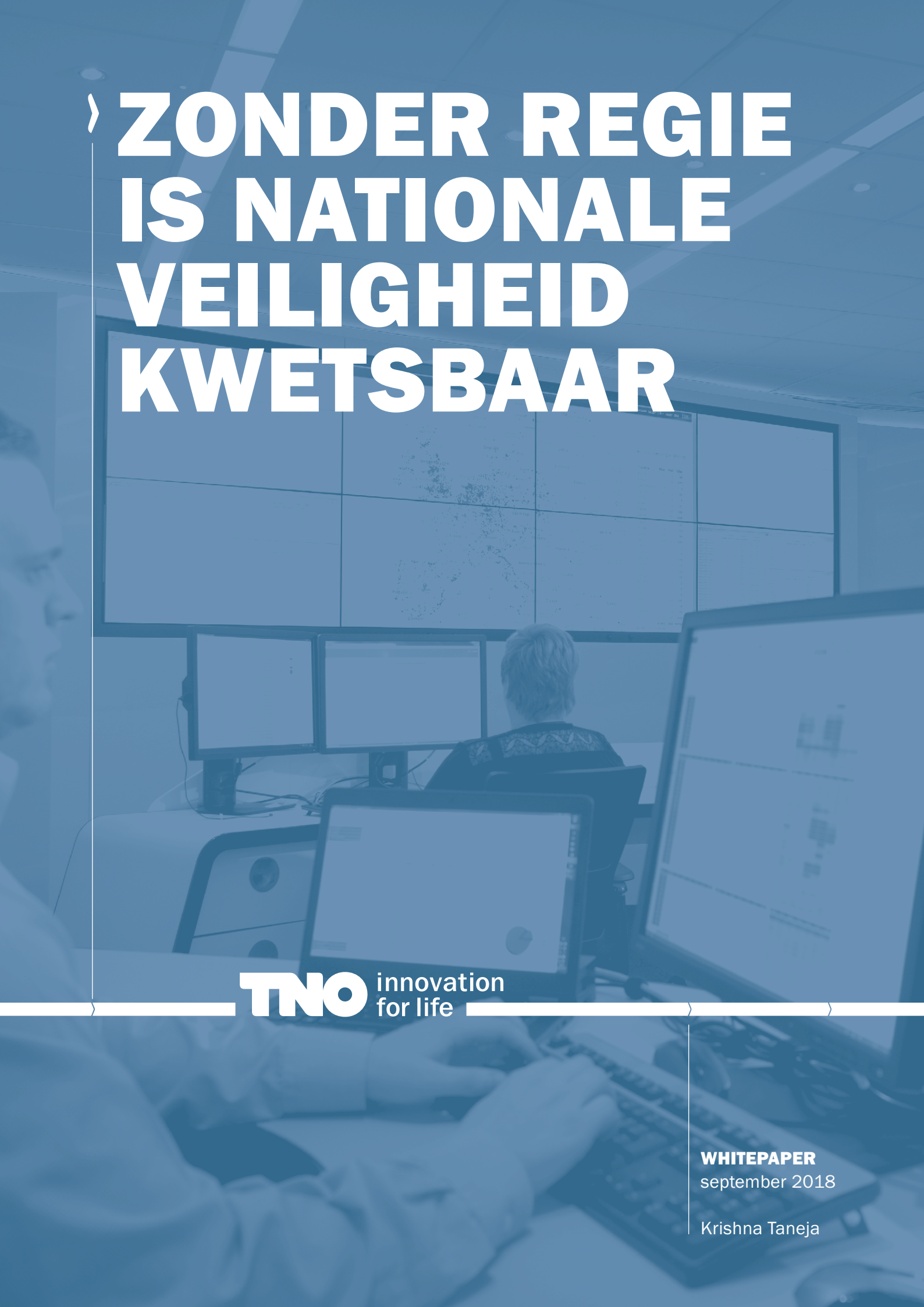
ZONDER REGIE IS NATIONALE VEILIGHEID KWETSBAAR



TNO innovation for life

WHITEPAPER
september 2018

Krishna Taneja

De **ontwikkelingen** binnen het **veiligheidsdomein** gaan sneller dan ooit, vooral door de enorme groei van de hoeveelheid informatie en nieuwe technologieën als artificial intelligence, augmented reality en krachtige sensoren.

Veiligheidsorganisaties in Nederland zoals **Defensie** en de **politie** besteden vanzelfsprekend aandacht aan deze ontwikkelingen, maar doen dit doorgaans afzonderlijk op voor hen relevante vraagstukken.

