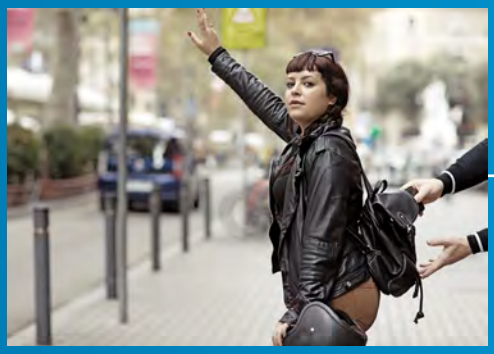
Smart Cities en stedelijke veiligheid

Slim delen en samen leren

The Hague Security Delta

Smart Cities en stedelijke veiligheid

Slim delen en samen leren



Inhoudsopgave

1 **Inleiding** 5

2 **Smart Cities** 7
2.1 Wat zijn Smart Cities? 7
2.2 Smart City architectuur 8
2.3 Kansen en dreigingen Smart City technologie en concepten 10

3 **Stedelijke veiligheid** 13
3.1 Wat is stedelijke veiligheid? 13
3.2 Veiligheidsbeleid van steden 15
3.2.1 Analyse huidige veiligheidsvraagstukken 15
3.2.2 Huidige aanpak veiligheidsvraagstukken 17
3.2.3 Toekomstige veiligheidsvraagstukken 18
3.2.4 Aanpak toekomstige veiligheidsvraagstukken 19

4 **Smart Cities en stedelijke veiligheid** 21
4.1 Het veiligheidspotentieel van een slimme stad 21
4.2 Specifieke kansen van Smart City voor stedelijke veiligheid 26
4.2.1 Kansen voor huidige veiligheidsvraagstukken 26
4.2.2 Kansen voor toekomstige veiligheidsvraagstukken 28
4.3 Bestuurlijke kansen voor stedelijke veiligheid 29
4.4 Benutten van Smart City kansen voor stedelijke veiligheid 30

5 **Conclusies en aanbevelingen** 33
5.1 Conclusies 33
5.2 Aanbevelingen 34
5.3 Hoe verder 36

Literatuurlijst 37

Bijlagen 38
Bijlage 1 – Overzicht van geanalyseerde integrale veiligheidsplannen 39
Bijlage 2 – Specifieke aanpakken per prioriteit 41
Bijlage 3 – Checklist ten behoeve van succesvolle implementatie 45
Bijlage 4 – Vorm en inhoud workshop implementatie 47

1 – Inleiding

Meer dan de helft van de wereldbevolking woont in steden, en verwacht wordt dat verstedelijking verder toe zal nemen. Dit legt druk op de leefbaarheid en daarmee ook de veiligheid van de steden. De ontwikkeling van de slimme stad (Smart City) is een opkomende strategie om de problemen vanuit bevolkingsgroei en urbanisatie aan te pakken. Slim worden is een breed gedeelde ambitie van grotere steden. In de EU implementeert ongeveer 90% van de steden met meer dan 500.000 inwoners slimme stadsprogramma's. Voor steden met 100.000 tot 500.000 inwoners is dit 51% [1]. Volgens onderzoek van McKinsey heeft de implementatie van Smart City concepten het potentieel om op het gebied van veiligheid het aantal sterfgevallen met 8-10% te verminderen, het aantal misdrijven met 30–40% en de reactietijd voor noodgevallen met 20–35% [2]. Smart City technologie en -concepten bieden dus mogelijkheden voor de aanpak van stedelijke veiligheidsvraagstukken.

Smart Cities benutten technische hulpmiddelen, datastromen en data-analyse als onderdeel van een vernieuwende aanpak die onder andere moet leiden tot een verhoogde kwaliteit van leven en een vergrootte duurzaamheid en veerkracht. Hoewel techniek de *enabler* is vormt dit nadrukkelijk slechts een deel van het fenomeen Smart Cities. Mensen, organisatie, goederenstromen, juridische en ethische vraagstukken: ze zijn allen verweven in de ontwikkeling van de nieuwe slimme stad.

We zien verschillende Smart City initiatieven met diverse doelstellingen, onder andere op het gebied van energie, milieu en mobiliteit. Veiligheid is vaak geen standaard onderdeel of doel van de initiatieven, ondanks de potentiële maatschappelijke- en economische waarde zoals hiervoor geschetst. Door de veiligheidsdoelstellingen van een stad mee te nemen bij het ontwerp van initiatieven kunnen kosten verdeeld en gereduceerd worden. Door nieuwe Smart City functionaliteiten in de stedelijke infrastructuur ontstaan tevens weer nieuwe veiligheidsvraagstukken, waar ook op ingespeeld zal moeten worden.

De Stichting The Hague Security Delta (HSD) heeft de combinatie TNO en van Aetsveld verzocht een duidingsstudie uit te voeren naar de praktische en toepasbare kansen en mogelijkheden van de inzet van Smart City technologie ten behoeve van de aanpak van stedelijke veiligheidsvraagstukken.

Deze publicatie is het resultaat van die compacte duidingsstudie en geeft een hoog-over schets van de intersectie van de twee aandachtsgebieden Smart Cities en stedelijke veiligheid. Daarnaast geeft de publicatie enkele handvatten voor de ontwikkeling van Smart City concepten voor de veiligheid van een stad. De publicatie beoogt beslissers en programmamanagers binnen overheid en bedrijfsleven te ondersteunen bij keuzen voor, en het ontwikkelen van, (*triple-helix*) trajecten op het gebied van Smart Cities en stedelijke veiligheid.

Voor deze duidingsstudie zijn een literatuurstudie en beleidsonderzoek uitgevoerd en zijn verschillende experts bevraagd. Daarnaast is een workshop georganiseerd waarin met materiedeskundigen vanuit gemeenten, bedrijfsleven en kennisinstellingen is nagedacht over hoe Smart City technologie kan worden ingezet voor de aanpak van verschillende stedelijke veiligheidsvraagstukken en wat daartoe moet gebeuren.

Deze publicatie geeft achtereenvolgens:

- Een compacte beschouwing van Smart City ontwikkelingen: Wat behelst het en waarvoor is het van meerwaarde? Wat zijn de kenmerken, ontwikkelingen en kansen en dreigingen?
- Een compacte beschouwing van maatschappelijke ontwikkelingen en stedelijke veiligheid: Wat zijn de verschillende aspecten van veiligheid? Wat zijn de huidige en toekomstige stedelijke veiligheidsvraagstukken?
- Een overzicht van kansen van Smart City technologie ten behoeve van stedelijke veiligheid: Hoe kunnen Smart City concepten inspelen op bestaande en toekomstige veiligheidsvragen?
- Als conclusie een samenvattende duiding van de mogelijkheden, beperkingen, en meerwaarde van Smart City ontwikkelingen voor stedelijke veiligheid. Daarnaast beschrijft het een aantal concrete aanbevelingen voor (*triple-helix*) samenwerking om tot innovatieve veiligheidsoplossingen te komen.

2 – Smart Cities

2.1 Wat zijn Smart Cities?

Een stad heeft allerlei verschillende functies, zoals een woonfunctie, onderwijsfunctie, werkfunctie, recreatieve functie, bestuursfunctie, handelsfunctie verzorgingsfunctie en beschermingsfunctie. Om ervoor te zorgen dat alle functies kunnen worden uitgevoerd, zal de omgeving daar zoveel mogelijk aan moeten bijdragen, zodat het voldoet aan alle behoeften en wensen van hen die in de stad wonen, werken of de stad doorkruisen of bezoeken. In dit onderzoek richten wij ons op een 'slimme stad' oftewel, een Smart City. Met het toevoegen van intelligentie aan een stad, door het inzetten van digitale innovatie en digitale technologie, kunnen de infrastructuur, de bronnen en de ruimtes optimaler benut worden ten behoeve van het gebruik en leefbaarheid van en in de stad. Grote steden kennen meer complexiteit, en er komen meer mensen en middelen bij elkaar, waardoor Smart City concepten ervoor erg bruikbaar kunnen zijn. Dat neemt niet weg dat Smart City concepten ook behulpzaam kunnen zijn voor kleinere steden en buiten stedelijk gebied. In een slimme stad worden technologie en data ingezet om betere beslissingen te nemen en bij te dragen aan een verbeterde leefomgeving. Technologie is daarbij een middel en geen doel op zich. De mens is het uitgangspunt.

De Europese Unie (EU) definieert de slimme stad als "Een systeem van mensen die omgaan met en gebruikmaken van energiestromen, materialen, diensten en financiering, op een zodanige wijze dat duurzame economische ontwikkeling, veerkracht en hoge kwaliteit van leven wordt gekatalyseerd. De stromen en interacties worden slim door strategisch gebruik te maken van informatie- en communicatie-infrastructuur en -diensten in een proces van transparante stadsplanning en -beheer dat inspeelt op de sociale en economische behoeften van de samenleving."

De uitdagingen waar steden mee te maken hebben omvatten verschillende domeinen: zorg, transport en logistiek, onderwijs, veiligheid, etc. Wanneer de problemen los beschouwd worden en deze door steden met intelligentie worden aangepakt, wordt vaak gesproken over bijvoorbeeld 'Smart Transport', 'Smart Energy' of Smart Environment'. Er circuleren ook nog andere termen die soms een overlappende betekenis hebben, zoals 'Resilient', 'Safe' en 'Sustainable Cities'. We beschrijven ze om een wat bredere context te geven aan de ontwikkelingen in steden.

