TNO Integrale Veiligheid
Kampweg 5
3769 DE Soesterberg
Postbus 23
3769 ZG Soesterberg

www.tno.nl

T +31 88 866 15 00
F +31 34 635 39 77
infodesk@tno.nl

TNO-rapport

TNO 2012 R10591

Thema Integrale Veiligheid Vraaggestuurd Programma 2012-2014 VP Security Bijstelling 2013

Datum	september 2012
Auteur(s)	Dr.ir. J.A. Don Regievoerend departementMinisterie van Economische zaken, Landbouw en Innovatie
Regievoerend departement	Ministerie van Economische zaken, Landbouw en Innovatie
Projectnummer	053.01011/01.02
Aantal pagina's	32 (incl. bijlagen)

Authorisatie door drs. H.G. Geveke, directeur TNO Thema Integrale Veiligheid:

Handtekening:

Inhoudsopgave

Samenvatting

In het kader van het nieuwe innovatiebeleid van de overheid is voor de topsector *High Tech Systems & Materials* een roadmap Security opgesteld. Deze roadmap wordt gedragen door een breed consortium van bedrijven, overheden, TNO, NLR en STW/NWO (zie www.htsm.nl).

Het voorliggende VP Security bevat de vertaling van de roadmap naar een plan voor verkennend onderzoek bij TNO, dat aansluit bij de ambities van de partijen die een intentieverklaring tot deelname in de roadmap Security hebben ondertekend. Dit VP omvat een aantal lopende projecten met financiële ondersteuning vanuit nationale en internationale innovatiestimuleringsregelingen. Daarnaast is in april 2012 gestart met drie zgn. voorloopprojecten, waarin de samenwerking met partners uit bedrijfsleven, overheid en universiteiten nader ontwikkeld wordt.
Na de recente verduidelijking van de governance voor roadmap-initiatieven vindt nu een verdere concretisering van commitment van partijen plaats.
De drie voorloopprojecten hebben betrekking op:

- Real-time intelligence voor de deelroadmap Systems-of-Systems
- Nieuwe toezichtssystemen voor de deelroadmap Passieve sensoren
- Cybersecurity voor de deelroadmap Cybersecurity

Bij de uitvoering van deze drie projecten blijkt een fors deel van de deelnemende bedrijven hun nek uit te steken voor het ontwikkelen van gezamenlijke innovatietrajecten en daarbij ook committment voor eigen investeringen (in-kind èn cash) te willen bevestigen. Kritische succesfactor is het perspectief op betrokkenheid van launching customers bij de publieke en private sector. Aan de publieke kant is het wel gelukt om inhoudelijke betrokkenheid te creëren, maar de verankering van innovatie in de overheidsorganisaties vraagt verder initiatief.

Voor 1 november 2012 wordt de roadmap voor de periode 2013-2017 geactualiseerd en wordt deze bijstelling van het VP-plan in projectplannen voor 2013 uitgewerkt.
Op basis van de eerste resultaten in 2012 wordt voor 2013 een doorzetten en focussering van de voorloopprojecten voorzien. Bijstelling van de inhoud op basis van voortschrijdend inzicht en besluitvorming in het roadmapteam Security wordt echter nadrukkelijk opengehouden. Daarbij zal ook de daadwerkelijke bereidheid van partners om te investeren meewegen.

1. Inleiding thema Integrale Veiligheid

1.1 Het Strategisch Plan 2011-2014 van TNO

De TNO-wet 2005 positioneert TNO als een zelfstandige en onafhankelijke organisatie, met als doelstelling het dienstbaar maken van toegepast onderzoek aan algemeen belang en daarbinnen te onderscheiden deelbelangen (artikel 4). De middelen die de wet noemt om deze doelstelling te bereiken zijn (a) het zelf verrichten van onderzoek, (b) het overdragen van resultaten, (c) de samenwerking met andere onderzoeksinstellingen, (d) bijdragen aan de coördinatie van onderzoek en internationale samenwerking en (e) het uitvoeren van opgedragen werkzaamheden (artikel 5).

De wet noemt een Strategisch Plan dat TNO eens in de vier jaar moet maken (artikel 19), rekening houdend met het overheidsbeleid ter zake. Dit plan geeft een uitwerking van de algemene doelstelling op (middel)lange termijn en de voorwaarden die daartoe vervuld moeten worden. Eén van die voorwaarden is het uitvoeren van een Meerjarenprogramma.

Jaarlijks wordt daartoe aan TNO van rijkswege een subsidie verstrekt, waarbij nadere regels omtrent de aanvrage kunnen worden bepaald (artikel 21). Als zodanig functioneert de Procedurebeschrijving Overheidsfinanciering TNO (1996). Deze Procedurebeschrijving spreekt over op te stellen en goed te keuren vierjaarlijkse MeerJarenProgramma's, gebaseerd op de hoofdlijnen uit het Strategisch Plan.

De hoofdlijnen van het Strategisch Plan 2011-2014 van TNO zijn de volgende zeven thema's:

- Gezond Leven
- Industriële Innovatie
- **Integrale Veiligheid**
- Energie
- Mobiliteit
- Gebouwde Omgeving
- Informatie Maatschappij

1.2 Beschrijving van het TNO-thema Integrale Veiligheid

Binnen TNO is het Thema Integrale Veiligheid gericht op een veiliger samenleving. Veiligheid èn het gevoel van veiligheid zijn meer dan ooit onderhevig aan bedreigingen die voortkomen uit de verdeling van welvaart, botsende opvattingen en toenemende schaarste aan grondstoffen. Wereldwijd zetten defensie, overheden, hulpdiensten en industrie zich in om ons te beschermen tegen steeds minder eenduidige en zichtbare bedreigingen. TNO ondersteunt innovaties om deze activiteiten slimmer, efficiënter en beter beschermd te doen.

Binnen het Thema Integrale Veiligheid heeft TNO twee innovatiegebieden gevormd:

1. Defence Research
Defensie staat voor de uitdaging om een duurzaam, dynamisch evenwicht te vinden tussen de ambitie, capaciteiten en beschikbare financiële middelen. Binnen dit innovatiegebied focust TNO op vier samenhangende onderwerpen c.q. business lines om Defensie bij deze uitdaging te helpen:

- Military Operations
- Military Information Superiority
- Force Protection
- Human Effectiveness

2. Safety and Security Research
Veiligheid heeft zich ontwikkeld van een verzameling ad-hoc reacties op incidenten tot een samenhangend complex van maatregelen en effecten.
De potentiële impact en het domino-effect van incidenten, maar ook de maatschappelijke kosten/baten van veiligheidsmaatregelen vereisen een integrale op risico en effect gebaseerde aanpak en regie. Perceptie en acceptatie spelen een grote rol in de keuze van oplossingen.
TNO gaat deze uitdagingen aan door te focussen op de volgende onderwerpen c.q. business lines:

- Security and Protection
- Resilience and Society

1.3 Vraaggestuurd onderzoek in de strategieperiode 2011-2014 voor het Thema Integrale Veiligheid

Voor de ontwikkeling van de strategie en de programmering van het Vraaggestuurde onderzoek voor het Innovatiegebied Defence Research vindt de afstemming tussen de overheid en TNO plaats onder regie van het Ministerie van Defensie. Hiervoor zijn strikte procesafspraken voor het jaarlijks bijstellen en vernieuwen van de portfolio van meerjarenprogramma's.

Met ingang van 2012 zijn er twee Vraaggestuurde Programma's (VP's) die primair aan het Innovatiegebied Safety and Security Research verbonden zijn:

- Het VP Veilige Maatschappij;
- Het VP Security.

Voor de ontwikkeling van de strategie en de programmering van het VP Veilige Maatschappij vindt de afstemming tussen de overheid en TNO plaats onder regie van het Ministerie van Veiligheid en Justitie (VenJ) en in nauwe samenspraak met stakeholders uit de diverse overheidsgeledingen.

In nauwe interactie met de departementen VenJ, Defensie en EL&I en het bedrijfsleven is in de tweede helft van 2011 binnen de Topsector High Tech Systems & Materials een Roadmap Security opgesteld (zie bijlage A). Het VP Security is de vertaling van deze roadmap naar TNO-onderzoeksprojecten. Bij alle projecten in het VP Security zijn bedrijven en/of veiligheidsorganisaties van de overheid betrokken met in-kind- en/of cash- commitment.

1.4 Aansturing van VP Security vanuit Roadmapteam Security

Het VP Security wordt begeleid door het door de topsector benoemde roadmapteam Security, bestaande uit Thales als industrieel boegbeeld, VenJ, Defensie, NLR, STW/NWO en TNO. Het Roadmapteam heeft hieraan als leden toegevoegd: NIDV, Gemeente Den Haag en zal ook een MKB'er benaderen om het team aan te vullen. Het ministerie EL&I heeft een eigen vertegenwoordiger aan het Roadmapteam toegevoegd.

In 2012 wordt in het kader van de topsectoren-ontwikkeling de samenwerking van bedrijfsleven met GTI's, universiteiten en overheden verder vormgegeven en geïntensiveerd. Zo neemt het team voor de roadmap Security initiatief tot:

- Concretisering van ambities voor via NWO en STW uit te zetten onderzoek.
- Structurele verbindingen met de publieke veiligheids-organisaties als Nationale Politie, Brandweer, Veiligheidsregio's en KMar.
- Publiek-private samenwerkingsinitiatieven voor innovatie en implementatie van vernieuwingen op de deelterreinen.

In de periode 1 september - 1 november 2012 wordt de Roadmap Security geactualiseerd en het onderzoeksprogramma voor 2013-2017 geconcretiseerd. Dit zal ook de basis zijn voor een uitwerking op projectniveau van het TNO-VP Security voor 2013. De in 2012 opgestarte projecten zullen ook in 2013 doorlopen gezien de inmiddels gerealiseerde voortgang bij het ontwikkelen van het commitment van partijen uit bedrijfsleven en overheid.

