TECHNOLOGIE VOOR TERRORISME-BESTRIJDING

TNO innovation for life

Overzicht van technologiegebieden om de gezamenlijke aanpak van contra-terrorisme, extremisme en radicalisering te versterken.

TECHNOLOGIE VOOR TERRORISMEBESTRIJDING
Overzicht van technologiegebieden om de gezamenlijke aanpak van contra-terrorisme, extremisme en radicalisering te versterken

COLOFON

Deze publicatie is opgesteld in het kader van het Vraaggestuurd Programma Veilige Maatschappij, een programma dat TNO uitvoert onder regie van het Ministerie van Justitie en Veiligheid om structureel kennis te ontwikkelen voor toekomstige vraagstukken.

AUTEURS
Ingrid Weima
Anneke Schwedersky
Hans van Vliet
Jeroen van Rest

VORMGEVING
Jennifer van Oers-Keek, Coek Design

DRUK

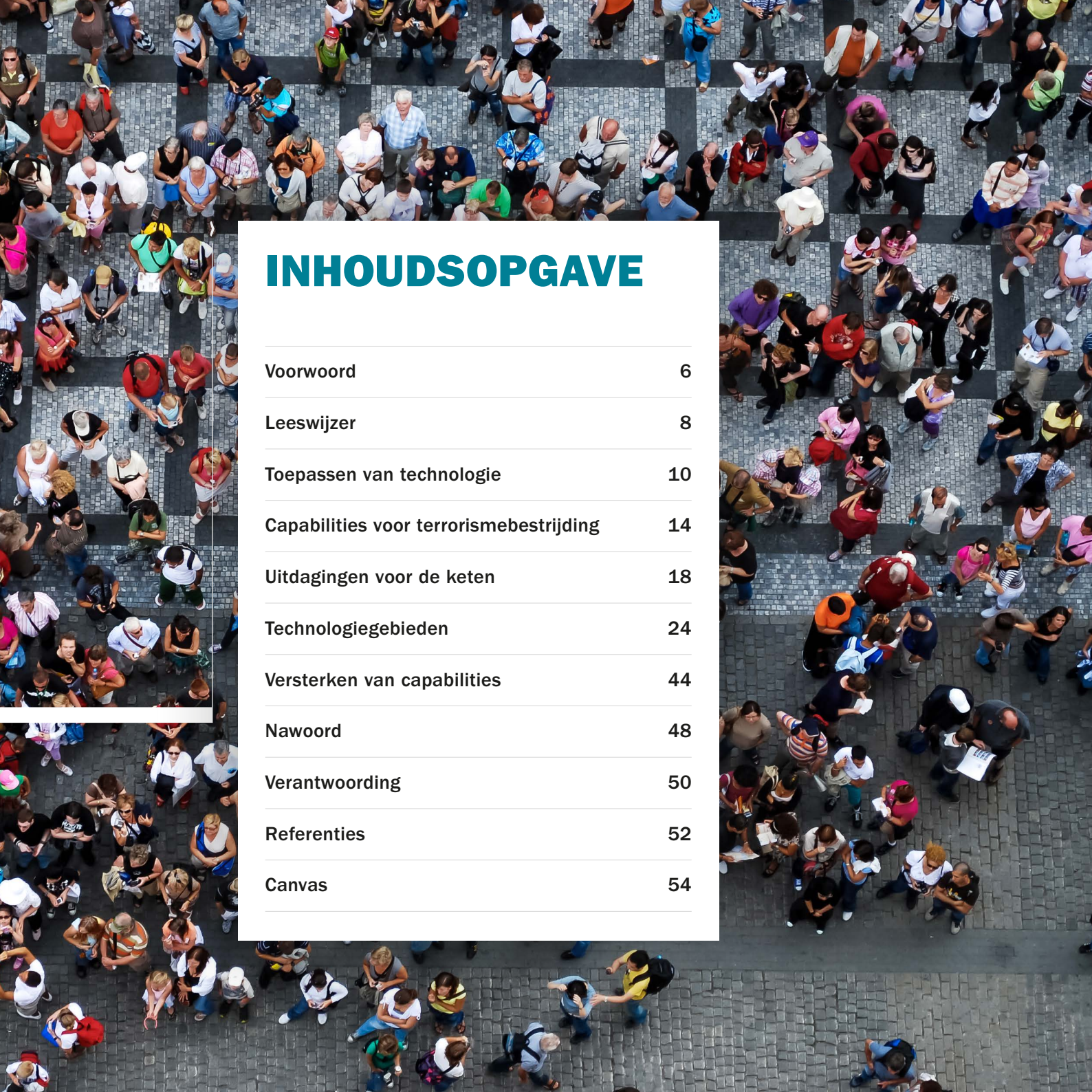
De huidige dreiging vraagt om ontwikkeling van oplossingen voor de korte maar vooral ook de langere termijn. Daarvoor is niet alleen de inzet van de mens nodig, maar ook ondersteunende technologie.

WAAROM EEN OVERZICHT VAN TECHNOLOGIE VOOR TERRORISMEBESTRIJDING?

- Omdat het huidige dreigingsbeeld in Nederland (en het buitenland) vraagt om aandacht voor ontwikkeling van oplossingen voor de korte maar vooral ook de langere termijn. Daarvoor is niet alleen de inzet van de mens nodig, maar ook ondersteunende technologie.
- Omdat de grenzen van de bestaande *capabilities* snel worden bereikt en ook behoefte is aan nieuwe *capabilities* als antwoord op de complexiteit van terrorismebestrijding.
- Om meer inzicht te krijgen in technologie en combinaties daarvan voor verschillende uitdagingen van de terrorisme-bestrijdingsketen.
- Om de kennis- en technologieontwikkeling voor de aanpak van terrorisme in Nederland sterker te agenderen. TNO wil hiermee bijdragen aan een gericht en samenhangend programma op dit gebied, dat ook proactief vooruitkijkt.

HOE KAN HET OVERZICHT VAN TECHNOLOGIE VOOR TERRORISMEBESTRIJDING WORDEN GEBRUIKT?

- Als handvat voor partners in de keten van terrorismebestrijding voor het verkrijgen van inzicht in de relevante technologieën om op (door-) te ontwikkelen;
- Als handvat bij het opzetten van samenwerkingen tussen partners in de keten, kennis- en technologieinstituten en andere relevante organisaties;
- Dit handvat kan worden gebruikt voor alle partners in de keten van terrorisme-bestrijding. Voor zowel publieke als private organisaties.



INHOUDSOPGAVE

INTRODUCTIE

Dit overzicht van technologie is bedoeld om de gezamenlijke aanpak van contra-terrorisme, extremisme en radicalisering (CTER) te versterken. Het is een eerste aanzet vanuit TNO om technologieontwikkeling te agenderen bij samenwerkende overheden en (veiligheids)organisaties en om inzichtelijk te maken wat mogelijk is binnen de aanpak van CTER, en waar op doorontwikkeld kan worden. Het overzicht richt zich met name op de **kansen** van technologie, daarbij niet uit het oog verliezend dat technologie ook een dreiging kan vormen door de wijze waarop deze door kwaadwillenden kan worden ingezet en dat technologie ook niet een oplossing is voor alles.

Terrorismebestrijding is al jaren een geprogrammeerd onderwerp binnen de kennisopbouw van TNO. TNO wil haar kennis (over technologie in brede zin) dichter bij toepassing door overheidsorganisaties, operationele diensten en bedrijfsleven brengen, en hun innovatievermogen versterken; met name als het gaat om organisatie-overstijgende netwerken, informatie uitwisselen en samenwerken, met integrale aandacht voor value-based design (zoals ethical by design, privacy by design). Het veranderende dreigingsbeeld, de ontwikkelingen op het gebied van CTER en trends in de maatschappij vragen hierom.

Begin 2015 zijn door het kabinet extra structurele maatregelen genomen die in het bijzonder een impuls hebben gegeven aan de capaciteit van de veiligheidsdiensten (Rutte, 2015). Er lijkt voornamelijk geïnvesteerd te zijn in nieuwe maatregelen, wetgeving en menskracht en nog weinig gericht op technologische ontwikkelingen. Om deze inzet, en specifiek de xinzet van de mens te versterken, kan zowel kennis over technologietoepassing als technologieontwikkeling bijdragen aan ondersteuning aan de huidige capaciteiten. Het is daarom essentieel om kennis en technologie meer centraal te stellen en meer samenhang aan te brengen in reeds aanwezige, maar veelal verdeelde ontwikkelingen op het gebied van CTER.

Dit overzicht van technologie is geen klassieke technologie-verkenning. Om het doel te bereiken om technologie dichter bij de toepassing te brengen is bij het ontwikkelen van dit overzicht gekeken naar de toepassing op het gebied van CTER; kortom de bijdrage en de kansen die ontwikkeling van een bepaalde technologie of (meestal een combinatie van technologieën) kan leveren op het gebied van CTER. Het overzicht van technologie bestaat uit acht technologiegebieden, waarbij ieder technologiegebied bestaat uit diverse technologietoepassingen die nuttig zijn om de keten van contra-terrorisme, extremisme en radicalisering te versterken.

VOORWOORD

In september 2018 overhandigde een Nederlandse delegatie, bestaande uit koningin Maxima, premier Rutte, de minister van Buitenlandse Zaken Blok en de Nationaal Coördinator Terrorismebestrijding en Veiligheid Schoof, het Travel Information Portal (TRIP) aan de VN. Dit door Nederland ontwikkelde opsporingssysteem vormt een goed voorbeeld van hoe technologie kan bijdragen aan de bestrijding van terrorisme en de bevordering van veiligheid.

Het TRIP wordt ingezet om zogenoemde Passenger Name Record (PNR) gegevens te analyseren op reisbewegingen van terroristen en internationale criminelen. Deze PNR-gegevens komen beschikbaar bij het boeken van tickets. Met behulp van de analyse ervan kunnen personen worden gesignaleerd en, zo nodig, worden tegengehouden nog voordat zij vertrekken of terugkeren. Met de overhandiging van het opsporingssysteem aan de VN is dat nu wereldwijd toepasbaar.

Dat betekent echter niet dat het terrorisme hiermee de voet definitief is dwars gezet. Hoewel er hoopgevende ontwikkelingen zijn, zoals in Syrië en Irak waar jihadisten steeds meer door hen beheerst grondgebied verliezen, moeten we waakzaam en alert blijven. Het jihadisme gaat in toenemende mate weer ‘ondergronds’ waarbij aanslagen en liquidaties als openlijke manifestaties ervan nog immer voortduren. Het recent verschenen Dreigingsbeeld Terrorisme Nederland 50 toont dat ook voor Nederland de kans op een aanslag nog reëel is. De recente aanslag in Utrecht onderstreept dat.
Hoewel de groei van de Nederlandse jihadistische beweging stagneert en zij momenteel meer nadruk legt op propaganda en werving dan het ten uitvoer brengen van gewelddadige intenties, is deze beweging toch vele malen groter dan vóór de uitbraak van de oorlog in Syrië. Dit maakt dat de jihadistische dreiging in Nederland nog steeds aanwezig is.

Door deze aanhoudende substantiële dreiging is het noodzakelijk dat we blijven investeren in maatregelen en daarbij de mogelijkheden die de toepassing van nieuwe technologieën ons bieden optimaal te benutten. Alleen wanneer concrete invulling wordt gegeven aan het streven om aanslagen te voorkomen en de gevolgen van aanslagen die desondanks gepleegd worden zoveel mogelijk te mitigeren, kan dit streven succes dragen. Dit betekent echter niet dat de ethiek met betrekking tot de inzet van nieuwe technologische middelen over het hoofd moet worden gezien. Integendeel: gezien het

geregeld intrusieve karakter ervan zal telkens moeten worden afgewogen of de inzet ervan proportioneel, ethisch gerechtvaardigd en juridisch geborgd is.

In dit kader is de onderhavige technologieagenda van TNO een nuttige stap. Deze agenda is opgesteld vanuit het Vraaggestuurd Programma Veilige Maatschappij (2018) om meer inzicht te bieden in de kansen en mogelijkheden die technologieontwikkeling en –toepassing bieden ten behoeve van de versterking van de CTER-capaciteiten. De agenda maakt daarnaast transparant wat de mogelijkheden van de technologische toepassingen in het kader van CTER kunnen zijn of zijn, en faciliteert daarmee de discussie over de condities waaronder de ontwikkeling en/of inzet ervan verantwoord en gerechtvaardigd zijn. Met stappen als deze zullen we beter in staat zijn om tot een gewogen inzet van nieuwe technologieën te komen die helpen bij het voorkomen van aanslagen en mitigeren van de gevolgen van de aanslagen die desondanks plaatsvinden.

PATRICIA ZORKO
Plaatsvervangend Nationaal Coördinator Terrorisme-bestrijding en Veiligheid en Directeur Cyber Security

LEESWIJZER

Een *capability* is het vermogen van een organisatie om in en gedurende een bepaalde periode met de haar beschikbare personele en/of materiële middelen de betreffende taak of functie adequaat uit te voeren.

CYBER-TECHNOLOGIEËN

DATA TECHNOLOGIEËN

BESLIS-ONDERSTEUNING EN COÖRDINATIE TECHNOLOGIEËN

LEER- EN ANTICIPATIE-TECHNOLOGIEËN

Een technologiegebied is een cluster van verschillende technologietoepassingen, waarmee CTER-*capabilities* in de keten kunnen worden vergroot, versterkt of ontwikkeld.

UITDAGINGEN VOOR DE KETEN

2

De aanhoudende dreiging van terrorisme stelt de keten van terrorismebestrijding voor aanzienlijke uitdagingen en zorgt voor behoefte aan duurzaam inzetbare capaciteit.

- **VOORKOMEN**
- **BESCHERMEN**
- **REAGEREN**
- **OPSPOREN EN VERVOLGEN**
- **HERSTELLEN**

TECHNOLOGIE

TECHNOLOGIE IS NIET DE OPLOSSING VOOR ALLES, MAAR VEILIGHEIDS-ORGANISATIES KUNNEN ER NIET MEER OMHEEN.

TOEPASSEN VAN TECHNOLOGIE

In dit hoofdstuk wordt beschreven hoe in deze publicatie tegen het toepassen van technologie aan wordt gekeken voor het versterken van contra-terrorisme, extremisme en radicalisering. Er wordt kort ingegaan op technologie als kans en als dreiging en ingegaan op de ethiek van het ontwikkelen en toepassen van technologie voor terrorismebestrijding.

