Algemene gegevens	
Titel VP/ERP	Vraaggestuurd Programma Veilige Maatschappij (VPVM) [P102]
ERP/Missiegedreven Thema / MMIP	Veiligheid
Contactpersonen TNO (DM/SD/VPM)	Dr. T.W.J. van Ruijven
Contactpersoon overheid of topsector	Mr. H. Hanoeman en drs. B. ter Luun (Ministerie van Justitie en Veiligheid)

Programma 2021	
Samenvatting	Veiligheid is een voorwaarde voor welzijn en economische ontwikkeling. Veiligheid is niet vanzelfsprekend. De bedreigingen voor veiligheid zijn divers en veranderen voortdurend. De snelheid van ontwikkelingen is dusdanig dat het justitie- en veiligheidsdomein op hoog tempo moet innoveren om de dreiging het hoofd te kunnen bieden en Nederland veilig te houden. Veiligheid is één van de vijf centrale maatschappelijke thema's binnen het missiegedreven topsectoren en innovatiebeleid van het kabinet. Het is de ambitie van het kabinet om daarbij gebruik te maken van de nieuwste wetenschappelijke inzichten en (sleutel) technologieën met aandacht voor ethische en maatschappelijke vragen. Om veiligheidsvraagstukken aan te pakken, zal volgens dit vastgestelde beleid steeds een combinatie van technisch, digitaal, sociaal, maatschappelijk, juridisch, gedragswetenschappelijk, organisatorisch, sociaalpsychologisch en (geo)politiek onderzoek nodig zijn[1]. TNO draagt bij aan deze ambitie door met het Vraaggestuurd Programma Veilige Maatschappij (VPVM) relevante nieuwe kennis en technologie te ontwikkelen en deze te vertalen naar innovatieve toepassingen in de praktijk. TNO zet middels het VPVM in op een meerjarige onderzoeksprogrammering voor justitie- en veiligheidsorganisaties. Het doel van deze meerjarige programmering is toepassingsgerichte wetenschappelijke kennis op te bouwen en technologie te ontwikkelen op díe onderwerpen die voor het justitie- en veiligheidsdomein het belangrijkst zijn. Voor 2021 zijn elf meerjarige programmeringen ingericht[2] waaronder onderzoek met de Dienst Justitiële Inrichtingen (DJI), het Nationaal Cyber Security Centrum (NCSC) en het Landelijke- en de Regionale Informatie en Expertise Centra (LIEC en RIEC's) voor de bestrijding van ondermijnende criminaliteit. Om voor deze organisaties het verschil te maken, wordt de onderzoeksprogrammering in 2021 gefocust op zes thema's die al centraal stonden in VPVM en deze aan te vullen met verkennend, breed geprogrammeerd onderzoek op een drietal onderzoekslijnen die naar verwachting in de (nabije) toekomst van groot belang zullen worden voor het justitie- en veiligheidsdomein. De thema's voor 2021 zijn: - Cybersecurity & societal resilience (CYBER) - Versterking van de strafrechtketen (CRIME) - Crisisbeheersing (CRISIS) - Contraterrorisme (CTER) - Intelligence (INTEL)