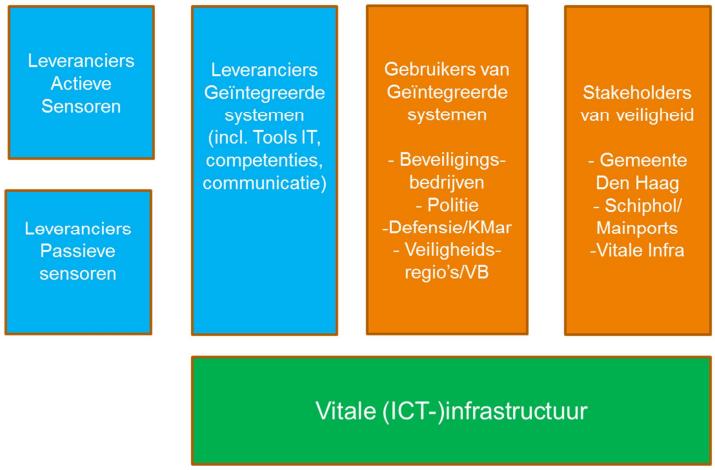
2. Vraaggestuurd Programma Security

2.1 Beoogde Impact en Doelgroep

De ontwikkelingen in het VP Security zijn gericht op de volgende impact:

1. Versterken van de concurrentiekracht van het Nederlandse bedrijfsleven met betrekking tot systemen, IT-producten en sensoren en voor veiligheid;
2. Effectiever/efficiënter optreden van publieke en private veiligheidsorganisaties door innovatie van informatievoorziening, meldkamers, besluitvorming, doctrines, materieel, uitrusting en competenties;
3. Vergroten van veiligheid in verschillende maatschappelijke sectoren (waaronder de vitale infrastructuur en de topsectoren Logistiek en Water) en een beter kunnen afwegen van de maatschappelijke en economische effecten van risico beperkende maatregelen;
4. Verbetering van de resilience van de maatschappij tegen cyberrisico's en van de bestrijding van de cybermisdaad.

Waardeketen voor Roadmap Security



In het kader van de roadmap is het versterken van innovatie-initiatieven door de samenwerking in bovenstaande waardeketen voor veiligheid een kerndoel. Dit betreft zowel gezamenlijke projecten als infrastructuur voor validatie van nieuwe opties en launching customership. In het VP Security wordt dit ook integraal aandacht gegeven om de doorlooptijd van innovatietrajecten te verkorten en de kans op implementatie te vergroten. De gouden driehoek van bedrijfsleven, overheid en kennisinstellingen heeft in de security-sector bijzondere betekenis doordat de overheid niet alleen een beleidsbetrokkenheid heeft maar ook uitvoerende taken in bedrijfsmatig gerunde organisaties.

Van bijzonder belang voor het participerende bedrijfsleven is het optimaal gebruik maken van de kennis die internationaal ontwikkeld wordt en aansluiting op internationaal in ontwikkeling zijnde praktijk van veiligheidsorganisaties. Interoperabiliteit en standaardisatie zijn ook in het Europese kaderprogramma belangrijke aspecten. Vanuit de stakeholders van de Roadmap Security zullen initiatieven genomen worden om dit te versterken. De al bestaande sterke deelname van TNO in de Europese arena is hier een goede uitvalsbasis.

2.2 Focus van de inhoud van het VP Security

2.2.1 Aansluiting op lopende VP's bij TNO

De vier onderdelen van het VP Security sluiten alle aan op onderdelen van al lopende Vraaggestuurde Programma's bij het TNO-thema Integrale Veiligheid. In onderstaande tabel wordt dit verder gespecificeerd:

Deelroadmap Securityl	**Topic VP Veilige Maatschappij**	**Mogelijk aansluitende Defensieprogramma's**
1. Systems of systems	Topic 4. Delen en benutten informatie-stromen voor het samen uitvoeren van veiligheidstaken	• V923 UGV's krijgsmacht • V932 Onderwatersystemen en dreiging • V1206 MCM operaties met AUV's • C1210 Gecoördineerde inzet onderwatersensoren • V1216 Superieure SA
2. Cybersecurity	Topic 5. Cybersecurity	• V1126 Integraal beheer • V1232 Cyberdefence
3a Actieve sensoren	-	• V1105 Multifunctie radar • V1114 Maritime SA
3b Passieve sensoren	Topic 1. Herkennen afwijkend gedrag	• V920 Geïntegreerde ISR • V922 Explosievenbestrijding • V934 Vraaggestuurde beeldvorming in sensornetwerken • V935 Grondwaarneming vanuit lucht • V1236 Geïntegreerde EOV

De aansluiting van het VP Security op de topics in het VP Veilige Maatschappij is geborgd, doordat binnen TNO de projectleiders van de projecten in het VP Security en het VP Veilige Maatschappij duo's vormen die aangestuurd worden door de TNO-programma-manager die voor beide programma's gelijk is.
De aansluiting op de defensieprogramma's moet in de tweede helft van 2012 verder uitgewerkt worden; hierbij geldt ook de strikte confidentialiteit voor Defensie als een randvoorwaarde.

2.2.2 Lopende projecten met verplichtingen voor 2013

Zoals in het Plan 2012 voor het VP Security is gespecificeerd zijn er voor alle vier de onderdelen van de roadmap al projecten in uitvoering met participatie van andere Nederlandse partijen. Het betreft:

- Het project STARS met een nationaal consortium, dat uit FES financieel gesteund wordt.
- Projecten met nationale consortia, die uit de middelen van de Maatschappelijke Innovatie Agenda-Veiligheid gesteund worden.
- Projecten met internationale consortia, die uit het EU-kaderprogramma financieel gesteund worden.
- Project Competentie-profiler, die door Nederlandse bedrijven gecofinancierd worden in het kader van de TNO-cofinancieringsregeling.

Het totale budget van deze projecten is in de orde van 150 M€, waarbij ruim 10 M€ bestemd is voor uitvoering van onderzoek door TNO. In 2013 gaat het om een budget van ca. 4 M€ voor TNO, waarbij TNO zelf een bedrag van ruim 1,5 M€ investeert uit zogenaamde SMO-middelen (SMO= Samenwerkings Middelen Onderzoek). De SMO-middelen zijn een samenvoeging van de voormalige EL&I-cofinancieringsmiddelen en de Kennis-als-Vermogen-middelen. Als rand-voorwaarde geldt voor de SMO-middelen van TNO dat er matchende investeringen door publieke en private partijen met een omvang van 40% van het budget plaatsvinden. Parallel aan de opstelling van de projectplannen voor 2013 zal een planning van de benodigde middelen voor matchende projecten worden opgesteld en aan het Roadmapteam worden voorgelegd.

Het portfolio van lopende projecten vormt een substantiële basis voor uitbouw van het VP Security.

2.2.3 Ontwikkeling projectenportfolio voor 2013

Het totale TNO-budget voor het VP Security in 2013 is 2,7 M€. Naast de verplichtingen in lopende projecten is er nog een vrij budget van ca. 1,1 M€ voor 2013. Dit budget wordt gealloceerd voor de projecten van TNO in de deelroadmaps Systems-of-Systems, Cybersecurity en Passieve sensoren.

Voor elk van deze drie deelroadmaps zijn de meest betrokken bedrijven in januari/februari 2012 gevraagd naar specificatie van hun ambities voor nieuwe samenwerkingsprojecten in het kader van de roadmap en een indicatie van daarbij horende in-kind- of cash-bijdragen. Uit deze bilaterale contacten zijn door TNO in overleg met het Roadmapteam kennisinvesteringsplannen (zgn. KIP's) voor 2012 opgesteld. Daarbij is zo goed mogelijk rekening gehouden met de kansen op toepassing bij de uitvoerende veiligheidsorganisaties; ook is rekening gehouden

met de door TNO geambieerde sterktes qua expertise. Na goedkeuring van deze plannen in de vergadering van het roadmapteam op 20 maart 2012, is de uitvoering in april gestart.

Op 9 mei heeft NIDV in samenwerking met TNO een bijeenkomst voor alle roadmapdeelnemers uit het bedrijfsleven georganiseerd. Het ministerie van VenJ is gevraagd een bijeenkomst te organiseren voor potentieel geïnteresseerde behoeftestellers uit veiligheidsorganisaties van de overheid.

In onderstaande sub paragrafen wordt voor elk van de drie deelroadmaps ingegaan op de ambitie, de eerste resultaten in 2012 en de nu voorziene zwaartepunten in 2013.

2.2.3.1 Deelroadmap Systems of systems

A. Doelstelling TNO-VP-project voor de deelroadmap System-of-Systems:

High Reliability Organisaties belast met de uitvoering van veiligheidstaken, zoals politie, veiligheidsregio's en het meldkamerdomein, staan voor de uitdaging om meer veiligheid te leveren in een toenemend complexe maatschappij. In tijden waarin er eerder minder dan meer geld beschikbaar is voor hun taken, betekent dat ook: met minder mensen zullen we dus onontkoombaar meer moeten doen.

In antwoord op deze maatschappelijke uitdaging, zien we de rol van informatiesturing toenemen binnen de veiligheidsketen. Informatiesturing binnen bijvoorbeeld politie, brandweer en GHOR in het veiligheidsveld, maar vooral ook in de samenwerking tussen de partijen. In een netcentrisch samenspel, dat je als een systeem van deelsystemen kunt beschouwen: een System-of-Systems. Niet alleen 'traditionele' systemen maken deel uit van het System-of-Systems. Want veiligheid is al lang niet alleen meer iets van de fysieke wereld. Ook de virtuele wereld van internet en social media speelt een steeds belangrijker rol.