- *Resilient Cities* zijn steden waarin het vermogen aanwezig is van individuen, gemeenschappen, instellingen, bedrijven en systemen om te overleven, zich aan te passen en te groeien, ongeacht de soort tegenslagen. Deze veerkracht vereist van steden om acties te ondernemen die steden beter maken op de korte en lange termijn, en laat steden gedijen in zowel goede als slechte tijden [3]. Een voorbeeld komt uit Kopenhagen. Aan de Helenevej, één van de straten in Kopenhagen is asfalt vervangen door tegels om regenwater door het oppervlak te laten sijpelen, in een poging overstromingen te voorkomen. Openingen tussen de tegels transporteren het water onder het wegdek, waar zich een reservoir bevindt. Bij extreme regenval kan daar het water worden vastgehouden. De weg is in staat gebleken om grote waterhoeveelheden probleemloos te verwerken tijdens hevige regenval. [4]
- *Safe Cities* worden vaak gezien als een subsysteem van Smart Cities [5]. Een Safe City omvat alle veiligheidsaspecten binnen een stad. De technologieën die op het gebied van veiligheid worden gebruikt, dragen bij aan een Safe City. De beschrijving van een Safe City die Maroš Lacinák en Jozef Ristvej hanteren is vergelijkbaar met de definitie van Smart City: "Een Safe City is een stad, die door de integratie van technologie en natuurlijke omgeving de effectiviteit van processen op het gebied van veiligheid verhoogt, om zo criminaliteit en terreurdreigingen te verminderen, om het leven van burgers te ondersteunen met een gezonde omgeving en eenvoudige toegang te verlenen tot gezondheidszorg, en het bereiken van snelle actie en/of noodhulpverlening bij dreigende of ontstane noodsituaties". In Chicago is een samenwerking aangegaan met Smart911, een gratis en vrijwillige service voor burgers om persoonlijke, medische of situationele informatie te verstrekken aan hulpverleners in geval van een noodsituatie. De stad is nu de grootste gebruiker van de dienst. Via de dienst kunnen gebruikers een veiligheidsprofiel maken met alle kritieke informatie waarvan ze willen dat

noodhulpverleners dit zouden weten, zoals locatie, voertuiggegevens, gezinsleden, reeds bestaande lichamelijke of psychische aandoeningen en andere opmerkingen die nuttig kunnen zijn in een noodgeval. De dienst kan bijdragen om hulpverleners te helpen sneller en adequater te reageren op noodsituaties. Voor alle deelnemende meldkamers in de Verenigde Staten waarmee een burger contact opneemt in geval van nood, is de informatie zichtbaar. [6]

- Tenslotte het begrip *Sustainable Cities*, oftewel duurzame steden. Het 'ICLEI - Local Government for Sustainability', een wereldwijd netwerk waarbij meer dan 1.500 steden, dorpen en regio's zijn aangesloten die zich samen committeren aan een duurzame toekomst, hanteert voor Sustainable Cities de volgende definitie: "Duurzame steden werken aan een milieuvriendelijke, sociaal en economisch gezonde en veerkrachtige leefgebied voor bestaande populaties, zonder afbreuk te doen aan het vermogen van toekomstige generaties om hetzelfde te ervaren" [7]. In de stad Vancouver in Canada is een strategisch actieplan ontwikkelt om voorop te blijven lopen in stedelijke duurzaamheid. Er ontplooien zich allerlei initiatieven met bedrijven, burgers en andere partijen om deze doelen te bereiken. Een voorbeeld is het doel om lopen, fietsen en openbaar vervoer aantrekkelijk te maken, ten behoeve van 'groen vervoer'. Daartoe hebben zij in 2017 en 2018 verbeteringen aangebracht door in bepaalde gebieden wandelpaden en fietspaden te onderscheiden, om het comfortabeler en veiliger en daarmee aantrekkelijker te maken. Verder investeren zij in verhoging van openbaar vervoerscapaciteiten [8].

Het mooie van Smart Cities is juist dat stedelijke opgaven cross-sectoraal kunnen worden aangepakt doordat verzamelde informatie voor meerdere domeinen meerwaarde kan hebben. Zowel bedrijven als burgers kunnen worden betrokken bij het oplossen van problemen, doordat zij over relevante data beschikken en/of doordat zij bij kunnen dragen aan oplossingen. Dit biedt kansen en win-win situaties voor meerdere sectoren en partijen. Het biedt ook de mogelijkheid voor een stedelijke gemeenschap om zich te ontwikkelen naar een *Smart Resilient City*. Dit vraagt overigens wel van het gemeentebestuur (college, gemeenteraad en ambtelijke organisatie) daar integraal en in partnership met burgers en het bedrijfsleven richting aan te geven.

Er worden al verschillende Smart City concepten toegepast in de wereld. In het kader op bladzijde 9 geven we voorbeelden daarvan. Het betreft concepten die daadwerkelijk geïmplementeerd zijn in een real-life setting. Ze zijn data-gedreven en dragen bij aan het oplossen van een maatschappelijk probleem, bijvoorbeeld op het gebied van transport of milieu. Hierbij heeft de gemeentelijke organisatie een actieve rol (direct of indirect). Vaak lag de aanleiding in ervaren problematiek in een ander dan het veiligheidsdomein, maar als spin-off heeft het ook effecten op de veiligheid of het veiligheidsgevoel. Soms zit er ook een keerzijde aan. Zo geldt voor het voorbeeld van milieuverbeteringen in Songdo dat het een heel milieuvriendelijke stad is, maar de stad wel ervaren wordt als een weinig 'levendige stad'. Alles is zo gedigitaliseerd, dat mensen interactie missen met elkaar. Menselijk contact wordt meer ervaren als koud en afstandelijk [9].

In Nederland is een NL Smart City Strategie opgesteld [10] waarin een visie over de richting voor Smart Cities is beschreven. Ook hebben de G5-steden samen aan een Smart City agenda gewerkt, die elke twee jaar vernieuwd wordt. Dit met als doel om de inzet van digitale innovatie te versnellen, ondersteund door de VNG en vanuit integraliteit samen te werken. Het doel van deze agenda is de ontwikkeling van Smart Cities uit te breiden naar andere gemeenten.

2.2 Smart City architectuur

De extra meerwaarde van Smart Cities zit in de combinatie van infrastructuur, data en/of diensten over verschillende domeinen heen. Daarom is het gebruikelijk voor Smart City architecturen een lagenmodel te gebruiken, in plaats van een verticaal model met silo's voor elk van de domeinen afzonderlijk.

Smart City toepassingen zijn er in verschillende domeinen in de *maatschappij*, zoals energie, zorg, transport en logistiek, onderwijs, milieu, veiligheid, bestuur en media, maar ook over domeinen heen. De *toepassingen* maken gebruik van *diensten,* zoals informatiediensten en dashboards, ten behoeve van monitoring en efficiënte besluitvorming. Die diensten zijn gebaseerd op *data,* bijvoorbeeld met betrekking tot verkeer, statistische gegevens, bewegingen en locaties. De data komt vanuit objecten, apparaten sensoren netwerken in de *infrastructuur*, zoals gebouwen, wegen, voertuigen, camera's en telecommunicatienetwerken. In deze duidingsstudie hanteren we daarom als denkmodel onderstaande Smart City architectuur (figuur 1).

Voorbeelden Smart City concepten

Verbeterde mobiliteit

Op het gebied van mobiliteit kunnen Smart City toepassingen ervoor zorgen dat verkeersstromen beter te beheersen en te optimaliseren zijn. In Helmond is een 'living lab' opgezet waar nieuwe innovaties op het gebied van mobiliteit getest worden in de praktijk. Met gebruik van slimme software worden de verkeersregelinstallaties aangestuurd op een kruispunt, op basis van allerlei data die ontvangen wordt, zoals data vanuit GPS-signalen, lussen in de weg en verkeerscamera's. Dit alles ten behoeve van een betere verkeersdoorstroming: de wachtrijen worden ermee verkort, en voertuigen hoeven minder vaak te stoppen. Dit zorgt direct voor minder vervuiling en grotere verkeersveiligheid en is dus een goed voorbeeld van de combinatie van verschillende domeinen, in dit geval ook het milieu en veiligheidsdomein [11].

Schoner en duurzamer milieu

Smart City concepten op het gebied van milieu- en omgevingsveiligheid worden primair geïnitieerd om de energieproductie en het energiegebruik te optimaliseren, het milieu te monitoren en te interveniëren als er onveilige situaties (gemeten waarden) ontstaan. In 2009 is in Zuid-Korea de nieuwgebouwde stad Songdo gelanceerd. Deze ontwikkeling kwam vanuit de politieke drive voor een stad met lage CO2-uitstoot en duurzame groei. Sensoren in de hele stad houden van alles bij. Van de temperatuur tot de verkeersomstandigheden. In sommige gevallen kan deze informatie ook naar bewoners worden gestuurd, bijvoorbeeld om te waarschuwen voor veiligheidsrisico's.

Betere zorg

Op het gebied van zorg kunnen slimme toepassingen een rol spelen bij het verschuiven van de behandeling van ziekten naar het voorkomen ervan en de burger in staat te stellen langer, gezonder en productiever te leven. Daarnaast kunnen diezelfde toepassingen zorgen voor adequatere (nood)hulpverlening. Steden versterken aan de ene kant bepaalde gezondheidsrisico's, zoals lucht- en geluidshinder, vervuiling, en uitbraken van overdraagbare ziekten. Steden kunnen aan de andere kant een rol spelen in het voorkomen en/of snelle behandelen van gezondheidsrisico's door het verzamelen van data. Hierdoor wordt de onveiligheid weer verminderd. Een goed voorbeeld komt uit de stad Zurich, waarbij in de stad luchtvervuilingscontrolenetwerken aanwezig zijn, die de luchtkwaliteit meten. Er is voor de burgers een app ontwikkeld die het minst vervuilde pad tussen twee locaties in de stad aangeeft, waarmee de blootstelling aan slechte stoffen wordt geminimaliseerd.

Versterking burgerparticipatie

Digitale middelen zoals apps en platforms kunnen bijdragen aan de verbondenheid tussen de burger en overheid. Het kan burgerparticipatie of overheidsparticipatie stimuleren, waarbij kennis of diensten tussen beide partijen wordt uitgewisseld ten behoeve van een betere leefbaarheid en veiligheid van de stad. Een voorbeeld is het betrekken van burgers bij de stadsplanning. In Singapore zag men goede redenen om burgers te betrekken bij het plannen van openbare ruimtes. Burgers kunnen betrokken worden door e-participatie en online ontwerptools. Een toepassing in Singapore is de 'Quick Urban Analysis Kit', een online ontwerptool waarin burgers 3D-objecten kunnen aanpassen of verplaatsen om te visualiseren hoe zij denken over hoe de ruimte zou moeten worden ingericht. Door het betrekken van burgers kunnen belangrijke gemeenschappelijke ruimtes zodanig worden aangepakt dat zorgt voor inclusieve samenleving en de cohesie tussen burgers wordt gestimuleerd. Dat draagt bij aan vermindering van de onpersoonlijkheid en de gevoelde onveiligheid. Het betrekken van burgers stimuleert het gevoel van eigenaarschap en verantwoordelijkheid en creëert een groter vertrouwen in de overheid.

Meer veiligheid

In het veiligheidsdomein bieden Smart City concepten rechtstreeks kansen. Publieke veiligheid omvat veel, van de reactietijd van hulverleningsdiensten, toezicht en handhaving, veiligheidsinspecties en -interventies, tot economische, omgevings- en sociale criminaliteit. Data kan worden ingezet om de algemene veiligheid te waarborgen, incidenten te voorkomen en waar nodig interventies (hulpverlening, aanhoudingen, verstoringen en bescherming) efficiënt en effectief in te zetten. Een voorbeeld komt uit Antwerpen, waar een crowd management-oplossing werd toegepast tijdens de Tour de France. Crowd management gaat om de mogelijkheid van het monitoren van groepen mensen en ze eventueel te sturen om hun veiligheid te waarborgen. In Antwerpen werden bezoekersaantallen gemonitord door het aantal verbonden mobiele telefoons met de masten, en werd ook de positie bepaald van deze mensen. Op een dashboard werden deze gegevens getoond, zodat de hulpdiensten real time op de hoogte gehouden konden worden [12].