TECHNOLOGIE ALS KANS EN ALS DREIGING

Terrorisme en de bestrijding daarvan verandert onder andere door technologie. Innovatie en adaptiviteit speelt aan beide zijden een grote rol. Technologie kan zowel worden gebruikt aan de kant van de kwaadwillenden als aan de kant van de betrokken overheidsinstanties (en betrokken private partijen) om terrorisme, extremisme en radicalisering te bestrijden. Dit betekent dat (gebruik van) technologie zowel kansen biedt als gevaren met zich mee kan brengen.

Technologische ontwikkelingen dragen bij aan nieuwe modus operandi waardoor het continu noodzakelijk is om te kunnen anticiperen en adaptief te zijn om een aanslag tijdig te voorkomen of te verhinderen.

Inzicht in – zich ontwikkelende – (potentiële) nieuwe vormen van (technologische) dreigingen is nodig om hier proactief op in te kunnen spelen en op voor te kunnen bereiden. Het gaat bijvoorbeeld om de risico's van technologieën als: biologische agentia, kunstmatige intelligentie, onbemande systemen en het Internet of Things. Voor het feit dat terroristen met drones een aanslag kunnen plegen, waarschuwde de NCTV al in 2017 (RTL nieuws, 2017). Ook zijn terroristen al actief in het cyberdomein (AIVD, 2018b).

In de modus operandi, de manier van werken van kwaadwillenden, kan technologie worden ingezet (technologie als dreiging). Eveneens kan dezelfde technologie door veiligheidsorganisaties (technologie als kans) worden ingezet. Een voorbeeld hiervan is de ontwikkeling op het gebied van sociale media. Voor de veiligheidsorganisaties zijn op dit gebied de kansen groot, zo kunnen meer gedetailleerde sociale netwerk analyses worden uitgevoerd en kunnen verdachten makkelijker worden opgespoord. Echter ontstaan ook gevaren door de ontwikkelingen op dit gebied. Zo kunnen (geradicaliseerde) personen elkaar bijvoorbeeld makkelijker vinden, kennis uitwisselen en is het ook makkelijker om nep-nieuws en propaganda te plaatsen.

ETHIEK BIJ TECHNOLOGIETOEPASSING

Als het gaat over het ontwikkelen en toepassen van (nieuwe) technologie voor terrorismebestrijding, bestaan belangrijke ethische argumenten om daar voorzichtig, zelfs terughoudend mee te zijn. Ethiek is het kennisgebied over moraliteit: over de vraag wat goed en fout is. Zoals, wat voor de één een terrorist is, is voor de ander een vrijheidsstrijder. Daarnaast, het bestrijden van terrorisme heiligt níet alle middelen: terrorismebestrijding impliceert een verantwoordelijkheid om beschikbare middelen proportioneel in te zetten. En ten slotte, de Nederlandse staat heeft vanuit de theorie van ethiek een

'actieve' verantwoordelijkheid om krachtige *capabilities* niet in verkeerde handen te laten vallen. Dat betekent dat de overheid van te voren een standpunt dient in te nemen, continu gevoed vanuit een maatschappelijk debat over de vraag "Wat voor samenleving willen we zijn?"

Maar er is aan de andere kant ook een ethisch argument om stimulerend te zijn over toepassing van technologie voor terrorismebestrijding. De overheid heeft namelijk ook een ethische actieve verantwoordelijkheid om er voor te zorgen dat nieuwe technologie ook daadwerkelijk operationeel inzetbaar is als de situatie daar om vraagt, en dat eindgebruikers op dat moment getraind zijn om het verantwoord in te zetten. En om het ontwikkelen van betere maatregelen en technologie (bijv. meer proportioneel, kosten-effectief of flexibel) te stimuleren en faciliteren. Inzet van nieuwe technologie voor terrorismebestrijding vereist dus dat besluitvorming op allerlei aansturingsniveaus ook voldoet aan ethische principes. Dat gaat om veel meer dan alleen de vraag of een bepaalde inzet van middelen wel of niet gepleegd moet worden: deze actieve verantwoordelijkheid vereist pro-actie, van te voren zien aankomen dat er een ethische afweging aan zit te komen (NCTV, 2018).

Naast pro-actie is ook samenwerking nodig tussen bestuurlijk verantwoordelijken, eindgebruikers en degenen die de nieuwe technologie realiseren. Op basis van het beginsel van *separatisme* wordt verondersteld dat de ethische verantwoordelijkheden van ingenieurs, van eindgebruikers en van politici gescheiden zijn (van de Poel & Royakkers, 2011). Politici en de hen ondersteunende beleidsmakers zijn verantwoordelijk voor het stellen van de doelen en randvoorwaarden van een nieuwe interventie, en voor het ter beschikking stellen van de daartoe benodigde middelen. Ingenieurs zijn verantwoordelijk voor de realisatie en technisch correcte werking, en eindgebruikers beslissen over het daadwerkelijk gebruiken ervan. Op basis van dit beginsel kunnen eindgebruikers redeneren dat indien middelen hen ter beschikking zijn gesteld door politici, het toch zeker de bedoeling is dat zij ook gebruikt worden. En ingenieurs kunnen redeneren dat zij toch niet verantwoordelijk kunnen worden gehouden voor het (verkeerd) gebruiken van technologie. Het is evident dat deze redeneringen geen serieuze ethische toets doorstaan, en dat inhoudelijke samenwerking essentieel is, en zo vroeg mogelijk begonnen dient te worden om te voorkomen dat eventueel onethisch gehandeld wordt.

Om in een vroegtijdig stadium van nieuwe (technologische) ontwikkelingen, beleid of werkwijzen na te denken over ethiek, privacy en data-protectie zijn ontwerpprincipes als *value- sensitive-design*, zoals *ethics-by-design, privacy-by-design, security-by-design* en *data-protection-by-design* ontstaan. Deze ontwerpprincipes zijn in de jaren negentig opgekomen als reactie op grote ICT-projecten in het maatschappelijk domein, die in (te) late fase fors moesten worden bijgestuurd, gestopt of zelfs teruggedraaid (van Rest, Boonstra, Everts, van Rijn, & van Paassen, 2014). Het gaat hierbij om het idee dat menselijke waarden gedurende de hele levensduur – dus ook vanaf het eerste begin- moeten worden meegenomen. Elementen uit dit gedachtegoed - met name over data bescherming - zijn terug te vinden in de nieuwe privacy richtlijn en verordening, welke een prikkel geven om daar dus vroegtijdig aan te denken. Echter, het is totaal onduidelijk wat *data-protection-by-design* precies betekent

voor terrorismebestrijding, laat staan het meer abstracte *ethics-by-design*. Europese projecten zoals bijvoorbeeld *Tactical Approach to Counter Terrorists in Cities* (TACTICS) hebben daar wel een aanzet toe gegeven (TACTICS, 2012). Ook heeft afgelopen jaar de Verenigde Naties een compendium uitgebracht over het gebruik van gezichtsherkenning voor terreurbestrijding (CTED & UNOCT, 2018). Maar dit waren slechts invullingen voor zeer specifieke onderdelen van contra-terrorisme, en waarvan het niet duidelijk is in welke mate de uitwerkingen voldoende gevalideerd zijn in de Nederlandse (beleids)context en samenleving.

Het vraagstuk van het ontwikkelen en gebruiken van nieuwe technologie voor terrorismebestrijding vereist een pro-actieve aanpak waarin bestuurders, eindgebruikers en technisch specialisten samenwerken aan een zich voortdurend verder ontwikkelend ethisch raamwerk. *Value-sensitive-design* biedt een goed uitgangspunt voor een dergelijke aanpak, maar het is inherent aan ethiek dat het voortdurend aandacht behoeft en niet kan vervallen tot statische checklists die uitbesteed kunnen worden.


TERRORISME EN BESTRIJDING DAARVAN VERANDEREN DOOR TECHNOLOGIE. DAAROM SPELEN INNOVATIE EN ADAPTIVITEIT EEN GROTE ROL.

CAPABILITIES VOOR TERRORISMEBESTRIJDING

Het versterken van de aanpak van contra-terrorisme, extremisme en radicalisering vereist bepaalde *capabilities*. Een *capability* is het vermogen van een organisatie om in en gedurende een bepaalde periode met de haar beschikbare personele en/of materiële middelen de betreffende taak of functie adequaat uit te voeren. Een *capability* kan worden beschreven vanuit verschillende perspectieven, zoals: organisatie, proces, informatie, technologie en mens. Technologie kan bijdragen om deze *capabilities* te vergroten, te versterken of te vernieuwen (zie figuur 1) en daarmee de keten van terrorismebestrijding te versterken.

Het huidige dreigingsbeeld in Nederland (NCTV, 2018a) vraagt om aandacht voor ontwikkeling van oplossingen voor de korte en de langere termijn. De grenzen van de huidige aanpak van de keten van CTER worden snel bereikt mede door de complexiteit van terrorisme en aanhoudende dreiging daarvan, waardoor de behoefte aan nieuwe aanpakken ontstaat. Dit vereist sterkere, grotere of nieuwe *capabilities*. Daarvoor is naast inzet van de mens ook ondersteunende technologie nodig. Technologie is niet de oplossing voor alles, maar veiligheidsorganisaties kunnen niet meer om technologie heen.

Het is de kunst te identificeren welke technologieën van belang zijn en daar tijdig afwegingen in te maken, zeker omdat technologieontwikkelingen tijd en geld kosten. Voor technologie ontwikkeling is het van belang dat enerzijds duidelijk is wat de ambitie is op de verschillende *capabilities* voor terrorismebestrijding, en anderzijds wat de (technologische) mogelijkheden zijn. Dit vereist echter dat er goed zicht is op de *capabilities* die nodig zijn voor het versterken van de keten van terrorismebestrijding en respectievelijk de *capability*-gap, het gat tussen de ambitie en de mogelijkheden. Hieronder wordt verder ingegaan op de benodigde *capabilities* voor CTER als basis voor het verder kunnen identificeren van relevante technologieën, waarmee uiteindelijk de keten van terrorismebestrijding versterkt kan worden.

FIGUUR 1
Versterken van de keten door middel van technologieontwikkeling

CAPABILITIES IDENTIFICEREN

Het identificeren van de benodigde *capabilities* is iets dat regelmatig dient te gebeuren met alle betrokken organisaties op basis van ontwikkelingen in dreigingen voor de Nationale Veiligheid. Het in kaart brengen en kwalificeren (*capability-assessment*) van deze *capabilities* helpt richting te geven en focus aan te brengen in de benodigde (technologische) ontwikkelingen: welke *capabilities* moeten verder gebracht worden om ons voor te bereiden op de volgende generatie dreigingen en met de ontwikkeling van welke technologieën die daar aan bijdragen moeten we nu al beginnen? Daarnaast kunnen veel (technologische) middelen voor meerdere *capabilities* worden ingezet.

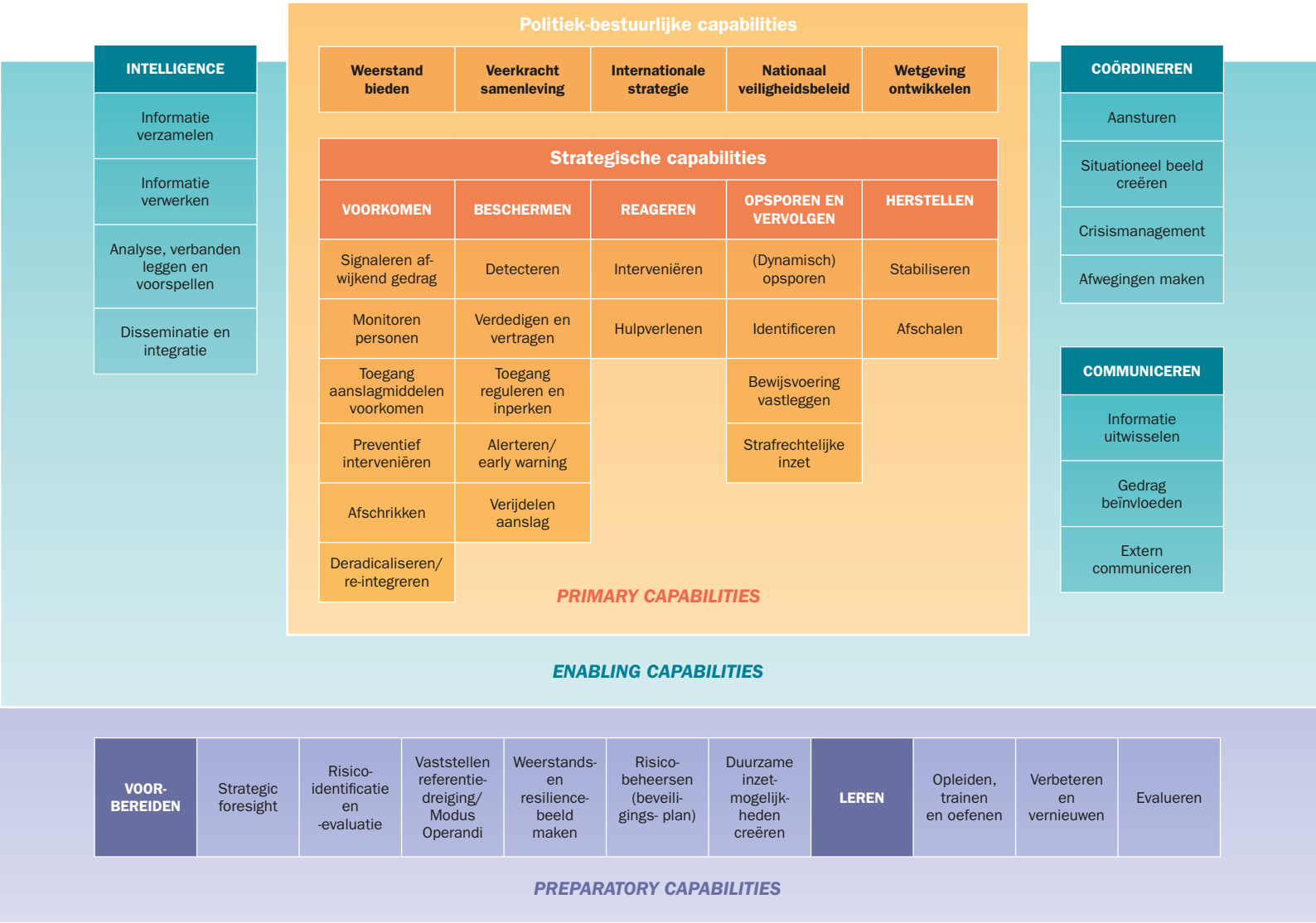
Op basis van diverse modellen, interviews en documentenstudie heeft TNO in het Vraaggestuurd Programma Veilige Maatschappij een initieel *capability*-model voor terrorismebestrijding ontwikkeld. Dit model is visueel weergegeven in figuur 2. Nadere verantwoording van de ontwikkeling van dit model staat achterin dit boekje. Dit model is gebruikt om de technologiegebieden en onderliggende technologietoepassingen te identificeren.

