

# De impact van technologie op nationale veiligheid

G. Klein Baltink\*

## Inleiding

Technologie<sup>1</sup> is geen panacee voor alle problemen van onze hedendaagse samenleving. Wel kan technologie leiden tot het verkrijgen van een voorsprong ten opzichte van concurrenten of tegenstanders, of tot de opheffing van onvolkomenheden in organisaties of in menselijke prestaties. Naar mijn mening wordt technologie reeds eeuwenlang goed benut binnen krijgsmachten, maar tot op heden nog onvoldoende in het domein van nationale veiligheid.

Bestudering van de mate waarin technologie wordt gebruikt, vereist een grondig inzicht in de verschillende schakels in de keten van maatschappelijke besluitvorming en implementatie. In de dagelijkse praktijk bepalen deze schakels (in onderlinge samenhang) of een maatschappelijk vraag-

stuk met succes kan worden opgelost door innovatieve ideeën of systemen. In een sterk vereenvoudigde vorm kunnen de vier elementaire schakels in die keten als volgt benoemen:<sup>2</sup>

- de politieke agenda c.q. wil om een maatschappelijk probleem op te lossen;
- de beschikbaarheid van vernieuwende kennis om een innovatiesprong te kunnen maken;
- de aanwezigheid van economische bedrijvigheid die de innovatie kan vertalen naar toepasbare producten of diensten;
- de inpasbaarheid van de producten of diensten in de samenleving.<sup>3</sup>

Vanuit dit denkkader wil ik een aantal algemene en bijzondere technologische ontwikkelingen behandelen die in het kader van de nationale veiligheid, en in het bijzonder voor het in



Afb. 1: De verschillende schakels in de innovatieketen

dit themanummer geschetste scenario, van belang zijn. Ik zal echter eerst enkele algemene opmerkingen plaatsen over technologie en de mogelijkheden om daarvan effectief gebruik te maken.

## De rol van technologie bij de krijgsmacht

Van oudsher zijn veel technologische vernieuwingen voortgekomen uit het militaire bedrijf, waarbij periodes van operationele inzet vaak als katalysator dienden. Zo zijn er veel voorbeelden bekend van de introductie van nieuwe technologie, alternatieve materialen en geheel andere werkwijzen vlak voor en tijdens de Tweede Wereldoorlog. Zowel aan Duitse als aan Geallieerde zijde zijn daardoor fundamentele doorbraken bereikt op tal van

\* De auteur heeft na zijn KMA opleiding diverse functies binnen de Koninklijke Landmacht vervuld en is in 1994 overgestapt naar TNO. Momenteel is hij Directeur Markt bij TNO Defensie en Veiligheid.

1 Technologie wordt hier gebruikt als een generieke aanduiding – het betreft niet alleen harde betakennis, die veelal in hardware zijn toepassing vindt, maar ook onder meer sociaal-psychologische kennis, die bijvoorbeeld toegepast kan worden bij training en opleiding en bij het zoeken naar verbeteringen van menselijk presteren.

2 Afkomstig uit een strategische beschouwing van technologie door Jan Vogel en Maurits Butter, TNO. Deze basisbenadering is onderdeel van *Dynamo: dynamic and systematic monitoring of future developments*.

3 In deze sterk vereenvoudigde weergave van werkelijke interactie worden belangrijke elementen weggelaten (evolutie in de tijd, evaluatie van de geïmplementeerde oplossing etcetera). Voor een juist begrip van de mate waarin technologie bruikbaar kan zijn en de beoordeling of aan primaire randvoorwaarden is voldaan, kan zij naar mijn mening echter volstaan.

terreinen. Hoewel veel voorbeelden die daarbij horen tot de verbeelding spreken (zoals de feitelijke introductie van radar, moderne raketssystemen, slimme encryptietechnieken en hoogwaardige legeringen), zijn het vaak de onopvallende innovaties die voor de echte doorbraak zorgen. Soms gaat het daarbij helemaal niet om nieuwe technologie als zodanig, maar om een innovatie in een productieproces of in een procedure voor het analyseren van inlichtingen.

Tijdsdruk, het evidente maatschappelijke belang, de politieke bereidheid om middelen ter beschikking te stellen en de wil om een echte verbetering te bereiken zijn daarbij van doorslaggevend belang geweest. Dergelijke voorbeelden van succesvolle innovaties kunnen we eveneens ontleen aan de recente krijgsgeschiedenis (grootschalige inzet van onbemande waarnemingssystemen in de Golf-regio) of aan het verdere verleden (standaardisatie van de bewapening en het stelselmatig gebruik van 'drills' door het Staatse leger onder Prins Maurits).<sup>4</sup>

Daarmee is echter nog niet de vraag beantwoord of dergelijke doorbraken



**Exercitie met musket**  
**Afbeelding uit: Jacob de Gheijn,**  
**Wapenhandelinge van roers,**  
**musquetten ende spiessen**  
(Collectie NIMH)

nu te danken zijn aan de ervaren noodzaak ten tijde van de gevechtshandelingen, of dat zij juist voorwaardenscheppend waren om met kans op succes de strijd aan te gaan. Dat dilemma speelt ook in de toepassing van moderne technologie bij nationale veiligheid: maakt de inzet van hoogwaardige technologische oplossingen het mogelijk om de nationale veiligheid te garanderen, of moeten alle technologische zeilen worden bijgezet om inbreuken te repareren en vervolgens te voorkomen?