Figuur 1 **Smart City architectuur**

Smart City concepten bieden een bijdrage aan maatschappelijke doelen, door gebruikers in en over verschillende domeinen van bruikbare informatie te voorzien, op basis van data en informatie vanuit objecten, apparaten, sensoren en netwerken. Door het modelleren van een stad (digital twin) kunnen via simulaties vroegtijdig risico's in kaart worden gebracht en het effect van inrichtingskeuzes worden voorspeld voor betere besluitvorming.

In de voorbeelden van Smart Cities vanuit allerlei plekken in de wereld ligt soms de nadruk op de slimme infrastructuur, bestaande uit objecten, apparaten, sensoren en netwerken (*Smart Infrastructure*) en soms de nadruk op de slimme maatschappij (*Smart Society*), vanuit maatschappelijke doelen op het gebied van *People* (sociaal), *Planet* (milieu, omgeving) *Profit* (economisch) en *Government* (participatieve democratie). Uiteindelijk gaat het om één holistisch ontwikkelmodel waarin zowel maatschappelijke doelen vanuit mensen als de daarvoor benodigde elementen vanuit de technologie samenkomen. In de Smart City architectuur uit figuur 1 hebben wij dat aan elkaar verbonden.

De stedelijke veiligheidsvraagstukken uit het volgende hoofdstuk passen bij de maatschappelijke doelen. Van daaruit (*top-down*) én vanuit de technische mogelijkheden (*bottom-up*) zijn kansen voor Smart City en stedelijke veiligheid geïdentificeerd.

2.3 Kansen en dreigingen Smart City technologie en concepten

Smart City technologie en concepten bieden kansen voor verschillende domeinen waaronder voor stedelijke veiligheid. Dit onder meer door informatie-gedreven te kunnen werken en beslissen, gebaseerd op (real-time) data uit alle domeinen van de stad. Kansen liggen op het gebied van het verbeteren van de kwaliteit van leven van de inwoners (*People*), door bijdrage aan de maatschappelijke doelen. Ook zijn er kansen voor duurzaam gebruik van grondstoffen en milieu (*Planet*), door efficiëntere besteding en effectiever gebruik van publieke middelen. Verdere kansen liggen nog op het gebied van een betere (groenere) economie (*Profit*) door de innovatiekracht en economisch rendement en het bevorderen van een goed ontwikkelde lokale democratie (*Governance*), door samenwerking, betrokkenheid en verbinding [13]. Hoofdstuk 4 gaat nader in op de kansen specifiek voor het veiligheidsdomein.

Naast de kansen, zijn er ook potentiele risico's en dreigingen vanuit de toepassing van Smart City technologie. Deze hebben te maken met de afhankelijkheid van infrastructuren (zoals voor informatie, mobiliteit, energie en water) die al dan niet moedwillig kunnen worden verstoord of misbruikt. Een ander risico heeft te maken met de ethische kanten van het gebruik en combineren van data en het trekken van conclusies daaruit. En wie is aansprakelijk als in de slimme stad iets misgaat? Onderstaande vraagstukken gaan zich sowieso voordoen. Smart City concepten bieden een kans om deze vraagstukken cross-sectoraal en met burgers en bedrijven aan te pakken.

Kwetsbaarheid van infrastructuren

Smart City concepten bouwen op data uit de digitale wereld van sensoren, databronnen en datanetwerken. In toenemende mate is deze digitale wereld verweven met de fysieke wereld waarin we leven. Zo is het vliegverkeer afhankelijk van de ICT-systemen voor het inchecken, het openbaar vervoer afhankelijk van systemen voor verkeersgeleiding en het energienetwerk afhankelijk van aansturing door controlesystemen. Een 'intelligente' stad maakt gebruik van sensoren, netwerken, databronnen en actuatoren[1] voor het monitoren van situaties, het nemen van beslissingen en het uitvoeren/regelen van interventies. Daarmee is de stad in potentie kwetsbaar voor al dan niet moedwillige verstoringen in de infrastructuren, die kunnen leiden tot verkeerde beslissingen, uitval van voorzieningen en in het uiterste geval chaos in- en om de stad.

1 Apparaat dat iets in beweging kan brengen of in werking kan stellen.

Juridische en ethische risico's

In Smart City concepten kan allerlei data worden gecombineerd. Dit leidt in potentie tot meer en betere inzichten, o.a. ten behoeve van de veiligheid. Belangrijk hierbij is de authenticiteit en betrouwbaarheid van data, en ook het doel waarvoor het verzameld is (doelbinding). Het combineren met en gebruik van onjuiste data kan leiden tot verkeerde inzichten en beslissingen. Daarnaast is bij dit soort concepten de afweging tussen privacy en veiligheid van belang. De juridische en ethische vraag is 'hoe ver mag en wil je gaan?' Toepassingen met een puntensystemen zoals in China waarbij met behulp van camera's met gezichtsherkenning burgers worden herkend bijvoorbeeld wanneer ze door een rood verkeerslicht lopen, passen niet goed bij de Europese cultuur en maatschappelijke waarden. Maatschappelijke discussies over het vertrouwen in de bescherming van data en algoritmen die data verwerken naar bepaalde inzichten spelen op het terrein van veiligheid sterker dan bij de voorspelling van verkeersdrukte of het weer. Het is belangrijk een goede balans te vinden tussen veiligheid en vrijheid en zorg te dragen voor inclusie, door als overheid samen met de samenleving zorg te dragen voor democratische wetten en regels in het digitale, publieke domein, ten behoeve van wenselijke en gelijke (digitale) behandeling.

Eigendom, beheer en gebruik van data

Allerlei partijen bezitten allerlei data. Deze data kan van meerwaarde zijn voor andere partijen. Soms direct, en soms indirect door het combineren van deze data met andere data waardoor nieuwe inzichten verkregen worden. Vanwege het eigenaarschap van data is het niet altijd wenselijk, of (wettelijk) mogelijk deze data te verkrijgen. Met Smart City concepten kan er ook weer nieuwe data beschikbaar komen. Voor al deze data is het de vraag wie daar de (wenselijke) eigenaar van is. Dit zal moeten worden vastgelegd. Dat geldt ook voor wie en waartoe de data gebruikt mag worden, en hoelang en waar de data wordt opgeslagen, waarbij rekening gehouden wordt met geldende wet- en regelgeving. Het gaat ook om de rol en macht van tech-bedrijven, zoals Google, Amazon en Facebook. Er zal nagedacht moeten worden over welke data van hen mogelijk nuttig is, maar ook welke rol we dergelijke bedrijven laten spelen in een Smart City. Daarbij spelen ook ethische kwesties: is er in dit opzicht vertrouwen in bedrijven, of vertrouwen in de overheid en in hoeverre is afhankelijkheid van derde partijen gewenst? En wat is in de toekomst de impact van aanbieders van platformdiensten zoals Airbnb en Uber op de veiligheid in de stad?

Aansprakelijkheid

Door ver doorgevoerde digitalisering en integratie kan het gebruik van de fysieke infrastructuur als een *service* worden aangeboden. Een voorbeeld hiervan is *mobility as a service*: op het juiste moment staat de juiste vervoersmodaliteit voor je klaar tegen voor jouw aantrekkelijk voorwaarden. Wanneer dit in een slimme stad gaat convergeren met autonome voertuigen en intelligente kruispunten ontstaat er nieuw vraagstuk. Namelijk: wat nu als het fout gaat? Wie is er verantwoordelijk voor het veroorzaken van een aanrijding en hoe kan de wet door politie en justitie in een dergelijk complexe situatie nog gehandhaafd worden? Een andere belangrijke Smart City ontwikkeling is *peer-to-peer*. Digitalisering maakt niet alleen dat veel behoeftes in de stad als dienst (*as a service*) kunnen worden afgenomen. Ze maakt die diensten ook veel beter vindbaar en aan elkaar te koppelen. Burgers in de stad doen steeds vaker rechtstreeks zaken met elkaar zonder tussenkomst van een tussenpersoon. Door het koppelen van diensten ontstaat ook een nieuw soort ruileconomie waarin "mijn" decentraal uit zonnepanelen opgewekte energie in "jouw" huis gaat in ruil voor toegang tot "jouw" vervoersservice. Waar de afspraken decentraal en veilig in bijvoorbeeld een blockchain kunnen worden geregistreerd. Maar ook hier geldt: wat nu als het fout gaat?

Voor al deze juridische, ethische en governance vragen rond privacy, dataopslag, datatoegang en dataverwerking is het van belang verantwoordelijkheden in de keten duidelijk te maken: wie doet wat en wat is de rol van de overheid ten opzichte van de rol van bedrijven. Wat betreft cyberveiligheid van stedelijke (smart city) infrastructuur is het belangrijk om, net als voor kritische infrastructuren, te zorgen voor maatregelen ter voorkoming van verstoringen en/of ter beperking van de negatieve ('domino')effecten. Transparante en ethisch verantwoorde ontwikkeling van concepten vraagt om verantwoorde waardecreatie [14] samen met burgers: *Privacy by Design* en ook *Ethical by Design* ofwel *Responsible by Design*.