Het *capability*-model voor terrorismebestrijding beschrijft *capabilities* om een overzicht te geven van de taken, kennis en kunde die nodig zijn voor terrorismebestrijding op verschillende organisatiesturingsniveaus (politiek-bestuurlijk, strategisch en tactisch). Het gaat bij al deze *capabilities* om iets wat de ketenpartners als geheel moeten kunnen, de *capabilities* zijn meestal niet direct aan één organisatie toe te wijzen.

Tevens zijn in het model ook ondersteunende *(enabling) capabilities* en voorbereidende *(preparatory) capabilities* weergegeven. Deze *capabilities* ondersteunen verschillende (en vaak meerdere) strategische en tactische *capabilities*. Het operationele organisatieniveau is niet vertegenwoordigd in het model omdat de uitvoeringsvormen daarvan vaker en sneller kunnen verschillen.

In het overzicht van technologie wordt de relatie tussen technologiegebieden en de strategische *capabilities* aangeduid. Bij het ontwikkelen van dit overzicht van technologie en daarmee het identificeren van de technologietoepassingen zijn ook de onderliggende ondersteunende *capabilities* in beschouwing genomen.

FIGUUR 2
Initieel *capability*-model terrorismebestrijding



HET IS DE KUNST TE IDENTIFICEREN WELKE TECHNOLOGIEËN VAN BELANG ZIJN VOOR DE KORTE ÉN LANGE TERMIJN.

VOORKOMEN

- Vroegtijdig signaleren en beïnvloeden van keuzegedrag van mensen
- Delen en combineren van informatie
- Juiste keuzes voor interventies en beschikbare capaciteit
- Zowel in de fysieke wereld als in de virtuele wereld

BESCHERMEN

- Fysieke maatregelen integreren in de omgeving
- Met fysieke maatregelen gewenst gedrag faciliteren
- Informatie-uitwisseling met zowel publieke als private partijen
- Een goed beeld krijgen van de omgeving
- Effectieve inzetkeuzes maken

REAGEREN

- Sneller inzicht in de situatie en het mogelijke verloop
- Anticiperen om de impact en de gevolgen beperken
- Slimme keuzes maken ten aanzien van de juiste inzet van mensen en middelen

UITDAGINGEN VOOR DE KETEN

Het dreigingsniveau in het Dreigingsbeeld Terrorisme Nederland van oktober 2018 (NCTV, 2018a) is substantieel. Dat betekent dat een reële kans bestaat op een aanslag ergens in Nederland. De aanhoudende dreiging van terrorisme stelt de keten van terrorismebestrijding voor aanzienlijke uitdagingen en zorgt voor behoefte aan duurzaam inzetbare capaciteit.

"De aanhoudende jihadistisch-terroristische dreiging tegen het Westen lijkt een structureel onderdeel van onze samenleving te zijn geworden" (AIVD, 2018a). De dreiging is in de afgelopen jaren veranderd maar vooralsnog niet verminderd. Naast de jihadistisch – terroristische dreiging is het rechtsextremisme en gewelddadige activisme in beweging (AIVD, 2018c). Alles bij elkaar stelt dat de veiligheidsketen voor aanzienlijke uitdagingen.

FIGUUR 3
Mogelijke versterking van de *capabilities*

Terroristen gebruiken bijvoorbeeld steeds vaker eenvoudig te verkrijgen voorwerpen, zoals (vracht)auto's en messen en richten zich op niet of nauwelijks beveiligde en dus makkelijk te treffen doelwitten richten (AIVD, 2017), zgn. '*soft targets*'.

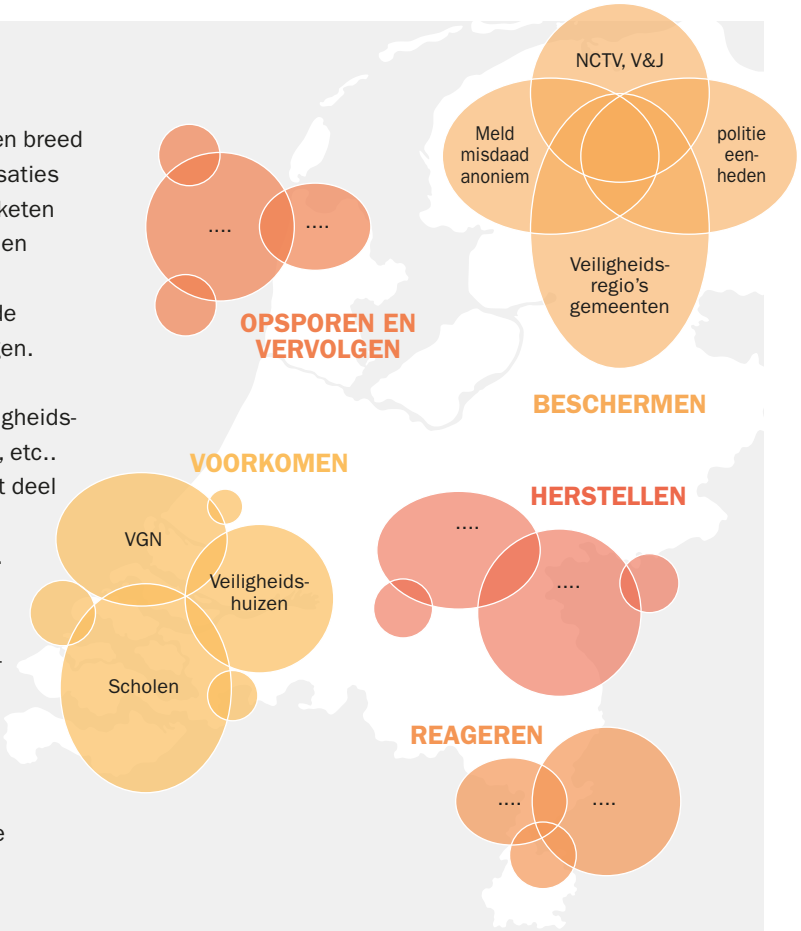
Door het langdurige substantiële dreigingsniveau is het een uitdaging om voldoende capaciteit te organiseren en duurzame inzet te creëren. Daarnaast spelen voor al deze uitdagingen privacy vraagstukken een rol, hetgeen in de aanpak een uitdaging op zichzelf vormt. Mogen gegevens worden uitgewisseld en op basis waarvan? En wie mag het wel, wie niet? Bijvoorbeeld, mogen psychologen het beroepsgeheim loslaten als er dreigingen zijn, en zo ja wanneer dan precies?

De volgende bladzijden beschrijven eerst wat wordt verstaan onder de keten van terrorismebestrijding en vervolgens de uitdagingen voor de verschillende strategische *capabilities*: Voorkomen, Beschermen, Reageren, Opsporen en Vervolgen en Herstellen. In figuur 3 staat een samenvatting van de mogelijke versterking van de *capabilities*. In het volgende hoofdstuk worden de technologiegebieden beschreven en de link gelegd tussen de *capabilities* en de wijze waarop technologie deze kan versterken of vernieuwen.

KETEN VAN TERRORISMEBESTRIJDING

De keten van terrorismebestrijding bestaat uit een breed scala aan organisaties en partijen. Welke organisaties dit zijn verschilt per casus. Organisaties in deze keten zijn o.a.: het Ministerie van Justitie en Veiligheid en daarbinnen specifiek de NCTV, DGPOL, IND etc. Verder het Ministerie van Defensie en specifiek de KMAR voor grenstoezicht en bewaken en beveiligen. Daarnaast partijen als Veiligheidsregio's, Politie eenheden, Meld misdaad anoniem, scholen, veiligheidshuizen, private beveiligingsbedrijven, gemeenten, etc.. Ieder van deze organisaties of instellingen maakt deel uit van de keten voor terrorisme bestrijding, tot uiteindelijk winkeliers en burgers zelf als het o.a. gaat om melden van verdachte situaties.

Elk van deze organisaties beschikt over mogelijkheden om taken uit te voeren die bijdragen aan de aanpak van terrorisme, of informatie te leveren over indicatoren of gebeurtenissen. Een school zal meer informatie hebben op het gebied van voorkomen en beschermen; de politie kan meer invloed uitoefenen op het gebied van opsporen en vervolgen.



Doordat organisaties door de gehele keten samenwerken, ontstaan er meer mogelijkheden tot handelen, en wordt informatie beter benut. Zo worden CTER maatregelen effectiever, en dragen ze meer bij aan het versterken van de Nationale Veiligheid.

UITDAGINGEN VOOR DE KETEN

VOORKOMEN

Voor het kunnen voorkomen (en verstoren) van aanslagen is inzicht nodig in een potentiële dreiging en de oorsprong daarvan. Het is de uitdaging om vroegtijdig signalen te detecteren om radicalisering te voorkomen, maar ook om eenlingen en gefrustreerde mensen die bereid zijn extreem of grof geweld te gebruiken te signaleren. Daarvoor is het nodig risicotaxaties uit te voeren en te weten welke indicatoren daarvoor bepalend zijn en mogelijk te gebruiken zijn. Bij de inzet van technologie bij de-radicalisering zou kunnen worden gekeken naar technieken voor het beïnvloeden van het keuzegedrag van mensen (nudging). Voorkomen van verdere gewelddadige radicalisering is gewenst, bijvoorbeeld in gevangenissen of in woonwijken. Het delen van data tussen verschillende partners is daarbij noodzakelijk met daarbij privacy in acht te nemen, af te stemmen, keuzes te maken, verantwoordelijkheden te delen en leren van de effecten. Het gaat om het delen van (werk)processen voor risicotaxatie, monitoren en alerteren. Vanuit de hoeveelheid signalen die wordt opgevangen is het van belang om met de beschikbare capaciteiten de juiste keuzes te maken voor inzet. Een wens is ook om signalen bij te sturen, zoals door middel van *counter narratives*. Vraag is daarbij hoe kan worden bepaald waar preventieve middelen het meest effectief op kunnen worden gericht, zowel in de fysieke als de virtuele wereld.

BESCHERMEN

De uitdagingen met betrekking tot het beschermen van objecten, personen, diensten etc. hebben onder meer betrekking op de vraag hoe technologie kan ondersteunen om maatregelen te integreren in de omgeving. Het gaat daarbij om maatregelen die het risico beheersen versus het risico uitsluiten. De fysieke maatregelen dienen mensen in een publieke ruimte (*open space*) te helpen en gewenst gedrag te faciliteren ten tijde van een aanslag (bijvoorbeeld t.a.v. schuilplaatsen of vluchtroutes) zonder dat deze maatregelen de omgeving dusdanig negatief beïnvloedt. Ook bij beschermen is informatie-uitwisseling belangrijk met zowel publieke als private partijen, om een goed en gezamenlijk beeld te hebben van de omgeving. Verschillende partners in de keten hebben hierbij verschillende taken en verantwoordelijkheden. Het is in dat licht een uitdaging om informatie (en signalen) bij elkaar te brengen en te delen tussen verschillende partners vanuit hun verschillende doelen en vaak ook door wetgeving aangegeven grenzen. Een uitdaging voor beschermen is het maken van effectieve keuzes ten aanzien van de juiste inzet van mensen en middelen, rekening houdend met de mogelijkheden en beperkingen.

REAGEREN

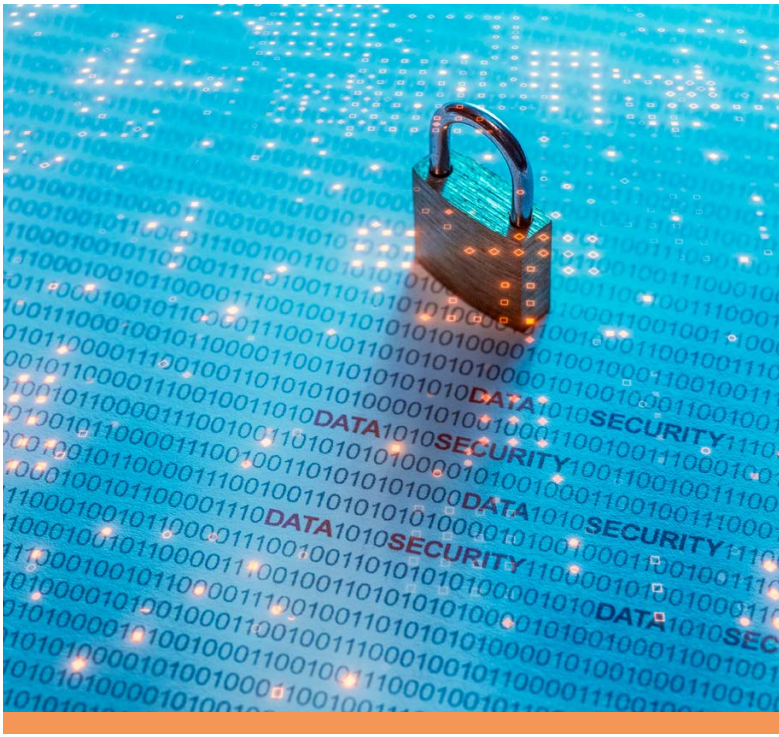
Voor het adequaat kunnen reageren is het de uitdaging om snel inzicht te krijgen in wat er aan de hand is (*situational awareness*). Het verkrijgen van inzicht in de situatie, verdachten en mogelijk verloop van de situatie staat hier centraal. Dit met als doel om een beter beeld te krijgen van de mogelijkheden hoe er gereageerd kan worden op de situatie. Uiteindelijk doel is het beperken van de impact en gevolgen (terrorismegevolgbestrijding) en het neutraliseren van de dreiging. Het is een uitdaging informatie te gebruiken om de juiste interventies toe te passen met daarbij real-time inzicht in de beschikbare capaciteit. Crisiscommunicatie en crisisbeheersing speelt hier een belangrijke rol. De daarbij horende uitdaging is de afstemming tussen de verschillende betrokken partijen. Het optimaal delen van informatie in de keten is nodig om snel kennis paraat te hebben. Daarnaast is het een uitdaging om de impact zo gering mogelijk houden. Bestaat een vervolgdreiging en zo ja welke, en hoe voorkom je vervolgaanslagen dan wel meer slachtoffers? Reageren is ook gericht op het voorkomen van maatschappelijke ontwrichting.