In deze bijdrage zal ik proberen dit dilemma van kanttekeningen te voorzien en door middel van voorbeelden aan te geven hoe naar mijn mening technologie aan nationale veiligheid kan bijdragen.

### **Spelers in het nationale veiligheidsdomein**

De rol van de krijgsmacht in het kader van nationale veiligheid verschilt traditioneel sterk van die van de andere spelers, zoals politie, brandweer, hulpverleningsdiensten en civiele opsporingsautoriteiten. Van oudsher zijn militairen gewend om grootschalig geweld toe te passen, als andere (diplomatieke) middelen falen. Traditioneel speelt daarbij technologie (in de vorm van sensor-, wapen- en commandovoeringssystemen) een grote rol en is de militair gewend om daar optimaal gebruik van te maken.

De laatste decennia is daarbij tevens een hernieuwde aandacht voor de individuele militair als 'wapensysteem' zichtbaar. De trend 'van bewapende mannen naar bemande wapens' lijkt daarmee te eindigen en te worden vervangen door '(on)bewapende mannen en onbemande wapens'.<sup>5</sup> De militair was traditioneel gewend om zijn taken eindeloos te oefenen en zich feitelijk naast de dagelijkse samenleving voor te bereiden op een grootschalige, zeer gewelddadige activiteit gericht tegen een soortgelijke tegenstander, die kon beschikken over vergelijkbare systemen.

Door de wapenwedloop was er een voortdurend wederzijds streven naar verbetering van de beschikbare wapensystemen, dat soms absurde vormen aannam. In de laatste twintig jaar zien we echter dat de inzet bij vredesoperaties van militairen een andere werkwijze verlangt. De tegenstander verschilt behoorlijk van de gedachte tegenstanders uit de periode van de Koude Oorlog, zowel kwantitatief als kwalitatief. De 'spelregels' zijn behoorlijk aangepast en de feitelijke inzet vindt plaats te midden van de burgerbevolking, die vaak tegen wil en dank bij de operatie betrokken is.

Het geweldsniveau van het eigen optreden is gemiddeld veel lager dan in het traditionele grootschalige conflict. De tegenstander schuwt gewelddadige activiteiten niet, maar deze kenmerken zich vaak door een incidenteel karakter en de inzet van primitieve of zelfs verouderde middelen. Het voorkomen van nevenschade speelt bij dergelijke tegenstanders kennelijk geen rol.

### **Van elkaar leren**

De militaire inzet verschuift door deze ontwikkelingen in de richting van het type inzet van politie en hulpdiensten rondom bijvoorbeeld een natuurramp of een grootscheepse brand. Dat brengt aanpassingen mee in organisatie, optreden, training en uitrusting die voor een deel afgekeken kunnen worden uit het civiele domein (denk bijvoorbeeld aan *crowd and riot control*).

Anderzijds is het besef van terroristische dreiging voor ons eigen land en

<sup>4</sup> Zie voor de invoering van de standaard-exercitie door Prins Maurits het interessante boek *Wapenhandelinge van roers, musquetten ende spiessen*, van Jacob de Gheijn uit 1607 (in facsimile uitgave door De Tijdstroom, Lochem 1973, met zeer uitvoerige toelichting door J.B. Kist).

<sup>5</sup> Het woord onbewapend duidt hier op de andere inzet van militairen, zowel qua optreden (vredesoperaties te midden van burgerbevolking) als qua middelen, waar het gaat om de zogenoemde niet-letale wapens.



**NBC ontsmetting** (Foto Directie Voorlichting MvD, P. Wiezoreck)

de directe omgeving groter dan ooit. Hierdoor worden aan politie en andere hulpdiensten eisen gesteld die eveneens vragen om aanpassingen in organisatie, optreden, training en uitrusting. Daardoor lijken zij soms op te schuiven in de richting van de organisatie en uitrusting van de krijgsmacht.

Een groot deel van de ervaring van de krijgsmacht en van het bij de krijgsmacht reeds beschikbare materieel zou in dat kader ook goed gebruikt kunnen worden door politie en hulpdiensten. Een dergelijk inzicht leidt ertoe dat samenwerken bij opleidingen en oefeningen, alsmede het gebruikmaken van elkaars faciliteiten en diensten, gemakkelijker kan plaatsvinden dan voorheen. Een uitstekend voorbeeld van dit naar elkaar toegroeien, zie we bij de recent opgerichte Dienst Speciale Interventies, waarin specialisten van politie en krijgsmacht eendrachtig samenwerken en van elkaars kennis en ervaring gebruik maken.

