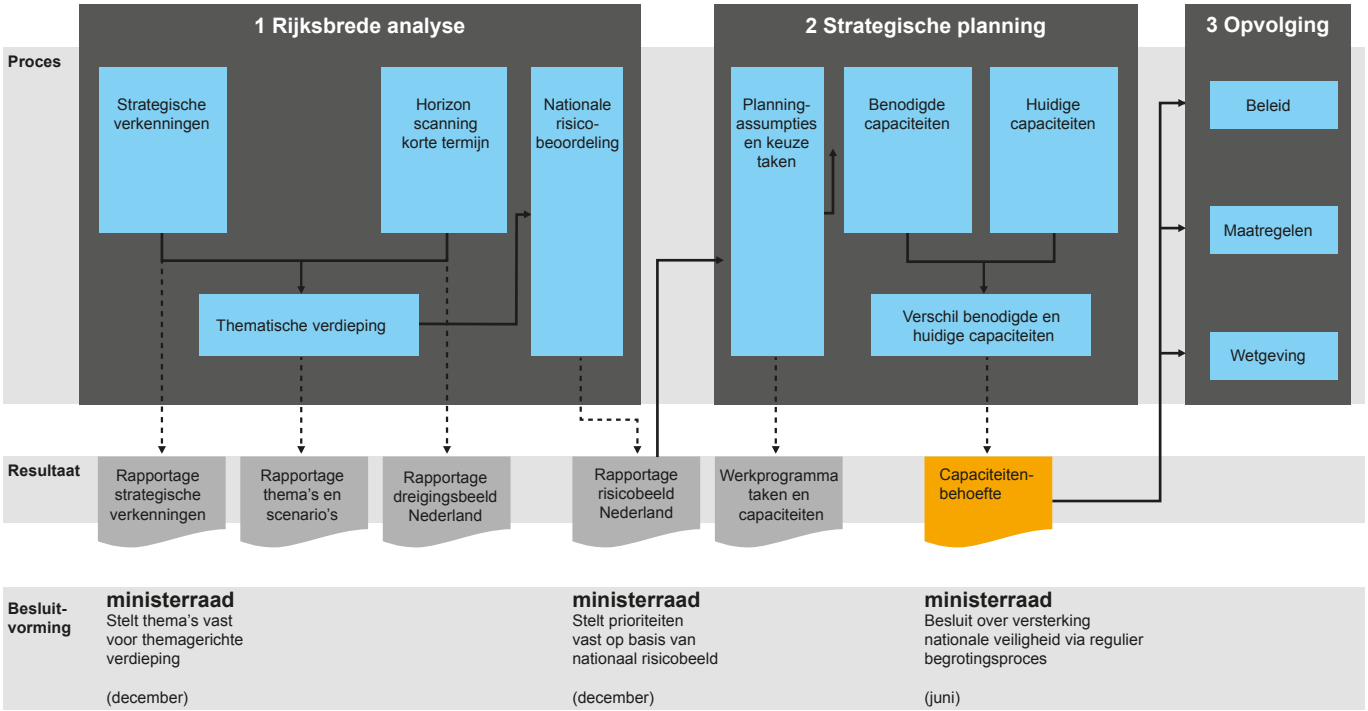
Een belangrijk onderdeel van de werkwijze Nationale Veiligheid is de jaarlijkse Nationale Risicobeoordeling (NRB). De NRB geeft een actueel overzicht van risico's en dreigingen voor de nationale veiligheid en van hun eventuele gevolgen. De NRB is de meest omvattende analyse in zijn soort en heeft de meeste steun, vanwege de rijksbrede betrokkenheid en toenemende inbreng vanuit de vitale sectoren. Opkomende nieuwe dreigingen of verschuivingen in het risicobeeld kunnen leiden tot de behoefte aan nieuwe of andere capaciteiten, en dat weer tot mogelijke innovatievragen. Daarmee kan de NRB waardevolle input leveren voor de NIAV. Omgekeerd kan de NIAV helpen in de stap naar daadwerkelijke opvolging door capaciteiten te ontwikkelen.

4.2 Investeringen in veiligheid

Om de NIAV tot een succes te maken, moet de innovatie-agenda verbonden worden met de inkoop- en verwervings-agenda's van de nationale, regionale en lokale overheden en publieke en private operationele diensten. Maar ook met die van de semipublieke en private partijen in de belangrijkste vitale sectoren:

- *Energie*; elektriciteitsnetwerkbeheerders, gasnetbeheerders en energieleveranciers.
- *Telecommunicatie en ICT*; telecomoperators.
- *Water*; drinkwaterbedrijven, keren en beheren van oppervlaktewater; waterschappen.
- *Transport*; mainports Schiphol en haven Rotterdam.
- Financiële infrastructuur; banken.

Figuur 1: Werkwijze Nationale Veiligheid overheidsbreed



Ook publiek-private aanpak in de stedelijke veiligheid valt hieronder: evenementen, uitgaan, leefbaarheid in de wijken. Voorbeelden van initiatieven op het terrein van inkoop en investeringen zijn:

- het programma Inkoop Innovatie Urgent van het ministerie van Economische Zaken, bedoeld om 2,5 procent van het relevante inkoopvolume van de overheid te richten op innovatie;
- de rijksbrede *Small Business Innovation Research* (SBIR), een methode om innovatieve oplossingen te ontwikkelen voor maatschappelijke problemen;
- de VeiligheidsInnovatieCompetitie (VIC), die in samenwerking en onder regie van de ministeries van Defensie en VenJ plaatsvindt;
- de wijze waarop het ministerie van Defensie een stimulerende rol speelt bij innovatie, met instrumenten als *launching customership*.[36]

Het *Dutch Institute for Technology, Safety and Security* (DITSS) heeft bijvoorbeeld positieve ervaringen met regionale veiligheidsateliers en *field labs* om innovatieve veiligheidsoplossingen te ontwikkelen. Dergelijke initiatieven in de inkoop- en verwervingstrajecten verdienen brede navolging.

Publieke-private samenwerking in een innovatie- en experimenteerfase die voorafgaat aan een aanbestedingstraject, is in het veiligheidsdomein zeer gewenst. Veel producten en diensten in de veiligheidsmarkt zijn immers relatief complex en specifiek. Zonder de kennis en kunde van de partners en praktijkervaring in het voortraject is het voor de behoeftesteller lastig de gewenste of noodzakelijke vernieuwing te specificeren en te waarderen. Dit leidt tot aanbestedingen die op de laagste prijs sturen en die niet erg toekomstgericht zijn.
Ook moet worden voorkomen dat bedrijven die zijn betrokken in het voortraject worden uitgesloten van de aanbesteding.[37] Het is zaak de inkoop- en verwervingsprocessen zodanig vorm te geven en te versterken dat de objectiviteit geborgd is én er ruimte is voor innovatieve aanbestedingen. Het opzetten van pre-competitieve experimenteeromgevingen, bijvoorbeeld op terreinen van realtime intelligence, cybersecurity en het meldkamerdomein, lijkt daarvoor aangewezen.