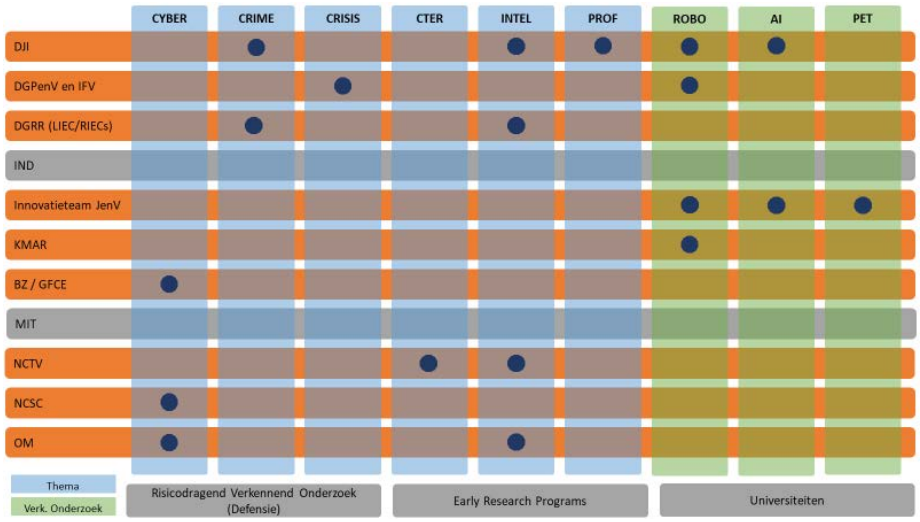
[1] Tweede Kamerbrief Missiegedreven Topsectoren- en Innovatiebeleid d.d. 26 april 2019

[2] Naast het VPVM is een apart maar samenhangend kennisopbouwprogramma voor de Politie (KOP) ingericht.

	- Weerbaarheid van veiligheidsprofessionals (PROF)
	- Verkennend onderzoek:
	  o Kunstmatige intelligentie (AI)
	  o Privacy Enhancing Technologies (PET)
	  o Robotica
	
	In het verkennend onderzoek wordt ingezet op technologie ontwikkeling zoals multi sensor integratie (robotica), de efficiëntie van AI beslisalgoritmen in relatie tot operationele vereisten (Kunstmatige intelligentie) en de ontwikkeling van een *secure inner join* om attributen van versleutelde informatie te kunnen analyseren (PET). Daarnaast wordt voor elk onderwerp in het verkennend onderzoek een serie use cases ontwikkeld waaronder de inzet van robots voor surveillance, veilige datadeling voor het bestrijden van ondermijnende criminaliteit en de inzet van AI beslisondersteuning voor het bepalen van beveiligingsregimes in justitiële inrichtingen.

Korte omschrijving	Binnen het VPVM wordt kennis opgebouwd en toepasbaar gemaakt ten aanzien van fenomenen zoals ondermijnende criminaliteit, nieuwe technologie zoals robotica, sociaalwetenschappelijke vraagstukken zoals de invloed van sociale media op het politieoptreden of organisatiekundige vraagstukken zoals innovatiemanagement. In het onderzoek wordt altijd gezocht naar het verband tussen techniek, processen, mensen en organisaties. Ook wordt expliciet gekeken naar de praktijk waarin kennis en technologie moeten worden toegepast. Innovatie staat immers niet voor uitvinden, maar voor toepassen in de praktijk. TNO zet in het VPVM 2021 – 2024 in op een thematische, meerjarige samenwerking met justitie- en veiligheidsorganisaties. Voor 2021 zijn elf[3] meerjarige onderzoeksprogrammeringen ingericht of voorzien met: - Dienst Justitiële Inrichtingen (DJI) - Directoraat-Generaal Politie en Veiligheidsregio's (DGPenV) en het Instituut Fysieke Veiligheid (IFV) - Directoraat-Generaal Rechtspleging en Rechtshandhaving (DGRR) / Landelijke- en de Regionale Informatie en Expertise Centra (LIEC en RIEC's) - Immigratie en Naturalisatie Dienst (IND) - Innovatieteam ministerie van Justitie en Veiligheid - Koninklijke Marechaussee - Ministerie van Buitenlandse Zaken - Multidisciplinair Interventie Team (ondermijning) - Nationaal Coördinator Terrorisme en Veiligheid (NCTV) - Nationaal Cyber Security Centrum (NCSC) - Openbaar Ministerie (OM) Om voor deze organisaties het verschil te maken, wordt de onderzoeksprogrammering gefocust op díe onderwerpen die voor het veiligheids- en justitiedomein het belangrijkst zijn. Voor 2021 is ervoor gekozen zes thema's uit VPVM te behouden en deze aan te vullen met verkennend onderzoek op drie onderzoekslijnen die naar verwachting in te toekomst van groot belang zullen worden. De thema's zijn:

[3] TNO werkt ook meerjarig samen met de Politie. Vanwege de omvang van deze samenwerking vindt dit plaats in een separaat vraaggestuurd programma.