Afbakening op Real Time Intelligence:
Onder de noemer 'Real Time Intelligence' zijn Politie, maar ook andere spelers uit de veiligheidsketen informatiesturing gestalte aan het geven in het meldkamerdomein. Door informatie te combineren met kennis, wordt voorspellend vermogen verkregen, zodat betere besluiten kunnen worden genomen. Naast organisatorische veranderingen gaat de interesse uit naar het slim combineren van data uit verschillende open en gesloten bronnen. Dat kan sensordata zijn in de vorm van bijvoorbeeld videofeeds, maar ook locatiegegevens van telefoons, informatie uit basisadministraties, of bronnen als websites en Twitter. In het real time combineren van deze bronnen schuilt de kracht met als beoogd resultaat: 'first time right'.

Dat betekent concreet bijvoorbeeld dat bij een brand de juiste blusmiddelen tijdig beschikbaar zijn, dat bij een overval de meest waarschijnlijke vluchtroutes zijn afgezet en dat surveillerende politiemensen precies weten wat er waar speelt. De heterdaadkracht is hoger, Particuliere Alarm Centrales vormen een vast onderdeel binnen het totale veiligheidssysteem, etc. 'First time right' maakt het veiligheidsoptreden goedkoper en effectiever.

Doelstelling TNO-project Real Time Intelligence:
Het is de doelstelling van het TNO-project Real Time Intelligence binnen de deelroadmap System-of-Systems om door middel van action research sámen met bedrijfsleven en veiligheidspartners grenzen te verkennen van technologie, organisatie, processen en gedrag. Om in gezamenlijke ontwikkelprojecten nieuwe concepten te ontwikkelen en te beproeven om de Real Time Intelligence functie te versterken.
TNO zet haar kennis, ervaring en resources graag in om bij te dragen aan beter functionerende RTIC-eenheden binnen de politie en andere veiligheidspartners enerzijds, en economische kansen voor de deelnemende bedrijven in de vorm van nieuwe of verbeterde producten en diensten anderzijds.

B. Eerste resultaten van het TNO-project Real Time Intelligence in 2012

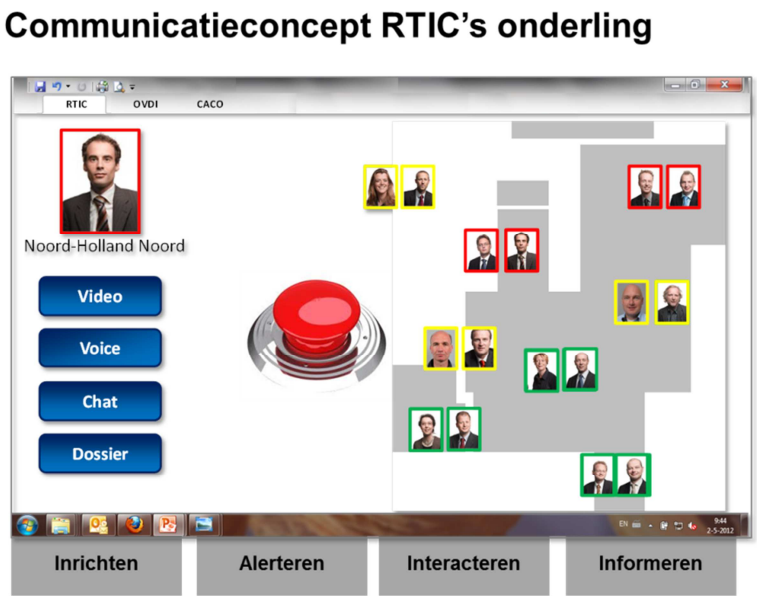
In de afgelopen maanden is hard gewerkt aan het leggen van contacten en aan het verkennen van mogelijkheden voor samenwerking met zowel bedrijfsleven als met het veiligheidsveld (met name Veiligheidsregio's en Politie). In kader van deze oriëntatiefase is een tweetal geconcentreerde ontwikkelinspanningen (zgn 'Challenges') uitgevoerd voor politie Noord-Holland Noord en voor het Korps Landelijke Politiediensten (KLPD).

De eerste Challenge leverde een oriëntatie op het thema RTIC op. Het TNO-team leverde op grote lijnen een ontwikkelroadmap op van de Real Time Intelligence Centra van de Nationale Politie-in-wording.

ROADMAP RTIC

	plateau 1	plateau 2	plateau 3
PROCES	**kort cyclisch** vraag	**lang cyclisch** aanbod	**integratie** evenwicht
ORGANISATIE	**inbedding rollen** bewust onbekwaam	**ontwikkeling kennisniveau** bewust bekwaam	**ontwikkelen vakmanschap** onbewust bekwaam
TECHNIEK	**informatie ontsluiting en registratie** informatie	**signalering en info integratie** kennis	**visualisatie adviseren** intelligence

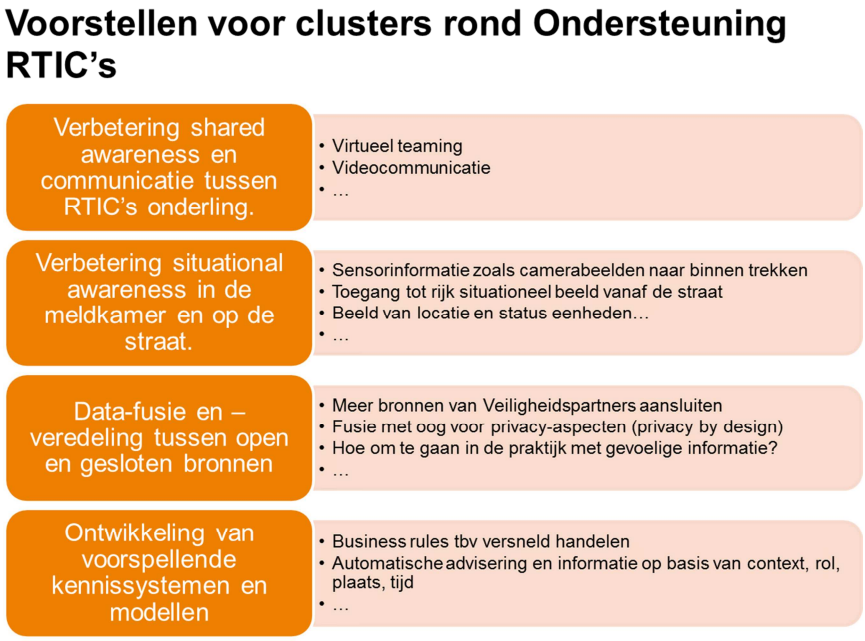
De tweede Challenge voor de KLPD leverde een concept op voor communicatie tussen RTIC's-onderling, en voor expert-raadpleging. Deze Challenge werd door TNO uitgevoerd samen met het D-CIS lab van Thales.



Op 10 september 2012 staat een werksessie gepland waarbij het aanbiedersveld zal worden uitgenodigd samen met het veld van eindgebruikers (met name politie en veiligheidsregio's) met als doel vraagarticulatie en clustervorming rond nieuwe initiatieven. Nieuwe initiatieven waarbij innovatieve (combinaties van) producten en diensten in de praktijk worden toegepast en geëvalueerd, en waar TNO graag een bijdrage aan levert in de vorm van onderzoek en ontwikkeling. Deze werksessie is bepalend voor hoe het vervolg van het huidige project Real Time Intelligence vorm zal krijgen in 2013.

Clusters die op 10 september zullen worden voorgesteld zijn:

- *Verbetering shared awareness en communicatie tussen RTIC's onderling*: hoe creëren we een virtueel team van de enkele RTIC'ers in de verschillende landelijke meldkamers, zodat snel opgeschaald kan worden, mensen elkaar goed begrijpen en informatie effectief gedeeld wordt?
- *Verbetering situational awareness in de meldkamer en delen hiervan met eenheden op de grond*. Hoe krijgt een meldkamer een beter beeld van de situatie ter plekke door bijvoorbeeld camerabeelden snel ter beschikking te hebben en deze beelden ook te kunnen delen met grondeenheden? Maar ook: hoe kunnen eenheden in het veld ook makkelijk informatie toevoegen?
- *Data-fusie en –veredeling tussen open en gesloten bronnen*: Hoe kunnen relevante bronnen van Veiligheidspartners zoals de GBA, Sociale Dienst, Jeugdzorg effectief worden ontsloten om tot waardevolle inzichten te komen. Maar wel op een privacy vriendelijke wijze, met waarborgen voor de rechtsgang.
- *Ontwikkeling van voorspellende kennissystemen en modellen:* Welke kennis uit de intelligence organisatie en welke tacit knowledge van operators van de meldkamer en RTIC's kunnen worden gevangen in 'business rules' en voorspellende modellen ten behoeve van het versnellen van het handelen van een RTIC?



C. Zwaartepunten voor 2013

In afwachting van de bewuste werksessie van 10 september wordt verwacht op tenminste een, maximaal drie van deze onderwerpen een cluster te kunnen vormen in de vorm van een samenwerking met een of meerdere bedrijven en een politie-eenheid / Veiligheidsregio. Met als meest waarschijnlijke partijen aan de vraagkant:

- CO24 (Veiligheidsregio Twente)
- KLPD
- Politie Haaglanden

En vanuit het aanbiedersveld:

- AGT
- Centric
- Thales
- Sentient
- HP

2.2.3.2 Deelroadmap Cybersecurity

Uit de inventarisatie van de ambities van de bedrijven die een intentieverklaring met belangstelling voor Cybersecurity hebben ondertekend, volgt grote belangstelling voor het gezamenlijk opzetten van innovaties voor het ontwerpen van veilige ICT infrastructuur en het adequaat detecteren van ICT-misbruik.

