Technologie en misdaad

Kansen en bedreigingen van technologie bij de beheersing van criminaliteit

Commissie Criminaliteit en Technologie
Den Haag, januari 2005

Voorwoord

Blik op de weg, verstand op nul en de verkeersveiligheid is er nog bij gebaat ook. Dat is geen schone droom, want dankzij de *Advanced Driver Assistance* kunnen voertuigen hun bestuurder behoeden voor fatale fouten in het verkeer. Radarsensoren meten de afstand tot voor- en achterliggers. Optische sensoren geven de gesteldheid van het wegdek door aan het ABS-remsysteem. Een camera in de achteruitkijkspiegel controleert de frequentie waarmee de bestuurder met zijn ogen knippert en slaat alarm wanneer hij onvoldoende activiteit registreert. Een actief gaspedaal geeft lichte tegendruk bij het overschrijden van de maximumsnelheid. Sensoren waarschuwen voor het verkeer naast en vlak achter de auto. Wanneer de wagen uit koers dreigt te raken, geeft een slim stuur tegendruk. En mocht dat allemaal onvoldoende zijn om een ongeluk te voorkomen, dan waarschuwt de airbag de noodhulpdiensten. Volgens het Zweedse ministerie van Verkeer en Waterstaat zou alleen al de automatische snelheidsaanpasser het aantal verkeersslachtoffers met twintig tot dertig procent doen dalen.

Het voorbeeld van de *Advanced Driver Assistance* illustreert hoezeer de technologie de zwakke schakels in het functioneren van de mens kan compenseren. Apparaten maken – in principe althans – geen fouten. Ze zijn weliswaar 'dom', ze kunnen zelf niet denken, maar zijn wel beter dan de mens in staat werkzaamheden snel en nauwkeurig te verrichten, bovenmenselijk zware arbeid op zich te nemen en prestaties te leveren die het menselijke vermogen te boven gaan. Zo beschouwd, mag het geen wonder heten dat de mens in de loop der eeuwen naarstig heeft gespeurd naar instrumenten die zijn eigen tekortkomingen konden compenseren. Op tal van terreinen is de technologie thans niet meer weg te denken uit onze samenleving. Denk bijvoorbeeld aan de gezondheidszorg, de ruimtevaart, defensie, de informatievoorziening, de amusementsindustrie, de huishoudelijke markt en het vervoer. Technologische ontwikkelingen volgen elkaar in hoog tempo op. De drijfveer is niet louter economisch gewin; technologie wordt ook ontwikkeld ter bevordering van het algemeen nut en welvaren.

In dat licht bezien mag het enige bevreemding wekken dat er bij Justitie geen systematische aandacht is voor de mogelijkheden van de technologie. Immers, de moderne technologie kan in alle schakels van de veiligheidsketen een belangrijk hulpmiddel zijn bij het beheersen van de criminaliteit. Dat geldt zowel voor het toezicht op en de handhaving van de openbare orde en het tegenhouden en voorkomen van criminaliteit, als voor de opsporing van plegers van strafbare feiten, de vervolging en berechting van daders en de uitvoering van strafrechtelijke sancties. Uiteraard is Justitie niet geheel blind voor de mogelijkheden van de technologie. In elke schakel van de keten zijn wel voorbeelden te noemen van technologieën die ten dienste staan van de criminaliteitsbeheersing. Zo worden camera's ingezet om de openbare orde te handhaven tijdens voetbalwedstrijden en registeren flitspalen langs de weg snelheidsovertredingen. Voorbeelden van het voorkomen en tegenhouden van criminaliteit zijn respectievelijk de sinds 1998 verplichte startonderbreker die diefstal van voertuigen voorkomt, en de gsm-bom die een onbekommerd gebruik van gestolen mobiele telefoons verhindert. Zo ook staan bijvoorbeeld DNA-technieken de opsporing ten dienste, verlopen de vervolging en berechting efficiënter via videoverhoren en behoort elektronisch toezicht sinds enkele jaren tot de sanctiemodaliteiten.

Deze voorbeelden maken duidelijk dat de technologie een toegevoegde waarde kan hebben bij het beheersen van de criminaliteit. Echter, van een regelmatige en systematische zoektocht naar een technologisch antwoord op de criminaliteitsproblemen is geen sprake. Dat is jammer, want voor wie zich verdiept in de wereld van de technologie, rijst al snel een wereld van ongekende en onverkende mogelijkheden. Menig crimineel is, sneller dan Justitie, tot dat inzicht gekomen en dat is nog een extra reden waarom Justitie zich in de wereld van de technologie zou moeten verdiepen.

Maar de wil tot een koerswijziging is er. Dat Justitie bereid is meer structurele aandacht te besteden aan de mogelijkheden van de technologie, bewijst de instelling van de commissie Criminaliteit en Technologie. Deze commissie heeft zich het afgelopen jaar verdiept in een breed scala aan technologische vindingen die behulpzaam kunnen zijn bij het voorkomen en bestrijden van de criminaliteit. Ze heeft zich bovendien gebogen over de risico's, randvoorwaarden en barrières die hiermee verbonden zijn. De uitkomst van deze studie, die in lijn is met vergelijkbare exercities in onder meer de Verenigde Staten, Groot-Brittannië en Australië, stemt ons hoopvol. Niet dat we nu meteen een technologische revolutie verwachten in de wereld van de criminaliteitsbeheersing; daarvoor zijn de barrières die overbrugd moeten worden wellicht op de korte termijn te groot. Maar met de presentatie van dit advies willen we wel de hoop uitspreken dat de commissie de motor moge zijn, of – zo u wenst – de *Advanced Driver Assistance*, die Justitie op de wat langere termijn mag leiden naar een veiliger samenleving dankzij de inzet van de technologie.

Pieter Winsemius
Voorzitter van de commissie Criminaliteit en Technologie

Inhoud

Samenvatting III

1. Inleiding 1

2. Criminaliteit en technologie 2
2.1 Criminaliteit en misdaadbestrijding 2
2.2 Technologie en samenleving 2
2.3 Technologie en misdaadbestrijding 3

3. Veelbelovende terreinen 5
3.1 Technologische ontwikkelingen 5
3.1.1 Ernstige vormen van criminaliteit 5
3.1.2 Veelvoorkomende criminaliteit en overlast 6
3.1.3 Vereenvoudigen van routineklussen 7
3.1.4 Verhoging van het opheldering spercentage 8
3.2 Technologie van de toekomst 9
3.2.1 Veelvoorkomende criminaliteit: inbraak in woningen en bedrijven 9
3.2.2 Vereenvoudigen van routineklussen: controle op wapenbezit 10
3.2.3 Verhoging van het opheldering spercentage: toezicht en controle in de openbare ruimte 10
3.2.4 Verhoging van het opheldering spercentage: identiteitsfraude 11
3.3 Meest veelbelovend: patroon- en gezichtsherkenning 11

4. Criminele bedreigingen 12
4.1 Nieuwe kansen voor criminelen 12
4.2 Toekomstige trends en ontwikkelingen 12
4.3 Wapenwedloop met politie en justitie 13

5. Barrières voor politie en justitie 15
5.1 Culturele barrières 15
5.2 Organisatorische barrières 16
5.3 Technische barrières 16
5.4 Juridische barrières 16
5.5 Ethische barrières 17

6. Aanbevelingen 18

Bijlagen:
a. Samenstelling van de commissie Criminaliteit en Technologie 21
b. Korte beschrijving van relevantie technologieën voor criminaliteitsbeheersing 22
c. Geraadpleegde bronnen 27

Samenvatting

Opdracht
De commissie Criminaliteit en Technologie is in 2002 ingesteld door de minister van Justitie met de opdracht hem te adviseren over de mogelijkheden die de technologie kan bieden bij het voorkomen en bestrijden van de criminaliteit en de wijze waarop Justitie kan zorgdragen voor een structurele inbedding van de technologie in het denken over criminaliteitsbeheersing. Daarnaast dient de commissie aandacht te besteden aan technologische ontwikkelingen die kunnen leiden tot het ontstaan van nieuwe vormen van criminaliteit. Aanleiding voor het instellen van de commissie vormt de interdepartementale nota *Criminaliteitsbeheersing: Investeren in een zichtbare overheid* (juni 2001), waarin gesignaleerd wordt dat nieuwe ontwikkelingen in de technologie zowel kansen als bedreigingen voor het werk van justitie en politie kunnen inhouden.

Technologie en misdaadbestrijding
De afgelopen decennia is de criminaliteit in Nederland sterk toegenomen. De opsporing en in het verlengde daarvan de vervolging en berechting hebben geen gelijke tred gehouden met deze ontwikkeling. Slechts een klein deel van het totale aantal delicten wordt door de politie opgehelderd en mondt uit in strafrechtelijke vervolging. Zowel de repressieve aanpak als de preventie van criminaliteit behoeven dan ook verbetering. Het antwoord van politie en justitie zal mede gezocht moeten worden in de technologie, want dit is bij uitstek het terrein waar men excelleert in het vinden van innovatieve oplossingen. In tal van facetten van de moderne samenleving is dit tot uiting gekomen. Des te opmerkelijker is het dat politie en justitie geen systematische aandacht besteden aan de mogelijkheden van de technologie om criminaliteit te voorkomen en bestrijden. De traditionele alfa- en gamma-oriëntatie, onbekendheid met de wereld van de technologie en het ontbreken van een centraal punt van waaruit de overheid technologische ontwikkelingen ten gunste van de criminaliteitsbeheersing coördineert, stimuleert en faciliteert, zullen daar mede debet aan zijn.

De technologie biedt politie en justitie tal van mogelijkheden om de criminaliteit te helpen voorkomen en bestrijden. De keuze welke technologie ingezet dient te worden, is mede afhankelijk van het doel dat beoogd wordt en de mogelijkheden die de technologie in zich bergt. Vier aspecten zijn van invloed op deze keuze:

1. Sommige *delicten* zijn eenvoudiger met behulp van technologie te bestrijden of te voorkomen dan andere.
2. Op de ene *locatie* is de inzet van een bepaalde technologie meer passend dan op de andere locatie.
3. Bescherming van het *doelwit* vergt de inzet van andere technologieën dan maatregelen gericht op de *dader*.
4. De taken en doelen in de schakels van de *strafrechtketen* verschillen en daarmee de inzet van de technologie.

Bij de bepaling van de keuze welke technologie ingezet zal worden om de criminaliteitsproblematiek het hoofd te bieden, zullen al deze vier aspecten in onderlinge samenhang met elkaar in ogenschouw genomen moeten worden. De juiste keuze van de technologie kan vergemakkelijkt worden door te denken in termen van functies. Functies van de technologie die dienstig kunnen zijn voor de criminaliteitsbeheersing, zijn onder meer: waarnemen (camera's), identificeren (biometrie, gezichtsherkenning), alarmeren (alarmsystemen, patroonherkenning), gegevens koppelen en communiceren (computers). Behalve voor de selectie van bestaande technologieën biedt het denken in termen van functies tevens een handvat voor de speurtocht naar nieuwe technologische toepassingsmogelijkheden voor de beheersing van de criminaliteit.

Veelbelovende technologieën
De wereld van de technologie heeft zich nog lang niet uitgekristalliseerd. In hoeverre preventie en repressie hun voordeel kunnen doen met nieuwe ontwikkelingen, valt niet met zekerheid te voorspellen. Immers, nu al is er veel (in theorie) ontwikkeld, maar nog onbenut gebleven. Waar al zoveel op de plank ligt, is het verstandig eerst te inventariseren welke technologische mogelijkheden reeds zijn verkend, alvorens te bepalen op welke terreinen het wenselijk is nieuwe, veelbelovende ontwikkelingen in gang te zetten. In opdracht van de commissie is dan ook geïnventariseerd welke technologieën ten dienste kunnen staan van preventie en repressie. Deze inventarisatie was gericht op:

1. vier ernstige vormen van criminaliteit: terrorisme, georganiseerde criminaliteit en organisatiecriminaliteit, mensenhandel en –smokkel, drugshandel;
2. zeven vormen van veelvoorkomende criminaliteit en overlast: fietsdiefstal, inbraak en diefstal in woningen en bedrijven, wildplassen, vervuiling in woonwijken, vandalisme, mishandeling, diefstal met geweld;
3. drie aspecten van het vereenvoudigen van routineklussen bij de politie: alcoholcontrole, controle op wapenbezit, proces-verbaal opmaken;
4. drie criminaliteitsgebieden waar technologie onorthodoxe methoden zou kunnen bieden voor het verhogen van het opheldering spercentage: toezicht en controle in de openbare ruimte, milieuhandhaving, identiteitsfraude.

Uit de verkenning is naar voren gekomen dat niet op elk terrein winst te verwachten valt van een intensievere technologische benadering van de criminaliteitsproblematiek. Veelbelovend zijn wel technologische toepassingen op het terrein van inbraak in woningen en bedrijven, controle op wapenbezit, toezicht en controle in de openbare ruimte en identiteitsfraude. Het verdient aanbeveling op deze terreinen de technologische mogelijkheden nader te verkennen. Daarbij dienen bij de keuze van de meest geschikte technologie vier criteria richtinggevend te zijn:

- effectiviteit: is de technologie voldoende effectief
- efficiëntie: staan de investeringen in de ontwikkeling en toepassing in verhouding tot de verwachte baten
- eerlijkheid: stuit de technologie niet op ethische en juridische barrières
- haalbaarheid: stuit de technologie niet op maatschappelijke en/of politieke weerstanden

Voor elk van de vier geselecteerde veelbelovende terreinen – inbraak in woningen en bedrijven, controle op wapenbezit, toezicht en controle in de openbare ruimte en identiteitsfraude – zijn deze criteria toegepast op de diverse mogelijk inzetbare technologieën. Daarbij is een onderscheid gemaakt tussen preventie en repressie. Opvallend in deze nadere analyse is de rol die patroon- en gezichtsherkenning kan spelen als nieuwe methodiek om de criminaliteit te beheersen. Sterker nog, patroon- en gezichtsherkenning – hoewel in de kinderschoenen – is ook op tal van andere dan de onderzochte criminaliteitsterreinen zeer veelbelovend.

Criminele bedreigingen

De technologie biedt niet alleen politie en justitie kansen voor een betere uitoefening van hun taken, ze biedt ook criminelen meer gelegenheden en mogelijkheden tot het plegen van criminaliteit. Deze hangen ten eerste samen met bepaalde *algemene technologische ontwikkelingen*, waardoor criminelen hun werkterrein (internationaal) kunnen uitbreiden, zich eenvoudiger toegang kunnen verschaffen tot systemen, goederen en diensten, alsmede sneller en in grotere anonimiteit kunnen opereren zonder sporen na te laten en met het vooruitzicht op een grotere buit. Ten tweede doen zich ontwikkelingen op *productniveau* voor die in het voordeel van de crimineel werken, zoals de productie van luxe elektronische goederen, het aanbod van nieuwe bancaire diensten als de chipknip en pinpas en de fabricage van goederen met behulp van miniaturisatietechnieken, waardoor het formaat van de goederen handzamer en de goederen zelf diefstalgevoeliger worden.

Naar verwachting zullen met het voortschrijden van de technologische ontwikkelingen algemene trends als mondialisering, individualisering en informatisering van de samenleving op grotere schaal voorkomen, met alle consequenties van dien. Daarnaast zullen op productniveau zich nieuwe ontwikkelingen voordoen die van invloed zijn op het ontstaan van (nieuwe vormen van) criminaliteit. Omdat het in het bestek van dit advies ondoenlijk is alle mogelijke criminogene trends en ontwikkelingen op productniveau in kaart te brengen, wordt volstaan met te wijzen op de 'levenscyclus' die criminaliteitsgevoelige goederen, diensten en systemen doorlopen. Deze cyclus vangt aan met toenemende criminaliteit en mondt na verloop van tijd uit in afnemende kwetsbaarheid. Een voorbeeld vormen de pinautomaten. De eerste jaren na hun introductie lokten ze – vanwege hun relatieve onbekendheid en derhalve spaarzame gebruik door de burger – geen criminaliteit uit. Naarmate echter de populariteit van het 'flappentappen' toenam, steeg ook het aantal berovingen. Pas toen troffen de banken (technologische) maatregelen om de pinautomaten beter te beveiligen.