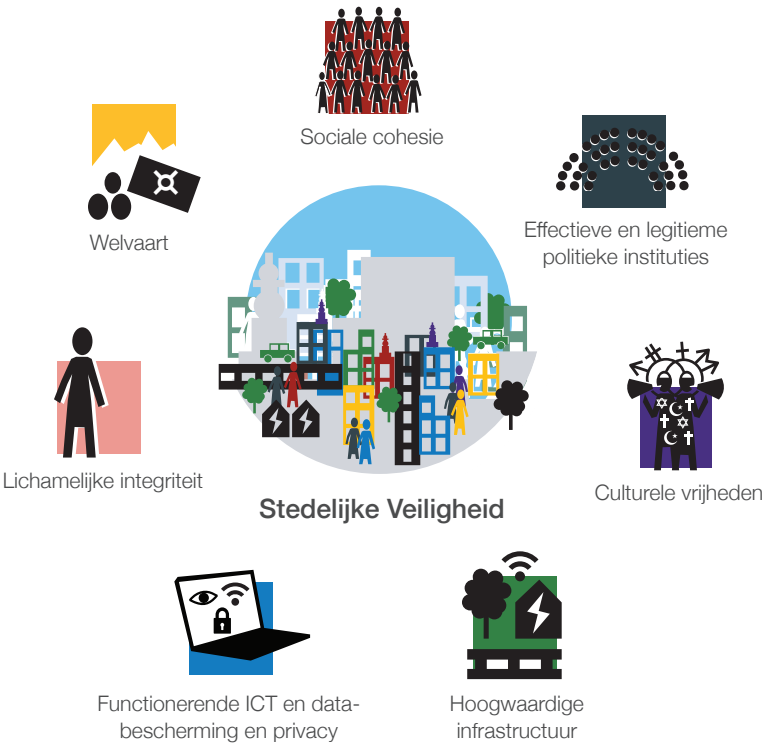
3 – Stedelijke veiligheid

3.1 Wat is stedelijke veiligheid?

Onze verwachtingen van steden op gebied van zaken als werkgelegenheid, veiligheid en leefbaarheid nemen toe. Gelijktijdig worden steden en hun autoriteiten geconfronteerd met oude en nieuwe risico's en bedreigingen. Er is geen breed gedragen opvatting over wat er allemaal wel en niet onder stedelijke veiligheid valt (dit loopt van hondenpoep tot radicalisering), hoe dit met elkaar samenhangt (bijvoorbeeld de gezamenlijke impact van ruimtelijke inrichting, woningbeleid, kwaliteit scholen en handhaving) en hoe veiligheid het best in de praktijk gerealiseerd kan worden. In de beleidspraktijk heeft stedelijke veiligheid de volgende breedte [15]:

- Veilige woon- en leefomgeving (overlast, veelvoorkomende criminaliteit zoals inbraken en diefstal (high impact crimes), het onveiligheidsgevoel);
- Bedrijvigheid en veiligheid (veilig ondernemen, veilige winkelcentra, veilig uitgaan en veilige evenementen, veilig toerisme);
- Jeugd en veiligheid (jeugdoverlast, jeugdgroepen, alcohol & drugsgebruik, veiligheid in en om de school);
- Fysieke veiligheid (verkeersveiligheid, rampenbestrijding & crisisbeheersing, brandveiligheid, gevaarlijke stoffen);
- Integriteit en veiligheid (aanpak georganiseerde criminaliteit, ondermijning, veilige publieke taak (VPT), polarisatie & radicalisering, informatieveiligheid, integriteit).

In de studie naar een visie op Amsterdamse stedelijke veiligheid onderbouwt *The Hague Centre for Strategic Studies* stedelijke veiligheid als "de mate waarin de kernwaarden en -belangen van een stedelijke gemeenschap weerbaar zijn tegen huidige en toekomstige dreigingen, en dit ook als zodanig wordt ervaren" [16]. Deze kernwaarden, zoals weergegeven in figuur 2, reflecteren wat mensen in een stad van belang vinden om te beschermen en omvatten: lichamelijke integriteit, welvaart, sociale cohesie, effectieve en legitieme politieke instituties, culturele vrijheden, hoogwaardige infrastructuur inclusief goed functionerende ICT en data, bescherming en privacy.



Figuur 2 **Kernwaarden van stedelijke veiligheid** [16]

Wanneer mensen fysieke en/of psychische schade hebben of ervaren als gevolg van criminaliteit (inbraak, straatroof), ongelukken of leefomstandigheden, dan is hun *lichamelijke integriteit* in het geding. De veiligheid van de stad wordt negatief beïnvloed wanneer (bepaalde groepen) inwoners van de stad onvoldoende *welvaart* hebben of dat zo ervaren door bijvoorbeeld economische recessie hetgeen zich uit in werkloosheid of slechte economische vooruitzichten. Er is sprake van een sterke *sociale cohesie* in de stad wanneer bewoners elkaar onderling vertrouwen en minderheden geïntegreerd zijn. Kortom, iedereen ervaart zich onderdeel van de stedelijke gemeenschap. Een ander kenmerk van stedelijke veiligheid is de mate waarin inwoners kunnen en willen deelnemen aan politieke processen. Vertrouwen in *effectieve en legitieme politieke instituties* (autoriteiten, politieke partijen en politici) is hiervoor een voorwaarde. Ook de mate waarin mensen hun identiteit (taal, seksuele oriëntatie of geloof) mogen uitdragen en zij dat ook zo ervaren, de *culturele vrijheid*, draagt bij aan de veiligheid van de stad. Een veilige stad biedt ook een *goede infrastructuur* zoals transport, energie (stroom), natuurlijke ruime en recreatiemogelijkheden. Deze zaken en ook de mate waarin dit door de inwoners zo wordt ervaren, verhogen de kwaliteit van de leefomgeving. Ten slotte is het leven in de stad steeds meer gerelateerd aan *goed functionerende ICT*. Hieronder valt ook de *bescherming van data en de privacy* van inwoners.

Als we naar de definitie van stedelijke veiligheid en genoemde kernwaarden kijken, dan vallen een paar zaken op:

Veiligheid gaat over alles en iedereen
Stedelijke veiligheid is een aspect dat iedereen raakt want de stedelijke gemeenschap omvat alle denkbare actoren: autoriteiten, burgers, maatschappelijke organisaties en bedrijven. Voor een bewoner gaat veiligheid over het voorkomen van persoonlijke fysieke of psychische schade (lichamelijke integriteit) en het zich veilig genoeg voelen om de eigen identiteit uit te dragen (culturele veiligheid). Maar het kan ook gaan om het uitvallen van één van de infrastructuren van de stad, bijvoorbeeld het elektriciteitsnetwerk. Dit kan leiden tot sociale onrust en in extreme gevallen zelfs maatschappelijke ontwrichting. Bij een individuele kernwaarde zoals lichamelijke integriteit kan veiligheid gaan over de aantasting van fysieke integriteit als gevolg van bijvoorbeeld criminaliteit maar ook als gevolg van (verkeers)ongelukken, natuurrampen of luchtvervuiling.

Bijna alles hangt met alles samen
De verschillende kernwaarden beïnvloeden elkaar: een significante daling van de welvaart voor bepaalde groepen in de stad werkt sociaaleconomische ongelijkheid en tweedeling in de hand. Dit heeft logischerwijs uiteindelijk invloed op verloedering en zet bijvoorbeeld de sociale cohesie in de stad onder druk. Dat laatste vergroot weer het gevoel van onveiligheid. Het vergt al met al een echt integrale (of holistische) benaderingswijze en afstemming binnen de steden. We herkennen dit bijvoorbeeld in diverse beleidsplannen waarin duidelijk wordt gemaakt dat er bij gebiedsontwikkeling of vergunningsverlening ook met een veiligheidsperspectief naar de betreffende onderwerpen wordt gekeken.

Feiten én perceptie zijn belangrijk
De definitie daagt uit om niet alleen naar feiten te kijken, maar ook naar percepties. Immers, feitelijke criminaliteitscijfers kunnen dalen, maar het hoeft niet per se zo te zijn dat het gevoel van veiligheid toeneemt. Mogelijk omdat mensen de sociale cohesie voelen afnemen en via (sociale) media meer worden geconfronteerd met dreigingen. Daarnaast is het ook zo dat de laatste jaren het aantal geregistreerde misdrijfdelicten is afgenomen [17], maar er wel een verschuiving plaatsvindt naar ‘onzichtbare criminaliteit’ dan wel naar vormen met een lagere aangiftebereidheid (bijvoorbeeld *phishing* en *sextortion*), waardoor bepaalde veiligheidsissues verminderen, maar anderen weer toenemen.

Sterke nadruk ligt op weerbaarheid
In deze tijd van individualisering vindt er een verschuiving plaats in het denken over veiligheid: van de bestrijding van risico’s naar het omgaan met allerlei bedreigingen door alle actoren in de stedelijke gemeenschap. Die bedreigingen vergen een maatschappelijke én een bestuurlijke weerbaarheid. Dit kan worden bereikt door het stimuleren van zaken zoals gemeenschapszin, bewustzijn van digitale dreigingen, duurzame stedelijke planning of integriteitsbevordering bij het bestuur. We zien dit ook in de stedelijke aanpakken, waar overheden de gemeenschap (burgers en bedrijven) nadrukkelijker betrekt en aanspoort zelf problemen aan te pakken, bijvoorbeeld via buurtpreventie, Whatsapp-groepen en Meld Misdaad Anoniem. Dit bevordert ook de zelf- en samenredzaamheid.

