Technologie-verkenning Nationale Veiligheid

Technologie-verkenning Nationale Veiligheid

Technologieverkenning Nationale Veiligheid

Een verkenning van kansen en dreigingen van technologische ontwikkelingen voor de nationale veiligheid

Analistennetwerk Nationale Veiligheid
Ir. P.J. van Vliet (editor, TNO)
Dr. M.G. Mennen (editor, RIVM)

Colofon

Deze studie is uitgevoerd door TNO, partner in het Analistennetwerk Nationale Veiligheid. Een groot aantal experts van het Analistennetwerk Nationale Veiligheid en andere organisaties heeft meegewerkt.

Het Analistennetwerk Nationale Veiligheid is een consortium van:
Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael'
Erasmus Universiteit Rotterdam, Institute of Social Studies (ISS)

Contcact: drs. C.W. d'Huy (TNO)

Projectnummer: E/609042/13

Inhoud

Management-samenvatting

Achtergrond

De nationale veiligheid is in het geding als vitale belangen van de Nederlandse staat en/of samenleving zodanig worden bedreigd dat sprake is van potentiële maatschappelijke ontwrichting. Met de strategie nationale veiligheid wil de Rijksoverheid voorkomen dat zulke ontwrichting optreedt, als gevolg van een ramp, dreiging of crisis. Of - wanneer zich toch een ramp of crisis voordoet - daar zo goed mogelijk op reageren, opdat de gevolgen beperkt blijven. Als onderdeel van de strategie worden rampen en crises, die potentieel kunnen voortvloeien uit het optreden van bepaalde onderkende risico's, uitgewerkt in de vorm van scenario's. Deze worden vervolgens langs een vaste 'meetlat' gelegd.
Bij de vaststelling van thema's en onderwerpen voor de Nationale Risicobeoordeling (NRB) 2012 heeft de Stuurgroep Nationale Veiligheid besloten om het thema 'nieuwe technologieën' binnen de Strategie Nationale Veiligheid verder uit te werken, maar daartoe eerst een verkennende studie te laten verrichten. Deze studie moet inzicht geven in technologische ontwikkelingen en toepassingen daarvan die de komende vijf jaar kansen en/of dreigingen voor de nationale veiligheid met zich mee kunnen brengen.

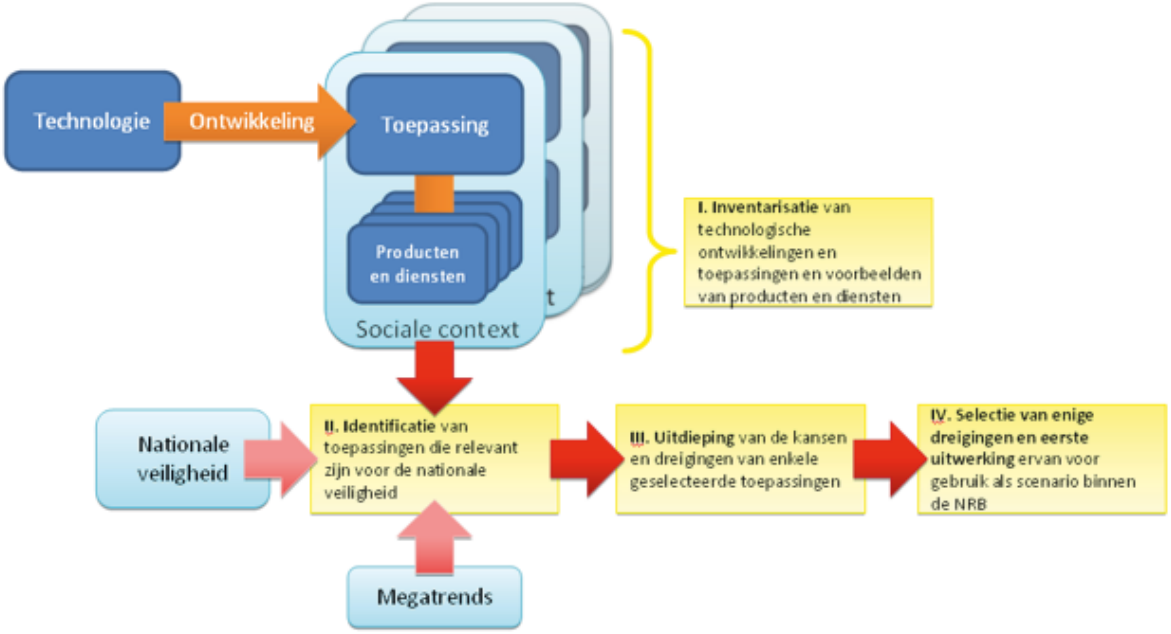
Doelstelling en werkwijze

Technologische ontwikkelingen, en vooral de daaruit voortkomende toepassingen, bieden enerzijds kansen voor het versterken van capaciteiten om onze samenleving beter bestand te kunnen laten zijn tegen grootschalige rampen, crises en dreigingen (de scope van de nationale veiligheid). En daarmee ook het versterken van de weerbaarheid tegen maatschappelijke ontwrichting. Anderzijds kunnen technologische ontwikkelingen en hun toepassingen een dreiging vormen voor de nationale veiligheid.
De doelstelling van deze verkennende studie is het op hoofdlijnen inzicht verschaffen in technologische ontwikkelingen en de aan hun toepassing verbonden kansen en dreigingen voor de nationale veiligheid.

In deze verkenning zijn de volgende technologiegebieden beschouwd:
- Nanotechnologie;
- Bio- / gentechnologie;
- Neurotechnologie;
- Materiaaltechnologie;
- Informatietechnologie.

Daarnaast is kort aandacht besteed aan 'convergerende technologieën', het bij elkaar komen van verschillende technologische ontwikkelingen, en aan energietechnologie.

Figure I: Schematisch overzicht van de gevolgde werkwijze.



De gevolgde werkwijze bestaat uit vier stappen, weergegeven in Figuur I.

- I. In de eerste stap is door middel van interviews en literatuurstudie een brede inventarisatie gemaakt van toepassingen van technologische ontwikkelingen, ter illustratie aangevuld met voorbeelden van producten en diensten.
- II. Vervolgens zijn met en door een brede groep experts toepassingen geïdentificeerd die - in positieve of negatieve zin - relevant worden geacht voor de nationale veiligheid. Daarbij is onder andere gebruik gemaakt van de omschrijvingen van de vitale belangen en de capaciteitenlijst uit de Strategie Nationale Veiligheid en een overzicht van megatrends en maatschappelijke ontwikkelingen.
- III. In de derde stap zijn de - met het oog op de nationale veiligheid - meest relevante toepassingen geselecteerd voor nadere uitdieping. Die uitdieping bestaat uit het beoordelen van de aan deze toepassingen verbonden kansen en dreigingen en hun potentiële impact op de nationale veiligheid.
- IV. In aanvulling op bovenstaande stappen is een selectie gemaakt van dreigingen die in aanmerking komen voor uitwerking in een mogelijk scenario binnen de NRB.

Conclusies

Geselecteerde toepassingen

De in tabel I aangegeven toepassingen zijn-met het oog op de nationale veiligheid- het meest relevant.

Tabel I: Meest relevante toepassingen.

Toepassingen	Korte omschrijvingen
Nano- en micro-elektro-mechanische systemen (NEMS/MEMS)	Miniaturisering heeft ertoe geleid dat sensoren en actuatoren steeds kleiner en soms goedkoper kunnen worden geproduceerd. Dit biedt nieuwe mogelijkheden voor het toepassen van NEMS en MEMS (respectievelijk nano- en micro-elektromechanische systemen).
Nanomaterialen	Materialen krijgen op nanoschaal andere eigenschappen. Met de kennis die nu wordt ontwikkeld kunnen aan materialen steeds meer gecontroleerd bepaalde eigenschappen worden meegegeven. De bij deze toepassing geïdentificeerde producten die mogelijk invloed hebben op de nationale veiligheid, zijn nanodeeltjes in wapens (zoals een vuile bom) en nanomaterialen ingezet voor identiteitsmanipulatie.
DNA methodieken	Technologische ontwikkelingen hebben het mogelijk gemaakt om met minder en andersoortig materiaal, steeds sneller en goedkoper, een completer DNA profiel te vergaren. Efficiëntere DNA methodieken bieden mogelijkheden voor identificatie van personen.
Sensoren	Ontwikkelingen op de gebieden van materiaal-, bio- en nanotechnologie zorgen ervoor dat meer typen en kleinere sensoren beschikbaar komen - die meer verschillende dingen, beter kunnen meten - en dat sensoren goedkoper worden. Geïdentificeerde nieuwe producten en diensten hebben met name betrekking op het koppelen van verschillende sensordatastromen. In het geval van '*crowdsourcing*' van sensoren worden verschillende sensoren die in het bezit zijn van individuen of organisaties, samen voor een specifiek doel ingezet.
Energieopslag	De uitputting van fossiele brandstoffen en milieuproblemen zijn de drijvende krachten achter transformaties in de energieketen. Een voorwaarde om stappen te maken naar gebruik van meer natuurlijke energiebronnen is de ontwikkeling van nieuwe manieren van energieopslag.
3D *printing*	3D *printing* maakt het mogelijk driedimensionale producten, waaronder gebruiksvoorwerpen, te produceren. Daarvoor zijn alleen een 3D printer, basismaterialen en data met de 'bouwtekening' benodigd.
Robotica voor veiligheid	Technologische ontwikkelingen - onder meer op het gebied van informatietechnologie - leveren de bouwstenen voor verdere ontwikkeling van intelligente en slimme robots. Deze robots kunnen worden ingezet ten behoeve van de veiligheid. Bijvoorbeeld voor het verrichten van inspecties in voor de mens gevaarlijke omgevingen of voor het uitvoeren van surveillances.
Big data, open data	De hoeveelheid data die dagelijks gecreëerd wordt, groeit exponentieel. Data wordt in toenemende mate open aangeboden. Met veel verwerkingscapaciteit en/of slimme methodieken is er de mogelijkheid informatie te extraheren uit de zeer grote hoeveelheden ongestructureerde data.
Internet of things	Technologische ontwikkelingen op het gebied van informatietechnologie leiden er toe dat ook steeds meer 'dingen' - zoals apparaten, infrastructuur en voertuigen - via internet worden verbonden en gegevens met elkaar kunnen uitwisselen.

Tabel II: Geïdentificeerde toepassingen met indicatie van kansen en dreigingen.

Technologie	Toepassingen	Kansen	Dreigingen
Nanotechnologie	Nano- en micro-elektromechanische systemen (NEMS/MEMS)	Gebruik voor communicatie, monitoring en observatie	Communicatie, monitoring en observatie door 'kwaadwillenden'
	Nanomaterialen	Verbeteren hulpmiddelen veiligheidsdiensten	Gebruik in wapens, schadelijke stoffen
Bio- / gentechnologie	DNA methodieken	Identificatie van personen	Misbruik van DNA data
Neurotechnologie	--	--	--
Materiaaltechnologie	Sensoren	Inzicht in wat in omgeving gebeurt, voorspellend vermogen	Gemanipuleerde of onjuiste data
	Energieopslag	Continuïteit energievoorziening	--
Informatietechnologie	3D *printing*	Printen van hulpmiddelen en reserveonderdelen	Ondermijning gereguleerde producten (o.a. wapens)
	Robotica voor veiligheid	Surveillance en inspectie	Explosieven of gif op een bepaalde plaats brengen
	Big data, open data	Informatiepositie versterken	Manipulatie of misbruik door derden
	Internet of things	Monitoren van trends en objecten	Grootschalige uitval, manipulatie en misbruik

Kansen en dreigingen

Tabel II geeft voor de geselecteerde toepassingen een globaal overzicht van de kansen en dreigingen met mogelijke impact op de nationale veiligheid.

Convergerende en overige technologieën

Naast de ontwikkelingen binnen de eerder genoemde technologieën zijn convergerende technologieën (*converging technologies*) van belang. Dit behelst het bij elkaar komen van verschillende technologische ontwikkelingen, zoals de zogenaamde NBIC-convergentie waarbij ontwikkelingen in nanotechnologie, biotechnologie, informatietechnologie en cognitieve technologie samenkomen. Verder zijn technologische ontwikkelingen op het gebied van energie (waaronder decentralisatie, duurzame energiebronnen, herwaardering bestaande technologieën) relevant voor de nationale veiligheid. Ontwikkelingen op dit gebied komen deels aan de orde bij de hierboven genoemde technologieën. Deze ontwikkelingen bieden kansen in ecologische en geopolitieke zin: zij verhogen de duurzaamheid en zorgen mogelijk voor minder afhankelijkheid tussen landen. Door ontwikkelingen op het gebied van energietechnologie kan de afhankelijkheid van - relatief schaarse - fossiele brandstoffen minder worden en daarmee de sterke afhankelijkheid van politiek instabiele landen of landen die hun machtspositie soms uitbuiten.

Selectie van dreigingen voor een mogelijk scenario binnen de NRB

In de NRB worden - aan de hand van scenario's - rampen, dreigingen en crises geanalyseerd die in potentie een dreiging kunnen vormen voor de nationale veiligheid. 'Hyperconnectiviteit' door de toenemende verwevenheid van systemen vormt een risico. Vitale processen en systemen raken steeds verder verknoopt, zowel onderling als met niet-vitale processen en systemen. De systeemsamenhang wordt complex. Eén kleine verstoring kan verstrekkende - van te voren onbekende - consequenties hebben, die in vele andere systemen doorwerken. Hyperconnectiviteit kan de nadelige effecten van technisch falen, menselijke fouten en moedwillige verstoringen versterken. Een ander risico is dat (een aantal) technologische ontwikkelingen en hun maatschappelijke impact moeilijk controleerbaar zijn, doordat de ontwikkelingen autonoom lijken te verlopen, met name waar het gaat om convergerende technologieën. Het is moeilijk toezicht en grip te houden op deze ontwikkelingen.
Omdat juist in de connectiviteit en convergentie van technologieën een potentieel risico wordt gezien, is het aan te bevelen een aantal van de toepassingen NEMS/MEMS, sensoren, *internet of things*, *big data*, *open data* in één scenario te combineren. In een dergelijk scenario staat de verstoring van vitale processen, systemen of diensten waarin (een aantal van) deze toepassingen worden gebruikt centraal.
Om het scenario niet te breed te maken wordt aanbevolen een selectie te maken voor één specifieke sector of één specifiek toepassingsgebied, bijvoorbeeld de energiesector of het gebruik van diverse sensoren voor monitoring door bedrijven of overheid.

1 Achtergrond en doelstelling

1.1 Aanleiding

De nationale veiligheid is in het geding als vitale belangen van de Nederlandse staat en/of samenleving zodanig worden bedreigd dat sprake is van potentiële maatschappelijke ontwrichting. Met de strategie nationale veiligheid wil de rijksoverheid voorkomen dat zulke ontwrichting optreedt, als gevolg van een ramp, dreiging of crisis. Of - wanneer zich toch een ramp of crisis voordoet - daar zo goed mogelijk op reageren, opdat de gevolgen beperkt blijven. Als onderdeel van de strategie worden rampen en crises, die potentieel kunnen voortvloeien uit het optreden van bepaalde onderkende risico's, uitgewerkt in de vorm van scenario's. Deze worden vervolgens langs een vaste 'meetlat' gelegd. Deze activiteit wordt uitgevoerd door het Analistennetwerk Nationale Veiligheid (ANV), in opdracht van de Stuurgroep Nationale Veiligheid (SNV).

De Taakgroep van het ANV heeft in haar advies [24] over de thema's en onderwerpen die in aanmerking komen voor de Nationale Risicobeoordeling (NRB) 2012 geadviseerd om het thema 'nieuwe technologieën' binnen de Strategie Nationale Veiligheid verder uit te werken. De Stuurgroep Nationale Veiligheid (SNV) en de Interdepartementale Werkgroep Nationale Veiligheid (IWNV) hebben ervoor besloten om daartoe eerst een verkennende studie te laten verrichten. Deze studie moet inzicht geven in technologische ontwikkelingen en toepassingen daarvan die de komende vijf jaar kansen en/of dreigingen voor de nationale veiligheid met zich mee kunnen brengen. De NCTV/Directie Dreigingen en Risico's van het ministerie van Veiligheid en Justitie treedt op als opdrachtgever.

Binnen deze verkennende studie gaat het om technologische ontwikkelingen, en vooral de daaruit voortkomende toepassingen, die enerzijds kansen bieden voor het versterken van capaciteiten om onze samenleving beter bestand te kunnen laten zijn tegen grootschalige rampen, crises en dreigingen (de scope van de nationale veiligheid). En daarmee ook het versterken van de weerbaarheid tegen maatschappelijke ontwrichting. Anderzijds gaat het om technologische ontwikkelingen en hun toepassingen die in zichzelf een dreiging kunnen vormen voor de nationale veiligheid (zie ook paragraaf 1.4).

1.2 Doelstelling

De doelstelling van deze verkennende studie is het op *hoofdlijnen* inzicht verschaffen in technologische ontwikkelingen en de aan hun toepassing verbonden kansen en dreigingen voor de nationale veiligheid. Daarmee wordt een bijdrage geleverd aan de inhoudelijke voorbereiding van de (beleids)keuzes ten aanzien van bepaalde technologische ontwikkelingen en hun toepassingen (i) die kansrijk zijn voor verbeteringen in de nationale veiligheid of (ii) waarvan juist een dreiging uitgaat voor de nationale veiligheid.

Deze studie is *verkennend* omdat 'technologie' een zeer breed terrein betreft met veel verschillende ontwikkelingen, elk met een eigen dynamiek en specifieke aspecten. Het doel is niet een volledig en diepgaand inzicht in alle technologieën en hun gevolgen te geven, maar wel een breed overzicht op hoofdlijnen, aangevuld met een verdere verdieping van die technologische ontwikkelingen en toepassingen die relevant worden beschouwd voor de nationale veiligheid.

Deze studie beoogt verder in de behoefte van de NCTV aan een actualisatie en verbreding op dit onderwerp ten opzichte van de studie naar kansen en dreigingen van (toepassingen van) technologische ontwikkelingen voor contra-terrorisme en bewaken & beveiligen uit 2011 [1] te voorzien. De resultaten kunnen tevens gebruikt worden om richting te geven aan een specifieke uitwerking van één of meer dreigingen in de vorm van een scenario voor de Nationale Risicobeoordeling (NRB).

1.3 Scope en focus

De scope, focus en het begrippenkader van de studie worden hieronder toegelicht.

Technologieën

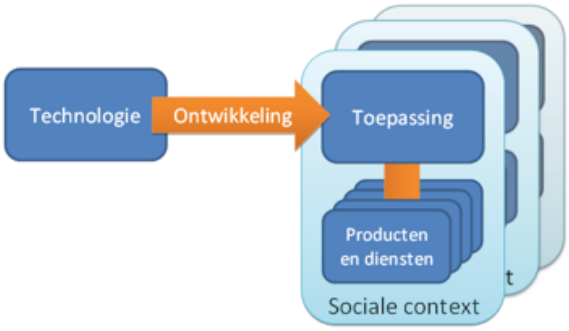
In deze verkenning worden - zoals afgesproken met de opdrachtgever - de **technologische ontwikkelingen** beschouwd volgens de indeling van de voorgaande NCTV-technologiestudie [1]:

- Nanotechnologie;
- Bio- / gentechnologie;
- Neurotechnologie;
- Materiaaltechnologie;
- Informatietechnologie.

Technologische ontwikkelingen, toepassingen en producten en diensten

De studie richt zich op de **technologische ontwikkelingen** én de **toepassingen** daarvan binnen de bovengenoemde technologieën. Toepassingen worden niet alleen beschouwd omdat zij feitelijk 'beeld en geluid' bieden bij veelal moeilijk te doorgronden technologische ontwikkelingen, maar ook omdat mogelijke kansen en dreigingen vooral zijn gerelateerd aan de toepassingen en niet zozeer aan de technologische ontwikkelingen zelf. Toepassingen van technologische ontwikkelingen worden met behulp van concrete **producten en diensten** gerealiseerd (d.w.z. in gebruik genomen). Waar mogelijk worden in dit rapport concrete producten en diensten als voorbeelden gebruikt van manieren waarop een technologie toegepast kan worden.

Figuur 1: Technologische ontwikkelingen vinden plaats vanuit de technologieën. Deze leiden tot toepassingen die via verschillende concrete producten en diensten in verschillende sociale contexten operationeel (d.w.z. feitelijk gebruikt) kunnen worden.



Voorbeeld *om de verschillen tussen technologische ontwikkeling, toepassing en product/dienst duidelijk te maken:*
Een technologische ontwikkeling in de informatietechnologie is intelligente en slimme robots. Een toepassing van deze ontwikkeling is robotica: robots die worden ingezet voor het monitoren of verbeteren van bijvoorbeeld de veiligheid. Een product dat daaruit voort komt is de *surveillance bot:* een robot of *drone* die surveilleert.

Een belangrijke factor bij toepassingen van technologische ontwikkelingen zijn de verschillende gebruikersgroepen van een technologie. Naast de technische dimensie van een toepassing is er dus ook een sociale context: binnen verschillende gebruikersgroepen wordt technologie op verschillende wijze, positief dan wel negatief, gebruikt waardoor zij hun eigen toepassingen creëren.

Nationale Veiligheid

De verkenning vindt plaats binnen het kader van de Strategie Nationale Veiligheid. De **nationale veiligheid** is in het geding als vitale belangen van de Nederlandse staat en/of samenleving zodanig worden bedreigd dat sprake is van potentiële maatschappelijke ontwrichting. De vitale belangen zijn: territoriale, fysieke, economische en ecologische veiligheid alsmede sociale en politieke stabiliteit [15]. Toepassingen van technologische ontwikkelingen (of direct van de eraan ten grondslag liggende technologie) kunnen een kans vormen maar ook een dreiging, afhankelijk van de aard van het gebruik.

Onder **kans** wordt verstaan het gebruik van een toepassing (en daarmee van de eraan ten grondslag liggende technologische ontwikkeling of technologie) dat leidt tot het versterken van capaciteiten om negatieve effecten op het niveau van de nationale veiligheid te verminderen of te

voorkomen of om de weerbaarheid tegen negatieve effecten te verhogen.

***Voorbeeld** van een kans:*
Robots die worden ingezet voor het monitoren of verbeteren van de veiligheid zijn een kans voor de nationale veiligheid omdat het de mogelijkheid biedt voor hulpdiensten om surveillance automatisch en op afstand uit te laten voeren in moeilijke of gevaarlijke omstandigheden.

Onder **dreiging** verstaan we het gebruik of misbruik van een technologische toepassing (en daarmee van de eraan ten grondslag liggende technologische ontwikkeling of technologie) dat leidt tot een aantasting van de (vitale belangen van de) nationale veiligheid of verslechtering van de weerbaarheid daartegen.
Bij de analyse van de dreigingen voor de nationale veiligheid wordt gekeken naar zowel opzettelijk misbruik als onbewust menselijk handelen of systeemfalen. Ook directe onbedoelde effecten (bijvoorbeeld mogelijk negatieve lange termijn effecten) worden beschouwd.

***Voorbeeld** van een dreiging:*
Robots die op afstand taken kunnen uitvoeren zijn een dreiging voor de nationale veiligheid wanneer deze door kwaadwillende personen worden ingezet om een aanslag te plegen.

Tijdshorizon

Wat de **tijdshorizon** van de verkenning betreft, worden technologische ontwikkelingen beschouwd die toepassingen opleveren die binnen een termijn van vijf jaar operationeel kunnen zijn. Daarnaast worden ook lange termijn technologische ontwikkelingen beschouwd, die binnen een termijn van vijf jaar vragen om beleidskeuzes.

1.4 Kansen en dreigingen - algemene opmerkingen

Voor de toepassingen van technologische ontwikkelingen geldt een aantal opmerkingen over kansen en dreigingen in het algemeen. Deze kansen en dreigingen worden hieronder genoemd en zullen, tenzij daarvoor een specifieke reden is, niet meer bij de behandeling van de afzonderlijke technologieën worden herhaald.

Iedere technologische toepassing is potentieel kwetsbaar voor falen of kan (bewust of onbewust) door menselijke handelen verstoord raken. Zeker wanneer een toepassing op grote schaal wordt gebruikt, wordt ingezet in vitale processen of een cruciale rol speelt in het functioneren van andere toepassingen - en dus de afhankelijkheid ervan groot is - is het ongestoord functioneren van een toepassing van groot belang. Het falen, uitval of verstoring kan dan resulteren in uiteenlopende vormen van schade. Bij de inzet van een technologische toepassing moet hier zeker rekening mee worden gehouden. Veelal zijn maatregelen wenselijk voor het geval zich dit voordoet, bijvoorbeeld door dubbele uitvoering van een technologie of adequate beveiliging. In deze technologieverkenning is deze kwetsbaarheid in combinatie met afhankelijkheid alleen expliciet als dreiging benoemd, wanneer daarvoor specifieke argumenten gelden.

Eenzelfde opmerking geldt voor duaal gebruik van een technologische toepassing: een technologie kan ten goede worden ingezet of ten kwade. Zo gebruiken hulpverleners bijvoorbeeld smartphones, maar gebruiken ook criminelen deze voor hun criminele activiteiten. In deze technologieverkenning wordt bij zowel kansen als dreigingen volstaan met deze algemene opmerking. Alleen in het geval dat er een specifieke vorm van gebruik (kans) als misbruik (dreiging) valt te onderkennen, is deze expliciet benoemd.

Verder geldt in algemene zin dat een technologische toepassing zowel voor- als tegenstanders zal kennen. Zeker bio-, neuro, informatie- en nanotechnologie beïnvloeden of gebruiken fundamentele bouwstenen: genen (bouwsteen voor erfelijk materiaal), neuronen (lichaamsdeel behorend tot belangrijkste elementen van het zenuwstelsel), bit of byte (eenheid van informatieopslag, -verwerking en –transport) en moleculen of atomen op nanoschaal (bouwsteen voor materialen, vloeistoffen, etc.). Volgens sommigen sleutelt de mens daarmee aan de schepping en ook lang niet altijd is te doorzien wat op voorhand de mogelijke gevolgen zijn van ontwikkelde toepassingen. Dit mogelijk controversiële karakter van een nieuwe technologie kan leiden tot een felle ethische en/of maatschappelijke discussie, (forse) maatschappelijke weerstand of in uitzonderlijke gevallen zelfs tot extremistische of terroristische activiteiten. Voordat een discussie echter een dreiging vormt voor de nationale veiligheid, moet er wel heel wat gebeuren. In het geval van extremisme en terrorisme ligt dat uiteraard anders en wanneer daar aanwijzingen voor zouden zijn, dan zijn deze expliciet benoemd bij dreigingen.

Tenslotte is denkbaar dat niet iedereen op gelijke wijze toegang heeft of kan krijgen tot technologische toepassingen. Sommigen sluiten zichzelf uit van het gebruik, bij anderen kunnen daar andere oorzaken aan ten grondslag liggen, bijvoorbeeld gebrek aan financiën of kennis. Zo gebruiken lang niet alle hoogbejaarden het internet. In theorie zou dat kunnen leiden tot sociale uitsluiting van bepaalde groepen voor technologische toepassingen.

Tenzij er heel specifieke argumenten gelden waardoor een geselecteerde toepassing zou kunnen leiden tot een aantasting van de nationale veiligheid, is het aspect van uitsluiting niet benoemd bij de beschouwde toepassingen.

1.5 Maatschappelijke en sociale betekenis van technologie

In deze studie ligt de focus op technologische ontwikkelingen en worden verbanden met andere maatschappelijke ontwikkelingen (bijvoorbeeld de duurzaamheidsproblematiek) zijdelings aangestipt vanuit het veiligheidsperspectief en maatschappelijke megatrends. Dit is zinvol omdat technologie een belangrijke vormende werking heeft binnen de maatschappij.

Het is echter niet zo dat technologie zich autonoom ontwikkelt en dat mens en maatschappij maar moeten meebewegen. Technologie wordt (nog altijd) ontwikkeld door de mens. De mens die een plaats inneemt binnen de maatschappij. Technologieën moeten dan ook gezien worden als onderdeel van de (maatschappelijke en sociale) entiteiten die in een voortdurend krachtenspel met elkaar de vormgeving van de maatschappij bepalen.

Kennis over de werking van de maatschappij, haar instituties, individuen en geschiedenis is daarom een noodzakelijke voorwaarde om technologie in een bredere context te begrijpen dan binnen de focus van deze studie. Naarmate technologie complexer, intelligenter, zelfstandiger en alomtegenwoordig wordt, groeit de noodzaak na te denken over de rollen die technologie speelt, zal gaan spelen, en zou moeten spelen (normatief). Een mooi voorbeeld hiervan is de discussie die momenteel speelt rondom privacy; een discussie die eigenlijk alleen door (het gebruik van) informatie- en communicatietechnologie actueel geworden is.

1.6 Leeswijzer

Hoofdstuk 2 geeft een beschrijving van de aanpak en werkwijze van de studie.

De hoofdstukken daarna zijn ingedeeld naar de eerder genoemde technologieën:
- Hoofdstuk 3: Nanotechnologie;
- Hoofdstuk 4: Bio- / gentechnologie;
- Hoofdstuk 5: Neurotechnologie;
- Hoofdstuk 6: Materiaaltechnologie;
- Hoofdstuk 7: Informatietechnologie.

Per technologie komen in de hoofdstukken 3 tot en met 7 in achtereenvolgende paragrafen de drie onderzoeksvragen van de verkennende studie (zie paragraaf 2.1) aan de orde. De paragrafen in deze hoofdstukken nemen de lezer mee in de stappen die in de verkenning zijn gezet:

i. In de eerste paragraaf worden de **geïnventariseerde** technologische ontwikkelingen en toepassingen toegelicht die een mogelijke impact hebben (positief of negatief) op de nationale veiligheid.
ii. De tweede paragraaf beschrijft de resultaten van de volgende stap, de **identificatie** van technologische ontwikkelingen en toepassingen die door de geraadpleegde experts als mogelijk relevant zijn genoemd voor de nationale veiligheid. Een aantal van deze toepassingen is, op grond van hun geschatte impact op de nationale veiligheid en/of hun potentie tot versterking van de weerbaarheid, geselecteerd voor een nadere uitdieping (zie werkwijze in hoofdstuk 2). De derde paragraaf geeft een overzicht van deze geselecteerde toepassingen.
iii. De vierde paragraaf beschrijft[1] de **uitdieping** van de kansen en dreigingen van de geselecteerde toepassingen van technologische ontwikkelingen.