De toekomstige ontwikkelingen, en de grote rol van technologie daarin, maken een **nationale technologie-agenda** onmisbaar.

In zo'n agenda kunnen ministeries en veiligheidsorganisaties **vraagstukken schetsen** die van belang zijn en deze vertalen in **onderzoeks- en ontwikkelprogramma's**.

De agenda zorgt voor een natuurlijke verbinding tussen alle betrokkenen, leidt tot kennisdeling en tot het **bundelen van krachten** op dominante ontwikkelvragen.

INHOUDSOPGAVE

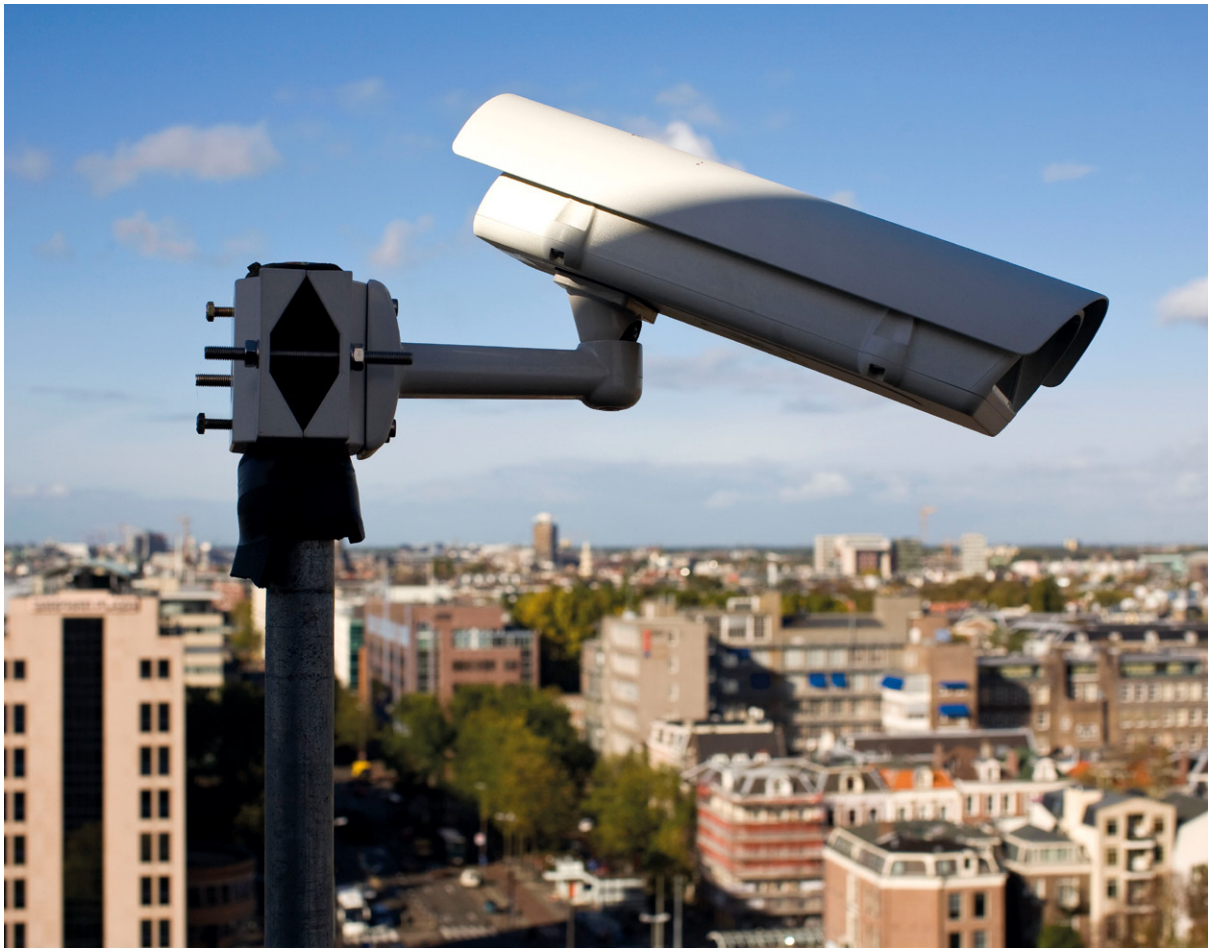
INLEIDING

Technologie ontwikkelt zich snel. Dit biedt zowel kansen als bedreigingen voor de Nederlandse overheid en veiligheidsorganisaties. Juist vanwege de breedte en snelheid van de ontwikkelingen is samenwerking cruciaal. Door kennis, ervaring en middelen te bundelen vergroot de overheid het rendement van haar research and development-inspanningen. Een goede aanzet daartoe is het opstellen van een nationale technologie-agenda, die accenten legt op geprioriteerde ontwikkelingen en de samenwerking versterkt tussen betrokken organisaties.