Criminaliteitsgevoelige producten onderscheiden zich doordat ze, zoals criminoloog Ron Clarke het noemt, 'CRAVED' zijn: Concealed, Removable, Available, Valuable, Enjoyable, Disposable. Over het algemeen geldt: hoe begeerlijker, aangenamer, waardevoller, makkelijker te vervoeren, breder verkrijgbaar een product is, des te groter de gevoeligheid voor criminaliteit is. Als bedrijven ertoe bewogen kunnen worden in een vroeg stadium aan deze criteria aandacht te besteden, zou criminaliteitspreventie meer standaard worden in plaats van – zoals thans het geval is – louter een van de mogelijke opties in de productontwikkeling.

Wapenwedloop

Behalve dat de technologie nieuwe mogelijkheden biedt voor het plegen van criminaliteit, dient er aandacht te zijn voor de tegenreactie die de inzet van nieuwe technologieën oproept bij het beheersen van de criminaliteit. De meest in het oog springende risico's zijn: verharding van de criminaliteit, verplaatsing van criminaliteit, toename van identiteitsfraude en meer diefstal langs elektronische weg. Iedere technologische maatregel roept vroeg of laat een weerwoord op van criminelen. In zekere zin is er sprake van een wapenwedloop. Het antwoord op de vraag wie deze wedloop zal winnen, hangt mede af van de beschikbare financiële spankracht. Een teken aan de wand is dat de echte 'professionele' crimineel het zich kan veroorloven de meest geavanceerde technologie in te schakelen, terwijl politie en justitie het niet alleen met minder ruime middelen moeten stellen, maar ook bepaalde ethische en juridische voorwaarden in acht moeten nemen.

Barrières
Een aantal knelpunten kan een optimale inzet van technologie in de weg staan. Deze zijn onderscheiden in culturele, organisatorische, technische, juridische en ethische barrières:

- *Culturele barrières* zijn het gebrek aan beleid, visie en coördinatie op centraal niveau en in het verlengde daarvan het ontbreken van voldoende financiële middelen voor het ontwikkelen en toepassen van nieuwe technologische oplossingen voor de beheersing van de criminaliteit. Beide kunnen voor een belangrijk deel verklaard worden door de kloof tussen de bèta-georiënteerde technologen en de alfa- en gamma-georiënteerde ambtenaren, die al in hun (juridische) opleiding worden bevestigd in hun 'natuurlijke onvermogen' om in de technologische hoek oplossingen te zoeken voor veiligheidsproblemen.
- Onder de *organisatorische barrières* vallen onvoldoende inbedding van de technologie in de organisatie en het achterwege blijven van een politiële of justitiële reactie op technologische informatie.
- Tot de *technische barrières* behoren tegenvallende prestaties van de technologie, de moeilijkheidsgraad in de bediening en een gebrek aan standaardisering.
- *Juridische barrières* worden gevormd door de wetgeving op het gebied van de privacy en het copyright voor nieuwe technologische uitvindingen.
- Mogelijke *ethische barrières* ten slotte zijn het risico van minder controle op de snelle technologische ontwikkelingen, weerstand tegen de aantasting van de integriteit van het menselijk lichaam en het ontstaan van een samenleving waar Big Brother de scepter zwaait.

Aanbevelingen
De commissie besluit haar advies met het formuleren van acht aanbevelingen voor een succesvolle inzet van de technologie, waarbij tevens beter het hoofd wordt geboden aan (mogelijke) knelpunten in de uitvoering:

1. *Houd technologische ontwikkelingen structureel in de gaten*: de commissie beveelt aan om elke twee jaar in kaart te brengen welke technologie beschikbaar is en waar nieuwe technologische kansen liggen. Voor deze analyse kan het beste de systematiek gevolgd worden die ook in het onderhavige rapport gehanteerd is.
2. *Wees de beste imitator en excelleer op één terrein als innovator*: mede vanwege het ontbreken van voldoende capaciteit, knowhow en financiële middelen moet ons land niet de pretentie hebben voor elk probleem zelf de technologische oplossing te willen ontwikkelen. De commissie beveelt dan ook aan zich vooral toe te leggen op informatie-uitwisseling en op het imiteren van veelbelovende en/of succesvolle buitenlandse technologische vindingen, onder meer via een 'veiligheidsattachee' op de Nederlandse ambassade in de VS. Om op technologisch vlak niet geheel achter te blijven en 'in ruil' voor waardevolle informatie van andere landen dient ons land zich op één terrein als innovator te onderscheiden.
3. *Excelleer de komende zes jaar in de ontwikkeling van gezichts- en patroonherkenning*: uit de verkenning van de technologische mogelijkheden bij de beheersing van de criminaliteit is de commissie gebleken dat gezichts- en patroonherkenning een zeer veelbelovende technologie is. Wil Nederland zijn (bescheiden) ambitie als innovator waarmaken, dan heeft het de meeste kans van slagen, indien het zich hierop de komende zes jaren concentreert.
4. *Prikkel industrie en wetenschap om te investeren in imitatie en innovatie*: ook wanneer de overheid haar rol bij de introductie van nieuwe technologieën zo veel mogelijk wil beperken tot imitatie en op een enkel terrein wil optreden als innovator, is ze voor de verwezenlijking van dit voornemen afhankelijk van de wetenschap en met name de industrie. Om hen te stimuleren tot medewerking oppert de commissie drie mogelijkheden: a. een fonds voor het implementeren van veelbelovende en/of succesvolle buitenlandse technologieën in het eigen productieproces; b. het afsluiten van convenanten tussen verzekeraars en branches die zich inspannen om hun producten, diensten en systemen te beveiligen tegen criminaliteit, in ruil voor een lagere verzekeringspremie; c. de uitreiking van een jaarlijkse onderscheiding voor bedrijven en wetenschappers die zich aantoonbaar verdienstelijk hebben gemaakt bij de introductie van *crime-proof* producten, diensten en systemen.
5. *Rapporteer elke vier jaar welke resultaten bereikt zijn*: de commissie beveelt aan om elke vier jaar verantwoording af te leggen over de bereikte resultaten.
6. *Besteed bij justitie stelselmatig aandacht aan technologie*: ter overbrugging van de kloof tussen de alfa- en gamma-georiënteerde justitieambtenaren en de bètawereld van de technologen doet de commissie vier aanbevelingen: a. belast een strategische (beleids)unit met de taak elke vier jaar aandacht te besteden aan technologie; b. stel bij de start van nieuw onderzoek door het Wetenschappelijk Onderzoek en Documentatie Centrum standaard de mogelijkheden van de technologie aan de orde; c. organiseer discussiebijeenkomsten over technologie en criminaliteitsbeheersing; d. besteed regelmatig aandacht aan de communicatie rond technologie.
7. *Benoem een probleemeigenaar in de persoon van de directeur-generaal Rechtshandhaving*: de commissie omschrijft daarbij ook zijn takenpakket en wijze van verantwoording afleggen.
8. *Richt een netwerk Criminaliteit en Technologie op*: dit netwerk wordt minimaal één keer per twee jaar – voorafgaand aan het opstellen van de periodieke verkenning – geconsulteerd over de knelpunten bij de implementatie van nieuwe technologieën en de mogelijkheden deze te verhelpen.

1. Inleiding

"Nieuwe vormen van technologie (…) kunnen leiden tot nieuwe vormen van criminaliteit. Tegelijk kunnen zij kansen bieden om criminaliteit op innovatieve wijze te voorkomen en te bestrijden," schrijven de ministers van Justitie en Binnenlandse Zaken in hun gezamenlijke nota *Criminaliteitsbeheersing. Investeren in een zichtbare overheid* van juni 2001. De kansen en bedreigingen van de technologie dienen zowel op het terrein van de preventie als van de opsporing systematisch in kaart gebracht te worden. In de nota kondigt de minister van Justitie dan ook aan een commissie Criminaliteit en Technologie te zullen instellen.

Medio 2002 treedt de commissie Criminaliteit en Technologie onder voorzitterschap van P. Winsemius aan. Haar opdracht is drieledig:

1. De commissie adviseert de minister over de technologische mogelijkheden bij de beheersing van de criminaliteit. Daartoe presenteert ze een overzicht van exact-wetenschappelijke terreinen en praktische techn(olog)ische toepassingen waarmee mogelijk winst te behalen valt bij de preventie en opsporing van criminaliteit. De bestuurlijke en economische haalbaarheid van deze technologische mogelijkheden mag ze daarbij niet uit het oog verliezen.

2. De commissie adviseert de minister over de wijze waarop het departement kan zorgdragen voor een structurele inbedding van de technologie in het denken over criminaliteitsbeheersing. Immers, tot nu toe benadert de overheid criminaliteit vooral vanuit een juridische, economische en sociaal-wetenschappelijke invalshoek. Afgezien van beveiligingsmogelijkheden en ICT-toepassingen is er amper aandacht voor de technologie. De kloof die gaapt tussen bèta-wetenschappers en de alfa- en gamma-ambtenaren, zal overbrugd moeten worden.

3. De commissie besteedt aandacht aan de bedreigingen die van technologische ontwikkelingen uitgaan voor het plegen van (nieuwe vormen van) criminaliteit.

In de periode van november 2002 tot mei 2003 heeft de commissie zich over haar opdracht gebogen. Ze heeft een inventarisatie gemaakt van de ernst en omvang van de criminaliteitsproblematiek en het ontoereikende antwoord daarop van politie en justitie (hoofdstuk 2). Daarnaast is, met steun van het Instituut voor Maatschappelijke Innovatie (IMI), in kaart gebracht welke technologieën de criminaliteitsbeheersing ten dienste staan. Toepassingen in de sfeer van ICT en de beveiliging zijn, conform de opdracht aan de commissie, buiten beschouwing gelaten. Op basis van vier criteria – effectiviteit, efficiëntie, eerlijkheid en haalbaarheid – is vervolgens beoordeeld op welke criminaliteitsterreinen de meeste winst van de technologie te verwachten valt (hoofdstuk 3). Tegenover de kansen die de technologie biedt voor de preventie en bestrijding van criminaliteit, staan bedreigingen zoals het ontstaan van (nieuwe vormen) van criminaliteit (hoofdstuk 4) en culturele, organisatorische, technische, juridische en ethische barrières die een belemmering kunnen vormen voor de toepassing van technologie bij de beheersing van de criminaliteit (hoofdstuk 5). De commissie besluit haar advies met het formuleren van een aantal aanbevelingen voor een succesvolle inzet van de technologie, waarbij tevens beter het hoofd geboden wordt aan criminele bedreigingen en (mogelijke) knelpunten in de uitvoering (hoofdstuk 6).

2. Criminaliteit en technologie

2.1 Criminaliteit en misdaadbestrijding

De afgelopen decennia is de criminaliteit in Nederland fors toegenomen. Was er veertig jaar geleden nog sprake van 'slechts' 131.800 geregistreerde delicten, in 2002 is dit aantal toegenomen tot 1.422.800. De toename heeft zich vooral voorgedaan op het terrein van vermogensdelicten, geweldsdelicten, vernielingen en openbare-ordeproblemen. In feite weerspiegelt de ontwikkeling van de geregistreerde criminaliteit nog maar het topje van de ijsberg. Buiten beschouwing blijven immers delicten waarvan geen aangifte is gedaan en die evenmin door de politie opgespoord zijn. De slachtofferenquête van het CBS rept van 5.142.000 delicten in 2002 waarvan burgers het slachtoffer zijn geworden. Voeg hieraan toe de circa 3,5 miljoen delicten waaraan het Nederlandse bedrijfsleven jaarlijks ten prooi valt, zo'n 1,5 miljoen delicten waarvan de publieke sector het slachtoffer is en zo'n half miljoen delicten gepleegd tegen de 'vlottende bevolking' (toeristen), dan kom je op jaarbasis uit op ongeveer 10 miljoen misdrijven. Buiten beschouwing gelaten zijn dan nog de verborgen slachtoffers van criminaliteit, zoals mishandelde kinderen en vrouwen die bijvoorbeeld door loverboys of via mensenhandel tot prostitutie gedwongen zijn. Ook fraudedelicten als belastingfraude, uitkeringsfraude en EG-fraude zijn niet meegeteld.

De opsporing en in het verlengde daarvan de vervolging en berechting hebben geen gelijke tred gehouden met de sterke toename van de criminaliteit. Dit blijkt onder meer uit de gedaalde ophelderingspercentages, de achterstanden waarmee de rechtbanken kampen en de heenzendingen en het gebrek aan cellen die de executie regelmatig parten spelen. Het resultaat is dat slechts een heel klein percentage van de pakweg tien miljoen delicten per jaar door de politie opgehelderd wordt en uitmondt in een onvoorwaardelijke (gevangenis)straf. Zo beschouwd is het effect van de politiële en justitiële inspanningen op het beheersen van de criminaliteit nogal gering. Onvermijdelijk leidt deze constatering tot de conclusie dat de repressieve aanpak, maar ook de preventie van criminaliteit verbetering behoeven. De preventieve en repressieve aanpak dienen zich zodanig te ontwikkelen dat enerzijds de aanwas van nieuwe daders vermindert en de gelegenheid tot het plegen van delicten beperkt wordt en anderzijds daar waar criminaliteit de kop opsteekt, deze in een vroeg stadium tegengehouden wordt en een adequaat antwoord van politie en justitie krijgt, opdat misdaad minder lonend wordt.

De urgentie van een betere preventie en bestrijding van de criminaliteit wordt in de maatschappij inmiddels breed onderschreven. Blijkens het Permanent Onderzoek Leefsituatie (POLS) van het CBS deed de kentering zich voor in 1997, toen de problemen op het gebied van de criminaliteit en het optreden van justitie en politie op de eerste plaats belandden van de top-16 van belangrijkste problemen waarvoor de burgers het land gesteld zagen. Voor die tijd voerden steeds andere problemen – milieu, werkgelegenheid, minderheden, sociale voorzieningen – de ranglijst van nationaal ervaren problemen aan. De bezorgdheid van de samenleving over de toegenomen misdaad in het land is begrijpelijk. Criminaliteit tast de kwaliteit van het leven en de structuur van de samenleving aan. Behalve dat ze veel psychisch leed veroorzaakt, zijn er bovendien hoge kosten mee gemoeid.

2.2 Technologie en samenleving

Er zijn verschillende richtingen denkbaar waarlangs de preventieve en repressieve aanpak van de criminaliteit zich kan versterken. De oplossing kan gezocht worden in meer wetgeving, strengere straffen en een uitbreiding van het aantal rechters, officieren en 'blauw op straat'. Ook kunnen de inspanningen gericht zijn op een betere beveiliging van goederen en objecten, vroegtijdig ingrijpen in misdaadcarrières en het vergroten van het bewustzijn van burgers en bedrijven dat zij medeverantwoordelijk zijn voor het voorkomen van criminaliteit. Omdat op deze terreinen in de loop der jaren – terecht – reeds tal van initiatieven zijn ontplooid, zijn ze te beschouwen als traditionele oplossingen voor de misdaadproblematiek. Ze passen in de traditie om de criminaliteit vanuit een juridische, economische en sociaal-wetenschappelijke invalshoek te benaderen. Wie echter op zoek is naar nieuwe wegen om de misdaad te bestrijden, zal buiten deze gebaande paden dienen te treden. Onvermijdelijk zal deze zoektocht leiden naar de wereld van de technologie, want dit is bij uitstek het terrein waar men excelleert in het vinden van innovatieve oplossingen.

De razendsnelle ontwikkelingen in de technologie in de tweede helft van de twintigste eeuw hebben een onuitwisbaar stempel gedrukt op de westerse samenleving. Zowel in de inrichting van het openbare leven – denk alleen al aan het verkeer! – als in het arbeidsproces en het privé-leven van de burger heeft ze geleid tot ingrijpende veranderingen. In feite vormt de technologie de basis van drie majeure trends – individualisering , mondialisering en informatisering – die kenmerkend zijn voor de moderne maatschappij:

- *Individualisering*
  Dankzij de technologie kunnen burgers hun leven beter afstemmen op hun individuele behoeften. Aan de andere kant creëert de technologie meer dwarsverbanden. Er is dus zowel sprake van een grotere onderlinge afhankelijkheid als van een toegenomen onafhankelijkheid, die gepaard gaat met meer anonimiteit en een bijbehorende grotere aandacht voor privacyaspecten.

- *Mondialisering*
  De moderne mens is in veel opzichten een wereldburger geworden. Hij kan binnen een mum van tijd over de aardbol reizen. Letterlijk, maar ook figuurlijk: vanuit zijn luie stoel voor de televisie, luisterend naar de radio, via de telefoon of het internet. Grenzen worden probleemloos overschreden en veel producten en diensten op de wereldmarkt zijn, dankzij een snelle distributie, onder handbereik.