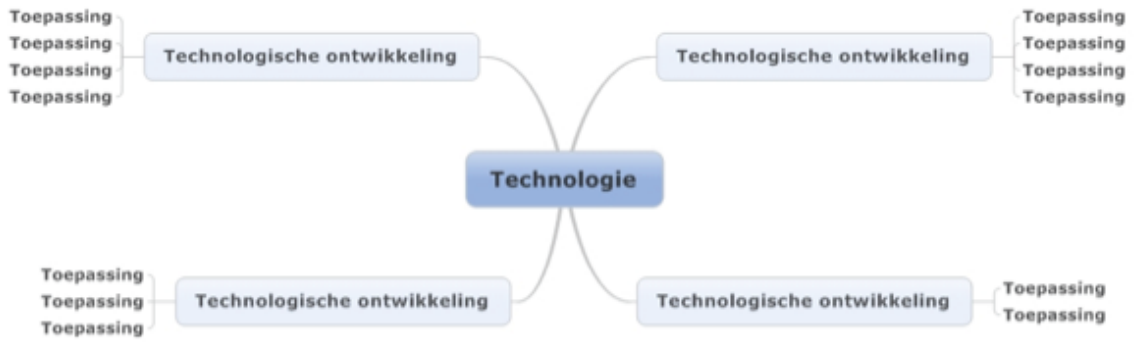
Ad i) Per technologie toont een figuur de geïnventariseerde ontwikkelingen en toepassingen die worden toegelicht (zoals geschematiseerd in figuur 2).

De vlaggetjes, die in de figuren in de eerste paragrafen van de hoofdstukken per technologie zijn geplaatst bij verschillende toepassingen, representeren de voorselectie van toepassingen door geïnterviewde experts op basis van de criteria: 1. in beginsel relevant voor de nationale veiligheid én 2. passend binnen de tijdshorizon. In bijlage G zijn argumenten uit de interviews voor de voorselectie opgenomen.

Ad ii) De tweede paragrafen geven per technologie een overzicht van de door de experts bij de geïnventariseerde toepassingen genoemde relevante producten en diensten. Tevens is per geïdentificeerde toepassing de door de experts ingeschatte mate van kans of dreiging (bijlage H) aangegeven, inclusief de resultaten van de workshop met experts op het gebied van de nationale veiligheid (bijlage C).

[1] Voor zover er toepassingen voor verdere uitwerking zijn geselecteerd. Dat is niet het geval bij neurotechnologie in hoofdstuk 5.

Figuur 2: Per technologie: technologische ontwikkelingen en toepassingen.



Opmerking: Wanneer meningen van experts over de impact van toepassingen elkaar tegenspreken - zoals de mening van materiaaltechnologie-experts en informatietechnologie-experts over decentralisatie van energieopslag - is dat bij de identificatie van toepassingen aangegeven in een vergelijkbaar tekstblok als dit.

Ad iii) Per geselecteerde toepassing is - voor zo ver relevant - een beschrijving gegeven van de voorziene kansen of dreigingen die er aan zijn verbonden. Daarbij is gebruik gemaakt van de nationale vitale belangen die in de Strategie Nationale Veiligheid worden genoemd, van de criteria die in de Nationale Risicobeoordeling worden gebruikt en van de capaciteitenlijst die voor de Strategie Nationale Veiligheid is ontwikkeld. Bij de kansen en dreigingen is aangegeven aan welk vitaal belang of vitale belangen deze zijn gerelateerd. Wanneer er een relatie is met de weerbaarheid is dit eveneens aangegeven.

Hoofdstuk 8 geeft een analyse van toepassingen en dreigingen voor een mogelijk scenario binnen de NRB.

Tenslotte bevat hoofdstuk 9 de samenvattende conclusies.

In de bijlagen is het volgende opgenomen:

- Bijlagen A, B en C geven een overzicht van de geïnterviewde experts en deelnemers aan de workshops;
- Bijlagen D, E en F geven achtereenvolgens een overzicht van de toegepaste megatrends, impactcriteria en capaciteitenlijst;
- Bijlagen G en H geven een overzicht van de argumenten bij de voorselectie van toepassingen en de score voor de selectie van toepassingen voor verdere uitwerking;
- Bijlage I geeft een overzicht van de toepassingen per technologie met een argumentatie van de score door de experts en de argumentatie voor de selectie van toepassingen voor verdere uitwerking.

2 Beschrijving van de aanpak en werkwijze

2.1 Onderzoeksvragen

Om de in het vorige hoofdstuk gegeven doelstelling te bereiken worden in deze studie drie onderzoeksvragen beantwoord:

I. Welke technologische ontwikkelingen en toepassingen daarvan zijn er (te verwachten)?

II. Welke van de geïnventariseerde technologische ontwikkelingen en toepassingen zijn in termen van kansen en dreigingen relevant voor de nationale veiligheid?

III. Welke specifieke kansen en dreigingen zijn verbonden aan de technologische ontwikkelingen en toepassingen die relevant zijn voor de nationale veiligheid?

In aanvulling op bovenstaande onderzoeksvragen wordt als voorbereiding van een mogelijk scenario in de NRB een vierde onderzoeksvraag beantwoord:

IV. Welke geïdentificeerde dreigingen komen het meest in aanmerking voor uitwerking als scenario in de NRB?

2.2 Stappen in de werkwijze

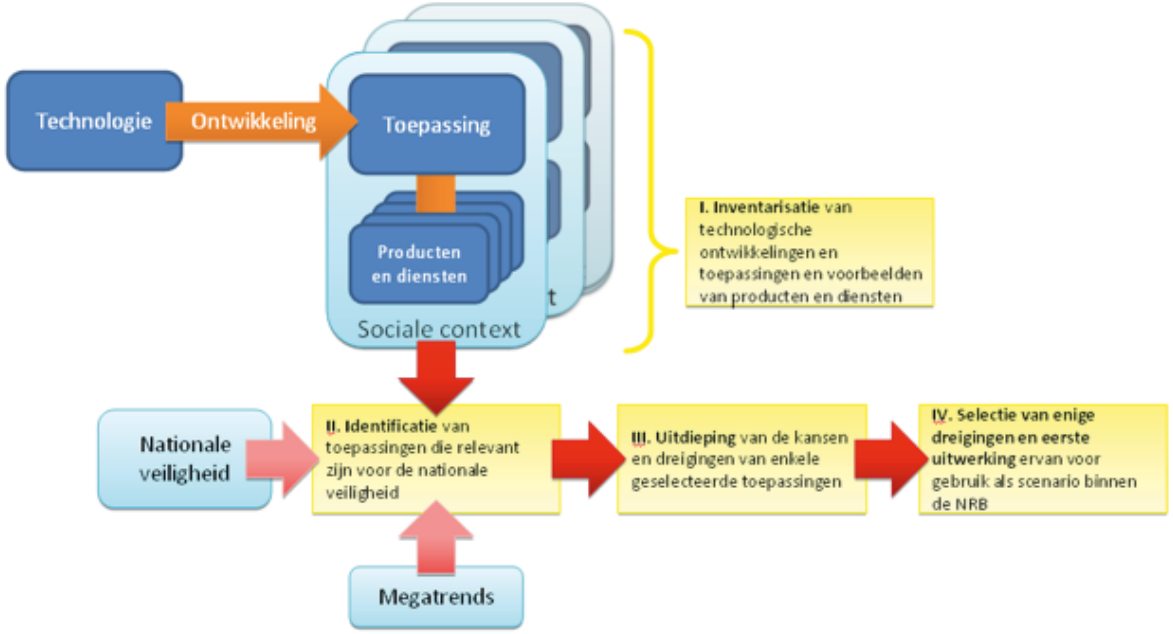
Onderstaande figuur biedt een schematisch overzicht van de gevolgde werkwijze. De procesonderdelen van figuur 3 worden aan de hand van elk van de onderzoeksvragen kort toegelicht.

I. *Inventarisatie van technologische ontwikkelingen en toepassingen en voorbeelden van producten en diensten*

Dit betreft de inventarisatie van de technologische ontwikkelingen en toepassingen binnen de scope van de verkenning. Via *desk research* en interviews met experts zijn relevante technologische ontwikkelingen in kaart gebracht en is op basis van expert opinie een voorselectie gemaakt van toepassingen die mogelijke relevant zijn voor de nationale veiligheid en binnen de genoemde tijdshorizon vallen. Een overzicht van de geraadpleegde experts is te vinden in bijlage A. In bijlage G zijn de argumenten uit de interviews voor de voorselectie opgenomen. Een overzicht van de gebruikte literatuur is te vinden in de literatuurlijst (pagina 66). Op basis daarvan is een overzicht gemaakt van de toepassingen van deze ontwikkelingen. De resultaten van de inventarisatie zijn ter verificatie aan enkele experts voorgelegd die aan de inventarisatie hebben meegewerkt.

Deze stap beantwoordt onderzoeksvraag I. De geïnventariseerde technologische ontwikkelingen en toepassingen

Figuur 3: Schematisch overzicht van de aanpak.



worden gepresenteerd in de eerste paragrafen van de hoofdstukken 3 tot en met 7.

II. *Identificatie van toepassingen van technologische ontwikkelingen die relevant zijn voor de nationale veiligheid*

Van de geïnventariseerde technologische ontwikkelingen en toepassingen zijn die ontwikkelingen en toepassingen **geïdentificeerd** welke relevant zijn voor de nationale veiligheid. De eerste stap van de identificatie is gebeurd in een workshop waarvoor experts op de vijf technologieën en experts op het gebied van maatschappelijke ontwikkelingen en sociale context zijn uitgenodigd[2]. In deze workshop zijn de geïnventariseerde toepassingen, met relevante voorbeelden van producten en diensten, getoetst aan de verschillende vitale belangen van de nationale veiligheid en eveneens getoetst op mogelijkheden tot versterking van de weerbaarheid, met daarbij de sociale context en belangrijke maatschappelijke ontwikkelingen ('megatrends', zie bijlage D) als 'denkraam'. Tabel 1 illustreert de opzet van dit proces. De criteria voor de identificatie van toepassingen worden verder toegelicht in paragraaf 2.3.

De toetsing hield in dat potentieel kansrijk dan wel dreigend gebruik van toepassingen in de vorm van producten en diensten is benoemd, aangevuld met een eerste kwalitatieve inschatting van de mate waarin dat gebruik kansrijk dan wel dreigend zou kunnen zijn. De criteria die zijn gebruikt bij deze toetsing zijn beschreven in de volgende paragraaf. De resultaten van de beoordeling (kwalitatieve inschatting) zijn samengevat in Bijlage H. Vervolgens zijn op basis van consultatie van enkele experts op de vijf technologieën en experts op het gebied van de nationale veiligheid[3], de resultaten van de kwalitatieve inschatting gebruikt om een selectie te maken van toepassingen voor verdere uitdieping. De experts hebben daartoe aangegeven in welke mate een toepassing een kans of dreiging kan vormen.

Deze stap beantwoordt onderzoeksvraag II. De aldus geselecteerde toepassingen worden gepresenteerd in de tweede en derde paragrafen van de hoofdstukken 3 tot en met 7.

[2] Workshop Technologieverkenning ten behoeve van de Nationale Risicobeoordeling; Analistennetwerk Nationale Veiligheid; datum: 26 November 2012; locatie: KiviNiria, Prinsessegracht 23, Den Haag. De deelnemerslijst van de workshop is opgenomen in bijlage B.

[3] Workshop Technologieverkenning met de Taakgroep Analistennetwerk Nationale Veiligheid; datum: 20 juni 2013; locatie: TNO, Oude Waalsdorperweg 63, Den Haag. De deelnemerslijst van de workshop is opgenomen in bijlage C.

Tabel 1: Proces van toetsing van toepassingen (met voorbeelden van producten en diensten) aan de verschillende vitale belangen van de nationale veiligheid en aan weerbaarheid.

Technologieën	Vitale belangen					
	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Toepassing 1 (producten/diensten)						
Toepassing 2 (producten/diensten)						
...						

III. *Uitdieping van de kansen en dreigingen van enkele geselecteerde toepassingen van technologische ontwikkelingen*

De geselecteerde toepassingen van technologische ontwikkelingen zijn vervolgens **uitgediept.** Per toepassing is een meer precieze kwalitatieve beoordeling van de positieve en/of negatieve effecten van die toepassing op de nationale veiligheid gegeven.
De uitdieping van de kansen en dreigingen heeft plaatsgevonden op basis van een kwalitatieve beoordeling van de impact van de toepassingen op (de vitale belangen van) de nationale veiligheid en hun mogelijkheden tot versterking van de weerbaarheid. Ook is een inschatting gemaakt van de waarschijnlijkheid waarin een toepassing een kans of dreiging kan zijn. Daarbij is gebruik gemaakt van de impactcriteria uit de methodiek van de Nationale Risicobeoordeling [15] en van de capaciteitenlijst die voor de Strategie Nationale Veiligheid is ontwikkeld [15].
De uitdieping maakt gebruik van de resultaten van de eerder genoemde workshop, respectievelijk gevolgd door een beoordeling door inhoudelijke experts op het gebied van de technologieën en door experts op het gebied van de nationale veiligheid.

Deze stap beantwoordt onderzoeksvraag III. De resultaten staan beschreven in de vierde paragrafen van de hoofdstukken 3 tot en met 7.

IV. *Selectie van enige dreigingen en een eerste uitwerking ervan voor gebruik als scenario binnen de NRB*

In aanvulling op bovenstaande stappen zijn toepassingen van technologische ontwikkelingen die een potentiële dreiging vormen voor de nationale veiligheid verder geanalyseerd ten behoeve van een mogelijk **scenario** voor de NRB. Aangezien de NRB gericht is op dreigingen, is hier uitsluitend uitgegaan van dreigingen en niet van kansen.
De keuze van deze toepassingen is gebaseerd op de criteria die het ANV (Analistennetwerk Nationale Veiligheid) gebruikt voor het agenderen van nieuwe thema's en onderwerpen [2].

Deze stap beantwoordt onderzoeksvraag IV. De resultaten van deze stap staan beschreven in paragraaf 8.4.

2.3 Criteria voor identificatie van toepassingen

Nationale veiligheid en vitale belangen

Om experts een inschatting te laten maken van de wijze waarop toepassingen een kans of dreiging vormen voor de nationale veiligheid, maakt deze technologieverkenning gebruik van de binnen de Strategie Nationale Veiligheid benoemde vitale belangen [14].

De nationale veiligheid is in het geding als vitale belangen van de Nederlandse staat en/of samenleving zodanig worden bedreigd dat sprake is van potentiële maatschappelijke ontwrichting. De vijf gedefinieerde vitale belangen zijn [15]:

- *Territoriale veiligheid:* Het ongestoord functioneren van Nederland als onafhankelijke staat in brede zin, dan wel de territoriale integriteit in enge zin.
- *Fysieke veiligheid:* Het ongestoord functioneren van de mens in Nederland en zijn omgeving.
- *Economische veiligheid:* Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie.
- *Ecologische veiligheid:* Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland.
- *Sociale en politieke stabiliteit:* Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de

verworvenheden van de Nederlandse democratische rechtstaat en daarin gedeelde waarden.

Voor elk van de vitale belangen zijn impactcriteria gedefinieerd [15]. In bijlage E is een overzicht van deze impactcriteria opgenomen.

Voor deze technologieverkenning zijn de impactcriteria gebruikt om op hoofdlijnen inzicht te krijgen in de mate waarin technologische toepassingen (via producten en diensten) een kans of dreiging vormen voor de nationale veiligheid. De toepassingen met een naar verwachting relatief hoge totale impact zijn geselecteerd voor verdere uitwerking.

Weerbaarheid

Behalve met vitale belangen hebben we ook te maken met weerbaarheid. Onder weerbaarheid verstaan we het vermogen tot bescherming en verdediging tegen rampen en dreigingen en tot snel en adequaat herstel van de situatie nadat zich een ramp of crisis heeft voltrokken.

Een toepassing van een technologische ontwikkeling kan niet alleen een kans of dreiging zijn voor de vitale belangen maar ook:

- een kans om capaciteiten te versterken en daarmee de weerbaarheid te vergroten;
- een dreiging die capaciteiten verzwakt en daarmee de weerbaarheid vermindert.

De capaciteiten zijn door de methodiekgroep voor de Nationale Risicobeoordeling gedefinieerd in de zogenaamde capaciteitenlijst. De hoofdcategorieën van de capaciteiten zijn opgenomen in bijlage F. Tijdens de workshop ‘Technologieverkenning ten behoeve van de Nationale Risicobeoordeling’ is de capaciteitenlijst gebruikt als handvat om op hoofdlijnen inzicht te krijgen in kansen en dreigingen van de toepassingen van technologische ontwikkelingen met betrekking tot de weerbaarheid.

3 Nanotechnologie

3.1 Inventarisatie van toepassingen van technologische ontwikkelingen

Introductie

Nanotechnologie is de technologie die zich bezighoudt met de ontwikkeling van materialen en componenten die het formaat hebben van individuele atomen en moleculen (afmetingen van 0,1 tot ongeveer 100 nanometer[4]) [18]. Nanotechnologie kan worden uitgesplitst in twee verschillende onderdelen. Het betreft enerzijds de technologie van het produceren en gebruik maken van artefacten of producten, waarvan de onderdelen in één dimensie qua afmeting niet groter zijn dan enkele tientallen nanometer (<100 nm). Anderzijds betreft het de technologie waarmee nanomaterialen worden gemaakt en toegepast. In het eerste geval betreft het miniaturisering en in het tweede geval de nanomaterialen zelf. Nanomaterialen zijn materialen die volgens de definitie van de Europese Commissie uit deeltjes bestaan waarvan minstens 50% een of meer externe dimensies bezitten binnen het bereik van 1 nm tot 100 nm [23].

Het steeds kleiner uitvoeren van technologische artefacten - **miniaturisering** -biedt nieuwe toepassingsmogelijkheden. Door de miniaturisering van bijvoorbeeld elektronica wordt het mogelijk om - meer dan nu het geval is - alledaagse 'dingen', zoals smartphones, uit te rusten met sensoren en chips. Door de toevoeging van sensoren en processoren kan 'intelligentie' worden toegevoegd aan apparaten en 'dingen'. Miniaturisering maakt daarmee het 'slim' maken van onze omgeving en het tot stand komen van het *internet of things* (verder behandeld onder informatietechnologie, zie hoofdstuk 7) mogelijk.

Het bijzondere van nanomaterialen is dat materialen op nanoschaal andere eigenschappen hebben dan zij op grotere schaal hebben [1]. Door beter begrip van materiaal- en structuureigenschappen kunnen **nieuwe nanomaterialen en -structuren** worden ontwikkeld waarbij aan materialen bepaalde eigenschappen kunnen worden meegegeven. Een voorbeeld daarvan is dat materialen op nanoschaal soms door celwanden heen kunnen bewegen. Deze eigenschap kan worden toegepast in de geneeskunde. Het gebruik van nanomaterialen in levende organismen (van mensen tot dieren en planten) is het gebied van de **bio-nanotechnologie**.

De succesvolle ontwikkelingen op het gebied van **nanofabricage en -instrumentatie** kunnen gezien worden als belangrijke ontwikkeling voor het mogelijk maken van het op grote schaal toepassen van nanomaterialen. Een

[4] Eén nanometer (nm) is één miljardste meter.

voorbeeld van een product zijn aangepaste lithografische instrumenten voor het bedrukken van materialen. Daarmee kunnen op oppervlakten zeer dunne (<100 nm) structuren worden aangemaakt, bijvoorbeeld voor het laag voor laag vervaardigen van producten als sensoren en onderdelen voor telecom- en datacommunicatietoepassingen.

Over de eigenschappen van nanomaterialen - en in het bijzonder de risico's die verbonden zijn aan het gebruik van nanotechnologie - is nog niet zoveel bekend. Er wordt veel van nanotechnologie verwacht [3], maar de onzekerheid over de effecten houdt nog veel ontwikkelaars van nieuwe toepassingen tegen uit angst voor de mogelijke consequenties.

Een belangrijke vraag is of de risico's van nanotechnologie voldoende kunnen worden ingeschat met bestaande risicomanagementmethoden. Op dit moment is er geen specifieke wetgeving voor nanotechnologie, maar wordt bestaande wet- en regelgeving toegepast. Wel is een gedragscode voor verantwoord nanowetenschappelijk en nanotechnologisch onderzoek opgesteld [4] en wordt gepleit om afstemming over risicobeheersing van nanomaterialen op Europees niveau te regelen. De ontwikkeling van een adequaat instrumentarium voor de risicoanalyse is hier onderdeel van. Binnen het vakgebied van de nanotechnologie vindt onderzoek plaats naar toepassingsmogelijkheden en de risico's, bijvoorbeeld in het Nederlandse programma NanoNextNL. Daarnaast zijn er diverse platforms waarbinnen het publieke debat wordt gestimuleerd en gevoerd, zoals het RATA thematische programma in NanoNextNL [20].

Nano- en micro-elektromechanische systemen (NEMS/MEMS)

NEMS en MEMS zijn acroniemen voor respectievelijk nano- en micro-elektromechanische systemen. NEMS kunnen gezien worden als de volgende stap in miniaturisatie na MEMS. MEMS zijn kleine systemen die geïntegreerd zijn in gebruiksartikelen of apparaten en die uit een combinatie van elektronische, mechanische en eventueel chemische componenten bestaan. Dat kan bijvoorbeeld het geval zijn in microsatellieten (voor communicatie- en observatiedoeleinden). Deze zijn goedkoper dan gewone satellieten en eenvoudiger te lanceren. MEMS variëren in grootte van een micrometer tot enkele millimeter [19]. NEMS bieden door hun nog kleinere omvang weer nieuwe mogelijkheden, bijvoorbeeld de mogelijkheid om zich in omgevingen te bewegen die niet of minder toegankelijk zijn voor MEMS, zoals lichaamscellen. Bij specifieke producten kan gedacht worden aan bijvoorbeeld nanobots die kunnen worden gebruikt voor chirurgie en biopsie, en microsystemen die kunnen worden gebruikt bij afvalwaterzuivering. Nanobots in allerlei producten, in combinatie met informatietechnologie bieden de mogelijkheid tot het '*internet of nanothings*': zeer kleine systemen en producten die kunnen communiceren met elkaar en de omgeving om bijvoorbeeld metingen door te geven.

Nanomaterialen

Qua concrete toepassingen van nanotechnologie in producten zijn het op dit moment vooral bestaande producten die door middel van nanotechnologie zijn verbeterd. Dit komt door de toevoeging van nanomaterialen die zorgen voor specifieke eigenschappen van de producten. Voorbeelden zijn coatings en verf binnen de automobielindustrie en de bouw, zonnecellen en consumentenartikelen als zonnebrand en beschermingsspray voor kleding en schoenen. Zo worden in coatings en verf nanomaterialen toegevoegd om te zorgen voor kras-

Figuur 4: Nanotechnologie: technologische ontwikkelingen en toepassingen.

Tabel 2: Nanotechnologie: overzicht van geïnventariseerde toepassingen met voorbeelden van producten en diensten.

Nano- en micro-elektromechanische systemen (NEMS/MEMS) *Producten en diensten:*	
Microsatellieten	Kleine satellieten die relatief goedkoop zijn.
Nanobots voor waterzuivering	Zeer kleine elektromechanische systemen voor het zuiveren of ontzilten van water.
Internet of nanothings	Systemen en producten die slimme onderdelen bevatten die steeds kleiner en onzichtbaarder worden en met elkaar kunnen communiceren.

Nanomaterialen *Producten en diensten:*	
Nanodeeltjes in grondstoffen	Nanodeeltjes als toevoeging aan grondstoffen, waardoor de eigenschappen worden verbeterd (bijvoorbeeld zelfherstellende lak).
Identiteits-manipulatie	Nanotechnologie gebruikt voor bijvoorbeeld het vervalsen van een vingerafdruk met *nanocoating*.
Nanodeeltjes in zonnecellen	Nanodeeltjes verwerkt in zonnecellen waardoor de werking ervan wordt verbeterd.
Nanodeeltjes in kleding	Nanodeeltjes in beschermende kleding en schoenen (tegen kou, warmte, besmetting, etc.).
Nanodeeltjes in wapens	Nanotechnologie ingezet als wapen, bijvoorbeeld nanodeeltjes in de munitie of stof die vrijkomt bij een explosie.

Gepersonificeerde geneesmiddelen *Producten en diensten:*	
Lab-on-a-chip	Laboratorium op een chip dat gebruik maakt van nanotechnologie voor bijvoorbeeld medische diagnostiek of zelfdiagnose. Bijvoorbeeld voor het thuismeten van bloedwaarde.
Medische *bots*	Nanotechnologie voor bijvoorbeeld transport van medicijnen, diagnose en monitoring.

bestendigheid, brandwerendheid of het afstoten van water. Nanomaterialen zouden mogelijk ook kunnen worden ingezet als wapen door nanodeeltjes toe te voegen in de munitie of stof die vrijkomt bij een explosie.

Gepersonificeerde geneesmiddelen

Een voorbeeld van de mogelijkheden met miniaturisatie in de medische sector is het gebruik van zelftesten (thuismonitoring) als een van de producten van *lab-on-a-chip* (verschillende meet- en analysefuncties geïntegreerd op één chip). De commercialisering van chips voor bloedmetingen is dichtbij, onder andere omdat verzekeraars hier heil in zien. Een ander product kan mogelijk de 'nano-pil' zijn, waarmee al in een vroeg stadium gewaarschuwd kan worden voor het risico op kanker. Daarnaast verbetert nanotechnologie met 'medische bots' gerichte levering en activering van medicijnen in het lichaam (*drug delivery* en *targeted medicine*) (zie ook NEMS/MEMS), bijvoorbeeld door gebruik te maken van op nanoschaal gevouwen DNA ('DNA origami'), dat als transportmiddel voor een farmaceutische stof wordt ingezet.

3.2 Identificatie van toepassingen relevant voor de nationale veiligheid

Tabel 2 geeft voor nanotechnologie een overzicht van de geïnventariseerde toepassingen met voorbeelden van producten en diensten die volgens de geraadpleegde experts mogelijk relevant worden geacht voor de nationale veiligheid[5].

De door de experts ingeschatte mate van kans of dreiging (zie bijlage H) wordt hieronder per geïnventariseerde toepassing toegelicht.

Nano- en micro-elektromechanische systemen (NEMS/MEMS)

Microsatellieten bieden de mogelijkheid tot observatie of spionage vanuit de ruimte waardoor allerlei middelen, zoals schepen voor grensbewaking, maar ook wapens tijdens conflicten, efficiënter kunnen worden ingezet. Doordat satellieten goedkoper worden kunnen meer landen aan deze ontwikkeling deelnemen. Deze mogelijkheden kunnen tot een hoge impact op de territoriale veiligheid leiden, omdat relatief eenvoudig vanuit de ruimte kan worden gespioneerd. Voor de fysieke veiligheid wordt een gemiddelde (positieve) impact verwacht omdat hulpeenheden mogelijk efficiënter zijn in te zetten. Daarmee kan toepassing van microsatellieten ook een positieve invloed hebben op het versterken van de weerbaarheid.

[5] Op basis van de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling'. Zie werkwijze in paragraaf 2.2.

Van nanobots voor waterzuivering wordt een lage tot zeer lage impact op de nationale veiligheid verwacht. De voordelen zitten hem vooral in milieuwinst en kostenbesparing.
Internet of nanothings biedt een kans doordat zeer kleine onderdelen in gekoppelde systemen metingen kunnen verrichten. Dit is een uitbreiding op het *internet of things* met bijvoorbeeld systemen in het menselijk lichaam of in vloeistofstromen binnen fabrieken, waar 'grote' sensoren niet opgenomen kunnen worden. Hiervan wordt een gemiddelde impact verwacht voor zowel de territoriale, de fysieke, als de economische veiligheid omdat bijvoorbeeld incidenten in chemische fabrieken mogelijk eerder gedetecteerd of zelfs voorkomen kunnen worden. Daarmee wordt ook de weerbaarheid tegen zulke incidenten versterkt.
In hoeverre er op een termijn van vijf jaar een brede uitrol van NEMS/MEMS is, valt nog te bezien. De verwachting is dat de toepassing langzaam zal groeien en een brede uitrol pas op langere termijn het geval zal zijn.

Nanomaterialen
Van nanodeeltjes in grondstoffen en in zonnecellen wordt een mogelijke, maar beperkte impact verwacht op de ecologische veiligheid. Dit is gebaseerd op eventuele (maar nu nog onduidelijke) effecten op de leefomgeving als zulke deeltjes vrijkomen. Hetzelfde geldt voor nanodeeltjes in kleding. Ook gezondheidsrisico's door blootstelling van de mens aan bepaalde nanodeeltjes (fysieke veiligheid) zijn niet uit te sluiten, al wordt daar wel veel onderzoek naar gedaan.
De verwachting is dat nanotechnologie ook gebruikt kan worden voor identiteitsmanipulatie, zoals het vervalsen van een vingerafdruk door bijvoorbeeld met behulp van *nanocoating* een kopie te maken. Dit kan enig negatief effect hebben op de weerbaarheid (niet in staat zijn kwaadwillenden uit groepen personen te filteren op basis van een vingerafdruk).
Nano DNA spray biedt een kans als identificatiemiddel in het kader van opsporing. Dit kan bijdragen aan verbetering van de rechtsgang door het verkrijgen van betere bewijsmiddelen.
Nanodeeltjes in wapens kunnen een dreiging vormen. De mogelijkheden vanuit nano-, bio- en materiaaltechnologie kunnen - hoewel de waarschijnlijkheid daarvan momenteel door experts laag wordt ingeschat - leiden tot (de aanwending van) nieuwe wapens, explosieven of giftige stoffen, nieuwe manieren om explosieven of gif te 'verpakken' en tot nieuwe dragers van explosieven of gif [1].

Gepersonificeerde geneesmiddelen
Van de toepassing van een *lab-on-a-chip* gerelateerd aan gepersonificeerde geneesmiddelen wordt een beperkte impact op de nationale veiligheid verwacht. Door sommige toepassingen zou de privacy van burgers geschonden kunnen worden. Er zijn groeperingen actief die zich hierover zorgen maken en daartegen in actie komen[6]. Hiervan wordt echter geen maatschappelijke ontwrichting verwacht.
Medische *bots* geven de mogelijkheid de gezondheid van personen te monitoren en eerder afwijkingen te detecteren. Medische *bots* hebben hiermee echter geen rechtstreekse invloed op de nationale veiligheid, hoewel er enige zorg is over mogelijk misbruik van dergelijke systemen voor medicijnafgifte in biologische wapens. Het inzetten van medische bots als biologisch wapen wordt echter niet waarschijnlijk geacht.