	- Cybersecurity & societal resilience (CYBER)
	- Versterking van de strafrechtketen (CRIME)
	- Crisisbeheersing (CRISIS)
	- Contraterrorisme (CTER)
	- Intelligence (INTEL)
	- Weerbaarheid van veiligheidsprofessionals (PROF)
	- Verkennend onderzoek:
	  o Kunstmatige intelligentie (AI)
	  o Privacy Enhancing Technologies (PET)
	  o Robotica
	
	In onderstaande matrix zijn de meerjarige samenwerkingen weergeven ten opzichte van de thema's. Per thema is aangegeven in welke samenwerkingen onderzoek is geprogrammeerd.
	
	 

Resultaten 2021	**Onderzoeksprogrammering 2021 – 2024** **Cyber Security & Societal Resilience (CYBER)** Het doel van onderzoek binnen het thema Cyber Security & Societal Resilience is kennisopbouw op vijf met het Nationaal Cyber Security Centrum (NCSC) vastgestelde onderzoeksonderwerpen: - Herstelvermogen na cyberincidenten - Supply chain risico - Kwantificering van cyber risico's - Forecasting - Digitaal veilig thuiswerken Het onderzoek naar herstelvermogen is gefocust op de identificatie van kernfactoren die van invloed zijn op het herstelvermogen van organisaties na cyberincidenten, zowel in de context van information technologie (IT) als operationele technologie (OT). Het onderzoek resulteert in kennis voor een self-assessment instrument waarmee organisaties, specifiek de doelgroep van het NCSC, het eigen herstelvermogen van cyberincidenten kan beoordelen. Het onderzoek naar supply chain risico is gericht op de capabilities die organisaties moeten ontwikkelen voor het beheersen van ketenrisico's. De opgebouwde kennis ten aanzien van supply chain risico's wordt vastgelegd in