De snelle veranderingen in technologie, de toenemende verwevenheid van op ICT gebaseerde infrastructuren, de snelle introductie van nieuwe gebruiksmogelijkheden en de incoherentie van beschermingsmaatregelen over (ketens van) organisaties heen, zorgen voor nieuwe dreigingen en kwetsbaarheden. Een goede beheersing vereist steeds opnieuw risico-afwegingen en innovatieve maatregelen.
Aangezien voorkomen van incidenten beter is dan genezen, is het wenselijk om al in het ontwerpstadium van ICT-infrastructuur en grootschalige op ICT-gebaseerde

infrastructuur rekening te houden met bescherming (*security by design*). Hierbij richt het onderzoek zich op het opzetten van een referentiekader om risicofactoren van nieuwe technologie snel te kunnen inschatten en op het uitvoeren van technologiescans naar nieuwe ICT-ontwikkelingen. Voor de ontwikkeling van het referentiekader wordt gebruik gemaakt van een case studie naar een infrastructuur waarin grootschalige ontwikkelingen in de ICT-toepassingen gepland staan. Voor de case studie is gekozen voor de smart grid ontwikkelingen in de energiesector, aangezien de ICT-ontwikkelingen daar sterke consequenties hebben in de besturingsmogelijkheden en maatschappelijke impact hebben voor de gebruikers.

Effectieve bescherming tegen een ongewenste verstoring bestaat in het algemeen uit een evenwichtige verzameling maatregelen op het gebied van pro-actie, preventie, preparatie, detectie en respons. Een belangrijke pijler binnen het onderwerp cyber security wordt gevormd door detectie van ICT-misbruik en bijbehorende mogelijkheden voor opsporing en vervolging. Voor ICT geldt dat zowel de overheid als het bedrijfsleven ieder voor zich maatregelen op dit gebied nemen. Een speciaal aandachtsgebied wordt gevormd door cyber security voor de vitale infrastructuur. De vitale infrastructuur bestaat uit sectoren en voorzieningen waarvan verstoringen of uitval ernstige impact kunnen hebben op de Nederlandse samenleving (en daarbuiten), zoals de energievoorziening, drinkwatervoorziening en de transportsector. Ook deze vitale sectoren zijn in steeds grotere mate afhankelijk van ICT. Op het gebied van monitoring en detectie heeft iedere organisatie hiervoor zijn eigen monitoring tools en –systemen met daarbij eigen specifieke parameter instellingen. Op basis hiervan bouwt men binnen de organisatie zijn eigen situational awareness (SA) op. Op nationaal niveau ontbreekt het nog aan een coherent beeld op de actuele cyberstatus van de Nederlandse vitale infrastructuren. Dit beeld zou het Nationale Cyber Security Centrum versterken in haar taakuitvoering. Hierbij richt de vraag naar nader onderzoek zich niet op de afzonderlijke (vaak commercieel verkrijgbare) detectiesystemen, maar op het opbouwen van een gezamenlijk gedeeld beeld van ICT-misbruik uit een diversiteit aan informatiebronnen, zowel in aantal als type systemen.

A. Doelstelling van het VP-project Cybersecurity Topsectoren HTSM

Het programma kent de volgende doelstellingen over de periode 2012-2014:

1. Het ontwikkelen van roadmaps voor behoud van de digitale veiligheid in een wereld waarin technologische (ICT) oplossingen elkaar snel opvolgen.
2. Het ontwikkelen van tools voor Security-by-Design in de op ICT gebaseerde vitale infrastructuur. Dit werkpakket richt zich op het identificeren van de factoren die de inbedding van bescherming tegen ICT-dreigingen al in het ontwerpstadium van infrastructuur en grootschalige systemen mogelijk maken. Deze onderzoeksvraag wordt onderzocht aan de hand van een smart grid case binnen de energiesector.
3. Het ontwikkelen van methoden en middelen voor het monitoren van de cyber security status van de Nederlandse vitale infrastructuur op een uniforme wijze

Naast deze doelstellingen is het de bedoeling om een Fieldlab te realiseren, waarin verscheidene labs van TNO en producten van verschillende leveranciers worden samengebracht. Hiermee kan toegepast onderzoek worden gedaan naar de

capabilities van bestaande producten en gezamenlijke innovatie worden gedaan op het gebied van nieuwe methodes en technieken en interoperabiliteit.

Deze doelstellingen sluiten nauw aan op de kennisontwikkeling met betrekking tot cybersecurity in het VP Veilige Maatschappij.

B. Eerste resultaten van het TNO-project Cybersecurity in 2012

Het VP project is in juni 2012 gestart. Inmiddels zijn de inhoudelijke lijnen uitgezet (scope) en voorzien van de eerste inhoudelijke activiteiten. Elke activiteit hangt samen met een aantal concrete onderzoeksvragen. Met enkele partijen die in de LOI hebben aangegeven interesse te hebben in het onderwerp cybersecurity is contact gelegd (IBM, HP, Alliander, Fox-IT). Deze contacten worden de komende maanden geïntensiveerd, terwijl tevens met de andere LOI-partners contacten worden gelegd. Uiteindelijk doel is het realiseren van gezamenlijke onderzoeks-activiteiten.

De verwachte resultaten voor 2012 komen in grote lijnen overeen met die in het Projectvoorstel Kennisinvesteringen:
- Bijgewerkte roadmap en trendoverzicht
- Concept referentiekader secure infrastructuur case Smartgrids
- Demonstratie gekoppelde monitoring

In afstemming met private partijen zal nog in 2012 gestart worden met het onderzoek naar:
- Algemeen referentiekader security implicaties van nieuwe ICT
- Concept demonstrator cyberstatus

De ontwikkeling op deze punten loopt door in 2013.

Onderzoeksvragen rond 'Roadmapping'
Deze onderzoeksvragen omvatten onder meer:
- Welke (relevante) ontwikkelingen en onderzoeken vinden er nationaal en internationaal plaats op het gebied van cyber security?
- Welke behoefte is er aan cyber security onderzoek?
- Hoe kunnen deze twee tegen elkaar afgezet worden?
- Welke producten, diensten en oplossingen dienen er ontwikkeld te worden om aan de behoefte te voldoen?
- Hoe kan hierop dan actie genomen worden?

Deze vragen komen voor het bedrijfsleven samen in bestaande processen om de risico's binnen en buiten de eigen scope te beheersen. Het bedrijfsleven onderkent de tekortkomingen van bestaande risicomanagement methodes, die vrijwel altijd gebruik maken van dreigingslijsten aan de hand waarvan het risico wordt ingeschat. Dit gebeurt ook voor de verwachte impact bij het daadwerkelijk optreden van een incident. De combinatie van ingeschatte dreiging en ingeschatte impact leidt tot het wel of niet nemen van maatregelen. De scope van de dreigingslijsten beperkt zich in de regel tot het eigen proces of de eigen organisatie. Per definitie zijn de 'bekende' dreigingen opgenomen en komen nieuwe of onverwachte dreigingen niet aan bod ('zero-days'). Bovendien zijn bestaande dreigingslijsten veelal generiek en lastig te mappen op de betreffende specifieke context. Dit principe werkt niet goed meer in de networked society.

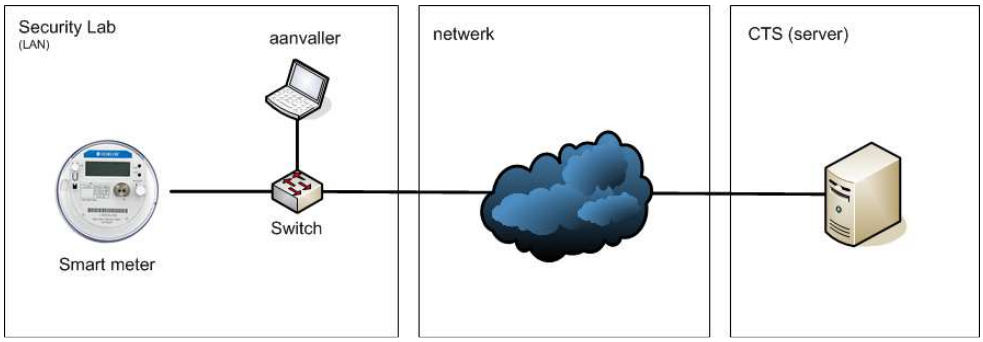
Gestart is met onderzoek naar de kwantificering van cybersecurity om de cybersecurity dreigingen beter inzichtelijk te maken en een verbeterde dreigingslijst op te kunnen stellen. Verder wordt gekeken naar het verplichtingenmodel.
(Beoogde) Partners: Consulting firma's (KPMG, Logica, Ordina), TNO 'El Metodo'

Onderzoeksvragen rond 'Security-by-Design'
Grootschalige ICT-infrastructuren worden nog steeds ontworpen, zonder dat voldoende rekening wordt gehouden met security of bijvoorbeeld privacy. Maatregelen worden nogal eens achteraf worden ingebouwd, tegen hoge kosten of met een onbevredigend resultaat. Voorbeelden zijn de OV-chipkaart, rekeningrijden en het EPD, maar ook het ontwerp van de slimme meter, het inbouwen van onveilige chips in autosleutels en het skimmen van bankpasjes. Security-by-Design gaat niet alleen over het technisch veilig maken van systemen, maar ook om het dusdanig ontwerpen dat de techniek in te bedden is in de overkoepelende governance structuur en mogelijkheden van gebruikers.

Onderzoeksvragen:
- Hoe kwetsbaar is het centrale ICT regelsysteem dat communiceert met de vele slimme meters en de energievoorziening bijstuurt?
- Is de communicatie tussen dit regelsysteem en de slimme meters te compromitteren?
- Welke algemene designprincipes kunnen worden afgeleid uit deze case?

Gestart is met onderzoek naar de security in 'Smartgrids'.
Partners: Alliander, EMCS, mogelijk Siemens.