'De staat is de echte technologische vernieuwer, niet het bedrijfsleven.'[38] Mariana Mazzucato

'Publiek ondernemerschap' is niet alleen nodig voor de continuïteit van publiek-private samenwerking in het traject van innovatie naar verwerving, maar ook omdat tussen innovatie en regelgeving fundamentele verschillen in tempo bestaan. Er zijn twee mogelijke oplossingen. Enerzijds is het zaak om aspecten als regelgeving, privacy, ethiek en besturingsvraagstukken vroegtijdig te betrekken in innovatietrajecten. Anderzijds moet de wet- en regelgever zo veel mogelijk flexibiliteit inbouwen en benutten. Tijdelijke ontheffingen bieden ruimte om te experimenteren met innovatieve benaderingen. Dit helpt vervolgens weer om praktisch relevante en afdwingbare wet- en regelgeving te formuleren, zeker op gebieden waar snelle ontwikkelingen plaatsvinden, zoals in het cyberdomein, forensics of bij de inzet van onbemande vliegtuigen. Het is opvallend dat de focus en urgentie bij *high profile* events als de recente Nuclear Security Summit in maart 2014, vaak leidt tot creatieve oplossingen die veel mogelijk maken. In combinatie met doelgericht budget zorgt dit voor een dynamiek die leidt tot goede proces-, keten- en productinnovaties. Vergelijkbare ervaringen op kleinere schaal zijn er in de *field labs* voor bijvoorbeeld evenementenveiligheid. De flexibiliteit die daarbij goed mogelijk blijkt, zou structureel moeten worden gemaakt.

Specifieke aandacht verdient het delen van ontwikkel- en testfaciliteiten. Voorbeelden zijn de Twente Safety Campus; bestaande uit de Troned-trainingslocatie, de Risk Factory en het *Safety Field* lab, de meld- en toezichtkamers in Brabant en de cybertestfaciliteiten in Den Haag. Deze zijn vaak duur en vanwege een lage bezettingsgraad lastig rendabel te maken. Hier is – pre-competitieve – samenwerking niet alleen goed mogelijk, maar vanuit economisch oogpunt vaak ook noodzakelijk. Gedeelde investering en beheer kan eventueel samengaan met gescheiden benutting.

4.3 Bestuurlijke complexiteit en regie op systeemniveau

De overheid is in de Nederlandse veiligheidsmarkt niet alleen beleidsbepalend, maar is als uitvoerder ook de belangrijkste vragende partij. Tegelijkertijd is de publieke structuur sterk horizontaal en verticaal gelaagd en decentraal georganiseerd. Er is sprake van bestuurlijke drukte in een complexe governancestructuur.

Crisisbeheersing in Nederland is in beginsel eenvoudig ontworpen: degene die verantwoordelijk is voor een beleidsterrein of ketens daarbinnen, is ook verantwoordelijk voor de beheersing van een crisis op dat terrein. Maar de praktijk is weerbarstiger door de complexiteit van de gedistribueerde verantwoordelijkheden, omdat die bij grotere incidenten meerdere beleidsterreinen raken. Er zijn dan ook meer dan vijftig aparte ketens met elk hun eigen bevoegdheden, daardoor blijkt regelmatig hoe ingewikkeld de coördinatie tussen veel verantwoordelijken in de praktijk is.[39] De complexiteit wordt nog eens vergroot doordat ketens verschillend georganiseerd zijn. Het gevolg is dat decentrale maatregelen in de ene keten afgestemd moeten worden met centrale maatregelen in een andere keten.

Samenwerkingsvorm	Collectieve besluitvorming	Interactie tussen partijen	Informatiedeling
netwerk	impliciet zelforganiserend, maatwerk, dynamisch	naar behoefte, onbegrensd	alle beschikbare en relevante informatie is toegankelijk
gezamenlijk	gezamenlijke processen en gedeelde plannen	breed en significant	breed over samenwerkings-gebieden en -functies
coördinatie	afgestemde processen en gekoppelde plannen	beperkt en toegespitst	specifiek over gecoördineerde gebieden en functies
deconflictering	afgesproken randvoorwaarden	erg beperkt en sterk toegespitst	informatie over randvoorwaarden en interfaces
geen	geen	geen	volledig operationeel gericht

Anders gezegd: de taken, verantwoordelijkheden en bevoegdheden (TVB's) zijn in erg veel hokjes verdeeld vis-à-vis een werkelijkheid die zich weinig van deze hokjes aantrekt. De TVB's van veel processen of incidenten vallen onder veel verschillende spelers, en daardoor in de praktijk vaak juist onder niemand. 'Strategische verlamming' ligt op de loer, waarbij iedereen beseft dat er iets moet gebeuren, maar niemand in staat, in de gelegenheid of bereid is het voortouw te nemen. Dat geldt voor operationele situaties, maar ook voor innovaties die de ketens doorsnijden en voor innovaties op systeemniveau.

In de praktijk constateren we een behoefte aan een partij – een *systeemintegrator* – die de regie voert in de vernieuwing van het integrale systeem van veiligheid in Nederland en die het voortouw neemt in de processen die tot samenwerking leiden. In de eerste alinea van het voorwoord van de *Strategie Nationale Veiligheid* uit 2007 stelde de toenmalige minister-president Balkenende: 'De regie voor versterking van de nationale veiligheid ligt bij de rijksoverheid.' Dit kan in de vorm van facilitatie – 'lichte' regie – of van sturing – 'zware' regie – en in de praktijk meestal in een zekere balans daartussen. Ter inspiratie geven we in de tabel hierboven de ontwikkelingsstappen die de NAVO in haar 'genetwerkt optreden' onderscheidt.[40] Hoewel dit model primair gebruikt wordt voor operationele samenwerking, kan het ook toegepast worden op samenwerking in innovatieprocessen.

4.4 Topsectorenbeleid en de roadmaps Security en ICT

De triple-helixbenadering die het fundament onder de NIAV vormt, sluit volledig aan op het algemene beleid van het ministerie van Economische Zaken (EZ). Het topsectorenbeleid benadrukt het belang van krachtige innovatie voor het verdienvermogen van onze economie. In de evolutie van dit beleid heeft EZ, in lijn met de adviezen van AWT (Adviesraad voor Wetenschap Technologie en Innovatie) en WRR (Wetenschappelijke Raad voor het Regeringsbeleid)[41] en het Europese beleid rond de 'grand challenges',[42] aangegeven de topsectoren beter te willen verbinden met maatschappelijke uitdagingen. In het topsectorenbeleid zijn afspraken gemaakt over hoe bedrijfsleven, overheid, universiteiten en onderzoekscentra samenwerken aan kennis en innovatie, die zijn vastgelegd in zogeheten *innovatiecontracten*. In het innovatiecontract voor de 'Topsector Thema Maatschappelijke Veiligheid' staat onder meer: 'Maatschappelijke veiligheid is bij uitstek een terrein waar de gouden driehoek als vanzelfsprekend aanwezig is. Omdat bij maatschappelijke veiligheid de behoeftestellende (vragende) partijen overheidspartijen zijn wordt er van oudsher samengewerkt met kennisinstellingen en bedrijven. Het thema maatschappelijke veiligheid is een stimulans om cross-overs te realiseren, om overheden als lead customer op te laten treden of innovatieve producten in te kopen.'[43]

Onder de topsector High Tech Systems and Materials is de *roadmap HTSM Security* vastgesteld.[44] Dit plan benoemt de volgende 'prioritaire gebieden van toepassing en technologische uitdaging':

- **System of systems**
  De evolutie naar een genetwerkt veiligheidsdomein vereist dat nieuwe technologieën en ICT-netwerken samen evolueren tot robuuste *system of systems*-oplossingen. Het is van essentieel belang dat deze evolutie gemanaged wordt met betrokkenheid van de volledige waardeketen: leveranciers van onderdelen, systeemleveranciers, kennisinstellingen en eindgebruikers.
- **Cyber security**
  De steeds grotere invloed van ICT op de samenleving vergroot het belang van cyberweerbaarheid en de bestrijding van cybercrime. De groeiende ketenafhankelijkheid van onderling verbonden ICT-systemen vereist nieuwe concepten. Er is al een groot kennisreservoir en het onderwerp is zeer urgent.
- **Sensoren**
  Voor effectieve beveiliging is informatie cruciaal. Zowel actieve als passieve sensortechnologieën zijn van belang. Er zijn veelbelovende ontwikkelingen op het gebied van intelligente sensoren en zelflerende systemen.