Er doen zich derhalve uitstekende kansen voor om door standaardisatie of gebruikmaking van elkaars kennis en materieel de beschikbare technologie optimaal te gebruiken. Helaas blijkt dat in de praktijk, om vele uiteenlopende redenen, nog lang niet altijd gemakkelijk realiseerbaar. Dat is enerzijds een gevolg van historisch gegroeide verschillen, maar anderzijds ook van onbekendheid en onmacht.

Het wordt daarom hoog tijd dat alle betrokkenen zich realiseren dat dergelijke belemmeringen op zichzelf een bedreiging voor onze nationale veiligheid vormen. Als we oprecht willen dat het onderwerp nationale veiligheid de onverdeelde aandacht krijgt die het verdient, zal het nodige moeten gebeuren. Het openingsscenario is immers verre van denkbeeldig. Uitsluitend door gezamenlijk de uitdagingen op te pakken zullen de verschillende ministeries en uitvoerende diensten in staat zijn zich op een dergelijk scenario voor te bereiden.

### **Technologie en nationale veiligheid**

Zoals hiervoor al aangegeven, maakt de krijgsmacht van oudsher intensief gebruik van moderne technologie. Technologische superioriteit heeft aantoonbaar (tijdelijke) waarde gehad bij militaire operaties. Bij de andere spelers in het veiligheidsdomein is deze traditie minder geworteld. Mogelijk voor een deel als gevolg van de taakstelling, maar zeker ook als gevolg van beperkte budgetten voor materieel en de veel kleinere schaal waarop aansturing, beheer en inkoop van materieel plaatsvinden (tot nog niet zo lang geleden zelfs lokaal!). Hierdoor valt weliswaar belangstelling voor technologie te ontdekken bij deze spelers, maar ontbreekt tot nu toe de noodzakelijke kennis en ervaring om technologie grootschalig te gebruiken.

In haar beleidsdocument *Visie op veiligheid en technologie, Technologie is mensenwerk*<sup>6</sup> bevestigt het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) dat er tot op heden relatief weinig aandacht is besteed aan technologische mogelijkheden ter verhoging van de veiligheid. Om die lacune op te heffen wordt, onder andere vanuit het project Intensivering Civiel-Militaire Samenwerking<sup>7</sup> en door de start van het Vraaggestuurd Programma Veiligheid,<sup>8</sup> inmiddels hard gewerkt.

Hoewel BZK niet expliciet aangeeft hoe deze veronachtzaming van de technologiecomponent te verklaren valt, passeren wel een aantal knelpunten de revue:

- gebrek aan structureel en integraal inzicht in technologische ontwikkelingen, toepasbaar binnen het veiligheidsdomein;
- gebrek aan structureel onderzoek en ontwikkeling van dergelijke nieuwe technologie;
- versnipperde geldstromen voor onderzoek, ontwikkeling en verwerking;
- onvoldoende oog voor mogelijkheden om technologie met succes over de grenzen van sectoren heen in te zetten en daarmee synergie-effecten te realiseren (bijvoorbeeld door hergebruik van bestaande defensiekennis in het politiedomein).

Het mag duidelijk zijn dat dergelijke knelpunten serieus van aard zijn en niet eenvoudig zijn te verhelpen. Bovendien zijn ze deels structureel van aard en hangen zij samen met de staatkundige structuur van ons koninkrijk.

Vanuit het eerder geschetste model rondom maatschappelijke besluitvorming is duidelijk dat synchronisatie van informatie en acties bij de ver-

<sup>6</sup> Ministerie van BZK, Directie Strategie, voorjaar 2006.

<sup>7</sup> Ministerie van BZK, rapportage van 24 mei 2006 aan de Tweede Kamer.

<sup>8</sup> *Vraaggestuurd Programma Veiligheid*, Bert Don et al., TNO en BZK, 1 juli 2006.

schillende schakels essentieel is. Mocht dat lukken (en aan de goede wil ontbreekt het niet), dan kan de beschikbare technologie naar mijn mening al op korte termijn worden benut om bestaande knelpunten op te lossen. Overigens zal dan ook aandacht moeten worden besteed aan het samen benutten van nieuwe innovatiekansen. Onze nationale veiligheid kan daar haar voordeel mee doen!

Het is daarvoor noodzakelijk aandacht te geven aan structurele samenwerking, niet alleen op het terrein van technologie (onderzoek, ontwikkeling, testen/keuren en verwerven), maar ook in het gezamenlijk formuleren van beleid, het samen opleiden en trainen en een voortdurend zoeken naar complementariteit. De nauwere samenwerking tussen onder meer de ministeries van BZK en Defensie, het succes van bijvoorbeeld de Dienst Speciale Interventies en een voortdurende dialoog tussen alle betrokken spelers zijn randvoorwaarden voor het snel en effectief kunnen implementeren van oplossingen. Naast technologische innovaties zullen echter ook procesmatige en organisatorische vernieuwingen nodig zijn om uiteindelijk dit resultaat te kunnen behalen.