Figuur 1 geeft een beeld van de testopsteling waarmee de security in (een deel van) het Smartgrid netwerk wordt onderzocht:



Figuur 1 Testopstelling Security-by-Design in Smartgrids

Onderzoeksvragen rond 'Monitoring en Reporting'
Technische monitoring van relatief eenvoudige parameters (IP-poorten, pakketten) is inmiddels prima mogelijk met bestaande monitoringproducten, IDS- en IPS-systemen. Hiermee kunnen vooraf gespecificeerde parameters en 'events' worden gedetecteerd, als ze boven een ingestelde drempel komen. Monitoring van 'cybersecurity' vergt echter een geavanceerder model, dat terugkomt in de volgende onderzoeksvragen:
- Hoe kan bepaald worden of een 'event' afwijkt?
  Deze vraag is uitgezet in het project ASCII (Adaptive Sensors for Cyber

Intrusion Incidents) waarin Dynamic Baselining wordt onderzocht (i.s.m. AMSN)
Partners: IBM, HP, Fox-IT, mogelijk KPN

- Welke technische parameters zijn interessant om te meten? Welke kunnen gecorreleerd worden?
- Is combineren van technische monitoring-informatie met human intelligence mogelijk? Hiervoor kunnen Big Data en slimme mining technieken worden gebruikt
- Is een (geaggregeerde) rapportage mogelijk die een zinvolle indicatie geeft van de 'status van Cybersecurity in Nederland'? Deze rapportage moet inzicht verschaffen en bijsturing mogelijk maken.
- Is het mogelijk om tooling voor SOCs te maken voor benchmarking van SOCs (functioneel en performance)?

Gestarte activiteiten:

- ASCII projectaanvraag is ingediend (AMSN)
- Overeenstemming met IBM voor een onderzoek naar de capabilities van bestaande systemen
- Onderzoek naar slimme mining strategie
- Gesprekken met Rabobank en KPN om tooling te ontwikkelen voor SOC benchmarking
- Gesprekken met andere partijen uit de topsector.

C. Zwaartepunten voor 2013

In 2013 zullen de net opgestarte activiteiten worden uitgebouwd, waarbij aansluiting op de initiatieven om een cyberlab te realiseren prioriteit zal krijgen. Op basis van de roadmapping activteiten en het committment van de partners in de roadmap Security zal een verdere toespitsing van de ontwikkelingen plaatsvinden.

In het nog chaotische veld van initiatieven rond cybersecurity zal in afstemming met NCSC en universiteiten gewerkt worden aan versterking van de samenwerking.

2.2.3.3 Deelroadmap Passieve sensoren

Uit de inventarisatie van de ambities van de bedrijven die een intentieverklaring met belangstelling voor Passieve sensoren hebben ondertekend, volgt grote belangstelling voor het gezamenlijk opzetten van innovaties voor toezichtstaken. Dit onderwerp sluit ook goed aan op de kennisontwikkeling met betrekking tot het herkennen van afwijkend gedrag in het VP Veilige Maatschappij.
Veiligheid staat in Nederland hoog op de politieke en maatschappelijke agenda. De politiek stelt letterlijk dat het “veiliger moet worden op straten, in wijken en de openbare ruimte”. Men wil de straatterreur, overlast, intimidatie, agressie, geweld en criminaliteit daadkrachtig aanpakken. Bovendien moet terrorisme zo veel mogelijk worden voorkomen. Vooral in de voor terroristische aanslagen kwetsbare openbare vervoersector.
Toezicht gaat gepaard met grote investeringen in mensen en middelen. Zowel de overheid als de particuliere beveiligingsbranche als hun toeleveranciers investeren fors in toezicht. Het gevolg is een toename in (cameratoezicht)centrales, professioneel beveiligingspersoneel en medewerkers met extra beveiligingstaken die de veiligheid in de openbare ruimte moeten waarborgen. Verschillende toezichtsituaties stellen echter verschillende eisen aan de mate van toezicht, zoals

de mate van professionalisering, technische ondersteuning, beschikbare informatie of de competenties van de toezichthouders. Het streven is naar *toezicht op maat*: voor elke toezichtsituatie de optimale mix van organisatie, mensen en middelen, techniek, informatiebronnen, werkwijzen en competenties.

A. Doelstelling TNO-VP-project voor de deelroadmap Passieve Sensoren

In 2012 heeft TNO zich voor wat betreft de deelroadmap passieve sensoren geconcentreerd op toezicht ten behoeve van handhaving, beveiliging, bewaking en opsporing.

Verbeterde toezichtconcepten zijn nodig, inclusief de onderbouwing van de bijbehorende design-choices. Het ene toezichtconcept is niet intrinsiek beter dan een ander, dat hangt o.a. af van beschikbaar budget, dreigingsniveau, mate van gevoeligheid van waarop toezicht gehouden wordt, acceptatie van loze alarmen en intrinsieke structuur van het veiligheidsprobleem. Het probleem is om de juiste keuzes te maken in het ontwerp van een toezichtconcept. Niet alleen in de keuze tussen deze vier typen, maar ook in de verdere uitwerking daarvan, inclusief configuratie en componenten. Een van de achterliggende uitdagingen is om maatschappelijk draagvlak voor een toezichtconcept zo groot mogelijk te krijgen.

De belangrijkste hoofdvraag waar in het onderhevige plan inzicht in ontwikkeld moet worden is: welk type toezichtsysteem en in welke configuratie, is het meest geschikt in welke situatie en waarom? Het beantwoorden van deze vraag draagt bij aan het ontwikkelen van de mogelijkheid voor bedrijven om zich te profileren ten opzichte van andere bedrijven, en beter aansluiting te vinden bij hun specifieke klantsegment.

Dit begint met het eens worden over de mogelijkheden in variatie van toezicht-systemen, en in het afbakenen van de relevante situaties. Vervolgens is het nodig om het eens te worden over de terminologie om dit in te beschrijven. Parallel daaraan dient gewerkt te worden aan toezichttypen die nog pril zijn.

B. Eerste resultaten van het TNO-project Passieve Sensoren in 2012

In de eerste helft van 2012 is het contact geïntensiveerd met het bedrijfsleven dat heeft geleid in een door hen uitgesproken afbakening voor Passieve Sensoren op de volgende toepassingsgebieden: bewaken & beveiligen, grootstedelijke veiligheid, crowd management, veiligheid van werknemers met een publieke taak, retail, transport & logistiek en crisis management. Binnen deze toepassingsgebieden zijn “issues” benoemd waarvan de verwachting is dat “passieve sensoren” kunnen bijdragen aan de oplossing daarvan.

Haaks daarop is een inventarisatie gedaan van mogelijke toezichttypen om van ruwe sensordata naar zinvolle informatie (waaronder alarmen) te komen. Hier komen toezichttypen uit zoals (behavioural) profiling (0+0=1), het ringenmodel van bewaken en beveiligen, enkelvoudige alarmen en “bag of signals”.

In de zomer van 2012 heeft TNO een wetenschappelijk paper geschreven over de requirements die gesteld kunnen worden aan een formele taal om over toezicht-scenario’s te redeneren. TNO levert hiermee een bijdrage aan de interoperabiliteit

tussen (de producten en diensten van) bedrijven en hun klanten, die voorwaardelijk is voor de samenwerking zoals het topsectorenbeleid die ambieert.

Tenslotte is in 2012 met name op de toezichttypen *behavioural profiling* en *modus operandi* wetenschappelijk onderzoek verricht ten behoeve van het beter begrijpen van de voor- en nadelen van deze toezichttypen. Dit zal resulteren in minstens twee wetenschappelijke papers.

C. Zwaartepunten voor 2013

Op de kruising van toezichttypen en toepassingsgebieden liggen de kansen. Een scenario voor 2013 is om op kansrijke kruispunten in nauwe samenwerking met het bedrijfsleven kleine projecten te starten (“challenges”). De in-kind bijdrages van bedrijfsleven en andere stakeholders kunnen dan ingezet worden om in een zeer kort tijdsbestek de meerwaarde van een mogelijke oplossing aan te tonen. Waarbij de concrete vraagstelling van een probleemeigenaar vanuit het betreffende toepassingsgebied de uitdaging geeft.

2.2.3.4 Deelroadmap Actieve sensoren

Voor de deelroadmap Actieve sensoren bestaat er al jaren een intensieve samenwerking tussen Defensie, Thales, TNO en TU-Delft. Er is hier sprake van een Gouden driehoek avant la lettre. In het kader van de Roadmap Security zijn voor 2012 naast de lopende defensieprogramma’s, het STARS-project en het DAISY-initiatief geen extra onderzoeksactiviteiten voorzien. Wel worden voor de volgende jaren een contour voor een nieuw Defensieprogramma en een NTP-projectvoorstel uitgewerkt.

A Roadmap Security

1 Societal and economic relevance of security

1.1 The core theme of public security

In the security domain, there are risks of **deliberate** threats to people and society (the so-called security threats) and of **non-intentional** incidents, disasters and crises, such as natural disasters or failure of safety systems, equipment failures, poor design or incompetent use of safety systems (the so-called safety risks). The government has a societal responsibility to prevent risks and to reduce harmful effects by repression and aftercare.

In this *security roadmap* we limit ourselves to the risks to people, goods and society arising from deliberate acts and the dealing with incidents, crises and disasters where the government is responsible for repression, aftercare and - the preparation of - prosecution. The biggest technological challenges are found in this area and this area offers the highest market potential in the sense of international competitiveness for a robust Dutch knowledge infrastructure.

Security covers several policy areas in government. For the Ministry of Security & Justice this involves the physical safety or public order and national (internal) security, including the protection of our vital infrastructure and the prevention and combat of crime, whereas the Ministry of Defence looks after the external (international) security and, at the request of a competent domestic authority, will contribute to internal security as well. Security is a precondition for the functioning and wellbeing of our society. Therefore, the government is not only responsible for the national security policy, but it also operates large organisations for carrying out security interventions.