3.3 Selectie voor verdere uitwerking

De volgende toepassingen zijn op basis van de consultatie van experts[7] geïdentificeerd voor verdere uitwerking van kansen en dreigingen:
- NEMS/MEMS (meest relevante producten en diensten: microsatellieten, *internet of nanothings*);
- Nanomaterialen (meest relevante producten en diensten: nanodeeltjes in wapens, identiteitsmanipulatie).

3.4 Uitdieping van kansen en dreigingen van geselecteerde toepassingen

De uitdieping van kansen en dreigingen wordt hieronder beschreven voor de voor verdere uitwerking geïdentificeerde toepassingen.

Nano- en micro-elektromechanische systemen (NEMS/MEMS)
Miniaturisering heeft ertoe geleid dat sensoren en actuatoren steeds kleiner en soms goedkoper kunnen worden geproduceerd. Dit biedt nieuwe mogelijkheden voor het toepassen van NEMS en MEMS (respectievelijk nano- en micro-elektromechanische systemen).

Kansen
- Inzet NEMS ter voorkoming grootschalige industriële incidenten: NEMS kunnen vanwege hun kleine omvang worden toegepast in het lichaam, in het oppervlakte-

[6] Bijvoorbeeld tijdens de Mexicaanse griepvaccinatie enkele jaren geleden waren er geruchten dat de overheid mensen wilde injecteren met een nanochip zodat ze heimelijk gevolgd konden worden.
[7] Zie werkwijze in paragraaf 2.2.

water, in stromen vloeistoffen in de industrie, in verpakkingsmaterialen, etc. NEMS kunnen met hoge resolutie metingen verrichten en communiceren met elkaar en de buitenwereld. Kleine afwijkingen ten opzichte van normwaarden kunnen worden gedetecteerd. Dit vormt een kans in het herkennen en (vroegtijdig) bestrijden van bijvoorbeeld incidenten in (chemische) fabrieken.

- Inzet MEMS voor communicatie, monitoring en observatie door 'veiligheidsdiensten': MEMS bieden kansen voor observatie- en communicatiedoeleinden, bijvoorbeeld voor inlichtingenvergaring ter voorkoming van ongewenste zaken, tijdens de responsefase van een crisis (*situational awareness*) of voor het bewaken en volgen van transport van goederen.
  Daarnaast bieden MEMS de mogelijkheid om specifieke personen gericht en langdurig te volgen en hun bewegingen, gesprekken, etc. vast te leggen. Inzet op soortgelijke manier als bij *crowd management* kan door de verkregen informatie over de beweging van groepen mensen helpen bij het voorkomen van grootschalige rellen.
  Met MEMS in de vorm van goedkope en kleine microsatellieten kunnen grenzen worden geobserveerd (voor Nederland bijvoorbeeld op zee) en de omgeving worden gemonitord (bijvoorbeeld om in te grijpen bij bosbranden). Microsatellieten bieden ook een kans voor Defensie en nationale veiligheidsdiensten als aanvullend communicatiemiddel. Door het kunnen beschikken over een aanvullend communicatiemiddel naast de bestaande communicatiemiddelen verhoogt dit de weerbaarheid.

Dreigingen

- Inzet NEMS en MEMS voor communicatie, monitoring en observatie door 'kwaadwillenden': In het 'klein zijn' van NEMS schuilt hun succes, maar tevens ook een dreiging. Door hun zeer geringe afmeting zijn NEMS moeilijk te traceren. Daardoor kunnen zij (al dan niet opzettelijk) terecht komen of aanwezig zijn in omgevingen waar zij niet thuishoren. Het onttrekken van NEMS uit producten of uit de omgeving brengt vooral kosten met zich mee (bijvoorbeeld tijdens recycling van materialen). Het opzettelijk inbrengen van NEMS in een bepaalde omgeving is een dreiging omdat het derden de mogelijkheid geeft om die omgevingen te monitoren. Dit laatste wordt echter niet erg waarschijnlijk geacht omdat het ontwikkelen en het 'planten' van NEMS veel kennis en een enorme inspanning vergt. Daardoor is dit niet eenvoudig te doen door bijvoorbeeld een enkel kwaadwillend individu. De kans is groter dat MEMS worden gebruikt tegen Nederland voor het verzamelen van informatie door statelijke actoren (spionage). Microsatellieten zullen naar verwachting pas op langere termijn impact hebben, maar het effect kan groot zijn als de bestaande internationale verdragen niet aangepast worden.
  Een mogelijke dreiging van het *internet of nanothings* is de vraag wie er controle heeft over (of mee kijkt met de besturing van) systemen. Als de beveiliging tekort schiet (*cybersecurity*) kunnen burgers en economische belangen beperkt schade ondervinden. Een buitenlandse actor (statelijk dan wel niet-statelijk) kan informatie uit NEMS/MEMS gebruiken om kwetsbaarheden en falen te benutten of informatie manipuleren waardoor de verkeerde actie wordt genomen.

Conclusies

- *Kansen:*
  - Inzet NEMS ter voorkoming grootschalige industriële incidenten;
  - Inzet MEMS voor communicatie, monitoring en observatie door 'veiligheidsdiensten'.
- *Dreigingen:*
  - Inzet NEMS en MEMS voor communicatie, monitoring en observatie door 'kwaadwillenden'.

Nanomaterialen

Materialen krijgen op nanoschaal andere eigenschappen. Met de kennis die nu wordt ontwikkeld kunnen aan materialen steeds meer gecontroleerd bepaalde eigenschappen worden meegegeven.

Kansen

- Verbetering hulpmiddelen veiligheidsdiensten door middel van nanomaterialen: Nanodeeltjes als toevoeging aan grondstoffen bieden de mogelijkheid eigenschappen van materialen te verbeteren. Nanomaterialen vormen daarmee een kans om allerlei hulpmiddelen van veiligheidsdiensten te verbeteren. Het kan gaan om middelen zoals lichtere *drones* of kleine bestuurbare vliegtuigjes, kogelwerende vesten, munitie, sensoren, etc. Nanomaterialen bieden daarmee mogelijkheden voor andere toepassingen.

Dreigingen

- *Dirty bomb* door toevoeging nanomaterialen: Met behulp van nanomaterialen zou een nieuw soort *dirty bomb* kunnen worden ontwikkeld. Een *dirty bomb* bevat giftige stoffen[8]. Door nanomaterialen toe te voegen, kunnen

[8] Strikt genomen bevat een *dirty bomb* radioactieve stoffen. Hier wordt bedoeld een bom waarmee giftige (chemisch of radiologisch…. of mogelijk zelfs biologisch) nanodeeltjes worden verspreid, die 1) moeilijk of niet detecteerbaar zijn, 2) gemakkelijk via de lucht (misschien zelfs huid) kunnen binnendringen bij mens en dier en daarmee voor gezondheidsschade zorgen, 3) een besmetting van een gebied, gewassen e.d. genereren die niet eenvoudig ongedaan is te maken. Hiermee wordt een bredere interpretatie gegeven aan het begrip *dirty bomb*.

deze giftige stoffen effectiever worden gemaakt of worden gemaskeerd waardoor detectie lastiger is (zie ook [1]). Belangrijk is te beseffen dat het niet zo veel uitmaakt of het nano- of microdeeltjes zijn (beide zijn inhaleerbaar) en dat vooral de werking van de stof(fen) in de deeltjes relevant is. De waarschijnlijkheid hiervan wordt door experts zeer laag geschat. Er is veel kennis van zaken nodig om een *dirty bomb* te fabriceren. Bovendien zal een dergelijke bom dan vooral voorbehouden zijn aan statelijke actoren en dus alleen ingezet worden ten tijde van gewapende conflicten. Mocht een dergelijke *dirty bomb* worden ingezet, dan zou dit grote gevolgen kunnen hebben voor de fysieke veiligheid (doden of gewonden door vrijgekomen giftige stoffen), ecologische veiligheid (aantasting van flora en fauna), territoriale veiligheid (in onbruik raken van land of infrastructuur) en economische veiligheid (kosten voor herstel kunnen hoog zijn vanwege de moeilijkheid om nanomaterialen op te ruimen).).

- Vergiftiging door (toevoeging van) nanomaterialen: Kwaadwillende actoren (statelijk dan wel niet-statelijk) zouden schadelijke nanomaterialen toe kunnen voegen aan bijvoorbeeld drinkwater of voedingsmiddelen, of hiermee kunnen dreigen. Dit heeft mogelijk impact op de fysieke veiligheid, de sociale en politieke stabiliteit en de economische veiligheid.
- Identiteitsmanipulatie met behulp van nanomaterialen: Nanomaterialen kunnen mogelijk worden gebruikt voor identiteitsmanipulatie, zoals het vervalsen van een vingerafdruk door bijvoorbeeld met behulp van *nanocoating* een kopie te maken. Daarnaast bestaat de mogelijkheid dat bij gebruik van nanomaterialen voor zelfherstellende lak eventuele achtergelaten vingerafdrukken door de lak geabsorbeerd worden en daarmee niet meer afneembaar zijn.

Conclusies

- *Kansen:*
  - Verbetering hulpmiddelen veiligheidsdiensten door middel van nanomaterialen.
- *Dreigingen:*
- - *Dirty bomb* door toevoeging nanomaterialen;
  - Vergiftiging door (toevoeging van) nanomaterialen;
  - Identiteitsmanipulatie met behulp van nanomaterialen.

4 Bio- / gen-technologie

4.1 Inventarisatie van toepassingen van technologische ontwikkelingen

Introductie

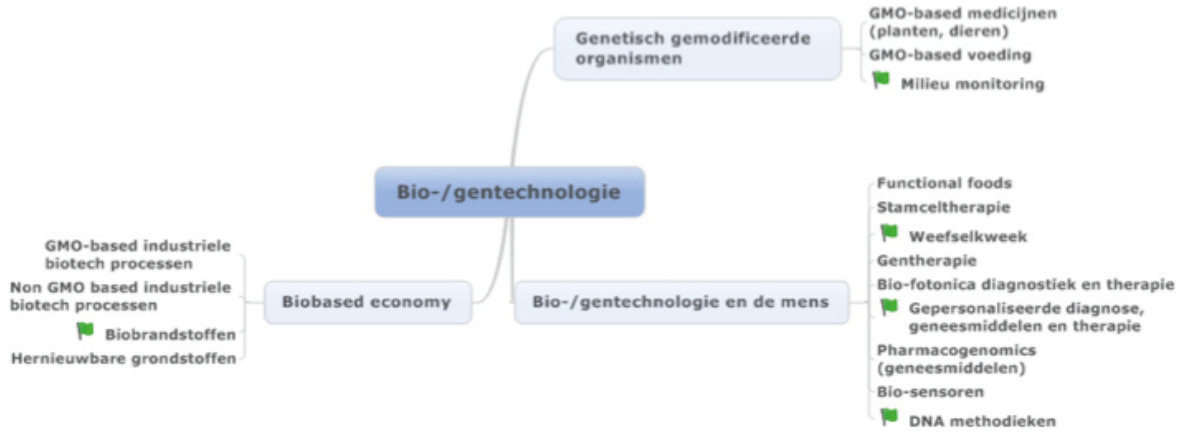
Bio- / gentechnologie is de technologie waarbij organismen worden bewerkt met de doelstelling het functioneren van planten, mensen of dieren te verbeteren. De technologie biedt onder meer kansen in de preventie en behandeling van ernstige ziekten en in het verbeteren van gewassen voor de wereldvoedselvoorziening. Onder gentechnologie vallen methoden en technieken waarbij **organismen genetisch gemodificeerd** (Genetically Modified Organism - GMO) worden gericht op een bepaalde toepassing. Het (genetisch) materiaal van levende organismen (planten, dieren, schimmels, bacteriën, etc.) wordt ingezet om producten te maken of te verbeteren [1]. Voor synthetische biologie (het ontwerpen van cellen of delen daarvan) maken synthetisch biologen veel gebruik van genetische modificatie. In sommige gevallen gaan de onderzoekers zelfs verder en bouwen en ontwerpen ze (met standaard stukjes DNA) zelf het DNA dat ze willen gebruiken. Zo hebben synthetisch biologen meer controle over de cel waaraan ze bouwen [19]. **Bio- / gentechnologie** kan worden toegepast op **mensen**[9] en op dieren.

Technologische ontwikkelingen op het gebied van de '**Biobased economy**' zijn onderdeel van de biotechnologie. De *biobased economy* (BBE) is een economie waarin gewassen en reststromen uit de landbouw en voedingsmiddelenindustrie worden ingezet voor niet-voedseltoepassingen. Hierbij worden deze groene grondstoffen - ofwel biomassa - toegepast als materialen, chemicaliën, transportbrandstoffen of energiebronnen (voor elektriciteit en warmte) [5]. Het aanpassen van gewassen, om deze bijvoorbeeld meer geschikt te maken als brandstof, behoort tot de mogelijkheden van bio- / gentechnologie.

Eén van de discussies die momenteel speelt rondom bio- / gentechnologie gaat over de risicoanalysemethodiek die door de overheid wordt gebruikt om beoordelingen omtrent de risico's van bio- / gentechnologie uit te voeren. De Commissie Genetische Modificatie (COGEM), het adviesorgaan van het Ministerie van Infrastructuur en Milieu, heeft geconcludeerd dat de huidige methodiek van

[9] Hierbij wordt opgemerkt dat de ontwikkelingen gericht op mensverbetering (*human enhancement*) in deze studie niet onder biotechnologie worden geschaard, maar (voor een deel) onder neurotechnologie; met name als het gaat over onderwerpen als prestatieverbetering.

Figuur 5: Bio- / gentechnologie: technologische ontwikkelingen en toepassingen.



risicoanalyse de komende jaren nog bruikbaar is, maar dat de moeilijkheidsgraad van de risicobeoordeling zal toenemen [6]. Verder spelen rondom bio- / gentechnologie discussies over publieke acceptatie [7].

Milieu monitoring

Een toepassing van de technologische ontwikkeling van genetisch gemodificeerde organismen is milieu monitoring. Dit betreft het verzamelen van informatie over, en toezicht houden op, ons leefklimaat. Hiervoor kan gebruik worden gemaakt van een biosensor. Een biosensor is een gemodificeerde bacterie, die een stof kan detecteren en afbreken of waarbij een cel oplicht ter detectie. De mogelijkheden voor verbeterde of nieuwe sensoren vanuit biotechnologie - in combinatie met ontwikkelingen in de informatietechnologie, nanotechnologie en materiaaltechnologie - bieden tal van kansen voor detectie en identificatie van milieuvervuilende stoffen. Te denken valt aan de controle op schoon water of het detecteren van bedorven voedsel door een biosensor in de verpakking. Biosensoren kunnen ook worden ingezet op andere gebieden, zoals voor de detectie van explosieven en medische toepassingen die zijn gerelateerd aan de technologische ontwikkeling bio- / gentechnologie en de mens.

Weefselkweek

Weefselkweek is het met behulp van onder andere stamcellen kweken van weefsel, botten en organen. Weefselkweek van lichaamseigen weefsel kan worden toegepast in de medische wereld om patiënten te helpen (bijvoorbeeld behandeling van brandwonden). Ook dierlijk weefsel kan wellicht in de toekomst worden gekweekt. Vlees 2.0 zou mogelijk als voedsel kunnen dienen. Weefselkweek is gerelateerd aan therapieën als stamceltherapie en gentherapie. Bij stamceltherapie gaat het om de transplantatie van stamcellen ter vervanging van bijvoorbeeld defecte cellen of weefsels. Gentherapie betreft het inbrengen van genetisch materiaal in cellen in het kader van een geneeskundige behandeling, bijvoorbeeld om erfelijke aandoeningen te voorkomen.

Gepersonaliseerde diagnose, geneesmiddelen en therapie

Gepersonaliseerde diagnostisering en medicatie is een toepassing waarbij gericht medicatie wordt toegediend - of therapie wordt gepleegd - op basis van leefstijl of genetische variatie. In combinatie met de toepassing weefselkweek ontstaat bijvoorbeeld de mogelijkheid tot een *lab-on-a-chip*. Heel kleine beetjes weefsel kunnen worden opgekweekt op een chip waarna bijvoorbeeld medicijnen op het weefsel kunnen worden getest. Hierdoor worden gepersonaliseerde diagnose, geneesmiddelen en therapie mogelijk. Geneesmiddelen die geënt zijn op iemands genetisch profiel worden ook wel *pharmacogenomics* genoemd. *Pharmacogenomics* zouden bijvoorbeeld kunnen worden gebruikt voor het beter op een patiënt afstemmen van chemotherapie bij kanker [17].

DNA methodieken

Met DNA methodieken kan op basis van DNA materiaal van levende organismen de identiteit van een individu en de mate van verwantschap tussen individuen worden vastgesteld. Doordat DNA profielen betrouwbaarder zijn geworden, heeft DNA onderzoek de laatste jaren een belangrijke plaats gekregen in het forensisch onderzoek en de rechtspraak. Daarbij zijn opvallende successen behaald waaronder recent de aanhouding van een verdachte in de geruchtmakende zaak Marianne Vaatstra. Dergelijke successen voeden de roep om een DNA databank waarin het DNA profiel van iedere burger of veroordeelde opgenomen kan worden. De ontwikkelingen op het gebied van DNA onderzoek hebben het mogelijk gemaakt om met minder en andersoortig DNA materiaal, gebruikmakend van DNA informatie in databanken, steeds sneller en meer informatie over de identiteit van een persoon te verzame-

Tabel 3: Bio- / gentechnologie: overzicht van geïnventariseerde toepassingen met voorbeelden van producten en diensten.

Milieu monitoring	
Producten en diensten:	
Biosensoren	Sensoren die gebruik maken van een biologische component (zoals bacteriën) voor diagnostisering of identificatie van stoffen. Zo kunnen sommige bacteriën verkleuren bij een bepaalde hoeveelheid vervuiling van water.
Weefselkweek	
Producten en diensten:	
Snelle EHBO kit voor *first responders*	Kweken van weefsel voor het behandelen op wonden of brandwonden.
Vlees 2.0	Het met behulp van o.a. stamcellen kweken van dierenvlees voor consumptie.
Gepersonaliseerde diagnose, geneesmiddelen en therapie	
Producten en diensten:	
Persoonlijke medicatie	Medicatie afgestemd op de persoon op basis van informatie uit bijvoorbeeld DNA of leefstijl of door testen de effectiviteit van medicijnen op het weefsel waar het medicijn op zou moeten werken.
Gepersonaliseerde diagnose	Systeem voor diagnose zodat behandeling kan worden afgestemd op persoon op basis van informatie uit bijvoorbeeld DNA of leefstijl.
DNA methodieken	
Producten en diensten:	
Opstellen van DNA databanken	Vastleggen en gebruiken van DNA informatie in databanken.
Biobrandstoffen	
Producten en diensten:	
Biodiesel of bio-ethanol	Brandstof gemaakt uit biomassa.

len. De snelheid waarmee dit kan, biedt mogelijkheden voor identificatie van personen bijvoorbeeld ten behoeve van grensbewaking, voor het opsporen van virussen, of om diensten op afstand te ontsluiten.

Biobrandstoffen
Biobrandstoffen zijn niet-fossiele brandstoffen die zijn verkregen uit biomassa. Micro-organismen kunnen worden gebruikt voor het verbeteren van een productieproces maar ook om bepaalde eindproducten te produceren. Zo kunnen micro-organismen (bijvoorbeeld algen of gistcellen) als 'fabriekje' worden gebruikt om biobrandstof te produceren. In hoog tempo worden dan genen in deze cellen geïntroduceerd om de productie te verbeteren. Voorbeelden van producten zijn bio-ethanol en biodiesel. Bij deze manier van produceren van biobrandstof is in principe geen landbouwgrond nodig, waardoor de productie niet concurreert met de productie van voedsel. Dit is hoogstwaarschijnlijk een noodzakelijke voorwaarde om tot een *biobased economy* te komen.

4.2 Identificatie van toepassingen relevant voor de nationale veiligheid

Tabel 3 geeft voor bio- / gentechnologie een overzicht van de geïnventariseerde toepassingen met voorbeelden van producten en diensten die volgens de geraadpleegde experts mogelijk relevant worden geacht voor de nationale veiligheid[10].

De door de experts ingeschatte mate van kans of dreiging (zie bijlage H) wordt hieronder per geïnventariseerde toepassing toegelicht.

Milieu monitoring
Biosensoren voor milieu monitoring bieden kansen voor detectie en identificatie van milieuvervuilende stoffen, maar dit heeft naar verwachting - op een (zeer) beperkte impact op de ecologische veiligheid na - geen betekenis

[10] Op basis van de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling'. Zie werkwijze in paragraaf 2.2.

voor de nationale veiligheid. Behalve voor milieu monitoring kunnen biosensoren ook worden ingezet voor de detectie van explosieve stoffen.

Opmerking: De onder bio- / gentechnologie bij de toepassing **milieu monitoring** genoemde sensoren worden, in tegenstelling tot de onder materiaaltechnologie genoemde **sensoren** (zie paragraaf 6.3), niet meegenomen in een verdere uitwerking van toepassingen. Het verschil in scores door de experts is mogelijk te verklaren doordat sensoren genoemd onder materiaaltechnologie over allerlei typen sensoren gaat. Vooral de bundeling en interpretatie van al die verschillende gegevens maakt sensoren interessant voor de nationale veiligheid.

Weefselkweek

Weefselkweek biedt kansen om bijvoorbeeld bij de behandeling van brandwonden patiënten te helpen met gekweekte huid in plaats van donorhuid en wellicht in de toekomst om voedsel te kweken. Van de toepassing weefselkweek met producten zoals een snelle EHBO kit voor *first responders* en vlees 2.0 wordt een lage tot zeer lage impact op de nationale veiligheid verwacht.

Gepersonaliseerde diagnose, geneesmiddelen en therapie

Persoonlijke medicatie is vooral nuttig voor het beter en gerichter behandelen van patiënten, maar de impact hiervan op de nationale veiligheid is naar verwachting zeer beperkt. Voor de sociale en politieke stabiliteit is naar verwachting de impact gemiddeld tot hoog, omdat het mogelijk is dat er voor mensen met een bepaald DNA profiel wel een geneesmiddel mogelijk is en voor anderen niet.
Gepersonaliseerde diagnose kan positieve en negatieve effecten hebben; voor individuen betekent het een effectievere behandeling, maar grote kennis over het DNA van patiënten kan ook leiden tot aantasting van het recht tot behandeling of verzekering en tot aantasting van de privacy. Een negatief effect kan ook zijn dat de betaalbaarheid van de gezondheidszorg en het verzekeringsstelsel, in het bijzonder het daaraan ten grondslag liggende solidariteitsprincipe, onder druk komen te staan. Het is nu al zo dat de toename van (dure) behandelmethoden een zware druk legt op de gezondheidszorg en nieuwe (persoonlijk afgestemde) methoden dragen daar verder aan bij. Momenteel is er een discussie gaande over welke medicijnen verzekeraars moeten vergoeden bij (zeldzame) erfelijke afwijkingen, waarbij medicatie erg duur is en slechts een kleine groep patiënten geholpen wordt (zoals de ziekte van Pompe). Een aantasting van het solidariteitsprincipe zou, als dat tot grote ongelijkheid leidt, een negatief effect kunnen hebben op de sociale en politieke stabiliteit. De verwachting is echter dat het zelfcorrigerend vermogen van onze maatschappij op basis van ethische discussie en nationaal debat groot genoeg is om weerstand te bieden tegen ongewenst gebruik van dit soort toepassingen.

DNA methodieken

DNA methodieken bieden mogelijkheden voor identificatie van personen, bijvoorbeeld ten behoeve van grensbewaking. Een indirect effect op de nationale veiligheid is een betere bestrijding van criminaliteit doordat betere identificatie- en opsporingsmiddelen kunnen leiden tot een hogere pakkans. Waar echter een overzicht van de kennis over DNA tot grote inzichten in erfelijke aanleg van personen kan leiden, kan een dergelijk overzicht ook worden misbruikt. De verwachte impact voor de fysieke veiligheid en sociale en politieke stabiliteit is gemiddeld tot hoog.
De convergentie van DNA methodieken en ontwikkelingen in de neurotechnologie voor de toepassing van het verkrijgen van inzicht in menselijk gedrag (zie paragraaf 5.1) kunnen mogelijk een opmaat zijn voor de selectie of juist het ontzeggen van mensen voor bepaalde taken.

Biobrandstoffen

Van het gebruik van biobrandstoffen, zoals biodiesel of bio-ethanol wordt een beperkte impact op de economische en ecologische veiligheid verwacht. Het gaat hier vooral om de vervanging van fossiele brandstoffen.

Opmerking: Twee grote op handen zijnde veranderingen op het gebied van energie worden zeer verschillend beoordeeld. Materiaaltechnologie-experts verwachten dat decentralisatie van **energieopslag** grote gevolgen zal hebben voor de nationale veiligheid, terwijl bio- / gentechnologie-experts verwachten dat het gebruik van **biobrandstoffen** een beperkte impact zal hebben op de nationale veiligheid. Mogelijk zit het verschil in de onzekerheid die de decentralisatie van energieopslag met zich meebrengt. Er is nog weinig te zeggen over hoe de energiedistributie zal plaatsvinden en hoe stabiel het netwerk zal zijn. Een instabiel netwerk in deze tijd waarin alles draait op elektriciteit zou snel een nationale ramp zijn. Voor biobrandstoffen geldt dat dit naast de fossiele brandstoffen kan blijven bestaan, waarmee de onzekerheid betreffende het gebruik ervan minder is.

Opmerking: Vanuit bio- / gentechnologie zijn **biobrandstoffen** als een van de toepassingen naar voren gekomen. Ook vanuit andere technologieën zijn er energie gerelateerde toepassingen. Daarom gaat hoofdstuk 8 behalve op convergerende technologieën ook kort in op energietechnologie.

4.3 Selectie voor verdere uitwerking

De volgende toepassing is op basis van de consultatie van experts[11] geïdentificeerd voor verdere uitwerking van kansen en dreigingen:

- DNA methodieken (meest relevante product en dienst: opstellen van DNA databanken).

4.4 Uitdieping van kansen en dreigingen van geselecteerde toepassingen

De uitdieping van kansen en dreigingen wordt hieronder beschreven voor de voor verdere uitwerking geïdentificeerde toepassing.

DNA methodieken

Technologische ontwikkelingen hebben het mogelijk gemaakt om met minder en andersoortig materiaal, steeds sneller en goedkoper, een completer (en daarmee nauwkeuriger) DNA profiel in kaart te brengen.

Kansen

- Identificatie van personen met behulp van DNA profiel: Het sneller en goedkoper kunnen vergaren van een completer DNA profiel biedt een kans voor identificatie van personen, bijvoorbeeld ten behoeve van grensbewaking. Identificatie van personen zou dan mogelijk op basis van het DNA profiel kunnen gebeuren in plaats van op basis van andere biometrische kenmerken.
- Opsporing van virussen op basis van DNA: Een kans die wordt gezien is ook het sneller en beter opsporen van virussen en de verspreiding er van op basis van het DNA/RNA[12] van de virussen. Door de technologische ontwikkelingen op het gebied van DNA methodieken, kunnen virussen sneller worden geïdentificeerd en kan hun aanwezigheid dus beter in kaart worden gebracht.

Dreigingen

- Misbruik van DNA data: Een dreiging komt voort uit misbruik van DNA gegevens die onvoldoende zijn beschermd door de overheid of andere organisaties en worden gestolen door hackers of misbruikt door derden. Dit kan leiden tot verlies van vertrouwen in de overheid en andere organisaties. Misbruik van data is een algemene dreiging die geldt voor meerder toepassingen waarbij data wordt opgeslagen, zoals bijvoorbeeld ook rond *big data*. Omdat deze dreiging bij DNA data specifiek door experts is benoemd en dus blijkbaar specifiek geldt bij DNA data, is deze hier expliciet opgenomen.

Conclusies

- *Kansen:*
  - Identificatie van personen met behulp van DNA profiel;
  - Opsporing van virussen op basis van DNA.
- *Dreigingen:*
  - Misbruik van DNA data.

[11] Zie werkwijze in paragraaf 2.2.

[12] RNA (Ribonucleic Acid) is een van drie macromoleculen (met DNA en proteïnen) die essentieel zijn voor alle bekende levensvormen en lijkt qua chemische structuur sterk op DNA. RNA dient voor het kopiëren van genetische informatie die is opgeslagen in het DNA [19].

5 Neuro-technologie

5.1 Inventarisatie van toepassingen van technologische ontwikkelingen

Introductie
Onder de term neurotechnologie worden alle technologieën gegroepeerd die erop gericht zijn de werking van **hersenen en cognitie beter te begrijpen** dan wel te beïnvloeden. Het brein verwerkt prikkels uit de omgeving en ontwikkelt een respons op basis van deze prikkels. Elk brein is daarin uniek en heeft een eigen wijze van prikkelverwerking en responsopbouw. Toch zijn er ook patronen te vinden die veel mensen met elkaar delen.

Wanneer meer bekend wordt over deze patronen en de afwijkingen daarop, wordt het mogelijk normaal gedrag en afwijkend gedrag beter te begrijpen en wellicht te beïnvloeden. Ook biedt het mogelijkheden om aandoeningen of stoornissen van de hersenen beter te behandelen. Dit is het gebied van **neurodiagnostiek, therapieën en geneesmiddelen**.

Ook het aanbrengen van technologische middelen in of aan het brein om hersenactiviteit 'af te tappen' of te beïnvloeden behoort tot de mogelijkheden wanneer hersenactiviteit beter begrepen wordt. Hier **convergeert neurotechnologie met biotechnologie** (toevoegen van materialen aan organismen) **en informatietechnologie** (dataverzameling uit verschillende sensoren).

Inzicht in menselijk gedrag
De neurowetenschap kan gekarakteriseerd worden als een experimentele en technologie gedreven wetenschap. De verschillende technologieën die hun stempel gedrukt hebben op de neurowetenschap hebben gemeen dat zij het brein op een versimpelde manier willen benaderen; het gaat over de fysieke details, over de werking van neuronen, neurotransmitters, neurale netwerken, etc. [8]. Dit maakt duidelijk hoe het brein werkt, maar niet hoe (complex) menselijk gedrag tot stand komt. Het is een wetenschap die relatief theorie-arm is en juist theoretische modellen - waarin al die breindata die beschikbaar is een plaatsje kan vinden - kunnen de discipline verder brengen. Er moeten relaties gevonden worden tussen hersenactiviteit, beïnvloeding van deze activiteit én observeerbaar gedrag. Wanneer deze relaties helder zijn kan gedrag worden geduid en gestuurd door de hersenactiviteit te beïnvloeden. Dit laatste heet ook wel *optogenetics*. Beter inzicht in het functioneren van de hersenen geeft beter inzicht in menselijk gedrag en maakt het mogelijk om determinanten te identificeren waardoor mensen zijn te identificeren die meer kans maken op afwijkend (wellicht onwenselijk) gedrag.

