



InnovationScan

“Veiligheid in kennis en toepassing”

Inhoudsopgave

Inhoudsopgave.....	2
Samenvatting & conclusies.....	2
Hoofdstuk 1. Algemene bevindingen.....	8
1.1 Doel & Werkwijze van deze InnovationScan.....	8
1.2 Scope “Veiligheid in de private sector”.....	8
1.3 Opvallende uitspraken van geïnterviewden.....	9
Hoofdstuk 2. Kansrijke deelgebieden: de bevindingen.....	12
Inleiding	12
2.1 Network security, Security protocols, Secure mobile communication	16
2.2 E-commerce, e-business, PKI, digitale handtekening, data-privacy, Smartcards	21
2.3 Digital Rights Management, Digital Watermarking, digital copyright, content protection	26
2.4 Tracking & tracing, tagging: Location Based Services	29
2.5 Biometrie	32
2.6 Intelligente camera’s, computervision, beeldverwerking, video&audio-analyse (sensordata-fusie)	35
2.7 Cybercrime.....	39
Hoofdstuk 3. Overige terreinen van Safety & Security	42
Inleiding	42
3.1 Cryptografie	42
3.2 Radartechnologie.....	43
3.3 Fysieke beveiligingssystemen (algemeen).....	44
BIJLAGE I: Lijst betrokken bedrijven, kennisinstellingen, instituten.....	47

Samenvatting & conclusies

Het uitgevoerde onderzoek behelst een verkenning naar de status van R&D-activiteit in Nederland op het gebied van ICT & Veiligheid. De focus hierbij was exclusief gericht op de praktijk binnen de private sector (bedrijfsleven) en de kennisinfrastructuur. Het *doel* van de Verkenning is het identificeren van dié kansrijke veiligheidsthema's voor Nederland, waarop Nederland haar internationale concurrentiepositie kan verstevigen als kennisintensief land of wellicht kan ontwikkelen. De uitkomsten van de Verkenning zijn verkregen middels bedrijfsbezoeken, bezoeken aan kennisinstellingen, telefonische interviews, Internetresearch, het bestuderen van projectplannen en allerhande literatuurstudie.

Conclusies

Op basis van de bevindingen uit het onderzoek zijn de volgende **conclusies** te trekken:

Veiligheid is niet één vastomlijnd toepassingsgebied of een gebied wat volledig omsloten wordt door bepaalde technologiegebieden. Veiligheid is in wezen een kwaliteitsaspect dat vaak inherent besloten ligt in projecten. Veiligheid speelt een cruciale rol binnen een onbegrensde opsomming van sectoren en domeinen zoals transport & logistiek, gezondheidszorg, financiële dienstverlening, embedded systemen etc. In de praktijk worden verschillende ICT-technologieën ingezet om veiligheid te ondersteunen. Voor dit onderzoek is een globale opdeling gemaakt in de *fysieke beveiliging* enerzijds en de (virtuele) *elektronische beveiliging* anderzijds.

Het kennisniveau op het gebied van Veiligheid is hoog in Nederland. Dit wordt onderschreven door het feit dat de TU/e een doctorale opleiding Security én een post-doctorale opleiding Information Security Technology kent, waarbij het leeuwendeel van de studenten uit het buitenland komt. De vraag vanuit het buitenland om Nederlandse beveiligingstechnieken te leren is zeer groot en neemt alleen maar toe. De Veiligheidsomgeving in Nederland is gefragmenteerd. Een gemis is een breed Veiligheidsplatform, een expertisecentrum, met een brugfunctie tussen de industrie en de wetenschap. Er bestaat een kloof tussen de universiteiten en de wetenschap. Er is veel technologie en kennis aanwezig binnen de kennisinstellingen, echter deze bereiken de bedrijven nog onvoldoende. Het is noodzakelijk het bedrijfsleven te laten kennismaken en bewust te maken van wat er mogelijk is aan technologie. De technology-transfer moet leiden tot nieuwe toepassingen, door het bedrijfsleven op te pakken (turning technology into business). Nederland heeft een zeer actieve systeemintegrerende industrie en heeft al een naam in de wereld als innovator en bedenker van concrete toepassingen. De vele entrepreneurs in Nederland triggeren een buitengewone vraag naar concrete Veiligheidstoepassingen.

Winning areas

De onderzoeksbevindingen hebben geresulteerd in de identificatie van de volgende 7 (groepen van) *kansrijke* gebieden voor Nederland betreffende ICT & Veiligheid ("the winning areas"):

1. *Network security, Security protocols, Secure mobile communication*

Kennispositie NL is *zeer goed!* Nederland is traditioneel sterk in formele methoden (verificatie, testen) en ook zeer sterk in systeemcorrectheid (security-protocols). Nederland behoort tot de top in de wereld samen met Frankrijk en UK. In het bedrijfsleven valt CMG op als toonaangevende speler in de mobiele communicatie en Philips met een sterke focus op Ambient Intelligence. Binnen het wetenschappelijke domein is het onderzoek in netwerk security internationaal georiënteerd: Nederlandse kennisinstellingen zijn intensief betrokken bij een aantal spraakmakende Europese projecten. Het CWI is (internationaal) sterk in verificatie van security-protocols; bij de UT beschikt men over de snelste protocol-verifier ter wereld.

Kansrijke toepassingen zijn legio, in tal van marktsectoren: binnen de telecom, de domotica/home-electronics (things-to-things-communication), medical monitoring systems, incidentmanagement, intelligent traffic assistance, etc.

2. *E-commerce, e-business, PKI, digitale handtekening, data-privacy, Smartcards*

Kennispositie NL is *zeer goed!* Veel onderzoek vindt plaats bij banken, echter security in banking is een gesloten wereld.

Er zijn veel bedrijven in Nederland die op eigen initiatief onderzoek doen naar PKI. Johan Enschede/SDU ontwikkelt PKI-software m.b.t. digitale certificaten, zelfs ook voor andere landen in de wereld! Op het gebied van smartcards is er veel R&D (Philips, Chess, AET). Binnen het academische domein is Nederland zeer sterk in programmacorrectheid voor smartcards, en lopen ze voorop samen met Frankrijk en Duitsland. Nederland leidt in smartcard security evaluatie! Vanuit het buitenland wordt vaak een beroep gedaan op TNO-EIB voor onafhankelijke Security-audits. Vanwege de Europese wetgeving wordt voorzien dat deze vraag naar Security-audits sterk zal toenemen. Kansrijke opportuniteiten zijn er zeer veel: identity-management, mobile banking, next-generation e-commerce, e-government (e-dienstverlening naar burgers), health (teleconsulting) etc.

3. *Digital Rights Management, Digital Watermarking, digital copyright, content protection*

Kennispositie NL is *redelijk tot goed*. Philips doet veel onderzoek in DRM en Watermarking, en heeft zelfs samen met Sony dé R&D-trekkersrol in de wereld. Ook andere multinationals beginnen behoorlijk te investeren in DRM-onderzoek (Microsoft investeert nu 500 miljard dollar!).

Content protection wordt langzaam opgepakt door Nederlandse bedrijven die nauwlettend de sporen volgen van grote multinationals (Microsoft, Nokia, Sharp).

In het academische veld is intensief onderzoek gaande, zij het bij een beperkt aantal instellingen. Nederland is sterk op het gebied van digital signal processing en wordt steeds sterker. Er is veel potentie qua toepassingsmogelijkheden, aangezien er zeer veel vraag is naar robuuste watermarking technieken (vooral vanuit het MKB). De filmindustrie (Hollywood) zit gespannen te wachten op dé lang verwachte 100% solide technieken waarmee hun films beschermd kunnen worden tegen kopiëren.

4. *Tracking & tracing: Location Based Services*

Kennispositie NL is *redelijk tot goed*. Nederland is goed in GIS (geographical information systems) en in mobiele communicatie (CMG wereldspeler). Er zijn veel Nederlandse GIS-bedrijven met security-producten, echter in research zijn er beduidend minder.

M.b.t. het vastleggen van de zgn. x/y-coördinaten (cruciaal bij de locatiebepaling) zijn de 3 grootste spelers in de wereld van Nederlandse komaf (NavTech, TeleAtlas, AND).

Bij de universiteiten vindt redelijk wat onderzoek plaats (vooral in spatial modelling).

Er zijn zeer veel kansen in toepassingen: locatiebepaling verscherpen door UMTS, nieuwe radio-tag voor goederen ipv een barcode, etc. Voorspeld is dat Location Based Services in 2005 de meest gebruikte mobiele toepassingen zullen zijn.

5. *Biometrie*

Kennispositie NL is *redelijk*. Nederland profileert zich in de wereld niet zo sterk als biometrie-researcher, maar trekt wel de internationale aandacht als het gaat om biometrie-toepassingen.

Nederland is de proeftuin geweest voor de eerste grootschalige biometrie-pilots in de wereld (Privium-controle bij Schiphol obv irisscan, controle bij nachtclubs obv gezichtsherkenning, etc.).

Nederlandse bedrijven leggen zich veelal toe op het leveren van biometrie-oplossingen, zonder goed op de hoogte te zijn van wat het Nederlandse wetenschappelijke kennisdepot allemaal biedt.

Intensief biometrisch onderzoek vindt plaats binnen een selecte kring van Nederlandse kennisinstellingen (verenigd binnen het Nederlandse Biometrie Forum).

Biometrie is een veelbelovende techniek voor Veiligheid, met zeer kansrijke toepassingen in de gezondheidszorg (medical card), overheid (identiteitskaart), mobile communication, financiële dienstverlening (smartcards), home -security, etc. Nog veel is te doen aan het robuust maken van biometrische technieken.

6. *Intelligente camera's, computervision/beeldverwerking, video/audio-analyse (sensor-datafusie)*

Kennispositie NL is *redelijk*. Er zijn zeer veel installateurs van camera- en toegangscontrolesystemen in Nederland, en slechts een relatief klein aantal R&D-bedrijven (Bosch Security, ASB, etc). Op het gebied van Beeldverwerking/Computervision is binnen de academia veel kennis aanwezig en moet nu de stap gemaakt worden naar toepassingen. De onderzoeksschool ASCI (Advanced School for Computing and Imaging) legt als landelijk samenwerkingsverband tussen universiteiten een zeer stevige basis voor onderzoek in beeldverwerking en patroonherkenning, ook in internationaal opzicht. Opportuniteiten zijn er voor geluidsdetectie (onontgonnen onderzoeksgebied in de wereld), early-warning (agressiedetectie, gedrag van massa's, etc). Veel potentiële marktsectoren zijn te onderkennen: fysieke beveiligingsindustrie, openbaar vervoer, zorg, consumentenelectronica (smarthomes).

7. *Cybercrime*

Kennispositie NL is *matig tot redelijk*. Cybercrime is een groot probleem, niet alleen voor Nederland, maar voor de gehele internationale gemeenschap. Helaas zijn er in Nederland zeer weinig R&D-bedrijven die zich specifiek richten op cybercrime (intrusion-detection). Wel vindt er bij de kennisinstellingen veel onderzoek plaats, weliswaar niet direct gericht op cybercrime, maar meer in het algemeen op networksecurity. Het weren tegen (intrusion)aanvallen van buitenaf behoort ook tot het eisenpakket van networksecurity. De grootste uitdaging in de wereld (dus opportunity) is het introduceren van robuuste preventieve en repressieve applicaties die cybercrime kunnen weerstaan. Vele sectoren zullen er bij gebaat zijn zoals de retail, banking, e-business, industry én de sector van particuliere internetgebruikers.

Programma's en veiligheidsgebieden

Onderstaand wordt een overzicht gegeven van de projecten uit de SenterNovem-programma's BSIK/IOP/CIC (www.senternovem.nl) die een aanknoping hebben met één of meerdere geïdentificeerde *kansrijke* veiligheidsgebieden. De mate waarin een veiligheidsgebied de aandacht krijgt binnen het betreffende project, wordt aangegeven door een '+'.
 ++ = betreffende veiligheidsgebied krijgt sterke primaire focus in project
 + = betreffende veiligheidsgebied is secundair aandachtsgebied in project

<i>Veiligheidsgebieden:</i>	Network security, security protocols ...	E-commerce, e-business, PKI	Digital Rights Management, ...	Tracking & tracing,	Biometrie	Intelligente camera's,	Cybercrime
BSIK	1	2	3	4	5	6	7
Smart Surroundings (Philips, UT, TUD, Thales, TNO, Oce, Nedap, Ericsson oa). Research theme Distributed control.	++				+	+	
Embedded Systems Institute (ESI, ASML, Philips, Oce, TUD, TU/e, UT, TNO oa)	++	+					
Gigaport Next Generation Network (Surfnet, Uva, TNO, Telematica Instituut oa)	++	++	++				+

Freeband Communication (Telematica instituut, Philips, Lucent, Thales, TNO oa). Vision for Freeband for 2010 is to consider communication and information transfer from the perspective of the user, not the provider.	++	++						+
ICIS Interactive Collaborative Information Systems (Thales, TNO, TUD, UvA, UvM, KUN, UT, 4Tec) Research in secure collaborative decision support systems	++						+	
Bricks: Basic Research in Informatics for Creating the knowledge Society (CWI, TUD, TU/e, UT, Siemens, Stelvio oa). Het strategische project 'Security, identification, and authentication'	++	++	++	++	++			+
Virtual Lab e-Science (VU, UvA, TUD, Nikhef) Large-scale distributed systems - program Security	++	+						+
Space for Geo-information (thema Hoogwaardige Ruimte)				++				
MultiMedian. Nieuwe technologieën detecteren en tracking							++	
IOP								
PAW: Privacy in an Ambient World (TUD, UT, KUN, Philips, Microsoft) ontwikkelen architectuur voor de complete beveiliging van gebruikersgegevens	++	++	++					+
BASIS: Biometric Authentication Supporting Invisible Security (UT, TU/e, CWI, Philips, Nedap, Rabobank) transparant maken van biometrische authenticatie, anonimiseren biometrische informatie, systeem aanpassen voor gebruik binnenshuis.	++	++	++		++			
CIC		1	2	3	4	5	6	7
CIM Cybernetisch Incident Management (Almende, CWI, VU, Group4Falck, TUD). Multi-agent technologie voor dynamische, complexe netwerken (incidentmanagement).	++							
DIANA: Data Interception & Analysis (Moniforce, VU, Interpay, Robeco) Real-time analyseren van datastromen om bijv. automatisch creditcardfraudeurs te achterhalen.		++						
CANDELA Content Analysis and Network Delivery Architectures (Bosch Security systems, TU/e, Philips Medical, LogicaCMG) Automatische analyse van (stilstaande) digitale videobeelden (video-bewaking)	+						++	
ICT Breedspoor: Onderzoek naar toepassingen van breedband communicatietechnologie bij bedrijfsprocessen in de Spoorwegbranche – veiligheid in treinen							++	
Residential Gateway (KPN, Philips, TUE, TUD): Onderzoek naar seamless architectuur en QoS aspecten van residential gateway, domotica	+							
Beyond-3G (Ericsson, KPN, TUE, TUD) Onderzoek van nieuwe technologieën t.b.v. derde generatie mobiele netwerken (3G) en een transparante integratie.	+							
Multi agent Based (Thales, Acklin, TNO TM, TNO FEL, TUD, UvA) Chaotic world Multi agent Based Intelligent Network Decision support Systems-calamiteitmanagement	+							
Ksyos Health Management Research. Creëren client-safe prototypische proeftuin (security, autorisatie, authenticatie)		+						
End-to-End Quality of Service in Next-Generation Networks (Lucent, KPN Valley, UT, TU/e, CWI)	+							
Nutrace: ontwikkeling keteninformatiesysteem voor proces- en productinformatie uit de voedselproductie- en leveringsketen (tracking & tracing en early-warning tools)				++			+	

Concluderend kan gesteld worden:

- De veiligheidsgebieden *Network security, Security protocols, Secure mobile communication* en *E-commerce, e-business, PKI, digitale handtekening, data-privacy, Smartcards* krijgen relatief veel expliciete aandacht in nationale en Europese projecten.
- De rol van *Biometrie* is vaak inherent in deze projecten. Biometrie-technieken worden veelal impliciet toegepast.
- *Cybercrime* heeft een directe relatie met Networksecurity, en wordt tot op zekere hoogte meegenomen binnen dergelijke projecten. Er zijn echter vooralsnog niet veel spraakmakende projecten met een primaire focus op Cybercrime.
- Hetzelfde geldt voor *Digital Rights Management, Digital Watermarking, digital copyright, content protection*. Dit is een sterk opkomend gebied dat uitdrukkelijker gestalte moet krijgen middels projecten.
- De overige 2 gebieden *Tracking & tracing....* en *Intelligente camera's ...* staan meer op zichzelf en krijgen ten opzichte van de andere gebieden minder aandacht.