The private security sector has shown distinct growth the last years, due to privatisation of areas of government responsibility (outside the monopoly on the use of force) and the focus on and transfer towards the personal responsibility of citizens and businesses. Against this background, there is a good prospect for companies in the HTSM sector in the security domain to strengthen their economic activities.

Where security issues in general become more complex and dynamic, this applies even more to the digital domain. Cyber threats are developing super-fast and it is common knowledge that governments, companies and people are insufficiently equipped to deal with these threats.

Given the high degree of fragmentation in the security domain, formation of a platform for coordinating supply and demand between government, vital sectors, companies and research institutes (academic and applied) and the establishment of test and implementation environments are necessary to achieve impact in the security domain. Involving end-users and other parties concerned during the various phases of research, development and innovation processes contributes in a very direct manner to solving public security issues. In addition, it provides a significant spin-off effect to the competitive ability of the Dutch defence and security sector.[1]

Under the title "The Hague Security Delta" the region The Hague focuses on collaboration with other leading security clusters in the regions Twente and Brabant and proactively strengthens and connects the existing collaboration of the international institutions, governments, businesses, and research and education organisations within The Hague region. The Hague has already implemented a facilitating role with respect to the growth of the security sector, for example by putting itself forward as testing ground for innovative security solutions.[2,3]

[1] Growth through security, study report Ernst & Young, commissioned by the Ministry of Economic Affairs, Agriculture & Innovation
[2] The Security sector in the region The Hague and in the Netherlands, final report B&A Consulting B.V., April 2011
[3] Map "The Hague Security Delta"

1.2 The domestic and global market (2012-2020)

Through events like the September 2001 attacks in New York and Washington combined with the rapid introduction of new technologies, the development of the security market is dynamic but also very turbulent. The size of the European market for the security industry, excluding the defence industry, was estimated at approximately €30 billion in 2008.[4] The national market, in this *roadmap* described by the prioritised subjects, has an approximate market size of €1 billion per year, with a related R&D effort of more than €100 million annually.

1.3 Competitiveness of the Dutch industry

The starting point of the present *security roadmap* is the initiative by the government established long ago (in particular by the Ministry of Defence[5] and more recently also by the Ministry of Security and Justice) to create a strong security-related knowledge chain. In that sense, the golden triangle in the area of development and production of technological systems was effectively set up at the beginning of the last century. It has become evident that *launching customership* has been the guiding principle for these ministries for quite some time and in addition to the deployment by their own departments, these ministries also contribute to the export potential (in an economic and international political sense) of the Dutch industry in a *non-level global playing field*.[6] In 2008, the government adopted a broader approach through the establishment of the Maatschappelijke Innovatie Agenda Veiligheid.[7]

In the area of system of systems, an Embedded Systems and ICT technology driven agenda, the Dutch knowledge infrastructure is very well set-up to obtain a solid industry position in this emerging market. Nationally, there are significant opportunities for an emerging industry sector specialising in network centric based crisis management, in the functional connection of public crisis management systems with the crisis management systems of the vital infrastructure, etc. (see the ICT roadmap linking 9 top sectors and the Embedded Systems roadmap). From an international perspective, there is a very promising export potential.

The Dutch knowledge and industry base in the area of cyber security is of a high standard and is developing at an accelerated rate: suitable cyber security solutions have enormous national, but in particular also international market potential. Recent initiatives by the Ministry of Security & Justice and the Ministry of Defence to strengthen this knowledgebase and the national resilience against digital infringements confirm this.

The Netherlands has an excellent and confirmed market position in the global sensor market. Market analyses show significant further potential. In the area of active sensors, the Netherlands holds a top position in the world market, both in terms of knowledge and industry and facilitated by a launching customer of highest international standing, i.e. the Royal Netherlands Navy and is a powerful innovative player in this area. In the accessible markets the Netherlands is world leader in the area of radar and command and control systems in use by first and second tier Navy organisations.

[4] Study on the competitiveness of the European Security Industry, EU Framework contract ENTR/06/054, November 2009

[5] Strategic Knowledge and Innovation Agenda: Ministry of Defence

[6] Defence Industry Agenda, Ministries: DEF (Defence), EL&I (Economic Affairs, Agriculture & Innovation)

[7] Societal Innovation Agenda on Security, Ministries: DEF (Defence), V&J (Security & Justice) and EL&I (Economic Affairs, Agriculture & Innovation)

2 Areas of application and technological challenges

2.1 System of Systems

Solutions for public and social challenges in the security domain require an integrated approach. The challenges for the security domain with respect to this integrated approach are very complex. It must be possible to closely monitor dynamic situations for various purposes: monitoring, taking action in case of (imminent) incidents, crises and investigation. The right people and authorities must have access to the right information at the right time, allowing quick, effective and flexible action. In other words, they must be able to function in chains and networks, using observations and information from many sources[8].

Currently, systems are developed and further developed in an uncoordinated manner[9]. If subsequently systems are not only linked, but also expanded with communication channels to multiple user categories, the effectiveness of the application comes under considerable pressure. The increasing need for communication with and the use of competencies of civilians and companies within the security domain constitutes a complicating factor in this. Besides reconfigurability, intelligent user-specific collective memories are important developments. Furthermore, it is essential that systems of systems are developed with the involvement of the entire value chain: component suppliers, system suppliers, security organisations, public and private security stakeholders.

The methods, techniques and tools required to further develop systems of systems for optimal support of security tasks in chains and networks include sensors, models, augmented reality, ICT, data mining and data fusion, info mining, communication techniques, tools for education and training (e.g., simulation), but in particular also integrated system design and development (see also the HTSM Embedded Systems roadmap). To have various systems function properly together also requires attention to ethical and privacy issues. *Security-by-design*, *data-protection-by-design* and *privacy-by-design* are important issues here.

2.2 Cyber security

Our society is becoming increasingly dependent on ICT. Therefore, the protection of our vital ICT infrastructure is a matter of national security. Due to the ever increasing vulnerabilities and the rapidly changing pernicious threats, cyber security is becoming increasingly important for businesses, vital sectors, the government and individuals.

Combating cybercrime is an explicit focus of the current government. The government has drafted the National Cyber Security Strategy (NCSS) for an integrated approach to cyber security. Overarching objectives are public confidence and resilience of the vital infrastructure. As part of this, the Cyber Security Counsel, consisting of representatives from the government, the corporate sector and science community, was established to advise the government and to provide private parties with solicited an unsolicited advice in the area of digital security. Another important component of the NCSS is the National Cyber Security Research Agenda (NCSRA).[10]

The NCSRA distinguishes the following research topics:

- identity, privacy and trust
- malicious software
- forensics
- data and policy management
- cybercrime and the underground economy
- risk management, economy and legislation
- secure design & engineering

NCSRA distinguishes the need for shorter-term, applied research to quickly identify security problems and solutions, and the need for long-term research as in-depth investment in knowledge in this area

[8] Societal Innovation Agenda on Security: "Operating in Chains and Networks".
[9] Point One: “Phase 2 Multi-Annual Roadmap and Annual Plan 2011”.
[10] National Cyber Security Research Agenda: “Trust and Security for our Digital Life”. http://www.iipvv.nl/IIP-VV-kanaal/IIPVV-Downloads.html

with (embedded) training of more qualified staff with expertise in cyber security being an important spin-off effect.

2.3 Sensors

Effectiveness in guaranteeing security is increasingly determined by the availability and quality of information. This information dominance is seen as the most critical success factor for action in both the public security domain and in the military domain, the security domain at large.

The targeted introduction of innovative sensor technologies and sensor, data, information and communication networks is very important for the optimisation of the chain of observing, analysing, deciding and acting. Sensors, including active sensors, such as radar, and passive sensors, such as acoustic (vector) sensors and (day and night vision) cameras, are essential in this process.

2.3.1Active sensors

As radar is an active sensor, it is pre-eminently suitable for the detection and classification of so-called non-cooperative objects in a large area in all weather conditions. Radar can be deployed in a wide range of applications, such as defence, coast and harbour surveillance, peace and humanitarian missions, the prediction of extreme weather and the control of traffic on land, water and in the air, and is often essential for our security and quality of life. This wide range of applications does not only generate direct economic activities but is generally one of the preconditions for the creation of a climate that stimulates the economy. Market research shows a substantial global market potential of many billions per year with an annual growth of >10%. In the Netherlands relevant economic activities are developed in which Dutch industry positions itself as a serious contender on the global market.

In the years to come the range in which radar operates is to be further enlarged. For instance, to enable the detection and classification of objects that constitute a threat from the higher layers of the atmosphere or space and objects, such as (improvised) miniature UAVs with reflecting characteristics that make them very difficult to distinguish from their natural background. New challenges must be addressed, for instance if radar is to be deployed in an operational environment with a high asymmetrical character to support flexible defence systems or where free propagation is restricted, for instance the observation of the lower airspace or deployment in urban environments. Radars will more and more be at the basis of heterogeneous (i.e., active and passive) sensor suites, among others, for multispectral observation. To respond to a continuously changing world where radars are deployed and to prevent that systems will have to be developed over and over again, research will have to be made into reconfigurable systems that enable the quick and simple change of the system's inherent functionality.

In the period ahead, developments in radar signal processing can be summarized as the step from detection to classification, in which more and more information in the very signal will be used to generate an ever increasing quantity of usable and reliable radar output. In most instances, increasing use of operational and context information will be made and systems will be given a more cognitive and intelligent quality. Examples of enabling technology to attain this are: particle filtering, compressive sensing, use of micro-Doppler, coloured space, etc.