	een Secure Supply Chain leidraad van het NCSC. Het onderzoek naar kwantificering van cyber risico's focust zich onder andere op de vraag of in hoeverre vernieuwende methodieken (zoals simulaties) bijdragen aan het integreren van het cyberrisicomanagement in organisaties en in hoeverre modellen en data gebruikt door financiële instellingen en verzekeraars kunnen bijdragen aan het systematisch analyseren van risico's in de Nederlandse vitale processen. Daarnaast wordt kennis opgebouwd ten aanzien van het gebruik van incidentinformatie voor kwantitatieve risicoanalyse voor vitale processen. De opgebouwde kennis wordt vastgelegd in een ontwerpmethodiek voor de kwantificering van cyberrisico's inclusief aanwijzingen over hoe deze methodiek kan worden geïntegreerd met bestaande risicomanagement methoden. Het onderzoek naar forecasting is gericht op het versterken van de forecasting capaciteit van het NCSC en de organisatie in haar doelgroep en focust onder andere op de vraag welke meerwaarde en inzichten het gezamenlijk forecasten op specifieke cyberthema's oplevert. De kennisopbouw wordt onder andere vastgelegd in een blauwdruk voor een samenwerkingsplatform en een overzicht van forecasting *best practices*. Het onderzoek naar digitaal veilig thuiswerken is nieuw in deze programmalijn en komt voort uit de gevolgen van COVID-19. Het onderzoek richt zich onder andere op de vraag wat de toename van thuiswerken betekent voor de mogelijkheden om Nederlandse overheidsorganisaties en vitale aanbieders aan te vallen en welke systemen en applicaties de grootste kwetsbaarheid vormen. De kennisopbouw op dit onderwerp moet onder andere als input dienen voor de Alert Online weken in 2021. Het onderzoek in het thema CYBER wordt geprogrammeerd in samenhang met onderzoek binnen het Vraaggestuurd Programma ICT en verschillende EU H2020 projecten. **Versterking strafrechtketen (CRIME)** Het onderzoek in het thema CRIME vindt plaats in onderzoeksprogramma's met DJI, het OM, het Ondermijningslab en verschillende programma's van het Ministerie van Justitie en Veiligheid. Binnen het DJI-programma wordt onder andere gewerkt aan kennis ten behoeve van beslisondersteuning voor de indicatiestelling van het beveiligingsniveau en de zorgbehoefte in de forensische psychiatrie, een verkenning naar de toepassing van robotica binnen justitiële complexen en de ondersteuning van het verbeteren van het innovatieproces binnen de organisatie. De opgebouwde kennis wordt onder andere vastgelegd en beproefd in een prototype adviessysteem voor indicatiestelling en een DJI-innovatieradar. Het onderzoeksprogramma met het OM gaat met een verkennende fase van 1 jaar van start in 2021 en is gericht op kennis voor het versterken van het innovatieproces van de OM-organisatie en de identificatie van kennisbehoeften en gerelateerde onderzoeksvragen ten behoeve van de transformatiethema's van het OM (effect gestuurd werken, strategisch inzicht en versterking analysekracht). Hierbij wordt aangesloten bij de Gemeenschappelijke Kennisbasis (GEKI) activiteiten die inmiddels ook voor andere veiligheidsorganisaties (zoals Politie, DJI en Defensie) zijn gestart. De onderzoeksresultaten worden onder andere opgenomen in een trendradar voor de strafrechtketen en een OM-innovatieagenda en -roadmap. De in de afgelopen periode ontwikkelde Privacy Coin Monitor wordt geactualiseerd

	waarmee het OM inzicht kan verkrijgen in de ontwikkelingen en eigenschappen van *privacy crypto valuta* (zoals bijv. Monero) en hoe deze de strafrechtketen raken. Ook zal in het kader van OMTestlab verkennend onderzoek worden gedaan naar een “jurisprudentierobot” door de bruikbaarheid van nieuwe vormen van *machine learning* en *text mining* in dat kader te onderzoeken. Het Ondermijningslab programma voor Zuid-Nederland kent vanaf 2021 een vervolg waarbij naast de TaskforceRIEC Brabant-Zeeland nog 6 andere RIEC-regio’s en het LIEC zullen aansluiten. Gegeven de behoefte aan integrale aanpak van ondermijnende criminaliteit wordt binnen het Ondermijningslab 2.0 kennis opgebouwd ten behoeve van inzicht in ondermijnende criminele fenomenen en netwerken, als mede in het doorgronden van de door hun gehanteerde modus operandi. Deze kennis komt ook organisaties buiten de strafrechtketen ten goede zoals gemeenten en de belastingdienst. Daarnaast speelt de analyse en beïnvloeding van het individuele gedrag van subjecten een dominante rol. Daarbij ligt de focus op hoe deze kennis middels prototypes praktisch toepasbaar kan worden gemaakt zodat ze in potentie van direct van nut kan zijn voor de professionals betrokken bij de bestrijding van ondermijnende criminaliteit. Ten aanzien van ondermijningsfenomenen wordt onderzocht hoe wetenschappelijke kennis en open source data kan worden opgenomen in een Dynamisch Ondermijningsdashboard als inlichtingeninstrument in de bestrijding van ondermijnende criminaliteit. Op individueel niveau staat onderzoek centraal naar de vraag hoe gedragsmatige inzichten en modellen uit de sociale wetenschappen kunnen worden toegepast, dan wel vertaald ten nutte van gedragsanalyse en gedragsbeïnvloeding van individuen en groepen (daders, slachtoffers, getuigen) die relevant zijn in het kader van preventie, opsporing of waarheidsvinding. Uitgangspunt hierbij is dat de kennis moet kunnen worden gebruikt ten behoeve van concrete interventies. Het onderzoek binnen het thema CRIME maakt onder andere gebruik van uitkomsten van onderzoek binnen de Europese projecten LION-DC en ASGARD. **Crisisbeheersing (CRISIS)** Het onderzoek binnen het thema Crisisbeheersing is gericht op het ontwikkelen van kennis die nodig is om Nederland te beschermen, voor te bereiden en te reageren op gebeurtenissen die de maatschappij (op grote schaal) kunnen ontwrichten. De opgebouwde kennis wordt onder andere toegepast ten behoeve van de Veiligheidsregio’s, het Analistennetwerk Nationale Veiligheid en de bescherming van vitale infrastructuur. Een voorbeeld hiervan is de toepassing van kennis op het gebied van scenario ontwikkeling en systeemanalyse in het kader van de bestrijding van de COVID-19 crisis. Centraal in het onderzoek staan informatievoorzieningen voor de veiligheidssector (waaronder scenario ontwikkeling en voorspelmodellen), nieuwe samenwerkingsmodellen en onderzoek naar de missie kritische technische systemen van de incident- en rampenbestrijding zoals C2000, de meldkamers en de ontwikkeling van mobiele breedband verbindingen die in de toekomst beschikbaar komen voor hulpdiensten. Verder zal, in aansluiting op het verkennend onderzoek Robotica, gezocht worden naar nieuwe use cases van robotica voor incident- en rampenbestrijding.