- *Informatisering*
  Moderne communicatiemiddelen maken informatie wereldwijd eenvoudig toegankelijk. Een, qua omvang, lomp medium als de computer krijgt duchtige concurrentie van kleinere informatiedragers, die de uitwisseling van gegevens naar verwachting zullen bevorderen.

De onmiskenbare invloed van de technologie op de inrichting van de moderne samenleving maakt het des te opmerkelijk dat politie en justitie geen systematische aandacht besteden aan de technologische mogelijkheden om criminaliteit te voorkomen en bestrijden. De traditionele oriëntatie op een juridische, economische en sociaal-wetenschappelijke benadering van de misdaadproblematiek zal daar debet aan zijn, maar ook de onbekendheid van de veelal alfa- en gamma-geschoolde politie- en justitiemedewerkers met de wereld van de technologie speelt een rol. Hier komt bij dat de criminaliteitsbeheersing een kleine en dus minder interessante afzetmarkt voor het bedrijfsleven vertegenwoordigt en de overheid vooralsnog niet in deze lacune voorziet door ontwikkelingen op dit terrein vanuit een centraal punt te coördineren, stimuleren en implementeren.

2.3 Technologie en misdaadbestrijding

Zoals de technologie de burger meer mogelijkheden biedt zijn leven vorm te geven en te beheersen (*selfcontrol*), zo ook biedt de technologie politie en justitie ideale mogelijkheden om *controle* uit te oefenen. Het spreekt vanzelf dat niet iedere technologie daartoe geëigend is. Alvorens te verkennen welke technologieën politie en justitie bij uitstek van dienst kunnen zijn, is het van belang een aantal algemene opmerkingen te plaatsen over de inzet van technologie bij de beheersing van de criminaliteit. Die keuze is immers mede afhankelijk van het doel dat beoogd wordt en de mogelijkheden die de technologie in zich bergt. Vier aspecten spelen daarbij een rol:

- *Type delict*
  Traditiegetrouw worden delicten in zeven categorieën gegroepeerd. De technologische mogelijkheden voor preventie en repressie zijn in de ene categorie groter dan in de andere. Vermogensdelicten zijn bijvoorbeeld makkelijker met behulp van de technologie te voorkomen dan geweldsmisdrijven. Voorts geldt dat afhankelijk van het type delict een andere technologische benadering vereist is. In de categorie vermogensdelicten vergt bijvoorbeeld de bescherming van goederen tegen diefstal de inzet van andere technologieën dan de bescherming van woningen tegen inbraak.

- *Locatie*
  Van belang is ook op welke locatie het delict gepleegd wordt. De inzet van technologie in het privé-domein is van een andere orde dan in het publiek en semi-publiek domein. Zo vervult cameratoezicht op straat een andere functie dan in winkels of op de werkplek.

- *Dader of doelwit*
  Bij de keuze van de meest geëigende technologie speelt de vraag of deze gericht dient te zijn op de dader of op het doelwit (goederen of personen). Kiest men de potentiële dader als invalshoek, dan kan de technologie ertoe bijdragen dat diens gelegenheid beperkt, diens opbrengst geringer gemaakt en diens pakkans vergroot wordt en diens opsporing en vervolging zich effectiever en efficiënter voltrekken. Ook na diens veroordeling kan de technologie van nut zijn, bijvoorbeeld bij het toezicht op proefverloven of straatverboden via tracking en tracing. Voor het potentiële slachtoffer kan de technologie dienen om zich beter te beveiligen, de schade te beperken of het veiligheidsgevoel te vergroten. Behalve de dader en het slachtoffer kunnen ook goederen als invalshoek gekozen worden. De criteria die dan gebruikt kunnen worden om technologie in te zetten zijn: het

onsteelbaar maken, onbruikbaar maken na diefstal, het gebruik beperken tot de daartoe gerechtigden en het traceerbaar maken na diefstal.

- *Behoeften van de strafrechtketen*
  Afhankelijk van de specifieke taken en doelen in de schakels van de strafrechtketen – preventie, handhaving, opsporing, vervolging, executie – varieert de keuze van de inzet van technologie. De politie heeft voor een optimale uitvoering van haar taken andere technologische behoeften dan bijvoorbeeld de preventiewerker. Zo vormt de startonderbreker een goed instrument om autodiefstal te voorkomen, maar de opsporing van de dader heeft een grotere kans van slagen als de startonderbreker gecombineerd is met diefstalalarmering en/of tracking en tracing.

Bij de bepaling van de keuze welke technologie ingezet zal worden om de criminaliteitsproblematiek het hoofd te bieden, zullen al deze vier aspecten in onderlinge samenhang met elkaar in ogenschouw genomen moeten worden. De keuze van de technologie kan vergemakkelijkt worden door te denken in termen van functies. Iedere vorm van technologie kan vertaald worden in een of meerdere functies. Zo ook zal bij de (technologische) aanpak van een specifiek criminaliteitsprobleem een aantal functies vervuld moeten worden. Functies van de technologie die dienstig kunnen zijn voor de criminaliteitsbeheersing, zijn onder meer: waarnemen (camera's), identificeren (biometrie, gezichtsherkenning), alarmeren (alarmsystemen, patroonherkenning), gegevens koppelen en communiceren (computers). Behalve voor de selectie van bestaande technologieën biedt het denken in termen van functies een handvat voor de speurtocht naar nieuwe technologische toepassingsmogelijkheden voor de beheersing van de criminaliteit. Achtereenvolgens komen dan aan de orde:

- welke functies de huidige technologieën in zich bergen om bepaalde delicten op te sporen of te voorkomen;
- welke functies nodig zijn om de preventie en repressie te verbeteren en welke bestaande technologieën daarin reeds (kunnen) voorzien;
- welke functies in theorie dienstig zouden kunnen zijn bij het voorkomen of opsporen van criminaliteit, maar waar de huidige technologie nog niet in voorziet.

3. Veelbelovende terreinen

3.1 Technologische ontwikkelingen

De wereld van de technologie heeft zich nog lang niet uitgekristalliseerd en zal dat ook nooit zijn. Waarschijnlijk zullen in de nabije toekomst de ontwikkelingen elkaar in een steeds sneller tempo opvolgen en zal steeds vaker sprake zijn van interdisciplinaire technologische oplossingen voor maatschappelijke problemen. In hoeverre de preventie en opsporing profijt kunnen trekken van deze ontwikkelingen, valt niet met zekerheid te voorspellen. Nu al doet zich de situatie voor dat zelfs bestaande technologische mogelijkheden te weinig worden benut. Denk bijvoorbeeld aan het beveiligen van auto's via tracking en tracing. Hoewel dit systeem de opsporing van gestolen voertuigen vergemakkelijkt, beschikken de meeste wagens niet over een dergelijk detectiesysteem. Wel beschouwd is dat merkwaardig, wanneer je alle *gadgets* in ogenschouw neemt, zoals de airco, airbags, elektronisch bedienbare ramen, de *handsfree* telefoonset en audioapparatuur. Ook op andere terreinen is al veel ontwikkeld, maar worden de uitkomsten te weinig benut. Illustratief zijn de talrijke studies, pilotprojecten en verkenningen die op initiatief van het agentschap Senter van het ministerie van Economische Zaken in het kader van het deelprogramma 'Technologie en Criminaliteitspreventie' de afgelopen zes jaar zijn uitgevoerd. Ze variëren van intelligente verlichting, overdracht van beveiligingssignalen via de kabel en identificatie via oorherkenning, tot signaleringssystemen voor diefstal van vrachtwagens en nummerbordherkenning bij de toegang tot bedrijventerreinen.

Waar al zoveel op de plank ligt, is het verstandig eerst te inventariseren welke technologische mogelijkheden reeds zijn verkend, alvorens te bepalen op welke terreinen het wenselijk is nieuwe, veelbelovende ontwikkelingen in gang te zetten. In opdracht van de commissie is dan ook geïnventariseerd welke technologieën er al ten dienste kunnen staan van repressie en preventie. Niet alle vormen van criminaliteit zijn hierbij in ogenschouw genomen. Uit een oogpunt van capaciteit en kosten is het noodzakelijk grenzen te stellen aan de investering in technologische ontwikkelingen ten behoeve van de criminaliteitsbeheersing. Bij de keuze van de criminaliteitsvelden is dan ook een selectie gemaakt op basis van de volgende criteria:

- de impact van het delict op de samenleving in termen van omvang, ontwikkeling, ernst, schade en perceptie (ernstige vormen van criminaliteit);
- de (on)mogelijkheden om het delict adequaat aan te pakken (veelvoorkomende criminaliteit en overlast);
- het beslag dat het delict op de politie- en justitiecapaciteit legt (vereenvoudigen van routineklussen);
- de mogelijkheid om meer daders op te sporen via de technologie (verhoging van het oplossingspercentage).

3.1.1 Ernstige vormen van criminaliteit

Bij de aanpak van ernstige vormen van criminaliteit is geïnventariseerd in hoeverre de inzet van technologie van nut kan zijn bij het voorkomen en bestrijden van terrorisme, georganiseerde criminaliteit en organisatiecriminaliteit, mensenhandel en –smokkel en drugshandel. Onderstaand volgt een greep uit de technologische mogelijkheden.

- *Terrorisme*

Hoewel terroristische acties op tal van terreinen denkbaar zijn en vaak niet te voorkomen en moeilijk te bestrijden zijn, is toch een aantal belangrijke veiligheidsmaatregelen in ontwikkeling die enerzijds gericht zijn op het beter beveiligen van gebouwen en anderzijds op het detecteren van biologische wapens. Om met het eerste te beginnen, luchthavens en havens vormen een kwetsbaar doelwit voor terroristen. Veel is al gedaan om de technische beveiliging te optimaliseren, maar het personeel dat vrijelijk rond kan lopen vormt nog steeds een kwetsbare schakel. Werknemers beschikken meestal over een persoonsgebonden pas, waarmee ze de beveiliging kunnen passeren. Omdat hun pas overdraagbaar is, vormt dit uit een oogpunt van veiligheid geen ideale situatie. De combinatie van een persoonsgebonden pas met een biometrische toepassing kan een oplossing bieden. TNO heeft onlangs onderzocht welke vorm van biometrie de meeste kans van slagen biedt. Nadat diverse alternatieven in het voortraject waren afgevallen, resteerde de keuze tussen de irisscan en gezichtsgeometrie. Op basis van criteria als maatschappelijke acceptatie, snelheid van het verificatieproces, fraudebestendigheid en betrouwbaarheid kwam de persoonsgebonden pas gekoppeld aan een irisscan als de beste beveiligingsvorm naar voren. Deze combinatie ligt ook ten grondslag aan het nieuw te introduceren toegangsbeveiligingssysteem op de luchthaven Schiphol.

Voor de detectie van biochemische wapens wordt momenteel gewerkt aan de ontwikkeling van *smart dusts*. Dit zijn siliciumchips ter grootte van een stofdeeltje waarmee chemische stoffen snel ontdekt en geïdentificeerd kunnen worden. Toevoeging van *smart dusts* aan drinkwater moet het mogelijk maken om het water te testen op duizenden

verschillende stoffen. Overigens is de *smart dust* voorlopig nog een technologische droom en is de speurhond nog ons beste wapen. Een alternatief dat thans onderwerp van serieus onderzoek is, is de inzet van de sluipwesp bij de detectie van bepaalde gassen en biologische wapens.

- *Georganiseerde criminaliteit en organisatiecriminaliteit*

De aanpak van de georganiseerde criminaliteit en organisatiecriminaliteit is vooral het terrein van de forensische accountants. Daarnaast biedt speciale software voor het analyseren van afgeluisterde telefoongesprekken en andere vormen van elektronische communicatie een snelle manier om deze vormen van criminaliteit op te sporen. Zelfs als de inhoud ontoegankelijk zou worden – waartegen opgetreden kan worden met regelgeving op het gebied van encryptie – kan uit de contact- en verplaatsingspatronen veel opsporingsinformatie afgeleid worden. Van belang voor het bestrijden van deze vormen van criminaliteit is voorts het koppelen van bestanden, bijvoorbeeld om witwassen van crimineel vermogen tegen te gaan. Privacyaspecten staan echter een uitgebreide koppeling van bestanden in de weg.

- *Mensenhandel en -smokkel*

Bij het bestrijden van mensenhandel en –smokkel speelt de identificatie van personen een belangrijke rol. Alleen op basis van DNA-controle lijkt zekerheid mogelijk over de vaststelling van de identiteit; identiteitspapieren, zo al aanwezig, lenen zich immers goed voor vervalsing. De uitrusting van identiteitspapieren met biometrische kenmerken is volop in ontwikkeling. Er zijn hoge kosten mee gemoeid. Ook enige mate van fraudegevoeligheid en foutmeldingen spelen een rol, waardoor sommigen door de mazen van de controle kunnen glippen, terwijl anderen ten onrechte tegengehouden worden.

- *Drugshandel*

Drugshandel en –smokkel hebben op grote schaal plaats. Een goede wijze van detectie van drugs is dan ook een belangrijke aangelegenheid. Er zijn verschillende technologische mogelijkheden. Via röntgenapparatuur of een tetraherzcamera kunnen bijvoorbeeld bolletjesslikkers opgespoord worden. Deze vorm van controle geschiedt echter op vrijwillige basis en stuit daardoor op praktische bezwaren. Sniffers en snuffers – chemische stoffen die sensoren activeren – kunnen een belangrijke rol spelen bij de detectie van drugs. Technologisch moet het mogelijk zijn een detectiepoort te ontwikkelen voor het opsporen van drugs op personen en in bagage. Een tweede mogelijkheid is de ontwikkeling van een elektronische snuffelhond ter vervanging van de natuurlijke viervoeter. Voor het opsporen van drugs kunnen ten derde tracers worden ingezet. Tracers verzamelen lucht die zich rond drugs bevinden en destilleren hieruit minuscule hoeveelheden van de drug, die vervolgens wordt geanalyseerd.

3.1.2 Veelvoorkomende criminaliteit en overlast

Zeven vormen van veelvoorkomende criminaliteit en overlast zijn in ogenschouw genomen: fietsdiefstal, inbraak in woningen en bedrijven, wildplassen, vervuiling in woonwijken, vandalisme, mishandeling en diefstal met geweld. Het feit dat deze delicten veelvoorkomend zijn illustreert hoe lastig het is ze adequaat aan te pakken. Een korte schets van de technologische mogelijkheden volgt hierna.

- *Fietsdiefstal*

Tegen fietsdiefstal is menig middel zonder succes beproefd. Zelfs het meenemen van de pedalen na het stallen van de fiets biedt geen soelaas. Een mogelijke oplossing, die thans ook landelijk voorbereid wordt, is de inbouw van antidiefstalchips in de fiets gekoppeld aan een registratiesysteem. Het succes van dit systeem staat of valt met een goede regeling van de aangifte, opsporing van gestolen fietsen, retournering van de fiets bij de rechtmatige eigenaar, vervolging en berechting van daders en helers.

- *Inbraak en diefstal in woningen en bedrijven*

Inbraak is een veelvoorkomend delict, waarbij zowel veel buit te vergaren valt als veel beveiligingsmaatregelen mogelijk zijn. Voor de bewaking van het object kan gedacht worden aan cameratoezicht (eventueel, om kosten te besparen, in combinatie met fake-camera's) en mobiele video surveillance.

Voor het detecteren van verdachte personen en 'abnormaal' gedrag in de omgeving van een bedrijf zijn er onder meer vroegtijdige waarschuwingssystemen, persoon- en patroonherkenningssystemen (object pattern analysis). Persoon- en patroonherkenning maakt gebruik van videocamera's, opname - en compressietechnieken, datatransport, en gezichtsherkenningstechnologie. De beelden worden geanalyseerd op basis van beweging, kleur en vorm en worden vergeleken met beelden die opgeslagen zijn in een database. Opname en vergelijking van de beelden kent een redelijk grote betrouwbaarheid.

Vooral patroonherkenningssystemen (object pattern analysis) zijn bijzonder interessant. Een voorbeeld van de toepassing van dit waarschuwingssysteem is de bewaking bij pinautomaten. Wie geld wil pinnen, wordt gevolgd door een camera die de beelden verwerkt en opslaat in een computer. Personen die gedurende langere tijd in de buurt van de automaat verblijven, worden zichtbaar als ze door een (elektronisch) filter gescheiden worden van de beelden van degenen die de automaat gebruiken en meteen weggaan. Het beeld dat dan overblijft, toont de personen die opmerkelijk lang bij de automaat verblijven en wellicht kwade bedoelingen hebben, zoals de beroving van een geldpinner of het kopiëren van diens pinpas en ontfutselen van de pincode.