### **Technologie als oplossing voor al uw problemen...**

Dat gezegd zijnde, is nadere aandacht nodig voor de wijze waarop technologie zou kunnen bijdragen aan het oplossen van veiligheidsproblemen. Dat zijn de relevante beleidsmakers zich gelukkig bewust. Als gevolg van haar eerdere beleidskeuze om de aandacht voor en de mogelijk impact van technologie te vergroten, heeft BZK daarom aan TNO gevraagd om zogenoemde technologieverkenningen uit te voeren. Recent is het eerste resultaat daarvan verschenen in het rapport 'Technologieverkenningen Maat-

schappelijke Veiligheid 2006'.<sup>9</sup> Dit rapport kent dezelfde opzet als de technologieverkenningen die voor het ministerie van Defensie worden uitgevoerd.

Zonder dit omvangrijke rapport in zijn geheel te willen bespreken, lijkt het mij goed om met een citaat aan te geven wat het rapport beoogt.

'De Technologieverkenningen Maatschappelijke Veiligheid bieden gestructureerde en beargumenteerde inschattingen van (toekomstige) technologische ontwikkelingen op specifieke (taak)gebieden en de verwachte gevolgen daarvan voor taakorganisaties en individuele taakuitvoerders op het gebied van Maatschappelijke Veiligheid'.<sup>10</sup>

#### **Trends**

Naast aandacht voor de feitelijke technologische ontwikkelingen staat het rapport ook uitgebreid stil bij trends in de veiligheidssituatie en analyseert het ontwikkelingen bij de betrokken taakorganisaties. Het rapport behandelt achtereenvolgens de verschillende taakaspecten die bij nationale veiligheid een rol spelen. Deze worden in een zevental hoofdstukken gekoppeld aan specifieke

technologische ontwikkelingen. De hoofdstukken bieden een structuur die onder meer laat zien op welke relevante deelterreinen/taakgebieden technologie kan worden ingezet:

- Inspectie en monitoring
- Informatievoorziening en distributie
- Informatieanalyse
- Organisatie en voorbereiding
- Bescherming
- Middelen
- Gedrag

Voor al deze taakgebieden gaat het rapport na welke karakteristieken en aandachtsgebieden er zijn en wat de samenhang is met de andere taakgebieden. Vervolgens worden relevante technologische ontwikkelingen behandeld, die bruikbaar zijn voor het taakgebied als geheel c.q. voor een specifiek deelgebied daarbinnen.

Een praktisch voorbeeld: bij het taakgebied inspectie en monitoring speelt waarneming een belangrijke rol. Daarbinnen kunnen specifieke waarnemingssystemen een waardevolle bijdrage leveren, zoals een combinatie van passieve millimetergolf-waarneming en CO<sub>2</sub> metingen, die de ongewenste aanwezigheid van personen in het laadgedeelte van vrachtwagens



<sup>9</sup> TNO Rapport DV1 2005 C136, Kernkamp, A.C. et al., Den Haag, juli 2006.

<sup>10</sup> Ibidem, managementuittreksel, pagina 3.

kunnen helpen vaststellen. De uitdaging bij dit specifieke voorbeeld is overigens de kwaliteit van de beelden en de juiste inbedding in een praktijkomgeving, zoals bijvoorbeeld in geval van het gebruik van deze technologie in een vrachtterminal in de Rotterdamse haven.

Op deze wijze passeert een groot aantal technologieën de revue, in verschillende stadia van praktische bruikbaarheid. De beleidsmakers en operationele gebruikers beschikken daardoor over een gestructureerd inzicht in mogelijkheden en beperkingen van technologie. Dat inzicht kan hen behulpzaam zijn bij het maken van keuzes en toont tevens de samenhang tussen de technologie en de andere schakels in de maatschappelijke besluitvorming. Juist daardoor zullen ook anderen hierbij betrokken moeten worden: het politieke niveau, andere spelers in het kennisdomein (onder meer de universiteiten), industriële spelers en ook de toekomstige gebruikers. En daarbij geldt opnieuw dat de oplossing zelden uitsluitend door technologische innovatie kan worden bereikt. Aanpassingen in processen, procedures en organisatievorm zullen nodig zijn om de gewenste effecten te bereiken.

Het rapport is een bijzonder bruikbaar uitgangspunt voor een praktische vertaling van technologische mogelijkheden naar gewenste toepassingen. Bij de hierna volgende schets van technologie, toepasbaar op het openingsscenario van deze Militaire Spectator, heb ik daarom veelvuldig van het rapport en de onderliggende bronnen gebruik gemaakt.