Developments in radar front-ends are strongly dominated by Active Electronic Scanning Antenna (AESA) that is to be deployed in a wide scope of applications during this planning period. AESA developments are strongly related to the European Key Technology and HTSM Roadmap Circuits & Components. This is to yield low profile / thin AESAs that can be easily integrated in a platform or an operational environment. Another path in the AESA roadmap is the reconfigurable antenna array that is to facilitate the multi-domain deployment of one and the same system.

2.3.2 Passive sensors

In the security domain, the Netherlands has distinctive global market- and technology positions in both passive sensors and passive sensor systems. CCD/CMOS day light cameras are used for high resolution (airborne) surveillance. Night vision is enhanced by image intensifiers and/or infrared sensors. Unlike active sensors, passive sensors do not emit energy, making them robust against

electronic warfare. Their relatively low power consumption makes them stepping stones for widely distributed arrays of autonomous sensors (“smart dust”), and candidates for unmanned platforms. Acoustic vector sensors can provide 3D situational awareness, both in air and underwater.

The ongoing increase in gathering information necessitates novel concepts of processing these data. However, privacy of the citizens and the workload related to interpretation of the data collected put serious constraints. The technical solution is to process and interpret data automatically and locally, and to only report relevant data to control rooms. Sensor fusion is a powerful concept in reducing false alert rates by combining data in order to filter out irrelevant information. Relevant technologies are biometrics for identification, sensor fusion and signal processing, especially the currently used modalities video, person-tracking in outdoor and / or crowd-scenarios.[11] The next generation of passive sensors will contain algorithms developed by using the expertise of many professionals. Such intelligent sensors are able to exceed certain capabilities of human observers. For instance Intelligent passive sensors are able to detect the simultaneously occurrence of a number of weak deviations of the “normal” situation, while surveillants are concentrated on strong deviations. Further on, automized intelligent passive sensors enable the direct and reliable detection of certain types of incidents – e.g. a shot of a gun, breaking of a pane of glass, indications for behavior related to dealing of drugs -, while human observers will have difficulty with recognition of incidents they never experienced. On the other hand humans have observation competences which cannot be replaced by instrumented observations. For that reason optimal human-machine interaction and training of professionals in optimal use of the new approaches have to be developed.

This will not be the end of the developments. There are also promising perspectives for self-learning sensors, self-adaptation of sensors, applying autonomously moving clouds of passive sensors, reconfigurable sensors etc. The challenges of applying new generations of intelligent passive sensors is to support professionals on several tasks such as surveillance, maintenance, detection, forensics and incident handling. These tasks involve identification, observation, detection of people or other objects, behavior and behavior patterns that (might) lead to threats and incidents. A special challenge is supporting the collaboration between all the professionals in charge for security in crowded, complex places such as train stations, airports, celebrations, or (inter)national events such as Queensday.

[11] Point. One : Phase 2 Multi-Annual Roadmap and Annual Plan 2011

3 Priorities and programmes

3.1 System of Systems

Given the identified market potential for being the first in the world to realise robust system-of-systems solutions in the area of integrated security (which is confirmed by the enormous efforts in this area within the EU, see the ESRIF agenda and Security contribution in Horizon 2020) it is proposed to implement this topic as a TKI system-of-systems, starting with the parties who to date have contributed to the Point-One security roadmap[12], together with the parties participating in the MIA security programme Operating in Chains and Networks.

3.2 Cyber security

In June 2011 the Cyber Security Council approved the NCSRA and gave “IIP Veilig Verbonden” the task to prepare a specific research programme and to provide a framework for the organisation and financing. This detailed research program has been included in this roadmap. The parties participating in the MIA security program cyber security have been added to that. Given the high degree of urgency, the formation of a TKI cyber security is recommended.

The Hague region has a relatively large knowledge reservoir in this area due to the presence of a number of highly qualified companies and institutions, platforms and government bodies. The international profile linked to knowledge of international law in The Hague offer The Hague the opportunity to become the Cyber Security Capital of Europe.

3.3 Sensors

3.3.1 Active sensors

The Dutch activity aimed at the development and production of radar systems takes place within one of the longest existing golden triangles. Within this triangle, excellent research is carried out and good economic returns are realised. This activity has all the characteristics for the requirements of a TKI. The research within this context is fully linked with similar research programmes of the EU, EDA and national and regional authorities.

3.3.2 Passive sensors

The Societal Innovation Agenda on Security and the Roadmap Imaging Technology Security Domain are initiated by the Ministry of the Interior and Kingdom Relations. The resulting documents identify the needs and desired innovations for the security domain. Besides the various partners of this initiative industry also links up with the trends and necessary developments set out in this roadmap. The priorities have been included in this roadmap.[13]

Sensor fusion, i.e., combining cameras, directional acoustic information, and geo-referencing adds intelligence to applications ranging from urban surveillance to unmanned platforms, Also here, research is linked with EU and nationally supported research programmes. The formation of a TKI in passive sensors is recommended.

[12] Point-One Multi-Annual Roadmap and Annual Plan 2011.

[13] Roadmap Imaging Technology, Drafted in December 2010 by the DSP Group, the Rotterdam Rijnmond Police, Ministry of Foreign Affairs, Ministry of Justice, Royal Netherlands Military Constabulary, Organisation for Police Cooperation, Municipality of Utrecht, Netherlands Forensic Institute and National Coordinator Terrorism & Security.

3.4 Flagship project: Netherlands Security Monitoring & Information Centre

In order to create focus and momentum, the partners in The Hague Security Delta (including the City of The Hague, industry, chamber of commerce, and knowledge institutes) have proposed a large flagship project: the development and creation of the Netherlands Security Monitoring & Information Centre (NSM&IC). The ambition is to find a new optimum for the current largely dispersed and independent first responder dispatch centers and the also widely spread emergence of crisis management centers. Best in class knowledge and technologies will create an internationally distinctive centre that is innovative, optimizes the workflow of all security stakeholders in their day to day first responder tasks as well as their crisis management tasks (GRIP 2-5, in the future enhanced to level 6). The use of novel sensor, ICT and cyber security technologies will be applied in order to find a performance optimum, resulting in an affordable Centre, realizing significant lower life time cost compared to any other solution in use today. NSM&IC will result in international exposure of our industry, thus creating a point of departure for creating an European market position for such a functionality. More details are shown in the Attachment.

The organization of this flagship project and the involvement of all stakeholders requires a new approach to government investments: Launching Customership in a Multiple Final Customer setting. The Hague Security Delta has started the process to develop the business case for NSM&IC.

3.5 Fundamental technology needs

Fundamental technology domains to be maintained nationally as a precondition for the success of the sector include:

- Information & Communication (including cyber)
- Radar (including cyber)
- Micro electronics (including cyber)
- Mechatronics
- Smart Materials
- Embedded software (including cyber)
- Behavioural science
- System (of Systems) Engineering (including cyber)

4 Investments

The financial data in the context of the security roadmap differ significantly from the other roadmaps in the sense that the technology roadmap for security is already existing and functioning for many years, including the (pro) active participation of the government stakeholders, also in the launching customer role. Hence, the advice of the roadmap team is to continue consortia, co operations, actions and investment, as they are committed in national and international R&D programs.

Differentiation and further detailing based on fiscal regulations (RDA+ conditions and related TKI definition are not defined yet) is felt to be inappropriate at this stage.

From the LOI's a clear commitment from all stakeholders can be observed, whereas the following total seems to deliver a good and relevant representation of this commitment:

The total R&D effort of the sector and related to the roadmap Security for the period 2012 -2016 will amount approx. 78 M€ per year.

(LOI) Partners in the creation and in support of the HTSM Security Roadmap.
This overview includes large, medium and small enterprises.

Alliander
AVEQ
Cameramanager
Centric
Centrum voor Innovatie en Veiligheid
Cyber-TEC
Delft Dynamics
Eagle Vision Systems
ENAI
Ericsson
FOX-IT
Gemeente Den Haag
Geodan
HCSS
Hewlett Packard
Irdeto
KvK Den Haag
KLPD/ National High Tech Crime Unit
Microflown Avisa
Ministerie van Defensie
Ministerie van Veiligheid&Justitie
NIDV
NFI
Noldus
Novay
Nationaal Studiecentrum voor Criminaliteit en Rechtshandhaving
Nationale Cyber Security Raad
Nederlandse Vereniging van Banken
Ordina
Photonis
PI-lab (Universiteit van Tilburg)
Relion
Rijksmuseum
Riscure
Security Matters
Sound Intelligence
SSBV
Syntens
Surfnet
Thales Nederland
TNO
Van Goghmuseum
VCS Observation
Vebon
Veiligheidsberaad
Vicar Vision
V-Step
WMC
Wetenschappelijk Onderzoek en Documentatie Centrum Min V&J

Parties not included in this list that are interested in joining may contact the roadmap team for further information.

Roadmap Security 2012

Finance → / ↓ Execution	Company	State /TNO+	State /NWO	State /other	Univ	EC	Further funding
University	1,0		4,4	1,0	4,2	1,6	5,7
TNO+NLR	2,0	3,5		2,1		1,6	15,5
Company	14,0			3,3		1,6	12,5
Int'l R&D	1,0					5,0	
Total M€/yr	18,0	3,5	4,4	6,4	4,2	9,8	33,7

Roadmap Security 2013

Finance → / ↓ Execution	Company	State /TNO+	State /NWO	State /other	Univ	EC	Further funding
University	1,0	-	4,5	1,0	4,2	1,6	5,8
TNO+NLR	2,0	3,6	-	2,1	-	1,6	15,8
Company	14,3	-	-	3,4	-	1,6	12,8
Int'l R&D	1,0	-	-	-	-	5,1	-
Total M€/yr	18,4	3,6	4,5	6,5	4,2	10,0	34,4

Roadmap Security 2014

Finance → / ↓ Execution	Company	State /TNO+	State /NWO	State /other	Univ	EC	Further funding
University	1,0	-	4,6	1,0	4,3	1,6	5,9
TNO+NLR	2,1	3,6	-	2,1	-	1,7	16,1
Company	14,6	-	-	3,4	-	1,7	13,0
Int'l R&D	1,0	-	-	-	-	5,2	-
Total M€/yr	18,7	3,6	4,6	6,6	4,3	10,2	35,1

- **State /other**: nationale subsidies, TTI bijdragen, RDA+, etc. (niet WBSO en RDA)
- **University**: betreft ook vergelijkbare onderzoekscentra, zoals AMOLF en SRON
- **Further funding**: regiobijdragen, overheidstaken (bv defensie), SBIR, etc.