Drs. Henk Mohanlal RE
Senior Adviseur ICT
SenterNovem, februari 2004

Hoofdstuk 1. Algemene bevindingen

1.1 Doel & Werkwijze van deze InnovationScan

Doel: Verkennend onderzoek naar de status van R&D-activiteit in Nederland op het gebied van ICT&Veiligheid. Het beschouwingsdomein betreft expliciet de private sector (bedrijfsleven) en de kennisinfrastructuur. Het uiteindelijke doel is het identificeren van de kansrijke Veiligheidsthema's voor Nederland om haar internationale concurrentiepositie als kennisintensief land te verstevigen of te ontwikkelen op deze thema's.

Aanpak: Bezoek van bedrijven en kennisinstellingen, telefonische interviews, Internet-research, literatuurstudie (zie Bijlage 1 voor een overzicht van de benaderde bedrijven en kennisinstellingen).

De bevindingen in dit eindrapport zijn gebaseerd op de zijnsoordelen en de situatieschetsen zoals die zijn weergegeven door de bevrraagden. Getracht is deze bevindingen zoveel mogelijk te vrijwaren van persoonlijke waardeoordelen. Om er voor te zorgen dat de uitspraken in het rapport zowel wetenschappelijk als door de praktijk gedragen wordt, is een aantal personen op basis van hun specifieke expertise gevraagd tussentijds feedback te geven dan wel input te leveren aan conceptversies van het rapport.

1.2 Scope "Veiligheid in de private sector"

Er is niet één vastomlijnd technologiegebied of toepassingsgebied dat Veiligheid volledig omsluit. Veiligheid kan een kwaliteitsaspect zijn (in de zin van betrouwbaarheid) en ligt daarom vaak inherent besloten in projecten.

Beveiliging van netwerken, informatiesystemen bijvoorbeeld is een 'pervasive aspect' net als performance, en wordt doorgaans niet expliciet als een aparte kostenpost wordt opgenomen.

Deze slechte zichtbaarheid van Veiligheid in projecten maakt het zeer lastig om macro-economische grootheden te kwantificeren, zoals de totale omzet van de private veiligheidsindustrie of het aantal personen werkzaam op Veiligheid. Vandaar dat deze InnovationScan noodzakelijkerwijs verworpen is tot een kwalitatieve analyse met een beperkte kwantificering.

Globaal beschouwd kan men enerzijds praten over de *fysieke beveiliging* en anderzijds over de (*virtuele*) *elektronische beveiliging*. Er zijn diverse ICT-technologieën die ingezet kunnen worden om veiligheid te ondersteunen.

Binnen de InnovationScan zijn die technologiegebieden in beschouwing genomen die in de *private sector* toegepast worden op de verschillende onderdelen van de veiligheidsketen: pro-actie, preventie, preparatie, repressie en herstel (nazorg in technische zin).

Voor het begrip Veiligheid kan een onderscheid worden gemaakt in safety en security.

- Bij *safety*, oftewel 'veiligheid' wordt gezegd dat een systeem veilig is wanneer het onder normale omstandigheden doet wat het moet doen. Door 'bad luck' kan het systeem onveilig worden.
- *Security* (= beveiliging) daarentegen is safety under attack (veiligheid gerelateerd aan 'kwade opzet'). 'Security is about regulating access to assets'. Een systeem heet secure of beveiligd als alleen geautoriseerde partijen toegang hebben, oftewel indien het goed blijft functioneren ook wanneer kwaadwilligen het onderuit (willen) halen.

1.3 Opvallende uitspraken van geïnterviewden

TU/e	<p><i>"Bij de TU/e bestaat een doctorale opleiding Masters in Security en een post-doctorale opleiding Information Security Technology. Er is een grote en groeiende belangstelling vanuit het buitenland voor deze opleidingen; buitenlanders willen graag de Nederlandse beveiligingstechnieken leren!! (Banken sponsoren de opleiding)"</i></p>
TNO-Maat-schappelijke Veiligheid	<ul style="list-style-type: none">- <i>In principe is er voor 10 jaar vooruit voldoende technologie beschikbaar om de behoeften uit bestaande processen te dekken. Dus is er nu een sterke behoefte aan nieuwe toepassingen ipv aan nieuwe technologieën (turning technology into business – nieuwe technologieën kunnen 'geleend' worden uit andere domeinen)"</i>- <i>"Kennisinnovatie kan pas waarde krijgen als de volledige keten wordt gedekt. Dus de ketenbenadering: het bij elkaar lappen van alle individuele inspanningen op deelschakels tot de grote economische waardeketen"</i>- <i>"Noodzakelijk voor de markt is het bedrijfsleven laten kennismaken of bewust maken van wat er mogelijk is aan faciliteiten in termen van technologie"</i>
Universiteit Amsterdam	<p><i>"Gat dicht tussen techniek en bedrijfsleven. Systeemintegratie (met name in fysieke beveiliging - camera's, sensoren, etc.): er zijn veel losse technieken wetenschappelijk uitgezocht en in proefschriften vastgelegd. Nu moet de technologie geïntegreerd worden binnen toepassingen en in de bestaande infrastructuur ('kennis omzetten in bedrijvigheid' – technostarters en incubators zijn goede katalysatoren). Dus D van R&D stimuleren: hoe passen de technieken in bestaande middleware? hoe de architectuur op te zetten? Grote gebruikers zijn wel geïnteresseerd in oplossingen, maar er zijn geen kant-en-klare applicaties. Er zijn veel technieken, en weinig toepassingen/producten, dus systeemintegratie is noodzakelijk!!!"</i></p>
TUD	<p><i>"De universiteiten bereiken de bedrijven niet zo goed, en andersom. Er is een kloof. De bedrijven zijn niet zo op de hoogte van wat er technologisch allemaal kan. En voor universiteiten is het interessant om de problemen aan te horen van de bedrijven. De echte leuke uitdaging voor een universiteit is als een nieuw applicatiegebied nieuwe technologische vragen oplevert. Dus niet louter recht-toe-recht-aan het oplossen van een gegeven vraagstuk maar ook het uitbreiden van de onderzoeksvraagstukken".</i></p>
TNO-FEL	<p><i>"In Nederland is er weinig zelscheppende industrie, weinig echte research in het bedrijfsleven. Wel heeft Nederland een zeer actieve systeemintegrerende industrie. Er is genoeg kennis die nu toegepast moet worden. Helaas zijn er weinig goed geteste producten op de markt."</i></p>
Chess	<p><i>"De veiligheidsindustrie in Nederland is niet bloeiend. Veiligheid wordt niet expliciet gewaardeerd door de opdrachtgever zodanig dat het als een aparte post wordt opgenomen. Het wordt door de opdrachtgever verwacht als inherent en als vanzelfsprekend, en lijkt daarmee een ondergeschoven kind. Nederland is goed in het praktisch toepasbaar maken van security en om te komen tot concrete oplossingen."</i></p>
UT	<p><i>"Het klassieke model van een strikte scheiding tussen de fysieke beveiliging (toegang tot fysieke bedrijfsdomeinen als terrein, gebouwen, ruimtes) en de virtuele beveiliging (bedrijfsinformatiesystemen) moet losgelaten worden. In de toekomst zal een integratie van fysiek, virtueel en organisatorisch beveiligen veel meer gewenst zijn binnen bedrijven."</i></p>

NEDAP	<p><i>“De eisen die gesteld worden aan security worden steeds groter. Integrators integreren veel verschillende componenten. Er ontstaat meer behoefte aan Security Management en integratie- ondersteunende software, waarbij ook de processen en procedures worden meegenomen naast de componenten. Er moet effectieve merkonafhankelijke software komen die de vele technieken/componenten integreren en compatibel maken met de verschillende protocollen. Fysieke beveiliging gaat meer naar e-beveiliging waarbij IP-technologie in combinatie met biometrie (facial recognition) een zeer grote rol zal spelen.”</i></p>
CWI	<p><i>“De security-omgeving in Nederland is gefragmenteerd. Een gemis is een breed Veiligheidsplatform, een expertisecentrum, wat functioneel kan zijn voor zowel de industrie als voor de wetenschap.”</i></p>
KUN	<ul style="list-style-type: none"> - <i>“Er is een grote toekomst weggelegd voor Nederland om onafhankelijke (e-)Security-audits uit te voeren voor commerciële partijen in het buitenland. TNO heeft reeds naam gemaakt met eerdere internationale evaluaties (o.a. proberen te kraken van smartcards die in Frankrijk gemaakt worden).”</i> - <i>“Nederland is een klein land dat keuzes moet maken in zijn expertiseopbouw. De selectie van computerbeveiliging heeft als bijkomend voordeel dat Nederland controle kan houden over systemen en gegevens die van nationaal belang zijn. Een hele reeks van chipkaarttoepassingen worden de komende jaren voor Nederland voorzien die niet zonder een gedegen toetsing van de beveiliging kunnen: de openbaarvervoerkaart, de paspoortchip met biometrische kenmerken en nieuwe bankpassen.”</i>
VU	<ul style="list-style-type: none"> - <i>“Nederland is traditioneel sterk in handeldrijven (commerce) en heeft een uitstekende infrastructuur voor entrepreneurs. E-commerce heeft een groot potentieel in Nederland, maar dan wel secure en safe! Philips is de wereldleider in Ambient Technology, en is de grootste producent van consumentenelektronica; er is derhalve veel kennis in Nederland op het gebied van Grid, Large distributed systems en Ubiquitous computing. Mensen hebben tegenwoordig zoveel computers; things-to-things-communication ligt in het verschiet. Het is dus noodzakelijk dat er een security-infrastructuur komt!!”</i> - <i>“Er is genoeg technologische kennis bij de universiteiten. Ten behoeve van de technology transfer zouden er meer incubators moeten komen. Jonge, talentvolle studenten moeten gestimuleerd worden om hun ideeën te commercialiseren. Deze startende ondernemers moeten financieel gesteund worden. Technologische security is relatief nieuw in het bedrijfsleven, er is niet veel competitie.”</i>
Sentinels-programma	<p><i>Sentinels is een researchprogramma over Computer security & Secure networks, en is in behandeling bij STW. The SENTINELS program aims to give a very significant boost to security expertise in the Netherlands by providing and managing resources for scientific research in information security, by building a national IT-security community, and by disseminating the results into industry and government in the Netherlands. SENTINELS aims to make all kinds of computer systems and computer networks more secure. This includes standard systems such as PCs and corporate networks, but also hand held devices and embedded systems, and wireless and on-chip networks. At present most security solutions are only partial solutions. Therefore, SENTINELS aims to contribute to a comprehensive framework for secure systems engineering.</i></p>

Sentinels schrijft over The Netherlands in the international context:

“The Netherlands is primarily a trading nation, requiring technological innovation in security and privacy to support banking and commerce. In manufacturing, Philips is most concerned with technological innovation in security and privacy to support consumer electronics. Therefore SENTINELS focuses on two application areas that are directly linked to the main economic drivers. These are “security and privacy for ambient intelligence” and “security and privacy for e-government and e-business”.

The Netherlands has a strong international position in a number of security and privacy research areas, including digital watermarking (Philips, TUD), cryptography (Philips, TU/e, TUD), electronic voting (TU/e), security protocol analysis (UT, TU/e, CWI), smart cards (Philips, KUN, TNO), biometrics (UT, CWI) and distributed systems security (VU). It is of crucial importance that the Netherlands should strengthen its position to keep playing its role as an equal partner and to avoid becoming dependent on other nations in areas that are essential for the Dutch economy.”

Hoofdstuk 2. Kansrijke deelgebieden: de bevindingen

Inleiding

In dit hoofdstuk worden die deelgebieden weergegeven en uitgewerkt die voor Nederland als kansrijk worden bestempeld.

'Kansrijk' in de zin van 'winning areas' waarin R&D-Nederland al floreert op het wereldtoneel of kan floreren gelet op het aanwezige R&D-potentieel.

Op basis van kansrijkheid zijn de volgende groepen van Veiligheidsgebieden geïdentificeerd:

1. Network security, Security protocols, Secure mobile communication
2. E-commerce, e-business, PKI, digitale handtekening, data-privacy, Smartcards
3. Digital Rights Management, Digital Watermarking, digital copyright, content protection
4. Tracking & tracing, tagging: Location Based Services
5. Biometrie
6. Intelligente camera's, computervision, beeldverwerking, video&audio-analyse (sensordata-fusie)
7. Cybercrime

Binnen een aantal significante programma's (zoals BSIK, IOP, CIC) lopen projecten die in meer of mindere mate aanknopingen hebben met één of meerdere bovengenoemde veiligheidsgebieden.

Het onderstaande overzicht vermeldt die projecten uit deze programma's die raakvlakken hebben met (één of meer) benoemde veiligheidsgebieden.

De mate waarin het project zich richt op het betreffende veiligheidsgebied, wordt aangegeven door een '+'.

- ++ = betreffende veiligheidsgebied krijgt sterke primaire focus in project
 + = betreffende veiligheidsgebied is secundair aandachtsgebied in project

Veiligheidsgebieden:	Network security, security protocols ...	E-commerce, e-business, PKI ...	Digital Rights Management, ...	Tracking & tracing, ...	Biometrie	Intelligente camera's,	Cybercrime
BSIK	1	2	3	4	5	6	7
Smart Surroundings (Philips, UT, TUD, Thales, TNO, Oce, Nedap, Ericsson oa). Research theme Distributed control.	++				+	+	
Embedded Systems Institute (ESI, ASML, Philips, Oce, TUD, TU/e, UT, TNO oa)	++	+					
Gigaport Next Generation Network (Surfnet, Uva, TNO, Telematica Instituut oa)	++	++	++				+
Freeband Communication (Telematica instituut, Philips, Lucent, Thales, TNO oa). Vision for Freeband for 2010 is to consider communication and information transfer from the perspective of the user, not the provider.	++	++					+
ICIS Interactive Collaborative Information Systems (Thales, TNO, TUD, UvA, UvM, KUN, UT, 4Tec) Research in secure collaborative decision support systems	++					+	
Bricks: Basic Research in Informatics for Creating the knowledge Society (CWI, TUD, TU/e, UT, Siemens, Stelvio oa). Het strategische project 'Security, identification, and authentication'	++	++	++	++	++		+

Virtual Lab e-Science (VU, UvA, TUD, Nikhef) Large-scale distributed systems - program Security	++	+					+
Space for Geo-information (thema Hoogwaardige Ruimte)				++			
MultiMedian. Nieuwe technologieën detecteren en tracking						++	
IOP							
PAW: Privacy in an Ambient World (TUD, UT, KUN, Philips, Microsoft) ontwikkelen architectuur voor de complete beveiliging van gebruikersgegevens	++	++	++				+
BASIS: Biometric Authentication Supporting Invisible Security (UT, TU/e, CWI, Philips, Nedap, Rabobank) transparant maken van biometrische authenticatie, anonimiseren biometrische informatie, voor gebruik binnenshuis.	++	++	++		++		
CIC							
CIM Cybernetisch Incident Management (Almende, CWI, VU, Group4Falck, TUD). Multi-agent technologie voor dynamische, complexe netwerken (incidentmanagement).	++						
DIANA: Data Interception & Analysis (Moniforce, VU, Interpay, Robeco) Real-time analyseren van datastromen om bijv. automatisch creditcardfraudeurs te achterhalen.		++					
CANDELA Content Analysis and Network Delivery Architectures (Bosch Security systems, TU/e, Philips Medical, LogicaCMG) Automatische analyse van (stilstaande) digitale videobeelden (video-bewaking)	+					++	
ICT Breedspoor: Onderzoek naar toepassingen van breedband communicatietechnologie bij bedrijfsprocessen in de Spoorwegbranche – veiligheid in treinen						++	
Residential Gateway (KPN, Philips, TUe, TUD): Onderzoek naar seamless architectuur en QoS aspecten van residential gateway, domotica	+						
Beyond-3G (Ericsson, KPN, TUe, TUD) Onderzoek van nieuwe technologieën t.b.v. derde generatie mobiele netwerken (3G) en een transparante integratie.	+						
Multi agent Based (Thales, Acklin, TNO TM, TNO FEL, TUD, UvA) Chaotic world Multi agent Based Intelligent Network Decision support Systems- calamiteitmanagement	+						
Ksyos Health Management Research. Creëren client-safe prototypische proeftuin (security, autorisatie, authenticatie)		+					
End-to-End Quality of Service in Next-Generation Networks (Lucent, KPN Valley, UT, TU/e, CWI)	+						
Nutrace: ontwikkeling keteninformatiesysteem voor proces- en productinformatie uit de voedselproductie- en leveringsketen (tracking & tracing en early-warning tools)				++		+	
KP5/6 (http://fp6.cordis.lu/fp6/home.cfm)							
PISA: Privacy Incorporated Software Agent (TNO-FEL,TUD)	++	++	+				
CaberNet: Network of Excellence in Distributed and Dependable Computing Systems (VU, UT)	++						++
PAMPAS: Pioneering Advanced Mobile Privacy and Security (Telematica Instituut, TNO-FEL)	++	+	+				+
MobilSafe: Mobile Communications used for improvement of the safety and security of emergency personnel and citizens during critical situations (UT).	++						
ESORICS: European Symposium On Research In Computer Security (UT)	++	+					+
TRUST: Technology and Research for Ubiquitous Security and Trust (UT).	++	+					