### **Toepasbare technologie voor het geschetste scenario**

Uit het geschetste scenario komt een aantal specifieke vragen c.q. knelpunten naar voren, die mij uitdagen om daarbij passende oplossingen vanuit de technologie te schetsen. Ik kies enkele van deze vragen uit, maar besef dat er nog veel meer van dergelijke

vraagstukken in het scenario besloten liggen. Dat op zichzelf toont al aan hoe nuttig het is om goed doordacht het complexe vraagstuk van nationale veiligheid te benaderen. De intensieve samenwerking tussen onder meer de ministeries van BZK en Defensie is daarbij randvoorwaarde. Ik veronderstel gemakshalve dat de factoren ‘politieke wil’ en ‘economische productiemogelijkheden’ uitsluitend positief zullen uitwerken in de geschetste voorbeelden.

Om te kunnen beoordelen of een technologische innovatie behulpzaam kan zijn voor het vergroten van de nationale veiligheid, zal ik ter illustratie wat dieper ingaan op een drietal deelaspecten uit het gegeven scenario:

- tijdig beschikken over inlichtingen rondom de ‘andersglobalisten’;
- bescherming van hulpdiensten bij grootschalige branden met mogelijk catastrofale effecten;
- effectieve inzet van overheidsdiensten bij dreigende gewelddadigheden in achterstandswijken.

#### **Tijdige inlichtingen**

Het ‘andersglobalisme’ is een reeds bekende beweging – de inlichtingendiensten zijn op de hoogte van hun

motieven en publieke uitingen. Toch komt de feitelijke inzet van wapens (RPG’s) in de Rotterdamse haven als een verrassing. Ook de groepering ‘Empire’ is tot dan toe onbekend gebleven. Kennelijk waren de inlichtingen- en veiligheidsdiensten niet op de hoogte van het bezit van dergelijke wapens door andersglobalisten en had men evenmin waargenomen dat bewapende lieden zich in het gebied van de haven ophielden. Gelet op het vrij beperkte bereik, moeten deze leden van ‘Empire’ zich vrij dicht (minder dan 150 meter afstand) bij zowel de supertanker als bij de opslagplaatsen van Shell Chemie hebben bevonden.

Naar de oorzaken van het ontbreken van deze informatie kan alleen maar worden gegist. Wel is op te merken dat er vrij veel technologische mogelijkheden zijn om de aanwezigheid van personen en eventuele wapens of explosieven in een bepaald gebied vast te stellen.

Dat zou kunnen door bijvoorbeeld specifieke toegangscontrole uit te voeren – maar dat is in een uitgestrekt gebied met vele toegangsmogelijkheden via land en zee als de Rotterdamse haven een bijzonder kostbare operatie.

### *TUJDIGE EN ACCURATE INLICHTINGEN NOODZAKELIJK*



Een meer effectieve benadering vormt permanente waarneming vanuit de lucht. Dat kan met behulp van onbemande vliegtuigen, met aan boord een scala aan hoogwaardige sensoren. Een combinatie van bijvoorbeeld radar, infra-rood en een reguliere daglicht camera kan al de noodzakelijke basisinformatie voor gebiedsbewaking aanleveren. Op die wijze zouden verdachte (dat wil zeggen: niet vooraf bekende) verplaatsingen van personen en/of goederen permanent kunnen worden gevolgd.

De havenautoriteiten van Rotterdam beschikken momenteel al over een centrale meldkamer van waaruit zij alle scheepsbewegingen in hun gebied van verantwoordelijkheid kunnen volgen. Daarop zal de informatie uit het hiervoor geschetste waarnemingssysteem naadloos moeten aansluiten, om de introductie te vereenvoudigen en acceptatie door de betrokken partijen te vergroten.

Er zitten nog wel wat uitdagingen vast aan deze toepassing van technologie: de sensorinformatie zal zodanig gefuseerd moeten worden, dat het voor een menselijke of een geautomatiseerde gegevensverwerker relevante beelden oplevert. Bovendien zal de enorme hoeveelheid gegevens die beschikbaar komt zowel getransporteerd, bewerkt als opgeslagen moeten worden. Voor het vaststellen van de afwijkende zaken zal bovendien erg veel (gevalideerde) kennis over de normale bewegingen van personen en goederen bekend moeten zijn. Alleen maar beschikken over de informatie is daarbij niet voldoende: bij het constateren van afwijkingen moet adequate opvolging (inspectie ter plaatse, ingrijpen indien het inderdaad om onbevoegde aanwezigheid gaat etcetera) binnen afzienbare tijd plaats vinden.