Een rode draad binnen vrijwel alle ontwikkelingen is de sterk toenemende hoeveelheid data die beschikbaar is. Informatie uit de feitelijke en virtuele wereld is in volume en diversiteit inmiddels zo omvangrijk dat analisten en beslissers er makkelijk in verdwalen. Dit probleem wordt vaak geduid als information overload. Op veel veiligheidsterreinen lijkt de grens van de menselijke capaciteit bereikt en gaat technologie een steeds grotere rol spelen.

Dit whitepaper maakt de noodzaak duidelijk om te komen tot een technologie-agenda voor een gerichte aanpak van de veiligheid in Nederland. Deze agenda maakt het mogelijk de werkprocessen van veiligheidsorganisaties, onder invloed van technologische ontwikkeling, te verbinden en beschikbare kennis en capaciteit beter te richten.

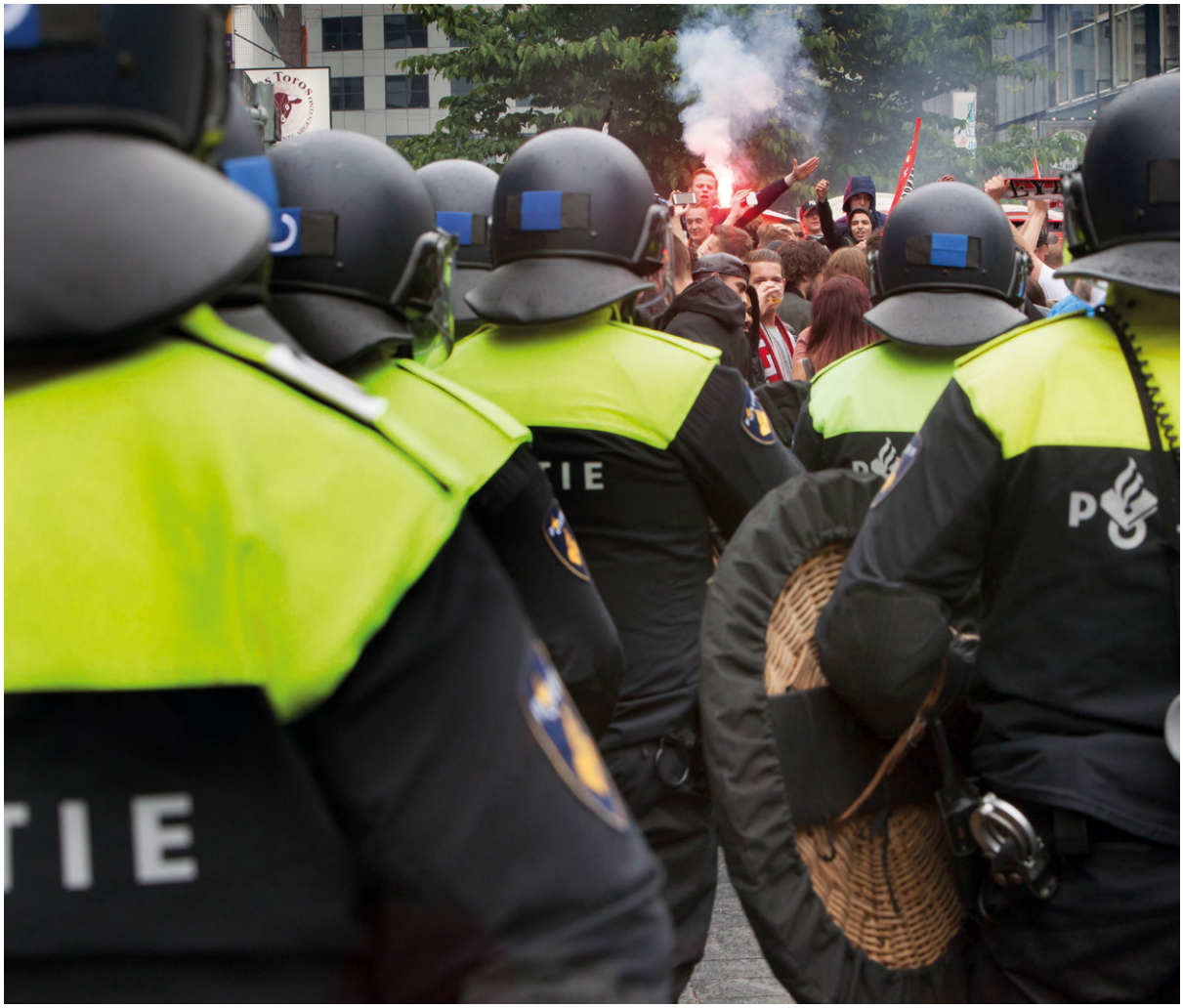
De technologie-agenda heeft als invalshoek de huidige praktijk, sterke verbondenheid tussen veiligheid en technologie en het geeft een antwoord op toekomstige ontwikkelingen.