	Bij het onderzoek rond Crisisbeheersing wordt, naast Europese partners, samengewerkt met de NCTV, de ministeries van Infrastructuur en Waterstaat en Economische Zaken en Klimaat, vitale aanbieders, Politie, gemeenten en veiligheidsregio's. Het onderzoek bouwt voor op de Europese projecten DRIVER+ en BROADWAY en het in uitvoering zijnde H2020 project STRATEGY. **Terrorismebestrijding (CTER)** Kennisopbouw op het gebied van Contra Terrorisme (CTER) en bewaken en beveiligen vindt plaats in afstemming met de Nationaal Coördinator Terrorisme en Veiligheid (NCTV). Het onderzoek is gefocust op vijf onderwerpen: - Detectie van intenties van kwaadwillenden - Technologie en preventie ten aanzien van Security (voorkomen aanslagen) - Beleidsontwikkeling - Risicowaarneming en taxatie - Technologie en preventie ten aanzien van Safety (vitale infrastructuur) Onderzoek op het gebied van detectie is onder andere gericht op de ontwikkeling van nieuwe scanningtechnologie. Het onderzoek naar risicowaarneming en taxatie wordt uitgevoerd in aansluiting op onderzoek voor de politie (taxatie) en Koninklijke Marechaussee (Risicowaarneming waarbij het onderzoek zich richt op onder andere de verbetering van grenstoezicht). Het onderzoek binnen het thema CTER bouwt voort op onderzoek in Europees verband in de projecten PERICLES, TRESSPASS en PRoTECT **Intelligence (INTEL)** Het onderzoek binnen het thema Intelligence is gericht op kennisopbouw ten aanzien van spraakherkenning en tekstanalyse, de toepassing van AI-beslisondersteuning (in aansluiting op het verkennend onderzoek AI-beslisondersteuning), beeldanalyse en organisatorische vraagstukken op het gebied van *collaborative intelligence*. Belangrijke onderzoeksvragen zijn hoe nieuwe technologie op het gebied van spraakherkenning en automatische tekstanalyse kan worden ingezet ten behoeve van justitie- en veiligheidsorganisaties, hoe beeldanalyse kan worden aangewend voor bewakings- en intelligence vraagstukken en hoe data veilig en vertrouwelijk kan worden gedeeld tussen meerdere organisaties. De uitkomsten van het onderzoek binnen het thema Intelligence worden ingezet ten behoeve van de Immigratie en Naturalisatiedienst (IND), het Openbaar Ministerie (OM) en de Belastingdienst. Het onderzoek wordt afgestemd met Intelligence gerelateerd onderzoek binnen het kennisopbouwprogramma Politie en bouwt voort op uitkomsten van de EU H2020 projecten ASGARD en D4FLY. **Weerbare professional (PROF)** Het onderzoek binnen het thema Weerbare Professional is gericht op het gebied van professionele fitheid en professionele ontwikkeling. Binnen het onderzoek naar professionele fitheid staan vragen centraal als wat betekent