Verificard: Tool-assisted Specification and Verification of JavaCard programs: nextgeneration secure smartcards KUN		++	+		+		
RAPID Roadmap for Advanced Research in Privacy and Identity management (PricewaterhouseCoopers,TNO-FEL)		++			++		
RESET Roadmap for European Research on Smartcard Technologies (UT, KUN).		++			+		
FormalCard. Formal methods for safe and secure smart card software (UT).		++			+		
CyberVote. Develops an innovative cyber voting system for Internet terminals and mobile phones (TU/e)	++	++					+
NESSIE New European Schemes for Signature, Integrity and Encryption		++			+		
EurEauWeb: European Waterways Networked Information System 'locationally-aware' tourist-information.	+			++			
SecureGrid. Industrial-Grade Security for Grids.	+			++			
BIOVISION Roadmap Biometrics.Commercial application of biometrics over the forthcoming 10 years and identifying research challenges (CWI).	+	+	++		++		
CLUES. Scientific and Technical Support for Cybersecurity Policy (TNO-FEL)		+					++
STW/NWO							
(STW) SENTINELS research programme on computer security and computer networks	++	++	++	++	++	++	++
UbiCom: Ubiquitous Communications: to envision the use of the available computational resources in personal wearable systems (TUD, TNO-TPD, Telematica Instituut, HP, Ericsson, Nokia, Philips)	++	+	+		+		
(NWO) UbiSec: Security in Ubiquitous Computing (VU)	++	+					
(NWO) ProSecCo: Program Security and Correctness, Pioneer (KUN)	++						
(STW) A Framework for the Electronic Sale of Information Products (VU, NOB, KPN, Océ, Netherlands Audiovisual Archive, PCM Interactive Media)		++	++		+		
(NWO) SAMASC: Security Analysis for Multi-Applet Smart Cards (KUN, TU/e, KPN)		++			+		
PINPAS: Program INferred Power Analysis in Software (TU/e TNO-TPD)		++					
(NWO). Account: Accountability in Electronic Commerce Protocols (CWI, VU, UT)		++			+		
(NWO) Execution of Transactional Contracted Electronic Services (UT)		++			+		
CERTIMARK Certification of Watermarking techniques (TUD, Philips Natlab oa)			++		+		
(STW) SiCas: Sinusoidal Coding of Audio and Speech. To develop a software encoder/decoder for encoding both audio and speech (Philips, TUD)						++	

De overzichten met KP5/6/STW/NWO-projecten pretenderen niet volledig te zijn. Echter ze volstaan wel om samen met de andere overzichten tot bepaalde conclusies te komen:

- De veiligheidsgebieden *Network security, Security protocols, Secure mobile communication* en *E-commerce, e-business, PKI, digitale handtekening, data-privacy, Smartcards* krijgen relatief veel expliciete aandacht in nationale en Europese projecten, met vaak een inherente rol van de *Biometrie*. Biometrie-technieken worden veelal impliciet toegepast.
- *Cybercrime* heeft een directe relatie met Networksecurity, en wordt tot op zekere hoogte meegenomen binnen dergelijke projecten. Er zijn echter vooralsnog niet veel spraakmakende projecten met een primaire focus op Cybercrime.
- Hetzelfde geldt voor *Digital Rights Management, Digital Watermarking, digital copyright, content protection*. Dit is een sterk opkomend gebied dat uitdrukkelijker gestalte moet krijgen middels projecten.
- De overige 2 gebieden *Tracking & tracing....* en *Intelligente camera's ...* staan meer op zichzelf en krijgen ten opzichte van de andere gebieden in kwantiteit minder aandacht.

2.1 Network security, Security protocols, Secure mobile communication

Omschrijving:

"Network security is one of the most important parts of today's computer security, because almost all computer systems are connected (nodes in a network). Many network security protocols and security components have been developed. Security protocols are sets of rules for computers about how to act in a particular scenario in order to achieve a certain security goal. The correctness of security protocols is crucial. Although many ingredients are available to build a secure network infrastructure, there are many problems that remain to be solved. Many protocols appear to contain errors, protocols do not co-operate, etc. Research is required on new secure protocols, and on defense against Denial of Service (DoS) attacks. More often fixed networks are replaced by ad-hoc networks with the problem of an insecure transient association. Wireless and mobile systems support the communication of different media (data, speech, audio, video). Security is also critical. Current mobile services center around 4 available technologies: WAP, UMTS, Bluetooth and mobile positioning systems. WAP, UMTS together with GSM will turn the mobile phone into a smart-phone with Internet functionalities. Bluetooth will allow short-range data communication between consumer appliances in a domestic environment. Positioning systems will become integral part of the mobile phone, so services can be offered based on the location of the user.

Computing resources are becoming ubiquitously (everywhere and at all time). Ubiquitous computing will be provided for many tasks and services in our daily environment. Ambient systems are networked, embedded systems that are intimately intertwined with everyday environments, and that support people in various activities. Things-to-things communication will be possible as many daily life consumables increasingly contain sensors, actuators, processing units and embedded software. Communication and computing becomes personal: the user's position, profile and environment are identifiable. Therefore security is a must ."

Kennispositie Nederland:

veel = # bedrijven met R&D-activiteit > 25; redelijk = tussen 10 en 25; beperkt = kleiner dan 10

R&D-bedrijven: (zeer) veel

Nederland is traditioneel sterk in formele methoden (verificatie, testen) en ook zeer sterk in systeemcorrectheid (security-protocols). Nederland behoort tot de top samen met andere Europese landen zoals Frankrijk (INRIA) en de UK (Bill Roscoe).

Opvallend is dat VS niet prominent aanwezig is op dit wereldtoneel. In het Nederlandse bedrijfsleven richten veel R&D-groepen zich op network security, met name in de telecom en financiële sector (en ten behoeve van het militaire domein).

Aan bepaald onderzoek wordt geen ruchtbaarheid gegeven vanwege de geheimhouding.

Bij Thales vindt veel onderzoek plaats mbt large-scale distributed real-time (militaire) networks om 'enemy agents' buiten te houden.

CMG loopt voorop in de wereld als het om mobiele communicatie gaat. Philips Natlab richt een groot deel van hun onderzoek op Ambient Intelligence.

Academia: zeer veel onderzoek

Onderzoek in network security heeft een sterke internationale oriëntatie, waarbij de internationale organisatie ETSI (European Telecommunications Standards Institute) een belangrijke en sturende rol speelt, ook voor Nederland. Nederland levert hele goede bijdragen: TUD, TNO-FEL zijn betrokken bij het prestigieuze Europese PISA-project; TUD is lid van de EWICS (European workshop on Industrial computer security).

Bij de meeste Nederlandse universiteiten vindt onderzoek plaats. CWI is (internationaal) sterk in verificatie van security-protocols en heeft een Security-platform (SAFE-NL) opgezet. Ook is de multi-agent technology-groep (Prof. La Poutre) zeer sterk. De UT beschikt over de snelste protocol-verifier ter wereld (CoProVe, tevens het enige tool waarmee 'guessing attacks' kunnen worden geïdentificeerd).

Op de VU leidt de internationaal vermaarde Prof. Tanenbaum het Globe-project (internet security, security in large-scale distributed systems) en is er veel kennis over security van Grid & parallel systems. Uiteraard doet TNO-Telecom (ex-KPN Research) veel research.

Key players:

Bedrijfsleven:

- CMG Wireless Data solutions
- Philips Natlab (groep Ambient Intelligence)
- Thales: research in Network Security
- Nedap (NL met vestigingen in Europa, veel R&D): connecting intelligent devices to Internet
- Consul Risk Management (NL met kantoor in US, 30R&D) security event management
- Symantec (US): wereldmarktleider in Internetbeveiliging
- Kahuna (NL, 5R&D): secure network solutions
- Emexus (NL, 13 R&D) zakelijke mobiele technologie
- Infopulse electronic commerce (NL, 15R&D) generiek security platform
- Ernst&Young (Prof. Michiels buitengewoon hooqleraar UT)

Academia:

- Utwente (Prof. Michiels – IS & Internet Security)
- TUD (dr. Spruit)
- VU (prof. Tanenbaum)
- CWI (Security platform - prof. Fokkink)
- TUE (Prof. Baten, prof. Mauw formele methoden)
- TNO-Telecom (fraud-management in network)
- Telematica Instituut (mobile internet technology – dr. Bob Hulschebosch)
- KUN (dr. Hoekman)
- TNO-TPD (dr. Jan Verschuren)
- TNO-FEL (dr. Huizenga - Security group)
- RUL (dr. Bos - secure network programming)

SAFE NL provides a forum for researchers, practitioners, and implementors from research institutions, industry and government agencies to exchange ideas on the state of the art in security technology, and application areas.

Relaties met significant onderzoek:

BSIK:

1. Smart Surroundings (Philips, UT, TUD, Thales, TNO, Oce, Nedap, Ericsson o.a.). Research theme distributed Control. Goal is to investigate architectures and frameworks for future ambient systems. Ambient systems should be designed to empower and support people in their activities, but in ways that would avoid the control or manipulation of non-authorized others: aspects from personal privacy to 'system trust'.
2. Embedded Systems Institute (ESI, ASML, Philips, Oce, TUD, TU/e, UT, TNO o.a.). Embedded systems are heterogeneous: they are multi-technology and they operate in physical environments under uncertainties, continuous changes and failures. The heterogeneous character adds considerably to the complexity of the software. Research on how to design such complex systems in a reliable and timely fashion.
3. Gigaport Next Generation Network (Surfnet, Uva, TNO, Telematica Instituut o.a.). Investigate methods to improve optical transport and optical switching as well as electronic switching and routing capabilities for networks, including the connections to other networks. Focus on new Internet features and secure protocols in the field of

- Ipv6 and Multicast and on preparing the network and network services for delivering secure grid and web services.
4. Freeband Communication (Telematica Instituut, Philips, Lucent, Thales, TNO o.a.). Vision for Freeband for 2010 is to consider communication and information transfer from the perspective of the user, not the provider. Freeband addresses the knowledge chain of the new ubiquitous communication paradigm: society, users and applications; networking, service provisioning and generic user interaction; enabling technologies.
 5. ICIS Interactive Collaborative Information Systems (Thales, TNO, TUD, UvA, UvM, KUN, UT, 4Tec) research in secure collaborative decision support systems, viz. a combination of innovative intelligent agents, self-learning and human-computer interface technology, supporting reasoning with uncertainty, reasoning with risks and reasoning under a lack of knowledge.
 6. Bricks: Basic Research in Informatics for Creating the knowledge Society (NWO – in beheer bij OC&W). Het strategische project 'Security, identification, and authentication' (binnen thema Parallel and Distributed computing), ihb 'Protocols for secure infrastructure and e-commerce': robustness of security-protocols and developing methods to analyse how far security protocols can withstand hostile attacks (CWI, TUD, TU/e, UT, Siemens, Stelvio).
 7. Virtual Lab e-Science (in beheer bij OC&W): Under the programline Large-scale distributed systems, the program Security: to create a secure and reliable distributed hardware/software infrastructure base that can be used for offering and accessing grid computing, storage and visualisation resources, instrumentation and information (VU, UvA, TUD, Nikhef)

KP 5/6:

1. PISA: Privacy Incorporated Software Agent. Coordinator: TNO-FEL, partner: TUD. The project aims to build an electronic intermediary that will be able to quickly and independently process tasks given by the Internet user and at the same time protect the user's privacy
2. CaberNet: Network of Excellence in Distributed and Dependable Computing Systems. Partners: Andy Tanenbaum (VU) and Pieter Hartel (UT).
3. PAMPAS: Pioneering Advanced Mobile Privacy and Security. Partners: Telematica Instituut, TNO-FEL.
4. MobilSafe: Mobile Communications used for improvement of the safety and security of emergency personnel and citizens during critical situations. Participants: Dimitri Konstantas, Pieter Hartel (UT).
5. ESORICS: European Symposium On Research In Computer Security. Member: Pieter Hartel (UT).
6. TRUST: Technology and Research for Ubiquitous Security and Trust. Participant: Sandro Etalle (UT).

Overig:

1. SENTINELS: (probably STW-funded) research programme on computer security and computer networks.
2. Vanuit *CIC*: project CIM Cybernetisch Incident Management (Almende, CWI, VU, Group4Falck, TUD). Onderzoek op het gebied van modellering, simulatie en representatie van dynamische, complexe netwerken d.m.v. multi-agent technologie, t.b.v. incident- en calamiteitenmanagement.
3. UbiCom: Ubiquitous Communications: to envision the use of the available computational resources in personal wearable systems. Partners: TUD, TNO-TPD, Telematica Instituut, HP, Ericsson, Nokia, Philips.

4. UbiSec: Security in Ubiquitous Computing (sponsored by NWO). Andy Tanenbaum (VU) (2003-2007).
5. ProSecCo: Program Security and Correctness, NWO Pioneer project lead by Jacobs (KUN) (2002-2007..)
6. Onderzoeksproject aan de TUD (Prof Wagenaar) – ‘Privacy protection in new mobile devices’: development of a component-based ICT-architecture that resolves the conflict between personal information owners (individuals) and information collectors (service providers) regarding privacy control. The architecture should give users more control functionalities of their personal information (sensitive info, such as location, preferences and activities) by letting them explicitly and permanently be able to provide their consent on the collection of their personal information in an autonomous and user-friendly way.