Ook de topsectoroverschrijdende ICT-roadmap[45] is van groot belang, onder meer vanwege de volgende thema's:

- **ICT om op te vertrouwen**
  Met aandacht voor veilige en betrouwbare infrastructuur, en privacy- en e-identiteitsvraagstukken.
- **ICT-systemen voor 'monitoring and control'**
  Richt zich onder meer op *sensor-based*-surveillance, grootschalige communicatie tussen sensornetwerken en koppeling van heterogene sensornetwerken.
- **Data, data, data**
  Innovatief datamanagement moet de verborgen werelden in grote datasets interpreteren. Heterogene data uit verschillende bronnen vereisen nieuwe manieren om trends te detecteren.

Naast HTSM hebben ook de topsectoren Water, Logistiek en Energie evidente raakvlakken met het veiligheidsdomein. Voor Creatieve Industrie, Agri & Food en Chemie is veiligheid ten minste een aandachtspunt. Organisaties in deze sectoren hebben vanuit de optiek van bedrijfscontinuïteit en klantbescherming belang bij cyber security, een betrouwbare digitale identiteit, leren van incidenten en rampen. In de praktijk hangen succesvolle innovaties in het veiligheidsdomein vaak samen met cross-overs tussen topsectoren.

4.5 Naar een lerende economie

'De belangrijkste manier om (...) de responsiviteit van de Nederlandse economie te vergroten, is het stimuleren van kenniscirculatie', aldus de WRR in zijn rapport *Naar een lerende economie*. De WRR stelt in zijn advies dat dit verder gaat dan het bevorderen van een kenniseconomie. Terwijl bij het streven naar een kenniseconomie de productie van nieuwe kennis boven aan de agenda staat, draait het bevorderen van kenniscirculatie erom bestaande kennis beter te gebruiken. Nieuwe kennis ontwikkelen blijft weliswaar belangrijk, maar er gaat daarnaast veel meer aandacht uit naar het mobiliseren en toepassen van ideeën en technieken die te vinden zijn in andere bedrijven, sectoren of landen. Dat vereist absorptievermogen: 'het vermogen om nieuwe en elders vigerende kennis te signaleren, op te nemen en vaardig te gebruiken'.

Om kenniscirculatie, het mobiliseren en toepassen van ideeën en technieken over de grenzen van bedrijven, sectoren of landen heen te verwezenlijken, doet de WRR aanbevelingen om menselijk kapitaal te vergroten en kennisinfrastructuur en instituties te versterken. In haar reactie op het WRR-advies[46] refereert de regering aan HSD als een van de 'sterktes van nu die de basis kunnen vormen van de sterktes over twintig jaar': 'Met The Hague Security Delta heeft Nederland de kennis in huis om in te spelen op de wereldwijd toenemende vraag naar oplossingen voor veiligheidsvraagstukken, bijvoorbeeld op het gebied van cyber security.' Het nationale veiligheidscluster HSD is ook een platform voor kenniscirculatie. Zoals het kabinet het stelt: 'Binnen het bedrijvenbeleid wordt kenniscirculatie bevorderd door de samenwerking tussen bedrijven en kennisinstellingen te versterken en onderzoeksagenda's beter af te stemmen op vragen uit de maatschappij.' Dit laatste is, voor het veiligheidsdomein, precies de opdracht die de NIAV zich stelt.

4.6 Smart Industry

We zitten midden in de vierde industriële revolutie. Dat biedt grote kansen. Een aantal partijen heeft onder de noemer *Smart Industry* het initiatief genomen om, naar voorbeeld van het grootschalige Duitse Industry 4.0-programma, het onderwerp ook in Nederland prioriteit te geven.[47] De centrale notie is dat we naar een wereld gaan waarin alles met alles verbonden is. ICT convergeert met sensortechnologie en robotica om een *internet of things* te vormen van zogenoemde *cyber-physical systems*. In het verlengde stellen fabrikanten hun systemen softwarematig open voor klanten en toeleveranciers. Zo kunnen de verschillende specialismen makkelijk worden gekoppeld om snel te vernieuwen en – zelfs realtime – de noden en wensen van de eindgebruikers te honoreren. Het wordt rendabel om kleine series of zelfs unieke klantspecifieke producten en diensten op de markt te brengen. *Openheid* gaat overigens niet alleen over de toegankelijkheid in het ontwikkelingsproces van een systeem, maar ook over het gebruik, het onderhoud en andere fasen van de levenscyclus. Technisch is dit alles al goed mogelijk, de open standaarden bijvoorbeeld zijn in grote lijnen voorhanden. Het knelpunt is vooral de terughoudendheid van de maakindustrie om daadwerkelijk open samen te werken. De industrie worstelt met haar verdienmodellen, als in principe iedereen met de ingebrachte open kennis aan de haal kan gaan en met zaken als aansprakelijkheid, continuïteit en intellectueel eigendom, als vele partijen, waaronder de eindgebruiker, kunnen 'meeprogrammeren' in bepaalde toepassingen.

Deze ontwikkeling is om een aantal redenen van belang voor de NIAV, als algemeen kader en mogelijk in de uitwerking van de innovatiespeerpunten:

- Hoewel gesproken wordt over de vierde industriële revolutie, zien we in de praktijk een evolutie. De benodigde sociale en procesinnovatie, maar ook zaken als wet- en regelgeving, zijn niet van vandaag op morgen voor elkaar te krijgen. Het nationale veiligheidscluster is hét platform waar voor de sector veiligheid de ontwikkeling richting Smart Industry stapsgewijs – maar wel sneller dan elders – gestalte kan krijgen. In *coalitions of the willing and able* van triple-helix-partijen kan in een enerzijds open, en anderzijds vertrouwde omgeving worden gewerkt aan technologieontwikkeling, samenwerkingsvormen en nieuwe businessmodellen die passen in het Smart Industry-paradigma.
- Een belangrijke trend is dat functionaliteit steeds meer in software en steeds minder in hardware wordt gestopt.

In een omgeving waarin via het internet alles met alles en iedereen kan worden verbonden, heeft zo'n benadering meer succes. Een voorbeeld is het succes van de software-centrische iPhone en Android-smartphone, afgezet tegen het falen van de hardwarecentrische Blackberry-toestellen. Deze trend heeft, ook in het veiligheidsdomein, grote consequenties voor verdienmodellen van bedrijven, de hele levenscyclus van systemen en de relatie tussen producenten en consumenten dan wel tussen veiligheidsprofessionals en burgers en raakt zo ten diepste bestaande economische modellen en maatschappelijke structuren.

- De kwetsbaarheid van *cyber-physical systems* voor cyber-aanvallen verdient veel meer aandacht. Op het raakvlak van de virtuele en de fysieke wereld kunnen cyberaanvallen op een heel directe manier maatschappelijk ontwrichtend en zelfs levensbedreigend worden. Dit wordt door zowel de overheid als de private sector nog onvoldoende herkend en aangepakt.

4.7 De Europese 'grand challenge' Secure Societies

Waar het Nederlandse topsectorenbeleid als hoofdstructuur economische sectoren hanteert, kiest de Europese Unie voor een primaire ordening langs zes maatschappelijke uitdagingen of 'grand challenges'. Een van die grand challenges is *Secure Societies – Protecting Freedom And Security Of Europe And Its Citizens*. In het kader van de NIAV is van belang hoe deze uitdaging zich vertaalt in het grote Europese onderzoeksprogramma Horizon 2020. Het onderzoek voor *Secure Societies* richt zich op het ontwikkelen van nieuwe kennis en technologie voor de bestrijding van misdaad en terrorisme, crisismanagement en de externe dimensie van veiligheid. Het onderzoek is civiel georiënteerd, maar ook technologieën die ingezet kunnen worden in zowel het civiele als het militaire domein, het zogenaamde 'dual-use', komen aan bod.