Voor het achterhalen van gestolen goederen komen vormen van tracking en tracing, gsm's in combinatie met detectoren en anti-diefstalchips in aanmerking. Het op afstand volgen van objecten gebeurt via labels die – soms ongemerkt – bevestigd worden. Veel labels kunnen al tijdens het productieproces aangebracht worden. In de toekomst maakt miniaturisering het mogelijk vrijwel alles te registreren en te volgen.

Nauw verwant met tracking en tracing zijn bepaalde alarmdetectiesystemen die kunnen worden gebruikt voor eigendomsvaststelling en voor het volgen van het object. Deze systemen, ook wel 'electronic tagging systems' genoemd, worden al ingezet voor de identificatie van boten, gsm-toestellen en juwelen. Sommige van deze systemen werken met RFID-technologie (radio frequency identification). Deze technologie maakt gebruik van een breed spectrum van radiofrequenties en is geschikt om diefstalgevoelige objecten te merken. Samen met sensortechnologie wordt deze toepassing geschikt geacht om uit te groeien tot een geïntegreerd en intelligent alarmdetectiesysteem.

- *Wildplassen*

Wildplassen is vooral een sociaal probleem. Waarschijnlijk biedt een gedragswetenschappelijke benadering meer mogelijkheden voor de aanpak van het probleem dan technologische oplossingen. Van maatregelen als schrikdraad en verzinkbare plaskruizen wordt niet anders verwacht dan dat ze binnen een mum van tijd worden gesloopt. Meer openbare toiletten kunnen ook uitkomst bieden.

- *Vervuiling in woonwijken*

Opnieuw een vooral sociaal probleem, hoewel verloedering van woonwijken – in overeenstemming met het concept van de *broken windows theory* – vaak de eerste stap zal vormen tot het ontstaan van broeinesten van criminaliteit. Verzonken vuilcontainers blijken in de praktijk redelijk goed te functioneren. Ook de introductie van statiegeld op wegwerpplastic en blik kan een oplossing bieden. Ten slotte kan de ontwikkeling van biologisch afbreekbare verpakkingsproducten bijdragen aan een vermindering van de vervuiling.

- *Vandalisme*

De aanpak van vandalisme van goederen is vooral een kwestie van het ontwikkelen van materialen voor objecten in de openbare ruimte die bestand zijn tegen vernieling en graffiti. Onderzoek naar de eigenschappen van materialen vormt dan ook een belangrijke voorwaarde voor de aanpak van dit probleem.

- *Mishandeling*

Technologisch zijn er weinig mogelijkheden om mishandeling te voorkomen. Voor het opsporen van dit type delict in de openbare ruimte ligt cameratoezicht het meest voor de hand. Noodzakelijk is wel dat de beelden gemonitord worden, zodat onmiddellijk ingegrepen kan worden in het geval van geweld. Ook kan gedacht worden aan het gebruik van gps in mobiele telefoons als peillood voor de locatie waar het misdrijf zich afspeelt na een oproep via 112.

- *Diefstal met geweld*

Net als bij mishandeling zijn er (vooralsnog) weinig technologische mogelijkheden om diefstal met geweld aan te pakken.

3.1.3 Vereenvoudigen van routineklussen

De politie zou erbij gebaat zijn wanneer een aantal tijdrovende routineklussen geautomatiseerd of anderszins versneld kan worden. De gedachten gaan vooral uit naar alcoholcontrole, controle op wapenbezit en het opmaken van processen-verbaal.

- *Alcoholcontrole*

Het controleren van automobilisten op het promillage aan alcohol dat ze in hun bloed hebben, legt een groot beslag op de politiecapaciteit. Door het proces van alcoholcontrole te versnellen kan veel tijdwinst geboekt worden, die vervolgens aan het opsporen van andere delicten besteed kan worden. De ontwikkeling van Pistool, waar ook

TNO/FEL bij betrokken is, is dan ook veelbelovend. Met deze wijze van alcoholcontrole wordt de doorlooptijd verkort van twee uur naar drie kwartier.

Preventief valt er enige winst te behalen door het starten van het voertuig te koppelen aan een blaastest. In Canada is dit reeds usance. Probleem met een dergelijk systeem is dat het nogal fraudegevoelig is; ook een nuchter persoon kan deze blaastest uitvoeren, waardoor de auto alsnog start. Invoering van deze technologie is overigens mede-afhankelijk van de medewerking van de autoindustrie, waardoor dus internationale consensus vereist is.

- *Controle op wapenbezit*

Op dit terrein zijn er tal van technologische mogelijkheden. Ten eerste zijn er diverse detectiemethoden voor het opsporen van metaal. De metaaldetectiepoort bijvoorbeeld waarschuwt via een magnetisch veld voor de aanwezigheid van metaal. De handmetaaldetector werkt eveneens op basis van magnetische velden, maar werkt alleen van nabij. Hoogfrequente microgolven vormen de basis voor detectie met de MRI-scan, terwijl de microwave radar camera en de microwave dielectrometer camera gebruik maken van respectievelijk elektromagnetische straling en dielektrometers. Infraroodcamera's ten slotte detecteren op basis van warmtestraling vooral koude wapens.

Behalve metalen wapens is het ook mogelijk explosieven en biologische wapens op te sporen. Explosieven zijn te detecteren via explosives trace detection (EDT) en explosives detection systems (EDS). Voor het opsporen van plastic explosieven biedt quadrupole resonance uitkomst. Biologische wapens zijn te traceren met behulp van biosensoren, trigger-technologie, aerodynamic particle sizer, biofluoricentie technieken en ionization trace detection.

Preventief interessant zijn wellicht de *smart guns*, vuurwapens die via smartcards of biometrie beschermd zijn tegen onbevoegd gebruik. Toepassing wordt echter eerder geschikt geacht voor gevangenistoezicht dan voor bijvoorbeeld toezicht op straat.

- *Proces-verbaal opmaken*

Hoewel zeer wenselijk, vormt een versnelling van de aangifteprocedure nog steeds een onderwerp van hoofdbrekens. Vooral de standaardisatie vormt een hindernis. Thans wordt de elektronische aangifte ingevoerd en is het elektronisch proces-verbaal in een vergevorderd ontwikkelingsstadium.

3.1.4 Verhoging van het ophelderingspercentage

Wellicht biedt de technologie onorthodoxe methoden om delicten aan te pakken die vooralsnog vanwege de moeilijkheidsgraad van de bewijsvoering en/of de gevergde tijdsinvestering onvoldoende aangepakt worden. Te denken valt aan milieuhandhaving en identiteitsfraude. Ook bij het toezicht en de controle in de openbare ruimte zou de technologie kunnen bijdragen aan het verhogen van het ophelderingspercentage. Onderstaand een verkenning van een aantal technologische mogelijkheden.

- *Toezicht en controle in de openbare ruimte*

Voor het intensiveren van het toezicht en de controle in de openbare ruimte kan gedacht worden aan het gebruik van microsatelliet technologie, die geschikt is voor het identificeren, lokaliseren en volgen van personen en goederen. Ook via geospatial digital information tools in (onbemande) vliegtuigjes kan intensief toezicht gehouden worden op de openbare ruimte.

- *Milieuhandhaving*

Tegen het illegaal storten van milieuvervuilende stoffen in de natuur valt vooralsnog weinig te beginnen. Een uitzondering vormt misschien het illegaal lozen op zee. Door containers, goederen en stoffen reeds in de fabriek te labellen kan de herkomst van het geloosde goed achterhaald worden.

- *Identiteitsfraude*

Met de invoering van de algemene identificatieplicht en de toename van het aantal organisaties dat een identiteitsbewijs verlangt alvorens zijn diensten te verlenen, zal het aantal gevallen van identiteitsfraude in de nabije toekomst naar verwachting sterk toenemen. Biometrie en biotechnologie zijn de meest genoemde oplossingen voor deze vorm van fraude. Deze technologieën berusten op het vaststellen van unieke lichaamskenmerken, die ze geschikt maken voor het verifiëren van iemands identiteit en op basis daarvan het verlenen van toegang tot bepaalde diensten of systemen. Te denken valt aan het koppelen van het identiteitsbewijs aan bijvoorbeeld de irisscan, een vingerafdruk, DNA-analyse, gezichtsherkenning of handgeometrie.

3.2 Technologie van de toekomst

Uit de inventarisatie van technologische mogelijkheden bij het beheersen van emstige en veelvoorkomende vormen van criminaliteit en het verlichten van de werkzaamheden van de opsporing blijkt dat niet op elk terrein veel winst te verwachten valt. In schema:

	weinig mogelijkheden	middenpositie	veelbelovend
Ernstige vormen van criminaliteit			
• terrorisme	?		
• georganiseerde en organisatiecriminaliteit		?	
• mensenhandel en –smokkel	?		
• drugshandel		?	
Veelvoorkomende criminaliteit			
• fietsdiefstal		?	
• inbraak en diefstal in woningen en bedrijven			?
• wildplassen	?		
• vervuiling in woonwijken	?		
• vandalisme	?		
• mishandeling	?		
• diefstal met geweld	?		
Vereenvoudigen van routineklussen			
• alcoholcontrole		?	
• controle op wapenbezit			?
• proces-verbaal opmaken		?	
Verhoging van het ophelderingspercentage			
• toezicht en controle in de openbare ruimte			?
• milieuhandhaving		?	
• identiteitsfraude			?

Veelbelovend zijn kortom technologische toepassingen bij controle op wapenbezit, toezicht en controle in de openbare ruimte, identiteitsfraude en inbraak in woningen en bedrijven. Het verdient aanbeveling op deze terreinen de technologische mogelijkheden nader te verkennen. Daarbij dienen bij de keuze van de meest geschikte technologie vier criteria richtinggevend te zijn:

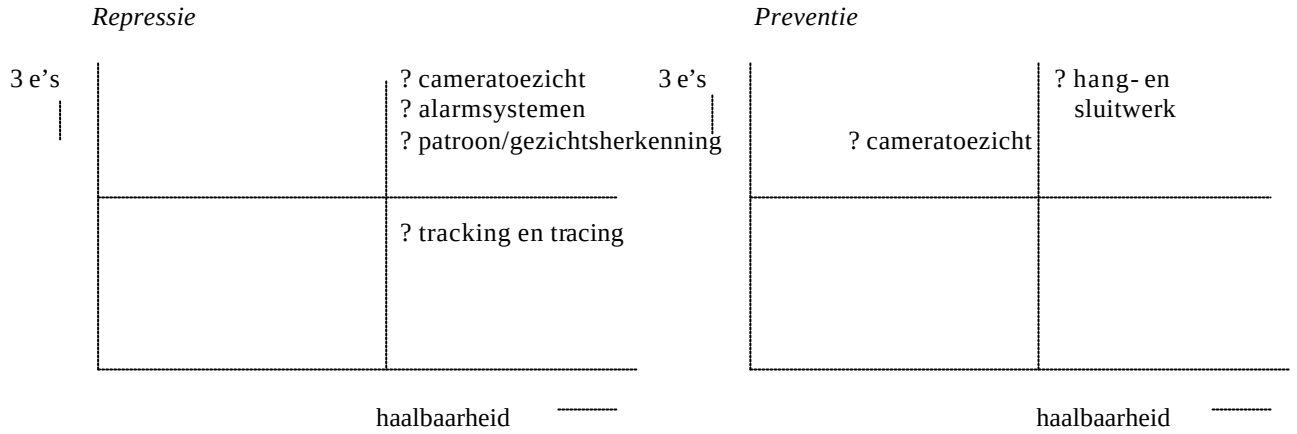
- effectiviteit: is de technologie voldoende effectief
- efficiëntie: staan de investeringen in de ontwikkeling en toepassing in verhouding tot de verwachte baten
- eerlijkheid: stuit de technologie niet op ethische en juridische barrières
- haalbaarheid: stuit de technologie niet op maatschappelijke en/of politieke weerstanden

Voor elk van de vier geselecteerde veelbelovende terreinen zijn deze criteria toegepast op de diverse mogelijk inzetbare technologieën. Daarbij is een onderscheid gemaakt tussen preventie en repressie. Immers, sommige technologieën kunnen voor bijvoorbeeld repressie zeer nuttig zijn, maar preventief geen effect sorteren.

Alvorens het resultaat van deze exercitie te presenteren, wil de commissie in herinnering brengen dat bij de ontwikkeling van deze technologieën rekening gehouden moet worden met aspecten als locatie, doelstellingen en functies van de technologie. Wat dat laatste betreft: de in dit advies beschreven technologieën zijn vooral gericht op het proces van analyseren van criminele incidenten – het waarnemen, bewerken en beoordelen van informatie – en niet op het verdere 'handelen' naar aanleiding van deze incidenten. Handelend optreden, zoals het geval is bij de sprinklerinstallatie nadat deze een brand heeft gedetecteerd, is (vooralsnog) niet aan de orde.

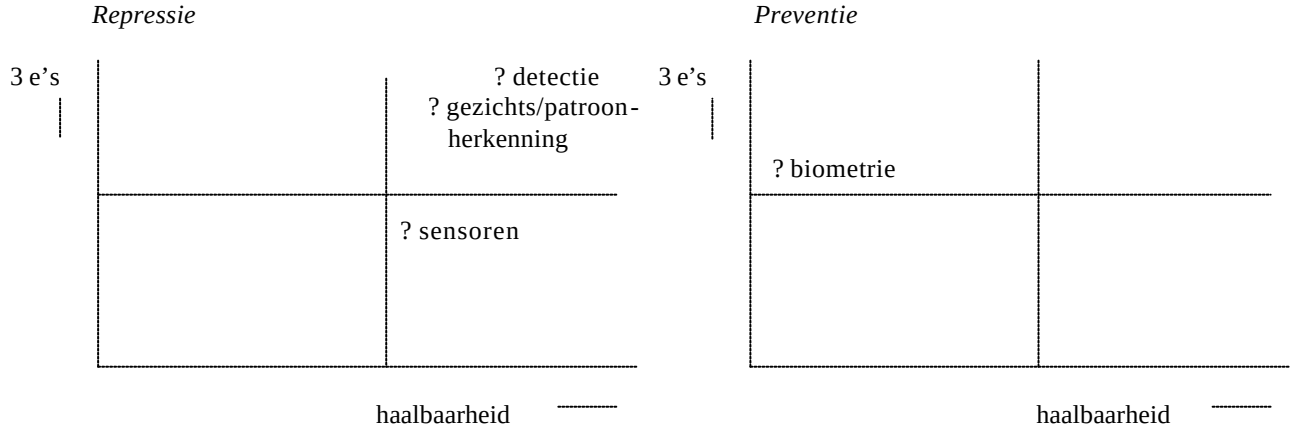
3.2.1 Veelvoorkomende criminaliteit: inbraak in woningen en bedrijven

Bij het voorkomen en bestrijden van inbraak in woningen en bedrijven liggen de technologische mogelijkheden op het terrein van de beveiliging van het gebouw (hang- en sluitwerk, cameratoezicht, alarmsystemen), het detecteren van verdachte personen en bewegingen (patroon- en gezichtsherkenning, object patern analysis) en het opsporen van gestolen goederen (tracking en tracing, radio frequency identification). Al deze technologieën worden, zo zij al niet wijd verbreid worden toegepast, zeer veelbelovend geacht.