DE GEVAREN EN KANSEN VAN TECHNOLOGIE

Wat gebeurt er als innovaties in de zorg, industrie of een ander domein in handen vallen van kwaadwillenden? Technologische innovaties bieden fascinerende mogelijkheden, die ook leiden tot nieuwe vormen van criminaliteit en rechtstatelijke beïnvloeding zoals identiteitsfraude, cybercrime en het snel mobiliseren van groepen mensen. Nieuwe mogelijkheden die de mens juist moeten helpen worden misbruikt. 3D printen van materialen en voedsel biedt bijvoorbeeld kansen, maar deze technologie maakt ook het vervaardigen van wapens mogelijk uit materialen die op Schiphol 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 kinderporno, wapen- en drugshandel.

Voor de overheid liggen er kansen om op basis van open en afgeschermde data verdachte personen realtime te monitoren en tijdig te intervenieren



Het zijn allemaal verontrustende ontwikkelingen waar de overheid, en in het bijzonder veiligheidsorganisaties, een antwoord op moet hebben in nauwe samenwerking met wetenschap en bedrijfsleven. Beleidsmakers en professionals in het veiligheidsdomein moeten in staat zijn de technologische ontwikkelingen te volgen en vooral te doorgronden, om vervolgens onveiligheid en criminaliteit gericht en doelmatig te kunnen aanpakken.

Met het verschuiven van criminaliteit van de fysieke naar de digitale wereld is het tijd om aandacht te vragen voor meer aanwezigheid op het web. Voor de overheid liggen er kansen om op basis van open en afgeschermde data verdachte personen realtime te monitoren en tijdig te interveniëren.

Een belangrijke ontwikkeling is de toepassing van artificial intelligence om gedrag van mensen te voorspellen. Neem het systeem Quin dat is ontwikkeld om voortvluchtigen op te sporen. Het werkt op basis van het scripten van gedragingen om daarmee voorspellingen te doen. Artifical intelligence in combinatie met het doorzoeken van data geeft de mogelijkheid te detecteren, analyseren en voorspellen. Sensorsystemen, van camera's tot radars, worden steeds intelligenter door uit alle gedetecteerde data snel bruikbare informatie te distilleren.

Zo kunnen technologische ontwikkelingen bedreigend zijn voor de veiligheid en vragen ze om nieuwe concepten. De overheid beschikt over een krachtig potentieel aan hoogwaardige veiligheidsorganisaties en kennisinstellingen die in samenwerking met bedrijven veel kunnen bereiken en een passend antwoord kunnen geven op dreigingen en maatschappelijke veiligheidsvraagstukken. Een voorwaarde voor succes is wel dat we werken vanuit een gezamenlijk perspectief van dominante technologische ontwikkelingen en oplossingen.

INNOVEREN IN VEILIGHEID DOOR DE OVERHEID

Met een begroting van ruim tien miljard euro heeft het ministerie van Justitie en Veiligheid (JenV) het op zes na grootste budget van de Rijksoverheid. Voor het aanjagen van innovatie en vernieuwing heeft het ministerie in mei 2017 de Strategische Kennis- en Innovatieagenda (SKIA) gepubliceerd. De SKIA 'richting en ruimte voor kennisontwikkeling en innovatie' legt verbinding met de innovatieagenda's van kennisinstituten, waaronder TNO, andere ministeries en bedrijven. Twee maanden daarvoor rondde het ministerie van JenV een technologiescan af die externe technologische ontwikkelingen in beeld brengt en afzet tegen de maatschappelijke opgaven van het ministerie. Beide documenten geven een goede aanzet tot het gezamenlijk ontwikkelen van innovaties, maar de praktijk laat zien dat grote organisaties als politie, Immigratie- en Naturalisatiedienst en Dienst Justitiële Inrichtingen dit zelf oppakken binnen hun eigen organisatie.