Cash

In-kind

Attachment 1: Flagship Project

Den Haag, 14-12-2011

HTSM boegbeeldproject Security

Netherlands Security Monitoring & Information Centre

NSM&IC

De security roadmap van de topsector High Tech Systems en Materialen (HTSM-Security) benadrukt het belang om focus aan te brengen, momentum te genereren en roadmaps en agenda's van leidende partners in het veiligheidsdomein te combineren. De Security Roadmap onderscheidt zich daarbij met het voortbouwen op programma's binnen de bestaande en zeer actieve gouden driehoek, onder aanvoering van de Ministeries van Veiligheid & Justitie en Defensie.

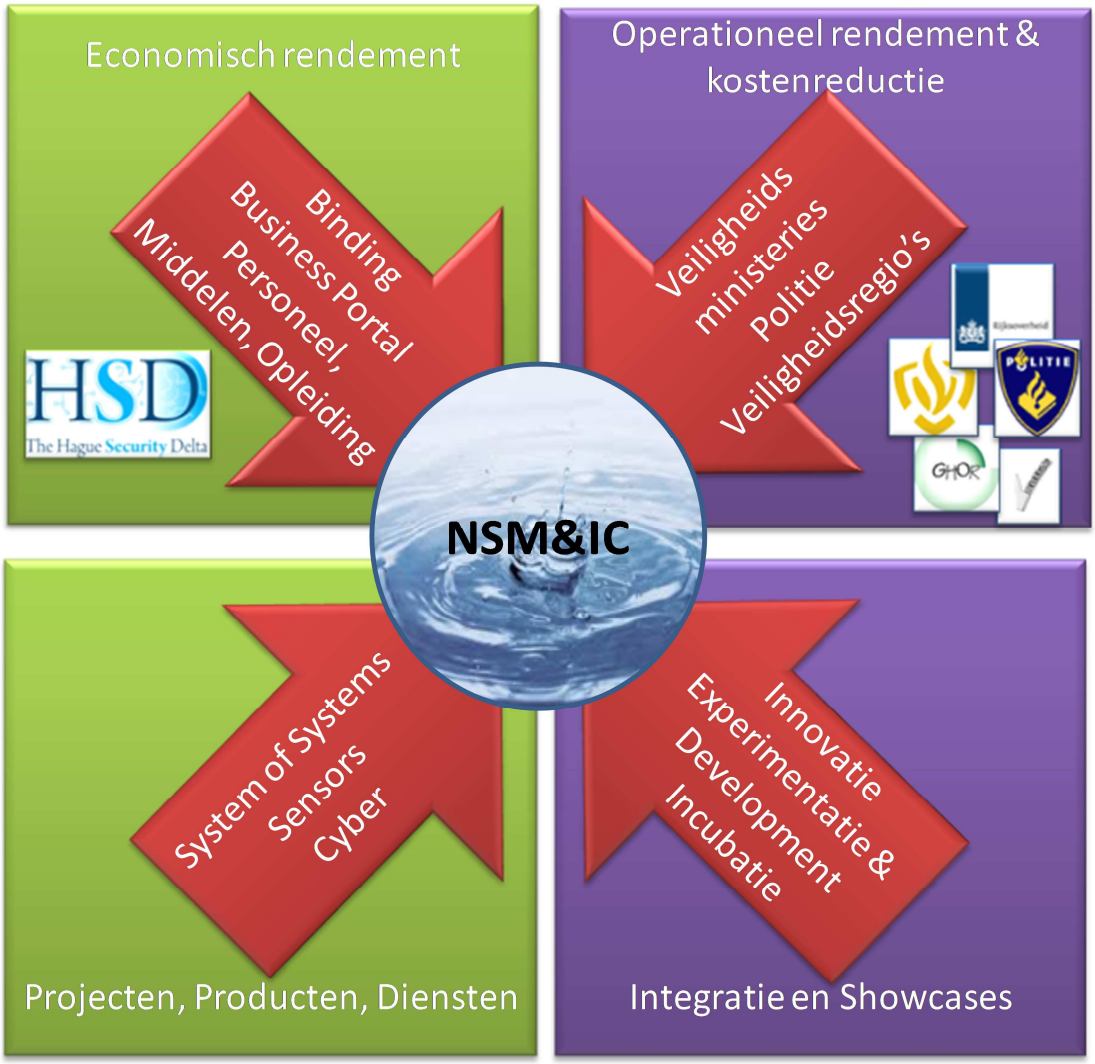
Het veiligheidsveld overziend heeft The Hague Security Delta het initiatief genomen om aan de Security Roadmap een boegbeeld project toe te voegen voor de ontwikkeling en oprichting van een innovatief, internationaal onderscheidend Netherlands Security Monitoring & Information Centre (NSM&IC). In dit innovatiecentrum worden alle roadmaps uit de HTSM-Security samengebracht in een omgeving die garant staat voor kennis en technologie van wereldklasse, waarin op innovatieve wijze activiteiten en inzichten worden geïntegreerd van de belanghebbenden in HTSM-Security , variërend van *first responders tot* crisismanagers. Daarmee worden Gecoördineerde Regionale Incidentbestrijdingsprocedures van niveau 2 tot en met het nog te ontwikkelen niveau 6 (Internationaal) geïntegreerd benaderd (GRIP2-6). Tevens wordt de verzuiling doorbroken.

Dit centrum biedt een nieuwe omgeving waarin toepassingen worden geoptimaliseerd en betaalbare oplossingen beschikbaar komen die tegen lagere levensduurkosten multidisciplinair samenwerken en de effectiviteit verbeteren. Daarmee moet het centrum niet alleen een nationale, maar ook een internationale zichtbaarheid krijgen waardoor op termijn meer onderzoeks- en ontwikkelingsactiviteiten en bedrijvigheid worden aangetrokken

Verder biedt het een incubatieomgeving waarin ook kleine innovatieve partijen, zich makkelijk kunnen aansluiten, diensten en technologische deeloplossingen kunnen ontwikkelen en testen, integreren in het centrum en zo geïntegreerd beschikbaar stellen voor eindgebruikers.

De organisatie van dit programma vraagt nieuwe manieren van omgaan met overheidsinvesteringen, de betrokkenheid van alle belanghebbenden en *lead customership* in een meervoudige eindgebruikers omgeving.

Het NSM&IC stuurt daarmee op operationeel rendement (meer veiligheid, met minder inspanning, slimmer en beter, goedkoper en duurzamer), maar ook op economisch rendement (snellere valorisatie) door nieuwe technologie, diensten en producten in samenhang naar de markt brengen. En als derde het beter nationaal en Internationaal onder de aandacht brengen van de kwalitatief hoogstaande oplossingen die Nederland te bieden heeft.



Figuur 1 HTSM Boegbeeld project NSM&IC als katalysator van veiligheid, innovatie en economie.

Plan van Aanpak

The Hague Security Delta ziet het als haar taak de realisatie van het linker boven kwadrant van figuur 1 verder invulling te geven. Het is van groot belang dat voor de realisatie van deze nationale pilot de belangrijkste belanghebbenden worden betrokken bij zowel de verdere gedachtevorming , de creatie, ontwikkeling en uitrol. Het cluster *The Hague Security Delta* zal daartoe een zorgvuldige procesbegeleiding en gelijktijdig de noodzakelijk inhoudelijke afstemming op zowel politiek-bestuurlijk als op beleidsmatig en operationeel niveau op zich nemen. Het betreft dan zowel eindgebruikers, overheden, bedrijven, kennisinstellingen als alle overige belanghebbenden.

Meer specifiek zal nadere afstemming plaats vinden tussen de bestuurders van de kennisclusters rond Eindhoven, Twente en Den Haag, de grote kennisontwikkelaars, industriële toeleveranciers en zeer belangrijk, operationele centra en diensten.

Met overige partners en belanghebbenden zal worden vastgesteld hoe binnen bestaande institutionele kaders innovatiegelden en voorgenomen verbeter- en investeringsprogramma's verder op elkaar kunnen aansluiten en elkaar kunnen versterken. Het doel is de pilot verder te uitbouwen en aanvullende investeringen in economische en kennisinfrastructuur te aan te trekken. Tevens zal vanuit dit startpunt verder worden gewerkt aan innovatie, *experimentation & development* en incubatie ter versterking van de onderste twee kwadranten van figuur 1.

Tenslotte zal de nationale en internationale zichtbaarheid van het project moeten bijdragen aan kostenreducties en de verbeterde effectiviteit van coördinatie en operaties op veiligheidsgebied. Hiertoe zal actief worden samengewerkt met diensten, ministeries en andere belanghebbenden om de innovaties die worden gerealiseerd ook daadwerkelijk geïmplementeerd raken in de dagdagelijkse werkzaamheden. Daarmee wordt het rechter boven kwadrant van figuur 1 nader uitgewerkt en het launching customership en het maatschappelijk rendement ingevuld.

Coördinatie

The Hague Security Delta biedt aan dit initiatief als onderdeel van de HTSM-Security Roadmap op te willen pakken in nauwe samenspraak met het Topteam HTSM.