OPSPOREN EN VERVOLGEN

Voor het kunnen opsporen en vervolgen van verdachten is het een uitdaging terroristische intenties tijdig te herkennen, (snel) identiteiten te achterhalen en sporen te detecteren. Dit geldt zowel voor de periode tijdens de voorbereiding van terroristische daden (vroeg-signalering), als nadat een gebeurtenis heeft plaatsgevonden. Het is gewenst meer inzicht te krijgen in potentiële daders en hun (sociale) omgeving en daarbij een vroegtijdige indicatie te krijgen van afwijkend gedrag en activiteiten via virtuele sporen of indicaties dat aanslagmiddelen worden verworven: explosieven, wapens of hele nieuwe typen middelen. Herkennen van personen en objecten uit beeld is een van de mogelijkheden daarbij. Voor opsporen en vervolgen is het ook in toenemende mate een uitdaging de crowd te betrekken bij bewijsvoering en bronnen en data te combineren vanuit een gegeven doel vanuit een integrale aanpak en coördinatie vanuit de overheid.

HERSTELLEN

Uitdagingen voor het kunnen herstellen liggen op het gebied van het normaliseren, dat wil zeggen het terugbrengen van de openbare orde en veiligheid na een terroristische dreiging of aanslag. Belangrijk daarin is het kunnen communiceren naar, en het weerbaar maken van, het publiek en ondernemers. Weerbaarheid verhogen vraagt om de juiste acties vóór een incident, maar ook om nazorg; bijvoorbeeld op het gebied van ‘PTSS-onderzoek’. Voor het communiceren naar het publiek gaat het om tweeweg communicatie, dus ook het luisteren naar het publiek en het wederzijds delen van informatie. In relatie tot herstellen is ook afschalen een uitdaging, wanneer kan het dreigingsniveau weer worden verlaagd? Reeds ingevoerde maatregelen kunnen mogelijk worden ingetrokken of inzet kan worden verlaagd: wat zijn daarbij de afwegingen?



EEN TECHNOLOGIE-GEBIED IS EEN CLUSTER VAN VERSCHILLENDE TECHNOLOGIETOEPASSINGEN, WAARMEE CTER-*CAPABILITIES* IN DE KETEN KUNNEN WORDEN VERGROOT, VERSTERKT OF ONTWIKKELD.

TECHNOLOGIEGEBIED 1

GEDRAGSANALYSE EN GEDRAGS-BEÏNVLOEDINGS-TECHNOLOGIEËN

- Gedragspatroonherkenning
- Adaptieve profilering
- Gedragsbeïnvloeding
- Normalisatie

TECHNOLOGIEGEBIED 2

IDENTIFICATIE- EN OPSPORINGS-TECHNOLOGIEËN

- Fysieke identificatie/biometrie
- Digitale identificatie
- Lokalisering en tracking
- Echtheidsvalidatie en authenticatie
- Sporendetectie
- Signaal interceptie, verstoring en detectie

TECHNOLOGIEGEBIED 3

FYSIEKE BEVEILIGING- EN BESCHERMINGS-TECHNOLOGIEËN

- Robotica en autonome systemen
- Remote sensing
- Nieuwe materialen
- Security-by-design

TECHNOLOGIEGEBIED 4

GEÏNTEGREERDE SENSING-TECHNOLOGIEËN

- Intelligente sensornetwerken
- Explosieven monitoring en detectie
- CBRN monitoring en detectie
- Cyber monitoring en detectie

TECHNOLOGIEGEBIEDEN

Acht technologiegebieden zijn geïdentificeerd die relevant zijn voor terrorismebestrijding. Een technologiegebied is een cluster van verschillende technologietoepassingen, waarmee CTER-*capabilities* in de keten kunnen worden vergroot, versterkt of ontwikkeld.

Langs de lijn van de benodigde *capabilities* voor terrorismebestrijding zijn relevante technologieën en daarbij horende toepassingen in kaart gebracht. Deze technologieën zijn geclusterd naar technologiegebieden en geverifieerd met eerdere en gelieerde technologieverkenningen op het gebied van Nationale Veiligheid.

Op de volgende pagina's worden de acht technologiegebieden nader toegelicht en wordt de verhouding tot de *capabilities* benoemd. Ieder technologiegebied bestaat uit diverse technologietoepassingen en richt zich op één of meerdere uitdagingen op het gebied van terrorismebestrijding. Wat de ontwikkelingen op ieder genoemd technologiegebied kan opleveren wordt steeds vermeld.

FIGUUR 4
Technologiegebieden voor terrorismebestrijding en onderliggende technologietoepassingen

De kern van dit technologiegebied is gedrag. Het gaat om het in kaart brengen van patronen of profielen van (afwijkend) gedrag en/of het beïnvloeden daarvan.

TECHNOLOGIEGEBIED 1

GEDRAGSANALYSE- EN GEDRAGS-BEÏNVLOEDINGSTECHNOLOGIEËN

GEDRAGSPATROON-HERKENNING

Op basis van vroegtijdig herkende risicovolle gedragspatronen, bijvoorbeeld die gerelateerd zijn met gewelddadige radicalisering en extremisme, kunnen interventies worden toegepast om bijvoorbeeld (verdere) gewelddadige radicalisering te voorkomen.
Meer concreet is dit bijvoorbeeld toe te passen bij het beschermen van objecten of bij het opsporen van misdrijven, zoals in een woonwijk of op een vliegveld.
Een voorbeeld van ontwikkeling op dit gebied is het H2020 project Pericles (Pericles, 2018), waarbij een *Vulnerability Assessment Tool* wordt ontwikkeld om te signaleren wanneer een individu kwetsbaar is voor gewelddadige radicalisering. De resulterende methode en technologie helpen multidisciplinaire teams van bijvoorbeeld politie, gemeente, justitie en scholen om gewelddadige radicalisering te herkennen (en te monitoren).

ADAPTIEVE PROFILERING

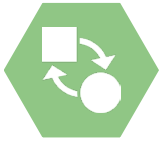
Bij profilering gaat het om het opbouwen van een beeld van een persoon of situatie. Het gaat daarbij om de eigenschappen van een persoon of situatie, bijvoorbeeld bij hoge dreigingen.
Het gaat om het vergelijken van die eigenschappen met bepaalde profielen. Aan de hand daarvan kan een statistisch onderbouwde aanname worden gedaan over de betreffende persoon en/of situatie. De nadruk bij deze technologie ligt vaak op de adaptiviteit. Dat betekent dat de profielen continu moeten worden aangepast aan nieuwe dreigingen en informatie. Dit is nodig, omdat op die manier beter kan worden geanticipeerd op ontwikkelingen en real-time informatie. Een voorbeeld van dit soort technologie is QUIN, waarbij statistisch onderbouwde aannames worden gedaan over de volgende stappen van een misdadiger. Voor doorontwikkeling op dit gebied kunnen andere technologieën zoals *deep-learning* algoritmen worden gebruikt, mits deze transparant en begrijpelijk werken.

VOORKOMEN, REAGEREN, HERSTELLEN

Ontwikkeling op dit technologiegebied levert beter inzicht in menselijk gedrag wat ervoor zorgt dat interventies meer vroegtijdig kunnen worden ingezet. Daarmee wordt o.a. radicalisering tegengegaan en kunnen incidenten mogelijk worden voorkomen.

GEDRAGS-BEÏNVLOEDING

Gedragsbeïnvloeding is het veranderen van gedrag van mensen door middel van meer of minder opvallende interventies. Dit kan variëren van expliciete interventies tot meer subtiele interventies. Bij expliciete interventies gaat het bijvoorbeeld om het direct vragen of iemand zijn/haar gedrag wil veranderen. Bij subtielere interventies kan gedacht worden aan het inzetten van sociale beïnvloedingsmechanismen, veelal uit de marketing. Een voorbeeld van een sociaal beïnvloedingsmechanisme is nudging. Daarbij krijgt men een ‘duwtje’ (een “nudge”) in een bepaalde richting, waardoor men het gewenste gedrag gaat vertonen. Nudging technologie kan wellicht ook bijdragen aan het veiligheidsbewustzijn van potentiële doelwitten en omstanders, of helpen om potentiële daders af te schrikken. Gezien de complexiteit van bijvoorbeeld radicaliseringsprocessen is het lastig te bepalen of een concrete gedragsbeïnvloedingsinterventie daar ook effectief is.



NORMALISATIE

Bij normalisatie gaat het om het terugbrengen van (sociale) structuren en verhoudingen naar normaalsituatie en om grip te krijgen op de omgeving. Het terugbrengen naar normaalsituatie houdt in dat zowel de overheid als burgers gebruikelijke taken en patronen weer op kunnen pakken, voornamelijk door het veiligheidsgevoel te herstellen en af te schalen. Door analysetechnieken toe te passen, zoals het analyseren van sociale patronen (en daarmee identificeren van ringleaders) en analyseren effecten van interventies (zowel micro, meso als macro niveau) kunnen methoden worden ontwikkeld aan de hand waarvan ondermijnende invloeden worden geneutraliseerd, het veiligheidsgevoel wordt hersteld en eventueel kan worden afgeschaald. Onderdeel van het proces kan het (tijdelijk) verwijderen van personen uit het betreffende sociale netwerk zijn, bijvoorbeeld door middel van interventies uit het strafrecht.

De kern van dit technologiegebied is het identificeren en opsporen van één of meerdere personen of sporen. Dit kan zowel proactief als reactief worden ingezet.

TECHNOLOGIEGEBIED 2

IDENTIFICATIE- EN OPSPORINGSTECHNOLOGIEËN

FYSIEKE IDENTIFICATIE/ BIOMETRIE

Het herkennen van personen kan met behulp van biometrie: het meten aan lichaamskenmerken met behulp van informatietechnologie. Dat kan bijvoorbeeld met een vingerafdruk of het patroon van de iris. Zelfs veranderlijke lichaamskenmerken (*soft biometrics*) zoals de stem (Grijpink, 2000) en gedrag (zoals toetsenbord aanslagen) zijn voor beperkte biometrische patroonherkenning bruikbaar. Biometrische technologie wordt bijvoorbeeld ingezet door de politie om gezochte personen te vinden en de identiteit van slachtoffers en daders vast te stellen. Identificatie vereist een koppeling tussen biometrische opnames en een database met identiteiten. Opkomende biometrische technologieën maken onder bepaalde omstandigheden ook biometrie op afstand, *on the move* en zelfs heimelijk en non-coöperatief mogelijk.

DIGITALE IDENTIFICATIE

De technologie van digitale identificatie omvat technologie waarmee de identiteit van personen digitaal wordt verwerkt. Op dit gebied zijn diverse ontwikkelingen gaande, zoals de DigiD die al eerder in werking trad en het gebruik daarvan door bijvoorbeeld bedrijven (eHerkenning). Momenteel wordt gewerkt aan de eNIK: de elektronische Nederlandse Identiteitskaart (Digitale Overheid, 2018). Deze technologie biedt niet alleen kansen voor de praktische toepassing, maar ook voor de lokalisering en opsporing van verdachten. Online informatie kan makkelijker worden gekoppeld aan een digitale identiteit bij doorontwikkeling op dit gebied. Sommige *smart city* concepten zijn gebaseerd op digitale identificatie technologie.

OPSPOREN EN VERVOLGEN

Ontwikkeling op dit technologiegebied zorgt voornamelijk voor versnelling en meer efficiëntie op het gebied van opsporing doordat personen beter en sneller kunnen worden herkend, maar ook makkelijker kunnen worden gelokaliseerd en de echtheid kan worden gevalideerd.

LOKALISERING EN TRACKING

Onder deze technologie wordt verstaan de manieren om iets, iemand of een groep mensen te lokaliseren of te volgen. Dit is van belang voor het monitoren van gevaarlijke personen en/of van personen die verdacht zijn van een ernstig misdrijf. Ook kan deze technologie gebruikt worden om belangrijke assets van een afstand te monitoren, zoals VIP's of menigtes. Een voorbeeld hiervan is de technologie van *"Bluetrace Crowd Control"* waarmee de politie en beveiliging mensenmassa's en hun bewegingen in kaart kunnen brengen door het schatten van het aantal aanwezigen op basis van telefoons met bluetooth-signaal.

Typisch worden hier communicatie en lokalisatie technologieën voor gebruikt zoals GPS, mobiele telefoons, wifi-tracking, maar ook *Internet-of-Things* kan bijdragen. Er zijn sterke raakvlakken met fysieke identificatie, met interceptie-technologie, met heimelijke observatie en met het technologiegebied Geïntegreerde Sensing Technologieën.

ECHTHEIDSVALIDATIE EN AUTHENTICATIE

Bij de technologie van echtheidsvalidatie staat het valideren van de echtheid van iets of iemand centraal. Identiteits-systemen kunnen gesaboteerd worden, bijvoorbeeld door identiteitskenmerken te vervalsen (En. *spoofing*). Het kan gaan om de echtheid van een identiteitsclaim, maar ook om andere soorten claims of statements. Dit validatieproces kan worden bereikt door middel van ondersteunende technologie zoals biometrie of documentauthenticatie systemen. Door ontwikkeling op dit gebied kunnen manieren om de echtheid van iets of iemand te valideren worden gebundeld waardoor dit proces beter of sneller kan worden afgerond. Hiervoor moet referentiemateriaal worden geprepareerd.