Het ontbreekt aan structurele organisatie-overschrijdende samenwerking op het gebied van innovatie

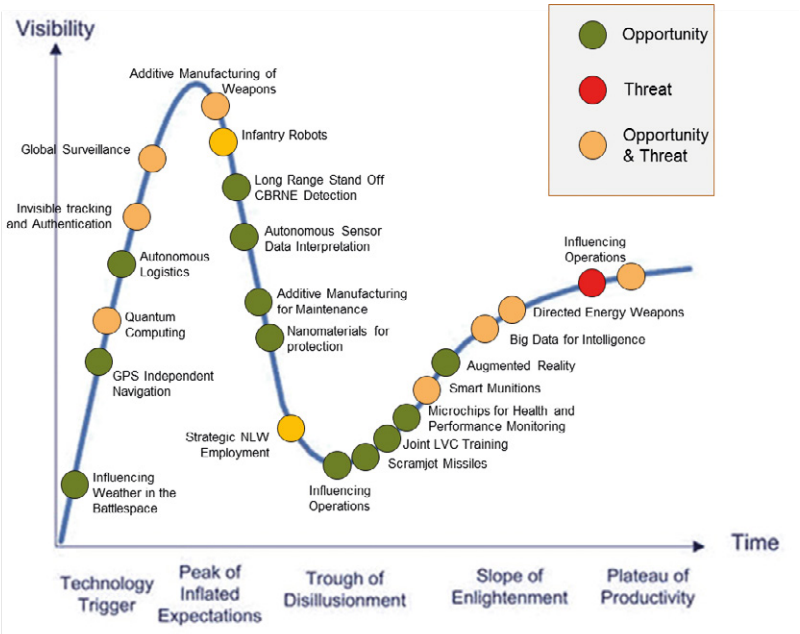
Het ministerie van Defensie geeft een prominente plek aan de ontwikkeling van technologische en andere innovaties in het kader van de permanente vernieuwing van de krijgsmacht. Defensie werkt gericht aan de versterking van relevante kennisgebieden, nationale en internationale samenwerking op het gebied van onderzoek en ontwikkeling, en het innovatieve vermogen van de defensieorganisatie. Om hieraan richting te geven heeft Defensie de Strategie-, Kennis- en Innovatieagenda 2016-2020 ‘Voorblijven in een onveiliger wereld’ opgesteld. Defensie maakt daarin onderscheid tussen programmatische innovatie en technologieontwikkeling via contractonderzoek. In de begroting voor 2018 is voor dit en ander wetenschappelijk onderzoek ruim 60 miljoen euro opgenomen. Innovatie en technologie zijn daarmee prominent verankerd in de ontwikkeling van de krijgsmacht. Maar door het ontbreken van een nationale agenda en het vaak vertrouwelijke karakter van het onderzoek word kennis in beginsel niet breder gedeeld.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, verantwoordelijk voor onder andere de Algemene Inlichtingen- en Veiligheidsdienst en de aanpak van ondermijning van de samenleving en rechtsstaat, kent verschillende innovatie-programma's. Die zijn bijvoorbeeld gericht op de verbetering van het contact tussen burger en overheid en het vergroten van de mogelijkheden van digitale dienstverlening. Ook werkt het ministerie aan beleid om overheidsdata optimaal beschikbaar te stellen. Innovatie lijkt daarmee minder gericht op de aanpak van veiligheidsvraagstukken, terwijl die zich hier juist wél voor leent in samenwerking met gemeentelijke overheden.