Figuur 6: Neurotechnologie: technologische ontwikkelingen en toepassingen.

Neurofarmaca

Het beïnvloeden van de hersenactiviteit kan op verschillende wijzen plaatsvinden. De meest voorkomende manier van beïnvloeden is het gebruik van neurofarmaca die de biochemische huishouding beïnvloeden. In de basis zorgt dit ervoor dat het brein op een andere wijze reageert op externe prikkels. Fysiologisch betekent dit dat de signalen die het brein creëert er anders uit gaan zien. Het gebruik van neurofarmaca waaronder antidepressiva is de laatste jaren behoorlijk gegroeid. Ontwikkelingen op het gebied van neurofarmaca zouden kunnen leiden tot medicijnen die heel gericht en zonder bijwerkingen een heel smal spectrum aan hersenactiviteit beïnvloeden. Te denken valt aan geneesmiddelen tegen dementie. Gebruik buiten een pathologische context, bijvoorbeeld in een context van *human enhancement*[13], lijkt daarmee voor de hand te liggen[14].

Brain Machine Interfacing

Een Brain Machine Interface (BMI) is een directe koppeling tussen een brein en een machine. De interactie met een machine vindt bij het gebruik van een BMI niet meer plaats via een reguliere interface, zoals een toetsenbord, *touchscreen,* op basis van bewegingen, of eventueel stembesturing, maar direct met hersenpotentialen[15]. Bij het gebruik van actieve BMI's worden signalen die in het brein gegenereerd worden, gemeten en geïnterpreteerd. Op basis van deze interpretatie wordt een actieve toepassing - zoals een elektrische rolstoel of een pc - aangestuurd. Een dergelijke toepassing kan ook een *drone* zijn, of een wapensysteem in een gevechtsvliegtuig. De grootste uitdaging bij BMI is het op de juiste wijze interpreteren van de potentialen die in het brein gecreëerd worden. Er is ook een passieve variant van BMI waarbij de breinpotentialen alleen geïnterpreteerd worden om zodoende gedrag te kunnen voorspellen. Dit kan gebruikt worden in leugendetectie en anomaliedetectie. Breinpotentialen kunnen ook direct worden beïnvloed, bijvoorbeeld met behulp van Deep Brain Stimulation of Transcraniële Magnetische Stimulatie, waarbij respectievelijk een elektrode in een specifiek deel van de hersenen wordt ingebracht of door middel van een korte magneetpuls een stroom wordt opgewekt in het brein. Het brein kan ook getraind worden, bijvoorbeeld met behulp van cognitieve gedragsinterventies om anders te reageren op specifieke invloeden. Dergelijke interventies zijn echter niet onomstreden, juist omdat het brein nog veelal als *blackbox* wordt benaderd, waarbij alleen naar de in- en output gekeken wordt.

5.2 Identificatie van toepassingen relevant voor de nationale veiligheid

Tabel 4 geeft voor neurotechnologie een overzicht van de geïnventariseerde toepassingen met voorbeelden van producten en diensten die volgens de geraadpleegde experts mogelijk relevant worden geacht voor de nationale veiligheid[16].

De door de experts ingeschatte mate van kans of dreiging (zie bijlage H) wordt hieronder per geïnventariseerde toepassing toegelicht.

Inzicht in menselijk gedrag

Toepassingen waarmee potentiële ontsporing ontdekt kan worden hebben naar verwachting een hoge impact op de fysieke veiligheid en sociale en politieke stabiliteit. De

[13] Mensverbetering. Neurofarmaca kan worden gebruikt om mensen beter te laten functioneren, bijvoorbeeld om gevechtspiloten beter en langer te laten presteren of om het leervermogen te verbeteren.

[14] Duidelijk is dat dit een onderwerp is waaraan verschillende (maatschappelijke) vraagstukken zijn gerelateerd. In 2012 heeft het Rathenau Instituut een eerste publieksverkenning naar mensverbetering uitgevoerd [9].

[15] Een klein stroompje door de hersenen dat gemeten kan worden.

[16] Op basis van de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling'. Zie werkwijze in paragraaf 2.2.

Tabel 4: Neurotechnologie: overzicht van geïnventariseerde toepassingen met voorbeelden van producten en diensten.

Inzicht in menselijk gedrag *Producten en diensten:*	
Determinanten voor ontdekken potentiële ontsporing	Bepalen van determinanten voor het ontdekken van potentiële ontsporing.
Profiling	*Profiling* van mensen ten behoeve van selectie (van asielzoekers tot personeel) op basis van hersenonderzoek / *brain imaging*.
Optogenetics	Nauwkeurig en gericht beïnvloeden van werking van de hersenen. Ongewenste acties/ handelen voorkomen of bijsturen.
Neurofarmaca *Producten en diensten:*	
Geneesmiddelen tegen depressies	Medicatie die de neurologische paden van het brein veranderen waardoor prikkels bij een persoon niet meer leiden tot gevoelens van depressiviteit.
Geneesmiddelen tegen dementie	Medicatie voor het voorkomen of verminderen dat neurologische paden in de hersenen afbreken, voor het voorkomen van dementie.
Middel voor het verbeteren van het leervermogen	Middelen voor het verbeteren van het leervermogen of het presteren onder druk.
Brain Machine Interfacing *Producten en diensten:*	
Systeem voor aansturen van externe apparaten vanuit de hersenen.	Het direct koppelen van de hersenen aan computers voor bijvoorbeeld het aansturen van computers, *drones* en robots.

mogelijkheid om mensen met een grotere kans op afwijkend gedrag te identificeren, vergroot aan de ene kant de roep om dat in te voeren, maar aan de andere kant zullen mensen groeperingen die de bescherming van de privacy vooropstellen hier negatief tegenover staan. *Profiling*, en in mindere mate ook *optogenetics*, kan de nationale veiligheid verbeteren door efficiëntere beveiliging van bijvoorbeeld evenementen of luchthavens (territoriale veiligheid). Wanneer inzicht in menselijk gedrag zou worden ingezet om bepaalde mensen te selecteren en bijvoorbeeld in hun bewegingen te beperken, zou dit echter ook sociale onrust kunnen veroorzaken (potentiële impact op de sociale en politieke stabiliteit).

Neurofarmaca

De ontwikkelingen op het gebied van neurofarmaca maken deze middelen specifieker en beter. Mensen die iets mankeren kunnen worden behandeld, maar het is ook mogelijk om mensen die gezond zijn beter te laten functioneren (*human enhancement*). Hiermee zou de weerbaarheid kunnen worden versterkt. Het 'verbeteren' van mensen die gezond zijn, kan plaatsvinden in een context waar hele specifieke functionaliteiten van het brein gewenst zijn, zoals bij piloten van gevechtsvliegtuigen. Ook een heel andere categorie mensen, bijvoorbeeld delinquenten die hun acties plegen als gevolg van een hersenstoornis, zouden mogelijk geholpen kunnen worden. Aan het gebruik voor *human enhancement* kleven echter veel (juridische, ethische, ...) haken en ogen.
Een dreiging is dat kwaadwillende mensen (of staten) gebruik maken van neurofarmaca voor hun eigen *human enhancement* of om mensen dingen te laten doen die ze zelf niet willen.
Als neurofarmaca gebruikt gaan worden, en dan specifiek de middelen die zijn bedoeld voor *human enhancement*, bestaat de mogelijkheid dat er een kloof ontstaat tussen 'gebruikers' en mensen die niet gebruiken. Bij toepassing op grote schaal zou die kloof kunnen leiden tot een zekere mate van impact op de sociale en politieke stabiliteit vanwege de (al dan niet gepercipieerde) ongelijke behandeling of sociale uitsluiting van (groepen) mensen. Het op grote schaal toepassen of gebruiken van neurofarmaca op korte termijn wordt echter onwaarschijnlijk geacht. Het zelfcorrigerend vermogen van onze maatschappij op basis van ethische discussie en nationaal debat wordt groot genoeg geacht om weerstand te bieden tegen ongewenst gebruik van dit soort toepassingen.

Geneesmiddelen tegen depressies en middelen voor het verbeteren van het leervermogen bieden de mogelijkheid het presteren van mensen te verbeteren en geven daarmee kansen voor het vergroten van de fysieke en economische veiligheid en voor het versterken van de weerbaarheid. Het gebruik van middelen voor het verbeteren van het leervermogen is echter zeer omstreden.
Een kans die wordt genoemd is het voorkomen van de toename van het aantal dementiepatiënten die wordt voorzien. De mogelijkheid om de grote financiële gevolgen hiervan te voorkomen heeft invloed op de weerbaarheid

van de samenleving. Van geneesmiddelen tegen dementie wordt een positieve impact op de economische veiligheid (aantasting van de vitaliteit van de Nederlandse economie) verwacht. De grote economische impact komt voort uit de verwachting van dementiespecialisten dat bij het uitblijven van investeringen in dementiemedicatie zich bij wijze van spreken een 'nationale ramp' zal voordoen, omdat het behandelen van het stijgende aantal patiënten veel geld kost[17].

Brain Machine Interfacing

Van de toepassing Brain Machine Interfacing, bijvoorbeeld voor het aansturen van externe apparaten vanuit de hersenen, wordt een gemiddelde impact voor fysieke veiligheid en een hoge impact voor territoriale veiligheid verwacht. De reden hiervoor is de mogelijkheid om bijvoorbeeld *drones* met behulp van Brain Machine Interfacing te besturen voor het bewaken van grenzen en grondgebied.

5.3 Selectie voor verdere uitwerking

Er is op basis van de consultatie van experts[18] op het gebied van de nationale veiligheid geen toepassing geïdentificeerd voor verdere uitwerking van kansen en dreigingen. Van alle besproken toepassingen werd de impact op de nationale veiligheid te beperkt gevonden.

[17] http://www.volkskrant.nl/vk/nl/2672/Wetenschap-Gezondheid/article/detail/3419831/2013/04/04/Alzheimerspecialisten-voorspellen-nationale-ramp.dhtml

[18] Zie werkwijze in paragraaf 2.2.

6 Materiaal-technologie

6.1 Inventarisatie van toepassingen van technologische ontwikkelingen

Introductie

Materiaaltechnologie betreft technologie die de kennis over eigenschappen van natuurlijke en synthetisch gemaakte materialen toepasbaar maakt voor tal van doeleinden [1]. Materiaaltechnologie richt zich onder andere op het ontwikkelen van nieuwe productieprocessen en het borgen van vereiste eigenschappen in (nieuwe) materialen. De huidige ontwikkelingen richten zich op **high performance materialen**, **functionele coatings**, **geavanceerde industriële materialen**, **elektronische en optische materialen**, **slimme materialen**, **biomaterialen** en **energie materialen**. Chemische en fysische kennis om de structuur van het materiaal beter te begrijpen en te beheersen wordt toegepast voor de ontwikkeling van nieuwe productieprocessen en het realiseren van nieuwe eigenschappen van materialen [10]. Materiaaltechnologie kan gezien worden als de basis voor het mogelijk maken van vele technologische toepassingen.
Materiaaltechnologie bouwt op haar beurt vaak weer voort op ontwikkelingen in bijvoorbeeld bio- en nanotechnologie.

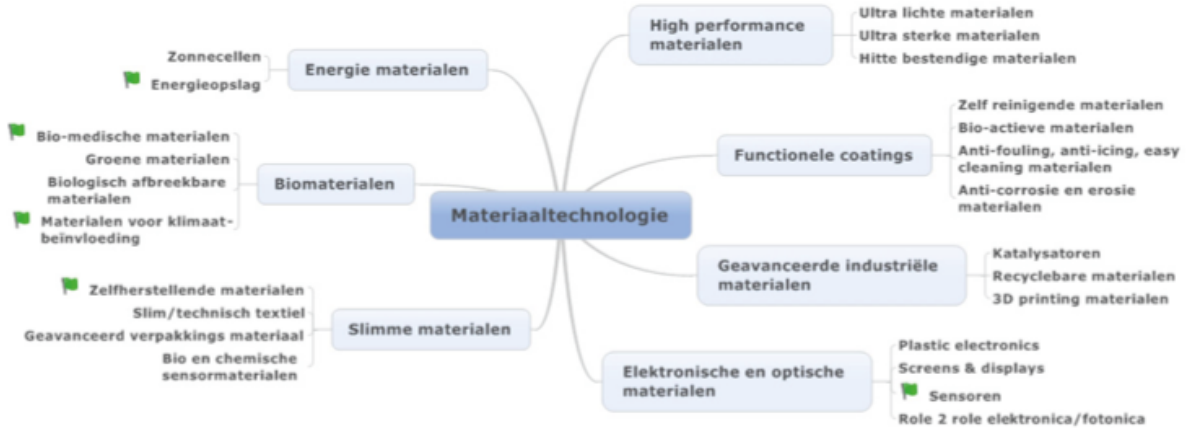
Sensoren

Sensoren kunnen gezien worden als elektronische voelers die één of meerdere omgevingsvariabelen in een elektronisch signaal[19] vertalen. Sensoren worden daarom ook weleens gekarakteriseerd als kunstmatige zintuigen en kunnen een machine interactief in contact brengen met zijn omgeving. Ontwikkelingen op het gebied van sensortechnologie hangen nauw samen met ontwikkelingen op het gebied van nanotechnologie en informatietechnologie (zie ook paragraaf 8.2)[20]. Sensoren worden kleiner, sneller, en nauwkeuriger en sensor data kan in steeds grotere hoeveelheden snel verwerkt en gecombineerd worden (zie ook *big Data* in paragraaf 7.1). Dit leidt ertoe dat sensoren in steeds meer producten toegepast worden en ook steeds meer aanwezig zijn in onze (dagelijkse) omgeving. Samen met de groeiende toepassing van kunstmatige intelligentie in producten, wordt het mogelijk de data die door sensoren gecreëerd wordt te verwerken. Bestaande producten zijn bijvoorbeeld mobiele telefoons met bewegingssensoren. Verschillende *apps* maken het mogelijk data te verzamelen en te

[19] In de context van informatietechnologie. Er zijn bijvoorbeeld ook mechanische sensoren en sensoren die gebruik maken van scheikundige, biologische of fysiologische principes.

[20] De toepassing sensoren wordt daarom verder in deze studie breder beschouwd dan alleen vanuit materiaaltechnologie.

Figuur 7: Materiaaltechnologie: technologische ontwikkelingen en toepassingen.



interpreteren voor de gebruiker. De bewegingen die je maakt in je slaap (gemeten door de telefoon op de matras) kunnen worden vertaald naar uitspraken over de kwaliteit van je slaap. Deze ontwikkelingen op het gebied van sensortechnologie zijn op hun beurt weer *enabling* voor het veld van robotica en het *internet of things*.

Zelfherstellende materialen

Zelfherstellende materialen zijn materialen die het vermogen hebben om, wanneer zij beschadigd raken, deze schade te herstellen zonder dat daar een (grote) externe stimulus voor nodig is [11]. De maatschappelijke waarde van zelfherstellende materialen kan liggen in het terugdringen van onderhouds- en herstelkosten en het voorkomen van incidenten ten gevolge van materiaalfalen. Wanneer een vliegtuig tijdens een vlucht schade oploopt dan kunnen de gevolgen rampzalig zijn en daarmee lijkt de vliegtuigindustrie een logische afnemer van zelfherstellende materialen. Ook kan gedacht worden aan gevechtssituaties waarbij het toebrengen en voorkomen van schade veelal de belangrijkste doelen zijn. Nanotechnologie is *enabling* technologie bij zelfherstellende materialen.

Materialen voor klimaatbeïnvloeding

Naarmate de invloed van het menselijk handelen op klimaatverandering minder betwist wordt en ondanks dat de transitie naar een duurzame samenleving maar langzaam lijkt te vorderen, steken steeds meer ideeën de kop op die actieve en directe klimaatbeïnvloeding als doel hebben. Uitgangspunt is dat wanneer de mens onbedoeld het klimaat kan beïnvloeden, zij dat ook welbewust kan doen in een voor de mens gewenste richting. Momenteel gebeurt het bijvoorbeeld incidenteel dat overheden zilverjodide in de lucht laten brengen om het te laten regenen, zoals tijdens de Olympische spelen in Peking van 2008. Het is echter een vervuilende methode.

Wanneer we het klimaat actief en gericht gaan beïnvloeden, zullen de gevolgen niet altijd vooraf duidelijk zijn omdat het klimaat als een zeer complex systeem beschouwd moet worden dat we maar ten dele begrijpen.

Bio-medische materialen

Bio-medische materialen zijn materialen van biologische of niet-biologische oorsprong die een medische toepassing hebben in een biologisch systeem. Een voorbeeld hiervan is een kunstgewricht. Doel van de toepassing is meestal het behoud, herstel of verbetering van lichaamsfuncties. Door ontwikkelingen op het gebied van biomedische materialen lukt het steeds beter om lichaamsfuncties te ondersteunen of over te nemen en lichaamsschade te herstellen. Ook 'mensverbetering', of het versterken van fysieke functies tot boven het normale niveau, behoort daarbij tot de mogelijkheden. Naarmate risico's op afstoting kleiner worden en de technische mogelijkheden groeien, zal de vraag naar 'buitengewone' toepassingen ook groeien. Hier zijn al voorbeelden van te vinden op het gebied van cosmetische ingrepen, maar ook ingrepen met als doel het verhogen van fysieke prestaties voor bijvoorbeeld sportbeoefenaars of militairen worden mogelijk.

Energieopslag

Er ontstaan andere mogelijkheden voor opslag van energie door gebruik te maken van nieuwe materialen. De toenemende toepassing van bijvoorbeeld windmolens, zonnecellen en elektrische auto's vraagt om energieopslag. Voor windmolens en zonnecellen omdat ze geen constante levering van energie hebben, en voor auto's omdat ze opgeslagen energie aan boord moeten hebben. Daarvoor zijn nieuwe manieren van energieopslag en efficiënte conversie noodzakelijk. Voor mobiliteit is elektrochemische accutechnologie vooralsnog het meest ontwikkeld. Het grootste nadeel van deze technologie is

Tabel 5: Materiaaltechnologie: overzicht van geïnventariseerde toepassingen met voorbeelden van producten en diensten.

Sensoren	
Producten en diensten:	
Crowdsourcing van sensoren	De overheid of andere instanties (ook personen) maken gebruik van de sensoren die mensen bij zich dragen (via mobiele telefoon of andere apparaten) of producten in zich hebben.
Overal sensoren en grote stromen informatie	Grote hoeveelheden producten bevatten sensoren en kunnen met elkaar en 'het internet' communiceren.
Zelfherstellende materialen	
Producten en diensten:	
Voor deze toepassing zijn tijdens de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling' geen relevante producten en diensten geïdentificeerd voor de nationale veiligheid.	
Materialen voor klimaatbeïnvloeding	
Producten en diensten:	
Beïnvloeden van het klimaat	Met producten, zoals zilverjodide, de atmosfeer beïnvloeden om het minder of meer te laten regenen op een (min of meer) gecontroleerde plek.
Bio-medische materialen	
Producten en diensten:	
'Mens-verbetering'	Producten voor het versterken van fysieke functies tot boven het normale niveau.
Energieopslag	
Producten en diensten:	
Decentralisatie van de energieopslag	Materialen waardoor lokaal energie kan worden opgeslagen.
CO_2 opvang	Materialen waardoor CO_2 gebonden kan worden en opgeslagen.

dat er in de accu's vaak gebruik gemaakt wordt van relatief zeldzame metalen, waarbij de winning van deze metalen milieuschade oplevert. Een mogelijk alternatief ligt in het gebruik van zogenaamde *phase change materials* kortweg PCM's[21]. Deze materialen zijn in staat om relatief grote hoeveelheden energie op te slaan dan wel los te laten. Hoewel dit bij alle faseovergangen (van vast naar vloeibaar, van vloeibaar naar gas, etc.) het geval is wordt bij de toepassing van PCM's gebruik gemaakt van de overgang van vast naar vloeistof (en vice versa). Voor grootschalige opslag van energie zoals dat bij intermitterende opwekkers[22] gewenst is, wordt ook gedacht aan opslag in koelhuizen, waterreservoirs of in de vorm van waterstof. Gerelateerd aan de uitstoot van kooldioxide (CO_2), dat onder andere vrij komt bij de opwekking van energie gebruikmakend van fossiele brandstoffen, kunnen nog genoemd worden nieuwe materialen waarmee kooldioxide kan worden gebonden, zodat er minder in de atmosfeer terecht komt.

[21] In het Nederlands wordt ook wel gebruik gemaakt van de naam Faseovergangsmaterialen (FOM).

[22] Energie-opwekkers met een sterke variatie van de geleverde energie, zoals bij windenergie en zonne-energie.

6.2 Identificatie van toepassingen relevant voor de nationale veiligheid

Tabel 5 geeft voor materiaaltechnologie een overzicht van de geïnventariseerde toepassingen met voorbeelden van producten en diensten opgenomen die volgens de geraadpleegde experts mogelijk relevant worden geacht voor de nationale veiligheid[23].

De door de experts ingeschatte mate van kans of dreiging (zie bijlage H) wordt hieronder per geïnventariseerde toepassing toegelicht.

Sensoren

Onder de toepassing sensoren zijn de hierboven genoemde producten en diensten '*crowdsourcing* van sensoren' en 'overal sensoren en grote stromen informatie' samen te

[23] Op basis van de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling'. Zie werkwijze in paragraaf 2.2.

nemen. De toepassing sensoren biedt kans om gedetailleerde informatie te verzamelen voor bijvoorbeeld de monitoring van de omgeving. Zo kan een sensor in combinatie met analysefuncties geïntegreerd op een chip (*lab-on-a-chip*) bijvoorbeeld worden gebruikt voor detectie van gif of explosieven (of grondstoffen daarvoor).
Een mogelijk risico is misbruik van de informatie en maatschappelijk verzet vanwege het overal plaatsen van sensoren. De verwachting is dat de weerbaarheid door de toepassing van sensoren kan worden versterkt.

Opmerking: De onder bio- / gentechnologie bij de toepassing **milieu monitoring** genoemde sensoren (zie paragraaf 4.2) worden, in tegenstelling tot de hierboven onder materiaaltechnologie genoemde **sensoren**, niet meegenomen in een verdere uitwerking van toepassingen. Het verschil in scores door de experts, is mogelijk te verklaren doordat sensoren genoemd onder materiaaltechnologie over allerlei typen sensoren gaat. Vooral de bundeling en interpretatie van al die verschillende gegevens maakt sensoren interessant voor de nationale veiligheid.

Zelfherstellende materialen

Tijdens de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling' (zie werkwijze in paragraaf 2.2) zijn voor de toepassing zelfherstellende materialen geen relevante producten en diensten geïdentificeerd voor de nationale veiligheid. Dat neemt niet weg dat deze materialen mogelijk interessant zijn. Te denken valt aan mogelijke consequenties voor sporenonderzoek. Als materiaal zichzelf kan herstellen zullen eventuele sporen mogelijk verloren gaan (vingerafdrukken, inbraaksporen, breuk en impactsporen, etc.). Deze toepassing is daarom een mogelijke kandidaat voor nader onderzoek na deze verkennende studie.

Materialen voor klimaatbeïnvloeding

Met materialen voor klimaatbeïnvloeding is het klimaat actief en gericht te beïnvloeden. Van de toepassing van materialen voor klimaatbeïnvloeding wordt een lage tot zeer lage impact verwacht voor de nationale veiligheid, omdat gebruik in Nederland de komende vijf jaar niet (op grote schaal) wordt voorzien De verwachting is dat het internationaal wel een grote rol kan spelen, in de zin dat gebruik van materialen voor klimaatbeïnvloeding buiten Nederland wel plaats zal vinden.

Bio-medische materialen

Bio-medische materialen bieden mogelijkheden voor 'mens-verbetering'. Net als voor neurofarmaca zou toepassing van deze materialen op grote schaal kunnen leiden tot (een al dan niet gepercipieerde) ongelijke behandeling of sociale uitsluiting van (groepen) mensen, met als gevolg een mogelijke impact op de sociale en politieke stabiliteit. Ook hier geldt dat het zelfcorrigerend vermogen van onze maatschappij op basis van ethische discussie en nationaal debat groot genoeg wordt geacht om weerstand te bieden tegen ongewenst gebruik van dit soort toepassingen.

Energieopslag

Decentralisatie van energieopslag biedt kansen in ecologische en geopolitieke zin; het verhoogt de duurzaamheid en zorgt mogelijk voor minder afhankelijkheid tussen landen[24]. Aan de andere kant kan decentralisatie mogelijk de kwetsbaarheid verhogen van de energievoorziening. De verwachte impact op de territoriale veiligheid, economische veiligheid en sociale en politieke stabiliteit is hoog tot zeer hoog.
Van CO_2 opvang wordt een lage tot zeer lage impact verwacht voor de nationale veiligheid, behalve voor de ecologische veiligheid waarvoor de verwachte impact gemiddeld tot hoog is.

Opmerking: Twee grote op handen zijnde veranderingen op het gebied van energie worden zeer verschillend beoordeeld. Materiaaltechnologie-experts verwachten dat decentralisatie van **energieopslag** grote gevolgen zal hebben voor de nationale veiligheid, terwijl bio- / gentechnologie-experts verwachten dat het gebruik van **biobrandstoffen** een beperkte impact zal hebben op de nationale veiligheid. Mogelijk zit het verschil in de onzekerheid die de decentralisatie van energieopslag met zich meebrengt. Er is nog weinig te zeggen over hoe de energiedistributie zal plaatsvinden en hoe stabiel het netwerk zal zijn. Een instabiel netwerk in deze tijd waarin alles draait op elektriciteit zou snel een nationale ramp zijn. Voor biobrandstoffen geldt dat dit naast de fossiele brandstoffen kan blijven bestaan, waarmee de onzekerheid betreffende het gebruik ervan minder is.

Opmerking: De impact van decentralisatie van **energieopslag** en de ontwikkeling van een **slimme energie infrastructuur (*Smart Grids*)** op de nationale veiligheid wordt door materiaaltechnologie-experts en informatietechnologie-experts zeer anders ingeschat; een hoge versus een lage impact op de nationale veiligheid. Op basis van deze conflicterende scores is voor deze toepassingen nader onderzoek aan te bevelen.

[24] Zie ook paragraaf 8.2, waar energietechniek in de breedte kort aan de orde komt.

Opmerking: Vanuit materiaaltechnologie is **energieopslag** als een van de toepassingen naar voren gekomen. Ook vanuit andere technologieën zijn er energie gerelateerde toepassingen. Daarom gaat hoofdstuk 8 naast op convergerende technologieën ook kort in op energietechnologie.

6.3 Selectie voor verdere uitwerking

De volgende toepassingen zijn op basis van de consultatie van experts[25] geïdentificeerd voor verdere uitwerking van kansen en dreigingen:

- Sensoren (meest relevante producten en diensten: '*crowdsourcing* van sensoren' en 'overal sensoren en grote stromen informatie');
- Energieopslag (meest relevante product en dienst: decentralisatie van de energieopslag).

6.4 Uitdieping van kansen en dreigingen van geselecteerde toepassingen

De uitdieping van kansen en dreigingen wordt hieronder beschreven voor de voor verdere uitwerking geïdentificeerde toepassingen.

Sensoren

Ontwikkelingen op de gebieden van materiaal-, bio- en nanotechnologie zorgen ervoor dat meer typen en kleinere sensoren beschikbaar komen - die meer verschillende dingen, beter kunnen meten - en dat sensoren goedkoper worden. Geïdentificeerde nieuwe producten en diensten hebben met name betrekking op het koppelen van verschillende sensordatastromen. In het geval van '*crowdsourcing* van sensoren' worden verschillende sensoren die in het bezit zijn van individuen of organisaties, samen voor een specifiek doel ingezet.

Kansen

- Vroegtijdig en gerichter ingrijpen bij incidenten door middel van sensoren: De ontwikkelingen van sensoren maken het mogelijk een informatie creërende en verwerkende laag op de bestaande samenleving te leggen. Sensorfusie, waarbij informatie uit verschillende sensoren wordt gecombineerd, kan leiden tot een beter inzicht dan de som der delen. Die inzichten helpen bij het treffen van maatregelen.

Voorbeelden van de mogelijkheden van sensoren zijn het nauwkeuriger en sneller identificeren en verifiëren van explosieve of giftige stoffen, nauwkeuriger verificatie en identificatie van personen op specifieke locaties (zoals vliegvelden), het monitoren van giftige stoffen in de lucht, of - zoals ook beschreven onder informatietechnologie - het real time monitoren van de conditie van dijken. Vroegtijdige waarschuwing van anomalieën maakt ingrijpen mogelijk, waardoor de kans op een incident of de impact daarvan wordt verminderd. Daarmee heeft het gebruik van sensoren effect op de territoriale veiligheid (geen of minder grondgebied dat onbruikbaar is), de fysieke veiligheid (minder doden of gewonden), de ecologische veiligheid (minder schade aan flora en fauna) en de economische veiligheid (lagere kosten voor het herstel). Het vergoot tevens de weerbaarheid tegen rampen en de gevolgen daarvan.

- Voorspellend vermogen ten aanzien van mogelijk optredende risico's: Het (grootschalig) verzamelen en integreren van (meet)gegevens van sensoren kan modelmatig inzicht verbeteren en het voorspellend vermogen van modellen vergroten. Daarmee zou beter voorspeld kunnen worden hoe groot het risico is op bepaalde incidenten (bijvoorbeeld monitoren van kwetsbare plekken in dijken in combinatie met meteorologische data en modellen) of – als zich een incident voordoet – hoe zich dat verder ontwikkeld.

Dreigingen

- Onjuiste of gemanipuleerde data: Net als bij onder meer NEMS/MEMS en het *internet of things* kunnen kwaadwillenden (statelijk dan wel niet-statelijk) data van sensoren misbruiken of manipuleren of het functioneren van sensoren en sensorsystemen verstoren, waardoor 'onnodig' incidenten en rampen gebeuren en/of verkeerde maatregelen worden genomen.

Conclusies

- *Kansen:*
  - Vroegtijdig en gerichter ingrijpen bij incidenten door middel van sensoren;
  - Voorspellend vermogen ten aanzien van mogelijk optredende risico's.
- *Dreigingen:*
  - Onjuiste of gemanipuleerde data.

Energieopslag

De uitputting van fossiele brandstoffen en milieuproblemen zijn de drijvende krachten achter de transformaties in de energieketen om meer gebruik te maken van duurzame energiebronnen. Tal van toepassingen worden ontwikkeld of gebruikt, bijvoorbeeld als het gaat om nieuwe manieren van energieopslag.