Ook zal de informatie zodanig deelbaar moeten zijn dat alle betrokken instanties en bedrijven tijdig geïnformeerd en gealarmeerd kunnen worden. Het besluit tot bijvoorbeeld evacuatie van het aanwezige personeel en inzet van specifieke hulpdiensten zal

tijdig moeten worden genomen, waarbij het besef van de vaak grote economische schade (zowel ingeval van een onnodige evacuatie als bij een daadwerkelijke aanslag) waarschijnlijk als een zwaard van Damocles boven de besluitvormers hangt.

Een extra complicatie vormt de afweziging wie in welk stadium over welke informatie moet kunnen beschikken. Een volledig open informatiesysteem voor alle betrokkenen zal niet werken, maar het niet delen van specifieke informatie is even ongewenst. Mogelijkheden om elkaars communicatie- en informatiesystemen te benaderen c.q. te gebruiken zullen wellicht vergezeld moeten gaan van een protocol om (gegeven de situatie) snel toestemming voor inzage/gebruik te kunnen verlenen.

Resumerend: voor het tijdig beschikken over inlichtingen zijn diverse sensor- en informatie-oplossingen denkbaar en beschikbaar. Of deze technologie ook daadwerkelijk wordt ingezet is deels een kwestie van tijd (verdere ontwikkeling en implementatie), maar ook van politieke wil en beschikbaarheid van middelen.

### **Bescherming van hulpdiensten**

Het scenario beschrijft hoe door de onverschrokken inzet van de brandweer en andere hulpdiensten de gevolgen van de aanslagen op de supertanker en de daaropvolgende brand bij Shell Chemie nog enigszins beperkt blijven. Een prachtig resultaat, maar aan welke gevaren zijn zowel de hulpverleners als de aanwezige burgerbevolking blootgesteld? Had technologie er voor kunnen zorgen dat dit met minder risico had kunnen gebeuren?

Gegeven de huidige technologische stand van zaken durf ik te beweren dat er inderdaad heel veel mogelijkheden tot bescherming zijn. Hoewel de brandweer ter plaatse vaak over adequate beschermende kleding en zuurstofmaskers beschikt, gaat dat niet op voor de overige hulpdiensten. Zelden beschikken zij over dergelijke uitrus-

ting, waardoor zij in het rampgebied nauwelijks beschermd zijn en bloot kunnen worden gesteld aan zowel giftige stoffen als aan de directe effecten van de brand zelf (rook, hitte).

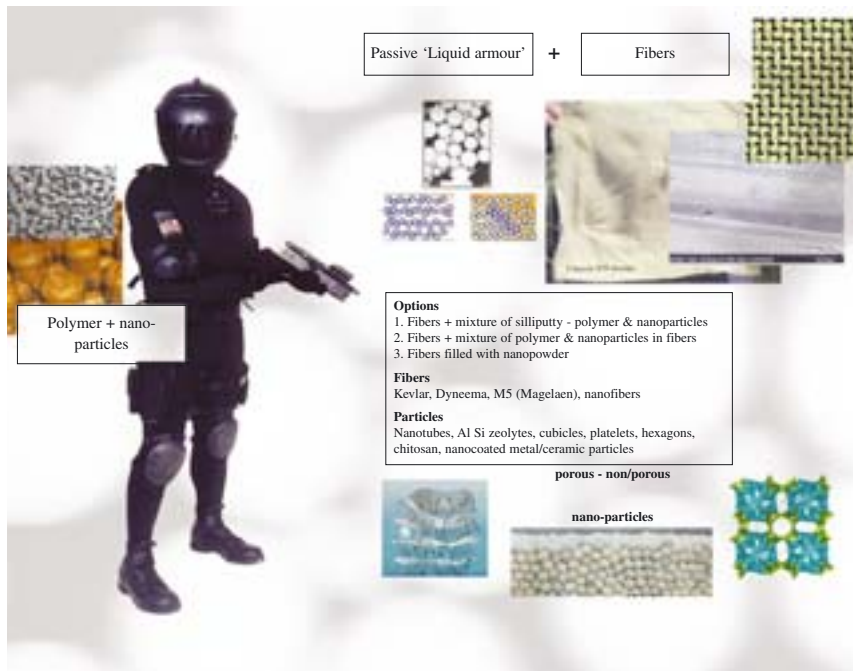
Ook kan (bijvoorbeeld als gevolg van niet tijdige evacuatie) het in de bedrijven c.q. aan boord van de schepen aanwezige personeel slachtoffer worden van een gebrek aan beschermende kleding en uitrusting. Omdat dergelijke middelen reeds bestaan, zal het een kwestie zijn van beschikbaarstelling en opleiding (bijvoorbeeld van ambulancepersoneel en politie) om adequaat met deze middelen te kunnen omgaan.

De ontwikkeling van hoogwaardige beschermende kleding en bijvoorbeeld geïntegreerde hoofdbescherming met communicatieapparatuur en ademhalingsbescherming, zorgt op termijn voor een verbetering van de persoonlijke bescherming. Nieuwe (lichte) vezels, met ontsmettende en brandwerende eigenschappen, zonnodig in combinatie met ballistische bescherming, maken de invoering van nog betere kleding in de nabije toekomst mogelijk.