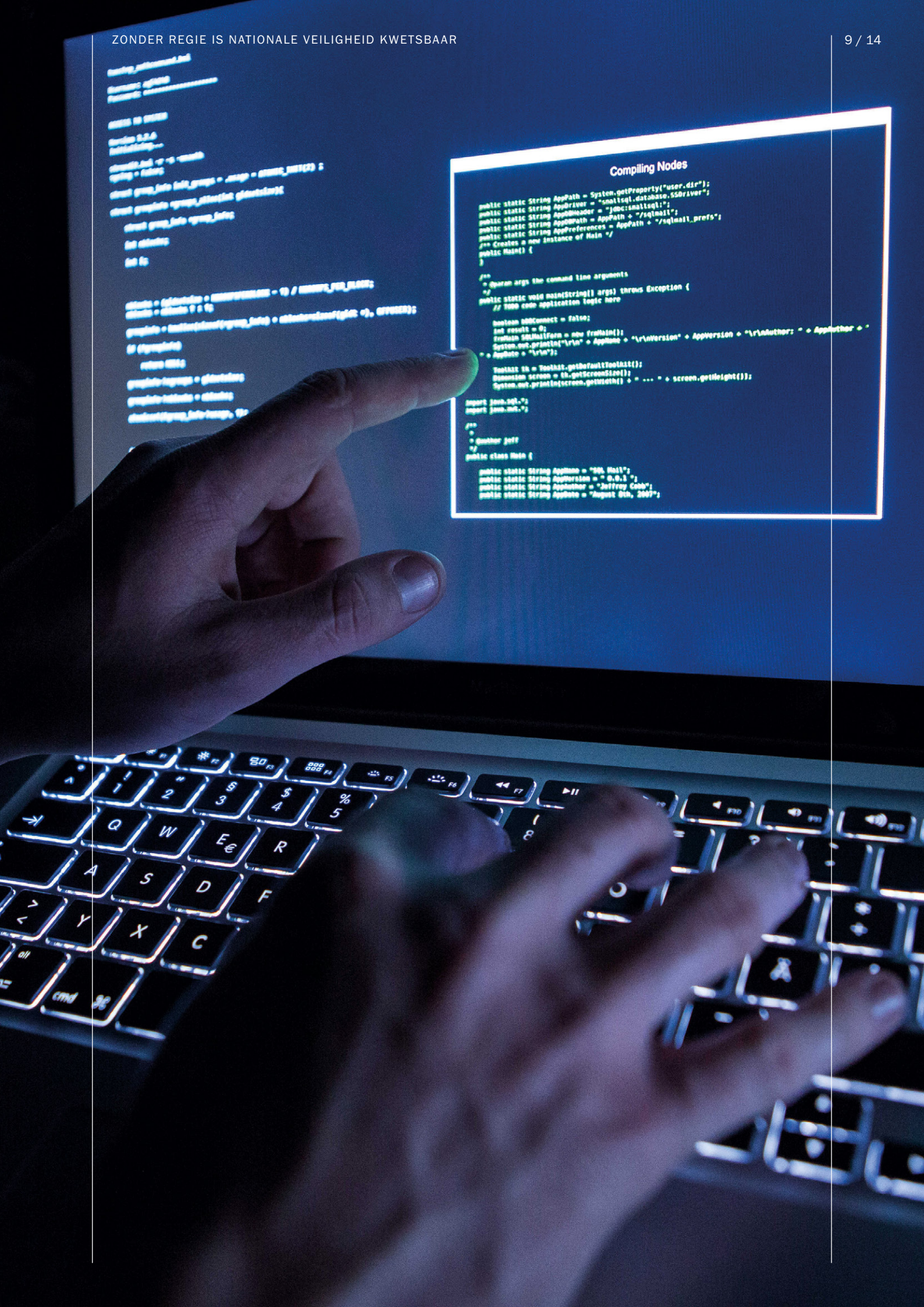
Dit korte overzicht van de huidige praktijk laat zien dat er in meer of mindere mate aandacht is voor innovatie en technologie. Het ministerie van Defensie werkt volgens een strak innovatieproces, terwijl bij Justitie en Veiligheid de SKIA vooral een verbindend karakter heeft. Het ontbreekt aan structurele organisatie-overschrijdende samenwerking op het gebied van innovatie. Daardoor gaan kansen verloren. Veel kennis ontwikkeld in het ene domein is vaak ook toepasbaar in een ander domein. Door kennisuitwisseling mogelijk te maken, kunnen ministeries en veiligheidsorganisaties van elkaars innovatiepraktijk leren.

VEILIGHEID EN TECHNOLOGIE VERBONDEN

Een veelgehoorde opvatting is dat overheden en andere organisaties steeds achterlopen waar het gaat om het toepassen van de nieuwste technologieën, omdat deze zich exponentieel ontwikkelen. De praktijk laat echter zien dat veel ontwikkelingen niet alleen al lang voor de snelle groei bekend zijn, maar ook dat veel organisaties er wel degelijk in slagen deze bij te houden. Onderstaand figuur brengt dit in beeld.



FIGUUR 1: INNOVATIES GEPLOT OP DE HYPE CYCLE


Compiling Nodes

De snelle groei betreft de toenemende hoeveelheid informatie die mensen te verwerken krijgen. De grens van de menselijke verwerkingscapaciteit lijkt in veel gevallen bereikt en de technologie krijgt een steeds grotere inbreng. Hieronder volgen drie voorbeelden.

1 TERRORISME EN RADICALISERING

Het in woord en geschrift verspreiden van jihadistische content en het zaaien van angst gebeurt in toenemende mate online. Detectie van dit soort boodschappen op het grote wereldwijde web blijkt moeilijk. Oplossingen voor dit vraagstuk zijn te vinden in monitoring van het internet, ondersteund door technieken om snel en adequaat informatie te kunnen duiden en methoden om effectief te kunnen interveniëren zoals het snel verwijderen van online content.