···→

TECHNOLOGIEGEBIED 2
IDENTIFICATIE- EN OPSPORINGSTECHNOLOGIEËN

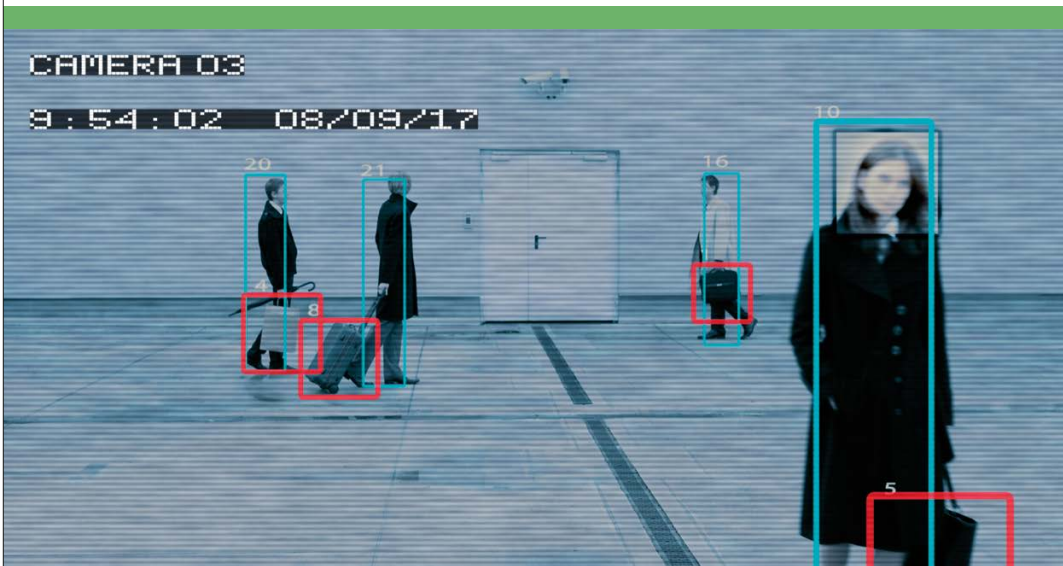
SPORENDETECTIE

Sporendetectie bestaat uit technologie waarmee steeds meer informatie gehaald kan worden uit steeds kleinere sporen, en wat steeds sneller kan worden uitgevoerd. Het gaat hier zowel om fysieke sporen als ook om digitale sporen halen uit elektronische systemen. Voorbeelden zijn forensische technieken in relatie tot de bron van explosieven (*matching*) of opsporingssystemen op basis van *Artificial Intelligence* (AI). Hierdoor kan mogelijk een aanslag worden voorkomen maar kunnen ook na een aanslag verdachten sneller worden gevonden. Ook digitale sporen halen uit elektronische systemen die niet meer werken (zoals mobiele telefoons of navigatiesystemen). Van belang zijn technologieën die sporen kunnen vinden en begrijpen. Het heel snel in kaart kunnen brengen hoe een plaats delict eruit ziet is van wezenlijk belang. Denk aan hoge resolutie millimeter nauwkeurige 3D-scans, multi-spectrale opnames die tegelijkertijd snel in de operatie beschikbaar kunnen zijn.

SIGNAAL INTER-CEPTIE, VERSTOREN EN DETECTIE

De technologie van signaal interceptie, verstoren of detectie gaat over het beïnvloeden, *jammen* of afluisteren van communicatie van de tegenstander. *Jammen* en *spoofen* is gericht op het verstoren of onderscheppen van GPS-signalen (en andere signalen) van bijvoorbeeld explosieven die van een afstand worden gedetoneerd om de aanslag te voorkomen. Het kunnen detecteren van communicatie of het lokaliseren van een communicatie device zoals 4g/5g mobiele telefoons kan actief (IMSI-catcher, triangulatie etc) of passief (*junction detection*). Het is ook mogelijk om elektronica van voertuigen op afstand te kunnen volgen en mogelijk beïnvloeden (traceren, demobiliseren). Van belang is heimelijke communicatie te kunnen intercepteren, op een manier zodat de tegenstander niet weet dat deze wordt afgeluisterd. Wat betreft het ontcijferen van gecodeerde communicatie (cryptografie) is de quantum technologie disruptief waardoor veel van de huidig veilig geachte versleutelingstechnologieën niet meer werken. De tegenstander zal in de nabije toekomst ook potentieel de beschikking krijgen over geavanceerde heimelijke communicatie middelen (denk aan communicatie middels laser of radar). Dan is interceptie wellicht lastig maar detectie ervan wel goed mogelijk. Binnen dit technologietoepassingsgebied valt ook het onderscheppen van fysieke communicatie (stemmen in een gesprek). Met *arrays* van veel kleine microfoons kan zeer gericht communicatie opgevangen worden.

DOOR FORENSISCHE TECHNIEKEN TE KOPPELEN AAN OPSPORINGSSYSTEMEN KAN MOGELIJK EEN AANSLAG WORDEN VOORKOMEN, EN KUNNEN OOK VERDACHTEN SNELLER WORDEN GEVONDEN NA EEN AANSLAG HEEFT PLAATSGEVONDEN.



De kern van dit technologiegebied is fysieke bescherming. Het gaat daarbij om technologieën die bijdragen aan de bescherming van objecten en personen met behulp van gebaseerd op nieuwe materialen en de toepassing van security op een fijne en veilige manier: *security-by-design*.

TECHNOLOGIEGEBIED 3

FYSIEKE BEVEILIGING- EN BESCHERMINGSTECHNOLOGIEËN

ROBOTICA EN AUTONOME SYSTEMEN

Het gebruik van robotica kan helpen om relatieve beperkingen van het menselijk lichaam te overwinnen. Met behulp van exoskeletten kunnen beveiligers straks langer of effectiever opereren. Op afstand bestuurbare of zelfs autonome systemen kunnen helpen om saaie, vieze of gevaarlijke taken uit te voeren. Daar zijn er op het gebied van veiligheid veel van, zoals surveilleren in “steriele” compartimenten, het volgen van verdachte personen of het alert houden van menselijke beveiligers. Bij ontwikkeling rondom het bewapenen van autonome systemen moet rekening worden gehouden met een ethisch dilemma.

REMOTE SENSING

Remote sensing is het waarnemen van een scene op zodanige fysieke afstand dat er vanuit die scene geen effect op de sensor kan zijn. Voorbeelden zijn satellietwaarneming, en het waarnemen vanuit bemande en onbemande luchtvaartuigen, zoals *remote piloted areal systems* (RPAS) en *drones*. De sensoriek en de informatieverwerking daarachter zijn speciaal gericht op het verwerken van de grote hoeveelheden data die uit dergelijke systemen komen. Een voorbeeld is *wide area motion imagery* (WAMI), een technologie waarmee een ultra-hoog resolutie optisch systeem onder een vliegend platform wordt gebruikt om in video opnames met groot geografisch bereik te maken.

NIEUWE MATERIALEN

De technologie van nieuwe materialen gaat over nieuwe productieprocessen van materialen (zoals 3D printen) en nieuwe toepassingen daarvan, en over nieuwe materialen op zichzelf. Nieuwe materialen zijn bijvoorbeeld metamaterialen, zelfhelende materialen en composieten. Deze nieuwe materialen hebben verbeterde eigenschappen met betrekking tot (on)zichtbaarheid, het gewicht en de bescherming en kunnen o.a. worden toegepast in voertuigen, bij gebouwen en voor persoonlijke beschermingsmiddelen. Bij bestaande infrastructuur gaat het over het upgraden van een gebouw met nieuwe technologieën om zo een

BESCHERMEN

Ontwikkeling op dit technologiegebied zorgt voor een betere bescherming van mensen, gebouwen en/of gebieden door bijvoorbeeld nieuwe materialen toe te passen. Daarbij staat de oplossing op maat centraal: iedere omgeving kan op een andere manier beter worden beschermd.

betere bescherming te bieden. Deze upgrade kan zowel met permanente beschermingsmaatregelen als met tijdelijke maatregelen.

SECURITY-BY-DESIGN

De methodiek van *security-by-design* gaat over het meenemen van veiligheid in alle fases van ontwikkeling, beheer en uitfasering van een systeem. Het is een voorbeeld van *value-sensitive-design*, een onderzoeksgebied waarin menselijke waardes centraal worden gesteld in de volledige levensduur van systemen, zoals ook *ethics*- en *privacy*- en *information security-by-design* (zie ook de sectie over ethiek). *Security-by-design* heeft een internationale basis in *Crime Prevention Through Environmental Design* (CPTED). Op het gebied van CTER gaat het hier vooral om het tegengaan van bijvoorbeeld (de gevolgen van) explosies of van *ram-raiding* waarbij de dader bijvoorbeeld inrijdt op een groep personen. Een belangrijke uitdaging voor CPTED is om dergelijke maatregelen proportioneel te ontwerpen in verhouding tot een dynamische dreiging. Voorbeelden van doorontwikkeling op dit technologiegebied zijn obstakels met een adaptieve component en het opzetten en verbeteren van een duurzame publiek-private samenwerking.

De kern van dit technologiegebied is het koppelen ofwel fuseren van data en sensoren. Het gaat daarbij om allerlei systemen, zowel cyber- als fysiek. Het gaat om het monitoren en detecteren van mensen, groepen en voorwerpen of stoffen zoals explosieven of CBRN middelen.

GEÏNTEGREERDE SENSING TECHNOLOGIEËN

INTELLIGENTE SENSORNETWERKEN

Hiermee wordt technologie bedoeld waarmee mensen of middelen in zowel het fysieke als digitale domein in meer of mindere mate integraal en zichtbaar of onzichtbaar in de gaten kunnen worden gehouden en/ of kunnen worden gedetecteerd terwijl zij zich door verschillende fysieke (en juridische) domeinen bewegen. Hiervoor kan een uiteenlopend scala aan onderliggende technologieën worden gebruikt, waaronder heimelijke observatie, lokalisatie en tracking en identificatie technologie. Belangrijke onderdelen van deze technologie zijn ten eerste het kunnen bepalen waar een stukje informatie bij hoort (informatieattributie), en het koppelen van verschillende soorten informatie dat over eenzelfde object of situatie iets zegt (informatiefusie). Voor specialistische deelgebieden zijn aparte deelgebieden gedefinieerd, zoals explosieven, CBRN en cyber.

EXPLOSIEVEN MONITORING EN DETECTIE

Hiermee worden technologieën bedoeld waarmee explosieven, precursoren voor explosieven of onderdelen van Improvised Explosive Devices (IEDs), zoals detonators, ontstekers en triggers, kunnen worden gedetecteerd. Dat kan worden uitgevoerd door middel van een veelheid van technologieën, afhankelijk van de beoogde scenario's en modus operandi. Een voorbeeld is explosieven damp detectie (Explosive Vapour Detection (EVD)). Binnen het EU FP7 project LOTUS (LOTUS, 2013) zijn bijvoorbeeld een aantal chemische detectie sensoren ontwikkeld, die als systeem, bijvoorbeeld door de politie, gebruikt kunnen worden om werkplaatsen te identificeren waar zelfgemaakte explosieven worden gemaakt. Zo'n systeem kan worden gebruikt om terroristen te betrappen tijdens het maken van IEDs.

VOORKOMEN, BESCHERMEN, REAGEREN, OPSPOREN EN VERVOLGEN

Ontwikkeling op dit technologiegebied zorgt voor het meer efficiënt en effectief kunnen waarnemen, monitoren en detecteren. Door systemen en daarbij horende attributen (bijvoorbeeld camera's, sensoren) aan elkaar te koppelen (fusie) kunnen bepaalde (mogelijke) gebeurtenissen sneller en meer adequaat kunnen worden herkend.

CBRN MONITORING EN DETECTIE

Het gaat hier om technologieën die kunnen worden ingezet voor de detectie en identificatie van CBRN middelen, hun precursoren en degradatieproducten. Deze technologieën kunnen worden ingezet voor zowel het voorkomen van een aanslag als het reageren na een aanslag. Voor het voorkomen betreft het voornamelijk de detectie van illegale productie, opslag of vervoer. Bij het reageren dienen de technologieën enerzijds als waarschuwing dat er een mogelijk gevaar is (detectie) maar worden ook veelvuldig gebruikt om onomstotelijk vast te stellen over welke stof het precies gaat (identificatie). Daarnaast worden er ook technologieën ontwikkeld om snel aan te kunnen tonen of een persoon daadwerkelijk is blootgesteld door analyse van biomedische samples en de in het lichaam aangetroffen degradatieproducten of adducten. Een laatste aspect van de CBRN detectie en monitoring is het op basis van analyse toekennen (attribute) van de inzet van het CBRN middel aan een mogelijke dader of productielocatie om vervolging van de daders mogelijk te maken.

CYBER MONITORING EN DETECTIE

Cyber monitoring gaat over het beschermen en monitoren van IT-systemen. Met cyber detectie wordt de mogelijkheid tot het detecteren, ofwel het opmerken van (ongewenste) gebeurtenissen in het digitale domein bedoeld. Door ontwikkeling op dit gebied kan een potentiële aanvaller of gevaarlijke gebeurtenis (sneller) worden gedetecteerd. Huidige virusscanners of Intrusion Detection Systems (IDS) op basis van signatures zijn niet meer voldoende. Een voorbeeld van een detectie systeem is een ADS (Anomaly Detection System) wat zou kunnen worden gebruikt door een Security Operating Center (SOC). Door de ADS en SOC te voorzien dan wel uit te breiden met Cyber Threat Intelligence (CTI) van aangesloten organisaties worden de monitoring en detectie mogelijkheden verrijkt en kunnen aanvallers of gebeurtenissen beter worden gedetecteerd.

De kern van dit technologiegebied is cyber. Het gaat daarbij om de voorbeiding op het plaatsvinden van een cyberaanval, het beschermen van eigen informatie en communicatie en het verkrijgen van informatie van de aanvaller.

CYBER REACTIEF

Onder deze technologietoepassing worden technologieën verstaan waarmee adequaat kan worden gereageerd op een cyberaanval. Het is van belang de beschikbaarheid, continuïteit en integriteit van IT-middelen te waarborgen. Het adequaat reageren op cyberaanvallen is essentieel en zorgt ervoor dat de beschikbaarheid, continuïteit en integriteit van IT-middelen beter kan worden gewaarborgd en de schade van een cyberaanval kan worden beperkt. Cyberaanvallen zijn divers, wat vraagt om multifunctionele technologie op het gebied van incident respons zoals identificatietechnologie, automatische dreigingsdetectie, etc. Deze technologieën kunnen bijvoorbeeld worden toegepast door een CSIRT (*Computer Security Incident Response Team*). Bij het ontwikkelen hiervan staat schadebeperking centraal, zoals ook het dubbel uitvoeren van IT-systemen of het toepassen van SOAR (*Security Orchestration and Automated Response*). Bij het ontwikkelen en in stand houden van dergelijke technologie is beslisondersteuning belangrijk, omdat het cyberdomein veranderlijk is maar ook omdat het gaat om (te) grote hoeveelheden data.