[25] Zie werkwijze in paragraaf 2.2.

Kansen

- Verminderen afhankelijkheid en kans op energie-uitval:
  De schaarste aan fossiele brandstoffen en de beperkte mogelijkheden tot energieopslag raken op twee manieren potentieel de nationale veiligheid. Allereerst levert de afhankelijkheid van fossiele brandstoffen en de relatieve schaarste hieraan tot een sterke afhankelijkheid van politiek instabiele landen of landen die hun machtspositie soms uitbuiten. Bij toenemende schaarste zou het ook tot internationale spanningen kunnen leiden. Daarenboven speelt dat fossiele brandstoffen vaak over grote afstanden getransporteerd moeten worden (pijpleidingen, tankschepen, etc). Deze transportlijnen vormen een kwetsbaarheid in de keten in zich zelf, maar in toenemende mate zijn zij ook subject aan piraterij die de kostbare *pay load* zich toe-eigent. Tevens is in enkele scenario's van de Nationale Risicobeoordeling aangegeven hoe groot de gevolgen kunnen zijn van energie-uitval. Met behulp van nieuwe vormen van energieopslag zouden de gevolgen kunnen worden beperkt.
  Nieuwe materialen voor energieopslag bieden kansen voor de transitie naar duurzame energiebronnen. Daarmee kunnen de bovengenoemde nadelen die verbonden zijn aan het verbruik van fossiele energiedragers worden beperkt. Wanneer decentrale energievoorziening gefaciliteerd wordt door nieuwe materialen voor energieopslag, waardoor lokaal grote hoeveelheden energie opgeslagen kunnen worden, en lange transportlijnen voorkomen kunnen worden, biedt dit een kans in het beperken van de gevolgen van grootschalige energie-uitval.

Conclusies

- *Kansen:*
  - Verminderen afhankelijkheid en kans op energie-uitval.

7 Informatie-technologie

7.1 Inventarisatie van toepassingen van technologische ontwikkelingen

Introductie

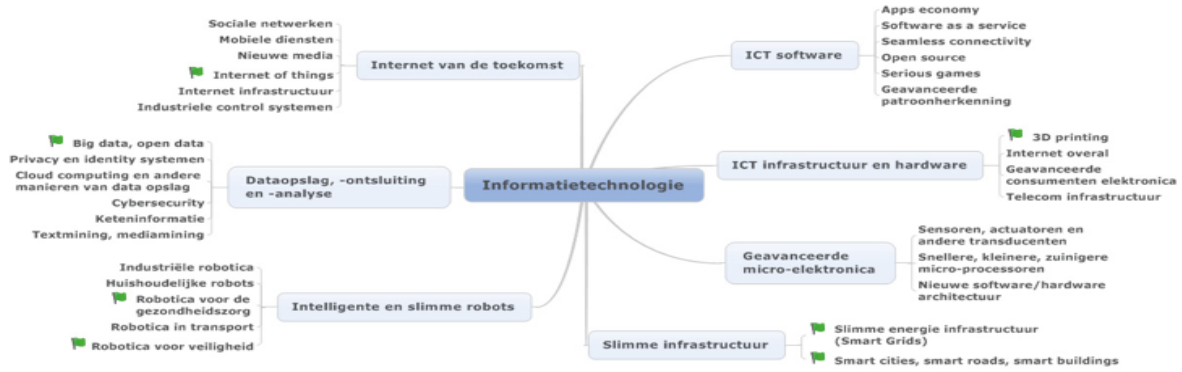
Informatietechnologie omvat alle technologie die gerelateerd is aan het conceptueel of fysiek definiëren, ontwerpen of fabriceren van systemen en toepassingen voor gegevensverzameling, -opslag, -verwerking, - transport en -beheer [1]. Op vele terreinen vervult informatietechnologie een ogenschijnlijk onmisbare rol, zoals in de zorg, het betaalsysteem, het energienet, wegennet, en het watermanagement. Informatie- en communicatietechnologie (ICT) biedt de mogelijkheid om via dataverbindingen op afstand te communiceren, te besturen en te overzien. Ontwikkelingen op het gebied van informatietechnologie leiden tot 'slimmere' en autonome systemen en maken bijvoorbeeld snelle complexe berekeningen en complexe simulaties mogelijk. Deze mogelijkheden dragen bij tot een efficiënte en effectieve taakuitvoering.

Ontwikkelingen op het gebied van informatietechnologie vinden plaats in de bouwstenen **ICT software**, **ICT infrastructuur en hardware** en **geavanceerde micro-elektronica**. Bestaande 'objecten' zoals dijken en wegen worden voorzien van ICT om zodoende **slimme infrastructuur** te vormen. Nieuwe 'objecten' zoals **intelligente en slimme robots** zien het levenslicht én al die producten raken steeds meer aan elkaar verbonden en wisselen data uit. Samen met technologische ontwikkelingen op het gebied van **dataopslag, -ontsluiting en –analyse -** die het mogelijk maken data aan elkaar te koppelen en daaruit conclusies te trekken - geven deze ontwikkelingen het **internet van de toekomst** mede vorm.

3D printing

3D *printing* is een toepassing waarmee driedimensionale producten door een printer gefabriceerd kunnen worden, waarbij alleen een basismateriaal en data over de vorm als invoer dienen. Het effect van toenemend gebruik van 3D *printing* kan verstrekkend zijn en het huidige economische paradigma van productie, transport en consumptie flink omgooien. De ontwikkelingen in de muziekindustrie van de afgelopen decennia kunnen daarvoor als illustratie dienen. Waar eerst de aanschaf van 'harde' producten - dragers van muziek - centraal stond, is deze langzaam opgeschoven naar de aankoop van data (bijvoorbeeld iTunes) en de aankoop van toegang tot data (bijvoorbeeld Spotify). Experts geven aan dat deze manier van aanschaffen waarschijnlijk vertaalbaar is naar 3D *printing*. Dit zou kunnen betekenen dat een consument geen producten meer aanschaft, maar alleen basismateriaal en de data om een product te printen. Dat kan gaan om gewone gebruiksvoorwerpen, maar ook om voedsel en wapens. 3D *printing* zou in zijn uiterste consequentie de vele nationale en internationale transportketens overbodig maken omdat producten overal op kleine schaal geprint kunnen

Figuur 8: Informatietechnologie: technologische ontwikkelingen en toepassingen.



worden en slechts de logistiek van basismateriaal doet voortbestaan. 3D *printing* doorbreekt het systeem van regulering van goederen doordat iedereen zelf producten kan maken.

Slimme energie infrastructuur (Smart Grids)

De huidige energievoorziening kan gekarakteriseerd worden als een gecentraliseerd systeem waarbij energie vanuit een aantal grote centrale opwekkers vervoerd wordt naar de vele eindafnemers. De ontwikkeling van slimme infrastructuren maakt de toepassing van een decentrale slimme energie infrastructuur (*Smart Grids*) mogelijk.
Een dergelijke nieuwe energie infrastructuur is meer dan de huidige infrastructuur geschikt voor tweerichtingsverkeer en het faciliteren van decentrale energieopwekking. In de praktijk betekent dit dat de huidige infrastructuur niet vervangen hoeft te worden, maar wel dat intelligentie toegevoegd moet worden. Op de bestaande infrastructuur moet als het ware een ICT infrastructuur gelegd worden die het mogelijk maakt om de energievraag te matchen met het energieaanbod van alle kleine opwekkers.
Een kenmerk van deze opwekkers is dat ze, in vergelijking met de klassieke massa-opwekkers, klein zijn. Klein in opbrengst, maar ook klein in omvang. Dit zorgt ervoor dat er veel meer van dit soort opwekkers nodig zijn om aan een bepaalde energievraag te kunnen voldoen. Maar dit maakt ook mogelijk dat ze op veel meer plaatsen relatief gemakkelijk te installeren zijn. De eindgebruikers - zoals we die kennen vanuit het oude centrale paradigma (waarbij energie centraal wordt opgewekt) - kunnen daarom nu ook de rol van energieproducent op zich gaan nemen. Zij kunnen bijvoorbeeld zonnecellen aanschaffen en daarmee in hun eigen energiebehoefte voorzien én mogelijk ook in de energiebehoefte van anderen.

Smart cities, smart roads, smart buildings

De toevoeging van een netwerk van sensoren en informatie- en communicatiemogelijkheden aan de harde infrastructuur, het interpreteren van de data en automatisch daarop sturen maakt van huidige steden in toenemende mate *smart cities*. Het gaat niet alleen over het slim aansturen van de infrastructuur om daarmee bijvoorbeeld verkeersstromen te leiden, maar ook om de connecties die ontstaan tussen mensen, gebouwen en producten. De ontwikkelingen op het gebied van slimme infrastructuur zullen de toepassing *smart roads* mogelijk maken.
Intelligente wegen kunnen zich een beeld vormen van de omstandigheden (gladheid, drukte, mist) en via informatieverstrekking het verkeer daarop laten reageren. Een toevoeging aan het wegdek maakt het mogelijk om energie op te wekken uit wegen [21]. Op termijn laadt je auto zich zelf op, waar hij ook staat, door elementen in het wegdek.
Ook gebouwen kunnen worden uitgerust met sensoren. Op basis van het opgebouwde beeld van de bewegingen in het gebouw kan klimaatbeheersing of de licht intensiteit worden aangestuurd op de voorkeuren van de medewerkers.

Robotica voor veiligheid

De ontwikkelingen op het gebied van micro-elektronica, sensortechnologie en kunstmatige intelligentie hebben ontwikkelingen op het gebied van robottechnologie enorm gestimuleerd. Semiautonome robots worden bijvoorbeeld al ingezet in de zorg, maar ook in oorlogsvoering. De *drone* aanvallen die uitgevoerd worden in Afghanistan en Pakistan zijn inmiddels bekend, maar robots met offensieve capaciteiten worden ook al gebruikt voor grensbewaking op de grens tussen Noord- en Zuid-Korea. Ontwikkelingen op het gebied van nanotechnologie, kunstmatige intelligentie en sensortechnologie zijn in de komende jaren belangrijke *enablers* en stimulatoren voor robottechnologie. De meest voor de hand liggende toepassingsgebieden van robottechnologie zijn die gebieden waar de inzet van mensen minder efficiënt, minder effectief of onmogelijk is. Hierbij kan gedacht

worden aan handelingen waarbij mensenlevens in gevaar komen (ontmantelen van explosieven, aanvalsacties op vijandelijke stellingen) of bijvoorbeeld zeer eenvoudige tijdrovende handelingen (observaties en surveillances) waar de inzet van mensen niet kostenefficiënt is.

Robotica voor de gezondheidszorg

Robotica is in de afgelopen jaren al een grote rol gaan spelen in de gezondheidszorg en ontwikkelt zich verder. Robotica kan ondersteunen bij het trainen van artsen en assistenten, maar een sociale robot kan bijvoorbeeld ook worden ingezet om ouderen die ontwikkelende dementie hebben, gerust te stellen (iCat [22]).
Door gebruik te maken van robotica kunnen chirurgen preciezer werken, doordat robots de aansturing van de instrumenten (deels) overnemen. Een extreme variant daarvan is het opereren op afstand, waardoor chirurgen bijvoorbeeld uitgezonden militairen op afstand kunnen behandelen.

Big data, open data

Technologische ontwikkelingen op het gebied van dataopslag, -ontsluiting en -analyse maken het genereren van informatie uit grote en complexe hoeveelheden data mogelijk. Data wordt in toenemende mate open aangeboden, zodat derden deze kunnen gebruiken voor een (informatie)dienst.
De hoeveelheid data die dagelijks gecreëerd wordt, groeit exponentieel en door ontwikkelingen op het gebied van sensortechnologie en kunstmatige intelligentie zal deze trend zich blijven doorzetten. Het internetverkeer stijgt naar een exabyte[26] per dag in 2013 (was een exabyte per jaar in 2001) [12]. Veel van deze data wordt opgeslagen in datasets in verschillende formats en op verschillende plaatsen.
Al deze data vormt in potentie een schat aan informatie, maar het ontwikkelen van informatie uit die data is een uitdaging. Informatie is namelijk pas informatie wanneer het op een zeker moment in een behoefte aan kennis voorziet. Denk bijvoorbeeld aan het verzamelen en ontsluiten van data ten behoeve van beeldopbouw bij rampenbestrijding. Om uit zeer grote hoeveelheden ongestructureerde data informatie te extraheren zijn veel verwerkingscapaciteit en/of slimme methodieken nodig. Zoek- en analysemethodieken worden ontwikkeld om gemakkelijk de juiste data te vinden of te combineren tot de gewenste informatie. Deze informatie kan worden gebruikt voor bijvoorbeeld het identificeren van gedragspatronen en het maken van correlaties en voorspellende evaluaties.

Internet of things

Het *internet of things* ontstaat doordat niet alleen mensen informatie via internet uitwisselen, maar doordat dit ook in toenemende mate door aan het internet gekoppelde 'dingen' gebeurt. De term *internet of things* duidt op de expansiedrift van 'het internet' dat op zichzelf als term een steeds diffuser karakter krijgt. Er kan nauwelijks meer gesproken worden over 'het internet' omdat 'het' steeds meer een constellatie wordt van verbindingen, activiteiten en mogelijkheden die slechts het transport van data en connectiviteit als gemene deler hebben. Nadat instituties en individuen zich met elkaar verbonden in cyberspace, is het nu aan gebruiksvoorwerpen om zich als het ware bij hen te voegen. In de praktijk betekent dit dat smartphones, thermostaten, televisies, auto's, etc. een internetverbinding krijgen. Er kan echter ook gedacht worden aan (de besturing van) bruggen en sluizen en het toepassen van diverse sensoren in dijklichamen, die de verschillende variabelen die van invloed zijn op de dijkkwaliteit continu monitoren. Door toevoeging van sensoren en kunstmatige intelligentie kunnen zodoende ook 'de voorwerpen' met elkaar gaan communiceren en wordt de noodzakelijkheid van menselijke interactie weggenomen; in ieder geval vanuit een strikt operationele doelstelling.
De eerder beschreven ontwikkelingen op het gebied van sensortechnologie en kunstmatige intelligentie zijn *enabling* voor deze toepassing.

7.2 Identificatie van toepassingen relevant voor de nationale veiligheid

Tabel 6 geeft voor informatietechnologie een overzicht van de geïnventariseerde toepassingen met voorbeelden van producten en diensten opgenomen die volgens de geraadpleegde experts mogelijk relevant worden geacht voor de nationale veiligheid[27].

De door de experts ingeschatte mate van kans of dreiging (zie bijlage H) wordt hieronder per geïnventariseerde toepassing toegelicht.

3D printing

3D *printing* maakt het mogelijk om zelf (desgewenst naar eigen behoefte aangepaste) gebruiksvoorwerpen te maken, zowel voor burgers als voor bedrijven en instellingen. Dat zal de huidige wijze van industriële productie

[26] 1 exabyte = 1.000 petabyte = 1.000.000 terabyte = 1.000.000.000 gigabyte.

[27] Op basis van de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling'. Zie werkwijze in paragraaf 2.2.

Tabel 6: Informatietechnologie: overzicht van geïnventariseerde toepassingen met voorbeelden van producten en diensten.

3D printing	
Producten en diensten:	
Printen van gebruiks-voorwerpen	Printers die het mogelijk maken allerlei gebruiksvoorwerpen te printen, waaronder wapens.
Printen van voedsel	Printers die het mogelijk maken voedsel te printen.
Slimme energie infrastructuur (Smart Grids)	
Producten en diensten:	
Infrastructuur voor decentralisatie van energieopwekking	Infrastructuur waarmee energie decentraal kan worden opgewekt.
Smart cities, smart roads, smart buildings	
Producten en diensten:	
Intelligente transport systemen	Intelligente systemen die multimodaal transport van mensen en middelen in en rond de stad mogelijk maken. *(Meegenomen onder Internet of things.)*
Robotica voor veiligheid	
Producten en diensten:	
Inspectierobots	Robots die in gevaarlijke omstandigheden inspecties kunnen uitvoeren.
Surveillance bots	Robots of *drones* die surveilleren bijvoorbeeld tijdens evenementen, crises of ten behoeve van grensbewaking.
Robotica voor de gezondheidszorg	
Producten en diensten:	
Robotica in de operatiekamer	Middelen om tijdens de operatie nauwkeuriger of langer te kunnen werken.
Telerobotica	Middelen om op afstand te kunnen opereren.
Big data, open data	
Producten en diensten:	
Big data voor rampen- bestrijding	Ontsluiting van *big data* (vooral open bronnen) voor de beeldopbouw tijdens rampen ten behoeve van crisiscoördinatie of communicatie met burgers.
Internet of things	
Producten en diensten:	
Intelligente transport systemen	Intelligente systemen die multimodaal transport van mensen en middelen in en rond de stad mogelijk maken.
Bewaking en aansturing kritieke infrastructuur	Monitoring en bediening van kritieke infrastructuur (zoals sluizen, bruggen, verdeelstations) volledig via sensoren en internet.
Dijkbewaking	Sensoren in een dijk voor het monitoren van de sterkte van het systeem.

gedeeltelijk op zijn kop zetten en daarmee gevolgen hebben voor de economie. Het zelf kunnen maken van gebruiksvoorwerpen kan positieve en negatieve gevolgen hebben. Bij negatieve gevolgen kan gedacht worden aan het zelf produceren van wapens. De verwachte impact van het 3D printen van gebruiksvoorwerpen, waaronder wapens, is gemiddeld voor de fysieke veiligheid en de economische veiligheid. Er wordt een negatieve invloed op de weerbaarheid verwacht, omdat het vermogen tot bescherming en verdediging tegen dreigingen door bijvoorbeeld de mogelijkheid tot het zelf produceren van wapens kan worden aangetast.

Van het 3D printen van voedsel wordt een lage impact voor de territoriale veiligheid en sociale en politieke stabiliteit verwacht en een gemiddeld tot hoge impact voor de fysieke, economische en ecologische veiligheid en een versterking van de weerbaarheid.

Opmerking: Gezien het feit dat de toepassing **3D *printing*** recent veel in het nieuws is geweest, waarbij ook het fabriceren van (onderdelen) van wapens aan de orde is gekomen, lijkt de door de experts gegeven score laag.

Slimme energie infrastructuur (Smart Grids)

De ontwikkeling van slimme infrastructuren maken de toepassing van een decentrale slimme energie infrastructuur (*Smart Grids*) mogelijk. De infrastructuur zou hierdoor enerzijds robuuster kunnen worden (door de decentralisatie). Anderzijds mogelijk ook kwetsbaarder (door de koppeling van systemen). Van decentralisatie van de energieopwekking wordt door informatietechnologie-experts een zeer lage impact verwacht op de territoriale veiligheid en sociale en politieke stabiliteit, een laag tot gemiddelde impact voor de ecologische veiligheid en de fysieke veiligheid en een hoge tot zeer hoge impact voor de economische veiligheid.

Opmerking: De impact van decentralisatie van **energieopslag** en de ontwikkeling van een **slimme energie infrastructuur (*Smart Grids*)** op de nationale veiligheid wordt door materiaaltechnologie-experts en informatietechnologie-experts zeer anders ingeschat; een hoge versus een lage impact op de nationale veiligheid. Op basis van deze conflicterende scores is voor deze toepassingen nader onderzoek na deze verkennende studie aan te bevelen.

Opmerking: Vanuit informatietechnologie is **slimme energie infrastructuur (*Smart Grids*)** als een van de toepassingen naar voren gekomen. Ook vanuit andere technologieën zijn er energie gerelateerde toepassingen. Daarom gaat hoofdstuk 8 naast op convergerende technologieën ook kort in op energietechnologie.

Robotica voor veiligheid

Inspectierobots bieden een kans omdat hiermee in gevaarlijke omstandigheden inspecties kunnen worden uitgevoerd. Van inspectierobots wordt een impact op de nationale veiligheid verwacht die rond laag en gemiddeld ligt. Voor de weerbaarheid wordt verwacht dat deze kan worden versterkt.
Surveillance bots komen naar voren in de selectie vanwege de mogelijkheden surveillance automatisch en op afstand uit te laten voeren ten behoeve van de hulpdiensten. De verkregen informatie kan ook worden ingezet om de zelfredzaamheid van burgers te vergroten. Keerzijde is dat zich privacy issues kunnen vormen en daarmee mogelijk weerstand tegen deze vorm van surveillance. De verwachte impact ligt tussen laag en gemiddeld voor de fysieke en economische veiligheid tot hoog en zeer hoog voor respectievelijk de territoriale veiligheid en de sociale en politieke stabiliteit. Voor de weerbaarheid wordt verwacht dat deze kan worden versterkt.

Robotica voor de gezondheidszorg

Robotica in de gezondheidszorg is vooral gericht op het automatiseren en verbeteren van de gezondheidszorg. Hiervan wordt een lage tot gemiddelde impact verwacht voor de nationale veiligheid.

Big data, open data

Veel organisaties zijn bezig zich op *big data* te oriënteren. Een eerste stap is vaak om te kijken naar alle data die in 'eigen huis' wordt gegenereerd. Een volgende stap is het combineren van die data met data uit andere gebieden. Dat kan *open data* betreffen of data die door samenwerking met een andere partij verkregen is. Voor de overheid is vooral die combinatie interessant: het relateren van de eigen data met die van anderen, bijvoorbeeld voor toezicht en handhaving.
Bij rampen kan *big data* worden gebruikt voor beeldopbouw ten behoeve van crisiscoördinatie of communicatie met burgers. Voor de weerbaarheid wordt verwacht dat deze hiermee sterk kan worden verhoogd, bijvoorbeeld door slim en efficiënt informatie uit grote en complexe hoeveelheden data te genereren.

Internet of things

Van intelligente transport systemen wordt een lage tot gemiddelde impact verwacht op de nationale veiligheid, omdat deze primair zijn gericht op transport en daardoor slechts een indirecte koppeling met de nationale veiligheid hebben.
Dijkbewaking en bewaking en aansturing van vitale infrastructuur scoren beide hoog. Dat geldt vooral met betrekking tot de fysieke veiligheid en ecologische veiligheid waar een hoge tot zeer hoge impact voor de nationale veiligheid wordt verwacht. Experts geven aan dat er zowel kansen als dreigingen zijn. Kansen omdat - ook in combinatie met *big data* - zwakke plekken gemonitord kunnen worden, dreigingen omdat door de steeds grotere graad van afhankelijkheid van elektronica voor de besturing van vitale infrastructuur deze ook kwetsbaar wordt voor (moedwillige) verstoring met mogelijk ongelukken en negatieve economische gevolgen. Een dreiging kan ook zijn dat anderen de informatie misbruiken, bijvoorbeeld door de zwakke plekken in een dijk te kunnen constateren.

7.3 Selectie voor verdere uitwerking

De volgende toepassingen zijn op basis van de consultatie van experts[28] geïdentificeerd voor verdere uitwerking van kansen en dreigingen:

- 3D *printing* (meest relevante product en dienst: printen van gebruiksvoorwerpen);
- Robotica voor veiligheid (meest relevante product en dienst: *surveillance bots*);
- *Big data, open data* (meest relevante product en dienst: *big data* voor rampenbestrijding);
- *Internet of things* (meest relevante producten en diensten: bewaking en aansturing kritieke infrastructuur en dijkbewaking).

7.4 Uitdieping van kansen en dreigingen van geselecteerde toepassingen

De uitdieping van kansen en dreigingen wordt hieronder beschreven voor de voor verdere uitwerking geïdentificeerde toepassingen.

3D printing

3D *printing* maakt het mogelijk driedimensionale producten, waaronder gebruiksvoorwerpen, te produceren. Daarvoor zijn alleen een 3D printer, basismaterialen en data met de 'bouwtekening' benodigd.

Kansen

- Printen van producten ten behoeve van veiligheidsdiensten: 3D *printing* biedt onder meer de mogelijkheid producten of reserveonderdelen uit te printen. Dit kan een kans zijn voor defensie en openbare orde - en veiligheidsdiensten om zelf deze onderdelen uit te printen. Hoewel de uiteindelijke gebruiksmogelijkheden momenteel nog niet helder zijn, is het denkbaar dat dit zou kunnen leiden tot een versterking van de weerbaarheid door snellere beschikbaarheid van hulpmiddelen of reserveonderdelen.

Dreigingen

- Ondermijning gereguleerde producten (o.a. wapens): Veel goederen en producten zijn gereguleerd (bijvoorbeeld wapenproductie en -export). 3D *printing* doorbreekt dit systeem doordat iedereen nu zelf producten kan maken. Regulering wordt lastiger te handhaven. Daarnaast bevordert 3D *printing* proliferatie. De verwachting is dat binnen redelijk afzienbare tijd iedereen toegang kan krijgen tot 3D *printing*. Via internet is data met productbeschrijvingen eenvoudig uit te wisselen. Wellicht kan het fabriceren van wapens - alhoewel vooralsnog waarschijnlijk van mindere kwaliteit dan echte wapens - dan ook voor particulieren (bijvoorbeeld de schooljeugd) toegankelijk worden. Het feit dat 'iedere burger zijn eigen wapens kan maken', kan ook leiden tot een sterker gevoel van onveiligheid. Door aandacht er omheen - bijvoorbeeld in combinatie met aandacht in het nieuws en berichten via de sociale media - kan dit onrust veroorzaken: angst en een gevoel van onveiligheid.

Conclusies

- *Kansen:*
  - Printen van producten ten behoeve van veiligheidsdiensten.
- *Dreigingen:*
  - Ondermijning gereguleerde producten (o.a. wapens).

Robotica voor veiligheid

Technologische ontwikkelingen - onder meer op het gebied van informatietechnologie - leveren de bouwstenen voor verdere ontwikkeling van intelligente en slimme robots. Deze robots kunnen worden ingezet ten behoeve van de veiligheid. Bijvoorbeeld voor het verrichten van inspecties in voor de mens gevaarlijke omgevingen of voor het uitvoeren van surveillances.

Kansen

- Inzet robots en *drones* voor veiligheidstaken: Er ontstaan nieuwe mogelijkheden voor (routinematige) surveillance en gevaarlijke inspecties (bijvoorbeeld op moeilijk bereikbare plekken bij een ramp) doordat robots deze taken van mensen kunnen overnemen. Dit geeft de overheid en hulpverleners de mogelijkheid om in extreme gevaarzetting toch in actie te komen, waardoor incidenten en rampen beter en efficiënter bestreden (en soms voorkomen) kunnen worden.
  De met gerobotiseerde observatie/surveillance verkregen datasets kunnen bijdragen aan verbeterde informatievoorziening en een actueel veiligheidsbeeld tijdens een incident. Die informatie kan worden gebruikt voor een verbeterde inzetbaarheid van hulpdiensten (versterking weerbaarheid) en mogelijk ook tot verbeterde zelfredzaamheid van de burger door deze (op basis van de informatie) een beter handelingsperspectief te bieden, bijvoorbeeld bij rampen.

[28] Zie werkwijze in paragraaf 2.2.

Dreigingen

- Inzet robots en *drones* door kwaadwillenden:
  Kwaadwillenden kunnen robots en *drones* inzetten voor hetzelfde type activiteiten als dat veiligheidsdiensten zouden kunnen. Het gaat dan om observatie en monitoring van activiteiten van burgers, overheidsdiensten en bedrijven. Veel verder gaat het gebruik van een robot of *drone* als platform voor het vervoer van gif of explosieven.
  Het gebruik als middel om een explosief of gif te vervoeren en 'af te leveren' op een doelwit is denkbaar en vormt een dreiging. Het afleveren van een explosief met een *drone* of robot maakt het lastiger te achterhalen wie er achter een aanslag zit. *Drones* kunnen momenteel al gedetecteerd worden in het Nederlandse luchtruim, de vraag is echter of er ook capaciteit is de *drone* te onderscheppen. Het feit dat het eenvoudiger wordt om explosieven af te leveren op normaal zeer goed beveiligde locaties heeft invloed op de fysieke veiligheid (mogelijk doden of gewonden) en de sociale en politieke stabiliteit (onrust, angst over wat mogelijk is).
  Robots en *drones* worden steeds goedkoper en komen ook beschikbaar voor burgers. Burgers kunnen zelf met goedkope (gedeeltelijk) gerobotiseerde vliegtuigjes gaan observeren. Hierbij komt de privacy van individuen in gevaar. Hetzelfde geldt overigens voor surveillance met *drones* uitgevoerd door overheidsinstanties.
- Hacken van robots voor veiligheid: Een dreiging is ook de mogelijkheid dat kwaadwillenden robots die worden ingezet voor veiligheid hacken of 'besmetten' met een softwarevirus waardoor hun functioneren verandert en daarmee overheidsactiviteiten worden verstoord.

Conclusies

- *Kansen:*
  - Inzet robots en *drones* voor veiligheidstaken.
- *Dreigingen:*
  - Inzet robots en *drones* door kwaadwillenden;
  - Hacken van robots voor veiligheid.

Big data, open data

De hoeveelheid data die dagelijks gecreëerd wordt, groeit exponentieel en grote hoeveelheden data wordt in toenemende mate 'open' (dat wil zeggen voor iedereen toegankelijk) beschikbaar. Door gebruik te maken van veel verwerkingscapaciteit en/of slimme methodieken - en ook die zijn steeds meer een gemakkelijker beschikbaar - is het steeds beter mogelijk uiteenlopende informatie te extraheren uit de zeer grote hoeveelheden (ongestructureerde) data.

Kansen

- Gebruik voor preventie, proactie en respons van incidenten en crises: De toepassing van *big data, open data* biedt in potentie kansen voor het verhogen van de weerbaarheid, bijvoorbeeld door slim en efficiënt informatie uit grote en complexe hoeveelheden data te genereren. Goede analyses (correlaties en voorspellende evaluaties) op grote databestanden kunnen nuttige informatie opleveren, zoals inzicht in gedragspatronen van (groepen) mensen, op basis waarvan gericht kan worden gehandeld.