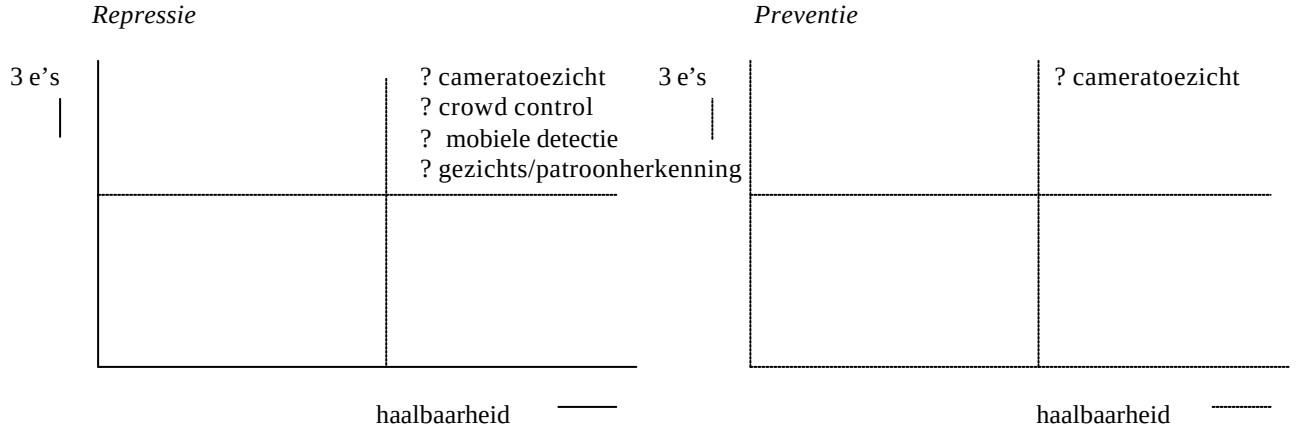
3.2.2 Vereenvoudigen van routineklussen: controle op wapenbezit

Bij de aanpak van wapenbezit liggen de technologische mogelijkheden vooral op het terrein van de repressie. Veelbelovend zijn volgens de experts: de diverse vormen van metaaldetectie, sensoren, biometrie en gezichts- en patroonherkenning. Op korte termijn zijn vooral ontwikkelingen op het terrein van detectie, sensoren en gezichts- en patroonherkenning de moeite van het bestuderen waard. Biometrie, dat ook preventief voordelen kan bieden, stuit vooralsnog op praktische problemen: een vingerscan die uitsluitend de eigenaar toegang geeft tot gebruik van het wapen, werkt te traag wanneer onmiddellijk ingrijpen noodzakelijk is.



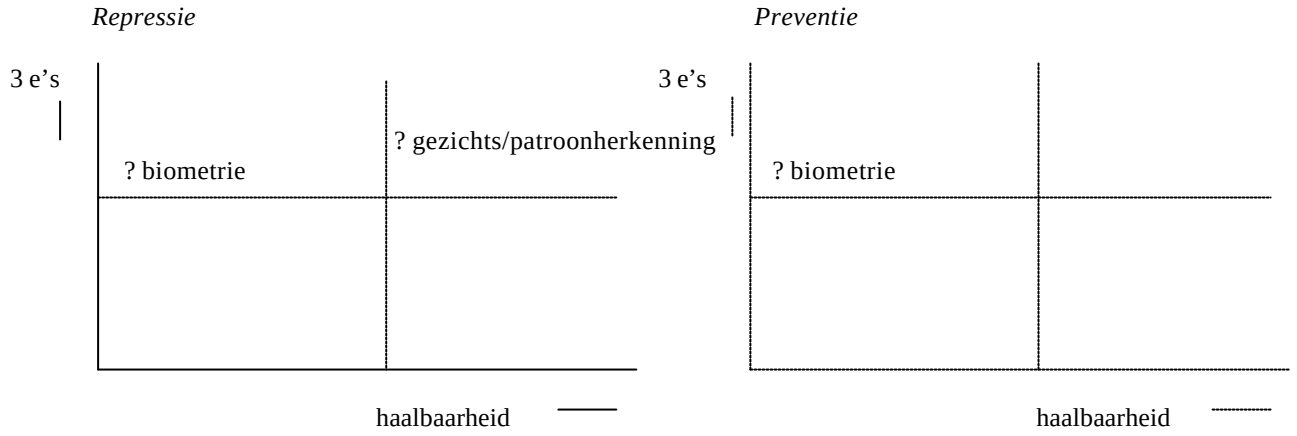
3.2.3 Verhoging van het ophelderingspercentage: toezicht en controle in de openbare ruimte

Bij toezicht en controle in de openbare ruimte ligt een effectieve aanpak vooral in: mobiele detectie, gezichts- en patroonherkenning, camerabewaking en crowd control (handhaving van de openbare orde bij massale bijeenkomsten).



3.2.4 Verhoging van het ophelderingspercentage: identiteitsfraude

Voor de aanpak van identiteitsfraude zullen vooral de mogelijkheden van biometrie nader uitgewerkt moeten worden. Zoals al eerder opgemerkt, kleven er thans nog veel praktische problemen aan (zie paragraaf 3.1.1).



3.3 Meest veelbelovend: patroon- en gezichtsherkenning

Uit voorgaande analyse van veelbelovende technologieën blijkt in bijna alle gevallen dat met name patroon- en gezichtsherkenning een veelbelovende technologie is om de onderzochte vormen van criminaliteit aan te pakken. Verdachte personen en gedragingen in de buurt van gebouwen kunnen opgespoord worden zonder dat intensieve surveillance nodig is. Bekende illegale wapenhandelaren en terroristen kunnen via gezichtsherkenning gesignaleerd worden zonder eerst een beroep te moeten doen op het menselijk geheugen. Hetzelfde geldt voor het toezicht in de openbare ruimte. Denk bijvoorbeeld aan het opsporen van voetbalsupporters met een stadionverbod en het in een vroeg stadium signaleren van opstootjes en relletjes. Zelfs bij identiteitsfraude kan gedacht worden aan de toepassing van gezichtsherkenning door identiteitsbewijzen te koppelen aan een database met portretten van de rechtmatige eigenaren. Ook op andere terreinen van de criminaliteits- en overlastbestrijding kan men zijn voordeel doen met deze technologie. Denk bijvoorbeeld aan de reeds gememoreerde beveiliging van pinautomaten, het detecteren van verdacht gedrag in winkels, het analyseren van agressief gedrag, het vergelijken van mogelijk gestolen goederen met afbeeldingen van ontvreemde objecten in een database. Tegelijkertijd staat deze technologie vooralsnog in de kinderschoenen. Voor het bereiken van successen op korte termijn met de inzet van nieuwe vormen van technologie bij het beheersen van de criminaliteit acht de commissie de verdere ontwikkeling van patroon- en gezichtsherkenning dan ook buitengewoon veelbelovend.

4. Criminele bedreigingen

4.1 Nieuwe kansen voor criminelen

De technologie biedt niet alleen politie en justitie kansen voor een betere uitoefening van hun taken, ze biedt ook criminelen meer gelegenheden en mogelijkheden tot het plegen van criminaliteit. Dit hangt ten eerste samen met bepaalde algemene ontwikkelingen in de technologie, die – zoals we in hoofdstuk 2 al zagen – mede de grondslag hebben gevormd voor de inrichting van de moderne samenleving. Kenmerkend voor deze ontwikkeling zijn:

- *Het vervagen van geografische grenzen*
  De mondialisering brengt met zich mee dat criminelen meer dan voorheen op nationaal en internationaal niveau samenwerking kunnen zoeken en hun werkterrein drastisch kunnen uitbreiden. De buit is navenant groter.

- *Een groter aanbod van goederen en diensten*
  Dankzij de informatisering zijn meer goederen, diensten en systemen binnen handbereik. Voor kwaadwillenden is het relatief eenvoudig hier misbruik van te maken. Denk bijvoorbeeld aan het bestellen van goederen via internet zonder deze af te rekenen, het inbreken in bedrijfssystemen om concurrentiegevoelige informatie te vergaren en het ongeoorloofd wegsluizen van grote sommen geld naar onnaspeurbare rekeningen. Ook de snelheid waarmee deze 'operaties' uitgevoerd kunnen worden, werkt in het voordeel van de crimineel.

- *Betere waarborgen voor de privacy*
  De individualisering is gepaard gegaan met meer anonimiteit en een grotere aandacht voor privacyaspecten. Dit werkt in het voordeel van de criminelen, die immers zonder sporen na te laten hun slag willen slaan.

Ten tweede doen zich ontwikkelingen op productniveau voor die in het voordeel van de crimineel werken. Te denken valt onder meer aan:

- *De productie van luxe goederen*
  De welvaart is de afgelopen decennia sterk gestegen en de productie van luxe goederen zoals audiovisuele apparatuur, laptops en mobiele telefoons houdt daarmee gelijke tred. Er komen meer waardevolle goederen op de markt en zolang deze niet voor iedereen financieel binnen handbereik zijn, vormen ze een lucratieve buit voor criminelen.

- *Het aanbod van nieuwe bancaire diensten*
  Pinpas en chipknip hebben een aanzienlijk deel van het papieren betalingsverkeer verdrongen. De beveiliging van dit plastic geld is echter (nog) niet optimaal, waardoor pincodes met behulp van afleesapparatuur eenvoudig achterhaald kunnen worden zonder dat de bezitter van de pas in de gaten heeft dat hij op het punt staat bestolen te worden.

- *Een handzamer formaat van goederen*
  Miniaturisatie – een verzameling van technieken die tot doel hebben een product kleiner te maken – vervult een belangrijke rol in het proces van productontwikkeling. De goederen worden kleiner en meestal lichter, waardoor ze niet alleen handzamer zijn, maar ook gevoeliger worden voor diefstal.

Vorenstaand overzicht biedt slechts een beknopte indicatie van de mogelijkheden die nieuwe technologieën bieden voor het plegen van (nieuwe vormen van) criminaliteit. Ze illustreert het belang dat toegekend moet worden aan het systematisch volgen van zowel de algemene technologische trends als de ontwikkelingen op productniveau, opdat politie en justitie zo goed mogelijk voorbereid zijn op het ontstaan van (nieuwe vormen van) criminaliteit.

4.2 Toekomstige trends en ontwikkelingen

Met het voortschrijden van de technologische ontwikkelingen zullen trends als de mondialisering, individualisering en informatisering van de samenleving zich naar alle waarschijnlijkheid op grotere schaal voordoen, met alle consequenties van dien. In het rapport *Met het oog op de toekomst* (2001) spreekt de Adviesraad voor het Wetenschaps- en Technologiebeleid (AWT) de verwachting uit dat de organisatiecriminaliteit en georganiseerde misdaad door zowel schaalvergroting als het verdwijnen van handelsbarrières en open grenzen de komende jaren in omvang zullen toenemen.

Daarnaast signaleert de AWT dat technologische ontwikkelingen niet alleen nieuwe misdrijven mogelijk maken, maar ook een ander type dader aantrekken: het type van de 'degelijke burger' die zijn kans waagt om betrekkelijk risicoloos snel veel geld te verdienen of ander voordeel te behalen in de anonieme hightech-wereld. Overigens ziet de raad de toekomst niet zó somber: in de praktijk blijkt dat ordehandhaving en criminaliteitsbestrijding, in weerwil van de voorspellingen, steeds meer gedragen worden door burgers en niet-gouvernementele instellingen.

In het bestek van dit advies is het ondoenlijk alle mogelijke criminogene trends en ontwikkelingen op productniveau in kaart te brengen. Volstaan wordt met te wijzen op de 'levenscyclus' die criminaliteitsgevoelige goederen, diensten en systemen doorlopen. Deze levenscyclus vangt aan met toenemende criminaliteit en mondt na verloop van tijd uit in afnemende kwetsbaarheid. Een voorbeeld vormen de pinautomaten. De eerste jaren na hun introductie lokten ze – vanwege hun relatieve onbekendheid en derhalve spaarzame gebruik door de burger – geen criminaliteit uit. Naarmate echter de populariteit van het 'flappentappen' toenam, steeg ook het aantal berovingen. Pas toen troffen de banken (technologische) maatregelen om de pinautomaten beter te beveiligen.

Criminaliteitsgevoelige producten onderscheiden zich doordat ze, zoals criminoloog Ron Clarke het noemt, 'CRAVED' zijn: Concealed, Removable, Available, Valuable, Enjoyable, Disposable. Over het algemeen geldt: hoe begeerlijker, aangenamer, waardevoller, makkelijker te vervoeren, breder verkrijgbaar een product is, des te groter de gevoeligheid voor criminaliteit is. Als bedrijven ertoe bewogen kunnen worden in een vroeg stadium aan deze criteria aandacht te besteden, zou criminaliteitspreventie meer standaard worden in plaats van – zoals thans het geval is – louter een van de mogelijke opties in de productontwikkeling.

4.3 Wapenwedloop met politie en justitie

Behalve dat de technologie criminelen meer gelegenheid en mogelijkheden biedt voor het plegen van delicten, zijn aan een grotere inzet van de technologie door politie en justitie bij het beheersen van de criminaliteit óók risico's verbonden die van invloed zijn op het ontstaan van (nieuwe vormen van) criminaliteit. Iedere technologische maatregel roept vroeg of laat een weerwoord op van criminelen. Er is in zekere zin sprake van een wapenwedloop. Is een technologische maatregel aanvankelijk nog afdoende, na verloop van tijd zullen criminelen een manier vinden om de maatregel te omzeilen. In dat opzicht raakt technologie als wapen tegen criminaliteit relatief snel verouderd. Een voorbeeld is de technologische bescherming tegen overvallen die na verloop van tijd aan kracht inboet: maskers en tweedehands kleding worden gebruikt om de camera te misleiden, stil alarm leidt ertoe dat de overvaller sneller te werk gaat en verfbommetjes in geldkoffers worden snel ontdekt door van tevoren de inhoud van de koffer te controleren.

Het behoeft geen betoog dat de politiële en justitiële autoriteiten zich bewust moeten zijn van deze ongewenste neveneffecten van de inzet van technologie bij het beheersen van de criminaliteit. De volgende vijf risico's springen het meest in het oog:

- *Verharding van de criminaliteit*
  Een betere beveiliging van goederen, diensten en systemen kan leiden tot een meer gewelddadig optreden en afpersing door criminelen die koste wat het kost hun doel willen bereiken.

- *Verplaatsingseffecten*
  Een betere beveiliging van goederen kan leiden tot een verschuiving van de criminaliteit naar diefstal van onderdelen, die vaak een eigen waarde vertegenwoordigen en daardoor de interesse van criminelen trekken. Het ontvreemden van chips uit computers, simcards uit mobiele telefoons en airbags uit auto's zijn hier voorbeelden van.

- *Meer identiteitsfraude*
  Wanneer legitimatie een belangrijker onderdeel gaat vormen ter bescherming van diensten en systemen, zal identiteitsfraude waarschijnlijk op grotere schaal voorkomen. Zo ook zullen daders vaker hun toevlucht zoeken tot afpersing en geweld om identiteitsdocumenten te bemachtigen. Een massale opslag van identiteitsgegevens brengt criminelen in de verleiding om in databestanden in te breken en gegevens te vervalsen.

- *Meer diefstal langs elektronische weg*
  Met het terugdringen van contant geld uit het betalingsverkeer neemt het risico van diefstal langs elektronische weg toe.

- *Averechtse neveneffecten*
  De invoering van nieuwe technologie kan onbedoeld ongewenste effecten hebben. Een bekend voorbeeld is de flitspaal langs de snelweg. Deze legt snelheidsovertredingen op de gevoelige plaat vast, maar leidt tevens tot onveilig rijgedrag doordat automobilisten in het vizier van een flitspaal hard op de rem gaan staan.

De wapenwedloop tussen politie en justitie enerzijds en criminelen anderzijds is door de Britse criminoloog Paul Ekblom vergeleken met de processen die in de evolutie een rol spelen: zowel in de wereld van de criminaliteit als in het dierenrijk is sprake van een permanent aanpassingsproces, waarbij het potentiële slachtoffer steeds probeert zijn agressor een stapje voor te zijn. Degene die verzuimt met enige regelmaat verbeteringen in zijn tactiek te treffen, is gedoemd de strijd te verliezen. Een teken aan de wand is dat de echte 'professionele' criminelen het zich financieel kunnen veroorloven zich uit te rusten met de beste moderne (technologische) wapens, terwijl politie en justitie het niet alleen met minder ruime middelen moeten zien te redden, maar ook nog bepaalde ethische en juridische voorwaarden in acht moeten nemen.

5. Barrières voor politie en justitie

Niet alleen juridische en ethische voorwaarden stellen grenzen aan de inzet door politie en justitie van technologie bij de beheersing van de criminaliteit. Ook op andere terreinen kunnen zich situaties voordoen die een belemmering vormen voor een optimale inzet van de technologie. In de formulering van de opdracht aan de commissie is expliciet gevraagd aandacht te besteden aan de bestaande kloof tussen het technologisch inzicht van de bèta's en de wereld van de alfa's en gamma's, die zo kenmerkend is voor de politie- en justitieambtenaren. Deze kloof komt aan de orde in de paragraaf 'culturele barrières'. Naast de juridische, ethische en culturele knelpunten stuitte de commissie in de loop van haar verkenning bovendien op een tweetal typen barrières die respectievelijk organisatorisch en technisch van aard zijn.