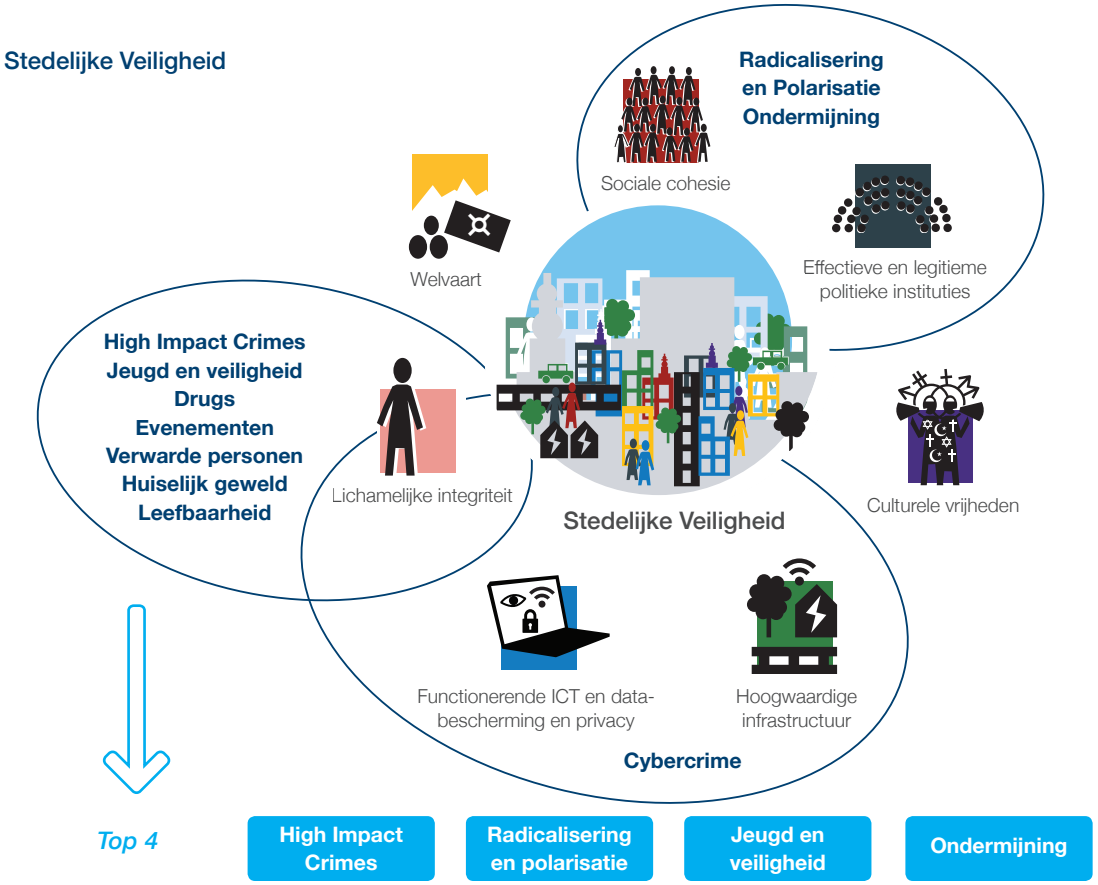
3.2 Veiligheidsbeleid van steden

Veiligheidsvraagstukken komen in steden en gemeenten expliciet tot uiting in het beleid en programma rondom Integrale Veiligheid, veelal vastgelegd in Integrale Veiligheidsplannen (IVP-en) [15]. Hoewel de hierboven genoemde dwarsverbanden tussen de kernwaarden wel steeds meer worden overgenomen is er vaak (nog) geen overkoepelende strategie gericht op alle aspecten van stedelijke veiligheid. Thema's als economische veiligheid en omgevingsveiligheid (bijvoorbeeld milieu) zijn in het algemeen geen groot onderdeel van het 'integrale' veiligheidsbeleid. Integrale veiligheid gaat vooral over 'bescherming van persoonlijk leed door intentionele en niet-intentionele dreigingen'. De focus van dat beleid is globaal gezien nog meer gericht op bescherming dan op het creëren van weerbaarheid, hoewel dit laatste onderwerp wel nadrukkelijker in beeld komt. Dit betekent niet een pleidooi voor het 'recht van de sterkste', maar een vergroting van ieders weerbaarheid tegen dreigingen.

3.2.1 Analyse huidige veiligheidsvraagstukken

De huidige veiligheidsvraagstukken zijn herleidbaar uit de gangbare beleidsinterpretatie van integrale veiligheid. Via het CCV zijn de IVP-en van de G40 beschikbaar gesteld die betrekking hebben op de periode 2019 tot 2022. In totaal zijn 14 IVP-en ontvangen (zie bijlage 1) en deze zijn geanalyseerd op de gestelde prioriteiten en bijbehorende aanpakken. In totaal zijn 49 prioriteiten in deze plannen geïdentificeerd en deze zijn vervolgens gescoord op het aantal keer dat een onderwerp in een van de onderzochte IVP-en voorkomt. Voor een goed begrip wordt hierbij opgemerkt dat in deze werkwijze dus niet besloten ligt om te komen tot de meest kansrijke Smart City toepassingen op veiligheidsvraagstukken. Uit de analyse is een top 10 samengesteld, die in volgorde van scores er als volgt uitziet: High Impact Crimes, Polarisatie & Radicalisering, Jeugd & Veiligheid, Ondermijning, Leefbaarheid, Verwarde personen, Huiselijk geweld, Cybercrime, Drugs en Evenementen.

Hoewel de onderhavige plannen niet (expliciet) de genoemde indeling naar kernwaarden hanteren zoals beschreven in paragraaf 3.1 hebben we voor de consistentie en het inzicht de top 10 prioriteiten toch 'losjes' hiernaar ingedeeld (zie figuur 3). We gebruiken hierbij het woord 'losjes' omdat er tussen de verschillende IVP-en natuurlijk definitie- en categorisatie-vraagstukken zijn te onderkennen over gelijksoortige onderwerpen.



Figuur 3 **Huidige veiligheidsprioriteiten gepositioneerd op kernwaarden stedelijke veiligheid** (gebaseerd op [16])

Zo is het onderwerp Outlaw Motorcycle Gangs in sommige IVP-en onderdeel van het vraagstuk Ondermijning, maar bij andere IVP-en een separaat onderwerp. Een ander voorbeeld betreft het nagenoeg niet benoemen als beleidsprioriteit van een onderwerp als terrorisme. Praktische beschouwd vanuit de gemeentelijke beleidspraktijk is dit onderwerp sterk verbonden met beleidsthema's als Polarisatie & Radicalisering, Verwarde personen en Rampenbestrijding en Crisisbeheersing.

In figuur 3 hebben we de top 10 prioriteiten weergegeven in relatie tot de kernwaarden. Het valt op dat, met zes van de tien geïdentificeerde prioriteiten, de meeste prioriteiten betrekking hebben op lichamelijke integriteitsvraagstukken. Daarnaast zien we dat sommige prioriteiten betrekking hebben op meerdere kernwaarden. In het bijzonder geldt dit voor cybercrime dat invloed heeft op maar liefst drie belangrijke kernwaarden (lichamelijke integriteit, infrastructuur en functionerende ICT, databescherming en privacy).

In de onderzoeksopzet hebben we in een workshop met een vertegenwoordiging van het veld gekeken naar de Smart City toepassingen van de vier meest genoemde prioriteiten in de geanalyseerde plannen. Deze vier worden hieronder nader toegelicht, de completerende 6 van de top 10 worden daarna kort geduid.

High Impact Crimes
Heeft betrekking op verschillende vormen van zichtbare criminaliteit dichtbij huis, zoals woninginbraken, straatroven en overvallen. Deze criminaliteitscijfers dalen gelukkig in veel steden, maar soms nog niet tot het gewenste niveau. Daarnaast is continue aandacht voor dit veiligheidsvraagstuk belangrijk omdat deze vormen de meeste inbreuk maken op de persoon of de persoonlijke levenssfeer en gezien de impact van directe invloed zijn op het veiligheidsgevoel van de inwoners.

Polarisatie & Radicalisering
Bij polarisatie is er in toenemende mate sprake tussen spanningen en onbegrip tussen bevolkingsgroepen onderling of jegens overheden en instituties. Voor steden staat dit hoog op de agenda omdat dit gedrag vaak een uiting is van andere diep verankerde sociale problemen (armoede, geen vooruitzichten) en zorgt voor ontwrichting in wijken en buurten. Voorbeelden zijn religieuze spanningen, maar ook onbegrip tussen bewoners in een straat of spanningen rondom gebruik van de openbare ruimte of speelplekken. Verder zijn kenmerken een toenemend wantrouwen tegenover instituties en autoriteiten, een groeiend wij-zij-denken en mentale segregatie. Zeker jongeren zijn hiervoor meer vatbaar. Polarisatie wordt gezien als het voorstadium van radicalisering (bereidheid consequenties te aanvaarden van de strijd voor een samenleving die niet strookt met onze democratische rechtsorde, naar definitie NJI), wat op haar beurt kan uitlopen naar extremisme en terrorisme (bereidheid ernstig geweld te gebruiken om daarmee de samenleving ingrijpend te veranderen of ontwrichten).

Jeugd & Veiligheid
Hoewel het met de meeste jongeren goed gaat, zijn er ook jongeren die overlast veroorzaken, risicogedrag vertonen voor criminaliteit, of al in de criminaliteit zijn beland [18]. Jeugd is enerzijds oorzaak, 'dader' van onveiligheid, anderzijds slachtoffer. Veel steden zien in hun veiligheidsanalyses een stijging van de jeugdcriminaliteit en willen dit tegengaan om de directe overlast te beperken. Daarnaast is het maatschappelijk van belang om criminele carrières in spé vroegtijdig te keren. Hoewel het vaak om criminaliteit gaat die niet uniek is voor jeugdige delinquenten (zoals geweld, diefstal of mishandeling) wordt het wel apart benoemd vanwege de verschillen in aanpak en interventiemogelijkheden.

Ondermijning
Bij ondermijning is er sprake van misbruik van maatschappelijke structuren of een aantasting van het vertrouwen in deze structuren. Bij ondermijning gebruiken of misbruiken criminelen legale middelen om op illegale wijze geld te verdienen. Het probleem is groter dan eerder aangenomen en in de praktijk weerbarstig op te lossen. Criminelen sluipen ons rechtssysteem in en kunnen hun gang gaan zonder bezorgd te zijn om gepakt te worden. De uiterst ongewenste situatie ontstaat dat normen en de grenzen tussen de boven- en onderwereld vervagen en er geen sprake meer is van een rechtsstaat en onafhankelijke rechtshandhaving. Het vergt weerbaarheid van de overheid en van de samenleving. Niet alle vormen van criminaliteit zijn per definitie ondermijning. In de praktijk blijken ondermijningsgevoelige criminele praktijken te zijn:

- Mensenhandel en –smokkel;
- Georganiseerde hennepteelt;
- Fraude en misbruik binnen de vastgoedsector;
- Witwassen en daaraan gerelateerde vormen van financieel-economische criminaliteit;
- Outlaw motorcycle gangs.

De overige zes van de tien prioriteiten worden kort in tabel 1 beschreven.

Prioriteit	Korte omschrijving
Leefbaarheid	De leefbaarheid van wijken en buurten komt onder druk door overlast, geweld, vermogenscriminaliteit en verwarde personen. De leefbaarheid van de woonomgeving werkt rechtstreeks door in de 'ervaren' veiligheid en door verschillende factoren (afnemende intramurale zorg, groeiende complexiteit in de samenleving) komt dit vaker voor dan in het verleden.
Verwarde personen	Bij personen met verward gedrag speelt vaak overlast (woon- of geluidsoverlast, alcoholmisbruik) en ook geweld (bedreiging, mishandeling). Betreffende personen/gezinnen hebben veelal problemen op meerdere leefgebieden. Veel steden en gemeenten streven naar een sluitende integrale aanpak.
Huiselijk geweld	Huiselijk geweld en kindermishandeling hebben vaak grote levenslange gevolgen zoals medische, sociale en psychische problemen. De impact op de samenleving is groot (denk aan verminderde schoolprestaties, arbeidsverzuim en maatschappelijke uitval). Daarnaast is de kans groot dat slachtoffers agressief of gewelddadig gedrag vertonen als jongere of zelfs als volwassene.
Cybercrime	Cybercrime is criminaliteit met ICT als middel én doelwit. Hierbij kunnen activiteiten gericht zijn tegen personen, eigendommen, organisaties, elektronische communicatienetwerken of informatiesystemen. De gevolgen van cybercrime zijn verstrekkend in financieel en persoonlijk opzicht. Er is een landelijke verschuiving zichtbaar van traditionele delicten naar digitale delicten. Twee doelgroepen zijn het vaakst slachtoffer: jongeren en MKB-bedrijven. Als het (lokale) infrastructuren raakt, zoals zorgvoorzieningen, beschikbaarheid van energie en water, kan het ook ontwrichtend werken voor de totale gemeenschap.
Drugs	Bij drugs moet gekeken worden naar de totale keten van gebruik en de overlast die dat met zich meebrengt, verkoop (zoals straathandel) en productie (zoals hennepkwekerijen en synthetische drugslabs, het dumpen van drugsafval). Het is feitelijk een onderwerp dat in veel veiligheidsvraagstukken terugkeert zoals bij verwarde personen, evenementenveiligheid en ondermijning (witwassen).
Evenementen	Evenementen zijn vaak belangrijke economische en sociale pijlers voor steden. De veiligheidsrisico's rondom grote evenementen hebben betrekking op fysieke en sociale veiligheidscondities zoals overlast, geweld, straatroof, alcohol en drugsmisbruik maar ook crowd management, brandveiligheid en verkeersveiligheid.