Dreigingen

- Vervuiling van databestanden: Mogelijke vervuiling van databestanden kan er toe leiden dat mensen hun identiteit kwijtraken of ten onrechte ergens van worden beschuldigd of dat de financiële huishouding van organisaties of overheden niet meer klopt.
- Manipulatie en misbruik van data en/of methodieken door kwaadwillenden: Data en methodieken om uit grote hoeveelheden data informatie te extraheren zouden kunnen worden afgevangen, gemonitord en/of gemanipuleerd door statelijke en niet-statelijke actoren voor (ondersteuning van) illegale activiteiten en tegenwerking van overheidsoptreden. Er ontstaat een issue over gegevenssoevereiniteit. Dit kan ook leiden tot een asymmetrie en een verstoring van de machtsbalans, omdat grote bedrijven en/of staten betere toegang hebben tot data en middelen.
  Daarnaast kan waar data uit vele verschillende bronnen wordt samengevoegd een zeer gedetailleerd beeld ontstaan over de gedragingen van een individu. Een dergelijk beeld kan op allerlei wijzen misbruikt worden door criminelen. Dit kan voornamelijk effect hebben op de sociale en politieke stabiliteit omdat de burgers verminderd vertrouwen hebben in de overheid of andere betrokken organisaties die, naar de mening van de burgers zelf, hun privacy moeten waarborgen. Ook in Nederland zijn er tegenbewegingen. Daarom zijn aan *big data, open data* veel randvoorwaarden als privacy (o.a. doelbinding van de data) verbonden.

Conclusies

- *Kansen:*
  - Gebruik voor preventie, proactie en respons van incidenten en crises.
- *Dreigingen:*
  - Vervuiling van databestanden;
  - Manipulatie en misbruik van data en/of methodieken door kwaadwillenden.

Internet of things

Technologische ontwikkelingen op het gebied van informatietechnologie leiden er toe dat ook steeds meer 'dingen' - zoals apparaten, infrastructuur en voertuigen - via internet worden verbonden en gegevens met elkaar kunnen uitwisselen.

Kansen

- Inzet ter identificatie van en voorkoming van incidenten: *Internet of things* biedt veel nieuwe mogelijkheden binnen verschillende domeinen van de samenleving zoals mobiliteit en logistiek, gezondheidszorg en industrie. De gegevens die binnen deze domeinen worden verzameld, kunnen worden gebruikt als basis om verschillende diensten te ontwikkelen. Het biedt een schier oneindig potentieel voor creatievelingen om nieuwe diensten en producten te ontwikkelen buiten de geijkte kaders. Een voor deze studie bij *internet of things* geïdentificeerde dienst is de bewaking en aansturing van processen in de vitale infrastructuur, zoals monitoring van dijken en monitoring en bediening van sluizen, bruggen en verdeelstations. Dit kan dan voor een groot deel automatisch geschieden. Ook kan monitoring van fysieke elementen worden gekoppeld aan digitale gegevens. *Internet of things* biedt daarvoor de infrastructuur en de ontwikkelingen rond *big data* bieden de analysemogelijkheden (convergentie van *internet of things* en *big data*).
  Het monitoren van trends en objecten met behulp van het *internet of things* (via het verzamelen van data van allerlei sensoren en 'dingen') is, zoals ook bij andere toepassingen - waaronder met name *big data, open data* - beschreven, een kans voor overheid en hulpdiensten om adequaat te reageren op een naderend of zich ontwikkelend incident. Dit heeft een positief effect op de weerbaarheid, de territoriale veiligheid (geen of minder grondgebied wat onbruikbaar is), fysieke veiligheid (minder doden en gewonden bij rellen of grootschalige ongevallen), ecologische veiligheid (minder schade aan flora en fauna) en de economische veiligheid (minder kosten voor het herstel).

Dreigingen

- Grootschalige uitval gekoppelde systemen: Een dreiging komt voort uit de extra kwetsbaarheid die ontstaat wanneer producten, maar ook volledige systemen (bijvoorbeeld vitale infrastructuren), informatietechnologie bevatten en aan elkaar gekoppeld en met elkaar verweven worden. Zij kunnen op onvoorziene wijzen met elkaar interacteren of het doelwit worden van kwaadwillenden waardoor het geheel van gekoppelde systemen niet goed functioneert. Systeemfalen of moedwillige verstoring kunnen leiden tot een zogenaamd cascade uitval. Bij cascade uitval worden - via het *internet of things* - gekoppelde systemen beïnvloed door het uitvallen van één systeem en ontstaat er een 'domino-effect'. Doordat de ontwikkeling van het *internet of things* ogenschijnlijk in autonomie verloopt, lijkt toezicht en grip op het geheel lastig. Daardoor is moeilijk te voorspellen of en wanneer er zaken uit de hand kunnen lopen. Dit geldt tot op zekere hoogte ook voor bijvoorbeeld big data, maar de complexiteit van het *internet of things* voegt hier een dimensie aan toe. Waar systemen voor energie, telecommunicatie, zorg en mobiliteit en logistiek in toenemende mate van elkaar afhankelijk en onderling verweven worden, nemen de kansen op, en de gevolgen van, cascade uitval toe. Dit kan effecten hebben op de territoriale veiligheid (bijvoorbeeld: grondgebied dat onbruikbaar raakt door sluizen die onterecht open gaan), fysieke veiligheid (bijvoorbeeld: doden of gewonden door uitval of verstoring van ziekenhuissystemen), ecologische veiligheid (bijvoorbeeld: schade door incident met chemische fabriek), economische veiligheid (kosten voor het herstel) en de sociale en politieke stabiliteit (afbreuk in het vertrouwen in het optreden van de overheid en hulpdiensten).
- Manipulatie en misbruik van data: Een dreiging is misbruik van data uit het *internet of things* door kwaadwillenden ten behoeve van geldelijk gewin of nationale en politieke belangen. Internet is transnationaal en allerlei buitenlandse statelijke en niet-statelijke actoren kunnen ongewenst data misbruiken of manipuleren. Dit zou ook kunnen worden gedaan met als doel (een deel van) de maatschappij te ontwrichten.

Conclusies

- *Kansen:*
  - Inzet ter identificatie van en voorkoming van incidenten.
- *Dreigingen:*
  - Grootschalige uitval gekoppelde systemen;
  - Manipulatie en misbruik van data.

8 Analyse van toepassingen en dreigingen voor mogelijk scenario NRB

8.1 Introductie

Dit hoofdstuk richt zich op de aanvullende onderzoeksvraag IV (zie paragraaf 2.1): 'Welke geïdentificeerde dreigingen komen het meest in aanmerking voor uitwerking als scenario in de NRB?'.

In de Nationale Risicobeoordeling (NRB) worden - aan de hand van scenario's - rampen, dreigingen en crises geanalyseerd die in potentie een dreiging kunnen vormen voor de nationale veiligheid. Een van de doelen van deze verkenning is vast te stellen welke toepassingen - gegeven die mogelijke dreiging - in aanmerking zouden kunnen komen om uit te werken in een of meer scenario's voor de NRB. Hoewel toepassingen van technologische ontwikkelingen ook kansen bieden, richten we ons hier dus uitsluitend op de dreigingen.

Voordat we in dit hoofdstuk ingaan op de selectie van toepassingen en dreigingen voor een mogelijk scenario binnen de NRB, volgt in de volgende paragraaf eerst een reflectie op de technologieën. Daarin wordt gekeken naar de samenkomst en mogelijke clustering van technologieën.

8.2 Reflectie op technologieën

Zoals beschreven in hoofdstuk 1 van dit rapport zijn in deze inventariserende studie technologische ontwikkelingen beschouwd volgens de indeling van de voorgaande NCTV-technologiestudie [1], namelijk: nanotechnologie, bio- / gentechnologie, neurotechnologie, materiaaltechnologie en informatietechnologie. Een dergelijke focus zorgt er enerzijds voor dat deze studie behapbaar blijft, anderzijds kunnen andere ontwikkelingen die moeilijker in dit kader te plaatsen zijn - maar die wel een significante impact op de nationale veiligheid kunnen hebben - hierdoor ongeïdentificeerd blijven.

Deze paragraaf besteedt daarom in aanvulling op de hoofdstukken 3 tot en met 7 kort aandacht aan convergerende technologieën en aan energietechnologie.

Convergerende technologieën

De term 'convergerende technologieën' (*converging technologies*) duidt op het bij elkaar komen van verschillende technologische ontwikkelingen. Deze samenkomst kan synergievoordelen opleveren, waardoor de ontwikkeling van technologische deelgebieden een bijzondere impuls krijgt. Veel van de hieruit resulterende toepassingen zijn al eerder bij de afzonderlijke technologieën in de hoofdstukken 3 tot en met 7 behandeld. Zo hangt bijvoorbeeld de ontwikkeling van sensoren nauw samen met ontwikkelingen op het gebied van nanotechnologie en informatietechnologie. Andere voorbeelden van bij elkaar komende technologische ontwikkelingen zijn: *internet of things* in combinatie met *big data, open data* en DNA methodieken in combinatie met *big data*.

De meeste aandacht rondom convergerende technologieën gaat momenteel uit naar de zogenaamde NBIC-convergentie. De term NBIC verwijst naar het samenkomen van vier sleuteltechnologieën: nanotechnologie, biotechnologie, informatietechnologie en cognitieve technologie [13]. Deze convergentie zal naar verwachting bijdragen aan tal van nieuwe innovaties met toepassingen met ingrijpende impact in de maatschappij. Voorbeelden hiervan zijn synthetische biologie, brein-machine interactie (zie paragraaf 5.1), moleculaire geneeskunde, *ambient intelligence*[29], persuasieve technologieën[30] en robotica [12].

Tevens kan een additioneel domein rond mechatronica[31], fotonica[32] en elektronica worden onderscheiden, waarin nano-, materiaal- en informatietechnologie bij elkaar komen. Deze drie technologische disciplines staan aan de basis van verschillende apparaten voor uiteenlopende toepassingsgebieden, van *automotive*- en productiesystemen, tot medische apparatuur, verlichting en militaire toepassingen. De uiteenlopende toepassingen in componenten, tools en technieken worden in een groot aantal sectoren toegepast en zijn belangrijke *enablers* en een stuwende kracht voor innovatie. Voorbeelden van thema's waar het onderzoek zich momenteel op richt zijn: *More than Moore*[33], actuatoren, medische technologie, sensoren, *nano manufacturing* en vermogenselektronica.

Zoals gezegd, zijn al veel convergerende technologieën behandeld in de hoofdstukken 3 tot en met 7. Daaruit blijkt dat juist ook de combinatie van technologieën tot een kans of dreiging voor de nationale veiligheid kan leiden.

Energietechnologie

Naast de clustering in technologieën vanuit de eerdere NCTV-technologiestudie [1], kunnen technologische ontwikkelingen ook vanuit een ander perspectief worden beschouwd. Een voor deze studie relevant voorbeeld daarvan zijn de technologische ontwikkelingen op het gebied van energie. Ontwikkelingen op dit gebied zijn voor een deel aan de orde gekomen bij de verschillende technologieën (toepassingen: biobrandstoffen, energieopslag en slimme energie infrastructuur (*Smart Grids*)), maar niet in de breedte en in samenhang.

De afhankelijkheid van fossiele brandstoffen en de relatieve schaarste hieraan leidt tot een sterke afhankelijkheid van politiek instabiele landen of landen die hun machtspositie soms uitbuiten. Bij toenemend schaarste zou het tot internationale spanningen kunnen leiden. In enkele scenario's van de Nationale Risicobeoordeling is aangegeven hoe groot de gevolgen kunnen zijn van energie-uitval.

De energiewereld is in beweging. Het schaarser worden van fossiele brandstoffen en de milieuproblemen die verbonden zijn aan het gebruik ervan, hebben (mede) gezorgd voor de ontwikkeling van alternatieve technologieën. De behoefte is met een energietransitie over te gaan van fossiele energiebronnen naar duurzame energiebronnen, zoals zonne-energie, windenergie, biomassa en waterkrachtenergie. Naast deze alternatieve technologieën wordt ook gekeken naar een herwaardering van bestaande technologieën zoals een verdere winning van fossiele brandstoffen (o.a. schaliegaswinning) en nucleaire energie waarbij nauwelijks CO_2 geproduceerd wordt.

[29] Het concept ambient intelligence houdt in dat het door miniaturisering van ICT mogelijk wordt een intelligente omgeving rond de mens te creëren. Deze overal aanwezige, onzichtbare, intelligentie biedt de gebruiker allerlei functionaliteit afgestemd op de wensen en behoeften.

[30] Persuasieve technologie wordt breed gedefinieerd als technologie die is ontworpen om de houding of het gedrag van de gebruikers door middel van overreding en sociale invloed te veranderen, maar niet door middel van dwang [19].

[31] Samenvoeging van de vakgebieden elektronica, werktuigbouwkunde en meet- en regeltechniek.

[32] Onderzoeken van de eigenschappen van licht.

[33] Ontwikkeling gericht op het opnemen van niet-digitale functionaliteiten (zoals draadloze communicatie, vermogensregeling, passieve componenten, sensoren en actuatoren) in een chip (behuizing of op de chip zelf). Daarmee het realiseren van functionaliteiten in chips die niet schalen volgens de Wet van Moore (die zegt dat het aantal transistoren in een chip elke twee jaar verdubbelt), maar extra waarde bieden.

Op dit moment is de enige rendabele vorm van nucleaire energie gebaseerd op kernsplijting. Deze techniek is omstreden vanwege het radioactieve afval dat het proces voortbrengt en vanwege het *meltdown* gevaar dat reactoren kan vernietigen, enorme milieuschade kan aanrichten en veel mensenlevens kan kosten. Incidenten zoals de recente *meltdown* van de Fukushima reactoren in Japan hebben daarbij een sterke invloed op het maatschappelijk sentiment rondom kernenergie. Kernenergie kan ook opgewekt worden door middel van kernfusie. Het grote voordeel van kernfusie is dat het proces (vrijwel) geen radioactieve afval voortbrengt en dat de energievoorraad zeer groot zou zijn. Kernfusie is in ontwikkeling, maar het is onduidelijk of het proces ooit de hooggespannen verwachtingen waar kan maken. De ITER reactor, die momenteel gebouwd wordt in Frankrijk (Cadarache), moet de eerste reactor zijn die meer energie oplevert dan er ingestopt wordt en naar verwachting zal deze reactor in 2018 in gebruik genomen worden. Naast onderzoek naar kernfusie zijn er ook studies naar thoriumreactoren. Daarbij vindt kernsplijting niet met uranium maar met thorium als brandstof plaats. Vooral Azië investeert hier veel in [25]. Thoriumreactoren zouden vele malen veiliger zijn en veel minder afvalstoffen afgeven, die minder lang radioactief blijven dan reactoren met uranium als brandstof. Bovendien komt thorium op aarde ongeveer driemaal zo veel voor als uranium.

Voor wat betreft duurzame energie opwekking zijn de ontwikkelingen meer incrementeel en soms wellicht interfererend. Wanneer we er echter in slagen om met kleine opwekkers in de persoonlijke energievraag te voorzien, dan zullen de maatschappelijke voordelen groot zijn. In dit geval kan ook gedacht worden technologiemix, waarin zon-, wind-, bio- en waterstoftechnologie samen in de brede energievraag voorzien.

Technologische ontwikkelingen op het gebied van energie bieden kansen in ecologische en geopolitieke zin. De technologische ontwikkelingen verhogen de duurzaamheid (en genereren daarmee milieuwinst) en zorgen mogelijk voor minder afhankelijkheid tussen landen. Hierdoor ontstaan op termijn economische verschuivingen en een verandering van politieke afhankelijkheid van andere landen. Decentralisatie van energieopslag biedt mogelijkheden de duurzaamheid te verhogen en de afhankelijkheid tussen landen te verminderen. Met behulp van nieuwe vormen van energieopslag zou energie-uitval kunnen worden voorkomen.

8.3 Selectie van toepassingen voor mogelijk scenario NRB

In de vorige paragraaf is het begrip ‘convergerende technologieën’ aan bod gekomen. Juist dit bij elkaar komen van verschillende technologische ontwikkelingen is interessant als uitgangspunt voor een scenario in de NRB. De grootste dreiging met potentiele impact op nationale schaal lijkt immers te worden gevormd door de toenemende verwevenheid (‘hyperconnectiviteit’), complexiteit en onderlinge afhankelijkheid van vitale processen en systemen waarin meerdere technologische toepassingen worden gebruikt. Allerlei vitale (en niet-vitale) processen, systemen en diensten raken steeds meer met elkaar verweven en verknoopt, en zijn daardoor afhankelijk van elkaar. Een kleine verstoring in één systeem kan hierdoor de kans krijgen extreem door te werken in andere systemen, systemen en diensten, waarin ook nog eens meerdere toepassingen van convergerende technologie worden gebruikt. Een verstoring of fout in een systeem kan grote gevolgen hebben, omdat de systemen niet zomaar te ontkoppelen zijn. De productie in een chemische fabriek kan zomaar verknoopt zijn met de logistieke aan- en afvoer, die weer verweven is met de verkeerstromen op de weg en de aansturing van bijvoorbeeld bruggen. Een fout signaal van een brug zou dan instabiliteit in het chemische proces kunnen veroorzaken. Een ander risico is dat het - mede door de globalisering en de explosieve groei van het internet - moeilijk is toezicht en grip te houden op (een aantal) technologische ontwikkelingen. Dergelijke ontwikkelingen lijken als het ware autonoom te verlopen.

Deze twee risico’s (‘hyperconnectiviteit’ en moeilijke controleerbaarheid) kunnen als Leitmotiv in een mogelijk scenario voor de NRB worden gebruikt, omdat ze gepaard gaan met veel onzekerheden. Het is niet exact te beoordelen of en wanneer er zaken op grote schaal uit de hand kunnen lopen, en ontwikkelingen rond deze risico’s spelen zich veelal af buiten het gezichtsveld en de controle van overheden.

Omdat juist in de connectiviteit en convergentie van technologieën een potentieel risico wordt gezien (vanwege de onvoorspelbaarheid van bepaalde ontwikkelingen en effecten), is het aan te bevelen een aantal van de toepassingen, bijvoorbeeld NEMS/MEMS, sensoren, *internet of things, big data, open data*, in één scenario te combineren.

Deze toepassingen (zullen) worden gebruikt in verschillende sectoren van de maatschappij. In de toekomst worden door overheid en bedrijfsleven steeds meer sensoren gebruikt om allerlei systemen te monitoren en waar nodig bij te sturen. Systemen zijn bijvoorbeeld

mensenmassa's (geobserveerd door camera's en *drones*), verkeerssystemen (met camera's en lussen in het wegdek), vitale infrastructuur (door sensoren in dijken en bruggen), het milieu (door sensoren in de omgeving), stemming van mensen (via sociale media), energienetwerken, financiële systemen, etc. Zulke systemen worden steeds vaker gekoppeld aan allerlei databronnen en gegevensbestanden. In deze toenemende koppeling (interconnectiviteit) en de convergentie van verschillende technologieën zit het gevaar dat een hierop gebaseerd systeem verstoord raakt of verstoord wordt.

8.4 Selectie van dreigingen voor mogelijk scenario NRB

Een technologische toepassing vormt op zichzelf geen dreiging. Zoals uiteengezet in paragraaf 1.4 ontstaat die pas door falen, uitval of verstoring, hetzij moedwillig, hetzij onopzettelijk. Of als gevolg van misbruik dan wel oneigenlijk gebruik door 'kwajongens', kwaadwillenden, criminelen en andere actoren die daarmee macht willen uitoefenen, hun positie willen versterken of uit zijn op gewin. Echter, zulke dreigingen worden pas relevant voor de nationale veiligheid als de betreffende toepassing (of combinaties daarvan) een cruciale rol speelt in het functioneren van vitale processen. En als die verstoring of dat misbruik een grote verstoring geeft.

Om te bepalen welke geïdentificeerde dreigingen het meest in aanmerking komen voor uitwerking als scenario zijn de geselecteerde toepassingen beoordeeld op de criteria die het Analistennetwerk Nationale Veiligheid gebruikt voor het agenderen van nieuwe thema's en onderwerpen in de NRB.

Verschillende categorieën van dreigingen

Naast de twee eerder genoemde risico's ('hyperconnectiviteit' en moeilijke controleerbaarheid) blijkt uit een analyse van de dreigingen van geselecteerde toepassingen[34] in de vierde paragrafen van de hoofdstukken 3 tot en met 7, dat ruwweg drie typen generieke categorieën van dreigingen als een rode draad door de beschrijvingen heen lopen[35].

Dat zijn:

- Manipulatie of (moedwillige) verstoring. Het betreft hier de toepassingen: NEMS/MEMS, sensoren, *big data, open data, internet of things.* Hierbij gaat het om systemen of processen, die zijn gebaseerd op een of meer van deze toepassingen, welke door kwaadwillenden worden gemanipuleerd of moedwillig worden verstoord. Als dat op grote schaal plaatsvindt, kan het leiden tot maatschappelijke ontwrichting. De toenemende verwevenheid en de oncontroleerbaarheid van technologische ontwikkelingen maakt dat de impact van falen, uitval of verstoring veel groter is dan vroeger. Technisch falen, menselijke fouten, 'kwajongensstreken' en manipulatie en moedwillige verstoringen werken veel sterker door.
- Misbruik van technologische toepassingen. Het betreft hier de toepassingen: NEMS/MEMS, nanomaterialen, DNA methodieken, 3D *printing*, robotica voor veiligheid, *big data, open data*. Hierbij wordt een technologische toepassing door kwaadwillenden gebruikt om ontwrichting te bewerkstelligen, bijvoorbeeld vanuit een politiek of idealistisch doel, of voor eigen gewin. Met name de oncontroleerbaarheid van technologische ontwikkelingen speelt hierbij een rol. Kwaadwillenden zouden bijvoorbeeld 3D *printing* kunnen gebruiken voor het fabriceren van wapens.
- Verlies van vertrouwen. Het betreft hier de toepassingen: robotica voor veiligheid, *internet of things.* Hierbij voelen mensen zich bedreigd of ondervinden zij grote hinder, doordat technologische toepassingen op grote schaal (al dan niet opzettelijk) verstoord of in opspraak raken. Zo kan bijvoorbeeld onrust ontstaan wanneer op grote schaal het elektronische betalingsverkeer uitvalt, men niet kan zien hoeveel geld er nog op de bank staat of in bestanden de identiteit van verschillende personen wordt verwisseld. Door de toenemende verwevenheid kan de impact van een kleine rimpeling grote gevolgen hebben.

Hoewel verlies van vertrouwen een afgeleide dreiging is (bijvoorbeeld ten gevolge van de kwetsbaarheid van technologische systemen), wordt deze hier expliciet als categorie van dreiging meegenomen omdat dit onderdeel van een scenario in de NRB kan worden gemaakt.

Selectie van dreigingen

Voor de selectie van de dreigingen voor een mogelijk scenario in de NRB zijn de criteria toegepast die het ANV (Analistennetwerk Nationale Veiligheid) gebruikt voor het agenderen van nieuwe thema's en onderwerpen:

- *Dekkingsgraad:* Draagt het onderwerp bij aan de breedte van de NRB en/of vult het een kennisleemte in?[36]

[34] De toepassing 'energieopslag' is hier verder niet meegenomen, aangezien de dreigingen beperkt zijn ingeschat (zie hoofdstuk 5).

[35] Daarnaast zou ook de categorie 'kwetsbaarheid in combinatie met afhankelijkheid' kunnen worden beschouwd. Deze categorie wordt hier niet verder meegenomen omdat dit in principe is op te lossen door maatregelen te nemen zoals dubbele uitvoering van een technologie (back-up systemen) of adequate beveiliging (zie ook paragraaf 1.4).

[36] Daarbij wordt ook beoordeeld of, naar verwachting, een nieuw onderwerp tot ontdekking van nieuw te versterken capaciteiten zou kunnen leiden (t.o.v. analyses van eerdere jaren).

- *Waarschijnlijkheid:* Hoe groot is de kans dat dit onderwerp gaat spelen op een termijn van 5 jaar of korter?
- *Impact:* Worden de effecten hoog of beperkt geschat, als dit scenario werkelijkheid wordt?
- *Tijdigheid:* Komt uitwerking in de NRB nog op tijd om er wat aan te doen? Welke urgentie is er?
- *Trends:* Speelt het onderwerp meer of minder in op huidige trendmatige ontwikkelingen?

Hieronder worden voor de in de vorige paragraaf genoemde categorieën van dreigingen de ANV criteria beschouwd.

Manipulatie of (moedwillige) verstoring:

- *Dekkingsgraad:* Het uitwerken van een scenario waarin dit type dreiging in combinatie met de twee aan technologieën verbonden risico's (toenemende verwevenheid en moeilijke controleerbaarheid) centraal staat, verhoogt de dekkingsgraad van de NRB. Er zijn wel eerder ICT gerelateerde scenario's uitgewerkt, zoals verstoring van communicatie in het scenario 'Satellietuitval' (NRB 2011), maar er is nog geen scenario uitgewerkt waar de analoge en digitale ogen en oren van overheid en bedrijfsleven niet meer gebruikt kunnen worden. De overheid maakt nu al gebruik van camera's in het centrum van grote steden, *drones*[37], camera's aan de grens en nummerplaatherkenning. De overheid - maar ook het bedrijfsleven - zal steeds vaker bouwen op verschillende sensoren die in de samenleving aanwezig zijn. Het is nu onzeker wat er gebeurt als die gegevens niet meer bereikbaar of betrouwbaar zijn voor de overheid en het bedrijfsleven.
- *Waarschijnlijkheid:* De kans wordt groot geacht dat falen, uitval of verstoring van processen en systemen met de in deze studie beschreven toepassingen - en vooral combinaties daarvan - tot ontwrichtende effecten kan leiden. De oorzaak van het falen, de uitval of verstoring is daarbij minder relevant. Dit kan manipulatie of moedwillig zijn, maar het kan ook gaan om een technische of menselijke fout of een 'kwajongensstreek'.
- *Impact:* Als 'manipulatie of (moedwillige) verstoring' van zulke processen en systemen op grote schaal plaatsvindt, kan de impact op verschillende vitale belangen groot zijn.
- *Tijdigheid:* De technologische ontwikkelingen gaan soms zeer snel, zoals de ontwikkelingen van analoge en digitale observatiemiddelen en het gebruik van de daarmee verkregen data. De ontwikkelingen voor verstoring van de observatiemiddelen (sensoren, etc.) of de dragers van de gegevens (*internet of things*, databestanden) gaan net zo snel mee. De urgentie om te werken aan de bewustwording en de mogelijkheden nog beter te beveiligen is groot.
- *Trends:* Deze categorie van dreigingen is gerelateerd aan toepassingen die inspelen op de trend om zoveel mogelijk processen te automatiseren, de kritische blik van een (beperkte) groep mensen op de overheid als Big Brother, maar ook de noodzaak voor de overheid om de veiligheid te garanderen. Wanneer we kijken naar de ontwikkelingen gerelateerd aan informatietechnologie is manipulatie of moedwillige verstoring te koppelen aan de trend van het hacken van allerlei diensten en systemen.

Misbruik van technologische toepassingen:

- *Dekkingsgraad:* Deze dreiging komt voor in het scenario 'Cyberspionage in combinatie met verlies van vertrouwen in informatie- en communicatietechnologie (ICT)' uit de NRB 2011.
- *Waarschijnlijkheid:* Voor sommige toepassingen vormt de complexiteit van de technologie een drempel. Andere toepassingen zijn relatief eenvoudig bereikbaar, maar de waarschijnlijkheid van misbruik door kwaadwillenden (met gevolgen op grote schaal) is voor een deel van de nieuwe toepassingen nog onbekend.
- *Impact:* Misbruik door derden kan potentieel grote impact hebben. Bijvoorbeeld wanneer *drones* worden ingezet als middel om explosieven of gif op een bepaalde plaats te brengen.
- *Tijdigheid:* Net als voor de categorie 'manipulatie of verstoring' is de urgentie ook hier groot, omdat de technologische ontwikkelingen erg snel gaan.
- *Trends:* Voor technologieën geldt altijd dat deze op verschillende manieren kunnen worden gebruikt (zie ook paragraaf 10.2). Misbruik van technologische toepassingen lijkt daarmee niet verbonden met een specifieke huidige trendmatige ontwikkeling. Een mogelijke trend is wel dat het voor overheden in toenemende mate lastig is om door middel van handhaving misbruik van bepaalde technologieën te voorkomen[38]. De ogenschijnlijk autonome wijze waarop technologische ontwikkelingen plaatvinden (wetgeving loopt vaak ver achter bij implementatie), speelt hierbij ook een rol.

[37] Artikel uit de Volkskrant, 'Wie ligt er nog wakker van de alwetende overheid?' - Volgens de Staatscourant hebben sinds 2009 132 vluchten plaatsgevonden - 20 maart 2013.

[38] Zoals bijvoorbeeld bij snelheidshandhaving met radarflitsers, met daarop de reactie van radarverklikkers, met daarop weer de reactie van het verbieden van radarverklikkers en de introductie van radarverklikker-verklikkers, met daarop weer de reactie van *crowd sourcing* voor het melden van flitsers op de radio en je navigatiesysteem. Met als vervolg weer dat sommige landen die meldingen weer verbieden, etc.

Tabel 7: De beoordeling van de drie categorieën van dreigingen op basis van de criteria van het ANV.

	Manipulatie of moedwillige verstoring	Misbruik van technologische toepassingen	Verlies van vertrouwen
Dekkingsgraad	Wordt verhoogd	Komt voor Cyber voor in bestaande scenario's	Komt voor ICT voor in bestaande scenario's
Waarschijnlijkheid	Wordt groot geacht	Onduidelijk	Naar verwachting laag
Impact	Divers en mogelijk groot	Potentieel groot	Onduidelijk, beperkt tot sociale en politieke stabiliteit
Tijdigheid	Urgent, ontwikkelingen gaan snel	Urgent, ontwikkelingen gaan snel	Heeft al veel aandacht
Trends	Processen automatiseren en *hacken* van diensten en systemen	*Mogelijk:* Handhaving misbruik technologieën lastiger	Verzet tegen technologieën als onduidelijkheden blijven bestaan of er geen vertrouwen is

Scoort hoog
Scoort gemiddeld
Scoort laag

Verlies van vertrouwen:

- *Dekkingsgraad:* Verlies van vertrouwen in informatie- en communicatietechnologie (ICT) komt voor in het scenario 'Cyberspionage' uit de NRB 2011.
- *Waarschijnlijkheid:* In het algemeen is verlies van vertrouwen een sluipend proces. Wanneer adequaat wordt gereageerd op crises en incidenten, is de waarschijnlijkheid naar verwachting laag.
- *Impact:* Verlies van vertrouwen, niet alleen in de overheid en mogelijk het bedrijfsleven, maar ook in de toepassingen van de onderliggende technologie, kan effect hebben op de sociale en politieke stabiliteit. De mate van impact is op voorhand lastig in te schatten.
- *Tijdigheid:* Het besef dat het belangrijk is om burgers goed op de hoogte te stellen van (technologische) ontwikkelingen is binnen de overheid goed doorgedrongen. In reactie op diverse scenario's is reeds nagedacht over hoe dit effectief te doen.
- *Trends:* Een trend van de huidige tijd is dat burgers zich tegen technologieën kunnen verzetten en deze technologie zelfs collectief in de ban kunnen doen als er onduidelijkheden blijven bestaan of geen vertrouwen is en de overheid of betrokken bedrijven niet adequaat reageren.