Het onderzoek voor *Secure Societies*[48] kent onder meer de volgende relevante vraagstukken:[49]

- misdaad, illegale handel en terrorisme bestrijden;
- de vitale infrastructuur beschermen en minder kwetsbaar maken;
- forensische identiteitsherkenning;
- cyber security versterken:
- privacyvraagstukken bij inzet big data voor de veiligheid;
- illegale informatie en handel opsporen het zogenaamde *dark web*;
- internationaal juridische richtlijnen en versterking standaardisatie bij cyber security;
- detectie oneigenlijk binnendringen;
- kwetsbaarheidanalyses;
- de weerbaarheid bij crises en rampen versterken, inclusief preparatie;
- interactieve crowdsourcing bij crises en rampen, inclusief analyse en besluitvorming;
- bescherming digitale identiteit om digitaal misbruik te voorkomen.

Aansluiting van nationale innovatiespeerpunten bij het Europees veiligheidsonderzoek is om twee redenen een goed idee. Ten eerste wordt aangesloten bij de internationale agenda, met zowel een maatschappelijke als economische dimensie. Hiermee wordt de juiste focus aangegeven. Ten tweede kan Europese onderzoeksgelden een hefboom vormen op bijdragen van nationale partijen. Hiermee bouwen we massa op.[50]

Ontwikkeling van de internationale dimensie van HSD is dus van groot belang. De deelname van HSD-partners in EU-netwerken en de bekendheid in Brussel zijn zeker van meerwaarde voor HSD.

'Het financieren van onderzoek en innovatie is essentieel voor de toekomst van Europa, daar het zal bijdragen aan groei, werkgelegenheid en een betere levenskwaliteit. Nederlandse onderzoekers hebben gezien hun kwaliteiten alle kansen in Horizon 2020, dat tot doel heeft de toponderzoekers van universiteiten, onderzoeksinstituten en bedrijven in Europa te laten samenwerken in grensverleggende projecten.'[51] Robert-Jan Smits

De Europese Commissie past de richting van de onderzoeksgebieden per tweejarig werkprogramma aan op basis van actuele ontwikkelingen. In de tabel hierna koppelen we het werkprogramma 2014-2015 voor *Secure Societies* aan de innovatiespeerpunten van de NIAV.

Topics Secure Societies	Relevante innovatiespeerpunten
Topic Disaster-resilience **Part I. Crisis management**	• Regievoering vraagarticulatie 'één overheid' • Leren van incidenten en oefeningen • Waardecreatie in triple-helixinnovatie • Sociale innovatie en zelforganiserend vermogen • Bewustwording: perceptie versus realiteit • Genetwerkte informatie op knooppunten • Visie- en conceptontwikkeling voor operaties met onbemande sensorplatformen • Geïntegreerd optreden met heterogene teams • Koppeling actuele werkelijkheid-virtuele omgeving
Topic Disaster-resilience **Part II. Disaster Resilience & Climate Change**	• Waardecreatie in triple-helixinnovatie • Security by design in stedelijke voorzieningen en bij evenementen
Topic Disaster-resilience **Part III. Critical Infrastructure Protection**	• Security by design in stedelijke voorzieningen en bij evenementen • Kenmerken en afbakening vitaal
Topic Disaster-resilience **Part IV. Communication technologies and interoperability**	• Ketenbenadering cyber security • Genetwerkte informatie op knooppunten • Vaststellen en garanderen van – digitale – identiteit
Topic Disaster-resilience **Part V. Ethical/Societal Dimension**	• Sociale innovatie en zelforganiserend vermogen • Bewustwording: perceptie versus realiteit • Kenmerken en afbakening vitaal
Topic Fight against crime and Terrorism, **Part I. Forensics**	• Ketenbenadering cyber security • Vaststellen en garanderen van – digitale – identiteit • Herkennen en voorspellen van afwijkend gedrag
Topic Fight against crime and Terrorism **Part II. Law enforcement capabilities**	• Ketenbenadering cyber security • Vaststellen en garanderen van – digitale – identiteit • Visie- en conceptontwikkeling voor operaties met onbemande sensorplatformen • Operationele autonomie UAV's • Koppeling actuele werkelijkheid-virtuele omgeving
Topic Fight against crime and Terrorism **Part III. Urban security**	• Security by design in stedelijke voorzieningen en bij evenementen
Topic Fight against crime and Terrorism **Part IV. Ethical/Societal Dimension**	• Sociale innovatie en zelforganiserend vermogen • Bewustwording: perceptie versus realiteit
Topic Border Security and External Security **Part I. Maritime Border Security**	• Herkennen en voorspellen van afwijkend gedrag • Visie- en conceptontwikkeling voor operaties met onbemande sensorplatformen • Operationele autonomie UAV's
Topic Border Security and External Security **Part II. Border crossing points**	• Herkennen en voorspellen van afwijkend gedrag • Vaststellen en garanderen van – digitale – identiteit
Topic Border Security and External Security **Part III. Supply Chain Security**	• Vaststellen en garanderen van – digitale – identiteit

Topics Secure Societies	Relevante innovatiespeerpunten
Topic Border Security and External Security **Part IV. External Security**	• Genetwerkte informatie op knooppunten • Herkennen en voorspellen van afwijkend gedrag • Vaststellen en garanderen van – digitale – identiteit • Koppeling actuele werkelijkheid-virtuele omgeving
Topic Border Security and External Security **Part V. Ethical/Societal Dimension**	
Topic Digital Security **Cyber security, Privacy and Trust**	• Sociale innovatie en zelforganiserend vermogen • Bewustwording: perceptie versus realiteit • Kenmerken en afbakening vitaal • Cybersecurity 'Internet of Things' • Ketenbenadering cyber security • Genetwerkte informatie op knooppunten • Herkennen en voorspellen van afwijkend gedrag • Vaststellen en garanderen van – digitale – identiteit

‘Voor mij is HSD geslaagd als we binnen Europa te boek staan als ‘the place to be’ voor veiligheid en innovatie; een soort Sillicon Valley waar nationale en internationale overheden, bedrijven en kennisinstellingen graag bij willen horen, de NIAV is daarvoor een essentieel instrument op een cruciaal moment.’[53]

Ida Haisma

5 – Finale overwegingen

Met thema's en speerpunten brengt de Nationale Innovatieagenda Veiligheid 2015, koers, focus en inhoud aan. De speerpunten behoeven verdere uitwerking, waarin nieuwe accenten naar voren kunnen komen. De NIAV is geen voorschrift, maar brengt samenwerkingsprocessen tussen triple-helixpartners op gang.

Essentieel is dat partijen zich herkennen in de speerpunten, ermee aan de slag gaan, ze eventueel bijpunten en ze vervolgens verwezenlijken. Hier ligt een belangrijke verantwoordelijkheid van de partners in de nationale veiligheidscluster: de overheid op alle niveaus en in alle toepasselijke hoedanigheden en rollen, de bedrijven en de kennisinstellingen.

De volgende stappen zijn:
Consortia rondom de thema's en speerpunten vormen voor de verdere programmering, de buitengewone kennis en expertise uit de triple helix bundelen en een hieraan gekoppelde nationale verwervingsagenda opbouwen.
Een werkwijze waarbij dwars door de ketens heen met elkaar wordt samengewerkt aan nieuwe oplossingen en aan een security delta met internationale faam. Samenwerken in de triple helix is niet nieuw, maar samenwerken in deze omvang en reikwijdte is dat wel en vergt veel van de samenwerkende partijen. Openheid, vertrouwen en rekening houden met elkaars belangen zijn belangrijke condities om *coalitions of the willing and able* te vormen. Vanuit het perspectief van de bv Nederland redeneren is van belang om succesvolle innovatietrajecten te kunnen doorlopen die maatschappelijk en economisch renderen.