Tabel 1 **Korte omschrijving van de stedelijke veiligheidsprioriteiten 6 tot en met 10**

3.2.2 Huidige aanpak veiligheidsvraagstukken

Bij de benoemde en beschreven prioriteiten horen diverse interventies of aanpakken om deze vraagstukken te benaderen. Uit de analyse van de top 4 prioriteiten herkennen we een aantal die vaak terugkeren (in bijlage 2 zijn de specifieke aanpakken per prioriteit aangegeven):

1 Specifieke aanpakken gericht op gebieden, personen, groepen, branches of thema's. Hierbij worden bijvoorbeeld specifieke personen via een top X lijst intensief gevolgd. Bij een gebiedsgerichte aanpak worden *hotspots* of *hot times* geïdentificeerd en de specifieke acties hierop gedefinieerd. Hierbij spelen repressie en preventie (bijvoorbeeld via voorlichting) in combinatie met bijvoorbeeld gebiedsontwikkeling een grote rol. Uit de plannen blijkt ook een grote noodzaak en bereidheid tot allerlei vormen van samenwerking en informatiedeling in het eigen veiligheidsdomein (bijvoorbeeld tussen politie, gemeente, brandweer, omgevingsdienst, Douane, IND en FIOD) maar ook met bedrijven en burgers.
2 Informatie gestuurd werken. Het structureel oppikken en verzamelen van signalen vanuit diverse publieke en private bronnen, deze analyseren, duiden en opvolgen is een belangrijke interventie. Voorbeelden zijn beelden uit cameratoezicht, het digitaal opkoop register om heling tegen te gaan en *track-and-trace* technologie (van apparatuur en vervoersmiddelen). Daarnaast worden buurt apps, Whatsapp-groepen en kanalen als Meld Misdaad (Anoniem) gepromoot.
3 Beleidsintegraliteit, bijvoorbeeld door samenwerking tussen de verschillende domeinen zoals het veiligheids-, economisch en sociaal domein. Men ziet een relatie met bijvoorbeeld het bevorderen van sociale cohesie, openbare ruimte, zorg en welzijn en arbeidsparticipatie. Dat betekent overigens niet dat dan centrale regie ook is ingericht. Het is in de praktijk een samenspel binnen het college van burgemeester en wethouders.

3.2.3 Toekomstige veiligheidsvraagstukken

Het leven in de steden verandert als gevolg van diverse maatschappelijke en technologische (inter)nationale trends. Deze trends hebben vervolgens ook weer invloed op de toekomstige veiligheidsvraagstukken in de stad. We hebben de toekomstige veiligheidstrends, in de context van maatschappelijke en technologische ontwikkelingen bekeken aan de hand van diverse studies [16, 19, 20]. We bespreken ze hieronder kort.

Bedreigingen vanuit klimaatverandering

Klimaatverandering brengt een aantal effecten op gang, die o.a. hun weerslag hebben op steden. Denk aan extreme regenval en hittegolven die de lichamelijke integriteit, hoogwaardige infrastructuur en welvaart van de stad bedreigen. Zie ook de eerder aangehaalde ontwikkeling van 'ICLEI - Local Government for Sustainability' [7].

Onveiligheid door verdere verstedelijking

Door migratie naar de steden raakt de stedelijke infrastructuur overbelast. Dit kan zorgen voor toename in het aantal verkeersslachtoffers, onveiligheid in openbaar vervoer en toenemende uitstoot. Dit zorgt vervolgens voor druk op de lichamelijke integriteit en hoogwaardige infrastructuur. De toenemende uitstoot heeft negatief effect op gezonde leefomgeving en lichamelijke integriteit van inwoners. Wel zijn er vele ontwikkelingen gaande op het gebied van mobiliteit, zoals elektrische en/of zelfrijdende auto's. Dit kan de negatieve gevolgen van migratie ook weer opheffen.

Toenemende verwijdering tussen burgers en groeperingen

Veel partijen (bijvoorbeeld statelijke, etnische, religieuze en politieke groepen) hebben een groter bereik met technologische en digitale toepassingen. Het versnipperde medialandschap, aangejaagd door de digitale 'echokamer' (waarin alleen gelijksoortige informatie beschikbaar komt) van de grote sociale media toepassingen, blijken een effectieve bron voor beïnvloeding. Dit leidt tot afnemend vertrouwen in politieke instituties en wakkert segregatie en polarisering in de hand [21]. Gelijktijdig is door de technologie het mobilisatie vermogen van groepen enorm toegenomen hetgeen deze polarisatie ook fysiek maakt.

(vitale) Infrastructuur digitaal onder vuur

Onze vitale infrastructuur is in toenemende mate afhankelijk van ICT-systemen. Conflicten maar ook criminele aanvallen zullen in toenemende mate gericht zijn op onze financiële infrastructuur, logistieke knooppunten en energie- of mobiliteitsvoorzieningen. Bijvoorbeeld door de besturende systemen uit te schakelen of te verstoren of via valse sensormeldingen paniek te veroorzaken. Daarnaast is er een grotere kwetsbaarheid van onze informatie infrastructuur door toename van systemen met veel data of persoonlijke data.

Sociale ongelijkheid door digitale kloof

De voortschrijdende integratie van technologie in ieders dagelijks leven maakt dat diverse groepen (zoals ouderen) deze ontwikkelingen niet goed meer kunnen of willen volgen en de aansluiting met de samenleving missen. Naast de reeds vaak genoemde ouderen zullen ook nieuwe groepen ontstaan zoals mensen die de technologische innovaties mijden om te voorkomen dat hun data in handen van derden komt. Deze groepen zijn vervolgens minder zichtbaar in de samenleving. Het betekent dat ze minder goed betrokken worden bij de gemeenschap hetgeen ten koste gaat van de sociale cohesie. Daarnaast zijn hun activiteiten ook minder goed te volgen vanuit overheidsperspectief.

Buitenlandse veiligheid = binnenlandse veiligheid

Door de steeds sterkere verwevenheid van de interne en externe veiligheid kunnen (sektarische) spanningen in buitenland zich sneller verspreiden naar ook Nederland(se steden). Tegenstellingen tussen sociale (bevolkings)groepen lijken verder te zijn verscherpt, dan wel te zijn geaccentueerd en gaan gepaard met een verhard debat. Op den duur kan dat resulteren in nieuwe (verschijningsvormen van bestaande) veiligheidsfenomenen, zoals polarisatie, extremisme en terrorisme.

Verdacht of verongelukt door de computer

Zelf beslissende systemen nemen menselijke taken zoals het besturen van een auto over. Deze algoritmen moeten in geval van nood ook keuzen maken die betrekking hebben op lichamelijke integriteit van medeweggebruikers. Ook machines hebben ondanks de data en hun algoritmen te maken met een 'bias' bij het maken van besluiten over bijvoorbeeld verdachtmaking of in vrijheidsstelling. Hierdoor kan besluitvorming leiden tot valse positieven of valse negatieven, discriminatie of etnische profilering. Dit kan vervolgens negatief doorwerken op bijvoorbeeld de sociale cohesie en legitimiteit van de autoriteiten.

Cybercriminaliteit als nieuwe fietsendiefstal

Door de massale verzameling, verwerking en analyse van data zal de zorgvuldige bewaking van privacy of zelfs identiteit van een persoon een uitdaging zijn.

Het risico van datalekken neemt met de toename aan informatie en verbonden apparaten (in de stad) navenant toe. Ook zullen nieuwe vormen van uitbuiting ontstaan, variërend van diefstal tot manipulatie van gegevens. Cybercriminaliteit is lucratief, gezien de lage pakkans en een groot aantal mogelijke doelwitten. Gecompromitteerde beveiligingssystemen, medische monitors en zelfrijdende auto's kunnen grote risico's opleveren, in het bijzonder wanneer het ook de vitale infrastructuren raakt (water, energie, financiële processen). Steden zullen zich hiertegen moeten wapenen maar ook voorbereiden op en weerbaar zijn tegen crises.

Zorgen over "Big Brother"

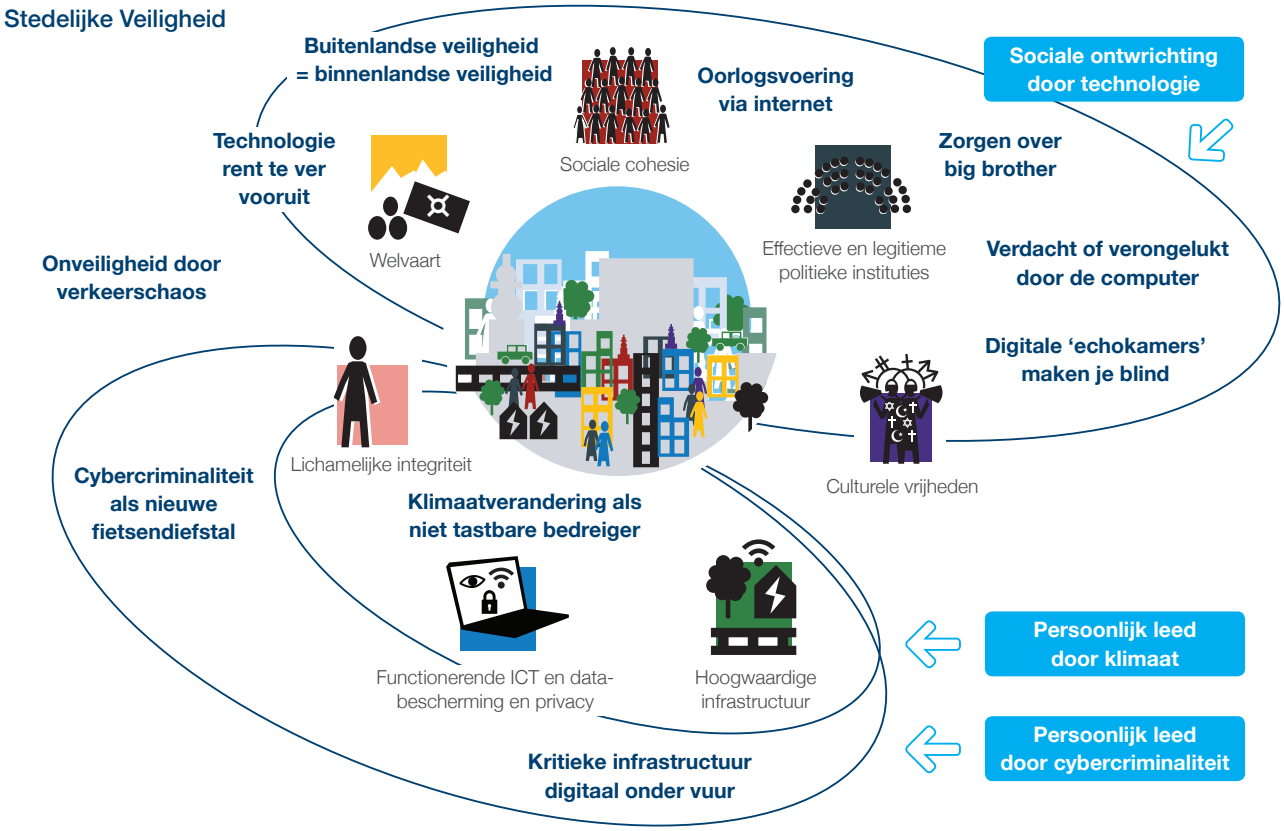
Overheden en spelers uit de particuliere sector houden en delen gevoelige persoonlijke gegevens. Dit kan het gevoel van de alwetende overheid en/of grote tech-bedrijven opleveren wat de kloof tussen burger en betrokken instantie en organisatie vergroot. Bijvoorbeeld van toezicht via organisatie met (menselijke) toezichthouders naar toezicht via digitale constellaties. Patroonherkenning in combinatie met permanente monitoring en automatische registratie door de politie, al dan niet gesponsord door bedrijven kan onveiligheid(sgevoelens) opleveren. Het is van cruciaal belang om de mate van bescherming en verstrekkings-protocollen vast te stellen.