2 AANPAK ONDERMIJNING

Veiligheidsorganisaties, gemeenten en samenwerkingsverbanden zoals de Taskforce Brabant-Zeeland verzamelen op dit moment grote hoeveelheden data om die vervolgens te analyseren voor de aanpak van ondermijning. Zo stellen de Regionale Informatie- en Expertisecentra integrale informatiedossiers samen en openen steeds meer gemeenten datacenters om eigen analyses te maken. Dit is bij uitstek een terrein waarin steeds meer informatie beschikbaar komt, maar waar het steeds moeilijker wordt voor de mens om verbindingen te leggen en de juiste conclusies te trekken. Daarom zijn slimme algoritmen nodig die snel data kunnen koppelen, verrijken en analyseren met de nodige aandacht voor rechtsstatelijkheid en privacy.

3 CYBERCRIME EN DIGITALE DREIGING

Cyberaanvallen, variërend van het verspreiden van virussen tot het lamleggen van vitale infrastructuren, vergroten de behoefte aan zicht op online dreigingen en middelen om te interveniëren. Er wordt hard gewerkt aan gereedschappen voor realtime dreigingsanalyses op organisatieniveau. Maar dat is slechts het begin, omdat het aantal actoren in cyberveiligheid groot is en de informatie vrijwel oneindig. Om een completer en duidelijker beeld te krijgen is een realtime analyse nodig die gebruik maakt van informatie die nationaal en internationaal wordt gedeeld. Ook voor interventies is betere nationale en internationale coördinatie gewenst.

Deze voorbeelden geven aan dat professionals in het veiligheidsdomein door de grote hoeveelheid data steeds afhankelijker worden van technologie. Die moet in staat zijn informatie te integreren, te filteren en te analyseren. Technologie moet in het geval van digitale dreigingen zelfs autonoom kunnen reageren omdat menselijke reactie-snelheden ernstig tekortschieten. Artifical intelligence en technieken als deep learning vragen op dit moment nog veel handwerk en zijn allerminst ‘plug and play’. Veel organisaties zijn er door schade en schande achter gekomen dat uitrol van nieuwe veelbelovende technologieën veel tijd kost, en bovendien kostbaar en risicovol is.

TECHNOLOGISCHE ONTWIKKELINGEN

Op basis van de huidige technologische ontwikkelingen, diverse prominente veiligheidsvraagstukken in Nederland en de stand van de ontwikkeling in de organisaties zijn technologiegebieden te identificeren[1] die de basis vormen voor een nationale technologieagenda. Hiervoor bestaan verschillende methodieken en zijn voorbeelden te vinden in de eerder genoemde documenten van JenV en Defensie. Een interessante methode is te kijken naar de technologie gebieden in relatie tot de processen in de (veiligheids)organisaties. Door dit te doen wordt zichtbaar dat de invloed van technologie en de noodzaak te ontwikkelen per proces kan verschillen. Het clusteren tussen de processen en organisaties geeft een goede inventarisatie voor verdere ontwikkeling.

De verschillende technologiegebieden en werkprocessen van veiligheidsorganisaties kunnen geclusterd worden tot prioritaire innovatiegebieden voor de nationale technologieagenda. De indeling hieronder is een voorbeeld van zo'n clustering. In het proces om te komen tot zo'n nationale technologieagenda zal een dergelijke methodiek helpen om behoeften en innovatiegebieden duidelijk te benoemen.

CLUSTERS:
– Data acquisitie – Waarneming
– Data analyse – Intelligence
– Menskunde – Gedrag en performance
– Command & Control – Besluitvorming
– Cyber Security – Digitale domein
– Autonome systemen – Slimme omgeving
– Fysieke bescherming – Materiaal en concepten
– Strategische toekomstplanning – Verkenningen en strategie

Een interessante methode is te kijken naar technologiegebieden in relatie tot de processen in (veiligheids) organisaties

1 Bronnen: Technologieradar Veiligheid 2014, TNO 2014 R10864 (2014); Technologieverkenning Nationale Veiligheid, Analistennetwerk Nationale Veiligheid (2014).

WAT LEVERT HET OP

DATA ACQUISITIE – WAARNEMING

Verwerving van data via sensoren en andere bronnen biedt de mogelijkheid om meer proactief, efficiënter en effectiever te werken op basis van informatie. Het leidt tot verhoging van het (relevante) waarnemingsvermogen en een versterking van de informatiepositie.

CYBER SECURITY – DIGITALE DOMEIN

(Vroege) detectie van dreigingen in het digitale domein en beveiliging en bescherming van informatie dragen bij aan de veiligheid in het digitale domein.