'Complimenten aan HSD voor de totstandbrenging van een innovatieagenda waarin partijen uit bedrijfsleven, overheid en kennisinstellingen zich met elkaar verbinden.'[52] Laetitia Griffith

De NIAV wordt gefaciliteerd, beheerd en periodiek geactualiseerd door het nationale veiligheidscluster HSD. De NIAV maakt onderdeel uit van de HSD-strategie. Als zodanig vormt de voortgang en actualisering van de NIAV een terugkerend onderwerp voor het nationale veiligheidscluster HSD.

Bijlage 1 – **Gesprekspartners in consultatie- en toetsingsrondes**

Achternaam		Voornaam	Functie en organisatie	Gesproken op
Akerboom		Erik	Secretaris-generaal ministerie van Defensie	05-10-2014
Asten	van	Arian	Afdelingshoofd en mt-lid Nederlands Forensisch Instituut	02-09-2014
Barthel		Jan-Piet	Programmamanager Cyber Security NWO/IIPVV	20-10-2014
Berg	van den	Steffie	Medewerker Innovatie NCTV	11-03-2014 17-06-2014
Berlo	van	Marcel	Trekker Innovatiehuis Urban Security en senior business developer Defense Safety and Security TNO	10-04-2014
Birkhoff		Kees	Senior vice-president en manager Public Sector, Capgemini Nederland en lid HSD-Board	26-06-2014
Brabander-Ypes	de	Heleen	Senior adviseur industriële participatie ministerie van Economische Zaken	13-05-2014 12-06-2014
Brandt		Dick	Voorzitter IIP VV	20-10-2014
Brouwers		Joep	Adjunct-directeur Brainport	21-08-2014
Brouwers		Juul	Communicatiemanager Cyber Security IIPVV/NWO	20-10-2024
Bruinen	den	Joris	Secretaris HSD-Board	11-06-2014
Burger		Helen	Adviseur Informatievoorziening, Strategie, Beleid en Bestuur Nationale Politie	05-03-2014
Casparie		Stefanie	Coördinerend adviseur Innovatie Nationale Politie	24-07-2014 25-08-2014
Cloo		Pieter	Secretaris-generaal ministerie van Veiligheid en Justitie	26-08-2014
D'Huy		Kees	Directeur Smart Cities, TNO en lid HSD-executive Committee	06-03-2014
Dobbenberg		Ernst	Hoofd Cluster Kennis en Innovatie Defensiestaf	02-09-2014
Don		Bert	Strategic Advisor National Security TNO	15-04-2014 03-09-1014
Drift	van der	Reinier	Directeur Authasas	20-10-2014
Engelshoven	van	Ingrid	Wethouder Kenniseconomie, Internationaal, Jeugd en Onderwijs en eerste locoburgemeester gemeente Den Haag	27-10-2014
Essen	van	Henk	Lid Korpsleiding Nationale Politie	15-07-2014
Freriks		Leo	Trekker Innovatiehuis Critical Infrastructure en City accountmanager Siemens	08-07-2014
Frinking		Erik	Trekker Innovatiehuis Nationale Veiligheid en director of the strategic futures programme HCSS	18-03-2014
Genet		Louis	Programmadirecteur Internationale stad Den Haag	23-06-2014 10-09-2014
Gieling		Albert	Sectorhoofd Brandweer Twente	11-09-2014
Gooijer		Dennis	Directeur KPN Critical Communications	15-10-2014
Haas	de	Robin	Cyber Security en Defense Safety & Security TNO	30-06-2014
Haisma		Ida	Executive directeur HSD	09-07-2014
Heer	de	Johan	Directeur T-Xchange	11-09-2014
IJzinga		Niek	Trekker innovatiehuis Cybersecurity en seniormanager Cyber Risk Services Deloitte	30-06-2014
Jacobs		Gabriele	Associate professor EUR/RSM center of excellence public safety management	22-05-2014
Jansen		Frederik	Programmamanager Twente Safety and Security (TS&S) en lid HSD-Adviesraad	11-09-2014
Keuning		Jelle	Directeur R&D ministerie van Defensie	20-10-2014 05-10-2014
Klaasen		But	Programmamanager Innovatie NCTV, ministerie van Veiligheid en Justitie en lid HSD-Adviesraad	02-07-2014 26-08-2014
Klaauw	van der	Marcel	Senior programmamedewerker Investeringen internationale stad gemeente Den Haag	10-09-2014
Kool		Henk	(Voormalig) wethouder Economie gemeente Den Haag	26-03-2014
Leeuwen	van	Michel	Afdelingshoofd binnen directie Cyber Security NCTV	27-03-2014
Luijken	van	Coen	Directeur Businessdevelopment Trigion	08-07-2014

Achternaam		Voornaam	Functie en organisatie	Gesproken op
Marel	van der	Menno	Directeur Fox-IT en lid HSD-Board	08-07-2014
Mennen		Marcel	Algemeen secretaris analistennetwerk nationale veiligheid en afdelingsmanager RIVM	03-07-2014
Noordanus		Peter	Burgemeester van Tilburg en lid HSD-Board	29-09-2014
Oosterom		Louis	Trekker Innovatiehuis Critical Infrastructure	16-04-2014
Otten		Jan	Strategisch adviseur Dutch Institute for Technology, Safety and Security (DITSS) en lid HSD-Adviesraad	07-05-2014
Oudsten	den	Peter	(vml.) Burgemeester van Enschede, voorzitter Veiligheidsregio Twente en lid HSD-Board	30-06-2014
Putten	van	Marieke	Programmamanager Inkoop Innovatie Urgent ministerie van Economische Zaken	19-03-2014
Remerie		Max	Directeur Business Development Siemens en lid HSD-Executive Committee	08-07-2014
Reyn		Sebastian	Directeur Integraal Beleid ministerie van Defensie	20-10-2014
Sluijter		Guus	Directeur Dutch Institute for Technology, Safety and Security (DITSS)	02-07-2014 09-09-2014
Smits		Aart Jan	Voorzitter Roadmap Security HTMS en lid HSD-Executive Committee	08-07-2014 21-10-2014
Tossings		Maarten	Directeur Beleid ministerie van Defensie	03-03-2014
Vet	van der	Hans	Plaatsvervangend directeur Openbare Orde en Veiligheid gemeente Den Haag	04-07-2014
Vianen	van	John	Directeur zakelijke markt KPN en lid HSD-Board	15-10-2014
Vroet	de	Stephanie	Medewerker Innovatie NCTV	11-03-2014 17-06-2014
Wiebes		Mark	Commissaris van politie en innovatiemanager Landelijke Eenheid Nationale Politie	01-07-2014
Wijk	de	Rob	Algemeen directeur HSD	18-06-2014
Wissen	van	Jaap	Veiligheids- en innovatieadviseur Rijkswaterstaat	20-10-2014
Zaal		Leo	Directeur Instituut voor Fysieke Veiligheid	08-07-2014
Zorko		Patricia	Hoofd Operaties Nationale Politie en lid HSD-Adviesraad	27-08-2014
Zunderd	van	Peter	Hoofd Landelijke Operationele Staf Nationale Politie en lid HSD-Adviesraad	21-07-2014

Bijlage 2 – **Geraadpleegde documenten**

Er zijn veel documenten die gewenste of geplande, dan wel lopende innovatietrajecten in het veiligheidsdomein beschrijven. Soms met innovatie als het centrale onderwerp, soms als hoofdstuk in een breder visie- of plandocument. De bronnen verschillen ook in de nadruk die ze leggen op de fasen in het traject van idee tot product. Zo is bijvoorbeeld de innovatieagenda Veiligheid en Justitie vooral gericht op de beginfase van innovatietrajecten, daar waar creatieve nieuwe ideeën moeten worden ontwikkeld die op termijn tot sprongsgewijze vernieuwing kunnen leiden, maar die ook vaak ook ergens in het traject stranden. Hoewel er duidelijk overlap in thematiek zit met de NIAV, het accent op de toepassing van innovatie, waar kansrijke innovatieve ideeën worden vertaald in oplossingen met marktpotentieel.