3.2.4 Aanpak toekomstige veiligheidsvraagstukken

Als we de toekomstige veiligheidsvraagstukken bekijken dan vallen een aantal zaken op. In de eerste plaats lijken de toekomstige dreigingen meer verspreid te zijn over de verschillende kernwaarden. Daarnaast lijkt een specifieke dreiging gelijktijdig meerdere kernwaarden te raken. Zeker daar waar ICT een rol speelt. In figuur 4 zijn de toekomstige veiligheidsvraagstukken gepositioneerd naar de relevante kernwaarden van stedelijke veiligheid zoals in eerste paragraaf beschreven. In de figuur zijn de veiligheidsvraagstukken logisch geclusterd tot drie hoofdthema's:

- sociale ontwrichting door technologie;
- persoonlijk leed door klimaat;
- persoonlijk leed door cybercrime.

Kortom, toekomstige veiligheidsvraagstukken zijn meer technologie gedreven of veroorzaakt. De vraagstukken richten zich vooral op het ondermijnen van de sociale cohesie, legitimiteit van instituties en (persoonsgerichte) cybercriminaliteit. Het veiligstellen en weerbaar zijn tegen verstoringen van publieke, private en individuele ICT lijkt vooral een belangrijke veiligheidsprioriteit voor de (nabije) toekomst te moeten worden.



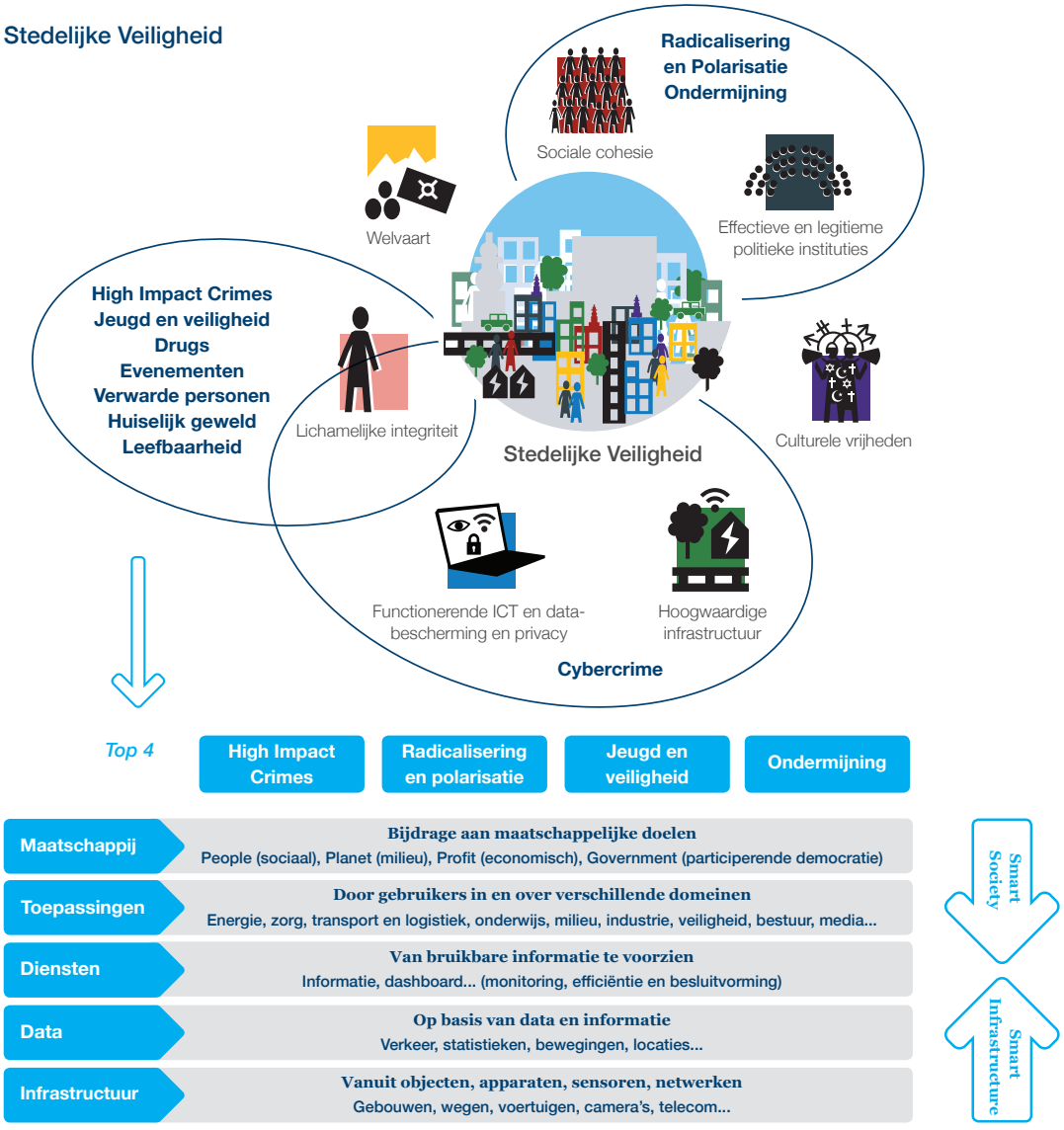
Figuur 4 **Toekomstige veiligheidsvraagstukken gepositioneerd op kernwaarden stedelijke veiligheid** (gebaseerd op [16])


187.88.25.112
4.465.6321.82
2464884123132165

4 – Smart Cities en stedelijke veiligheid

4.1 Het veiligheidspotentieel van een slimme stad

Dit hoofdstuk combineert de Smart City technologie en concepten, zoals beschreven in hoofdstuk 2, met de stedelijke veiligheidsvraagstukken, zoals weergegeven in hoofdstuk 3 (samengevoegd in figuur 5). En geeft op basis daarvan een overzicht van kansen van Smart City technologie en concepten ten behoeve van stedelijke veiligheid. Om de mogelijkheden concreet te maken, maken we gebruik van de huidige vier meest voorkomende beleidsprioriteiten met betrekking tot stedelijke veiligheidsvraagstukken uit hoofdstuk 3. Voor een indruk van hoe Smart City technologie en componenten kunnen bijdragen aan stedelijke veiligheid 'kruisen' we allereerst Smart City elementen met de kernwaarden van stedelijke veiligheid (zie tabel 2). Voor elk van de kernwaarden van stedelijke veiligheid zijn voorbeelden geschetst van infrastructuur en data, en diensten en toepassingen. Waar mogelijk is daarbij gebruik gemaakt van reeds bestaande voorbeelden.



Figuur 5 **Smart City en stedelijke veiligheid**

	Infrastructuur en data	Diensten en toepassingen
Lichamelijke integriteit	· Stedelijke sensoren · Camera's voor toezicht · Thuissensoren · Voertuigsensoren · Persoonlijke alarmknoppen en -apps · NL-Alert · Inrijbeperkende maatregelen	· Voorspellen van veiligheidsincidenten · (Real-time) misdaadkaarten · Vuurwerk of schotdetectie · Slimme surveillance · Optimalisatie van de reactietijd van noodhulpverlening · Vroegtijdige waarschuwingssystemen voor rampen · Persoonlijke alerteringssystemen · Huisbeveiligingssystemen · Crowd control · Monitoren buurt apps · Centralisatie van gemeentelijke en nooddiensten in één operationele meldkamer · Slimme verlichting
Welvaart	· Database statistische gegevens	· Inzicht in sociaaleconomische status per wijk
Sociale cohesie	· Sociale media · Buurtapps	· Stimuleren sociale (buurt)activiteiten · Sociale media analyse i.c.m. verplaatsingen of crowd vorming, extremistische uitingen
	· Internetloket · Digitale displays	· eGovernment: Dienstverlening, preventie, handhaving, intake · Burgers stimuleren bij verkiezingen · Burgerparticipatie · Data-analyse en verrijking om patronen in ondermijning te herkennen
Culturele vrijheden	· Sociale media · Media platforms	· Monitoren aantasting vrijheid van minderheden i.c.m. sociale media analyse
Hoogwaardige infrastructuur	· Slimme wegen · Slimme gebouwen · Goed toegankelijke infrastructuur	· Digitale recreatiediensten · Flexibele reisadviezen · Multimodale mobiliteitsdiensten · Data-gedreven gebouwen inspecties
Functionerende ICT, databescherming en privacy	· ICT-security · Secure Smart City architectuur	· Bewaken privacy

Tabel 2 **'Kruising' van Smart City elementen en kernwaarden van stedelijke veiligheid**

Net als in andere domeinen geldt ook voor het veiligheidsdomein dat er momenteel al verschillende Smart City concepten worden toegepast in steden. Het gaat dan om toepassingen zoals het voorspellen van veiligheidsincidenten, (Real-time) misdaadkaarten, vuurwerk of schotdetectie, slimme surveillance, optimalisatie van de reactietijd van noodhulpverlening, vroegtijdige waarschuwingssystemen van rampen, persoonlijk alerteringssystemen, huisbeveiligingssystemen en *crowd management* [2]. In het kader op bladzijde 23-25 zijn enkele voorbeeldtoepassingen opgenomen van wat er nu al op deze gebieden gebeurt.