professionele fitheid voor verschillende beroepsgroepen in het justitie- en veiligheidsdomein (conceptualisatie en modelvorming)? Hoe kan professionele fitheid worden vastgesteld en gemeten (monitoring en terugkoppelingsinstrumenten)? En welke interventies zijn mogelijk en effectief om professionele fitheid te vergroten (interventies en organisatie)? De kennisopbouw op het gebied van professionele fitheid wordt onder andere opgenomen in de ontwikkeling van een prototype weerbaarheidsmonitor waarmee professionals en hun leidinggevenden in het justitie- en veiligheidsdomein hun eigen weerbaarheid en dat van hun team kunnen vaststellen en volgen. Voor dit onderzoek wordt ook gekeken naar toepassing van nieuwe of verbeterde sensortechnologie.
Het onderzoek naar professionele ontwikkeling is gericht op leren en specifiek op de vraag hoe de leerbehoefte en het leervermogen van professionals in het justitie- en veiligheidsdomein kan worden vastgesteld, gevolgd en gestimuleerd. Daarnaast wordt onderzocht welke nieuwe (immersieve) lasertechnologieën kunnen bijdragen aan de professionele ontwikkeling. De opgebouwde kennis ten aanzien van professionele ontwikkeling en leren moet justitie- en veiligheidsorganisaties helpen om professionals mee te laten ontwikkelen met hun snel veranderende omgeving.

Het onderzoek rond de weerbaarheid van professionals vindt grotendeels plaats in samenwerking met de Dienst Justitiële Inrichtingen (DJI) en wordt afgestemd met gerelateerd onderzoek in het kennisopbouwprogramma voor de Politie.

Verkennend onderzoek

Organisaties in het justitie- en veiligheidsdomein willen voorbereid zijn op de toekomst. Om dat mogelijk te maken, doet TNO verkenningen van nieuwe technologieën, met impact op het veiligheidsdomein, die zijn geselecteerd uit de TechScan van het ministerie van Justitie en Veiligheid. In een verkenning worden, aan de hand van de binnen VPVM in 2020 ontwikkelde SELFI-methodiek, de technische mogelijkheden en de verwachte maatschappelijke, juridische en ethische gevolgen van toepassingen van nieuwe technologieën verkend en vastgelegd. De verkenningen maken onderdeel uit van het proces van technologie-adaptatie van het ministerie van Justitie en Veiligheid[4] en stellen TNO, het ministerie en organisaties in het justitie- en veiligheidsdomein in staat de risico's van nieuwe technologie te beperken en de kansen te benutten. Per jaar wordt in afstemming met het Innovatieteam van het ministerie van Justitie en Veiligheid een selectie van onderwerpen voor de verkenningen gemaakt.

Naast de verkenningen doet TNO verkennend onderzoek om kennis op te bouwen ten aanzien van technologieën die naar verwachting een grote impact zullen hebben op het brede justitie- en veiligheidsdomein. Dit verkennend onderzoek is gericht op robotica, AI-beslisondersteuning en Privacy Enhancing Technologies (PET).