CYBER OFFENSIEF

Hier gaat het om technologie waarmee offensief kan worden gehandeld. Het gaat daarbij voornamelijk om de IT-systemen die nodig zijn om deze offensieve handelingen uit te voeren in de *cyber kill chain* (Martin, 2014). Daarbij is het ook van belang cyber *operators* continu te trainen, door middel van het ontwikkelen van oefeningen en processen om deze handelingen uit te kunnen voeren. Doordat een toename bestaat van het aantal landen dat aan een offensieve (militaire) cybercapaciteit bouwt (NCTV, 2018b), zorgt ontwikkeling op dit gebied onder andere voor een sterkere positionering van Nederland en de opbouw van het vermogen tot afschrikking van (potentiële) tegenstanders.

INFORMATIEBEVEILIGING, ENCRYPTIE EN DECRYPTIE

Hier gaat het om informatiebeveiliging en zowel en- als decryptie. Informatiebeveiliging is essentieel, zowel voor

BESCHERMEN, REAGEREN, OPSPOREN EN VERVOLGEN

Ontwikkeling op dit technologiegebied zorgt voor een sterkere defensieve en offensieve positie op het gebied van cyber, maar ook voor betere informatiebeveiliging. Daarnaast kan een organisatie beter reageren wanneer een cyberaanval plaatsvindt.

veiligheidsdiensten als voor terroristen. Het is momenteel de trend dat steeds meer communicatie wordt beveiligd door middel van encryptie. In de context van CTER dient encryptie voornamelijk om eigen (gevoelige) informatie te beveiligen (bij opslag of uitwisseling van gegevens met partners). De technologie van decryptie dient in deze context voornamelijk om communicatie of informatie van tegenstanders te kunnen lezen en gebruiken. Als laatste kan het ook belangrijk zijn om technologie te ontwikkelen om encryptie en decryptie te omzeilen: en dus manieren te vinden waarop dezelfde doelen kunnen worden bereikt (zoals informatiedelen of informatie lezen van tegenstanders) zonder gebruik te maken van en- of decryptie.

SECURE COMMUNICATIE

De technologie van secure communicatie is een samenspel tussen communicatie technologie en security technologie, en heeft zowel digitale, fysieke als organisatorische aspecten. Bijvoorbeeld, als je met fysieke elektro magnetische systemen in het digitale domein naar een andere communicatiefrequentie springt, (En. *frequency hopping*), dan moet dit op een gesynchroniseerde manier gebeuren. Er zijn ook allerlei manieren om heimelijk communicatie mogelijk te maken, bijvoorbeeld door het verbergen van informatie in codecs van -op het eerste gezicht- onschuldige databestanden. Of door communicatie over een zeer breed spectrum te verspreiden waardoor een individueel communicatie moment ogenschijnlijk net als ruis wordt geïnterpreteerd. Communicatie op 60GHZ zorgt ervoor dat een signaal relatief snel door aanwezige vegetatie wordt gedempt. Geschikt om op korte afstand heimelijk met elkaar te communiceren zonder het risico dat deze op wat groter afstand gedetecteerd wordt. Ook is communicatie denkbaar buiten het radiospectrum. Denk aan communicatie via modulatie van laserlicht. Je krijgt dan een zeer gerichte bundel die alleen verstoorbaar is als je de bundel specifiek verstoord. Nieuwe vormen van crypotografie maken het mogelijk dat zelfs wanneer een signaal onderschept wordt het ontcijferen zeer lastig wordt. Quantum cryptologie doet daar nog een schepje bovenop. Het maakt ontcijferen niet alleen lastig maar elke poging om dat te doen kan in principe ook gelijk gedetecteerd worden.

De kern van dit technologiegebied is data. Het gaat daarbij om het verwerken van verschillende data stromen, zoals informatie, tekst, spraak en beeld.

ZELFLERENDE SYSTEMEN

De hoeveelheid data die beschikbaar is over personen, locaties en groepen neemt nog steeds exponentieel toe. Dat betekent dat het handmatig verwerken en duiden van informatie steeds moeilijker wordt, zeker als dat 'real-time' moet gebeuren. Zelflerende systemen kunnen de analisten daarbij helpen door geautomatiseerd te identificeren (bijvoorbeeld door *profiling* en social netwerk analyse), in een context te plaatsen (*predictive analyse*), en de meest relevante informatie uit te lichten (*mining*), gebruikmakend van zowel gestructureerde als ongestructureerde gegevens. Het kan daarbij 'leren' wat relevant is zowel door het gebruik van historische data (bijvoorbeeld eerdere aanslagen of geïdentificeerde subjecten) als de feedback van de gebruiker.

INFORMATIEDELING

Onder deze technologie vallen verschillende technieken ter ondersteuning van het uitwisselen van informatie tussen verschillende instanties, zonder dat gevoelige brondata wordt uitgewisseld. Het gaat dan vaak om het oplossen van de paradox tussen need-to-know en need-to-share. Hierbij kan worden gedacht aan o.a. Multi-Party Computation (MPC) en Blockchain-technologie. Doorontwikkeling op dit gebied kan leiden tot een meer veilige en effectieve informatiedeling, bijvoorbeeld omdat automatisch informatie wordt gedeeld zonder gevoelige aspecten daarin mee te nemen of duidelijk te maken wat de gevoelige informatie precies is. Gerelateerd is de ontwikkeling van 'schalende algoritmen' om meer bronnen toe te voegen.

GEAUTOMATISEERDE VERTALING EN ANALYSE

Deze technologie houdt in dat zowel gesproken als geschreven communicatie automatisch en (near) real time wordt vertaald en/of geanalyseerd. Hier vallen dus ook telefoon- en chatgesprekken onder. Analyse kan bestaan uit de extractie van entiteiten, maken van

VOORKOMEN, REAGEREN, OPSPOREN EN VERVOLGEN

Ontwikkeling op dit technologiegebied levert een beter vermogen om sneller en efficiënter data te verwerken. Doordat informatie efficiënter bij elkaar wordt gebracht en automatisch kan worden vertaald kunnen betere inzichten worden verkregen en betere voorspellingen worden gedaan.

samenvattingen en sentiment mining, gebruikmakend van o.a. speech-to-text en natural language processing. Deze technologie draagt bij aan een snellere (verduidelijking) van communicatie, bijvoorbeeld wanneer een aanslag heeft plaatsgevonden of dreigt plaats te vinden.

BEELDANALYSE EN -VERWERKING

Deze technologie richt zich op het automatisch verwerken en interpreteren van visuele data. Gezichtsherkenning en kentekenherkenning zijn hier volwassen voorbeelden van. Indringerdetectie en de detectie van bepaalde andere eenvoudige gedragingen komen nu beschikbaar. Binnen afzienbare termijn wordt het ook mogelijk om meer ingewikkeld gedrag, of gedrag in meer complexe omgevingen automatisch te detecteren. Ook kunnen relevante objecten of relaties tussen beelden automatisch worden bepaald. Voorbeelden zijn (achtergelaten) bagage, of bepaalde patronen in propaganda beeldmateriaal.

PRIVACY BESCHERMING

Veel bestaande en innovatieve technologieën verzamelen en verwerken persoonsgegevens. De (recent aangepaste) wetgeving vereist dat daar zorgvuldig mee wordt omgegaan. Dat vereist het gebruiken van methoden en technologieën die helpen om menselijke waardes te beschermen. Het gedachtegoed van value-sensitive-design stelt menselijke waardes centraal gedurende de hele lifecycle van een systeem. Methoden zoals ethics- en privacy-by-design zijn daar voorbeelden van (zie ook de sectie over ethiek). Naast dergelijke methoden bestaan er ook concrete technologieën die specifiek gebruikt kunnen worden om privacy te beschermen, zoals encryptie, anonimisering en pseudonimisering (zoals hashing) van persoonsgegevens.

De kern van dit technologiegebied is coördineren. Het gaat daarbij ook om het maken van beslissingen, het communiceren naar het publiek en het analyseren van de huidige situatie(s).

BESLISONDERSTEUNING EN COÖRDINATIE TECHNOLOGIEËN

SITUATIE AWARENESS EN ANALYSE

De technologie van situatie awareness en analyse bestaat uit methoden en analyse technologieën om een situatie in te schatten. Analysetechnologie waarbij alle componenten (en dilemma's) van een situatie kunnen worden ingevoerd, zoals zicht op de beschikbare capaciteit, het aantal mensen dat betrokken is en wat de rol is die zij hebben kan meer inzicht geven in een situatie (situatie awareness). Omgevingskenmerken kunnen daarbij ook worden geanalyseerd. Ondersteunende technologie is Artificial Intelligence (AI), maar ook de ontwikkeling van dynamische draaiboeken. Deze technologie kan voornamelijk worden ingezet voor, tijdens of na een aanslag om de huidige situatie snel te kunnen analyseren op basis waarvan betere en snellere beslissingen kunnen worden genomen.

REAL-TIME COÖRDINATIE

De technologie van *real-time* coördinatie richt zich op informatie en communicatietechnologie. Door de combinatie met AI kunnen inzichten snel met elkaar worden gedeeld. Ad hoc fysieke samenwerking in teams samengesteld vanuit verschillende geledingen wordt ondersteund in het delen van informatie en samenwerking in de groep ('ad hoc chatgroup'). Burgers op locatie die in staat zijn informatie te geven en te helpen worden ondersteund met deze technologie.

EFFECTGERICHTE INTERVENTIES

De technologie van effectgerichte interventies is gericht op technologie waarmee beslissingen kunnen worden gemaakt over het inzetten van interventies en inzicht in effecten van interventies (*effect based*). Met behulp van technologie kan snel vraag en aanbod op elkaar worden afgestemd: de match tussen de *capabilities* en capaciteit van de eigen eenheden (wie zit in de buurt en hebben we de juiste *capabilities* en capaciteiten) en

REAGEREN

Ontwikkeling op dit technologiegebied zorgt voor een beter vermogen om te coördineren en daarmee beslissingen te maken en te communiceren. Daarbij kan een meer adequate situatie analyse worden uitgevoerd wat de andere technologieën in dit gebied versterkt.

wat het incident vraagt. Technologieën ondersteunen in het geven van een opdracht aan een eenheid (taken delegeren) en het snel aansturen. In toenemende mate gaat het om het faciliteren van mensen op straat om zelf de benodigde interventie te bepalen (*"Power to the edge"*).

CROWD CONTROL

De technologie voor *crowd control* bestaat uit combinaties van gedragsanalyse, profilering, intelligente sensornetwerken, lokalisatie en tracking technologie in combinatie met communicatie technologie. *Crowd control* heeft een sterke relatie met communicatie omdat het gaat over het uitoefenen van invloed op het publiek. Dat publiek kan breed worden geïnterpreteerd: het gaat bijvoorbeeld om het sturen van groepen of massa's mensen naar de juiste plaatsen, zowel voor, tijdens als na een aanslag. Dat kan onder andere teweeg worden gebracht door middel van communicatie. Communicatie ten tijde van een crisis, bijvoorbeeld een terroristische aanslag, is cruciaal. Transparante communicatie is effectief om de negatieve impact van een crisis te minimaliseren (Huang & Su, 2009). Het gaat daarbij om zowel interne als externe communicatie.

De kern van dit technologiegebied is anticiperen op nieuwe dreigingen. Het gaat daarbij om het continu vooruit kunnen kijken, dit te vertalen naar nieuwe concepten door middel van experimenteren en modelleren en daarmee de inzetbaarheid en weerbaarheid van professionals te verhogen.

TECHNOLOGIEGEBIED 8

LEER- EN ANTICIPATIE-TECHNOLOGIEËN

HORIZON SCANNING

De technologie van *horizon scanning* bestaat voornamelijk uit procesgerichte technologie waarbij het verzamelen van informatie centraal staat. *Horizon scanning* is het systematisch vooruitkijken naar (gevolgen van) ontwikkelingen. Het kan daarbij gaan om zowel technologische ontwikkelingen, fenomenen als dreigingen. Hiervoor wordt informatie verzameld uit verschillende bronnen. De toepassing van *horizon scanning* is zeer divers en kan op het gebied van CTER meer inzicht leveren en zorgen voor een betere voorbereiding op bepaalde gebeurtenissen.

CONCEPT DEVELOPMENT THROUGH EXPERIMENTATION

Hier wordt de methode van concept-ontwikkeling door middel van experimenteren bedoeld, ook wel CD&E genoemd. Doorontwikkeling op dit gebied kan bijvoorbeeld leiden tot nieuwe beveiligingsconcepten of organisatiestructuren, welke kunnen worden getoetst aan de praktijk vóór implementatie, wat de kans op succes van concepten vergroot. Door toetsing kunnen nieuwe inzichten ontstaan waar men van kan leren en waardoor aanpassingen kunnen worden gedaan. Onder de technologietoepassing valt ook het concept van *serious gaming*, waarbij de creatieve aspecten van “spelen” benut wordt voor andere doeleinden.

De toepassingen zijn zeer divers en kunnen variëren van educatie in een gaming omgeving tot het oefenen van samenwerking tussen verschillende partijen of het bieden van hulpverlening bij een terroristische aanslag (van Kranenburg, Slot, Staal, Leurdijk, & Burgmeijer, 2006). Daarnaast kunnen serious games ook worden ingezet om nieuwe concepten te beproeven, hierbij kan ervaren worden wat de gevolgen zijn van nieuwe manieren van optreden of het inzetten van nieuwe technologieën in bestaande processen.

VOORKOMEN, REAGEREN, HERSTELLEN

Ontwikkeling op dit technologiegebied zorgt voor het beter kunnen reageren op een aanslag en het versnellen van het herstel na een aanslag. Door vooruit te kunnen kijken kan worden geanticipeerd op veranderingen zoals de ontwikkeling van nieuwe technologie. Door deze veranderingen systematisch in kaart te brengen en schematisch vast te leggen ontstaat overzicht, wat gebruikt kan worden om te oefenen als organisatie in de keten voor terrorismebestrijding.