Binnen de krijgsmacht is er al geruime tijd extra aandacht voor het 'systeem soldaat'. In het kader van het *Soldier Modernization Program* is daarbij veel energie gestoken in kennisoverdracht aan andere hulpverleners. Zo hebben onder andere de politie en de brandweer ruimschoots kennis kunnen nemen van dit militaire initiatief. De belangstelling vanuit onder andere BZK is groot, zodat ik verwacht dat de beschikbare kennis zal worden overgenomen en dat er mogelijk zelfs op onderdelen zal worden samengewerkt bij verdere ontwikkeling en aanschaf.

De grote aandacht voor nanotechnologie<sup>11</sup> brengt met zich mee dat deze

<sup>11</sup> Nanotechnologie beweegt zich op het snijvlak van natuur- en scheikunde en beoogt optimaal gebruik te maken van de chemische en fysische eigenschappen van kleine deeltjes, zodanig dat totaal nieuwe toepassingsmogelijkheden ontstaan.



**Afb. 2: Toepassing van nanotechnologie in toekomstige beschermende kleding**

kennis ook op het gebied van beschermende kleding en uitrusting kan worden toegepast. Verbetering van de eigenschappen van specifieke vezels zou er bijvoorbeeld voor kunnen zorgen dat beschermende BC-kleding zelfontsmettend wordt, minder kwetsbaar is voor beschadigingen, thermische protectie biedt en zodanig licht is dat het gebruikerscomfort is gegarandeerd. De *artist's impression* in afbeelding 2 biedt een blik op dergelijke ontwikkelingen.

De voornaamste hinderpaal op het gebied van effectievere persoonlijke bescherming bestaat vermoedelijk uit de beschikbare financiële middelen. Zelf ontwikkelen is immers kostbaar en bovendien is er een veel grotere groep gebruikers dan alleen maar het personeel van de huidige specialistische diensten.

Resumerend: reeds beschikbare beschermende kleding en uitrusting kan een waardevolle bijdrage leveren aan de persoonlijke bescherming van hulpverleners. Dat zal overigens forse financiële investeringen vergen.

### Effectieve inzet in achterstandswijken

In de context van het geschetste scenario is het begrijpelijk dat de achterstandswijken in diverse grote steden veranderen in *no go areas*. Naast het feit dat dit op zichzelf al ongewenst is, zorgt het voor een extra interne bedreiging van de nationale veiligheid. Ook hier kan technologie tot op zekere hoogte bijdragen aan oplossingen.

Wat betreft repressie (in dit scenario is er immers al sprake van *no go areas*) kan dat bijvoorbeeld door toepassing van niet-letale wapens en adequate persoonlijke beschermingsmiddelen. Daarmee kan de politie toch effectief optreden in deze gebieden. Immers, grotere groepen opstandige burgers kunnen worden beteugeld, zonder dat grootschalig geweld hoeft te worden toegepast. Het vereist wel een nadrukkelijke politieke bereidheid om op te treden tegen de eigen burgerbevolking, maar ook hier biedt de technologie een perspectief, omdat het met niet-letale middelen kan worden gedaan.

Hoewel bepaalde niet-letale wapens al langere tijd in gebruik zijn (denk aan traangas, pepperspray en de wapenstok) zijn er technologische ontwikkelingen die voor uitbreiding van dit arsenaal kunnen dienen. Voorbeelden daarvan zijn diverse soorten niet-letale munitie (rubberkogels die wel kunnen uitschakelen, maar in principe niet dodelijk zijn), thermische microgolfstraling (levert een onaangename verhitting van de huid op, maar hoeft niet tot blijvend letsel te leiden) en akoestische wapens (extreme knal of geluidsgolven die zodanig hinderlijk zijn dat mensen onwel worden). Adequate bescherming van diegenen die dergelijke wapens inzetten is mogelijk, zodat een eenzijdig effect kan worden bereikt.

Voor inzicht in de lokale situatie en een goed overzicht van de ontwikkelingen zal in dit deelspect van het scenario opnieuw behoefte zijn aan actuele *'situational awareness'* die tussen alle betrokken spelers naadloos kan worden gedeeld. Specifieke waarnemingssystemen, een toegesneden informatiesysteem, beveiliging, maar ook toegankelijke informatiebronnen (informanten) zijn een noodzakelijke voorwaarde. Hoewel op dit terrein grote ontwikkelingen plaatsvinden, zijn mij momenteel geen systemen bekend die nu reeds operationeel inzetbaar zouden zijn in een dergelijk scenario.