Er zijn, kortom, veel perspectieven mogelijk die allemaal zijn meegewogen in de selectie van innovatiespeerpunten in de NIAV. Door interviews met diverse partijen hebben we geprobeerd de verbintenis van de diverse documenten met de NIAV zo goed mogelijk te duiden. De lezer zal er begrip voor hebben dat de veelheid aan bronnen en invalshoeken het ondoenlijk maakt om via gerichte verwijzingen in de tekst recht te doen aan alle inbreng. We volstaan hier met een opsomming van geraadpleegde documenten.

Europa

European Commission. (juni 2013). *EU-research for a secure society, security research projects under the 7th framework.*

Fraunhofer Institute for Technological Trend Analysis. (2013). *Evaluation of critical and emerging security technologies for the elaboration of a strategic research agenda. Etcetera.*

Horizon 2020 Work Programme 2014-2015. (december 2013). *Secure Societies - Protecting freedom and security of Europa and its citizens.*

Netherlands Organisation for Scientific Research. (november 2013). *Call for proposals Cybersecurity 2014.*

Nationaal/Rijksniveau

Bruggen slaan. (oktober 2012). Regeerakkoord VVD-PvdA.

Capgemini.(2013). *Trends in Veiligheid 2013, Een digitale samenleving kan niet zonder digitale veiligheid.*

Capgemini Consulting. (april 2014). *Trends in veiligheid 2014, digitale ketensamenwerking.*

Denktank Nationale Veiligheid. (januari 2009). *Verantwoordelijkheid voor Nationale Veiligheid.*

Denktank Nationale Veiligheid. (juni 2013). *Veiligheid als gedeeld belang.*

DigiSafe Cyber Security Centre. (mei 2014). *The hub for cyber security professionals.*

ICT Innovatie Platform Veilig Verbonden (september 2013). *National Cyber Security Research Agenda II.*

Ministerie van Defensie. (2011). *Strategische Kennis- en Innovatie Agenda (SKIA).*

Ministerie van Defensie. (februari 2014). *Defensie Industrie Strategie.*

Ministerie van Economische Zaken. (augustus 2013). *Programma Inkoop Innovatie Urgent, een ondernemender houding van de overheid.*

Ministerie van Economische Zaken. (mei 2012). *Samenvatting Innovatiecontract Topsector, thema maatschappelijke veiligheid.*

Ministerie van Economische Zaken. (juli 2013). *Agentschap NL, Strategisch aanvalsplan NL: Digital Gateway to Europa.*

Ministerie van Economische Zaken. (juli 2014). *Strategisch Kader TO2 federatie en het Strategisch Plan TNO 2015-2018 en de kabinetsreactie daarop.*

Ministerie van Infrastructuur en Milieu. (juni 2012). *IenM maakt ruimte, strategische kennis- en innovatieagenda IenM 2012-2016.*

Ministerie van Veiligheid en Justitie. (2014). *Werken aan een veilige en rechtvaardige samenleving.*

Ministerie van Veiligheid en Justitie. (2014). *WODC, Onderzoeksprogramma 2014.*

Ministerie van Veiligheid en Justitie. (augustus 2013). *NCSC, Cybersecuritybeeld NL.*

Ministerie van Veiligheid en Justitie. (januari 2014). *Jaarplan NCTV 2014.*

Ministerie van Veiligheid en Justitie. (maart 2013). *Eenheid in Verscheidenheid.*

Ministerie van Veiligheid en Justitie. (mei 2013). *Aanzet tot SKIA Ministerie VenJ. (niet gepubliceerd)*

Ministerie van Veiligheid en Justitie. (oktober 2013). *National Cyber Security Strategy II, from awareness to capability.*

Ministerie van Veiligheid en Justitie. (oktober 2014). *Innovatieagenda VenJ (concept).*

Ministerie van Veiligheid en Justitie. (september 2013). *Evaulatiecommissie Wet Veiligheidsregio's en het stelsel van Rampenbestrijding en Crisisbeheersing.*

Ministerie van Veiligheid en Justitie, NCTV. (november 2013). *Strategie Nationale Veiligheid.*

Ministerie van Veiligheid en Justitie, NCTV. (november 2013). *Voortgangsbrief Nationale Veiligheid.*

Ministerie van Veiligheid en Justitie, NCTV. (september 2013). *Trendrapportage Veilig door Innovatie, Agenda 2013.*

Nationale Politie. (december 2012). *Inrichtingsplan.*

Nationale Politie. (december 2012). *Realisatieplan.*

Nationale Politie. (januari 2012). *Ontwerpplan Nationale Politie.*

Nationale Politie. (november 2011). *Politieacademie, Strategische Onderzoeksagenda.*

Nederland Ondernemend Innovatieland. (juni 2008). *Maatschappelijke Innovatie Agenda Veiligheid.*

OECD Directorate for science, technology and industry. (april 2014). *OECD review of the Netherlands' innovation policy, assesments and recommendations.*
Stichting Toekomstbeeld der Techniek. (mei 2014). *Horizonscan 2050, anders kijken naar de toekomst.*
Strategie Nationale Veiligheid. (oktober 2009). *Werken met scenario's, risicobeoordeling en capaciteiten.*
The Hague Security Delta. (oktober 2014). *Strategie en Urgentieprogramma.*
TNO. (april 2014). *Technologieverkenning Nationale Veiligheid.*
TNO. (augustus 2013). *Nationale Risico Beoordeling 2012.*
Uitwerking Advies Bestuurlijke Werkgroep Bovenregionale Samenwerking. (februari 2013). *Eenheid in verscheidenheid.*
Wegwijzer Horizon 2020. (oktober 2014). *Calls 2014-2015. Rijksdienst voor Ondernemend Nederland.*
Wetenschappelijke Raad voor het Regeringsbeleid. (februari 2014). *Naar een lerende economie, kabinetsreactie daarop.*
Wetenschappelijke raad voor het regeringsbeleid. (november 2011). *Evenwichtskunst, over de verdeling van verantwoordelijkheid voor fysieke veiligheid.*

Decentraal

Brainport 2020. (2011). *Top economy, smart society.*
Brandweer. (november 2012). *Strategisch Meerjaren Onderzoeks- en Innovatieprogramma Brandweer.*
Digitale Steden Agenda. (maart 2013). *Convenant Smarter Cities.*
Dutch Institute Technology, Safety and Security. (2014). *Business canvas model.*
ING. (september 2014). *Economisch bureau, na drie jaar weer groei voor Haagse economie.*
Roadmap smart city Den Haag. (maart 2014). *Samen naar een slimme stad.*
Veiligheidsberaad. (februari 2014). *Voorwaartse agenda.*
Veiligheidsberaad. (januari 2014). *Agenda van de Veiligheidsregio's.*
Veiligheidsberaad. (januari 2014). *Slotnotitie werkconferentie doorontwikkeling veiligheidsregio's.*
Veiligheidsberaad. (juni 2011). *Verbindende schakel in rampenbestrijding en crisisbeheersing.*
Veiligheidsberaad. (mei 2014). *Strategische agenda versterking veiligheidsregio's 2014-2016.*
Veiligheidsregio Twente. (oktober 2012). *Beleidsplan Veiligheidsregio Twente 2013-2015.*

Industrie

Hightech Systems and Materials. (31 mei 2013). *Roadmap HTSM Security, herziene versie.*
Rijksdienst Voor Ondernemend Nederland. (juli 2008). *Innovatie Agenda Energie*.