SYSTEM & BEHAVIOUR MODELLING

Hieronder wordt technologie verstaan waarmee simulatiemodellen realistischer kunnen worden gemaakt door deze te voorzien van relevant menselijk gedrag en interactie met andere systemen. Ook valt de techniek van modelleren en simuleren zelf onder deze technologietoepassing. Dit zijn technieken om bepaalde processen, systemen en wisselwerkingen in kaart te brengen. Het gaat daarbij (op het gebied van CTER) voornamelijk om maatschappelijke en sociale processen. Door de onderliggende verbanden expliciet te maken kunnen complexe processen worden ontcijferd en kunnen manieren worden gezocht om deze processen te beïnvloeden ofwel tegen te gaan. Door specifieke situaties of vraagstukken na te bootsen in een simulatie kan een meer visueel beeld van het vraagstuk en de effecten van mogelijke interventies worden gecreëerd. Modellering en simulatie kan een sleutelrol spelen op verschillende gebieden binnen het CTER domein.

VERHOGEN INZETBAARHEID EN WEERBAARHEID

Hieronder worden technologieën verstaan die het mogelijk maken om mentaal en fysiek mensen in staat stellen om langer (optimaal) te presteren. Bijvoorbeeld *coping flex* achtige situaties, technologieën die te maken hebben met de werving en selectie, wie zijn meer/minder geschikt in dat soort omstandigheden, voedingstechnologieën die de duurzaamheid vergroten, *mindfulness* training. Een voorbeeld is ook het monitoren van de mens tijdens de operatie of training, bijvoorbeeld door het meten van de hartslag. Trainen met *virtual reality* (niet alleen stimulering via ogen, maar ook reuk, etc) kan helpen potentieel stressvolle situaties of locaties al een keer op te zoeken. Het herkennen van een dergelijke situatie maakt dat men daar in de praktijk makkelijker mee om kan gaan. Het verhogen van de *endurance* van personeel dat tijdelijk langdurig ingezet moet worden door aangepaste voeding. Of het versnellen van herstel na langdurige of intensieve inzet zodat men weer snel(ler) inzetbaar is.

DOOR TECHNOLOGIEËN TE MATCHEN MET DE VERMOGENS EN TAKEN VAN DE KETEN TEZAMEN, ONTSTAAT EEN BEELD VAN DE KANSEN VAN DIE TECHNOLOGIEËN VOOR DE GEZAMENLIJKE UITDAGING DIE ZE HEBBEN.

VERSTERKEN VAN CAPABILITIES

In het voorgaande hoofdstuk zijn acht technologiegebieden en onderliggende technologietoepassingen beschreven waarmee de gezamenlijke aanpak van CTER kan worden versterkt. In figuur 5 zijn de technologietoepassingen in één overzicht gekoppeld aan de strategische *capabilities*. Hierdoor is te zien welke *capabilities* voornamelijk worden vergroot, versterkt of vernieuwd door middel van ontwikkeling op een technologiegebied.

Door technologieën te matchen met *capabilities* voor terrorismebestrijding, ontstaat een beeld van de kansen van die technologieën met betrekking tot de gezamenlijke uitdaging. Het is interessant om inzichtelijk te hebben welke technologieën bijdragen aan meerdere *capabilities*, aan de andere kant is het net zo interessant te weten welke technologieën zich richten op een niche in de keten om het geheel te versterken. In figuur 5 geven de blokjes mét icoon aan welke *capability* voornamelijk wordt versterkt door ontwikkeling van de betreffende technologie; de blokken zonder icoon geven aan waar ontwikkeling op deze technologie ook (gedeeltelijk) aan bijdraagt.

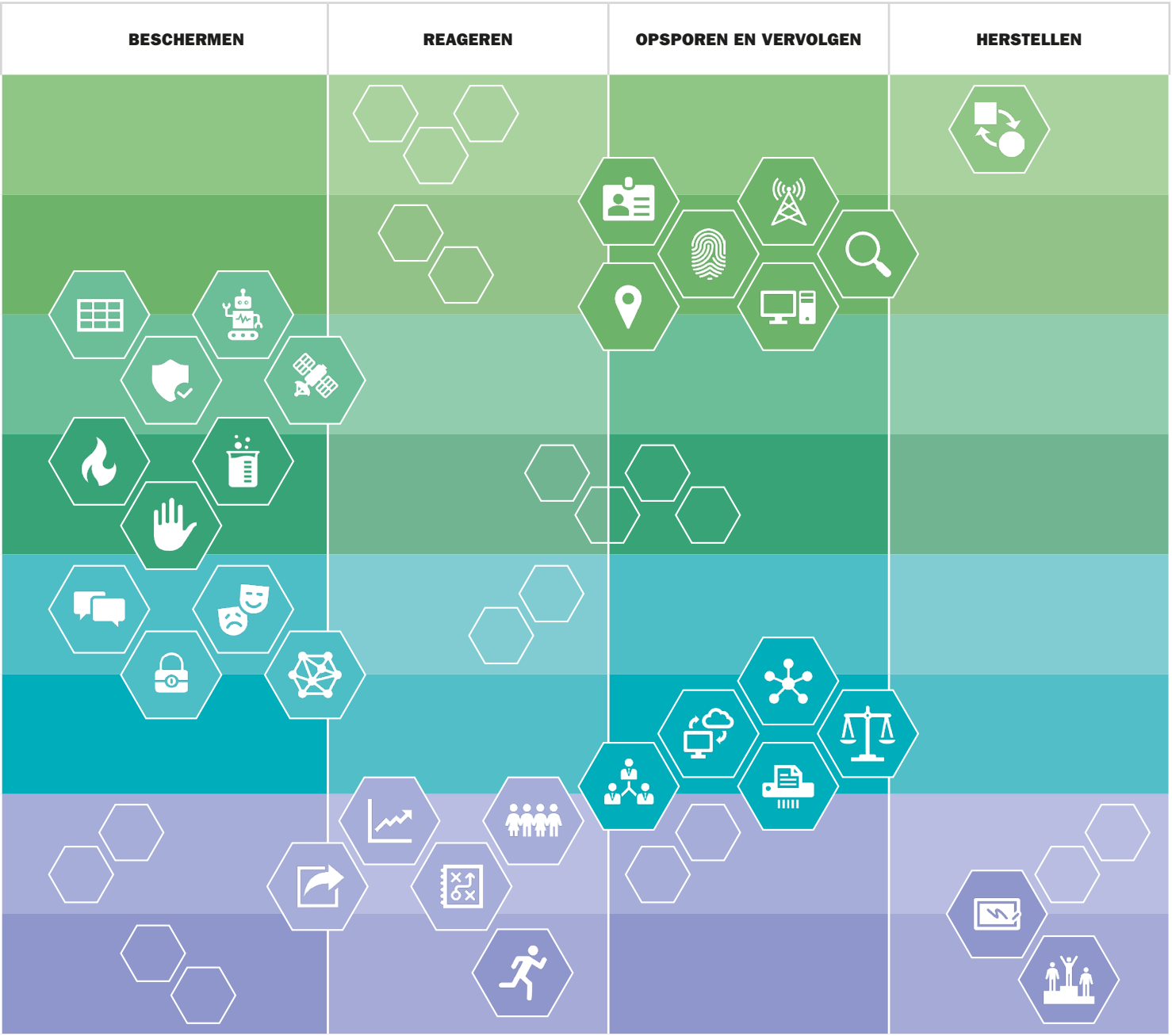
Hierdoor kan dit overzicht van technologie dienen als eerste aanzet om met elkaar te spreken over de behoefte, de prioriteiten en de manier waarop de krachten kunnen worden gebundeld. Om in te zetten op technologie is het noodzakelijk dat ketenpartners dezelfde vraagstukken en verwachtingen hebben én baat hebben bij de investering in de technologieontwikkeling. Dat laatste kan zijn direct of indirect, maar het helpt als inzichtelijk is hoe de keten erdoor wordt versterkt.

Het is duidelijk dat technologie een grote rol speelt in de gezamenlijke aanpak van CTER. Het afzonderlijk van elkaar investeren betekent dat je inboet aan slagkracht. Het gezamenlijk prioriteren of agenderen van technologieontwikkeling vergroot de kans om sneller nieuwe technologieën te adapteren en het anticiperend vermogen te vergroten.

HET OVERZICHT VAN TECHNOLOGIE KAN DIENEN ALS EERSTE AANZET OM MET ELKAAR TE SPREKEN OVER DE BEHOEFTE, DE PRIORITEITEN EN DE MANIER WAAROP DE KRACHTEN WORDEN GEBUNDELD.

FIGUUR 5
Technologiebieden ter versterking en vernieuwing van de *capabilities* voor terrorismebestrijding

		VOORKOMEN
	TECHNOLOGIEGEBIED 1 Gedragsanalyse en gedragsbeïnvloedingstechnologieën	
	TECHNOLOGIEGEBIED 2 Identificatie- en opsporings-technologieën	
	TECHNOLOGIEGEBIED 3 Fysieke beveiliging- en beschermingstechnologieën	
	TECHNOLOGIEGEBIED 4 Geïntegreerde sensing technologieën	
	TECHNOLOGIEGEBIED 5 Cybertechnologieën	
	TECHNOLOGIEGEBIED 6 Data technologieën	
	TECHNOLOGIEGEBIED 7 Beslisondersteuning en coördinatie technologieën	
	TECHNOLOGIEGEBIED 8 Leer- en anticipatietechnologieën	


BESCHERMEN
REAGEREN
OPSPOREN EN VERVOLGEN
HERSTELLEN

NAWOORD

In onze genetwerkte samenleving vereist het beheersen van terroristische risico's een hoge graad van samenwerking. Veranderingen in het werk van de ene dienst, werken direct door naar de ketenpartners. Kunnen we operationeel opschalen bij een terroristische dreiging door via moderne ICT- platformen de inzet van biometrie en slimme camera's dynamisch te vergroten? En kunnen we komen tot 24/7 real-time dreigingsinschattingen die professionals direct informeert? Dit zijn vragen waar in gezamenlijkheid een antwoord op gegeven zal moeten worden en waarmee de keten de ontwikkelingen bij universiteiten, kennisinstituten en bedrijven kan richten.

Vanuit het oogpunt van terrorismebestrijding en veiligheid is het van belang om de mogelijkheden van nieuwe technologie optimaal te benutten. Die technologische ontwikkeling gaat niet alleen snel, maar ook steeds sneller. Krachtige sensoren die de toegang van gebouwen en transportmiddelen veiliger maken, door bijvoorbeeld minuscule hoeveelheden explosieve stof te detecteren. Slimme algoritmen die met behulp van kunstmatige intelligentie en deep learning technieken gedrag van geradicaliseerden voorspellen en onbegrensde mogelijkheden van data koppeling om intelligence tijdig op de juiste plek te krijgen.

Maar er gaat ook dreiging uit van toenemende beschikbaarheid van nieuwe technologie. Ze kan aangewend worden voor nieuwe vormen van criminaliteit en rechtstatelijke beïnvloeding zoals identiteitsfraude, cybercrime en het faciliteren van criminele en terroristische communicatienetwerken. Nieuwe mogelijkheden die de mens juist moeten helpen, worden helaas ook misbruikt. 3D-printen van materialen en voedsel biedt bijvoorbeeld kansen, maar deze technologie maakt ook het vervaardigen van wapens mogelijk uit materialen die moeilijk te detecteren zijn. Onze vitale infrastructuren voor elektriciteit, water, telecom of betaalsystemen blijken kwetsbaar voor cyberhacks. En de onderwereld is actief op het dark web met wapen- en drugshandel.

Een aanzet tot een gedeelde technologieagenda, om daarmee innovatie en technologische ontwikkeling op gebied van contraterrorisme in Nederland te kunnen richten, is daarvoor een belangrijke eerste stap.

KRISHNA TANEJA
Directeur Nationale Veiligheid TNO


“HET BEHEERSEN VAN TERRORISTISCHE RISICO’S VEREIST EEN HOGE GRAAD VAN SAMENWERKING”

VERANTWOORDING

In dit hoofdstuk geven we inzicht in de onderzoeksmethoden en bronnen waarop dit overzicht van technologie is gebaseerd. We pretenderen daarbij niet om volledig te zijn; het overzicht dient als eerste aanzet. Ook evalueren of waarderen we de bronnen niet.

Dit overzicht van technologie voor CTER is tot stand gekomen op basis van gesprekken met professionals van diverse ketenpartners, gesprekken met beleidsontwikkelaars, informatie uit relevante beleids- en wetenschappelijke documenten (zoals andere technologieverkenningen), aanwezige kennis binnen TNO en een expertsessie met partners uit de CTER-keten op 11 september 2018. Daarnaast zijn er vele TNO experts betrokken geweest bij het nader duiden en beschrijven van de technologieën en toepassingen.

IDENTIFICEREN VAN CAPABILITIES

Het *capability*-model (figuur 3) is opgesteld aan de hand van bestaande modellen, namelijk onder andere de 5V's van CTER strategie (NCTV, 2016) , 3D's van CPNI (HM Government, 2014), Risicomanagement ISO 31000 (NEN, 2009), zowel risico management als specifiek ook risicobeheersing, *resilience*, Veiligheidsketen van crisisbeheersing (Veiligheid & crisisbeheersing, 2018) en de *Intelligence cycle* (de Graaf & van Reijn, 2010, p. 702) en is geverifieerd door middel van documentenstudie, domeinkennis aanwezig bij TNO en middels gesprekken met ketenpartners.

IDENTIFICEREN VAN INDIVIDUELE TECHNOLOGIEËN

Het vergroten, versterken of ontwikkelen van verschillende *capabilities* kan worden gefaciliteerd door middel van één of meerdere technologieën. Welke technologieën dit zijn, is geïdentificeerd door middel van een gestructureerde maar brede aanpak langs de lijn van *capabilities* voor CTER. Deze aanpak omvat gesprekken met professionals van diverse ketenpartners, gesprekken met beleidsontwikkelaars, informatie uit relevante documenten en reeds aanwezige kennis binnen TNO.

DEFINIËREN VAN TECHNOLOGIEGEBIEDEN

Vervolgens zijn deze technologieën en daarbij horende ontwikkelingen geclusterd tot technologiegebieden. Met deze technologiegebieden kunnen *capabilities* vergroot, versterkt en/of ontwikkeld worden.

Ten behoeve van verificatie zijn de resulterende technologiegebieden vergeleken met andere verkenningen, scans en clusters van technologie. Na het verifiëren en aanpassen van de technologiegebieden is de eerste versie van het overzicht van technologie voor CTER ontstaan. Dit overzicht bestaat uiteindelijk uit acht technologiegebieden.

In tabel 1 is een verkorte versie te zien van de vergelijking tussen technologieverkenningen en dit overzicht van technologie voor terrorismebestrijding, om de werkwijze te illustreren.