Opportunities qua toepassingen ('challenges for the future'):

1. De mensen hebben zoveel computers en mobile devices (GSM, PDA, etc.) die niet beveiligd zijn. Er wordt ook steeds meer data op gezet. Er zijn complexe crypto-algoritmes nodig om én de data en de onderlinge communicatie te beveiligen. De gebruikte devices bij wireless communication (GSM) hebben echter een beperkte rekencapaciteit. Er zijn veel beveiligingsproblemen geconstateerd bij o.a. ad-hoc netwerken, sim-kaarten en gepersonaliseerde diensten (zie artikel Telematica Instituut, dr. Bob Hulschebosch - "Mobiele beveiliging schiet tekort"). In de toekomst is binnen domotica/home-electronics things-to-things communicatie te verwachten welke uiteraard een strenge beveiliging vereist (een apparaat wordt door verschillende mensen benaderd en beheerd waarbij info bedoeld voor de één niet open mag staan voor de ander). Remote access/operation vraagt om beveiliging: er moet een Security-infrastructuur komen! De infrastructuur zal van niemand en van iedereen zijn (issue van network-ownership of ownership van verschillende layers van het network). Het probleem zal ontstaan hoe ervoor te zorgen dat iedereen zich netjes 'conform etiquette' binnen het netwerk gedraagt.
2. Vanuit BSIK-project Smart Surroundings: Ambient embedded systems have various application domains: consumerproducts for home control/kitchen appliances, white-good products, audio and video consumerproducts, desktop and mobile communication, health care, traffic control, environment, security, agricultural equipment, etc. Applications for security: automated assessment of situations and alarm generation, personal security, smart alarms, secure operation of dangerous devices, crisis detection, safety-critical services, location- and context based security.
3. Vanuit BSIK-project ESI: Research addresses 'reliability, predictability and robustness & verification, validation', including the aspects of safety (to the user, operator, service employee, etc) and security (protection against unwanted access). Intelligent products will be developed to improve our standard of living: audio-visual equipment, home appliances, automobiles, medical equipment, aircrafts, buildings, etc. Internet can be used to pass information to millions of people and to connect intelligent devices in order to reduce delays, energy usage, etc.
4. Vanuit BSIK-project Gigaport (see other BSIK-proposal Gigaport NG Applications) Application domains: (e-)business networks (trade, transport, retail, industry, finance, media, publishing), Healthcare, Education (e-learning), Government, SME (re-use and shared use of ICT-resources), Telecommunications (open end-to-end applications not dominated by just 1 or 2 telco's)
5. Vanuit BSIK-project Freeband: Onder thema 'Society, users, applications' – new applications based on ubiquitous broadband mobile networking technologies where security is of prime importance (emergency work, intelligent traffic assistance, home health care). Onder thema 'personal environment, services and network' – setting up a

- secure scalable broadband wireless environment, secure peer-to-peer and ad-hoc networks, realising unobtrusive context awareness. Onder thema 'enabling technology' – new electronic and optical technology for secure broadband wireless access, house networking, optical switching, body area networks (secure wearable systems)
6. Vanuit BSIK-project ICIS: Application domains: air traffic management/harbour control, crisis and incidentmanagement, military command & control (anti-terrorism, networkcentric warfare), medical monitoring systems, security industry (smart camera's, aggression detection), processing industry, Web-safety, Multicasting applications (multicasting is an optimization of communication amongst groups)
 7. Vanuit BSIK-project Bricks: a system will be developed for the engineering of provably secure multi-cast security protocols. Application domains: auction sites, multi-round negotiation, co-operating agent platforms, variable road pricing- kilometerheffing
 8. Vanuit BSIK-project Virtual Lab e-science: large, geographically distributed teams will be able to work together more efficiently (sharing global scarce resources) – application within multinationals; combine distributed resources from company and customer – application in hospitals and amongst medical professionals
 9. Nederland moet meer doen aan Open Source Security (wellicht een rol voor de overheid). Er zijn veel Open Source producten die beveiliging behoeven.
 10. Er is behoefte aan 1 secure operating system. Er is een Nederlands initiatief onder leiding van Prof. Andrew Tanenbaum van de VU. Het ontwikkelde OS, genaamd Minix, beslaat nu nog 100 pagina's aan code. Men wil dat terugbrengen naar maximaal 20, omdat iedere regel code extra beveiligingsrisico's met zich meebrengt.

Potentiële marksectoren:

- Trade & Logistics (secure web services)
- Telecom
- Embedded systems
- Consumer-electronics
- Education
- Healthcare
- Public services (information sharing at disaster management, environmental safety and welfare)
- Financial services
- Industry (platforms for collaborative design and effective communication and coordination)

2.2 E-commerce, e-business, PKI, digitale handtekening, data-privacy, Smartcards

Omschrijving:

Bij e-commerce gaat het om het elektronisch verhandelen van goederen en diensten via het Internet, waarbij 'vertrouwen' het sleutelwoord moet zijn. E-business is wat breder, waarbij elektronisch zaken wordt gedaan tussen de eigen organisatie, een klant en eventueel een partner met gebruikmaking van web-enabled on-line communicatiekanalen. Naast de e-B2C (business-to-customer) wordt de e-B2B (business-to-business) steeds populairder.

Beveiligingseisen zijn onder andere:

- goede bescherming van de uitgewisselde gegevens,
- zekerheid dat de andere partij ook inderdaad degene is voor wie hij zich uitgeeft (*Identity-management*),
- flexibiliteit in het toekennen van rechten aan personen om gegevens te kunnen benaderen of te manipuleren,
- vertrouwen in een goede afhandeling van de betaling en de bezorging,
- waarborgen dat de verstrekte informatie niet wordt doorverkocht aan derden.

Om doelgerichte e-commerce mogelijk te maken is het belangrijk dat de wensen (voorkeuren, profiel) van de consument zo nauwkeurig mogelijk bekend zijn. Hiervoor worden intermediairs, software agents, ingezet die voor consumenten en bedrijven vraag en aanbod op elkaar moeten afstemmen. De software agent, als alter ego van zijn gebruiker heeft veel informatie over de gebruiker die hij vertegenwoordigt. Wanneer onderhandeld wordt met andere agents of personen, wordt deze privacy-gevoelige informatie verstrekt. De agents moeten dus worden beveiligd, niet enkel de data die ze bevatten, maar ook de cryptografische berekeningen voor het vercijferen van de info en het ontcijferen van de info op de plek waar dat nodig is. De Privacy enhancing Technieken (PET) zorgen hiervoor.

Public key infrastructure (PKI) is een technologie die een cruciale rol vervult bij het realiseren van betrouwbare elektronische diensten. PKI zorgt dat elektronische transacties onweerlegbaar worden doordat de zogenaamde digitale handtekening gezet kan worden (PKI is een enabler voor de digitale handtekening). Daarnaast zorgt PKI dat de informatie beveiligd over Internet kan.

Een smartcard (chipcard) bevat een chip waarin persoonlijke gegevens kunnen worden opgeslagen, bewerkt en verwijderd. Door middel van de card is het mogelijk de betreffende persoonsgegevens te lezen, de persoon en de kaart te identificeren, informatie te versleutelen en wisselende gegevens geordend op te slaan. Smartcards worden met name gebruikt voor veilige elektronische transacties (betalen), voor toegangsbeveiliging m.b.t. gebouwen en netwerken (GSM), opslag van persoonlijke data, etc.

Kennispositie Nederland:

veel = # bedrijven met R&D-activiteit > 25; redelijk = tussen 10 en 25; beperkt = kleiner dan 10

R&D-bedrijven. (zeer) veel

Veel onderzoek vindt plaats bij banken, echter de security in banking is een gesloten wereld omgeven door een waas van geheimhouding. De meeste banken hebben een eigen PKI-oplossing en doen daar onderzoek naar (ook Interpay).

Johan Enschede/SDU ontwikkelt PKI-software voor de identificatie en het beheren van digitale certificaten, dat doen zij ook voor andere landen in de wereld! Er zijn veel bedrijven in Nederland die op eigen initiatief onderzoek doen naar PKI. Ordina Public Utopics ontwikkelt webbased PKI, LogicaCMG en Sogeti richten zich oa op PKI en identity-management. In Nederland is door de PKI-taskforce een PKI-standaard ingevoerd voor de overheid die voor 95% overeenkomt met de wereldstandaard. Echter het moet voor het bedrijfsleven nog optimaal werkend worden gemaakt (het initiatief ligt bij de ondernemer om het wel/niet te gebruiken). In US is er weinig PKI omdat smartcards nog niet zo populair zijn. In België bestaat een nationaal werkend PKI.

Veel R&D is er op het gebied van smartcards: Philips, SafeNet (cryptografische functies voor smartcards en gsm's), Chess (nieuw beveiligd serviceconcept met de functie van een centrale kassa voor internetwinkels), AET (wereldmarktleider in het integreren van smartcards met digitale handtekeningen binnen applicaties - afzetmarkt China, Australië, Zuid-Amerika, etc !!)

Academia: veel onderzoek

Nederland is zeer sterk in programmacorrectheid voor smartcards. Nederland zit zelfs aan de top, samen met Frankrijk en Duitsland (meer een Europese aangelegenheid; Frankrijk is koploper in het gebruik van smartcards). Fundamenteel smartcardonderzoek vindt voornamelijk plaats bij KUN en UT. Nederland leidt in smartcard security evaluatie! TNO-EIB is namelijk vooraanstaand in de wereld als dé onafhankelijke partij om security-evaluaties van payment terminals te doen (smartcards, terminals, PDAs, security tokens). Ze werken hierin samen met KUN en TU/e. Vanuit het buitenland wordt al vaak een beroep op hen gedaan voor onafhankelijke Security-audits. Voor de toekomst wordt een krachtigere rol voorzien. Ook vanwege de ontwikkelingen in de wetgeving. In Duitsland is al een wet van kracht die eist dat smartcards met digitale handtekeningen geëvalueerd moeten worden. De rest van Europa zal wellicht volgen met deze wetgeving.

Ook speelt Nederland een rol bij het internationale keurmerk voor IT-Security systemen (software/hardware), de zgn. Common Criteria. Nederland is nl. sinds kort opgenomen binnen de kring en opereert vanuit TNO ITSEF. TNO ITSEF (*Information Technology Security Evaluation Facility*) evalueert voor commerciële partijen de veiligheidsaspecten van ICT-producten zoals firewalls, audit software, access control applications (biometric) en PKI-software, inclusief het totstandkomingsproces. Door de internationale erkenning kunnen Nederlandse projecten nu dus een internationaal geldig certificaat krijgen.

Via het Europese PISA-project is de kennispositie van Nederland (TUD) zeer sterk op het gebied van Privacy-enhancing technieken. PET voor persoonlijke profielen kunnen het MKB doen innoveren. MKB-aanbieders van mobiele of sms-diensten zitten te wachten op betrouwbare beveiligingstechnieken. PET is een opkomend gebied waar Nederland goed in kan worden.

Key players:

Bedrijfsleven:

- De Nederlandse Bank (visionair Leon Strauss)
- Philips
- Siemens Information & communication Solutions (verst met het invoeren van PKI in Nederland)
- Chess (NL, 8 R&D) ontwikkelen van infrastructuur t.b.v. veilig e-betalen en e-voting

Academia:

- TNO-EIB, TNO ITSEF, TNO-FEL (PKI-lab), TNO-Telecom
- KUN (Prof. Jacobs – Security of Systems, Java-card security)
- TUD (Prof. Lagendijk – PET)
- TU/e - EIDMA

- Johan Enschede/Sdu (15 R&D)
- Ordina Public Utomics (26 R&D)
- AET (NL, 6 R&D)
- Irdeto Access (oorspronkelijk NL ca. 80R&D) cryptography for localised conditional access
- SafeNet (NL 34 R&D)
- The VisonWeb (NL R&D) smartcards, public & private key infrastructures, biometrie
- Stelvio (NL 11 R&D) beveiligingsvraagstukken rond intranet- en internettechnologie
- Hagenuk Smart Card solutions (NL 12R&D) transactie- en gegevensbeveiliging
- Fox-IT (NL R&D) ontwikkeling security operating systeem
- Bhold Company (NL 20R&D) ontwikkeling nieuwe security standaard tbv e-business transacties
- RSA Security (US, 150 R&D in Zweden en US): wereldleider identity- en access-management, e-security
- Computer Associates (US, in NL ook R&D) suite e-Trust met open interface naar producten van derden
- KPMG (doet certificering), Quint, Redwood, Wellington
- Telematica Instituut (vanuit project 'Virtuele Haven')
- VU
- KUB (Prof. Prins -ICT & Recht, juridische privacy aspecten)
- Nijenrode – Forensic Accountancy (Bob Hogeboom)
- PKI-taskforce (www.pkioverheid.nl)
- ETSI-European Telecommunications Standards Institute (standaardisatie elektronische handtekening)

Relaties met significant onderzoek:

BSIK:

1. Bricks: Basic Research in Informatics for Creating the knowledge Society (NWO – in beheer bij OC&W). Het strategische project 'Security, identification, and authentication' (binnen thema Parallel and Distributed computing), i.h.b. 'Protocols for secure infrastructure and e-commerce': to develop e-commerce protocols that are secure and fair, in the sense that no participant in the protocols has any advantage over the other participants; to develop a tool for the verification of multi-cast e-commerce protocols (CWI, TUD, TU/e, UT, Siemens, Stelvio)
2. Gigaport Next Generation Network (Surfnet, Uva, TNO, Telematica Instituut o.a.). The BSIK Gigaport NG –Applications will develop a set of basic ICT services to support e-business services over a wide range of domains.

IOP Generieke Communicatie

1. PAW: Privacy in an Ambient World (TUD, UT, KUN, Philips, Microsoft) ontwikkelen architectuur voor de complete beveiliging van gebruikersgegevens
2. BASIS: Biometric Authentication Supporting Invisible Security (UT, TU/e, CWI, Philips, Nedap, Rabobank) transparant maken van biometrische authenticatie, anonimiseren biometrische informatie, systeem aanpassen voor gebruik binnenshuis.

CIC-doorbraakproject

1. DIANA: Data Interception & Analysis (Moniforce, VU, Interpay, Robeco) Het real-time analyseren van datastromen ofwel mining van data streams om bijv. automatisch creditcardfraudeurs te achterhalen. Rekening moet worden gehouden met veranderend klantgedrag in de tijd.

KP5/6:

1. Verificard: Tool-assisted Specification and Verification of JavaCard programs. The next generation of smart cards will be used for services where security is a key issue: authenticated access to computer networks, e-commerce, high value wire-less services etc. Coordinator: Bart Jacobs (KUN).
2. PISA Privacy Incorporated Software Agent (TNO-FEL, TUD) secure solution to protect the privacy of the citizen when he is using Intelligent Agents (shopbots, buybots, pricebots) in E-commerce/M-commerce applications, according to EC-directives RAPID Roadmap for Advanced Research in Privacy and IDentity management. Coord. : PricewaterhouseCoopers), TNO-FEL.
3. RESET Roadmap for European Research on Smartcard Technologies. Founding members: P. Hartel (UT) and B. Jacobs (KUN).
4. FormalCard. Formal methods for safe and secure smart card software. Participant: Pieter Hartel (UT).
5. CyberVote. Develops an innovative cyber voting system for Internet terminals and mobile phones. Coord.: Schoenmakers (TU/e), partner: Bart Preneel (Leuven).
6. NESSIE New European Schemes for Signature, Integrity and Encryption. Coordinator: Bart Preneel (Leuven).

Overig:

1. SENTINELS
2. A Framework for the Electronic Sale of Information Products (funded by STW) VU (Prof. Tanenbaum), NOB, KPN research, Océ, Netherlands Audiovisual Archive, and PCM Interactive Media (2000-2005).
3. SAMASC: Security Analysis for Multi-Applet Smart Cards (sponsored by NWO). Partners: B. Jacobs (KUN), E. de Vink (TU/e), and KPN (2002-2006).
4. PINPAS: Program INferred Power Analysis in Software (sponsored by TU/e). Partners: E. de Vink (TU/e), and TNO-TPD
5. Account: Accountability in Electronic Commerce Protocols (sponsored by NWO). Partners: Wan Fokkink (CWI), Bruno Crispo (VU) and Sandro Etalle (UT) (2003-2007..
6. LicenseScript: a language and framework for calculating licenses on information over constrained domains. Partners: Sandro Etalle (UT), Wouter Teeuw (Telematica Instituut), Wim Jonker (Philips Research) (2002-2004).
7. Execution of Transactional Contracted Electronic Services (sponsored by NWO, UvT) (2003-07).
8. Finger_Card: integrated sensor on smart card
9. Onderzoeksplan PKI en Veilige elektronische dienstverlening (Min BZK)

Opportunities qua toepassingen ('challenges for the future'):

1. Vanuit BSIK-project Bricks: a next-generation of e-commerce protocols, and an improved trust in the security of negotiation protocols, resulting in many secure applications in the financial domain, retail, trade, etc.