Tabel 7 vat de beschouwing van de categorieën van dreigingen en de criteria van het ANV samen.

Op basis van deze kwalitatieve scores concluderen we dat de categorie '*manipulatie of moedwillige verstoring*' het meest in aanmerking komt om uitgewerkt te worden als scenario in de NRB.

8.5 Elementen voor het scenario

Concluderend stellen we dat de dreigingscategorie 'manipulatie of (moedwillige) verstoring' van een systeem of data het meest in aanmerking komt voor uitwerking tot een scenario in de NRB. Het gaat dan om een scenario waarin 'kwaadwillenden' (dat kunnen bijvoorbeeld hackers zijn die een statement willen maken, zich willen profileren of acties voeren 'voor de lol') processen en systemen verstoren, waarbij onbedoeld aanzienlijke effecten ontstaan zoals grootschalige uitval van vitale diensten. Of een scenario waarin verstoring en uitval het gevolg zijn van onbewust foutief handelen, waardoor een proces, systeem of data wordt verstoord en er onvoorziene keteneffecten optreden.
Die onbedoelde en onvoorziene effecten zijn een gevolg van de toenemende verwevenheid ('hyperconnectiviteit'), complexiteit en onderlinge afhankelijkheid van vitale processen en systemen waarin meerdere technologische toepassingen worden gebruikt. Te denken valt aan toepassingen als NEMS/MEMS, sensoren, *big data, open data* en *internet of things* bij elkaar.
Het is niet wenselijk om in één scenario een zeer groot aantal systemen mee te nemen. Er zal daarom een selectie moeten worden gemaakt. De selectie kan worden gemaakt door één specifieke sector of toepassingsgebied te beschouwen. Dat kan bijvoorbeeld de energiesector zijn of het gebruik van diverse sensoren voor monitoring door bedrijven of overheid betreffen.

Bij het uitwerken van het scenario is het belangrijk om nieuwe technologieën en toepassingen daarvan te beschouwen. Het gaat dus niet om huidige systemen en toepassingen, maar juist om toepassingen van nieuwe technologieën (of combinaties daarvan) zoals in deze studie zijn behandeld, zodat in het scenario qua technologie vooruit wordt gekeken.

9 Samenvattende conclusies

9.1 Verkennende studie

Deze verkennende studie verschaft op hoofdlijnen inzicht in technologische ontwikkelingen en de aan hun toepassing verbonden kansen en dreigingen voor de nationale veiligheid. De studie is uitgevoerd in opdracht van de NCTV/Directie Dreigingen en Risico's van het ministerie van Veiligheid en Justitie. De aanleiding voor de studie was onder andere het advies van de Taakgroep van het Analistennetwerk Nationale Veiligheid (ANV) om het thema 'nieuwe technologieën' binnen de Strategie Nationale Veiligheid verder uit te werken. De studie beoogt ook om in de behoefte van de NCTV aan een actualisatie en verbreding ten opzichte van de studie naar technologische ontwikkelingen uit 2011 [1] te voorzien.

De resultaten van deze studie kunnen worden gebruikt bij het formuleren van beleid rond technologische ontwikkelingen die kansrijk zijn voor verbeteringen in de nationale veiligheid of waarvan juist een dreiging uitgaat voor de nationale veiligheid. De resultaten bieden ook aanknopingspunten voor het ontwikkelen van een of meer scenario's voor de Nationale Risicobeoordeling (NRB).

In deze verkenning zijn technologische ontwikkelingen beschouwd volgens de indeling van de voorgaande NCTV-technologiestudie [1]:

- Nanotechnologie;
- Bio- / gentechnologie;
- Neurotechnologie;
- Materiaaltechnologie;
- Informatietechnologie.

9.2 Geselecteerde toepassingen

In dit rapport zijn de geïnventariseerde technologische ontwikkelingen en toepassingen die mogelijk relevant zijn voor de nationale veiligheid - en daar een mogelijke (positieve of negatieve) impact op hebben - toegelicht. De in tabel 8 weergegeven toepassingen zijn door experts geselecteerd voor een verdere uitwerking van de kansen en dreigingen voor de nationale veiligheid. De selectie is gebaseerd op de verwachte (relatief hoge) impact van deze toepassingen.

Tabel 8: Voor verdere uitwerking geïdentificeerde toepassingen.

Technologie	Toepassingen
Nanotechnologie	NEMS/MEMS Nanomaterialen
Bio- / gentechnologie	DNA methodieken
Neurotechnologie	--
Materiaaltechnologie	Sensoren Energieopslag
Informatietechnologie	3D *printing* Robotica voor veiligheid *Big data, open data* *Internet of things*

9.3 Algemene kansen en dreigingen

Uit de sessies met experts zijn de volgende punten naar voren gekomen die in het algemeen gelden waar het gaat om de kansen en dreigingen van toepassingen van technologische ontwikkelingen:

- Kwetsbaarheid voor falen of het verstoord raken van een toepassing is vooral van belang wanneer de maatschappij er afhankelijk van is (vitale sectoren, diensten en producten). Veelal zijn dan maatregelen wenselijk om die de kwetsbaarheid te verminderen, bijvoorbeeld door dubbele uitvoering van een technologie of adequate beveiliging
- Een toepassing van een technologische ontwikkeling kan ten goede of ten kwade worden ingezet.
- Nieuwe technologische ontwikkelingen kennen zowel voor- als tegenstanders. Het mogelijk controversiële karakter van een nieuwe technologie en het risico op misbruik kunnen leiden tot (forse) maatschappelijke weerstand en in uitzonderlijke gevallen zelfs tot extremistische of terroristische activiteiten, gericht tegen de betreffende technologie.
- Het is denkbaar dat niet iedereen op gelijke wijze toegang heeft of kan krijgen tot technologische toepassingen, bijvoorbeeld door gebrek aan financiën of kennis. In theorie zou dat kunnen leiden tot sociale uitsluiting van bepaalde groepen.

9.4 Kansen en dreigingen per toepassing

Hieronder worden de kansen en dreigingen van de geselecteerde toepassingen per technologie samengevat.

Nanotechnologie

Nano- en micro-elektromechanische systemen (NEMS/MEMS)

Miniaturisering heeft ertoe geleid dat sensoren en actuatoren steeds kleiner en soms goedkoper kunnen worden geproduceerd. Dit biedt nieuwe mogelijkheden voor het toepassen van NEMS en MEMS (respectievelijk nano- en micro-elektromechanische systemen).

- Kansen:
  - Inzet NEMS ter voorkoming grootschalige industriële incidenten;
  - Inzet MEMS voor communicatie, monitoring en observatie door 'veiligheidsdiensten'.
- Dreigingen:
  - Inzet NEMS en MEMS voor communicatie, monitoring en observatie door 'kwaadwillenden'.

Nanomaterialen

Materialen krijgen op nanoschaal andere eigenschappen. Met de kennis die nu wordt ontwikkeld kunnen aan materialen steeds meer gecontroleerd bepaalde eigenschappen worden meegegeven. De bij deze toepassing geïdentificeerde producten die mogelijk invloed hebben op de nationale veiligheid, zijn nanodeeltjes in wapens (zoals een vuile bom) en nanomaterialen ingezet voor identiteitsmanipulatie.

- Kansen:
  - Verbetering hulpmiddelen veiligheidsdiensten door middel van nanomaterialen.
- Dreigingen:
  - *Dirty bomb* door toevoeging nanomaterialen;
  - Vergiftiging door (toevoeging van) nanomaterialen;
  - Identiteitsmanipulatie met behulp van nanomaterialen.

Bio- / gentechnologie

DNA methodieken

Technologische ontwikkelingen hebben het mogelijk gemaakt om met minder en andersoortig materiaal, steeds sneller en goedkoper, een completer DNA profiel te vergaren. Efficiëntere DNA methodieken bieden mogelijkheden voor identificatie van personen.

- *Kansen:*
  - Identificatie van personen met behulp van DNA profiel;
  - Opsporing van virussen op basis van DNA.

- *Dreigingen:*
  - Misbruik van DNA data.

Materiaaltechnologie

Sensoren

Ontwikkelingen op de gebieden van materiaal-, bio- en nanotechnologie zorgen ervoor dat meer typen en kleinere sensoren beschikbaar komen - die meer verschillende dingen, beter kunnen meten - en dat sensoren goedkoper worden. Geïdentificeerde nieuwe producten en diensten hebben met name betrekking op het koppelen van verschillende sensordatastromen. In het geval van '*crowdsourcing*' van sensoren worden verschillende sensoren die in het bezit zijn van individuen of organisaties, samen voor een specifiek doel ingezet.

- Kansen:
  - Vroegtijdig en gerichter ingrijpen bij incidenten door middel van sensoren;
  - Voorspellend vermogen ten aanzien van mogelijk optredende risico's.
- Dreigingen:
  - Onjuiste of gemanipuleerde data.

Energieopslag

De uitputting van fossiele brandstoffen en milieuproblemen zijn de drijvende krachten achter transformaties in de energieketen. Een voorwaarde om stappen te maken naar gebruik van meer natuurlijke energiebronnen is de ontwikkeling van nieuwe manieren van energieopslag.

- *Kansen:*
  - Verminderen afhankelijkheid en kans op energie-uitval.

Informatietechnologie

3D printing

3D *printing* maakt het mogelijk driedimensionale producten, waaronder gebruiksvoorwerpen, te produceren. Daarvoor zijn alleen een 3D printer, basismaterialen en data met de 'bouwtekening' benodigd.

- *Kansen:*
  - Printen van producten ten behoeve van veiligheidsdiensten.
- *Dreigingen:*
  - Ondermijning gereguleerde producten (o.a. wapens).

Robotica voor veiligheid

Technologische ontwikkelingen - onder meer op het gebied van informatietechnologie - leveren de bouwstenen voor verdere ontwikkeling van intelligente en slimme robots. Deze robots kunnen worden ingezet ten behoeve van de veiligheid. Bijvoorbeeld voor het verrichten van inspecties in voor de mens gevaarlijke omgevingen of voor het uitvoeren van surveillances.

- *Kansen:*
  - Inzet robots en *drones* voor veiligheidstaken.
- *Dreigingen:*
  - Inzet robots en *drones* door kwaadwillenden;
  - Hacken van robots voor veiligheid.

Big data, open data

De hoeveelheid data die dagelijks gecreëerd wordt, groeit exponentieel. Data wordt in toenemende mate open aangeboden. Met veel verwerkingscapaciteit en/of slimme methodieken is er de mogelijkheid informatie te extraheren uit de zeer grote hoeveelheden ongestructureerde data.

- *Kansen:*
  - Gebruik voor preventie, proactie en respons van incidenten en crises.
- *Dreigingen:*
  - Vervuiling van databestanden;
  - Manipulatie en misbruik van data en/of methodieken door kwaadwillenden.

Internet of things

Technologische ontwikkelingen op het gebied van informatietechnologie leiden er toe dat ook steeds meer 'dingen' - zoals apparaten, infrastructuur en voertuigen - via internet worden verbonden en gegevens met elkaar kunnen uitwisselen.

- *Kansen:*
  - Inzet ter identificatie van en voorkoming van incidenten.
- *Dreigingen:*
  - Grootschalige uitval gekoppelde systemen;
  - Manipulatie en misbruik van data.

9.5 Selectie geïdentificeerde dreigingen voor mogelijk scenario NRB

Eén van de grootste risico's is de toenemende verwevenheid ('hyperconnectiviteit') en onderlinge afhankelijkheid van vitale processen en systemen waarin meerdere technologische toepassingen worden gebruikt. Een ander risico is dat het moeilijk is toezicht en grip te houden op (een aantal) technologische ontwikkelingen. Dergelijke ontwikkelingen lijken autonoom te verlopen. Vanwege deze verschijnselen (toenemende verwevenheid en globalisering) is niet exact te beoordelen of en wanneer er zaken op grote schaal uit de hand kunnen lopen.

Omdat juist in de connectiviteit en convergentie van technologieën een potentieel risico wordt gezien (vanwege de onvoorspelbaarheid van bepaalde ontwikkelingen en effecten), is het aan te bevelen een aantal van de toepas-

singen NEMS/MEMS, sensoren, *internet of things, big data, open data* in één scenario te combineren.

Op basis van de gehanteerde criteria van het analistennetwerk Nationale Veiligheid is geconcludeerd dat een scenario op het gebied van '*manipulatie of (moedwillige) verstoring*' van verweven, complexe en onderlinge afhankelijke systemen en de data die zij genereren het meest in aanmerking komt om uitgewerkt te worden als scenario in de NRB. Het gaat dan om een scenario waarin 'kwaadwillenden' (dat kunnen bijvoorbeeld hackers zijn die een statement willen maken of zich willen profileren) processen en systemen verstoren, waarbij onbedoeld aanzienlijke effecten ontstaan zoals grootschalige uitval van vitale diensten. Of een scenario waarin verstoring en uitval het gevolg zijn van onbewust foutief handelen, waardoor een proces, systeem of data wordt verstoord en er onvoorziene keteneffecten optreden. Die onbedoelde en onvoorziene effecten zijn een gevolg van de toenemende verwevenheid ('hyperconnectiviteit'), complexiteit en onderlinge afhankelijkheid van vitale processen en systemen waarin meerdere technologische toepassingen worden gebruikt.

Om het scenario niet te breed te maken is het aan te bevelen een selectie te maken voor één specifieke sector of toepassingsgebied, bijvoorbeeld de energiesector of het gebruik van diverse sensoren voor monitoring door bedrijven of overheid.

Literatuurlijst

[1] Technologische ontwikkelingen: kansen en dreigingen tot 2015 voor contra-terrorisme en bewaken en beveiligen, NCTb, januari 2011.

[2] Adviesdocument: Taakgroep van het Analistennetwerk aan de IWNV en de Stuurgroep Nationale Veiligheid Onderwerpen NRB 2013 inzake de thema's en onderwerpen die in aanmerking komen voor de Nationale Risicobeoordeling 2013, 12 september 2012.

[3] Ethics and Nanotechnology; Responsible development of nanotechnology at global level in the 21st Century, Malsch, N.H., 2011.

[4] Commission recommendation on a code of conduct for responsible nanosciences and nanotechnologies research, EU, 7 februari 2008.

[5] http://www.agentschapnl.nl/onderwerp/biobased-economy, website bezocht januari 2013.

[6] Signaleringsbrief trends in ggo-onderzoek, COGEM, 1 oktober 2012.

[7] Leven maken, Rathenau Instituut, 2007.

[8] Making Perfect Life, Science and Technology Options Assessment, 2008.

[9] Goed, beter, betwist, publieksonderzoek naar mensverbetering, Rathenau Instituut, 2012.

[10] http://www.tno.nl/content.cfm?context=kennis&content=etp_content&laag1=8&item_id=8, website bezocht januari 2013.

[11] http://home.tudelft.nl/index.php?id=6991, website bezocht januari 2013.

[12] http://www.nrc.nl/tech/2012/12/15/verdrinken-in-big-data/, website bezocht januari 2013.

[13] http://www.rathenau.nl/themas/thema/project/convergerende-technologieen.html, website bezocht januari 2013.

[14] De Strategie Nationale Veiligheid; Ministerie van Veiligheid en Justitie, NCTV, 2012.

[15] Werken met scenario's, risicobeoordeling en capaciteiten in de Strategie Nationale Veiligheid, oktober 2009.

[16] Megatrends: a broad outlook on innovation, TNO, December 2012.

[17] Watters JW, McLeod HL.; Cancer pharmacogenomics: current and future applications; Biochim Biophys Acta. 2003 Mar 17;1603(2):99-111.

[18] Van Dale - Woordenboek hedendaags Nederlands.

[19] Wikipedia (Onderwerpen: MEMS, synthetische biologie, RNA en persuasieve technologie).

[20] http://www.nanonextnl.nl/themes.html.

[21] http://www.tno.nl/content.cfm?context=thema&content=prop_case&laag1=895&laag2=912&laag3=99&item_id=1234&Taal=2.

[22] http://www.research.philips.com/technologies/robotics.html.

[23] Aanbeveling van de Commissie van 18 oktober 2011 inzake de definitie van nanomateriaal; 2011/696/EU.

[24] Rapportage 'Integraal advies onderwerpen NRB 2012'; kenmerk 20110297 IMG/mme; RIVM; Bilthoven.

[25] http://eoswetenschap.eu/artikel/thorium-kernenergie-zonder-afval.

Bijlagen

A. Geïnterviewde experts voor de inventarisatie van technologische ontwikkelingen en toepassingen

B. Deelnemers van de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling'

C. Deelnemers van de workshop 'Technologieverkenning' met de Taakgroep Analistennetwerk Nationale Veiligheid

D. Megatrends

E. Impactcriteria

F. Capaciteitenlijst

G. Voorselectie van toepassingen

H. Selectie van toepassingen voor verdere uitwerking

I. Geïdentificeerde toepassingen

Bijlage A Geïnterviewde experts voor de inventarisatie van technologische ontwikkelingen en toepassingen

Onderwerp	Organisatie
Experts	
Nanotechnologie	
Jeroen Terwoert	TNO
Dick Koster	TNO / NanoNext
Albert van de Berg	TU Twente
Arie Rip	TU Twente
Adrienne Sips	RIVM
Agnes Oomen	RIVM
Marc de Vries	TU Delft
Monique Groenewold	RIVM
Neurotechnologie	
Ira van Keulen	Rathenau
Karin Roelofs	Radboud Universiteit Nijmegen
Leo Kenemans	NOW
Jan van Erp	TNO
Ed van Swieten	NOW
Guillen Fernandez	Radboud
Materiaaltechnologie	
Ardi Dortmans	TNO
Olaf Adan	TNO
Rene Peters	TNO
Ingrid Kroon	TNO
Jan Hopman	TNO
Synthetische biologie	
Dirk Stemerding	Rathenau
Peter Punt	TNO
Frank van der Wilk	Cogem
Cecile v.d. Vlugt	RIVM
Informatietechnologie	
Heico Sandee	TU Eindhoven
Marc van Lieshout	TNO
Arnout Appeloo	Appelo Advies
Stefano Stramigioli	TU Twente
Vanessa Evers	TU Twente
Gabriela Bodea	TNO
Chris van 't Hof	TekTok
Silvain de Munck	TNO
Bart van de Vorst	TNO

Johanneke Siljee	TNO
Convergentie en methodiek	
Jaap van der Vlies	TNO
Maurits Butter	TNO
Rinie van Est	Rathenau
Amber Ronteltap	LEI Wageningen
Anne Dijkstra	TU Twente
Erwin van Rijswoud	TU Twente
Frans Brom	Rathenau
Jan Gutteling	TU Twente

Bijlage B Deelnemers aan de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling'

26 november 2012
KiviNiria, Prinsessegracht 23, Den Haag.

Genodigden	Organisatie
Agnes Oomen	RIVM
Allard Kernkamp	TNO
Anne Dijkstra	Universiteit Twente
Anne-Fleur Hemmer	TNO
Ardi Dortmans	TNO
Bart van der Vorst	TNO
Betsy van Dijk	Universiteit Twente
Carin de Hoog	RIVM
Chris van 't Hof	TekTok
Christien Enzing	Technopolis
Diana de Kreij	schrijver
Diederik Wijnmalen	TNO
Django Mathijsen	schrijver
Ellen Willemse	Stichting Toekomstbeeld der Techniek (STT)
Eric Luiijf	TNO
Erik Lebret	RIVM
Hans Marvin	Rikilt
Hans van Vliet	TNO
Harold Bousché	TNO
Huib de Vriend	Lis consult
Ibo v.d. Poel	TU Delft
Ineke Malsch	MalschTechnoValuation
Jacqueline de Jong	Min. VenJ
Jan Broenink	Universiteit Twente
Jelle van Aanholt	UAV
Johanneke Siljee	TNO
Judith Mathijssen	zelfstandige
Kees d' Huy	TNO
Koos v.d. Bruggen	KNAW
Leendert Gooijer	RIVM
Lennart Landman	Clingendael
Lonneke van Noije	SCP
Lotte de Groen	TNO
Marcel Mennen	RIVM
Marco Haas	Min. VenJ
Marius van Rooy	Min. Def

Mark van Staalduinen	iRN / iColumbo
Mark Wiebes	KLPD
Martijn Aslander	zelfstandige
Maurits Butter	TNO
Peter Duin	vtsPN Research & Innovatie
Polo Bais	Min. BZK
Reinout Pieneman	TNO
Rinie van Est	Rathenau
Ronald v.d. Graaf	RIVM
Stefanie Casparie	KNP Politie
Tim Sweijs	HCSS
Virgil Rerimassie	Rathenau

Bijlage C Deelnemers aan de workshop 'Technologieverkenning' met de Taakgroep Analistennetwerk Nationale Veiligheid

20 juni 2013
TNO, Oude Waalsdorperweg 63, Den Haag.

Genodigden	Organisatie
Susan van den Braak	WODC
Peter van Bergeijk	ISS
Paul Dercon	Min. BZK
Kees d' Huy	TNO
Jan Kortekaas	Min. VenJ
Erik Lebret	RIVM
Marcel Mennen	RIVM
Jarig van Sinderen	NMa
Maaike van Tuyll van Serooskerken - van Grieken	Min. VenJ
Harold Bousché	TNO

Bijlage D Megatrends

Om de technologische ontwikkelingen en toepassingen in een brede context van maatschappelijke en andere ontwikkelingen te plaatsen, is ter inspiratie gebruik gemaakt van 'megatrends'.

Megatrends zijn grote (op handen zijnde) ontwikkelingen of veranderingen in het maatschappelijk leven of de maatschappij en haar omgeving. Tegen de specifieke achtergrond van een megatrend kan een toepassing negatief of positief gebruikt worden. Megatrends zijn ontwikkelingen waarvan de verwachting is, dat zij over een lange periode (ten minste 15 jaar) zullen continueren en die wereldwijd van invloed zijn. Ze hebben impact op veel terreinen (politiek, economie, techniek, maatschappij) en beïnvloeden het persoonlijke leven van mensen (individu).

Megatrends zijn bijvoorbeeld [16]:

1. **Veroudering en fragmentatie**
   - toenemende levensverwachting;
   - toenemende fragmentatie en individualisme wat leidt tot plurale levenswijzen.

2. **Verdwijnen/verwateren van grenzen**
   - territoriaal (landgrenzen, multinationals);
   - sociaal (ontzuiling);
   - politiek-economisch (machtsverschuivingen en mondialisering).

3. **Verduurzaming**
   - klimaatverandering en schaarste;
   - duurzame energieopwekking;
   - maatschappelijk verantwoord ondernemen;
   - Gerelateerd thema: intensivering van verkeer en vervoer en infrastructuurgebruik.

4. **Toenemende zorg over risico's en security**
   - zorg over mogelijke negatieve gevolgen van ontwikkelingen op gebied van technologie, gezondheid en milieu;
   - gerelateerde thema's: hang naar gezondheid en voedselveiligheid;
   - gerelateerde thema's: terrorisme, criminaliteit, cyberspionage en cybercriminaliteit, uitval vitale diensten, polarisatie en radicalisering (sociale veiligheid, democratische rechtsorde).

5. **Netwerk samenleving**
   - beschikbaarheid van informatie en kennis;
   - toename van integratie van fysieke en virtuele werelden.

6. **Intelligent Age**
   - kunstmatige intelligentie gekoppeld aan objecten/toepassingen;
   - ICT komt steeds dichter bij (in/op) de mens.

Tijdens de workshop[39] zijn deze megatrends gebruikt als inspiratie om de toepassingen van technologische ontwikkelingen in een algemene context te plaatsten en zo op ideeën voor producten/diensten te komen.

[39] Workshop Technologieverkenning ten behoeve van de Nationale Risicobeoordeling; Analistennetwerk Nationale Veiligheid; datum: 26 November 2012; locatie: KiviNiria, Prinsessegracht 23, Den Haag.

Bijlage E Impactcriteria

Vitaal belang	Impactcriteria
Territoriale veiligheid	Criterium 1.1 Aantasting van de integriteit van het grondgebied: *Het feitelijke of functionele verlies van, dan wel het buiten gebruik en/of toegankelijk zijn van, dan wel het verlies van zeggenschap over delen van het Koninkrijk der Nederlanden (inclusief gebiedsdelen overzee en inclusief territoriale wateren en het luchtruim).*
	Criterium 1.2 Aantasting van de integriteit van de internationale positie van Nederland: *De beschadiging van het aanzien of de invloed of het optreden van Nederland in het buitenland.*
Fysieke veiligheid	Criterium 2.1 Doden: *Dodelijk letsel, direct (binnen een jaar) overlijden of vervroegd overlijden binnen een periode van 20 jaar.*
	Criterium 2.2 Ernstig gewonden en chronisch zieken: *Letselgevallen behorend tot triageklassen T1 en T2, en personen met langdurige of blijvende gezondheidsproblemen zoals ademhalingsklachten, ernstige verbrandingen of huidaandoeningen, gehoorbeschadiging, lijden aan post-traumatisch stress syndroom (PTSS). Slachtoffers behorend tot categorie T1 of T2 hebben onmiddellijk medische hulp nodig en behandeling dient direct aan te vangen (T1) dan wel moeten continu bewaakt worden met een behandeling binnen 6 uur (T2). Chronisch zieken zijn personen die gedurende lange periode (> 1 jaar) beperkingen ondervinden: medische zorg nodig hebben, niet of gedeeltelijk kunnen deelnemen aan het arbeidsproces, door hun ziekte belemmering ervaren in het sociale functioneren.*
	Criterium 2.3 Lichamelijk lijden (gebrek aan primaire levensbehoeften): *Blootstelling aan extreme weersomstandigheden, alsmede het gebrek aan voedsel, drinkwater, energie, onderdak, basale sanitair of anderszins primaire levensbehoeften.*
Economische veiligheid	Criterium 3.1A Kosten: *Geldbedrag in termen van herstelkosten voor geleden schade, extra kosten en gederfde inkomsten.*
	Criterium 3.1B Aantasting economie: *Aantasting van de vitaliteit van de Nederlandse economie.*
Ecologische veiligheid	Criterium 4.1 Langdurige aantasting van het milieu en natuur (flora en fauna): *Langdurige of blijvende aantasting van de kwaliteit van het milieu, waaronder verontreiniging van lucht, water of bodem, en langdurige of blijvende verstoring van de oorspronkelijke ecologische functie, zoals het verlies van soortendiversiteit flora en fauna, verlies van bijzondere ecosystemen, overrompeling door uitheemse soorten.*
Sociale en politieke stabiliteit	Criterium 5.1 Verstoring van het dagelijks leven: *De aantasting van de vrijheid zich te verplaatsen en samen te komen op publieke plaatsen en in openbare ruimten, waardoor de deelname aan het normale maatschappelijk verkeer wordt belemmerd.*
	Criterium 5.2 Aantasting democratische rechtstaat: *De aantasting van het functioneren van de instituties van de Nederlandse democratische rechtsstaat en/of de aantasting van rechten en vrijheden en andere kernwaarden verbonden aan de Nederlandse democratische rechtsstaat zoals vastgelegd in de grondwet.*
	Criterium 5.3 Sociaalpsychologische impact en maatschappelijke onrust: *De reactie van de bevolking die door negatieve emoties en gevoelens (zoals angst, boosheid, ontevredenheid, verdriet, teleurstelling, paniek, walging, gelatenheid/apathie) wordt gekarakteriseerd. Het betreft de bevolking als geheel, waaronder de direct getroffenen. De uitingen van deze emoties en gevoelens kunnen al dan niet waarneembaar (d.w.z. hoorbaar, zichtbaar, leesbaar zijn).*

Een uitgebreidere definitie is beschreven in de methodiek voor de Nationale Risicobeoordeling [15].

Bijlage F Capaciteitenlijst

A. Algemeen:
    10. Regie, aansturing, toezicht;
    11. Signalering en duiding;
    12. Kennisontwikkeling;
    13. Communicatie en informatiemanagement;
    14. Financiële arrangementen;
    15. internationale betrekkingen;
    16. Zelfredzaamheid van burgers en bedrijfsleven;
    17. OTOTEL (Opleiden, Trainen, Oefenen, Toetsen, Evalueren, Lessen leren);
B. Proactie en preventie;
C. Bescherming vitale systemen;
D. Bestrijding, basisvereisten;
E. Bestrijding, bevolkingszorg;
F. Bestrijding, brandweerzorg;
G. Bestrijding, geneeskundige zorg;
H. Bestrijding, politiezorg;
I. Bestrijding, milieu;
J. Herstel en nazorg.

Onder elk van deze hoofdcategorieën zijn in de capaciteitenlijst capaciteiten geformuleerd.

Bijlage G Voorselectie van toepassingen

Deze bijlage geeft een overzicht van de argumenten uit de interviews met experts op basis waarvan toepassingen in de voorselectie zijn opgenomen.