5.1 Culturele barrières

- *Gebrek aan coherent beleid, visie en coördinatie*

De activiteiten die tot dusverre op centraal niveau ondernomen zijn, vertonen weinig coherentie. De afgelopen jaren zijn bij de rijksoverheid onafhankelijk van elkaar diverse initiatieven ontplooid om de technologische mogelijkheden bij de beheersing van de criminaliteit in kaart te brengen. Zo startte het agentschap Senter van het ministerie van Economische Zaken het programma Technologie & Samenleving. Het ministerie van Binnenlandse Zaken liet TNO een technologieverkenning uitvoeren op het gebied van de openbare orde en veiligheid. De directie Wetgeving van het ministerie van Justitie wijdde een symposium aan de vraag: Gaat de justitiewetgever adequaat en consistent om met de ontwikkelingen in de techniek?

Uit deze voorbeelden blijkt dat de overheid enerzijds wel degelijk oog heeft voor de kansen en bedreigingen van de technologie. De aandacht is daarbij vooral gespitst op de virtuele wereld. Tegelijk kan geconstateerd worden dat een samenhangend beleid ontbreekt. Er worden geen dwarsverbanden gelegd tussen de diverse initiatieven. Er wordt niet voortgeborduurd op reeds verworven inzichten. Het ontbreekt aan een visie hoe de overheid kan inspelen op technologische ontwikkelingen. En het is onduidelijk waar de verantwoordelijkheid voor het uitstippelen van beleid en de coördinatie van nieuwe initiatieven moet worden gelegd. Waar het in feite aan ontbreekt, is een 'probleemeigenaar' bij de overheid. Dit blijkt bijvoorbeeld ook uit de evaluatie van de door Senter geïnitieerde projecten, die onlangs is afgerond. "Er zijn te weinig probleemhebbers. Maar dat komt ook doordat het werkveld erg ondoorzichtig en diffuus is. Er zijn veel organisaties die zich allemaal met bepaalde onderdelen van criminaliteitspreventie bezighouden. Het is erg lastig wie waarvoor verantwoordelijk is en wie wat wil bijdragen," aldus een van de geïnterviewden. En: "Een van de mijns inziens belangrijke oorzaken voor het gebrek aan coördinatie is de versnipperde ambtelijke organisatie zelf. Zeker op veiligheidsgebied bestaat er een achterhaalde kaste die, als ze zich een veiligheidsonderwerp toe-eigent, dit niet anders kan zien dan langs de door haar traditie bepaalde lijn."

- *Gebrek aan structurele financiële middelen*

Bij ontstentenis van een technologiebeleid stelt de rijksoverheid geen structurele financiële middelen beschikbaar voor het ontwikkelen van nieuwe technologische oplossingen voor de beheersing van de criminaliteit. Daardoor maakt ze zich afhankelijk van initiatieven van private partijen. Die laatsten echter reageren afwachtend op de ontwikkelingen in deze relatief complexe markt, waarvan de afzetmogelijkheden lang niet altijd duidelijk zijn. Immers, de ontwikkelings- en productiekosten moeten wel in verhouding staan tot de netto opbrengsten. De vrees dat er hoge kosten gemoeid zijn met de ontwikkeling van nieuwe technologische toepassingen en het inhuren van de bijbehorende expertise, maakt de overheid wellicht huiverig voor substantiële investeringen. Die vrees is naar het oordeel van de commissie echter niet geheel gegrond, mits uitgegaan wordt van intensievere publiek-private samenwerking. Dat er niet al te veel geld gemoeid hoeft te zijn met het stimuleren van innovatie blijkt uit de evaluatie van de Senter-projecten, die elk met een relatief klein budget van enkele tienduizenden euro's veelal voorspoedig van de grond zijn gekomen. Daarnaast biedt het structureel volgen en zo mogelijk overnemen van nieuwe technologische vindingen in het buitenland – en met name in de Verenigde Staten – veel financieel voordeel.

- *Gebrek aan kennis van en vertrouwen in de technologie*

Het ontbreken van een coherent beleid en navenante financiële middelen voor de inzet van technologie bij de beheersing van de criminaliteit kan voor een belangrijk deel verklaard worden door de kloof tussen technologen en veiligheidsambtenaren. De gemiddelde justitieambtenaar is geschoold in de sociale of juridische wetenschappen,

hetgeen zijn gebrek aan kennis van en ervaring met technologie verklaart en zijn 'natuurlijk onvermogen' om in de technologische hoek oplossingen te zoeken voor maatschappelijke problemen. Enkele uitzonderingen daargelaten, zoals de experts bij het Nederlands Forensisch Instituut, richt hij zijn aandacht traditiegetrouw liever op daders en slachtoffers dan op delicten, verlaat zich liever op gedragswetenschappelijke en sociale noties dan op technische voorzieningen. Gebrek aan kennis van de technologie leidt bovendien tot weerstand om optimaal gebruik te maken van nieuwe technologische mogelijkheden. Overigens mag niet onvermeld blijven dat ook technologen zich bepaald niet uitputten om de kloof met de dagelijkse (alfa)praktijk te overbruggen. Om de kloof te overbruggen kan justitie vier wegen bewandelen, die onder de noemers strategie, onderzoek, overleg en communicatie in de aanbevelingen uitgewerkt zullen worden.

5.2 Organisatorische barrières

- *Onvoldoende inbedding in de organisatie*

Zonder goede organisatorische inbedding zijn technologische maatregelen weinig zinvol. Camerabewaking in winkels bijvoorbeeld is bedoeld om de pakkans van overvallers te vergroten. Voor een herkenbare afbeelding van de overvaller is het noodzakelijk dat de camera op de juiste plaats geïnstalleerd wordt. In de praktijk blijken winkeliers de camera het liefst tegen het plafond te plaatsen, achterin de winkel, zodat zoveel mogelijk calamiteiten – variërend van winkeldiefstal en fraude tot agressieve klanten en overvallers – geregistreerd kunnen worden. Een onmogelijke combinatie die maakt dat er na een overval alleen een vage schim zichtbaar is, waarvan het gezicht zo klein is dat het niet voor identificatie of herkenning gebruikt kan worden. De organisatorische maatregelen strekken zich in dit voorbeeld niet alleen uit tot een goede plaatsing van de camera (bij voorkeur bij de ingang van de winkel), maar ook tot het beheer van het beeldmateriaal en de plaats van de recorder, opdat de overvaller er behalve met de buit niet ook met zijn 'eigen' videoband vandoor gaat.

- *Achterwege blijven van toezicht en handhaving*

Technologie is een hulpmiddel. Wanneer de opsporing verzuimt een adequaat vervolg te geven aan de informatie die middels de technologie verkregen wordt, boet de technologie in aan geloofwaardigheid en bruikbaarheid. Camera's op straat waarvan de beelden niet (continu) gemonitord worden, meldingen van alarmsystemen waarop niet (snel genoeg) gereageerd wordt en diefstalpreventiechips in scooters die niet met een tagreader afgelezen worden, zijn daar voorbeelden van.

5.3 Technische barrières

- *Gebrekkige prestaties van de technologie*

Niemand zal ervan uitgaan dat technologie een panacee is voor alle criminaliteitsproblemen. De mogelijkheden zijn groot, maar er moet wel rekening mee gehouden worden dat een nieuwe technologische toepassing niet oplevert wat je ervan had verwacht. Een voorbeeld is het alarmsysteem in voertuigen dat om de haverklap loeit, ook wanneer daartoe geen aanleiding is, en waaraan passanten inmiddels achteloos voorbijgaan.

- *Gebrek aan standaardisering*

Met name bij de introductie van nieuwe veelbelovende technologieën is het risico groot dat meerdere producenten de markt proberen te veroveren. Een voorbeeld is de introductie van tags tegen (brom)fietsdiefstal. Diverse producenten brachten tags op de markt, die elk gekoppeld waren aan hun eigen tagreader. Pas met de ontwikkeling van een multi-tagreader werd het probleem opgelost dat voor de opsporing van gestolen tweewielers zo'n zes verschillende tagreaders benodigd waren. Ook in de computerwereld is de incompatibiliteit van apparatuur van verschillende fabrikanten een bekend euvel.

5.4 Juridische barrières

- *Privacywetgeving*

Naarmate de mogelijkheden van de technologie groter worden, groeit ook de kloof tussen degenen die hechten aan de bescherming van bepaalde burgerrechten, waaronder de privacy, en degenen die voorrang willen geven aan het

waarborgen van de veiligheid. Het lijkt erop dat de balans thans langzaam in de richting van de veiligheidsadepten uitslaat. Dit blijkt bijvoorbeeld uit de toename van het cameratoezicht en uit het feit dat identificatie (bijvoorbeeld via biometrie, de digitale handtekening of DNA-analyse) een steeds belangrijker middel wordt om criminaliteit te voorkomen en misdadigers op te sporen. De privacy kan dan in het geding zijn. Bij het afwegen van de privacybelangen verschuift de aandacht van welke informatie bewaard mag worden naar hoe, door wie en voor wie deze informatie toegankelijk mag zijn. Dit vraagt om extra aandacht voor de beveiliging van de informatie én om het opstellen van standaarden, richtlijnen en procedures bestemd voor respectievelijk de overheid, het bedrijfsleven en non-profit organisaties.

- *Bescherming van copyright*

Veel technologische vindingen zijn beschermd door het copyright dat bij de geestelijke vader berust. Toepassing van deze technologie is dan aan (financiële) voorwaarden verbonden. Een voorbeeld is het Human Genome Project, waarbij het genetisch materiaal van de mens recent door een groep Britse en Amerikaanse wetenschappers in kaart is gebracht en waarop zij het patent hebben verkregen.

5.5 Ethische barrières

- *Verlies van de controle*

Technologische ontwikkelingen volgen elkaar in hoog tempo op. Dankzij de versnelling van het productieproces, de uitgekiende marketingstrategieën en efficiëntere distributienetwerken is technologie wereldwijd verkrijgbaar. Ook voor mensen met minder goede bedoelingen. De vraag doemt op of we nog wel voldoende greep hebben op de technologische ontwikkelingen.

- *Aantasting van de integriteit van het menselijk lichaam*

Technologie kan niet alleen gekoppeld worden aan dode objecten, maar ook ingebouwd worden in levende wezens. In de veeteelt is dit geen ongewoon verschijnsel. Wanneer echter het menselijk lichaam in het geding is, kan dit uitmonden in sterk afwerende reacties. Discutabel is bijvoorbeeld het implanteren van microchips als tracker en tracer in tbs'ers op proefverlof of recidiverende zedendelinquenten.

- *Big Brother*

Orwell schreef erover in zijn boek *1984*: de samenleving die geregeerd wordt door de technologie. Vaak wordt er verwezen naar het gevaar van het ontstaan van een Big Brother-maatschappij. Uit de Senter-evaluatie: "Het gebruik van technologie op het gebied van criminaliteit wordt door velen geassocieerd met een voorafschaduwing van een Orwelliaanse samenleving *where Big Brother is protecting you*." Overigens wordt hieraan meer gerefereerd dan dat men echt gelooft dat een dergelijke samenleving werkelijkheid zal worden.

6. Aanbevelingen

De verkenning naar de mogelijkheden en bedreigingen van de technologie voor de beheersing van de criminaliteit bracht de commissie tot de formulering van de volgende aanbevelingen.

1. Houd de technologische ontwikkelingen structureel in de gaten

De inzet van technologie bij de beheersing van de criminaliteit vergt structurele aandacht voor nieuwe ontwikkelingen en toepassingsmogelijkheden. Deze aandacht mag niet beperkt blijven tot het incidenteel inventariseren van technologis che mogelijkheden. De commissie beveelt aan om elke twee jaar in kaart te brengen welke technologie beschikbaar is en waar nieuwe technologische kansen liggen. Voor deze analyse is de systematiek die in het onderhavige rapport gevolgd is, zeer geschikt gebleken. Dit houdt dat:

a. in binnen- en buitenland geïnventariseerd wordt welke bestaande en/of veelbelovende technologieën voorhanden zijn voor de aanpak van: a. delicten die in termen van omvang, ontwikkeling, ernst, schade en perceptie een grote impact hebben op de samenleving (ernstige vormen van criminaliteit); b. delicten die niet of onvoldoende adequaat aangepakt worden (veelvoorkomende vormen van criminaliteit en overlast); c. delicten die een groot beslag leggen op de politie- en justitiecapaciteit (vereenvoudigen van routineklussen); d. delicten waarbij meer daders opgespoord kunnen worden via een technologische aanpak (verhoging van het oplossingspercentage).
b. op basis van de verkenning bepaald wordt welke technologieën het meest veelbelovend zijn om in eigen land geïntroduceerd te worden in termen van effectiviteit, efficiëntie, eerlijkheid en haalbaarheid.
c. bepaald wordt van welke veelbelovende technologie de overheid zelf de verdere ontwikkeling wil stimuleren en financieren.

2. Wees de beste imitator en excelleer op één terrein als innovator

Nederland is niet het enige land dat kampt met criminaliteitsproblemen waarvoor het oplossingen zoekt in de technologische hoek. Gebleken is dat er op internationaal niveau op een groot aantal terreinen dezelfde problemen en gedachten circuleren, maar dat er amper informatie over de (technologische) vorderingen uitgewisseld wordt. Mede vanwege het ontbreken van voldoende capaciteit, knowhow en financiële middelen moet ons land niet de pretentie hebben voor elk criminaliteitsprobleem zelf de technologische oplossing te willen ontwikkelen. De commissie beveelt dan ook aan zich vooral toe te leggen op informatie-uitwisseling en op het imiteren van veelbelovende en/of succesvolle buitenlandse technologische vindingen. Om op technologisch vlak niet geheel achter te blijven en 'in ruil' voor waardevolle informatie van andere landen dient ons land zich op één terrein als innovator te onderscheiden. Deze aanpak vergt enerzijds een regelmatige vorm van contact tussen (hoge) ambtenaren en hun *counterparts* in landen als de Verenigde Staten, Groot-Brittannië en Duitsland. De commissie stelt voor daartoe elke twee jaar een vergadering tussen de directeuren-generaal Rechtshandhaving of hun equivalenten te beleggen. Daarnaast moet een 'veiligheidsattachee' op de Nederlandse ambassade in de Verenigde Staten belast worden met het onder meer monitoren van en rapporteren over de technologische ontwikkelingen aldaar, omdat dit land voorop loopt in de ontwikkeling van nieuwe technologieën.

3. Excelleer de komende zes jaar in de ontwikkeling van gezichts- en patroonherkenning

Uit de verkenning van de technologische mogelijkheden bij de beheersing van de criminaliteit is de commissie gebleken dat gezichts- en patroonherkenning niet alleen een zeer veelbelovende technologie is, maar ook van groot nut voor tal van criminaliteitsterreinen, waaronder de aanpak van inbraak in woningen en bedrijven, de controle op wapenbezit, identiteitsfraude en het toezicht en de controle in de openbare ruimte. Wil Nederland zijn (bescheiden) ambitie als innovator waarmaken, dan heeft het de meeste kans van slagen, indien het zich concentreert op de verdere ontwikkeling van gezichts- en patroonherkenning. De commissie beveelt aan de inspanningen hierop te richten in de periode 2004-2010. De uitkomst dient op z'n minst te zijn dat bij gezichtsherkenning foute en gemiste *matches* gereduceerd worden tot minder dan 1% en dat bij patroonherkenning een signaalfunctie ontwikkeld is voor de detectie van inbraak, diefstal, beroving en geweld.

4. Prikkel industrie en wetenschap om te investeren in imitatie en innovatie

Ook wanneer de overheid haar rol bij de introductie van nieuwe technologieën zo veel mogelijk wil beperken tot imitatie en op een enkel terrein wil optreden als innovator, is ze voor de verwezenlijking van dit voornemen afhankelijk van de wetenschap en met name de industrie. Nu is het zo dat de bèta-wetenschap en industrie hun pijlen over het algemeen niet richten op de ontwikkeling en productie van technologie ten behoeve van de preventie en bestrijding van criminaliteit. Toch is de overheid sterk afhankelijk van hun expertise en medewerking. Ze zal dus mechanismen moeten identificeren

die ertoe leiden dat wetenschap en industrie geïnteresseerd raken in deze materie. Dit kan door interdisciplinaire netwerken op te richten en door interdisciplinaire onderzoeksprojecten – ook op EU-schaal – te starten. Daarnaast is een financiële prikkel om hen te stimuleren tot deelname onontbeerlijk. De commissie oppert drie mogelijkheden voor het financieel stimuleren van imitatie en innovatie:

- De eerste is de instelling van een (bescheiden) fonds waaruit geput kan worden voor het incorporeren van veelbelovende of succesvolle buitenlandse technologieën in het eigen productieproces. Een fonds kan niet alleen het beslissende zetje geven voor de overname van deze technologie, maar heeft ook als voordeel dat men zich meer bewust wordt van de behoefte aan technologische oplossingen voor criminaliteitsproblemen en dit vertaalt in eigen research naar mogelijk succesvolle buitenlandse technologieën.