2. Vanuit BSIK-project Gigaport (see other BSIK-proposal Gigaport NG Applications)
Application domains: (e-)business networks (trade, transport, retail, industry, finance, media, publishing), secure service-based infrastructure for Healthcare (teleconsulting, telemonitoring), Education (e-utility based, e-learning and knowledge management platforms promoting ubiquitous knowledge transfer and dissemination), service-based e-business and collaborative work applications in a broadband environment.
3. Vanuit CIC -project DIANA: Toepassingen in de forensic datamining, bijv. het detecteren van frauduleuze handelingen voordat iemand onrechtmatig een bankrekening leeghaalt.
4. Het MKB vraagt om PKI-technologie voor vele toepassingen. Onderzoek is noodzakelijk op vele punten: revocatie, validatie, interoperabiliteit (tussen PKI-eilanden, internationaal), privacy (PKI koppelen aan personen?), veiligheid van PKI (maken, analyseren en bewijzen van veiligheid via cryptografische algoritmes; de geldigheidsduur van certificaten; aantonen dat niet met timestamp geknoeid is), harmonisatie van PKI-systemen voor de afstemming binnen Europa, alternatieven voor PKI? etc.
5. E-billing is nog niet goed geregeld. Security bij het elektronische betalingsverkeer is een nog niet ontgonnen gebied. Er zijn veel partijen actief, maar de problemen zijn nog niet opgelost. Bij het elektronisch betalen binnen de particuliere omgeving (van PC naar bank) wordt de PC als de lek beschouwd, zeer gevoelig voor inbraak. Van bank tot bank lijkt het redelijk safe. Onderzoek naar bijvoorbeeld solide security protocollen is noodzakelijk. Niet alleen in Nederland maar in de hele wereld! Ook is te verwachten dan mobile-banking zal opkomen, waarvoor niet alleen nieuwe betaalschema's ingericht moeten worden, maar ook methoden ontwikkeld moeten worden die de security en de privacy waarborgen van zowel de klant als de verkoper.
6. Identity-management is een veelbelovend gebied, zeker in combinatie met biometrie. De digitale handtekening is wel erkend binnen het Civielrecht, maar niet binnen het Strafrecht; hoe het proces van digitaal ondertekenen in te richten o.b.v. biometrie?
7. Een goede rol is weggelegd voor Nederland als Security-auditor. Er is echter internationaal gezien procedureel niet veel geregeld voor wat betreft security-audits.
8. Privacy Enhancing technieken: er zijn grote problemen en veel kansen. Aldus is veel innovatie bij het MKB te realiseren.
9. Secure E-government: de overheid wil zich toeleggen op elektronische dienstverlening naar andere overheden, bedrijven en burgers (publieksgerichte dienstverlener). Communicatie zal wellicht via Internet zijn met de nodige zorgen van capaciteit en betrouwbaarheid.

Potentiële marksectoren:

- Banking & financial services (improved connection between international operations and wireless service access)
- Retail (e-billing, personalised services, transaction standards)
- Trade & Logistics (secure web services)
- Industry (e-procurement)
- Education (e-learning)
- Healthcare (privacy of patientdata)
- Public services (e-voting, e-government of passports, driving license)

2.3 Digital Rights Management, Digital Watermarking, digital copyright, content protection

Omschrijving:

Kopieerbeveiliging is dé manier om *content* te beschermen wat over de Web gaat. Uit angst voor illegaal kopiëren worden steeds meer cd's, video's, dvd's en spelletjes voorzien van kopieerbeveiligingsprogramma's, ook wel *digital rights management* genoemd.

"Digital rights management (DRM) is a type of server software developed to enable secure distribution - and perhaps more importantly, to disable illegal distribution - of paid content over the Web. DRM technologies are being developed as a means of protection against the online piracy of commercially marketed material, which has proliferated through the widespread use of Napster and other peer-to-peer file exchange programs. Although online content is protected by copyright laws, policing the Web and catching law-breakers is very difficult. DRM technology focuses on making it impossible to steal Web content. DRM can be seen as the whole collection of commercial, legal, and technical measures to enable trading of digital items on electronic infrastructures."

Digital watermarking wordt gebruikt om images en video, i.h.a. fysieke multi-media informatie, te beschermen. In een toenemend aantal applicaties moet bepaalde geheime informatie permanent worden gehecht aan de oorspronkelijke (compressed) image en video data.

Watermarking technieken bieden de mogelijkheid om deze geheime informatie in te bedden binnen image en video door net zoveel afgemeten hoeveelheden van deze informatie toe te staan dat het detecteerbaar wordt. Bij het consumeren van multi-media (bijv. bekijken van een film in de bioscoop) moeten de encrypties niet merkbaar zijn voor de consument. De encrypties van de geheime informatie (bijv. de bioscoop waar de film afgedraaid wordt, of de eigenaar van de film) moeten zodanig zijn dat wanneer illegaal gekopieerd wordt (met een videocamera in de bioscoop de film opnemen) deze watermerken te herleiden zijn.

Kennispositie Nederland:

veel = # bedrijven met R&D-activiteit > 25; redelijk = tussen 10 en 25; beperkt = kleiner dan 10

R&D-bedrijven: **redelijk** voor Digital Watermarking; **veel** voor Content protection en DRM. De grootste slachtoffers van content-piracy en illegaal kopiëren zijn de contentproviders (muziek, video, dvd, games-industrie) en leveranciers van consumenten-electronica (TV, VCR, etc.).

In Nederland doet Philips als voornaamste leverancier van consumenten-electronica veel diepgaand onderzoek in DRM. Ze hebben zelfs de trekkersrol in de wereld en bezorgen daardoor Nederland een sterke concurrentiepositie.

Voorheen bestond er een Amerikaans bedrijf Intertrust dat een zeer groot patentenportfolio binnen DRM en Watermarking had opgebouwd in de wereld. Zij zijn echter failliet gegaan, omdat ze kennelijk niet tot concrete toepassingen konden komen. Het bedrijf is toen door Philips (49% aandeel) en Sony opgekocht, waarmee Philips (en dus Nederland) vanwege de vele IPR behoorlijk kan domineren in de wereld. Philips wil nu de transformatie slag maken naar toepassingen.

In de wereld gaan steeds meer grote bedrijven investeren in DRM-onderzoek (Sun, Microsoft investeert 500 miljard dollar, etc.).

Er is in de private en de publieke sector veel vraag naar robuuste Watermarking technieken (met name veel MKB'ers willen deze technieken toepassen). Philips kan een grote aanbieder worden.

M.b.t. Content protection hebben multinationals als Microsoft, Sharp, Nokia, etc een grote impuls gegeven in de wereld, ook Nederlandse bedrijven pakken dit nu op (DMDSecure, Chess, Tridion, Océ, Enschede/SDU).

Academia: redelijk wat onderzoek, wordt sterker

Met name de TUD is gestart met pionierend onderzoek op het gebied van DRM, en zij hebben Philips op dit spoor gebracht. Buiten deze 2 trekkers in Nederland zijn er ook andere sterke onderzoeksgroepen ontstaan op het gebied van Digital Signal Processing: bij de TU/e (signaalverwerking, ook van geluid en spraak), de UT (DRM), het Telematica Instituut en het CWI.

Key players:

Bedrijfsleven:

- Philips Natlab: 25 R&D'ers werken op DRM, Digital Watermarking en Copy protection
- DMDSecure (NI, 20R&D) leader in unique software for content protection and DRM server-side solutions to broadband, broadcast&mobile operators and service providers
- Tridion (NL, 30 R&D) toonaangevende Europese leverancier van geavanceerde, op XML gebaseerde enterprise content managementsoftware
- Bosch Security (ex-Philips CSI)
- Chess: heeft architectuur Net.Engine voor DRM opgezet

Academia:

- TUD (Prof. Lagendijk).
- TU/e (Prof. Kalker – electronic watermarking, fingerprinting)
- UT (Prof. Hartel en Prof. K Slump – signals & systems).
- Telematica Instituut: Gigaport richt zich op DRM
- CWI (Secret-key Certificate)

Relaties met significant onderzoek:

BSIK

1. Bricks: Basic Research in Informatics for Creating the knowledge Society (NWO – in beheer bij OC&W). Het strategische project 'Security, identification, and authentication' (binnen thema Parallel and Distributed computing), ihb 'Biometrics and digital watermarking': to develop biometrical recognition techniques and interfaces which are transparant, together with digital watermarking tools for DRM. (CWI, UT)
2. Gigaport Next Generation Network (Surfnet, Uva, TNO, Telematica Instituut oa). Focus on DRM, secure vital identities and the related userprofile

IOP Generieke Communicatie

1. Onderzoekthema Security: User ID and Service Control
User-Service Control is a security issue that comprises of digital right management keys or certificates for the usage of services and the needed authentication (User ID).

Overig

1. CERTIMARK Certification of Watermarking techniques (TUD, Philips Natlab o.a.)
Certimark is a European task force in the field of watermarking technologies. The project aims at the design and development of a complete benchmark suite for watermarking technologies. This includes the design of watermarking algorithms and attacks on watermarked data.
2. Onderzoek bij Philips (Dr. Linnartz): Digital Rights Management in consumer electronics products.

Opportunities qua toepassingen ('challenges for the future'):

1. Multimedia Watermarking wordt steeds meer een krachtige tool voor allerlei IPR-bescherming toepassingen. Er is een grote noodzaak dat verbeterde én nieuwe technieken worden ontwikkeld, omdat de huidige methoden zich te beperkt richten op specifieke applicatie-gebieden en teveel parameters kennen die moeilijk te begrijpen zijn. Daarbij is er een grote vraag naar assessment en evaluatie-tools. Deze bestaan niet waardoor de e-business wordt bemoeilijkt alsook pogingen om standaardisatie te bereiken.
2. Onderzoek in DRM wordt steeds meer noodzakelijk. Hollywood verwacht 100% beveiliging van hun films, maar dat kan niet met de huidige watermarking technieken (er zijn bepaalde technieken om watermerken te verwijderen). De verbeterde technieken zullen gretig aftrek vinden in de (internationale) filmindustrie.
3. Vanuit BSIK Bricks: de combinatie van biometrie & digital watermarking is veelbelovend om bij transacties de identiteit vast te stellen van de entiteit (persoon) waarmee de transactie wordt aangegaan. Biometrie legt de identiteit van een individu vast aan de hand van bepaalde lichaamskenmerken of handelingen. Biometrische encryptie is nodig om het unieke biometrische patroon van een persoon om te zetten naar een private encryption of een coding key. Vele toepassingen zullen mogelijk worden bijv. om illegale kopieën te traceren (bij afgifte kan een gepersonaliseerd watermerk obv biometric key worden ingebed in de data), bij proof of ownership van afgifte van muziek of film over internet.
4. Vanuit BSIK Gigaport: toepassingen in de Publishing industry, Media & Entertainment (profiling and digital rights management in the media services; content delivery on demand and paid per use- requires integration of user authentication) Game-industry, Retail (personalised services), etc.
5. Vanuit IOP - User service control in context. User service control takes place in a context that determines what services can be offered, and how users will respond to the service provisioning. Issues relevant for application:
 - Watermarking and digital finger printing to link the identity of the rightful copyright owner, or distribution point to the content. This is useful to detect fraud in case content escapes the control of DRM systems
 - Processes for reliable certification of systems with trust classification. Methods and tools are needed to support efficient and effective certification.
 - Example environment is central storage of security key and policies in all inhouse devices as e.g. DRM keys of legal music such that music can be played on any device in the house of the key owner.

Potentiële marksectoren:

- Media
- Entertainment (film, audio, games)
- Consumer-electronics
- Retail
- Healthcare

2.4 Tracking & tracing, tagging: Location Based Services

Omschrijving:

Elektronisch identificeren en het kunnen volgen van goederen en personen. Producten (en personen) kunnen individueel en uniek geïdentificeerd worden middels een *tag* (= een kleine computerchip met een uniek nummer). Met de tags is het ook mogelijk de objecten met tags te volgen: *tracking & tracing*. De locatiebepaling kan plaatsvinden via de van oorsprong militaire GPS (Global Positioning System obv satelliet), DGPS (grotere nauwkeurigheid omdat naast de satellieten gewerkt wordt met een vast aardestation), AGPS, en de cel-id in een GSM.

Location based services (LBS) omvatten het geheel aan mobiele diensten welke specifiek zijn toegesneden op het aanbieden en bevragen van locatiegebonden informatie ter plekke. De locatie van het mobiele apparaat en van het gebruikersprofiel zijn hierbij van belang. Denkbare toepassingen zijn toegang tot bedrijfsdatabases, directory services, navigatie, opsporing, tracking en tracing, ondersteuning bij noodsituaties en locatie-afhankelijke m-commerce.

Kennispositie Nederland:

veel = # bedrijven met R&D-activiteit > 25; redelijk = tussen 10 en 25; beperkt = kleiner dan 10

R&D-bedrijven: veel

Het vakgebied van LBS bestaat al 15 jaar, en heeft een grote push gekregen vanuit de Amerikaanse wetgeving. In US werd destijds de eis ingevoerd dat wanneer een 111-call gedaan werd, ook precies de locatie direct bekend moest zijn van die call. In 2004 zal ook de Europese wetgeving dit eisen (112-call). Naar verwachting zullen LBS in 2005 de meest gebruikte mobiele toepassingen zijn. Nederland is goed in GIS (geographical information systems) en in mobiele communicatie (CMG wereldspeler). GIS, vroeger gericht op overheden (planning nieuwe infrastructuur, etc.) is nu verschoven naar de private sector (routeplanners, navigatiesystemen, etc.). Er zijn veel Nederlandse GIS-bedrijven met security-producten en R&D in security-technologie (Geodan, Ram Mobile Data, CityGis, CMG Wireless data solutions, Ordina Utilities, Tensing SKS, Nedap, Cross Point, Armada, Tethys, Vecos, etc). Daarnaast nog grote multinationals met R&D activiteit in Nederland als Honeywell, Alcatel, Blaupunkt (Bosch), Vodafone, Armada group, Zenitel (Belgisch).

Nederland is goed in GIS, met name in 3 uitdagende gebieden:

- Spatial modelling,
- Het vastleggen van de x/y coördinaten met een mapping naar databases,
- Visualisatie.

Mbt het 2^e (x/y-vastlegging) is Nederland wereldmarktleider: de 3 sterkste partijen in de wereld zijn Nederlands: Navtech (voorheen 100% Philips), Teleatlas (car navigation) en de kleinere AND. M.b.t. de 3^e, visualisatie en virtual reality in combinatie met GRID-computing, is ook sterke expertise aanwezig (CAVE, Green Dino, Lost Boys, etc.)

Academia: **veel** onderzoek zeker vwb spatial modelling (VU- Prof. Peter Nijkamp) en GRID (RUG, UVA, Sara).

Key players:

Bedrijfsleven:

- NavTech, Teletlas, AND
- Geodan (NL 60R&D): marktleider in LBS-toepassingen
- Ram Mobile Data (NL 30R&D): mobile oplossingen
- CityGis (NL 10R&D) marktleider Benelux in meldkamer-software om voertuigen te monitoren
- Tensing SKS (NL 40R&D): automatische voertuiglocatie
- Cross Point (NL 30R&D): wireless identification
- Armada (NL 6R&D): tagging
- Tethys (NL 6RD): draadloze beveiliging t.b.v. transport
- ESRI (US R&D) grootste GIS-security leverancier
- CapGemini

Academia:

- VU: Prof. H. Scholten (directeur Geodan), Prof. P. Nijkamp
- TUD: technische aspecten van LBS (Dr. E. Verbree), communicatie van de informatie (Prof. I. Lagendijk- Intelligente systemen)
- Universiteit Wageningen
- SARA (GRID)
- RUG

Relaties met significant onderzoek:

BSIK

1. Space for Geo-information (thema Hoogwaardige Ruimte): research in geo-information infrastructure concepts, spatio-temporal modelling, geographic man-machine interaction, geo-information & society

KP5/6:

1. EurEauWeb: European Waterways Networked Information System: development of a Pda which can be mounted on a boat, cycle, wheelchair, etc and will provide users with 'locationally-aware' tourist-information.
2. SecureGrid. Industrial-Grade Security for Grids.

Nederland is via Rotterdam betrokken bij het Amerikaanse SafePorts programma.

Opportunities qua toepassingen ('challenges for the future'):

1. N.a.v. het BSIK-project zal in Nederland nagedacht moeten worden over een hele goede geo-data infrastructuur om alle beschikbare geo-informatie te ontsluiten. Er is veel geo-data verzameld wat veel tijd en geld heeft gekost (AND doet het zo goed omdat ze over een groot aantal jaren data verzameld hebben). Het platform kan leiden tot productinnovatie en nieuwe diensten zullen mogelijk worden voor oa de topografische dienst en overheidsinstellingen (Stichting Ravi als vertegenwoordiging van publieke en private sector is de trekker)
2. Op dit moment vindt de meeste plaatsbepaling plaats via het Amerikaanse GPS (had een militaire oorsprong om kruisraketten op te sporen). De Europese tegenhanger heet Galileo en is puur bedoeld voor gebruikers in de civiele markt. Het zal een hogere nauwkeurigheid hebben en zeer gebruikersvriendelijk zijn. Galileo biedt veel opportuniteiten: alle Europese space-agencies werken eraan, ook de Nederlandse. De Europese richtlijn voor de 112-call, in 2004 van kracht, zet veel druk op het onderzoek. Galileo kan tot veel toepassingen leiden: gebruik in vrachtauto's, fleetmanagement, etc.