Deelsystemen zijn echter wel beschikbaar, zodat ik er alle vertrouwen in heb dat hier op korte termijn doorbraken kunnen worden bereikt. Het grootste probleem daarbij betreft natuurlijk de begrijpelijke discussie in hoeverre de overheid in de persoonlijke levenssfeer van haar burgers mag ingrijpen. Hoewel de samenleving in toenemende mate begrip lijkt te tonen voor de eisen die nationale veiligheid stelt aan het beperken van de privacy, is de politieke bereidheid om vergaande maatregelen door te voeren nog beperkt. Het beheersbaar houden van dergelijke informatiestromen en het ver weg blijven van totalitaire systemen à la het voormalige Oost-Duitsland, zijn daarom bijzondere uit-

dagingen rond deze technologische ontwikkelingen.

Resumerend: optreden tegen de eigen burgerbevolking kent vele complexe aspecten. Effectief gebruik van niet-letale wapens is echter vanuit beschikbare technologie mogelijk. Ook een adequaat informatiesysteem lijkt op redelijk korte termijn te implementeren. Met name politieke (en daarmee samenhangende juridische) afwegingen vormen een mogelijke belemmering voor de introductie van de geschetste oplossingen.

### Een overkoepelende aanpak

Een meer integrale benadering van deze technologische mogelijkheden biedt wellicht het begrip netwerkend optreden, zoals het ministerie van Defensie dat hanteert. In het internationale spraakgebruik beter bekend als 'network enabled capabilities' beoogt deze aanpak '(...) het verbeteren van de samenhang en de snelheid in het optreden..., zodat een beslissend voordeel kan worden bereikt ten opzichte van de tegenstanders. Hierbij wordt, door het optimaal gebruik van informatie, gestreefd naar een zo volledig mogelijke geïntegreerde en gecoördineerde inzet van alle beschikbare middelen'.<sup>12</sup>

Voor deze, op zich overigens niet nieuwe, militaire benadering van een steeds complexere omgeving, ontstaat steeds meer belangstelling buiten de krijgsmacht. Gegeven de gewenste samenwerking tussen uiteenlopende partijen, lijkt het mij de meest veelbelovende overkoepelende aanpak voor alle zaken die spelen rondom nationale veiligheid. Zowel nationaal als internationaal (rampen en aanslagen laten zich nu eenmaal niet door landsgrenzen tegenhouden) kan deze benadering zorgen voor een slagvaardige overheid, die zowel vooraf, tijdens als na een incident goed geïnformeerd tot een optimale inzet van middelen kan komen.

<sup>12</sup> Ministerie van Defensie, Defensiestaf, Brochure *netwerkend optreden*.

Nog enkele kanttekeningen bij het gegeven scenario: hoe ernstig de gevolgen ook zijn van de aaneenschakeling van gebeurtenissen die ons wordt geschetst, het kan allemaal nog veel erger. De laatste jaren doet immers het begrip catastrofaal terrorisme steeds meer opgang. Kleine groepen lijken een maximaal vernietigings-effect te willen bereiken. Slachtoffers aan eigen zijde worden daarbij niet uit de weg gegaan. In die context is het bewust gebruik van chemische, biologische, radiologische en nucleaire (CBRN) middelen niet uit te sluiten.

Niet alleen de omvang van de ramp in het gegeven scenario zou daardoor enorm kunnen toenemen, maar ook de complexiteit van de wijze waarop repressie en hulpverlening vorm moe-

te stellen dat technologie daadwerkelijk kan bijdragen aan het creëren en handhaven van nationale veiligheid. Het is daarom zeker niet te laat om gebruik te maken van beschikbare kennis en kunde.

Wel laat het scenario zien dat de inzet van relatief eenvoudige middelen door extreme groeperingen enorme consequenties kan hebben. Een zekere haast is dus geboden. Een impuls zal nodig zijn om op korte termijn gebruik te kunnen maken van de reeds aanwezige mogelijkheden. Het is echter geenszins een kwestie van eenvoudigweg invoeren van nieuwe systemen, methoden of technieken. Een bewuste keuze van de meest veelbelovende oplossingen, die passen bij een politiek gedragen taak, aansluiten op economische belangen en acceptabel



ten krijgen. De volledige en nauwe samenwerking tussen alle betrokken instanties zal in een dergelijk scenario doorslaggevend zijn. Dat de minister van Defensie dan pas na ruim 48 uur de Commandant der Strijdkrachten hierbij inschakelt lijkt mij persoonlijk ondenkbaar.

### Conclusie

Tot op heden wordt technologie nog onvoldoende benut in het domein van de nationale veiligheid. Ik durf echter

zijn voor de gebruikers, is een *conditio sine qua non*.

Als daarbij een netwerk-georiënteerde aanpak wordt gehanteerd, kan de overheid zich optimaal voorbereiden op de bedreigingen van onze nationale veiligheid.

Technologische innovaties staan daarbij niet op zichzelf – een nauwe samenhang met procesmatige en organisatorische innovaties is een gegeven waaraan we ons niet kunnen en mogen onttrekken.