- De tweede weg die bewandeld kan worden, is het belonen van bedrijven die zich inspannen om hun producten, diensten en systemen te beveiligen tegen criminaliteit door hen een lagere verzekeringspremie te laten betalen. Daartoe zouden per branche convenanten opgesteld moeten worden met de verzekeraars.

- De derde weg behelst het uitreiken van een jaarlijkse onderscheiding voor bedrijven en wetenschappers die zich aantoonbaar verdienstelijk hebben gemaakt bij de introductie van *crime-proof* producten, diensten en systemen. Een dergelijke *award* kan ondernemers stimuleren meer aandacht te besteden aan preventie en via de media meer bekendheid genereren voor de technologische mogelijkheden bij het beheersen van de criminaliteit. Voor de laureaten zal de positieve publiciteit ongetwijfeld haar nut bewijzen bij het opbouwen van een imago van betrouwbaarheid en maatschappelijk verantwoord opereren.

5. Rapporteer elke vier jaar welke resultaten bereikt zijn

Het is essentieel om de effectiviteit te meten in termen van reductie van de criminaliteit en/of vereenvoudiging van routineklussen en arbeidsintensieve processen. Dit vergroot het draagvlak voor technologische vernieuwing in de samenleving en meer in het bijzonder onder ambtenaren en politici. Afgezien daarvan is het – zeker nu de tijdgeest vraagt om resultaatgericht werken – überhaupt van belang te meten welke technologie goed werkt en in hoeverre bijstellingen gewenst zijn. De commissie beveelt aan om de vier jaar verantwoording af te leggen over de bereikte resultaten. Deze verantwoording dient gekoppeld te zijn aan de tweejaarlijkse verkenning, die in de eerste aanbeveling aan de orde gekomen is.

6. Besteed bij justitie stelselmatig aandacht aan technologie

Ter overbrugging van de kloof tussen de alfa- en gamma-georiënteerde justitieambtenaren en de bètawereld van de technologen doet de commissie de volgende aanbevelingen.

- Belast een strategische (beleids)unit met de taak elke vier jaar aandacht te besteden aan technologie

Justitie dient iedere vier jaar een strategie uit te stippelen voor de inzet van technologie bij het voorkomen en bestrijden van de criminaliteit. Deze strategie is zowel gebaseerd op de tweejaarlijkse verkenningen als op de effectrapportages. In deze strategische unit zitten ambtenaren van de directies Algemene Justitiële Strategie, Rechtshandhaving en Sanctie- en Preventiebeleid. Het spreekt vanzelf dat de departementsleiding de uitgestippelde strategie ten volle moet onderschrijven en in de praktijk moet willen verwezenlijken.

- Stel bij de start van nieuw onderzoek via het WODC standaard de mogelijkheden van de technologie aan de orde

Onderzoek naar de technologische mogelijkheden voor de beheersing van specifieke vormen van criminaliteit kan natuurlijk aan derden uitbesteed worden. Maar om de betrokkenheid van de justitieambtenaren te vergroten is het te verkiezen (een deel van) het onderzoek intern te verrichten. In het standaardformulier van het Wetenschappelijk Onderzoek en Documentatie Centrum (WODC) dat hoort bij de startnotitie voor het opzetten van nieuw onderzoek, dient ook expliciet aandacht te zijn voor de eventuele technologische mogelijkheden.

- Organiseer regelmatig discussiebijeenkomsten over technologie en criminaliteitsbeheersing

De derde weg die Justitie moet bewandelen, is bijeenkomsten organiseren waarin (beleids)ambtenaren, technologen en ervaren criminaliteitsbestrijders uit de praktijk discussiëren over specifieke criminaliteitsproblemen en de inzet van technologie. Aanleiding voor een dergelijke bijeenkomst kan een recent onderzoek van het WODC zijn, maar ook actuele trends en ontwikkelingen in de criminaliteit die gebaat zijn bij een technologisch antwoord.

- Besteed regelmatig aandacht aan de communicatie rond technologie

Regelmatig kond doen van de vorderingen van Justitie op het gebied van criminaliteit en technologie, successen én tegenslagen delen, is ten slotte de vierde pijler waarmee het technologiebewustzijn binnen de eigen organisatie vergroot kan worden. De tweejaarlijkse verkenningen en vierjaarlijkse effectrapportage vormen daarvoor een goede aanleiding, maar ook de vorderingen op het gebied van innovatie (gezichts- en patroonherkenning) komen ervoor in aanmerking.

7. Benoem een probleemeigenaar in de persoon van de directeur-generaal Rechtshandhaving

Ter voorkoming van versnippering van de inspanningen om technologie te incorporeren in het overheidsbeleid bij de bestrijding en preventie van criminaliteit moet een centraal coördinatiepunt aangewezen worden, van waaruit de visie op het beleid geformuleerd, gecoördineerd en uitgedragen wordt. Tevens zullen op een centraal niveau kansen en bedreigingen in kaart gebracht moeten worden en initiatieven ontplooid om veelbelovende of bewezen succesvolle (buitenlandse) technologieën te introduceren in de samenleving. Bijkomend voordeel is dat er een duidelijk aanspreekpunt komt voor ondernemers, wetenschappers en anderen. De commissie adviseert om de directeur-generaal Rechtshandhaving bij het ministerie van Justitie aan te wijzen als probleemeigenaar. Tot zijn verantwoordelijkheden behoren in ieder geval:

- de tweejaarlijkse verkenning van nieuwe (buitenlandse) technologische ontwikkelingen
- het innovatietraject, i.c. de ontwikkeling van gezichts- en patroonherkenning
- het onderhouden van relevante contacten, in het bijzonder met de internationale *counterparts* ter uitwisseling van informatie over technologische ontwikkelingen, de 'veiligheidsattachee' op de Nederlandse ambassade in de Verenigde Staten en waar nodig met de wetenschap en industrie
- het verankeren van het technologiebewustzijn in de justitieorganisatie
- de vierjaarlijkse rapportage van de behaalde resultaten

De directeur-generaal dient jaarlijks aan de ambtelijke en politieke leiding verslag uit te brengen van de ontplooide activiteiten op voornoemde terreinen.

8. Richt een netwerk Criminaliteit en Technologie op

Met de aanwijzing van een 'probleemeigenaar' mogen anderen zich niet ontslagen voelen van de verplichting zich om deze materie te bekommeren. Hun betrokkenheid en inbreng van expertise kan het beste gewaarborgd worden door de oprichting van een netwerk Criminaliteit en Technologie. Dit netwerk wordt minimaal één keer per twee jaar – voorafgaand aan het opstellen van de periodieke verkenning – geconsulteerd over de culturele, organisatorische, technische, juridische en ethische knelpunten bij de implementatie van nieuwe technologieën en de mogelijkheden deze te verhelpen. In het netwerk moeten in ieder geval de volgende organisaties vertegenwoordigd zijn:

- technologische 'experts' van politie- en justitiediensten, zoals het KLPD, het NFI en PIDS
- opsporingsdiensten als de FIOD/ECD, SIOD en AID
- de beveiligingsbranche
- commerciële dienstverleners zoals banken en verzekeraars
- producenten, publieke en private onderzoekers en adviesbureaus die zich bezighouden met de ontwikkeling van (nieuwe) technologie
- bèta-wetenschappers verbonden aan universiteiten en private onderzoeksinstituten
- private denktanks die zich bezighouden met innovatie
- opleidings- en trainingsinstituten die zich richten op de overdracht van technologische kennis en vaardigheden

Bijlagen

a) Samenstelling van de commissie Criminaliteit en Technologie

Leden van de commissie

dr. P. Winsemius (voorzitter), lid WRR
dr. R.J. van Duinen, voorzitter algemeen bestuur NWO
mr. I.W. Opstelten, burgemeester van Rotterdam
mr. D.W. Steenhuis, procureur-generaal
prof.dr.ir. B.P. Th. Veltman, oud-voorzitter AWT

Adviserende leden

mr.drs. C.W.M. Dessens, directeur-generaal Rechtshandhaving, ministerie van Justitie
drs. B.J.A.M. Welten, korpschef regiopolitie Groningen

Technologische ondersteuning

mr. G. Enthoven, directeur Instituut voor Maatschappelijke Innovatie
K. Roseboom, senior adviseur Instituut voor Maatschappelijke Innovatie

Ambtelijke ondersteuning

mevr. drs. J. Verschoor, clustercoördinator afdeling Criminaliteitspreventie, ministerie van Justitie (projectleider)
mevr. drs. I.L. van Erpecum, beleidsmedewerker afdeling Criminaliteitspreventie, ministerie van Justitie, secretaris
drs. R. Rijpkema, beleidsmedewerker directie Opsporingsbeleid, ministerie van Justitie, secretaris

b) Korte beschrijving van relevantie technologieën voor criminaliteitsbeheersing

1. Biometrie
Biometrie wordt gebruikt om personen te identificeren op basis van unieke lichaamskenmerken als vingerafdrukken, oorafdrukken, iris, handvorm, stem en verdeling van de gelaatstemperatuur. Deze technologie kan onder meer aangewend worden om mensen te autoriseren en toegang te verlenen tot beveiligde systemen, diensten en gebouwen.

Alcoholanalyse
De koppeling van biometrische systemen aan apparatuur voor alcoholanalyse, die op haar beurt verbonden is aan een startmechanisme voor auto's, voorkomt dat automobilisten die veroordeeld zijn voor rijden onder invloed met te veel alcohol in het bloed de weg op gaan.

Coating
Door draagbare en diefstalgevoelige apparaten te voorzien van een biometrische deklaag (coating) wordt voorkomen dat deze gebruikt kunnen worden door een ander dan de eigenaar. Eventueel kan de coating gekoppeld worden aan een alarmsignaal.

Gezichtsherkenning
De meest toegepaste vorm van biometrische identificatie is op dit moment de gezichtsherkenning. Bij deze techniek nemen digitale camera's een foto van een gezicht en worden de gefotografeerde gezichtskenmerken vergeleken met de kenmerken van personen die zijn opgeslagen in een database of op een smartcard. Gezichtsherkenning wordt onder meer toegepast voor toegangscontroles bij gebouwen, bij computerterminals waar gevoelige informatie ligt opgeslagen, bij transacties waar een hoog bedrag mee gemoeid is en bij geldautomaten. Ook op vliegvelden, in casino's en in gevangenissen wordt deze technologie ingezet. Een mogelijke toepassing is voorts het opsporen van illegale immigranten. Een bijzondere vorm van gezichtsherkenning is het *face in a crowd image capture system*, waarmee een gezicht dat op een videobeeld staat, snel gekoppeld kan worden aan een beeld dat is opgeslagen in bijvoorbeeld een database of smartcard. Een gezicht kan op deze wijze tot op 95% nauwkeurig geïdentificeerd worden.

Video-tracking
Onder video-tracking wordt verstaan: een persoon op basis van gezichtskenmerken met camera's volgen.

Vingerafdrukidentificatie
Middels deze technologie wordt de toegang tot een gebouw of systeem voorbehouden aan degenen die daartoe geautoriseerd zijn. In twee Australische ziekenhuizen bijvoorbeeld kunnen alleen de daartoe bevoegde artsen bij de patiëntendossiers, nadat ze hun vingerafdruk op elektronische wijze hebben laten scannen.

2. Biotechnologie
De biotechnologie maakt gebruik van de mogelijkheid om te interveniëren in biologische processen, waardoor optimalisatie van prestaties mogelijk wordt. Er kan zowel direct ingegrepen worden in het functioneren van mens en dier als indirect, bijvoorbeeld via de voedselketen. Deze technologie bestaat al eeuwen en is bekend van onder meer het enten en de kruisbestuiving van planten. Van recenter datum zijn de veredeling en de ontdekking, in 1953, van DNA als de genetische blauwdruk van elke levende cel.

Biologische (chemische) sensoren
Deze sensoren worden gebruikt voor de detectie en identificatie van eiwitten, bacteriën en virussen. De expertise is gericht op microbiologische wapens en toxinen. In de toekomst zouden mobiele sensoren ontwikkeld kunnen worden voor monitorings- en alarmsystemen.

Chromatografie
Deze analytische scheikundige techniek wordt gebruikt voor het chemisch scheiden van mengsel en substantieven.

DNA-onderzoek
Het DNA-onderzoek omvat het meten en analyseren van de kenmerken van DNA en het vergelijken van deze kenmerken met het soort, type en de eigenschappen van het DNA van specifieke personen.

DNA-testing (stofherkenning)
Twee categorieën worden over het algemeen bij DNA-testing onderscheiden. De eerste heeft betrekking op het vergelijken van DNA dat gevonden is op een slachtoffer of de plaats waar het delict gepleegd is, met dat van de mogelijke dader. De tweede categorie richt zich op micro-organismen (bacteriën, schimmels, virussen) en is van belang bij het detecteren van biologische wapens.

Mineralogie
De mineralogie bestudeert mineralen en in het bijzonder hun kenmerken, oorsprong en chemische classificatie, fysieke eigenschappen en kristallografie.

Serologie
Deze technologie wordt gebruikt voor de analyse van lichaamsstoffen.

Spectroscopie
Deze discipline richt zich op de kennis van licht en lichtverspreiding.

Toxicologie
De toxicologie omhelst de analyse van giftige stoffen.

3. Chemische technologie
De kennis van chemische stoffen en formules die gebruikt kunnen worden voor het analyseren van mogelijke sporen van daders en slachtoffers behoort tot het domein van de chemische technologie. Deze technologie wordt vooral gebruikt bij forensisch onderzoek ten behoeve van de opsporing van daders en slachtoffers.

4. Computertechnologie
Computertechnologie maakt gebruik van softwareprogramma's die de gebruiker in staat stellen een grote diversiteit aan taken uit te voeren, waaronder tekstverwerking, datacommunicatie, grafische producties, simulaties, opslag van gegevens en wiskundige berekeningen.

Beeldbewerking
De mens kan (deels) ontlast worden van intensieve observatieactiviteiten door de toepassing van beeldbewerking in combinatie met intelligente camera's en door gebruikmaking van een automatische selectie van beelden op basis van vooraf geformuleerde criteria als vorm, grootte, bewegingsrichting en kleur. De beeldbewerkingstechniek kan ook toegepast worden om de beeldkwaliteit te verbeteren en voor het stabiliseren van beelden opgenomen vanuit bewegende platforms, om zo te corrigeren voor trillingen en vliegbewegingen.

Digitale filtertechniek
Deze techniek omvat het elektronisch filteren van ingaande en uitgaande informatie, hetzij op basis van de inhoud van informatie, hetzij op basis van metadata. Bovendien is filtering op basis van profielen, modellen en normen mogelijk.

Kunstmatige intelligentie
In de breedste zin is kunstmatige intelligentie het genereren van digitaal probleemoplossend vermogen op een wijze zoals een menselijke gedachte werkt. Voor de beveiligingsbranche is kunstmatige intelligentie vooral van belang om snel verbanden te zien in complexe situaties.

Patroonherkenning
Patroonherkenning wordt toegepast voor het automatisch analyseren en opslaan van camera-, infrarood- of radarbeelden op de aanwezigheid van verdachte sociale situaties. Deze technologie bewijst vooral haar nut in situaties waarin een grote mensenmassa op de been is, zoals tijdens voetbalwedstrijden, en in het geval dat specifieke personen of objecten gevolgd moeten worden.

5. Data-opslagtechnieken
Systemen en diensten die het mogelijk maken een grote hoeveelheid informatie op te slaan en te raadplegen. Voor het opslaan van informatie zijn onder meer cd-rom's, dvd's en hologrammen beschikbaar. Datacentra (APS en de draadloze WASP) verhuren computerdiensten (rekenkracht), opslagdiensten en softwareapplicaties via het internet.

6. Displaytechnologie
Deze technologie maakt het mogelijk de werkelijkheid realistisch in beeld te brengen.

Augmented reality en augmented memory
Deze twee technologieën worden gebruikt voor het opvragen van relevante informatie zoals vergunningen, gegevens uit het kadaster en specificaties van giftige stoffen.
Cameratechnologie
Cameratechnologie maakt het mogelijk kleinere en goedkopere camera's te gebruiken die bovendien visuele beelden, infrarood en radar kunnen combineren. De camera's kunnen met beeldbewerking intelligent gemaakt worden.