3. De Radio-tag als opvolger voor de barcode om goederen over de hele wereld te kunnen volgen. Er vindt onderzoek plaats op de MIT (US) hoe alle producten te voorzien van zo een smart tag. Op dit moment kan er bij kassa's slechts 1 product tegelijk gescand worden. Met de tag kunnen dan meerdere producten tegelijk en op afstand gescand worden (kassa's kunnen dan in principe verdwijnen, nieuwe businessmodellen zullen ontstaan). De nieuwe tag zal betaalbaar zijn (5 dollarcent). Europa volgt het Amerikaanse onderzoek nauwlettend.
4. Nieuwe ontwikkelingen rondom UMTS (Mobility) zullen ervoor zorgen dat meer data in een kortere tijd overgebracht kan worden. Als de zendmasten dichter bij elkaar komen te staan is ook een hogere nauwkeurigheid van lokalisering te bereiken, met nieuwe toepassingsmogelijkheden voor LBS.
5. Het project SafePorts in Rotterdam is onder druk van de US geïnitieerd (de US-douane eist een strenge controle). Nieuwe tracking&tracing technieken dragen bij aan het beveiligen van goederenstromen (RF, tags, tracking&tracing) en het volgen van mensen (scheepsbemanning) bij main ports (haven, vliegveld).
6. In het algemeen neemt de vraag toe naar meer gebruikersvriendelijke en privacy-inachtnemende oplossingen voor het volgen van goederen en mensen.

Potentiële marksectoren:

- Transport & Logistiek
- Zorg
- Maritiem
- Defensie
- Consumentenmarkt
- Milieudienstverlening (volgen gevaarlijke stoffen)
- Automotive-industry (secure labelling of components)

2.5 Biometrie

Omschrijving:

Biometrie is de technologie die het mogelijk maakt bepaalde persoonlijke karakteristieken waar te nemen, te meten en vast te leggen. Het betreft zowel gedrags- als fysieke karakteristieken.

Met deze technologie kan men op elektronische wijze de identiteit van een persoon verifiëren (uiteraard indien de biometrische karakteristieken van die persoon vooraf in een systeem zijn opgenomen).

Enkele bekende karakteristieken zijn: de iris, de stem, de vingerafdruk, gelaat (gezichtsherkenning, gezichtsthermogram), de retina, de schriftdynamiek, de vorm van een deel van de hand, de bloedvaten op de rug van een hand, de loophouding (gait), de oorschelp, de menselijke geur, etc. Om de biometrische beveiligingsgraad te verhogen wordt vaak multiple biometrics toegepast waarbij gewerkt wordt met een samenstel van karakteristieken.

Kennispositie Nederland:

veel = # bedrijven met R&D-activiteit > 25; redelijk = tussen 10 en 25; beperkt = kleiner dan 10

R&D-bedrijven: veel (echter beperkte Research)

Europa is leidend in veel segmenten van de internationale biometrics markt.

US is in het bijzonder sterk in irisherkenning (Iridian technologies heeft alle patenten op irisherkenning). Maar op andere gebieden als herkenning van gezicht, vingerafdruk en loophouding heeft de US veel contracten lopen met Europese onderzoekers. Frankrijk (Sagem) is wereldleider op het gebied van large-scale fingerprint systemen.

Het Duitse bedrijf ZN Vision Technologies heeft de techniek van automatische gezichtsherkenning uitgevonden en is wereldleider op dit gebied. Ook voorop lopen Zweden (fingerprint sensorchiptechnologie) en België (multiple biometrics solutions).

Nederland valt op als het gaat om *toepassingen* in de biometrie, niet zozeer de zuivere research.

Nederland heeft een aantal grootschalige biometrie-pilots gedaan die de Europese aandacht hebben getrokken:

- het eerste biometric-based border crossing system in de wereld is bij Schiphol toegepast;
- vingerafdruk en gezichtsherkenning bij nachtclubs,
- handgeometrie bij Rotterdam Haven om de lading te kunnen volgen,
- verslaafdenzorg (methadonverstrekking).

Er zijn veel (kleinere) bedrijven die biometrie oplossingen leveren: HVL, IE Keyprocessor, TechID, CMG, Atos Origin etc. Sommige verschaffen de sensoren, andere meer specialistische softwarebedrijven ontwikkelen betere herkenningsalgoritmen of verbeterde middleware. Helaas blijkt soms dat de bedrijven niet goed op de hoogte zijn van de resultaten uit wetenschappelijk onderzoek.

Academia: intensief onderzoek

Bij een klein aantal kennisinstellingen vindt intensief onderzoek plaats.

Bij de UT is veel kennis voorhanden op het gebied van vingerafdrukken, handgreepherkenning en statistische patroonherkenning. De TNO-TPD heeft expertise in gezichtsherkenning, fingerprint hardware, earprint- en handschrift-analyse. Nederland is vanuit het CWI vertegenwoordigd in het Europese Biometrie Forum. In 2001 is het Nederlands Biometrie forum opgezet met een grote participatie van de Nederlandse onderzoekers.

Key players:

Bedrijfsleven:

- Johan Enschede/SDU: irisscan-technologie ontwikkeld voor Schiphol Privium-controle – Schiphol is de eerste luchthaven die gebruik maakt van de irisscan.
- Dartagnan (NL R&D) joint venture tussen Enschede/SDU en Schiphol; vermarkten van producten voor biometrische identificatie (o.a. automatische grenspassage middels irisherkenning).
- Philips Natlab: anonieme biometrie (consumer-electronics).
- Nedap: vingerafdruk, iris, handgeometrie, gezicht.

Academia:

- CWI (dr. Schouten)
- UT (dr. Veldhuis)
- TNO-TPD (dr. van Munster)
- TU/e (anonieme biometrie: hierbij houdt een persoon zijn unieke biometrische gegevens zelf bij zich i.p.v. dat het in een centrale database wordt gezet).

Relaties met significant onderzoek:

BSIK

1. Bricks: Basic Research in Informatics for Creating the knowledge Society (NWO – in beheer bij OC&W). Het strategische project 'Security, identification, and authentication' (binnen thema Parallel and Distributed computing), i.h.b. 'Biometrics and digital watermarking': to develop biometrical recognition techniques and interfaces which are transparant, together with digital watermarking tools for DRM. (CWI, UT)

IOP GenCom

1. BASIS: Biometric Authentication Supporting Invisible Security (UT, TU/e, CWI, Philips, Nedap, Rabobank) transparant maken van biometrische authenticatie, anonimiseren biometrische informatie, systeem aanpassen voor gebruik binnenshuis.

KP5/6

1. BIOVISION (participant CWI). Project supported by European Commission, preparing the ground for future R&D activities by investigating the likely commercial application of biometrics over the forthcoming 10 years and identifying research challenges. Project will lead to European Biometrics Forum as a central reference point. Focus on 5 areas: technology and applications (inventory of suppliers, research and trials), user perceptions, medical dimension (can race, illnesses, states of mind be deduced?), security (standards and addressing vulnerabilities), legal and regulatory issues.
2. RAPID Roadmap for Advanced Research in Privacy and IDentity management. Coord.: PricewaterhouseCoopers, TNO-FEL.

Opportunities qua toepassingen ('challenges for the future'):

1. Biometrie is een veelbelovende techniek om de safety en security van de samenleving te verhogen. Maar de echte doorbraak moet nog komen. Er zijn nog wat challenges te overwinnen: de technologie is nog niet volwassen, er zijn geen standaards, het is niet eenvoudig om biometrische karakteristieken te scheiden van het lichaam, de oplossingen voor verschillende toepassingsgebieden zijn te divers. Voor een aantal karakteristieken is veel kennis beschikbaar in de wereld, zoals voor iris- en vingerafdrukherkenning. Mbt gezichtsherkenning (bijv. op basis van camerabeelden) zijn er nog veel technologische vragen te beantwoorden. Grosso modo kan gesteld worden dat de bestaande biometrische technieken niet robuust genoeg zijn. Ook het proces rondom de integratie van de technieken binnen bestaande systemen en bedrijfsprocessen wordt nog niet goed ingericht. De omgevingsvoorwaarden bij het gebruik van biometrie lijken bepalend, en niet zozeer de biometrische aspecten. Invoering (implementatie) lijkt toch niet zo eenvoudig te zijn.

2. Z  r kansrijk is de toepassing van biometrie binnen de mobile communication voor authenticatie en autorisatie. Evenzo geldt dat voor het gebruik van biometrie rondom Smartcards. Uitdagende issues hierbij zijn: scalability, privacy van de biometrische data, gebruikersacceptatie, hoe PKI te combineren met biometrie, wet- en regelgeving, etc. De UT heeft met een sterkte in smartcards en vingerafdrukherkenning veel potentie voor Nederland.
3. Vanuit BSIK, IOP KP5/6- projecten zijn vele toepassingen te verwachten in verschillende sectoren:
 - (health) medical card, hospital services, fysieke beveiliging van ziekenhuizen, dataprotectie van pati ntenbestanden, invalidehulp
 - (government) paspoort, ID card, rijbewijs, werkvergunning, e-Voting, belastingbetalen, verhuizingen, etc.
 - (telecom) authenticatie van mobiele en vaste telefoons als diefstalbeveiliging,
 - (home security) personaliseren van producten en diensten als diefstalbeveiliging, fysieke toegang (sleutelgaten vervangen)
 - (office environment) fysieke toegangscontrole (tot gebouwen, tijds- en aanwezigheidsregistratie), logische toegang (e-mail, databases)
 - (manufacturing) toegangscontrole tot specifieke machines en processen
 - (financial) electronic Web-transactions, openen van rekeningen, verzekeringen afsluiten, creditcards, interbank transfers
 - (leisure services) age-limited services (tabak, alcohol, TV/Video/Internet), excluding entrance (casino's, nachtclubs, voetbalvandalen), privileged services (frequent users airmiles, season tickets, DRM, resorts, etc.), service sharing (personalisatie van auto, PC of TV-settings binnen een gezin), hotels (personalisatie van maaltijden, etc.)
 - (education) examination & tests, fysieke beveiliging scholen, registratie van kinderen
 - (criminal justice) tagging van criminelen, persoonlijke wapencontrole, surveillance van publieke ruimten
 - (defensie) identificeren vriend/vijand op het slagveld, wapencontrole
 - (transport) internationaal rijbewijs, cross-border travel, security of access to vehicles (trucks, planes), baggage-controle, security of hubs (airport, stations)

Met name vanuit BIOVISON worden de technisch-inhoudelijke application security issues gespecificeerd voor toepassingen in de toekomst (zoals anti-spoofing technology, performance and robustness improvements, transparency, etc.).

Potenti le marksectoren:

- Health
- Government
- Telecom
- Financial services
- Education
- Transport & logistics
- Manufacturing
- (Military) Defense
- Business and office-environment
- Leisure services

2.6 Intelligente camera's, computervision, beeldverwerking, video&audio-analyse (sensordata-fusie)

Omschrijving:

Videocamera's worden toegepast zowel in het publieke domein (stations, winkelcentra, etc) als in het private (binnen bedrijven) met het doel om normaal/afwijkend gedrag te detecteren (surveillance). In toenemende mate worden ook verschillende soorten sensoren ingezet als waarnemingssysteem.

Een '*intelligent camerasysteem*' moet niet alleen beweging detecteren (motiondetectie), maar ook kunnen 'classificeren' wat voor object het is (dier, mens, fietser, auto, etc.).

De camera moet men dus kunnen gebruiken als een intelligente sensor om beeldinterpretatie door de operator te ondersteunen zodat alerter en preventief kan worden gereageerd met een betere waarborging van de privacy. Bij '*sensordata-fusie*' is er sprake van het combineren van signalen van meerdere soorten sensoren. Camera-informatie in de vorm van slaande beweging, rennen, achteruit deinzen van mensen kan dan gecombineerd worden met audio-signalen zoals schreeuwen of glasbreuk of snelheidsinformatie zoals rennen.

Door de combinatie is het mogelijk agressie of sociaal ongewenste gedrag te detecteren (*early-warning*). De waarnemingssystemen leveren informatie op die bewerkt of verwerkt kan worden (image/video/acoustics/speech-processing).

Kennispositie Nederland: veel = # bedrijven met R&D-activiteit > 25; redelijk = tussen 10 en 25; beperkt = kleiner dan 10

R&D-bedrijven: **redelijk**

Er zijn zeer veel installateurs van camera- en toegangscontrolesystemen in Nederland (Aritech [US], ADT Security[US], Enai, Van Ovost, VCS International, ASR, IE Keyprocessor, Cisco [US] etc.). Slechts een relatief klein aantal bedrijven doet aan eigen R&D (ASB Security, Alphasatron Security, Bosch Security [ex-Philips CSI], Thales, Siemens, Getronics [ex-Koning&Hartman], Honeywell etc.). Nederland lijkt voorop te lopen als het gaat om sensortechnologie voor infrarood en glasbreukdetectie (Vitelec). M.b.t. complex sound analysis ligt bijzondere (wereldunieke) expertise bij het bedrijf Sound Intelligence (R&D samen met RUG). Verder zijn er nog wat kleinere bedrijfjes voor noise monitoring (o.a. AP Technology).

Op het gebied van Beeldverwerking/Computervision zijn er in Europa veel technologische projecten, en is er dus veel kennis beschikbaar - ook in Nederland - op een hoog niveau. Nu moet de stap gemaakt worden naar toepassingen in de private en publieke sector en gekeken worden naar de praktische haalbaarheid (werkt beeldverwerking wel?). Er is een beperkt aantal commerciële partijen goed actief in R&D in Nederland (oa Philips CFT, Philips Natlab, DVS, Dacolian, Thales). Er zijn echter wel veel actieve gebruikers van buitenlandse technologie verpakt in producten (InitialVarel, NS, Group4Falck). De US (DARPA) en Israël zijn toonaangevend in de wereld.

Academia: **veel** kennis aanwezig

Vwb intelligente-camera's en sensorfusie wordt veel onderzoek gedaan bij TNO-TPD, TNO-FEL, UVA (IAS). Op het gebied van computervision/beeldverwerking is sprake van een sterke as: UvA(ISIS), TUD, TNO-TPD, CWI. In Nederland is men in 1970 begonnen met de medische beeldverwerking en heeft men sindsdien diepgaande ervaring opgebouwd. De onderzoeksschool ASCI is opgezet (ASCI Advanced School for Computing and Imaging, erkend door KNAW), een landelijk samenwerkingsverband tussen TU Delft (penvoerder), VU, UvA, RuLeiden, Universiteit Utrecht, Utwente, RuGroningen, TU/e. Hun onderzoek richt zich op *Computer Systems* en *Imaging Systems* (Beeldverwerking en Patroonherkenning: ontwikkeling van algoritmen en theorievorming voor diverse beeldsensoren, computergraphics, interactietechnieken, computervision, visualisatie).

Key players:

Bedrijfsleven:

- Bosch Security (voorheen Philips CSI), Philips CFT, Philips Natlab, Thales
- ASB (NL 5R&D): camera-observatie, digitale beeldverwerking
- Aritech (US - moeder GE Interlogix BV, 30R&D in NL) digital video; academische lijnen met Duitse Universiteiten (faculteit voor Beveiligingstechniek!).
- DVS (NL R&D) imaging, intell. camerasystemen
- Dacolian (NL, 10 R&D): wereldleider mbt software voor nummerbordherkenning; beeldverwerking voor verkeer en transport
- Vitelec (NL, 8R&D): sensordetectie verschillende motions
- Prime Vision: character recognition technology
- Sound Intelligence (NL 6R&D): sensorfusion, early warning obv audio

Academia:

- Uva –IAS (Intelligent autonomous systems) sensingtechnology, computational intelligence (Prof. Groen)
- Uva-ISIS (Intelligent Sensory Information systems): smart camera's, hardware-based beeldverwerking (Prof. Smeulders)
- TNO-TPD (Imaging en Data-interpretatie – project Parkeerwachter
- TNO-FEL (van der Heuvel)
- Mediamill (joint TNO-TPD en UvA): semi-automatische analyse van video, beeld, geluid, tekst
- TUD (van Duin): patroonherkenning; intelligente systemen (Inald Lagendijk, Biemont)
- RUG (Prof. Petkov): patroonherkenning
- CWI
- KUN – NICI Nijmegen institute for cognition and information: interpretatie van geluid
- UT(P. Brey): maatschappelijke aspecten van video-surveillance
- ASCI: Image systems
- ESI: intelligent embedded systems

Relaties met significant onderzoek:

BSIK:

1. MultiMedian: nieuwe technologieën voor detecteren en tracking

CIC:

1. CANDELA Content Analysis and Network Delivery Architectures (Bosch Security systems, TU/e, Philips Medical, LogicaCMG) automatische analyse van (stilstaande) digitale videobeelden; netwerktechnologie in de zakelijke- en privé-omgeving. Toepassingen in videobewaking, consumentenelektronica en medisch (detectie, kwantificering, diagnose).