DATA ANALYSE – INTELLIGENCE

(Big) data-analyse biedt de mogelijkheid meer informatiegestuurd te werken: niet alleen achteraf, maar ook real-time. Koppelen van data uit verschillende bronnen kan leiden tot extra informatie en de ontwikkeling van voorspellende modellen. Het leidt tot informatie die relevant is voor het vergroten van de veiligheid.

AUTONOME SYSTEMEN – SLIMME OMGEVING

Autonome systemen die beschikken over artificial intelligence kunnen worden ingezet voor het verrichten van inspecties en surveillances in voor de mens ontoegankelijke of gevaarlijke omgevingen. Gegevens uit slimme infrastructuur, slimme platformen en het Internet of Things kunnen worden gebruikt voor het verkrijgen van een beter inzicht in de omgeving.

MENSKUNDE – GEDRAG EN PERFORMANCE

Automatische gedragsanalyse of -herkenning vergroot het identificerend vermogen. Naast toepassing voor analyse achteraf zijn er mogelijkheden om te beschikken over real-time informatie en voorspellende scenario's. Dit kan bijdragen aan een verschuiving van reactief naar preventie en proactief opereren.

FYSIEKE BESCHERMING – MATERIAAL EN MAATREGELEN

Ontwikkeling van nieuwe weerbaarheids- en beschermingsconcepten dragen bij aan veiligheid in het fysieke domein.

COMMAND & CONTROL – BESLUITVORMING

Situational awareness is van belang om op operationeel/tactisch/strategisch niveau ondersteuning van de operatiën te bieden en deze te kunnen aansturen. In toenemende mate bieden systemen ondersteuning voor het nemen van beslissingen.

STRATEGISCHE TOEKOMST-PLANNING – VERKENNINGEN EN STRATEGIE

De ontwikkeling van dit gebied biedt de mogelijkheid om proactief in te spelen op nieuwe ontwikkelingen: technologische mogelijkheden, nieuwe toepassingen en nieuwe proactieve werkwijzen.

TOT SLOT

In deze whitepaper is in het kort beschreven dat de veiligheid van de Nederlandse samenleving in toenemende mate onderhevig is aan technologische ontwikkelingen. Dit geldt ook voor de internationale veiligheid. De technologische ontwikkelingen zijn aan de ene kant complex en verlopen snel, maar tegelijkertijd zijn ze over het algemeen vrij goed voorspelbaar en terug te brengen tot een paar relevante technologiegebieden.

Nieuwe technologieën zorgen ervoor dat steeds grotere hoeveelheden data verwerkt en geanalyseerd kunnen worden. De veiligheid neemt toe door maatregelen die op basis van deze data-analyses worden genomen. Zo kan de veiligheid toenemen van specifieke locaties en personen. Op internet en social media kan betere monitoring plaatsvinden om dreigingen vroegtijdig te onderkennen en sneller te kunnen interveniëren.

Om als overheid adaptief te kunnen blijven in een veranderende omgeving is inzicht nodig in de werkprocessen van veiligheidsorganisaties en hoe die de komende jaren in meer of mindere mate worden beïnvloed door technologische ontwikkelingen en de behoefte aan nieuwe technologiën.

Door de werkprocessen van de verschillende organisaties te clusteren ontstaat een beeld van de collectieve opgave die ze hebben. Daardoor kan tussen de betrokken ministeries vervolgens het gesprek worden gevoerd over de methodiek, wijze van prioritering en vooral de wijze waarop de ontwikkeling in de organisaties met elkaar kunnen worden verbonden. Verbinding is noodzakelijk omdat complexe technologie om stevige aandacht en de beste beschikbare kennis vraagt in Nederland en daarbuiten. Dat lukt niet met autonome ontwikkeling binnen de organisaties als individuele speler.

Vanuit het verkregen inzicht kan de stap worden gezet naar de ontwikkeling van een technologieagenda die het mogelijk maakt een gemeenschappelijk beeld van de ontwikkelingen te vormen en vervolgens regie te voeren op de uitvoering, strevend naar synergie tussen onderzoek- en ontwikkelinspanningen van verschillende veiligheidsorganisaties in Nederland.

Dit paper is een uitnodiging, met hoge urgentie, om aan de slag te gaan. Wij roepen alle betrokken partijen op hierover met ons na te denken en samen concrete innovaties gestalte te geven in het belang van onze veiligheid.

CONTACT
Krishna Taneja MSc MA
Directeur Nationale Veiligheid
Unit Defence, Safety and Security
Den Haag - Oude Waalsdorperweg
krishna.taneja@tno.nl
+31 (0)88 866 10 00

TNO innovation for life

TNO.NL

18-9849