Close-circuit television (CCTV)
Een netwerk van camera's schept een totaalbeeld van een geografisch begrensde ruimte.

Datafusie
Datafusie voegt informatie met verschillende kenmerken en/of kwaliteiten samen tot een gemeenschappelijk beeld. Datafusie speelt een rol bij waarnemingssystemen, bijvoorbeeld bij het samenvoegen van visuele beelden en infraroodbeelden, en bij de analyse van informatie over een persoon, situatie of voorwerp.

Virtual reality
Met behulp van computerbeelden creëert virtual reality een driedimensionale wereld waarin men zich zodanig kan bewegen dat het lijkt alsof men zelf in die wereld rondloopt. Met de muis wordt de loop- en kijkrichting aangegeven, alsmede de hoogte waarop het 'oog' zich bevindt: vlak boven de grond, op ooghoogte, hoog in de lucht en alles daar tussenin. De technologie maakt het onder meer mogelijk nieuwbouw op veiligheidsaspecten te toetsen.

7. Elektrotechniek
De meeste detectiesystemen maken gebruik van elektrotechniek. Datzelfde geldt voor toegangscontrolesystemen en sommige sluitsystemen.

Camerabewaking
Camera's zijn bestemd voor het observeren van een omgeving en de gebeurtenissen daarin. Het doel van de camera kan bijvoorbeeld zijn agressie te detecteren of snelheidsovertredingen. De gewenste kwaliteit van het beeld hangt af van de doelstelling. Voor identificatie zal een persoon prominent afgebeeld moeten zijn, voor alleen herkenning kan een persoon kleiner in het beeldveld zijn en voor alleen observatie kan het beeld nog kleiner zijn. De combinatie met sensoren biedt de gebruiker de mogelijkheid extra informatie te vergaren over de gebeurtenissen in het bewaakte gebied.

Domotica
Deze technologie omvat alle apparaten en infrastructuren in en rondom een woning die elektronische informatie benutten voor het meten, programmeren en sturen van functies ten behoeve van bewoners en verleners van diensten. De apparaten worden in de woning aangesloten op een communicatie-infrastructuur, die onderlinge uitwisseling van informatie mogelijk maakt. De bewoner, maar ook de dienstverlener, kan centraal (ook op afstand) alles bedienen. Binnen domotica wordt aandacht besteed aan beheersystemen en bewaking, telemetrie, verwarming, ventilatie en lichtmanagement, aan telewerken, teleshoppen en tele-educatie en ook aan entertainment-alarmering, privacy en zorg.

Inbraakalarmsysteem
Alarmsystemen worden gebruikt voor het detecteren van een persoon die binnendringt in een door middel van organisatorische, bouwkundige of elektronische maatregelen beveiligde omgeving. Hierbij kunnen elektronische sensoren gebruikt worden die reageren op c.q. gebruik maken van bijvoorbeeld geluid, infrarood, druk, trilling en temperatuur.

Tracking en tracing
Het op afstand volgen van personen en goederen is mogelijk door het aanbrengen van labels. Miniaturisering maakt het mogelijk in de toekomst vrijwel alles te registreren en te volgen. Een bijzondere vorm van tracking en tracing is de situatie dat een persoon gevolgd wordt op basis van eigen kenmerken en niet op basis van een label, bijvoorbeeld door gebruikmaking van gezichtsherkenning.

8. Groupware
Groupware stelt afzonderlijke, geografisch verspreide organisaties en personen wereldwijd in staat hun werkkracht te bundelen en verdiepen, bijvoorbeeld door online te discussiëren, gezamenlijk te schrijven aan documenten en elektronisch te vergaderen.

9. Informatietechnologie
Informatietechnologie zorgt ervoor dat computerprogramma's met elkaar gecombineerd kunnen worden. Zo is het mogelijk spreadsheets te importeren in tekstverwerkingsprogramma's. Hierdoor kunnen bijvoorbeeld verschillend ontworpen databanken toch onderling ontsloten worden.

10. Materiaaltechnologie
Materiaaltechnologie richt zich op materialen (muren, deuren, ramen, hekken, hang- en sluitwerk, textiel en andere stoffen) die de gebruikt worden om de veiligheid te bevorderen en criminelen te weren. Deze technologie is vooral op preventie gericht en dus niet zoals elektronische beveiliging op de detectie van de dader wanneer deze zich al op de plaats van het mogelijke delict bevindt.

Kogel- en meswerende materialen
Persoonlijke beschermingsmaterialen zoals kogelwerende vesten en helmen moeten voldoen aan normen die vastgelegd zijn in internationale standaards. Het vaststellen of aan deze beschermingseisen wordt voldaan, is een belangrijk onderdeel van het beoordelen van het ontwerp.

11. Nanotechnologie
Nanotechnologie behelst het construeren en inzetten van extreem kleine constructies, tot op moleculair niveau. In de (met name Amerikaanse) krijgsmacht wordt inmiddels geëxperimenteerd met zeer kleine robotjes (nanobots) voor bijvoorbeeld het uitvoeren van verkenningen. De technologie zou ook gebruikt kunnen worden voor zeer kleine camera- en afluistersystemen.

Miniaturisatie
Miniaturisatie is een verzameling van technieken die tot doel hebben een product kleiner te maken dan het thans is. Als zodanig vervult deze technologie een belangrijke rol in het proces van productontwikkeling. Door producten kleiner (en dus meestal lichter) te maken, kunnen ze geschikt gemaakt worden voor gebruik waar dit voorheen niet mogelijk was en kunnen producten gecombineerd worden, waardoor nieuwe toepassingsmogelijkheden ontstaan.

12. Netwerktechnologie
Netwerktechnologie maakt communicatie tussen onderling verbonden systemen mogelijk. De datacommunicatie verloopt hetzij via vaste verbindingen (glasvezel, koper, kapel), hetzij via draadloze verbindingen (radiofrequenties, optische technieken als laser en infrarood), of via water.

13. Neurologie
De kennis over de werking van de hersenen is het terrein van de neurologie. Technologische ontwikkelingen in dit vakgebied kunnen van belang zijn voor onder meer het voorkomen van agressief gedrag en het behandelen van verslaafden.

Brain fingerprinting
Deze nieuwe technologie is gebaseerd op de zogeheten MERMER (de Memory and Encoding Related Multifacetted Electroencephalographic Response), een reactie die ontstaat als de hersenen informatie verwerken die herkend wordt. Een dader die informatie voorgelegd krijgt die alleen hij kan kennen, zou dus een MERMER afgeven.

Brainmachines
'Hersenmachines' bestaan uit een bril met *light emitting diodes* – halfgeleiders die licht geven als er gelijkstroom doorheen geleid wordt – en een koptelefoon die geluidssignalen afgeeft. De audiovisuele prikkels werken zodanig op de hersenen, dat de gebruiker zich ontspant en creatiever en gezonder zou gedragen. De machine is bedoeld voor de behandeling van verslaafden.

Crowd control
Aangenomen wordt dat individuen in een mensenmassa anders functioneren dan wanneer ze alleen of in een kleine groep optreden. Zo kunnen zich 'deïndividuatie' en een verlaging van het 'zelfbewustzijn' voordoen in het gedrag. Wanneer sprake is van groepsdynamische processen is een andere aanpak vereist. De wijze van reageren varieert per type groep en vereist andersoortige sturing om de veiligheid te handhaven. Gedragsmodellen en –simulaties kunnen inzicht geven in het gedrag van grote groepen en optimale strategieën opleveren om bij grote groepen de orde te handhaven.

Magneto-encefalografie
Deze nieuwe technologie maakt preciezer en omvangrijker onderzoek in de hersenen mogelijk. Ze meet onder meer gamma-hersengolven, die ervaringen in het brein coördineren en in een zingevend kader plaatsen. Verstoring van deze hersengolven zou onder meer leiden tot zinloos geweld.

13. Real Audio en real video
Deze technologieën maken het mogelijk een geluids- of filmbestand direct te beluisteren c.q. te bezien via internet. Vooral de webcam begint thans bekendheid te krijgen.

14. Rekenkracht
Via snel beschikbare rekenkracht, waaronder *optical computing*, *DNA computing* en *crystalline computing*, worden activiteiten als beeldmanipulatie, spraaktechnologie, encryptie en het raadplegen van databanken geoptimaliseerd.

15. Spraaktechnologie
De spraaktechnologie maakt een grote hoeveelheid van nieuwe diensten mogelijk. Daartoe behoren onder meer het voeren van *realtime* gesprekken via het internet, het verstrekken van gesproken opdrachten aan apparaten en het direct omzetten van bijvoorbeeld afgeluisterde telefoongesprekken in getypte verslagen.

16. Wapentechnologie
Deze discipline houdt zich bezig met het ontwikkelen van wapens.

Less lethal weapons en non lethal weapons
Beide vormen een aanvulling op de traditionele wapenstok en het pistool in de uitrusting van de politie. Less lethal weapons zijn geschikt voor handhaving van de openbare orde en veiligheid in situaties waar geen zware criminaliteit te verwachten valt. Onder voorwaarden is het denkbaar dat ook anderen dan politiefunctionarissen deze wapens gebruiken.

17. Wiskundige technologie
Diverse technologieën zijn gebaseerd op methoden en technieken uit de wiskunde.

Compressietechnologie
Via deze methodiek wordt de omvang van informatiebestanden verkleind door het efficiënter structureren van de notatiewijze. Dat is vooral handig om grote hoeveelheden data, zoals beeldmateriaal en audiomateriaal, in de kortst mogelijke tijd over de beschikbare bandbreedte te sturen.

Encryptie
Encryptie is het proces waarbij berichten, informatie of data worden omgezet in een vorm die onleesbaar is voor iedereen die niet geautoriseerd is kennis te nemen van de verzonden informatie. Ze is dienstig voor het beveiligen van de onderlinge datacommunicatie voor derden.

Privacy enhancing technology
Deze technologie beoogt de private levenssfeer in de digitale wereld te waarborgen. Het systeem kan bijvoorbeeld bestaan uit een *anonymiser* of een *identity-protector.*

Steganografie
Via steganografie wordt informatie verborgen door de inzet van middelen als onzichtbare inkt, microscopisch klein schrift, geheimschrift of – in de digitale wereld – het onzichtbaar verweven van het ene digitale bestand in het andere digitale bestand. Dat laatste is vooral nuttig om bij digitale opnamen van gesprekken snel bepaalde woorden te kunnen terugvinden.

Waarmerken
Een uniek en beveiligd kenmerk om een informatiedrager te identificeren. Vertrouwen blijkt zeer belangrijk in de digitale economie. Men moet soms immers de echtheid van elektronische transacties, verklaringen en documenten kunnen verifiëren. Een waarmerk van echtheid in de vorm van encryptie via een digitaal certificaat of een digitale handtekening kan daarvoor garanties geven.

c) Geraadpleegde bronnen

- C. Adams en R. Hartley: *Property crime reduction through the use of electronic tagging systems.* The Chipping of Goods Initiative, Home Office Police Scientific Branch, 2001.
- F. Albeda, J. van Heeswijk en G. Enthoven: *Evaluatie T&S Criminaliteitspreventie*. Den Haag, Senter, 2003.
- P.S. Anton, R. Silberglitt en J. Schneider: *The global technology revolution, 2015.* RAND, National Defense Research Institute, 2001.
- 'Bemoeizucht onder de kap'. In: *de Volkskrant*, 23 november 2002.
- G.J.N.Bruinsma, H.G. van de Bunt en I.H. Marshall: *Met het oog op de toekomst*. Rotterdam, Adviesraad voor het Wetenschaps- en Technologiebeleid, 2001.
- H.H. Burger: *Het koppelen van technologie, trend en beleid in DGOOV: een proefinstrument*. Den Haag, TNO, 2001.
- H.H. Burger: *Samenvatting van de uitvoering van een technologieverkenning ter ondersteuning kennisbehoefte BZK/DGOOV*. Den Haag, TNO, 2001.
- Crime Prevention Panel: *Just around the corner. A consultation document*. Foresight, 1999.
- Crime Prevention Panel: *Turning the corner*. Foresight, 2000.
- Crime Prevention Panel: *Foresight Futures 2020*. Foresight, 2002.
- DSP: *Technologieverkenning Integraal Veiligheidsprogramma*. Den Haag, Senter, 2000.
- Engineering and Physical Science Research Council: *Research landscape 2001-2002*. EPSRC, 2001.
- *Gaat de justitiewetgever adequaat en consistent om met de ontwikkelingen in de techniek? Verslag van het vijfde symposium van de Directie Wetgeving*. Den Haag, Ministerie van Justitie, 2001.
- J. Grijpink: 'Biometrie en privacy'. In: *Privacy & Informatie* 6, 2000.
- J. Grijpink: *Keteninformatisering*. Den Haag, SDU Uitgevers, 2002.
- H. van Hoof en G.P. van Voorthuijsen: *Handreiking cameratoezicht.* Senter, TNO-FEL, 2000.
- H. van Hoof: *Intern verslag van de 16th SPIE AeroSense*. TNO/FEL, 2002.
- Hunt, C. Tillery en N. Wild: 'Through-the-wall surveillance technologies'. In: *Corrections today*, 2001.
- Institute of Physics: *Physics and foresight. Science in our lives*. Londen, 1999.
- L. Mockensturm: 'From the lab to the field with facial recognition'. In: *Corrections today*, 2002.
- Openbaar Ministerie: *Goed beschouwd. Jaarverslag 2001*. Den Haag, Openbaar Ministerie, 2002.
- J.E. Pekema: *Oplossing voor de breinbreker. Onderzoek naar stimuleringsregelingen voor criminaliteitspreventie*. Den Haag, Ministerie van Justitie, 2003.
- D.L. Perry: *Report on benchmarking of 'hard science' research directed towards crime prevention*. Foresight Crime Prevention Panel, Science and Technology Task Force, 2002.

- PMSEIC Working Group on Science, Crime Prevention and Law Enforcement: *Science, crime prevention and law enforcement*. Prime Minister's Science, Engineering and Innovation Council, 2000.
- PMSEIC Working Group on Science, Crime Prevention and Law Enforcement: *Science and Security*. Prime Minister's Science, Engineering and Innovation Council, 2002.
- Projectgroep Opsporing, Raad van Hoofdcommissarissen: *Misdaad laat zich tegenhouden. Advies over bestrijding en opsporing van criminaliteit. Visiedocument*. 2001.
- H. Schmeets en F. Otten: 'Nieuw bevolkingsonderzoek van CBS: criminaliteit nationaal probleem nummer één'. In: *SEC* 1, 1998, pp. 5-7.
- W. Schwabe, L.M. Davis en B.A. Jackson: *Challenges and choices for crime-fighting technology. Federal support of state and local law enforcement*. RAND, Science and Technology Police Institute, 2001.
- Senter Technologie & Samenleving: *Technologie voor morgen*. Den Haag, 1999.
- B. Smith en T. Tolman: 'Can we talk? Public safety and the interoperability challenge'. In*: National Institute of Justice Journal*, 2000.
- T. Thijssen en V. de Pous: *Kansen zien, kansen benutten. Technologie-innovatie en de beveiligingssector. Een studie met specifieke aandacht voor de internettechnologie*. Den Haag, Senter, 2001.
- Turner en D. Blackburn: 'Biometrics: separating myth from reality'. In: *Corrections today*, 2002.
- U.S. Department of Justice: *Video surveillance equipment.* The National Institute of Justice, 1999.
- U.S. Department of Justice: *Guide for the selection of drug detectors for law enforcement applications.* The National Institute of Justice, 2000.
- U.S. Department of Justice: *Guide to the technologies of concealed weapon and contraband imaging and detection*. The National Institute of Justice, 2000.
- U.S. Department of Justice: *An introduction to biological agent detection equipment for emergency first responders.* The National Institute of Justice, 2001.
- U.S. Department of Justice: *Guide for the selection of personal protective equipment for emergency first responders.* The National Institute of Justice, 2002.
- U.S. Department of Justice: *Using DNA to solve cold cases.* The National Institute of Justice, 2002.
- J. de Waard en H. Willemse: 'In de schaduw van het strafrecht'. In: *SEC* 3, 1999, pp. 16-18.
- C. Yeoman: *Crime reduction through technologie*. Londen, Home Office Research Development and Statistics Directorate, 2001.
- R.A. Yim: *National preparedness. Integrating new and existing technology and information sharing into an effective homeland security strategy*. Testimony before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives. GAO, 2002.
- ZW3 Communicatie: *Alfa en bèta. Technologie en criminaliteitspreventie bij gemeenten*. Den Haag, Senter.