STW:

1. SiCas: Sinusoidal Coding of Audio and Speech. Collaboration between Philips Research, TUD, Royal Institute of Technology (KTH), Universities in Sweden. Objective : to develop a software encoder/decoder for encoding both audio and speech at a competitive bit rate with respect to state-of-the-art audio and speech coders

Opportunities qua toepassingen ('challenges for the future'):

MultiMedian zal met een aantal demonstrators komen die duidelijke toepassingen hebben (1 t/m 5):

1. Smart camera's voor inspectie.
De smart camera moet flexibel ingezet kunnen worden voor verschillende inspectietaken met variërende beeldopname omstandigheden. Er moet intelligentie zijn in het real-time uitrekenen van beelden onafhankelijk van schaduw, belichting en reflecties. Hardware moet gekoppeld worden met postbewerking embedded software. Toepassingen in visuele inspectie van producten, en het volgen van mensen in real-time. Potentiële afnemers: gemeenten (surveillance), Schiphol, Stork, marktsectoren: agro-industrie, packaging industrie, druk- en printindustrie.
2. Intelligente camera's voor het volgen van bewegende personen of andere objecten in video en het automatisch trekken van intelligente conclusies uit deze informatie.
A-priori kennis over 'verdacht of afwijkend gedrag' is noodzakelijk (early warning: potentiële zakkenrollers, gedrag van massa's, agressie verhoogt de temperatuur). Objecten moeten gedefinieerd kunnen worden en voorspellingen van het traject gemaakt kunnen worden met de intelligente analyse. Automatisch detecteren van afwijkend gedrag geeft een voorselectie, waardoor mensen in controlekamers sneller reageren. Potentiële afnemers: thuiszorginstellingen, openbaar vervoer, mobiele applicaties van streaming video, sport (tv-makers, coaches), overheid, bewakingsbedrijven, particuliere gebruikers
3. Bewegende object classificatie.
Het bewaken van persoonlijk eigendom op publiek/private terreinen; beveiliging op afstand voor diefstal, brand en agressie . Veel is wetenschappelijk bekend en ook in de markt kennen veel bewakingssystemen de basisprincipes. Interpretieren van de tracks naar een 3d-wereld is lastig en gebeurt nog niet goed. De uitdaging is versimpeling en real-time implementeren van bestaande algoritmes voor specifieke situaties. Potentiële afnemers: publieke sector, beveiligingsbranche, en toeleveranciers.
4. Tracken met een bewegende camera en videobeelden opnemen uit een bewegende bron.
De situatie is veel complexer dan met een stilstaande camera omdat ook de achtergrond beweegt. Potentiële afnemers: videoanalyse van mobiele camera's, driver-assist systemen
5. Object-tracker: het betrouwbaar kunnen volgen van objecten in omstandigheden waarbij de camera niet statisch is en het te volgen object ook achter andere objecten mag verdwijnen.
Er moet netwerkintelligentie zijn, het overnemen van een camera door een andere om het spoor te volgen, ook als er 1 uitvalt. Potentiële afnemers: producenten van geavanceerde beveiligingssystemen; omroepbedrijven die hoogtepunten van sportwedstrijden beschikbaar willen stellen op Internet; productiebedrijven die materiaal bij digitalisatie automatisch willen voorzien van metadata.
6. Hoe combineer je slim audio met video?
Geluidsdetectie (niet-spraak) is nog niet sterk ontwikkeld in de wereld (glasbreuk, voetstapherkenning, schreeuwen). Uitdagingen voor sound intelligence (bijv. onderscheid een auto van een vrachtwagen), ook uit het STW-project SiCas.
7. Het inzetten van biometrie vindt een goede toepassing wanneer personen geïdentificeerd moeten worden aan de hand van bepaalde opnametechnieken (belichting/ recht in de camera kijken). Beeldverwerking als onderdeel van biometrische herkenning is zeer kansrijk voor Nederland. Met name als het wordt toegepast op het gebied van consumenten-electronica. Philips zorgt in Nederland voor een zeer sterke industrie in consumer electronics, en zijn er dus kansen voor Nederland. Sterke concurrentiepositie.

8. Beelden leveren een berg aan informatie op, die vaak realtime verwerkt moet worden. Hoe de juiste informatie eruit te filteren? En over te brengen. Toepassingen in Incidentmanagement en network-centric warfare. Wie moet welke informatie wanneer weten – commander control technieken. Waarnemingssystemen verheffen tot waarschuwingssystemen!
9. Intelligente camera-systemen inzetten voor andere toepassingen als remote maintenance, wachtrijen observeren t.b.v. betere service, etc.

Potentiële marksectoren:

- Fysieke Beveiligingsindustrie
- Productiebedrijven
- Zorg
- Gemeenten
- Openbaar Vervoer
- Transport & Logistiek
- Machine- en apparatenbouw
- Consumentenelektronica (SmartHomes, Domotica)
- Agro-industrie
- Packaging industrie
- Druk- en printindustrie
- Evenementenbranche en soortgelijke branches.

2.7 Cybercrime

Omschrijving:

Cybercrime is criminaliteit waarbij gebruik wordt gemaakt van digitale dataopslag of datacommunicatie. Er zijn 7 belangrijke kenmerken (effecten) van digitalisering die de spelregels rond criminaliteit veranderen:

- plaats en afstand,
- tijd en frequentie,
- anonimiteit,
- kopieerbaarheid en gemak van verspreiding,
- manipuleerbaarheid en uitwissen van sporen,
- beschikbaarheid van informatie,
- beschikbaarheid van apparatuur.

Er zijn vele verschijningsvormen van cybercrime, zoals hacken, verspreiden van virussen/worms/trojan horses, defacing (vernielen of uitschakelen Websites), spamming (verzenden ongewenste e-mail), DoS aanval (aanval op systeem of service met het doel deze uit te schakelen – denial of service), spoofing (je voordoen als iemand anders – dmv IP, e-mail, etc.), portscan (scannen computerpoorten op zoek naar actieve services), password guessing, sniffing (bekijken netwerkverkeer). Al deze activiteiten vormen een bedreiging van de openbare orde en veiligheid op het informatienetwerk (daarbij komen de problemen van anonimiteit, grote snelheid, afstand, etc.)

Kennispositie Nederland: veel = # bedrijven met R&D-activiteit > 25; redelijk = tussen 10 en 25; beperkt = kleiner dan 10

R&D-bedrijven: beperkt

Cybercrime is een groot probleem, niet alleen voor Nederland, maar voor de gehele internationale gemeenschap. Een onderzoeksrapport van Symantec Corp. (wereldleider in Internet security) wijst uit dat Nederland voor het eerst de 'top-10' heeft bereikt van onveilige landen op het Internet. Dat wil zeggen dat vanuit Nederland veel virussen e.d. de wereld over gaan. De (financiële) schade die bedrijven oplopen door cybercrime is zeer groot. Helaas doet in Nederland een beperkt aantal bedrijven aan R&D in Intrusion detection. Wel zijn er veel integrators van security-oplossingen tegen cybercrime voor netwerken en Internet, zoals Kahuna, Anite, Irdeto Access, CrypSys Data Security, Telindus, Pinewood automatisering, etc.

Academia: veel

Nieuwe technieken moeten worden ontwikkeld voor intrusion detectie, bijv. gebaseerd op statistische analyse. De kennisinstellingen die zich in het algemeen bezighouden met netwerkonderzoek, nemen het veiligheidsaspect mee in hun technologisch onderzoek (zie ook 2.1 Network Security). Bij de UT doet Prof. Michiels (ook werkzaam bij Ernst & Young) specialistisch onderzoek naar intrusion detection en e-mail spam. Sommige kennisinstellingen hebben ook niet-technologische cybercrime expertise: TNO-FEL (dr. Smit heeft t.b.v. het onderzoeksprogramma Politie en Wetenschap een sociaal-maatschappelijk onderzoek gedaan naar cybercrime), de RUL, KUB en de UvA kijken naar de juridische implicaties van cybercrime.

Key players:

Bedrijfsleven:

- Irdeto Access (NL nu over de hele wereld, ca. 80R&D)
- Anite (NL, vestigingen in Europa, R&D) Enterprise Security Management
- Pinewood automatisering (NL, groot in Benelux) integreert netwerkbeveiliging
- CG Ernst & Young EDP Audit (Prof. Michiels)
- Aladdin Knowledge systems (US) software commerce and Internet security

Academia:

- TNO/FEL (ir. Huizenga, ir. Luiff, dr. Smit)
- UT (Prof. Michiels- intrusion detection, e-mail spam)
- VU (drs. Timmer, Centrum voor Politiewetenschappen, Prof. Tanenbaum)
- TUD (dr. Van der Lubbe)

Niet-technologisch:

- RUL (Prof. Franken, Ict & Recht)
- KUB (Prof. Prins, ICT & recht)
- UvA (Prof. Hugenholtz, Instituut voor Informatierecht IVir)
- KLPD Werkgroep Digital Politie t.b.v. cybercrime
- GOVCERT Computer Emergency Response Team van de Nederlandse overheid. Centraal meld- en coördinatiepunt voor relevante veiligheidsincidenten (initiatief Min. BZK).

Relaties met significant onderzoek:

KP5/6

1. CLUES. Scientific and Technical Support for Cybersecurity Policy. Partner: TNO-FEL and Leuven

Overig

1. SENTINELS (intrusion detection)
2. KWINT Kwetsbaarheid op Internet (vanuit Min. EZ) Doelstelling is het aandragen van concrete oplossingen (voorlichting, stappenplan) voor bedrijven, burgers, consumenten en overheid, om zichzelf beter te kunnen beschermen tegen de risico's die aan internetgebruik kleven.

Opportunities qua toepassingen ('challenges for the future'):

1. Binnen de meeste (grotere) bedrijven met een IT-afdeling wordt aandacht besteed aan de kwetsbaarheid van hun informatie en hun ICT-infrastructuur. De mogelijke R&D-inspanning die ze zich hiertoe getroosten is intern gericht. De organisaties die te maken hebben met cybercrime, zitten in alle sectoren (banken, retail, transport en logistiek, petrochemie, etc) en hebben preventieve en repressieve applicaties (software-producten) nodig. Veel grote Accountantsbureau's en Management Adviesbureau's bieden diensten en producten aan ter bescherming tegen cybercrime. Er moeten echter robuustere applicaties komen.
2. Oplossingen, en dus nieuwe toepassingen moeten gevonden worden voor de te verwachten cybercrime:
 - Wireless Lan introduceert nieuwe bedreigingen voor beheer en nieuwe virusbedreiging. De wijze van besmetting wordt eenvoudiger, de bestrijding en detectie moeilijker. Een goede encryptie methodiek is noodzakelijk evenals heuristic detection

- de PDA, de pocket pc's. Een PDA gekoppeld aan een normale PC (al dan niet via het Wireless Lan) biedt voor een 'virusbakker' weer nieuwe mogelijkheden
 - bij de nieuwe generatie mobiele telefoons wordt het mogelijk zowel JPG als Word-documenten over te zetten
 - bij UMTS en nieuwe versies zullen nieuwe bedreigingen ontstaan voor bijv. mailverkeer
 - hoe intrusion aanvallen van binnenuit te detecteren en te traceren; vooralsnog richt men zich veelal op aanvallen van buiten
3. Procedureel en in de wetgeving moet nog veel geregeld worden. Cybercrime beperkt zich niet tot landsgrenzen. Daarom heeft in 2001 de Raad van Europa het Cybercrime Verdrag aangenomen met als doel het harmoniseren van de opsporing en de wetgeving mbt cybercrime binnen Europa en enkele landen daarbuiten (zoals Canada, de Verenigde Staten en Japan). De implementatie hiervan vraagt nog steeds veel aandacht, ook in Nederland. In de praktijk is zichtbaar dat bedrijven zich gaan verenigen en gaan samenwerken in de vorm van Computer Emergency Response Teams (CERT) om de 'gemeenschappelijke vijand' te bestrijden. Dit vergt veel organisatie.

Potentiële marksectoren:

- Particuliere internetgebruikers
- Retail
- Banking & financial services
- E-business
- Industry (Shell, Unilever, Philips)
- E-government
- E-procurement

Hoofdstuk 3. Overige terreinen van Safety & Security

Inleiding

In hoofdstuk 2 zijn de kansrijke deelgebieden binnen het Veiligheidssegment benoemd en uiteengezet. De veiligheidssector strekt zich verder uit en omvat ook andere onderwerpen die binnen dit onderzoek helaas als minder kansrijk worden beschouwd en derhalve niet zijn behandeld.

Toch springen twee terreinen in het oog die beslist als *high potential area's* kunnen worden aangemerkt binnen Veiligheid, maar die spijtig genoeg weinig of een matig actieve R&D-industrie in Nederland kennen. Het betreft de gebieden *Cryptografie* en *Radartechnologie*, die vanwege hun significante potentieel ook onder de loep zijn genomen.

Dit hoofdstuk zal afsluiten met een aantal uit de praktijk afkomstige, interessante uitspraken en percepties over *fysieke beveiligingssystemen*. Deze reflecties onderbouwen waarom sommige aspecten uit de keten van de fysieke beveiliging niet zijn genomineerd en zijn geselecteerd als zijnde kansrijke deelgebieden.

3.1 Cryptografie

Omschrijving:

"Cryptology is the study of mathematical techniques in order to provide secrecy, authenticity and related properties for digital information. Therefore it is a fundamental enabler for security in the Information Society. Cryptology is at the core of computer security, of secure data transmission over shared networks, of digital identification and digital signatures, etc. Its applications vary from e-commerce and on-line payment systems to mobile phone protocols. Cryptology also provides us with basic building blocks for privacy enhancing techniques, guarding the legitimate rights of individuals to privacy."

Kennispositie Nederland:

R&D-bedrijven: matig

In de wereld zijn de VS en Israël de grootste aanbieders van cryptografie.

In Nederland lijkt er een zeer beperkt aantal bedrijven te zijn wat aan cryptografisch onderzoek doet. De meeste organisaties die cryptografische algoritmes gebruiken, zoals banken en telco's, zijn vanzelfsprekend gesloten over hun onderzoek en verworvenheden in de cryptografie. Het enige wat men ziet van hen zijn verzoeken en opdrachten om cryptografische algoritmes te testen. De crypto industrie is zeer matig in Nederland. Voorheen bestond Philips Crypto die zich heel sterk richtte op militaire toepassingen (NAVO). Deze is echter een stille dood gestorven. Het Philips Crypto Competence Centre is verplaatst naar Duitsland (Hamburg). Alleen Philips Natlab heeft nog enige affiniteit met cryptografie vanwege hun onderzoek in copyright protection. Philips ziet nu wel veel mogelijkheden voor crypto in de consumenten-electronica. Andere bedrijven actief op crypto zijn SafeNet (voorheen Pijnenburg) waarvan de R&D-groep thans is opgeheven, Enschede/SDU (zeer beperkt) en ICT Consultants.

Academia : **veel!!**

Nederland is wetenschappelijk zeer sterk in cryptografie, smartcards en software verificatie. Specifiek crypto onderzoek vindt plaats aan de TU/e bij de onderzoeksgroep Coding & Cryptografie (Prof. Van Tilborg). Bij het CWI (dr. Te Riele) is men bezig een Crypto-groep op te starten. Daarnaast zijn de KUN (Prof. Jacobs – smartcards) en de UT (dr. Etalle) dragers van Nederlands crypto onderzoek. Verder bestaat het research-instituut EIDMA (Euler Institute for Discrete Mathematics and its Applications) wat aanvankelijk was opgezet door TU/e, UT en TUD. Ondertussen zijn tal van andere Nederlandse én Belgische en Duitse universiteiten aangesloten.