Kennisinstituten

Amsterdam Economic Board. (november 2011). *Kennis en Innovatie Agenda.*
Erasmus Universiteit/Rotterdam School of Management. (januari 2014). *Center of Excellence for Public Safety Management.*
NFI. (februari 2014). *Het Nederlands Forensisch Instituut, in feite het beste.*
Sentinels. (oktober 2012). *Onderzoeksprogramma gericht op verbetering van kennis over computer en netwerkveiligheid binnen Nederland.*
TNO. (2014). *Voortgangsrapportage 2013 TNO, Vraaggestuurd Programma Security (concept).*
TNO. (december 2011). *An integrated approach to national security.*
TNO. (december 2012). *Veiligheid schreeuwt om innovatie.*
TNO. (december 2013). *Advanced Risk Management.*
TNO. (februari 2007). *De kracht van het Cyclische Concept.*
TNO. (september 2013). *Maatschappelijke Veiligheid.*
TNO. (september 2014). *Speurwerkprogramma 2015-2018.*
TNO. (september 2014). *Technologieradar Veiligheid t.b.v. NCTV en Nationale Politie.*
TU Delft. (april 2014). *De oplossing van de crisis kost niets, Manifest Nico Baken.*
TU Delft. (oktober 2014). *Technology-supported Risk Estimation by Predictive Assessment of Socio-technival Security.*

Bijlage 3 – **Noten**

1 Ivo Opstelten, minister van Veiligheid en Justitie, in een toespraak tijdens de opening van de HSD Campus, 13 februari 2014, rijksoverheid.nl.
2 Ivo Opstelten, minister van Veiligheid en Justitie, tijdens een toespraak op de ASIS-conferentie, 2 april 2014, World Forum Den Haag, rijksoverheid.nl.
3 *Bruggen slaan*, het regeerakkoord van de VVD en PvdA, stelt: 'Veiligheid is een kerntaak van de overheid. Burgers moeten zich veilig kunnen voelen op straten en in wijken. Politie en Justitie moeten daadkrachtig en gezaghebbend kunnen optreden (...) in de strafrechtketen krijgen (...) innovatie (...) bijzondere aandacht' (p. 26).
4 Regeerakkoord: 'De positie van Nederland in de top 5 van de meest concurrerende economieën moet de komende jaren verankerd en versterkt worden. Ons land heeft daarvoor een uitstekende uitgangspositie met zijn innovatieve bedrijven en excellente kennisinstellingen, een krachtige overheid (...) kan in belangrijke mate bijdragen aan de versterking van die positie' (p. 8); 'Onderwijs en wetenschap in Nederland zijn van hoog niveau, maar onze ambitie reikt verder, wij willen tot de top 5 van de wereld gaan behoren' (p.16); 'Nederland kent van oudsher een sterke internationale oriëntatie (...) Nederlandse bedrijven hebben grote belangen in het buitenland. Het buitenlands beleid is gericht op het behartigen en beschermen daarvan en bevordert de internationale rechtsorde' (p. 14); 'Europa is van groot belang voor onze vrede, veiligheid en welvaart, we verdienen er ons geld; onze banen zijn er voor een groot deel van afhankelijk' (p.13).
5 Zie 'De staat is de echte technologische vernieuwer', Het *Financieele Dagblad*, 6 februari 2014.
6 Erik Akerboom, secretaris-generaal van het ministerie van Defensie tijdens gesprek met opstellers van de NIAV, 5 november 2014.
7 Waarbij de regio's onderscheidende sterkten en speerpunten in het cluster inbrengen en zo aanvullend en herkenbaar te werk gaan om samen te streven naar maatschappelijke en economische waardecreatie.
8 In de praktijk is inbreng van de andere triple-helixpartners onmisbaar om vragen expliciet te maken.
9 De NIAV richt zich eerder op de commerciële toepassing van vernieuwende oplossingen, dan op conceptualisering of ontwikkeling van nieuwe ideeën.
10 Menno van de Marel, CEO Fox-IT, 'Cybersecurity in het regeerakkoord', Fox-IT.com, 14 september 2012.
11 Rob de Wijk, algemeen directeur HSD, *OndernemersClub*, RTL 7, 13 oktober 2014.
12 Soms als zelfstandig document, soms opgenomen in een algemeen visie-, strategie- of positioneringsdocument.
13 Voor deze bestuurdersbijeenkomst zijn uitgenodigd: de burgemeesters van de gemeenten Den Haag, Eindhoven, Tilburg, Enschede, de wethouder Kenniseconomie, Internationaal, Jeugd en Onderwijs van Den Haag, de secretaris-generaal van het ministerie van Veiligheid en Justitie, de secretaris-generaal van het ministerie van Defensie, de Nationaal Coördinator Terrorismebestrijding en Veiligheid, de korpschef van de Nationale Politie, de directeur-generaal Bedrijfsleven en Innovatie van het ministerie van Economische Zaken, de voorzitter van het Veiligheidsberaad, de algemeen directeur veiligheid van TNO, de voorzitter van de *roadmap security* HTSM, de voorzitters van de raden van bestuur van de TU-Delft, TU-Eindhoven, Haagse Hogeschool, decanen van de universiteiten van Twente, Tilburg en Leiden (Campus Den Haag), directeur HCSS, de voorzitter van de NIDV en de vertegenwoordigers KPN, Thales, Siemens, Haagse Hogeschool, Caggemini, Trigion en Fox-IT in de HSD-Board.
14 Er zijn in het veiligheidsdomein verschillende ketens van onderling afhankelijke en in elkaar grijpende processen en structuren die gezamenlijk vanuit een bepaalde invalshoek het veiligheidssysteem als geheel beschrijven. Voorbeelden zijn de operationele veiligheidsketen anticipatie-preventie-preparatie-repressie-nazorg, de onderling verbonden vitale nationale belangen territoriale veiligheid-economische veiligheid-ecologische veiligheid-fysieke veiligheid-sociale en politieke stabiliteit, de functionele zuilen politie-brandweer-Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR)-openbaar bestuur-krijgsmacht, en de fysieke-virtuele domeinen. In zekere zin vormt de triple helix ook zo'n keten. Een belangrijke notie hierbij is dat de keten zo sterk is als zijn zwakste schakel. Een cruciale functie van het nationale veiligheidscluster en de NIAV is om de afzonderlijke schakels in hun ketencontext te plaatsen, om zo innovatieprioriteiten te stellen die zowel concreet en gericht zijn (op schakelniveau) als bijdragen aan het oplossen van wezenlijke vraagstukken (op keten- of systeemniveau).
15 Dit criterium zorgt er ook voor dat we voortbouwen op bestaande sterktes, omdat anders zo'n effectieve coalitie niet tot stand kan komen.
16 Het gaat dus primair om innovaties in of na de fase van *proof of concept* en minder op die innovaties die in eerdere fase(n) van ontwikkeling zijn.
17 Henk Geveke, managing director Defence, Safety and Security TNO, ter gelegenheid van de presentatie van het boek *Veiligheid schreeuwt om innovatie*, tno.nl, 14 december 2012.
18 Laetitia Griffith, voorzitter Nederlandse Veiligheidsbranche in een schriftelijke reactie op de NIAV, 1 oktober 2014.
19 Een goed voorbeeld is de internationale zone waarin de gemeente Den Haag opdracht heeft verleend aan een consortium van HSD-partners om met diverse operationele gebruikersorganisaties een programma van eisen te ontwikkelen om een *shared security operations centre* te bewerkstelligen
20 Zie bijvoorbeeld WRR, *Evenwichtskunst; over de verdeling van verantwoordelijkheid voor fysieke veiligheid*, 2011; Denktank Nationale Veiligheid, *Veiligheid als gedeeld belang*, 2013; NCTV, *Voortgangsbrief Nationale Veiligheid*, 8 november 2013.
21 Dit sluit bijvoorbeeld ook goed aan bij ontwikkelingen in Twente zoals *Veilige Wijken, Community resilience, Burger participatie in scenario-ontwikkelingen, Smart connection* en *Gezamenlijk trainen en crisiscommunicatie*.
22 Landelijke evenementen als U-meet Cybersecurity en Alert Online dragen bij aan dit bewustzijn.
23 Zie ook speerpunt 10
24 NCTV, http://www.rijksoverheid.nl/vitale-sectoren.pdf
25 NCTV, *Tussen naïviteit en paranoia: nationale veiligheidsbelangen bij buitenlandse overnames en investeringen in vitale sectoren*. Eindrapportage Werkgroep Economische Veiligheid, april 2014.
26 Het programma *Sensing* van de Nationale Politie is op dit moment gericht op de koppeling van informatie binnen de publieke diensten, omdat dit eenvoudig te bereiken is. De verwachting is dat in de toekomst ook de beelden van professionele private bronnen zullen worden gekoppeld aan publieke bronnen. Alarmcentrales van beveiligingsbedrijven kunnen dan ook een belangrijke knooppuntrol spelen.
27 Veel van de huidige commercieel verkrijgbare UAVs worden feitelijk illegaal ingezet. Het huidig gebrek aan handhaving is bij de geprojecteerde groei van het zakelijk en privégebruik steeds minder vol te houden. De wettelijke veiligheidseisen zullen strikter worden en beter gehandhaafd. De veiligheidsspecificaties van commerciële systemen zullen dan sterk verbeteren, mogelijk tot een ook voor Politie en Defensie gewenst niveau. Tot het zo ver is blijven 'eigen' oplossingen noodzakelijk.
28 Laetitia Griffith, voorzitter Nederlandse Veiligheidsbranche in een schriftelijke reactie op de NIAV, 1 oktober 2014.
29 Ivo Opstelten, minister van Veiligheid en Justitie, in een mail aan HSD op 3 oktober 2014.
30 Kees Verhoeven, Tweede Kamerlid D66, woordvoerder Economie