TABEL 1
vergelijking van technologiegebieden met technologieradar en technologiescan

TECHNOLOGIERADAR VEILIGHEID 2014 (van Vliet, Smit-Rietveld, Gelevert, Hasberg, & Kernkamp, 2014)	**TECHNOLOGIESCAN VenJ** (NCTV, 2018c)	**TECHNOLOGIEGEBIEDEN TERRORISMEBESTRIJDING 2019**
Sensing-sensoren	Sensoren	Geïntegreerde sensing technologieën
(Big) data analyse	Data + Data-analyse/algoritmes	Data technologieën
Identificatie en privacy	Biometrie	Identificatie- en opsporingstechnologieën
Automatische gedragsanalyse	Mens & technologie	Gedragsanalyse- en gedragsbeïnvloedingstechnologieën
Command & control	Communicatie	Beslisondersteuning- en coördinatie technologieën
Mens-machine interface	Mens & technologie	
Cyber security en informatiebeveiliging		Cybertechnologieën
Slimme platformen en infra	Robotica en autonome systemen	Fysieke beveiliging- en beschermingstechnologieën
	ICT	
	Materiaal	
		Leer- en anticipatietechnologieën
	Life sciences	

REFERENTIES

- AIVD. (2017). Jaarverslag 2016. Algemene Inlichtingen- en Veiligheidsdienst. Opgehaald van https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2017/04/04/jaarverslag-2016/AIVD+Jaarverslag+2016.pdf
- AIVD. (2018a). De erfenis van Syrië. Den Haag: Algemene Inlichtingen- en Veiligheidsdienst. Opgehaald van https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2018/ 11/05/aivd-publicatie-de-erfenis-van-syrie-mondiaal-jihadisme-blijft-dreiging-voor-europa/Publicatie+De+erfenis+van+Syri%C3%AB%2C+mondiaal+jihadisme+blijft+dreiging+voor+Europa.pdf
- AIVD. (2018b). Jaarverslag 2017. Algemene Inlichtingen- en Veiligheidsdienst. Opgehaald van https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2018/03/06/jaarverslag-aivd-2017/Jaarverslag+AIVD+2017.pdf
- AIVD. (2018c). Rechts-extremisme in Nederland: Een fenomeen in beweging. Den Haag: Algemene Inlichtingen- en Veiligheidsdienst. Opgehaald van https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2018/10/02/rechts-extremisme-in-nederland-een-fenomeen-in-beweging/Rechts-extremisme+in+Nederland+een+fenomeen+in+beweging.pdf
- Akerboom, E. (2017, oktober 26). Nederlandse Politie: Technologie noodzakelijk voor aanpassing aan snel veranderende samenleving. Rathenau Instituut. Opgehaald van https://www.rathenau.nl/nl/digitale-samenleving/nederlandse-politie-technologie-noodzakelijk-voor-aanpassing-aan-snel
- Bogaerts, S., & Scheepmaker, M. P. (2008). Sociale netwerkanalyse. Justitiële verkenningen, 34(5), 7.
- Certified Secure. (2018, september 4). Grapperhaus: technologie steeds belangrijker in politiewerk. Security.nl. Opgehaald van https://www.security.nl/posting/575750/Grapperhaus%3A+technologie+steeds+belangrijker+in+politiewerk
- CTED & UNOCT. (2018). United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism. United Nations Office of Counter-Terrorism. Opgehaald van https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf
- de Graaf, B., & van Reijn, J. A. (2010). Inlichtingen- en Veiligheidsdiensten. Alphen aan den Rijn: Wolters Kluwer.
- Digitale Overheid. (2018, november 27). Identificatie en authenticatie. Opgehaald van Digitale Overheid: https://www.digitaleoverheid.nl/dossiers/identificatie-en-authenticatie/
- Grijpink, J. H. (2000). Biometrie en privacy. Privacy & Informatie, 3(6), 244-250.
- HM Government. (2014). Protecting Crowded Places: Design and Technical Issues. the Home Office: Crown. Opgehaald van https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/302016/DesignTechnicalIssues2014.pdf
- Huang, Y. H., & Su, S. H. (2009). Determinants of consistent, timely, and active responses in corporate crisis. Public Relations Review, 35(1), 7-17.
- LOTUS. (2013). Localisation of Threat Substances in Urban Society. Opgehaald van http://lotusfp7.eu/

- Martin, L. (2014). Cyber Kill Chain. Opgehaald van https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- NCTV. (2016). Nationale Contraterrorismestrategie. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid. Opgehaald van https://www.nctv.nl/binaries/CT-strategie%202016-2020_tcm31-80007.pdf
- NCTV. (2018a). Dreigingsbeeld Terrorisme Nederland 48. 2018: Nationaal Coördinator Terrorismebestrijding en Veiligheid. Opgehaald van https://www.nctv.nl/binaries/DTN48%2C%20samenvatting_tcm31-352621.pdf
- NCTV. (2018b). Nederlandse Cybersecurity Agenda. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
- NCTV. (2018c). Technologiescan: VenJ [Intern concept]. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
- NEN. (2009). ISO 31000. NEN.
- Pericles. (2018, december 11). Aims & objectives. Opgehaald van Pericles: http://project-pericles.eu/about/pericles-aimsobjectives/
- RTL nieuws. (2017, april 6). Terrorismebestrijder waarschuwt voor aanslag met drone in Nederland. RTL nieuws. Opgehaald van RTL nieuws: https://www.rtlnieuws.nl/node/133996
- Rutte, M. (2015, februari 27). Versterking veiligheidsketen [Kamerbrief]. Opgehaald van https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2015/02/27/kamerbrief-over-de-versterkingen-in-de-veiligheidsketen/kamerbrief-over-de-versterkingen-in-de-veiligheidsketen.pdf
- TACTICS. (2012). Conceptual Solution Description. Opgehaald van http://www.fp7-tactics.eu/files/documents/D3.1_Conceptual%20Solution%20Description.pdf
- TNO. (2014, maart 21). Voorbereid zijn voor een terroristische dreiging. TNO Insights. Opgehaald van https://www.tno.nl/nl/tno-insights/artikelen/voorbereid-zijn-voor-een-terroristische-dreiging/
- van de Poel, I., & Royakkers, L. (2011). Ethics, technology, and engineering: An introduction. Southern Gate, UK: John Wiley & Sons.
- van Kranenburg, K., Slot, M., Staal, M., Leurdijk, A., & Burgmeijer, J. (2006). Serious gaming: Onderzoek naar knelpunten en mogelijkheden van serious gaming. Delft: TNO. Opgehaald van http://publications.tno.nl/publication/105193/A94SOJ/33866.pdf
- van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2014). Designing Privacy-by-Design. In B. Preneel, & D. Ikonomou, Privacy Technologies and Policy (pp. 55-72). Limasol, Cyprus: Springer.
- van Vliet, P. J., Smit-Rietveld, C. J., Gelevert, H. F., Hasberg, M. P., & Kernkamp, A. C. (2014). Technologieradar Veiligheid 2014: Relevante technologische ontwikkelingen als input voor (kennis- en) innovatieagenda's. Delft: TNO. Opgehaald van http://publications.tno.nl/publication/34612295/SXJHzD/TNO-2014-R10864.pdf
- Veiligheid & crisisbeheersing. (2018, november). Opgehaald van Veiligheid en crisisbeheersing: http://www.veiligheid.org/

1. Gedragsanalyse- en gedragsbeïnvloedings-technologieën

2. Identificatie- en opsporings-technologieën

3. Fysieke beveiliging- en beschermings-technologieën

4. Geïntegreerde sensing technologieën

5. Cyber-technologieën

6. Data technologieën

7. Beslis-ondersteunings- en coördinatie technologieën

8. Leer- en anticipatie-technologieën

CANVAS OVERZICHT TECHNOLOGIE VOOR TERRORISMEBESTRIJDING

WAAROM EEN OVERZICHT VAN TECHNOLOGIE VOOR TERRORISME-BESTRIJDING?

- Omdat het huidige dreigingsbeeld in Nederland (en het buitenland) vraagt om aandacht voor ontwikkeling van oplossingen voor de korte maar vooral ook de langere termijn. Daarvoor is niet alleen de inzet van de mens nodig, maar ook ondersteunende technologie.
- Omdat de grenzen van de bestaande *capabilities* snel worden bereikt en ook behoefte is aan nieuwe *capabilities* als antwoord op de complexiteit van terrorismebestrijding.
- Om meer inzicht te krijgen in technologie en combinaties daarvan voor verschillende uitdagingen van de terrorismebestrijdingsketen.
- Om de kennis- en technologieontwikkeling voor de aanpak van terrorisme in Nederland sterker te agenderen. TNO wil hiermee bijdragen aan een gericht en samenhangend programma op dit gebied, dat ook proactief vooruitkijkt.

HOE KAN HET OVERZICHT VAN TECHNOLOGIE VOOR TERRORISME-BESTRIJDING WORDEN GEBRUIKT?

- Als handvat voor partners in de keten van terrorismebestrijding voor het verkrijgen van inzicht in de relevante technologieën om op (door-) te ontwikkelen;
- Als handvat bij het opzetten van samenwerkingen tussen partners in de keten, kennis- en technologieinstituten en andere relevante organisaties;
- Dit handvat kan worden gebruikt voor alle partners in de keten van terrorisme-bestrijding. Voor zowel publieke als private organisaties.

VERSTERKEN VAN DE KETEN DOOR MIDDEL VAN TECHNOLOGIEONTWIKKELING

TECHNOLOGIE ONTWIKKELEN

***CAPABILITIES* VERGROTEN, VERSTERKEN EN VERNIEUWEN**

KETEN VAN TERRORISMEBESTRIJDING VERSTERKEN

MOGELIJKE VERSTERKING VAN DE *CAPABILITIES*

VOORKOMEN

- Vroegtijdig signaleren en beïnvloeden van keuzegedrag van mensen
- Delen en combineren van informatie
- Juiste keuzes voor interventies en beschikbare capaciteit
- Zowel in de fysieke wereld als in de virtuele wereld

ACHT TECHNOLOGIEGEBIEDEN EN ONDERLIGGENDE TECHNOLOGIETOEPASSINGEN OM DE GEZAMENLIJKE AANPAK VAN CONTRA-TERRORISME, EXTREMISME EN RADICALISERING *CAPABILITIES* TE VERSTERKEN

TECHNOLOGIEGEBIED 1

GEDRAGSANALYSE EN GEDRAGS-BEÏNVLOEDINGS-TECHNOLOGIEËN

- Gedragspatroonherkenning
- Adaptieve profilering
- Gedragsbeïnvloeding
- Normalisatie

TECHNOLOGIEGEBIED 2

IDENTIFICATIE- EN OPSPORINGS-TECHNOLOGIEËN

- Fysieke identificatie/biometrie
- Digitale identificatie
- Lokalisering en tracking
- Echtheidsvalidatie en authenticatie
- Sporendetectie
- Signaal interceptie, verstoring en detectie

TECHNOLOGIEGEBIED 3

FYSIEKE BEVEILIGING- EN BESCHERMINGS-TECHNOLOGIEËN

- Robotica en autonome systemen
- Remote sensing
- Nieuwe materialen
- Security-by-design

TECHNOLOGIEGEBIED 4

GEÏNTEGREERDE SENSING-TECHNOLOGIEËN

- Intelligente sensornetwerken
- Explosieven monitoring en detectie
- CBRN monitoring en detectie
- Cyber monitoring en detectie

BESCHERMEN

- Fysieke maatregelen integreren in de omgeving
- Met fysieke maatregelen gewenst gedrag faciliteren
- Informatie-uitwisseling met zowel publieke als private partijen
- Een goed beeld krijgen van de omgeving
- Effectieve inzetkeuzes maken

REAGEREN

- Sneller inzicht in de situatie en het mogelijke verloop
- Anticiperen om de impact en de gevolgen beperken
- Slimme keuzes maken ten aanzien van de juiste inzet van mensen en middelen

OPSPOREN EN VERVOLGEN

- Sneller en beter identiteiten en sporen achterhalen
- In de fysieke en virtuele wereld
- Deze waar nodig met elkaar matchen

HERSTELLEN

- Weerbaarheid creëren en verhogen van publiek en ondernemers
- Tweeweg communicatie creëren tussen burgers en overheid
- Afwegingen ten aanzien van afschalen van maatregelen

TECHNOLOGIEGEBIED 5

CYBER-TECHNOLOGIEËN

- Cyber reactief
- Cyber offensief
- Informatiebeveiliging, encryptie en decryptie
- Secure communicatie

TECHNOLOGIEGEBIED 6

DATA TECHNOLOGIEËN

- Zelflerende systemen
- Informatiedeling
- Geautomatiseerde vertaling en analyse
- Beeldanalyse en -verwerking
- Privacy bescherming

TECHNOLOGIEGEBIED 7

BESLIS-ONDERSTEUNING EN COÖRDINATIE TECHNOLOGIEËN

- Situatie awareness en analyse
- Real-time coördinatie
- Effectgerichte interventies
- Crowd control

TECHNOLOGIEGEBIED 8

LEER- EN ANTICIPATIE-TECHNOLOGIEËN

- Horizon scanning
- Concept development through Experimentation
- System & behaviour modelling
- Verhogen inzetbaarheid en weerbaarheid

Terrorisme en terrorismebestrijding verandert door technologie. Innovatie en adaptiviteit speelt een grote rol. Het is de kunst te identificeren welke technologieën van belang zijn voor de korte én lange termijn. Met dit overzicht van technologiegebieden voor terrorismebestrijding is een eerste aanzet gegeven om technologie sterker te agenderen in de aanpak van CTER. Door technologieën te matchen met *capabilities* voor terrorismebestrijding, ofwel de vermogens en taken van de keten tezamen, ontstaat een beeld van de kansen van die technologieën voor de gezamenlijke uitdagingen. Hierdoor kan dit overzicht van technologie dienen als eerste aanzet om met elkaar te spreken over de behoefte, de prioriteiten en de manier waarop de krachten worden gebundeld. Een overzicht van technologie is nooit af. De technologische ontwikkelingen gaan snel, maar desalniettemin zijn ze over het algemeen vrij goed te identificeren tot relevante technologiegebieden. In dit boekje zijn acht technologiegebieden en onderliggende technologietoepassingen beschreven. Op deze manier wil TNO haar kennis en kunde (over technologie en innovatie met technologie) dichter bij de praktijk brengen.

TNO innovation for life

WWW.TNO.NL