Het doel van het verkennend onderzoek ten aanzien van robotica is tweeledig. Ten eerste worden technologische ontwikkelingen waar nodig verder gebracht om deze daadwerkelijk te kunnen toepassen voor justitie- en

[4] https://techfocus.pleio.nl/file/download/57979894/White%20paper%20-%20Focus%20op%20Technologie.pdf

	veiligheidsorganisaties. Ten tweede wordt samen met deze organisaties gewerkt aan een selectie toepassingen (use cases) waarbij in de ontwikkeling synergievoordelen zijn te behalen. De verdere ontwikkeling van robotica technologie is binnen VPVM gefocust op observatie capabilities (*situational awareness*), robot-mens interactie, de intuïtieve besturing van roboticasystemen en de ontwikkeling van autonome roboticasystemen die zelf hun weg vinden en beslissingen nemen met behulp van kunstmatige intelligentie. Voor de intuïtieve besturing van roboticasystemen is het onderzoek aangesloten op het onderzoek in het kader van xPrize Avatar[5] waarin een op afstand bestuurd roboticasysteem wordt ontwikkeld met een multi sensorische beleving voor de robotbestuurder. Een belangrijke kennisbehoefte op dit vlak is hoe verschillende typen sensortechnologie kunnen worden gecombineerd om een zo groot mogelijke beleving van aanwezigheid in de omgeving van de robot te creëren (*telepresence*). Het onderzoek naar robot-mens interactie is onder andere gericht op kennisontwikkeling over de inzet van service robots of robotsystemen met een sociale functie waarbij de vraag centraal staat hoe roboticasystemen kunnen worden ontworpen om een sociale functie te vervullen. De selectie van toepassingen bestaat op dit moment uit roboticasystemen voor observatie voor de Politie, KMar, Veiligheidsregio's en Defensie en roboticasystemen met een sociale functie voor de DJI en de Politie. Het verkennend onderzoek op het gebied van kunstmatige intelligentie (AI) is toegespitst op vier thema's: 1. Information Mining, Multi-source Intel Analysis & Automated Evidence (*text mining*) 2. Privacy Preserving Risk Analysis 3. Computer-Aided Concept Discovery 4. Quality, Impact and Ethics Het doel van het onderzoek is om voor een aantal kern AI-technologieën voor het justitie- en veiligheidsdomein een gedeelde kennisbasis op te bouwen, omtrent technologie, kansen en kwaliteit, rekening houdend met beleidsdossiers rond ethiek, bias, privacy en transparantie. De kennisopbouw is specifiek gericht op vragen zoals hoe groot is de meerwaarde van een automatisch opgebouwd profiel ten opzichte van een door mensen opgebouwd profiel, of enkel ruwe tekst? Zowel in effectiviteit als uitlegbaarheid? In hoeverre kan bias optreden bij het gebruik van dergelijke methodes en hoe kan deze worden gedetecteerd? En hoe kan deze worden tegengegaan? In hoeverre kan een voldoende efficiëntie van AI-algoritmes voor operationele inzet gegarandeerd blijven? Zijn Deep Reinforced Learning methodes al ver genoeg ontwikkeld om effectief te zoeken naar nieuwe modus operandi en hiaten in wetgeving? Het aantal toepassingen van AI-beslisondersteuning in het justitie- en veiligheidsdomein zal in de loop van 2021 worden uitgebreid. De use cases waar al onderzoek voor wordt gedaan zijn onder andere de opsporing van onvindbare veroordeelden, verdachte ondernemingen in het kader van ondermijning en de indicatiestelling van beveiligingsniveau en zorgbehoefte in de forensische psychiatrie.

[5] xPrize Avatar is een competitie waaraan TNO in consortium meedoet. Begeleiding van dit project gebeurt gezamenlijk door de ministeries van Justitie en Veiligheid, Economische Zaken en Klimaat, Defensie en Infrastructuur en Waterstaat.