in Het *Financieele Dagblad*, 14 oktober 2014.

31 Organisaties opgenomen in deze kolom, die zitting hebben in de HSD-Board, hebben toegezegd (co)trekker van het betreffend speerpunt te willen zijn.

32 European Network for Cyber Security (ENCS), een netwerk van (leden) Alliander, E.ON, KPN, Enexis, Westland Infra en DNV KEMA, en (partners) TNO, TU Delft, Applied Risk, Accenture en Wurldtech, is gericht op toegepast onderzoek, trainingen, testen en advies met betrekking tot de veiligheid van systemen voor industriële procescontrole.

33 TRONED biedt als *shared facility/operational field lab* voorzieningen aan om verschillende technologieën te testen of ermee te experimenteren, zoals RedSuit en UAV's. TRONED is ook een samenwerkingsvoorziening om nieuwe trainingsconcepten (*serious games*) en curricula te ontdekken, te ontwikkelen en uit te voeren in samenwerking met diverse instituten, het ministerie van Defensie, academies, hogescholen en een variëteit aan technologiebedrijven, bijvoorbeeld Re-Lion, KITT-engineering, E-Semble, V-Step en T-Xchange.

34 Ivo Opstelten, minister van Veiligheid en Justitie, ter gelegenheid van de presentatie van het boek *Veiligheid schreeuwt om innovatie*, tno.nl, 14 december 2012.

35 Plaatsen, processen of domeinen waar grootschalige investeringen, cross-overvraagstukken en innovatiebehoeften elkaar ontmoeten.

36 Ministeries van Defensie en Economische Zaken, *Defensie Industrie Strategie*, december 2013.

37 In beginsel is er voldoende ruimte in de aanbestedingsregels voor een zekere exclusiviteit die, vanwege marktfalen in de veiligheidsmarkt, bedrijven nodig hebben om risicodragend te investeren in innovatie. Die ruimte moet dan wel gezocht, gebruikt en bestuurlijk en politiek gerechtvaardigd worden. De nieuwe wet Aanbestedingen Defensie en Veiligheid (ADV) kan hierbij helpen. Deze wet voorziet in een aantal bijzondere aanbestedingsprocedures die het midden houden tussen een compleet 'openbare' aanbesteding en een aanbesteding onder het zogenoemde artikel 346 van het VWEU. De ADV biedt door de gekozen structuur mogelijkheden die onder een gewone aanbesteding niet mogelijk zijn; en is Europa-proof, want gebaseerd op de Rl 2009/81. Het lijkt erop dat het veiligheidsdomein nog niet of nauwelijks op de hoogte is van het bestaan van deze mogelijkheden; hier liggen nog onbenutte kansen.

38 Mariana Mazzucato, hoogleraar economie en innovatie University of Sussex UK, *Het Financieele Dagblad*, 6 februari 2014.

39 Instituut Fysieke Veiligheid, *Bestuurlijke Netwerkkaarten Crisisbeheersing*, 2013 (vijfde druk).

40 Vrij naar het *Network-Enabled Cooperation Maturity Model* van de NAVO.

41 Adviesraad voor wetenschap en technologie, *Waarde creëren uit maatschappelijke uitdagingen*, oktober 2013; Wetenschappelijke Raad voor het Regeringsbeleid, *Naar een lerende economie*, november 2013.

42 *Grand challenges* zijn de grote maatschappelijke uitdagingen, zoals de Europese Unie die definieert en als uitgangspunt neemt voor beleidsprioriteiten, onder meer in het innovatieraamwerkprogramma Horizon 2020. Een veilige maatschappij (*Secure Societies*) is een van deze *grand challlenges*.

43 *Samenvatting innovatiecontract Topsector Thema Maatschappelijke Veiligheid*, mei 2012.

44 *Roadmap HTSM Security*, herziene versie van 31 mei 2013.

45 *Roadmap ICT for the Top Sectors*, 2012.

46 Ministers van Economische Zaken en van Onderwijs, Cultuur en Wetenschap, *Kabinetsreactie WRR-rapport 'Naar een lerende economie'*, 22 februari 2014.

47 FME, TNO, ministerie van Economische Zaken, VNO-NCW en Kamer van Koophandel, *Smart Industry. Dutch industry fit for the future*, april 2014.

48 European Commission Decision C (2013)8631, *Horizon 2020 Work Programme 2014 – 2015. 14. Secure Societies – Protecting Freedom And Security Of Europe And Its Citizens*, 10 December 2013.

49 De meer monodisciplinaire vraagstukken zijn buiten beschouwing gelaten, zie ook het toetsingskader.

50 Merk op dat dit Horizon 2020 slechts een van de vele – maar wel de grootste – regeling is waar mogelijk budget gevonden kan worden. HSD houdt een lijst van financieringsinstrumenten bij en faciliteert in het benutten ervan.

51 Robert-Jan Smits, directeur-generaal Onderzoek en Innovatie, Europese Commissie (Kansen voor NL in eerste calls Horizon 2020, 11 december 2013, rijksoverheid.nl).

52 Laetitia Griffith, voorzitter Nederlandse Veiligheidsbranche in een schriftelijke reactie op de NIAV, 1 oktober 2014.

53 Ida Haisma, Executive Director HSD, 28 oktober 2015.

Colofon
Nationale Innovatieagenda Veiligheid 2015

Uitgave van
The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
T +31 (0)70 3028180
info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL

Projectmanagement en auteurs
Peter Elias
Frank Bekkers

Ontwerp
Studio Koelewijn Brüggenwirth

Druk
Ando Graphic

Fotografie
Hilbert Krane
Nationale Politie
Aerialtronics
Third

Met dank aan alle personen die betrokken zijn bij de totstandkoming van deze agenda, in het bijzonder aan Nathalie Zeerleder voor haar administratieve ondersteuning.