Industriële partners zijn: TNO, Philips en Nationaal Bureau voor Verbindingsbeveiliging. De research focus ligt oa op coding theory, information theory en cryptology.

Relaties met significant onderzoek:

BSIK - Bricks:

1. Basic Research in Informatics for Creating the Knowledge Society. Het strategische project Cryptographic methods (binnen het thema Parallel and Distributed computing): to study, improve and analyse existing algorithms and to develop new algorithms for the solution of the number-theoretic problems which underlie modern cryptosystems (CWI – dr. Te Riele)

KP5 - STORK

1. Strategic Roadmap for Crypto. Coordinator: Bart Preneel (Leuven).

KP6 – ECRYPT

1. European Network of Excellence in Cryptology (TU/e, Philips). Objectives: Strengthen security and enhance dependability of the information and communication systems and industry; development, testing and verification of underlying and novel crypto technologies for a wide spectrum of applications and of technologies for protecting, securing and trustable distribution of digital assets. Research areas: symmetric key algorithms, public key algorithms, protocols, implementation, watermarking.

Opportunities qua toepassingen:

Potentiële marktsectoren zijn: bancaire (Interpay) en financiële dienstverlening, telecom, e-business, defensie (Marine Inlichtingendienst, Nederlands Bureau voor Verbindingsbeveiliging), etc.

De KP5/6-projecten STORK en ECRYPT beschrijven tal van uitdagende onderwerpen en toepassingen (new trends in crypto, open problems in crypto) zoals:

- Nieuwe cryptografische algoritmes zijn nodig die kortere sleutellengtes en een gelaagde security toestaan. Voor draadloze applicaties zijn algoritmes nodig die minder rekenkracht en memory-eisen vergen. Cryptografische protocollen zijn nodig om de identiteit te controleren
- Anonimiseren bij Elektronisch betalen/stemmen
Anonimiteit is door elektronisch betalen zwaar achteruit gegaan. In Nederland zijn destijds door het CWI nieuwe technieken ontwikkeld voor het elektronisch betalingsverkeer (binnen de thans opgeheven spin-off Digicash). De technologie wordt nu gebruikt voor het elektronisch stemmen waarbij gecontroleerd wordt of de stem wordt meegeteld.

3.2 Radartechnologie

Opportunities qua toepassingen:

De radar wordt steeds goedkoper en heeft het voordeel dat het ook bij slechte weersomstandigheden is te gebruiken. Vanwege de lage kostprijs zijn nu ook micro-toepassingen ten behoeve van de veiligheid mogelijk, zoals in auto's: een intelligente cruise control zorgt ervoor dat de wagen niet alleen een constante snelheid aanhoudt, maar gebruikt radartechnologie om steeds een veilige minimumafstand met het voorste voertuig te bewaken. Daimler-Chrysler gebruikt technologie voor het veilig ontwerpen van auto's zodat eventueel geschepte voetgangers minimale schade krijgen.

Ook kunnen sensoren in combinatie met een intelligent camerasysteem uitgerust worden met radartechnologie.

De low-cost radartechnologie kan dan dingen zichtbaar maken die normaal moeilijk zichtbaar zijn (early warning van epileptische aanvallen door de afwijkende bewegingen te detecteren). Andere toepassingsmogelijkheden op het gebied van veiligheid zijn: het voorkomen van botsingen, het begeleiden van verkeer en vervoer, het onderzoeken van containers, utility location, road and airport runway inspection, avalanche victim search (via ground penetrating radar), the impact of the atmosphere on the quality of telecommunications links, etc.

Kennispositie Nederland:

R&D-bedrijven: matig

In de wereld is de VS toonaangevend. De Nederlandse R&D-industrie is matig. In Nederland zijn er relatief veel kleine spelers (Prime Vision) die ad-hoc dingen doen en weinig aan zelscheppend onderzoek of product vernieuwing doen. Daarnaast zijn er een paar grote (Thales, Volker Wessel Stevin, Philips, etc) die verantwoordelijk zijn voor al het Nederlands onderzoek in radartechnologie.

Academia : veel!!

Nederland heeft sinds WWII van beginaf aan een vooraanstaande rol gespeeld op het gebied van de ontwikkeling van geavanceerde radartechnologie. Bij TNO-FEL is veel radarkennis aanwezig.

Nederland heeft volgens een internationaal onderzoek de hoogste kennispositie in de wereld. (Aan Nederland werd als cijfer een 9 gegeven, boven de VS en Israel).

Binnen de TUD (Prof. Ligthart) is de internationale IRCTR opgezet - International Research Centre for Telecommunications-transmission and Radar – met een research focus op Radar. In het bijzonder zijn er de onderzoeksthema's radar design technology, radar networks, radar navigation en integrated radar-communication.

In 2002 is het Platform Nederland Radarland opgericht. Dit Platform wordt gevormd door TNO-FEL, TUD, Thales Nederland en de ministeries van Economische Zaken en Defensie.

3.3 Fysieke beveiligingssystemen (algemeen)

Omschrijving:

De basis van een fysiek beveiligingssysteem is dat verschillende sensoren in de vorm van bewegingsmelders, deur- en raamcontacten, glasbreukmelders etc. middels bekabeling verbonden zijn met een centrale unit, welke bij alarm een sirene doet afgaan en/of doormelding verzorgt naar bijv. een alarmcentrale. Traditioneel kent een beveiligingssysteem een eigen infrastructuur met eigen kabels en eigen protocollen voor de communicatie tussen sensoren en centrale unit. Pas na de centrale unit wordt gebruik gemaakt van de publieke communicatie-infrastructuur voor de alarmoverdracht middels een analoge telefoonlijn, een digitale ISDN-verbinding of een X25-verbinding van centrale unit naar de alarmcentrale.

Kennispositie Nederland:

Omzet Nederland binnen de beveiligingsbranche (brand, inbraak, overval) dd 2001: €546 miljoen, met verwachte groei van 12% voor 2002.

Vrager van technologie: Group4Falck (Deens). Zij zijn een toepasser van bestaande technologie (één van de grootste beveiligingsorganisaties in de wereld). Zij zien niet in waarom Nederland zelf zou moeten ontwikkelen (opnieuw het wiel uitvinden). Nederland is goed in het bedenken van oplossingsconcepten: slimme combinaties van mensen en middelen.

De marktleiders in Nederland qua het aanleveren van systemen, ontwikkelen de technologie ook niet zelf. In sommige landen is beveiligingspersoneel goedkoop, en zijn er geen slimme technologieën nodig. In Nederland daarentegen zijn de loonkosten hoog, en moet dus slim omgegaan worden met bestaande kennis.

Aanbieders van technologie:

Cisco (US R&D) leading supplier of (wireless) networking equipment	Momenteel is de veiligheidsmarkt een traditionele markt met veel gebruik van bestaande technologieën. Er zijn veel applicaties die op een eigen infrastructuur draaien, dus zijn er veel verschillende infrastructuren. Zo langzamerhand wil Cisco de markt sturen in de richting van IP-technologie. De trend moet zijn convergentie van die infrastructuren. Hun visie is dat alles zal convergeren naar 1 protocol, nl volgende versies van het IP-protocol. Men streeft naar 1 generiek netwerk waarop alle applicaties kunnen draaien. Cisco ontwikkelt technologie om applicaties aan elkaar te knopen. Ze werken samen met grote partners om dit te bereiken (Axis)
Conesco (NL, 13 RD) digitaal per ISDN doorsturen van video, geluid en data	<ul style="list-style-type: none"> • In de markt bestaat er een wirwar van aanbieders van (veelal buitenlandse) ontvangstations, architectuur en bedieningssystemen. Er zijn zeer veel installateurs van producten. Deze vragen woekerprijzen (vaak 4-voud van de kostprijs van een product) omdat ze weten dat er voldoende vraag is. Dus de installateurs hebben alle macht! Hoe de afhankelijke positie van de installateur uitschakelen? • IP-technologie heeft de toekomst, ook voor de fysieke beveiliging.
TNO-FEL	<p>Installateurs zijn 'dozenschuivers' en verkopen producten door. Ze ontwikkelen zelf geen technologie, maar integreren hooguit. Ze hebben de verplichting om veiligheid te garanderen en kopen dus van alles in (ook technologie uit het buitenland).</p> <p>Bij beveiligingsorganisaties zoals Group4Falck is weinig geld voor R&D. De concurrentie is scherp en de marges zijn laag. Bovendien wordt er per door de surveillant gereden kilometer betaald, en is men dus niet zo geïnteresseerd in technologieverbetering (om minder te hoeven uit te rijden). Ook al heeft technologie een toegevoegde waarde voor efficiëntie en betrouwbaarheid, economisch gezien is het onaantrekkelijk.</p>
Tethys (NL, klein R&D)	Toekomst moet zijn ketenintegratie . Nu zijn de meeste partijen bezig op componentenniveau, en kopen componenten en technologie standaard in. Er zijn veel faalmomenten in de keten van plaatsbepaling. Het grootste probleem voor een klein bedrijf is om volume te creëren (marketing).
Lobeco (NL, 80D) belangrijkste leverancier van elektronische beveiligingsapparatuur. Distributeur en halen hun systemen uit de hele wereld	Markt voor beveiligingssystemen wordt gedomineerd door grote multinationals, zoals Honeywell, Siemens, Bosch, GE, etc. Israël met 1 van de grootste beveiligingsindustrieën (zware overheidssubsidie) levert veel producten, daarnaast Amerika, Frankrijk en Duitsland. De prijzen van electronica in de beveiligingssystemen gaan omlaag. Dus het gaat om de aantallen. Wil een bedrijf rendabel zijn dan moet het flinke aantallen produceren en zich richten op de hele wereld als afzetmarkt. Vandaar dat slechts de grote multinationals het goed doen. Voor kleine Nederlandse bedrijfjes is het niet aantrekkelijk om zelf R&D te doen om eigen producten te leveren. Er zijn er maar een paar: Alphatronics, Aritech, ASB, Telesignaal.
Alphatronics (NL, 5R&D) ontwikkeling en verkoop elektronische beveiligingscentrales en apparatuur.	<ul style="list-style-type: none"> • Voor Nederlandse bedrijven die willen beginnen met de ontwikkeling en productie van beveiligingssystemen zal het lastig zijn. Er is veel concurrentie met het buitenland, met name met de zuidoostasiatische lagelonenlanden die goedkoop kunnen produceren. In Israël en Zuid-Afrika is de beveiligingstak zeer bloeiend vanwege de onveilige situatie aldaar, dus zorgt deze tak voor een bloeiende economie. • De universiteiten leveren iha weinig input aan het bedrijfsleven, ze geven slechts de globale lijnen aan hoe zaken zich zouden kunnen bewegen binnen de beveiligingsmarkt. De bedrijven maken concrete producten die directe behoeften moeten invullen. Ze richten zich op de oude vertrouwde markten, en durven niet in nieuwe marktgate te springen. Subsidie zou helpen om ook over de grenzen nieuwe markten (Europa) aan te boren.

Almende (NL,R&D) incident-
en calamiteitenmanagement

- In Nederland zijn er geen echte technologie-aanbieders, Nederland moet het hebben van manufacturing voor de manufacturing. Dus er moet geïnvesteerd worden in technology transfer vanuit de universiteiten, die veel kennis hebben. Almende constateert een verhoogde belangstelling voor en vanuit de gezondheidszorg.
- Binnen beveiligingsorganisatie is er een groot verloop bij bewakingspersoneel en zijn er geen goede garanties voor de kwaliteit van de integriteit van het personeel (sommige beveiligers hebben zelf criminele tendencies). Dus noodzaak voor Certificering van beveiligingsfirma's. (De politie zou de waarborgen kunnen afgeven en de vertrouwensrating in kaart kunnen brengen).

BIJLAGE I : Lijst betrokken bedrijven, kennisinstellingen, instituten

KENNISINFRASTRUCTUUR

INSTELLING	BETROKKEN ONDERDEEL/PERSOON
TNO	<ul style="list-style-type: none"> • Maatschappelijke Veiligheid - Ir. Schulein • FEL - dhr. vd Heuvel (waarneming), dhr. Van ES (smart sensor), dhr. Vink • TPD - dhr. Verschuren, Ir. Huizenga, dhr. Baan • Telecom - Prof. J. Bruijning, dhr. Albeda, dhr. Den Hartog • Technische Menskunde - dr. Post • ITSEF - dhr. Out
TUD	<ul style="list-style-type: none"> • Geodesie/GIS-technology - Prof P. van Oosterom • IRCTR radartechnieken - Prof. Ligthart • Patroonherkenning - Prof. Van Duin • Digital Video Processing - Prof. I. Lagendijk, Prof. Biemond • Security in banking - Prof. Van der Lubbe, ir. Verbree • TBM, sectie Veiligheidskunde– Prof. Wagenaar, Prof. Hale, Prof. Ale • Decis lab
TU/e	<ul style="list-style-type: none"> • Patroonherkenning Signal processing/Watermarking - Prof. Kalker • Coding & Cryptography - Prof. van Tilborg, Dr. Schoenmakers • Computer System Security – Dr. Mauw • Formele Methoden - Prof. Baten
UTwente	<ul style="list-style-type: none"> • Distributed systems/watermarking - Prof. Hartel, Dr. Etalle • Signals & systems - Prof. Slump, dr. Veldhuis
VU	<ul style="list-style-type: none"> • Distributed systems - Prof. Tanenbaum, Dr. Crispo • Mobiele GIS - Prof. Scholten • Spinlab: interfaculty laboratory for spatial IT - Prof. Beinat
UvAmsterdam	<ul style="list-style-type: none"> • Intelligent Autonomous Systems - Prof. Groen • Business Studies - Prof. Jagers
KUN	<ul style="list-style-type: none"> • Security in systems/Smartcards – Prof. Jacobs, Prof. Hoekman • Strafrecht/Digitaal rechercheren – Prof. Buruma
UvUtrecht	<ul style="list-style-type: none"> • Spatial information retrieval – dr. Kreveld • Automated camera motions - Prof. Overmars
CWI	<ul style="list-style-type: none"> • Signal & Imaging (Biometrie) – dr. Schouten • Security in Embedded Systems – prof. W. Fokkink
Mediamill	Applicatiecentrum voor multimediaoplossingen (TNO/UVA) - dr. Worring

PRIVATE SECTOR

A

ABB
ADT Security
AET
Aladdin
Alphatronics
Almende
anite
Aritech
ASB
ASR
AtosOrigin
Axis Communications

B

B&G Hekwerk
Bhold Company
Bosch Security

C

CapGemini E&Y
Chess
Chubb Lips
Cisco
CityGis
CNI Europe
Computer Associates
Controlware
Conesco
Consul Risk Management
Cross Point

D

Dacolian
Dartagnan
Deloitte & Touche
De Nederlandse Bank
Dialog ID
DMDSecure
DTO
DVS

E

Emexus
Enai
Ernst & Young
ESRI Nederland

F

Fox-IT

G

Geodan
Getronics
Group4Falck

H

Heras
Honeywell

I

IBM
IE Keyprocessor
Infosave
Infopulse electronic commerce
Initial Varel Security
Interpay
Irdeto Access

J

Johan Enschedé/SDU

K

Kahuna
KPMG

L

Lobeco
LogicaCMG

M

Meldkamer Holland

N

NCP
Nedap
NSecure

O

Ordina

P

Philips
Pijnenburg
Pinewood Automatisering
Pink Roccade
Pre ned
Prime Vision

Q

Quint, Redwood, Wellington

R

Railinfrabeheer
Ram Mobile Data
Ricas
RSA Security

S

SafeNet
Securicor
Securitas
Shell Chemicals
Siemens
Sogeti
Sound Intelligence
Stichting Smarthomes
Stork WorkspHERE
Symantec

T

Telesignaal
Telindus
Tensing SKS
Tethys
Thales
The VisionWeb
Tridion
Tyco

U

Ubizen

V

Van Ovost automatisering
VCS International
Vitelec
Vodafone
VPB

Z

Zenitel