G.1 Nanotechnologie

Ontwik-keling	Toepassing	Relevantie voor de Nationale Veiligheid (binnen 5 jaar)
Miniaturi-sering	NEMS/ MEMS	*Actuatoren kunnen steeds kleiner. Zo krijg je nanochips die kunnen monitoren (lab-on-a-chip). Bijvoorbeeld de water kwaliteit of waardes in het bloed. Een voorbeeld van microsystemen zijn microsatellieten. Deze geven veel (ook arme) landen de mogelijkheid te observeren / te spioneren.*
Nieuwe nanomate-rialen en -structuren	Nano-materialen	*Relevant voor de nationale veiligheid omdat het nanomateriaal andere eigenschappen heeft dan de 'gewone' variant van dat materiaal. Bijvoorbeeld: silica bestaat al heel lang, nano-silica nog niet. Nano-silica wordt in tegenstelling tot silica wél door de darmwand opgenomen. Dit zou dus mogelijk een risico kunnen vormen maar dat is nog niet duidelijk. Nu lopen de grote innovaties. Deze kunnen over vijf jaar op de markt zijn. Beeldvorming is erg belangrijk. Bedrijven kunnen terughoudend worden met innovaties omdat ze, ook bij onbekende effecten bij producten, primair verantwoordelijk zijn. De overheid heeft de verantwoording om innovaties mogelijk te maken.*
Bio-nanotech-nologie	Gepersonificeerde geneesmiddelen	*Nano pil: in de darmen kijken naar afwijkingen in DNA om zo al vroeg te kunnen waarschuwen voor risico op kanker. Dit betreft een screening tool, dankzij welke veel onnodige pijnlijke diagnoses (scopie) kunnen worden vermeden. Het wordt door nanotechnologie mogelijk drug delivery en targeted medicine te realiseren. Het mogelijk maken van het opsporen kan invloed hebben op de sociale stabiliteit; mensen die het kunnen betalen willen steeds meer weten.*

G.2 Bio- / gentechnologie

Ontwik-keling	Toepassing	Relevantie voor de Nationale Veiligheid (binnen 5 jaar)
Genetisch gemodifi-ceerde organismen	Milieu monito-ring	*De trend van miniaturisering i.c.m. monitoring (biochem.) kan leiden tot vele sensoren (bijvoorbeeld op een mobieltje). Dit kan een kans zijn voor de nationale veiligheid voor het monitoren van het milieu.*
Bio-/ gentech-nologie en de mens	Weefselkweek	*Wereldwijd wordt er ook veel onderzoek verricht naar Tissue Engineering, tegenwoordig Regenerative Medicine. Een kans voor de nationale veiligheid als je ziet wat het in de gezondheidszorg teweeg kan brengen.*
	Gepersonali-seerde diagnose, genees-middelen en therapie	*Door medicijnen af te stemmen op het DNA of de leefstijl kan veel gerichter medicatie worden uitgeschre-ven. Dit zal de kosten voor de gezondheidszorg mogelijk verminderen (effectiever) maar mogelijk ook verhogen (meer kans op 'uitstel' van de dood).*
	DNA metho-dieken	*Data die gegenereerd wordt, levert ook risico's op voor de maatschappij. Bijvoorbeeld met DNA data kan je ook knoeien. Interpretatie is niet waardenvrij.*
Biobased economy	Bio-brand-stoffen	*Er is een trend richting chemische geproduceerde verbindingen die biologische productie vervangen (from petrolbased to biobased). Bijvoorbeeld autobrandstoffen die eerder uit petrochemie werden gewonnen en nu door vergisting van biomassa. Dit biedt enorme kansen voor een schonere leefomgeving en is beter voor de wereldeconomie omdat het niet concurreert met gebruik van goede stoffen voor voedsel.*

G.3 Neurotechnologie

Ontwik-keling	Toepassing	Relevantie voor de Nationale Veiligheid (binnen 5 jaar)
Begrijpen van hersenen en cognitie	Inzicht in menselijk gedrag	*Een dreiging is gelegen in 'de publieke opinie'. Toepassing van neurotechnieken kan worden gezien als 'sleutelen aan de mens of natuur' en, zoals we ook bij andere technologieën hebben gezien, daardoor kan weerstand ontstaan die uiteindelijk kan leiden tot een rem op de ontwikkeling van dit soort technieken. De drang tot het steeds meer en beter presteren, die duidelijk merkbaar is in onze maatschappij, kan leiden tot toenemende acceptatie van technieken en middelen om de mens steeds beter te maken. Zowel sociale druk als druk vanuit werkgevers kan die 'acceptatie' versterken, ook al is de bereidheid er 'op individueel niveau' niet of veel minder. Deze ontwikkeling hangt samen met toenemende individualise-ring en de rat race in de moderne maatschappij. Indien toepassing van technieken en middelen met dit doel steeds meer geaccepteerd raakt, nemen de mogelijke risico's als gevolg van onjuist of oneigenlijk gebruik toe.*
Neuro-diagnos-tiek, therapieën en genees-mid-delen	Neurofarmaca	*Een potentieel risico is de trend dat mensen in toenemende mate aan zelfmedicatie doen. Doordat medicijnen en andere middelen steeds gemakkelijker en op grotere schaal buiten het gebruikelijke medische circuit zijn te verkrijgen, mede dankzij internet, zouden burgers kunnen overgaan tot het zelf aanschaffen van medicijnen.* *In feite gebeurt dat al met relatief onschuldige middelen (voedingssupplementen, vitamines, pijnstillers, 'doping', etc.), maar als 'de burger' ook minder onschuldige middelen gaat aanschaffen en zonder kennis van zaken gaat gebruiken, zouden daar risico's uit kunnen ontstaan.* *Het is ook de verwachting dat medicijnen (bijvoorbeeld Ritalin) meer gebruikt zullen worden door gewone mensen ter verhoging van de concentratie.*
Convergentie met bio- en informatie-technologie	Brain Machine Interfacing	*BMI gaat erg snel in Nederland: het afleiden van hersensignalen met zowel de schedel open als de schedel dicht om externe devices aan te sturen. De toepassingen van aansturing vanuit de hersenen zijn nu nog beperkt (bijvoorbeeld aansturing van de arm van iemand met handicap), maar kunnen worden uitgebreid naar het aansturen van bijvoorbeeld drones.*

G.4 Materiaaltechnologie

Ontwikkeling	Toepassing	Relevantie voor de Nationale Veiligheid (binnen 5 jaar)
Elektronische en optische materialen	Sensoren	*Convergentie tussen bio, nano, ict zie je op alle vlakken ontstaan, ook voor sensoren. Voorstelbaar is dat steeds meer producten sensoren bevatten en dat die informatie is in te zetten voor allerlei doeleinden zoals monitoring van het milieu.* *Er komen dagelijks nieuwe mogelijkheden bij.*
Slimme materialen	Zelfherstellende materialen	*Coatings worden steeds beter en kunnen zelfs zelf herstellend zijn. Voorbeeld is biofilms: schimmels die weer groeien over het basismateriaal heen. Maar ook zelfherstellende materialen bijvoorbeeld voor indringende kogels, Nederland heeft een leidende positie hierin.* *Ontwikkelingen lopen nu en komen de aankomende vijf jaar zeker op de markt.*
Biomaterialen	Bio-medische materialen	*Kunstgewrichten en kunstorganen zullen komen, maar het is de vraag welke effecten het heeft op de maatschappij. Zullen mensen zich kunstmatige ledenmaten gaan aanmeten om beter te kunnen presteren? Kunstgewrichten en -organen zijn er nu al. Of het gebruik daarvan binnen vijf jaar een grote vlucht neemt is nog wel de vraag.*
	Materialen voor klimaat beïnvloeding	*In potentie kunnen materialen voor klimaat beïnvloeding grote internationale spanningen met zich meebrengen (klimaatbeïnvloeding door bijvoorbeeld zilveroxide deeltjes in de lucht te brengen).* *De gevolgen zijn onzeker vanwege de verschillende feedback loops. Het thema raakt Nederland in het bijzonder vanwege de ligging.* *Het wordt al gebruikt en zal alleen maar meer worden.*
Energie materialen	Energieopslag	*Een mogelijk effect is de mindere afhankelijkheid van andere landen als energieopslag goed geregeld is. Jaarlijks sterven er 10.000 mensen aan energy poverty, terwijl er meer dan genoeg is. De distributie en opslag moeten echter nog veel beter worden om dat op de goede plek te krijgen, op het juiste moment.* *Zelf energie opwekken op lokale schaal: decentrale clubjes die energie gaan opwekken. Dit beïnvloedt (op negatieve wijze) de robuustheid van de energievoorziening.* *Met de ontwikkeling van nieuwe manieren voor energiewinning is de mogelijkheid voor lokaal energie opslag een barrière die genomen moet worden in de aankomende vijf jaar.*

G.5 Informatietechnologie

Ontwikkeling	Toepassing	Relevantie voor de Nationale Veiligheid (binnen 5 jaar)
ICT infrastructuur en hardware	3D *printing*	*Grote gevaar is dat je veel gevaarlijke producten kunt maken als je dat wilt, zonder dat dit te monitoren is: spijkerbommen, wapen(onderdelen), etc.* *Materialen worden steeds goedkoper> Het kan dus een flinke vlucht nemen de aankomende vijf jaar.*
Slimme infrastructuur	Slimme energie infrastructuur (*Smart Grids*)	*De transitie naar Smart Grids is onvermijdelijk, maar de robuustheid van een systeem is op grote schaal is nog onduidelijk. Vervangen we een nu werkend systeem niet voor een nieuwe afhankelijkheid en welke gevaren hangen daar aan?*
	Smart cities, smart roads, smart buildings	*Ontwikkeling van slimme wijken / slimme steden kan er toe leiden dat heel veel informatie kan worden afgelezen. Hier kan men heel veel van leren, maar de stap naar ingrijpen op individueel (fout) gedrag is dan niet ver meer.*
Intelligente en slimme robots	Industriële robotica	*Minder relevant: robots die op echt cruciale plekken zitten worden ook echt goed beveiligd. Gevaarlijker zijn robots in de consumenten wereld, die makkelijker zijn te hacken.*
	Robotica voor de gezondheidszorg	*Belangrijke toepassing is care, cure (om zorgkosten te onderdrukken). Robotica kan feitelijk overal worden toegepast waar het kostbaar of gevaarlijk is voor mensen om te wat doen; desnoods door mensen aangestuurd.* *Cyber is een opkomend fenomeen; zo kan het zijn dat robots worden overgenomen.*
	Gerobotiseerde veiligheid	*Een belangrijke toepassing is inspectie van de veiligheid (bijvoorbeeld controle van gasleidingen, plant, centrales). Dit is een kans voor de fysieke veiligheid van personeel. Maar ook het gebruik van drones tijdens een incident (rescue of creëren overzicht incident) biedt een kans.* *Inspectie gebeurt nu al in energiecentrales en de ontwikkeling loopt voor het controleren van gasleidingen door robots.* *Men kan kleine helikopters inzetten om Situational Awareness (SA) door te sturen naar de centrale bij kleine incidenten, maar ook bij grotere rampen. Camera's kunnen dan worden ingezet voor data acquisitie en detectie van slachtoffers. Momenteel is men bezig met 'Alpines' waar wordt gekeken naar toepassing van helikopters en fixed wing drones voor het verkrijgen van SA en om daarmee levens te kunnen redden.*
Data-opslag, -ontsluiting en -analyse	*Big data, open data*	*De ontsluiting van nu nog massa's ondoordringbare data brengt veel kansen en dreigingen met zich mee. Kansen zijn bijvoorbeeld betere opsporing, maar een dreiging is het als kwaadwillenden zelf allerlei informatie aan elkaar gaan koppelen en daarmee conclusies over personen kunnen trekken die we niet willen.*
Internet van de toekomst	*Internet of things*	*'The internet of things' zal heel veel dingen met elkaar verbinden. Dit brengt gevaren met zich mee. Waar we dus op afstand kunnen zien, in de tijd, hoe dijken op bepaalde plekken verzwakken kunnen terroristen dat ook. Bij de verstoring van internet verliezen we ook de mogelijkheid om infrastructuur te monitoren. Als dat een afhankelijkheid is geworden, is dat een gevaar.* *Een mogelijk gevaar zit ook in internet op zich. Internet geeft burgers een mogelijkheid zich heel snel te organiseren.* *De toepassingen van internet of things zullen tussen nu en 5 jaar beschikbaar worden voor consumenten / bedrijven.*

Bijlage H Selectie van toepassingen voor verdere uitwerking

Deze bijlage geeft een overzicht van de door enkele experts op de technologieën aangegeven mate van kans of dreiging bij de geïnventariseerde toepassingen genoemde voorbeelden van de bij de geïnventariseerde toepassingen genoemde relevante producten en diensten.

De mate van kans of dreiging is als volgt gescoord:

Vitale belangen:	
Impact van product of dienst (laag - hoog)	
•	= impact is zeer laag – laag
••	= impact is laag – gemiddeld
•••	= impact is gemiddeld – hoog
••••	= impact is hoog – zeer hoog

Weerbaarheid:	
Product of dienst verhoogt / verlaagt de weerbaarheid	
++	= sterk verhoogd
+	= verhoogd
o	= geen invloed
-	= verlaagd
--	= sterk verlaagd

H.1 Nanotechnologie

Nano- en micro-elektromechanische systemen (NEMS/MEMS)						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Microsatellieten	••••	•••	••	•	•••	o
Nanobots voor waterzuivering	•	•	•	•	•	o
Internet of nanothings	•••	•••	•••	•	••	+

Nanomaterialen						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Nanodeeltjes in grondstoffen	•	••	•	••	•	o
Identiteits-manipulatie	••	•••	•••	•	•••	-
Nanodeeltjes in zonnecellen	•	•	••	••	••	o
Nanodeeltjes in kleding	•	••	•	••	•	o
Nanodeeltjes in wapens	•••	•••	•	•••	••	-

Gepersonificeerde geneesmiddelen						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Lab-on-a-chip	•	••	••	••	••	o
Medische *bots*	•	••	••	••	••	o

H.2 Bio-/gentechnologie

Milieu monitoring						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Biosensoren	•	•	•	••	•	o

Weefselkweek						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Snelle EHBO kit voor *first responders*	•	•	•	•	•	o
Vlees 2.0	•	•	•	•	•	o

Gepersonaliseerde diagnose, geneesmiddelen en therapie						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Persoonlijke medicatie	•		••	•	•••	-
Gepersonaliseerde diagnose	•	••	•••	•	•••	o

DNA methodieken						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Opstellen van DNA databanken	•	•••	•	•	••••	+

Biobrandstoffen						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Biodiesel of bio-ethanol	•	•	••	••	•	+

H.3 Neurotechnologie

Inzicht in menselijk gedrag						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Determinanten voor ontdekken potentiële ontsporing	•	••••	•	•	••••	o
Profiling	•••	••••	•	•	••••	o
Optogenetics	•••	•••	•	•	•••	o

Neurofarmaca						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Geneesmiddelen tegen depressies	•	•••	••••	•	•••	+
Geneesmiddelen tegen dementie	•	•	••••	•	•••	o
Middel voor het verbeteren van het leervermogen	••••	•••	••••	•	••••	+

Brain Machine Interfacing						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Systeem voor aansturen van externe apparaten vanuit de hersenen	••••	•••	•	•	••	o

H.4 Materiaaltechnologie

Sensoren						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Crowdsourcing van sensoren	••	•••	••••	•	••••	+
Overal sensoren en grote stromen informatie	•••	•••	••••	••	••••	++

Materialen voor klimaatbeïnvloeding						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Beïnvloeden van het klimaat	•	••	•	••	•	o

Bio-medische materialen						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
'Mens-verbetering'	•	•••	••••	•	••••	o

Energieopslag						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Decentralisatie van de energieopslag	••••	••	••••	•••	••••	++
CO_2 opvang	•	•	••	•••	••	o

H.5 Informatietechnologie

3D printing						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Printen van gebruiks-voorwerpen	•	•••	••	•	•	-
Printen van voedsel	•	•••	•••	••••	•	+

Slimme energie infrastructuur (Smart Grids)						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Infrastructuur voor decentralisatie van energieopwekking	•	•••	••••	••	•	+

Robotica voor veiligheid						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Inspectierobots	•	•••	••	•••	•	+
Surveillance bots	••••	••	••	•••	••••	+

Robotica voor de gezondheidszorg						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Robotica in de operatiekamer	•	•••	•	••	•	o
Telerobotica	•••	•••	•	••	•	+

Big data, open data						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Big data voor rampenbestrijding	••	••	••	•••	•	++

Internet of things						
Producten en diensten:	Territoriale veiligheid	Fysieke veiligheid	Economische veiligheid	Ecologische veiligheid	Sociale en politieke stabiliteit	Weerbaarheid
Intelligente transport systemen	•	•••	••	•••	•	o
Bewaking en aansturing kritieke infrastructuur	•	••••	•••	••••	•	+
Dijkbewaking	•	••••	•••	••••	•	+

Bijlage I Geïdentificeerde toepassingen

De identificatie van toepassingen die relevant zijn voor de nationale veiligheid is gebeurd op basis van de door de experts aangegeven mate van kans of dreiging (bijlage H). De uiteindelijke selectie van toepassingen voor verdere uitwerking is vanuit nationale veiligheidsargumenten gemaakt door experts op het gebied van de nationale veiligheid in Nederland (bijlage C). De tabel hieronder geeft een overzicht waarin de toepassingen per technologie op een rij zijn gezet, met daarbij de argumentatie van de score door de experts[40] en de argumentatie waarom de toepassingen wel of niet zijn geselecteerd voor verdere uitwerking.

Vanwege de brede verkennende scope van deze studie is er een selectie gemaakt van toepassingen waarvoor de kansen en dreigingen verder zijn uitgewerkt. Dat neemt niet weg dat de overige in deze verkennende studie geïnventariseerde toepassingen ook interessant zijn in relatie tot de nationale veiligheid. Deze toepassingen vallen nu af maar zijn wel degelijk mogelijke kandidaten voor nader onderzoek.

[40] Wanneer meningen van experts over de impact van toepassingen elkaar tegenspreken, zoals de mening van materiaaltechnologie-experts en informatietechnologie-experts over decentralisatie van energieopslag is dat aangegeven in de opmerkingen in de tabel.

Toepassing	Toelichting score	Geselec-teerd	Toelichting selectie	Opmerkingen
Nanotechnologie				
NEMS / MEMS	Microsatellieten bieden de mogelijkheid tot observatie of spionage vanuit de ruimte. Internet of nanothings biedt een kans doordat zeer kleine gekoppelde systemen kunnen worden ingezet om bijvoorbeeld metingen te doen.	Ja	Geselecteerd als één van de twee op impact op nationale veiligheid hoogst scorende toepassingen onder nanotechnologie.	--
Nanomaterialen	Nanodeeltjes in wapens kunnen een dreiging vormen doordat schadelijke stoffen nog effectiever kunnen worden gemaakt. Nanotechnologie kan mogelijk worden gebruikt voor identiteitsmanipulatie.	Ja	Geselecteerd als één van de twee op impact op nationale veiligheid hoogst scorende toepassingen onder nanotechnologie.	--
Gepersonificeerde geneesmiddelen	Door sommige toepassingen kan de privacy van burgers geschonden worden. Medische bots geven de mogelijkheid de gezondheid van personen te monitoren en eerder afwijkingen te detecteren, maar hebben geen rechtstreekse invloed op de nationale veiligheid.	Nee	Niet geselecteerd, want lagere score dan de twee geselec-teerde toepassingen onder nanotechnologie.	--

Toepassing	Toelichting score	Geselec-teerd	Toelichting selectie	Opmerkingen
Bio- / gentechnologie				
Milieu monitoring	Milieu monitoring biedt kansen voor detectie en identificatie van milieuvervuilende stoffen. De koppeling met de nationale veiligheid is minder direct.	Nee	Niet geselecteerd, want lage impact op de nationale veiligheid verwacht.	De onder bio- / gentechnologie bij de toepassing **milieu monitoring** genoemde sensoren worden, in tegenstelling tot de onder materiaaltechnologie genoemde **sensoren**, niet meegenomen in een verdere uitwerking van toepassingen. Het verschil in scores door de experts, is mogelijk te verklaren doordat sensoren genoemd onder materiaaltechnologie over allerlei typen sensoren gaat. Vooral de bundeling en interpretatie van al die verschillende gegevens maakt sensoren interessant voor de nationale veiligheid.
Weefselkweek	Weefselkweek biedt kansen om patiënten te helpen. Van weefselkweek wordt een lage tot zeer lage impact op de nationale veiligheid verwacht.	Nee	Niet geselecteerd, want lage impact op de nationale veiligheid verwacht.	--
Gepersonaliseerde diagnose, geneesmiddelen en therapie	Van gepersonaliseerde diagnose gaat een kans en een dreiging uit; voor individuen betekent het een effectievere behandeling, maar grote kennis over het DNA van patiënten kan ook leiden tot aantasting van het recht tot behandeling of verzekering.	Nee	Niet geselecteerd, want beperkte impact op de nationale veiligheid verwacht.	--
DNA methodieken	DNA methodieken bieden mogelijkheden voor identificatie van personen. Waar een overzicht van de kennis over DNA tot grote inzichten kan leiden, kan een dergelijk overzicht ook worden misbruikt.	Ja	Geselecteerd als één van de twee op impact op nationale veiligheid hoogst scorende toepassingen onder bio- / gentechnologie.	--
Biobrandstoffen	Van biobrandstoffen, zoals biodiesel of bio-ethanol wordt een beperkte impact op de nationale veiligheid verwacht. Het gaat hier vooral om het vervangen van fossiele brandstoffen.	Nee	Niet geselecteerd, want beperkte impact op de nationale veiligheid verwacht.	Twee grote op handen zijnde veranderingen op het gebied van energie worden zeer verschillend beoordeeld. Materiaaltechnologie-experts verwachten dat decentralisatie van **energieopslag** grote gevolgen zal hebben voor de nationale veiligheid, terwijl bio- / gentechnologie-experts verwachten dat het gebruik van **biobrandstoffen** een beperkte impact zal hebben op de nationale veiligheid. Mogelijk zit het verschil in de onzekerheid die de decentralisatie van energieopslag met zich meebrengt. Er is nog weinig te zeggen over hoe de energiedistributie zal plaatsvinden en hoe stabiel het netwerk zal zijn. Een instabiel netwerk in deze tijd dat alles draait op elektriciteit zou snel een nationale ramp zijn. Voor biobrandstoffen geldt dat dit naast de fossiele brandstoffen kan blijven bestaan, waarmee de onzekerheid betreffende het gebruik ervan minder is.

Toepassing	Toelichting score	Geselec-teerd	Toelichting selectie	Opmerkingen
Neurotechnologie				
Inzicht in menselijk gedrag	Hiermee wordt het mogelijk mensen te identificeren die meer kans maken op afwijkend gedrag. Van producten en diensten zoals determinanten voor het ontdekken van potentiële ontsporing, *profiling* en *optogenetics* wordt gemiddeld een beperkte impact op de nationale veiligheid verwacht.	Nee	Niet geselecteerd, want beperkte impact op de nationale veiligheid verwacht.	--
Neurofarmaca	Geneesmiddelen tegen depressies en middelen voor het verbeteren van het leervermogen bieden de mogelijkheid het presteren van mensen te verbeteren en geven daarmee kansen voor het vergroten van de fysieke en economische veiligheid en voor het versterken van de weerbaarheid.	Nee	Niet geselecteerd, want beperkte impact op de nationale veiligheid verwacht.	--
Brain Machine Interfacing	Van de toepassing *Brain Machine Interfacing*, bijvoorbeeld voor het aansturen van externe apparaten vanuit de hersenen, wordt een beperkte impact op de nationale veiligheid verwacht.	Nee	Niet geselecteerd, want beperkte impact op de nationale veiligheid verwacht.	--

Toepassing	Toelichting score	Geselec-teerd	Toelichting selectie	Opmerkingen
Materiaaltechnologie				
Sensoren	De toepassing sensoren biedt kans om gedetailleerde informatie te verzamelen.	Ja	Geselecteerd als één van de twee op impact op nationale veiligheid hoogst scorende toepassingen onder materiaaltechnologie.	De onder bio- / gentechnologie bij de toepassing **milieu monitoring** genoemde sensoren worden, in tegenstelling tot de onder materiaaltechnologie genoemde **sensoren**, niet meegenomen in een verdere uitwerking van toepassingen. Het verschil in scores door de experts, is mogelijk te verklaren doordat sensoren genoemd onder materiaaltechnologie over allerlei typen sensoren gaat. Vooral de bundeling en interpretatie van al die verschillende gegevens maakt sensoren interessant voor de nationale veiligheid.
Zelfherstellende materialen[7]	Voor deze toepassing zijn geen relevante producten en diensten geïdentificeerd voor de nationale veiligheid.	Nee	Niet geselecteerd, want geen relevante producten of diensten geïdentificeerd.	Zoals aangegeven in paragraaf 6.2 zijn er tijdens de workshop 'Technologieverkenning ten behoeve van de Nationale Risicobeoordeling' (zie werkwijze in paragraaf 2.2) voor **zelfherstellende materialen** geen relevante producten en diensten geïdentificeerd voor de nationale veiligheid. Dat neemt niet weg dat deze materialen mogelijk interessant zijn gerelateerd aan de nationale veiligheid. Te denken valt aan mogelijke consequenties voor sporenonderzoek. Als materiaal zichzelf kan herstellen zullen eventuele sporen mogelijk verloren gaan (vingerafdrukken, inbraaksporen, breuk en impactsporen, etc.). Deze toepassing is daarom een mogelijke kandidaat voor nader onderzoek.
Materialen voor klimaatbeïnvloe-ding	Van de toepassing van materialen voor klimaat-beïnvloeding wordt een lage tot zeer lage impact verwacht voor de nationale veiligheid. De verwachting is dat het internationaal wel een grote rol kan spelen.	Nee	Niet geselecteerd, want lagere score dan de twee geselec-teerde toepassingen onder materiaaltechnologie.	--
Biomedische materialen	Bio-medische materialen bieden mogelijkheden voor 'mens-verbetering' en hebben naar verwachting een zeer lage impact op de territoriale veiligheid en ecologische veiligheid, een gemiddelde impact op fysieke veiligheid en een hoge impact op economische veiligheid en sociale en politieke stabiliteit.	Nee	Niet geselecteerd, want lagere score dan de twee geselec-teerde toepassingen onder materiaaltechnologie.	--
Energieopslag	Decentralisatie van energieopslag biedt kansen in ecologische en geopolitieke zin; het verhoogt de duurzaamheid en zorgt mogelijk voor minder afhankelijk-heid tussen landen.	Ja	Geselecteerd als één van de twee op impact op nationale veiligheid hoogst scorende toepassingen onder materiaaltechnologie.	Twee grote op handen zijnde veranderingen op het gebied van energie worden zeer verschillend beoordeeld. Materiaaltechnologie-experts verwachten dat decentralisatie van **energieopslag** grote gevolgen zal hebben voor de nationale veiligheid, terwijl bio- / gentechnologie-experts verwachten dat het gebruik van **biobrandstoffen** een beperkte impact zal hebben op de nationale veiligheid. Mogelijk zit het verschil in de onzekerheid die de decentralisatie van energieopslag met zich meebrengt. Er is nog weinig te zeggen over hoe de energiedistributie zal plaatsvinden en hoe stabiel het netwerk zal zijn. Een instabiel netwerk in deze tijd dat alles draait op elektriciteit zou snel een nationale ramp zijn. Voor biobrandstoffen geldt dat dit naast de fossiele brandstoffen kan blijven bestaan, waarmee de onzeker-heid betreffende het gebruik ervan minder is. De impact van decentralisatie van **energieopslag** en de ontwikkeling van een **slimme energie infrastruc-tuur (Smart Grids)** op de nationale veiligheid wordt door materiaaltechnologie-experts en informatie-technologie-experts zeer anders ingeschat; een hoge versus een lage impact op de nationale veiligheid. Op basis van deze conflicterende scores is voor deze toepassingen nader onderzoek aan te bevelen.

Toepassing	Toelichting score	Geselec-teerd	Toelichting selectie	Opmerkingen
Informatietechnologie				
3D *printing*	De verwachte impact van het printen van gebruiksvoorwerpen, waaronder wapens, met de toepassing 3D *printing* is gemiddeld voor de fysieke veiligheid en de economische veiligheid en voor de andere vitale belangen zeer laag.	Ja	Geselecteerd, want door technologie experts gemiddelde impact verwacht en door experts nationale veiligheid mogelijk hogere impact.	Doordat de toepassing **3D printing** recent veel in het nieuws is, waarbij ook het fabriceren van (onderdelen) van wapens aan de orde komt, lijkt de door de experts gegeven score laag. Binnen redelijk afzienbare tijd kan iedereen toegang krijgen tot 3D *printing*. Wellicht kan het fabriceren van wapens - alhoewel vooralsnog waarschijnlijk van mindere kwaliteit dan echte wapens ook voor bijvoorbeeld de schooljeugd toegankelijk worden.
Slimme energie infrastructuur (Smart Grids)	Door decentralisatie van de energieopwekking zou de infrastructuur enerzijds robuuster kunnen worden (door de decentralisatie), anderzijds mogelijk ook kwetsbaarder (door de koppeling van systemen).	Nee	Niet geselecteerd, want lagere score dan de geselecteerde toepassingen onder informatietechnologie.	De impact van decentralisatie van **energieopslag** en de ontwikkeling van een **slimme energie infrastructuur (Smart Grids)** op de nationale veiligheid wordt door materiaaltechnologie-experts en informatietechnologie-experts zeer anders ingeschat; een hoge versus een lage impact op de nationale veiligheid. Op basis van deze conflicterende scores is voor deze toepassingen nader onderzoek aan te bevelen.
Smart cities, smart roads, smart buildings	Meegenomen onder *Internet of things*	Nee	Meegenomen onder *Internet of things*	--
Robotica voor veiligheid	Surveillance bots komen naar voren in de selectie vanwege de mogelijkheden surveillance automatisch en op afstand uit te laten voeren ten behoeve van de hulpdiensten.	Ja	Geselecteerd als één van de op impact op nationale veiligheid hoogst scorende toepassingen onder informatietechnologie.	--
Robotica voor de gezondheidszorg	Robotica in de gezondheidszorg is vooral gericht op het automatiseren en verbeteren van de gezondheidszorg. Hiervan wordt een lage tot gemiddelde impact verwacht voor de nationale veiligheid.	Nee	Niet geselecteerd, want lagere score dan de geselecteerde toepassingen onder informatietechnologie.	--
Big data, open data	De verwachte impact van big data is laag tot gemiddeld voor de meeste vitale belangen. Voor de weerbaarheid wordt verwacht dat deze sterk kan worden verhoogd, bijvoorbeeld door slim en efficiënt informatie uit grote en complexe hoeveelheden data te genereren.	Ja	Geselecteerd, want verwacht dat weerbaarheid sterk kan worden vergroot.	--

Toepassing	Toelichting score	Geselec-teerd	Toelichting selectie	Opmerkingen
Informatietechnologie				
Internet of things	Dijkbewaking en bewaking en aansturing van vitale infrastructuur hebben naar verwachting een hoge tot zeer hoge impact voor de fysieke en ecologische veiligheid. Experts geven aan dat er zowel kansen als dreigingen zijn. Kansen omdat zwakke plekken gemonitord kunnen worden, dreigingen omdat besturing van vitale infrastruc-tuur deze ook kwetsbaar wordt voor (moedwillige) verstoring met mogelijk ongelukken en negatieve economische gevolgen.	Ja	Geselecteerd als één van de op impact op nationale veiligheid hoogst scorende toepassingen onder informatietechnologie.	--

Analistennetwerk Nationale Veiligheid
Ir. P.J. van Vliet (editor, TNO)
Dr. M.G. Mennen (editor, RIVM)

Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

Dit is een uitgave van:

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Algemene Inlichtingen- en Veiligheidsdienst (AIVD)

Stichting Nederlands Instituut voor Internationale Betrekkingen 'Clingendael'

Erasmus Universiteit Rotterdam, Institute of Social Studies (ISS)

Postbus 1 | 3720 BA Bilthoven
www.rivm.nl

januari 2014

006354