	Veel opgaven in het justitie- en veiligheidsdomein hebben baat bij informatie-uitwisseling tussen partijen. Naast betrouwbaarheid, kwaliteit en interoperabiliteit is het belangrijkste issue binnen het justitie- en veiligheidsdomein dat de data vaak gevoelig zijn, en dus niet zomaar onderling gedeeld kunnen worden. Het doel van het verkennend onderzoek naar privacy bestendige datadeling is het ontwikkelen van technologie voor veilige datadeling en het toepassen van deze technologie ten behoeve van actuele vraagstukken in het justitie- en veiligheidsdomein. De verdere ontwikkeling van technologie voor veilige datadeling is gefocust op Multi Party Computation, een verzameling technologieën gebaseerd op cryptografie die het mogelijk maken om analyses te doen op data van meerdere partijen zonder de data te hoeven prijsgeven. Kennisopbouw ten aanzien van deze technologieën is onder andere gericht op de ontwikkeling van een *secure inner join* waarmee veilig (versleuteld) de doorsnede en bijbehorende attributen van een database te bepalen zodat hier vervolganalyses op kunnen worden gedaan zonder de doorsnede zelf te leren. Een ander speerpunt is onderzoek naar *privacy preserving machine learning* waarbij onder andere kennis wordt opgebouwd over hoe MPC kan worden ingezet om AI-algoritmes te trainen, zonder de rekentijd te groot te laten worden. Naast technologieontwikkeling kent het verkennend onderzoek naar veilige datadeling toepassingsgericht onderzoek. De toepassingen waar onderzoek voor wordt gedaan zijn onder andere het opsporen van onvindbare veroordeelden, het delen van cybersecurity informatie, privacy vriendelijke beeldherkenning en fraudebestrijding. Voor deze use cases wordt onder andere onderzocht welke *identifiers* kunnen worden gebruikt om data te matchen, welke specifieke gevoelige data met behulp van welke technologieën kan worden gedeeld en welke juridische randvoorwaarden gelden.
Dynamiek	Het onderzoek en de kennisopbouw binnen VPVM worden gestuurd door middel van een meerjarige programmering. De structuur – zes thema's en verkennend onderzoek – is gelijk gebleven ten opzichte van 2020. De onderzoeksprogrammering van de thema's binnen de meerjarige samenwerkingen is hierboven toegelicht. Op hoofdlijnen worden, ten opzichte van voorgaande jaren, de volgende wijzigingen in de programmering doorgevoerd: - Het aandeel van het verkennend onderzoek ten opzichte van de totale programmering neemt toe met als doel de inbreng van nieuwe kennis en technologie die relevant is voor meerdere organisaties in het justitie- en veiligheidsdomein te vergroten. In het verkennend onderzoek zijn robotica, AI-beslisondersteuning en Privacy Enhancing Technologies (PET) voorlopig centraal gesteld. Op deze onderwerpen wordt technologie ontwikkeld en worden use cases uitgewerkt. In de komende jaren zal het aantal onderwerpen voor verkennend onderzoek en het aantal use cases per onderwerp worden uitgebreid. - Kennisopbouw en onderzoek buiten het verkennend onderzoek vindt nog uitsluitend plaats binnen meerjarige onderzoeksprogramma's met veiligheidsorganisaties - In 2021 wordt gestart met kennisopbouw in het kader van meerjarige samenwerkingen met het Openbaar Ministerie (OM), en de Immigratie en Naturalisatie Dienst (IND).

	- Het onderzoek binnen het thema Intelligence was gefocust op gemeentelijk intelligence maar wordt verbreed richting andere organisaties in het justitie- en veiligheidsdomein zoals de belastingdienst, het Openbaar Ministerie en mogelijk de Financial Intelligence Unit (FIU). - Voor een aantal onderwerpen is samenwerking met het bedrijfsleven onontbeerlijk. Dit geldt bijvoorbeeld voor de doorontwikkeling van slimme cameratechnologie, de implementatie van de weerbaarheidsmonitor binnen justitie- en veiligheidsorganisaties of de implementatie van use cases van Multi Party Computation. Waar mogelijk en relevant wordt kennisopbouw daarom gericht op samenwerking met het bedrijfsleven in het kader van de KIA Veiligheid en de Meerjarige Missiegedreven Innovatie Programma's.