Deze toepassingen adresseren enkele vraagstukken met betrekking tot veiligheid, maar betreffen voor een groot deel nog toepassingen specifiek in het veiligheidsdomein waarbij geen gebruik wordt gemaakt van data en/of technologie uit andere stedelijke domeinen. Ook gaan ze slechts in op een beperkt aantal componenten van stedelijke veiligheid.

De huidige toepassingen ondersteunen dus nog maar beperkt de belangrijkste stedelijke veiligheidsvraagstukken van vandaag en morgen, zoals aangegeven in tabel 3.

	Voorspellen veiligheidsincidenten	(Real-time) misdaadkaarten	Vuurwerk of schotdetectie	Slimme surveillance	Optimalisatie reactietijd noodhulpverlening	Vroegtijdige waarschuwings-systemen rampen	Persoonlijke alerteringssystemen	Huisbeveiligingssystemen	Crowd management	Inbraakvoorspeller	Tegengaan overlast gevende jongeren
High Impact Crimes	X	X						X		X	
Polarisatie & Radicalisering											
Jeugd & Veiligheid											X
Ondermijning											
Klimaatverandering als niet tastbare bedreiger						X					
Onveiligheid door verkeerschaos					X		X				
Oorlogsvoering via internet	X										
Kritieke infrastructuur digital onder vuur	X	X									
Digitale echokamers maken je blind											
Technologie rent te ver vooruit											
Buitenlandse veiligheid = binnenlandse veiligheid											
Verdacht of verongelukt door de computer	X	X									
Cybercriminaliteit als nieuwe fietsendiefstal	X	X									
Zorgen over big brother	X	X						X			

Tabel 3 **Huidige en toekomstige veiligheidsvraagstukken afgezet tegen voorbeelden van huidige toepassingen**

Voorbeelden Smart City toepassingen voor veiligheid [2]

Voorspellen van veiligheidsincidenten
Bij het voorspellen van veiligheidsincidenten, ook wel *Predicitive policing* genoemd, gaat het om gebruik van big data en analyses om te voorspellen waar en wanneer bepaalde veiligheidsincidenten plaats zouden kunnen vinden. Het helpt steden om inzet van surveillanten op locatie en tijdstip van de dag te optimaliseren, zodat ze beter in staat zijn proactief te zijn in plaats van reactief. Op verschillende plaatsen in de wereld worden misdaadvoorspellingssystemen gebruikt. Hiermee kan criminaliteit effectiever en efficiënter worden bestreden. [22]
Voorbeeld: Bij de Nederlandse Politie wordt het Criminaliteits Anticipatie Systeem (CAS) gebruikt, waarmee criminaliteitspatronen in kaart worden gebracht en voorspellingen gedaan worden op welke locaties inbraken of straatroof met welke waarschijnlijkheid zullen plaatsvinden. Naast gegevens over eerdere incidenten wordt er ook andere data verzameld op basis waarvan de voorspellingen gedaan worden, zoals de afstand tot bekende verdachten en demografische- en socio-economische gegevens van het Centraal Bureau voor de Statistiek (CBS). Het is echter nog wel beperkt tot gebruik door de politie. Er bestaan ook minder voor de hand liggende verbanden waarmee een misdaad voorspeld kan worden, zoals een positief verband tussen het aantal kliko's en het aantal woninginbraken in een wijk. Dit laatste was een resultaat van het project 'De voorspeller voor woninginbraak' van de gemeente Utrecht. De inbrekers bleken de kliko's te gebruiken om over een schutting heen te klimmen of een ruit in te gooien.

Innovatieve gebiedsbeveiliging
Door het versterken van de community van gebruikers en bewoners van een gebied in de stad, afspraken te maken over informatie-uitwisseling ten behoeve van de gemeenschappelijke veiligheid, inrichten van de gemeenschappelijke fysieke en digitale ruimte met sensoren (zoals camera's, geluidssensoren, sociale media- en netwerkmonitoring), het inrichten van een gebiedsmonitoringcentrale en benutten van elkaars interventiemogelijkheden kan veiligheid beter en efficiënter worden geregeld.
Voorbeeld: De Gemeente Den Haag heeft een Living Lab in de Internationale Zone, een uniek gebied waar meerdere internationale organisaties zich gevestigd hebben. Veiligheidsmaatregelen zijn zoveel mogelijk onzichtbaar, zodat de allure en leefbaarheid van het gebied behouden blijft. Verschillende innovaties op het gebied van Community Building, Informatie-uitwisseling, Webmonitoring, Oog en oor experiment en Gebiedsmonitoring worden hier gecombineerd.

(Real-time) misdaadkaarten
Bij misdaad monitoring (*crime mapping*) wordt technologie ingezet die door wetshandhavingsinstanties wordt gebruikt om patronen van misdaadincidenten (real-time) in kaart te brengen, te visualiseren en te analyseren. Deze informatie dient vervolgens als basis voor het effectief inzetten van mensen en middelen, het informeren van burgers en het creëren van verantwoording tussen de verschillende betrokken partijen. *Crime mapping* wordt ook gedaan door gemeenten en burgers zelf.
Voorbeeld: De politie geeft via Misdaad in Kaart overzichten van inbraken in de afgelopen periode. Gemeenten als Rotterdam, Groningen en Utrecht geven via wijkprofielen inzichten in de veiligheid in een wijk. In Groot-Brittannië is een technologie ingezet bij de politie waarbij op een kaart de laatste misdaden te zien zijn. Op die manier kan je zien waar en wat voor soort misdaad plaatsvindt.

Vuurwerk of schotdetectie
Bij *gunshot detection* wordt akoestische surveillancetechnologie met audiosensoren ingezet voor het detecteren, lokaliseren en waarschuwen van politie voor geweerschoten in real-time. Naast geweerschoten kan ook ander geluid opgevangen worden ten behoeve van het veilig houden of veiliger maken van een stad.
Voorbeeld: Een voorbeeld waarbij het opvangen van geluidssignalen ingezet wordt voor veiligheid, is rondom de jaarwisseling. In verschillende gemeenten worden geluidssensoren geplaatst, waarmee exact is na te gaan waar vuurwerk wordt afgestoken op tijden dat dit verboden is. Handhavers ontvangen vervolgens de locatie op hun smartphone en kunnen er dan opvolging aan geven. Ook voor het afsteken van illegaal vuurwerk kunnen de sensoren gebruikt worden. De sensoren kunnen het volume meten, en daarmee signaleren wanneer het vuurwerk boven het toegestane volume uitkomt. Monitoring en aanscherping van beleid rondom vuurwerk wordt daarmee makkelijker [23].

Slimme surveillance
Bij *smart surveillance* worden afwijkingen gedetecteerd door middel van intelligente monitoring op basis van beelden met daarbij onder meer gezichts- en kentekenherkenning. Via dergelijke cameranetwerken wordt verdacht gedrag gemonitord. Veel misdaden laten tegenwoordig ergens een soort digitale voetafdruk achter. Smart surveillance kan hier handig gebruik van maken.
Voorbeeld: In Amsterdam wordt op meerdere manieren gebruik gemaakt van de scanauto's van de gemeente die opzoek zijn naar illegaal geparkeerde auto's. Daarbij maken de camera's veel scans van autokentekens. Op een andere manier kan ook wat mis zijn met de auto, zoals dat de auto is gestolen, auto's die zich niet op de openbare weg zouden mogen bevinden of illegaal hergebruik van kentekens. Nu zet Amsterdam zijn scanauto's ook in om deze auto's te detecteren, door de gescande kentekens te vergelijken met databases van deze geregistreerde kentekens [24].

Optimalisatie van de reactietijd van noodhulpverlening
Bij *emergency response optimisation* worden analyse en technologie gebruikt voor het optimaliseren van de tijd tussen noodhulpvraag en noodhulpverlening. Het richt zich naast de operationele en tactische inzet van data en technologische koppelingen ook op de strategische allocatie van middelen.
Voorbeeld: Voertuigen van hulpdiensten, zoals brandweer en ambulance, kunnen gebruikmaken van verkeerslichtbeïnvloeding. Ze kunnen gebruikmaken van VETAG (Vehicle Tagging), waarbij men bijvoorbeeld een slagboom voor een bustunnel of bussluis kan openen. Op die manier wordt de aanrijtijd verkort.

Door het stationeren van brandweerwagens en ambulancevoertuigen op strategische plekken kan bij een nieuwe noodhulpvraag de afstand en daarmee de aanrijtijd ook worden verkort.

Vroegtijdige waarschuwingssystemen voor rampen
Technologie die is ontworpen om de gevolgen van natuurrampen zoals orkanen, aardbevingen, overstromingen en bosbranden te voorspellen en te verzachten.
Voorbeeld: Er bestaat bijvoorbeeld een Tsunami Warning Systeem (TWS) waarbij tsunami's worden opgespoord en kunnen waarschuwen voordat de tsunami het land bereikt, en zo levens kan sparen. Net als een Earthquake Early Warning System, welke aardbevingen detecteert. Dit waarschuwingssysteem geeft ook handelingsperspectief over hoe het beste gereageerd kan worden door burgers of hulpverleners.

Persoonlijke alerteringssystemen
Toepassingen die reageren op noodsituaties door hulpdiensten, sociale netwerken of beide te waarschuwen. Apparaten (zoals wearables voor persoonlijke veiligheid, detectoren voor auto-ongevallen en valbeveiligingssystemen) kunnen locatie- en spraakgegevens verzenden.
Voorbeeld: De website van het Rode Kruis stelt mensen in staat om na een ramp te laten weten dat ze veilig zijn. Je kunt via deze website zowel registreren als op zoek gaan naar mensen waarover je bezorgd bent [25].

Huisbeveiligingssystemen
Beveiligingssystemen die huizen controleren en gebruikers waarschuwen, hulpdiensten of beide aan ongewone activiteiten.
Voorbeeld: In een 'Home automation systems' worden slimme devices aan elkaar gekoppeld door internet. Door een interface naar een mobiele telefoon kan de huiseigenaar gewaarschuwd worden, bijvoorbeeld wanneer een koolstofdioxide sensor meet dat er teveel koolstof in de lucht is. Of een sensor die lekkage vroegtijdig kan meten.

Crowd management
Technologie om de drukte te bewaken en waar nodig mensenmassa's te bewaken om de veiligheid te waarborgen. Het gaat dan om inzicht in gedrag en groepen, het herkennen van onrust/vechtpartijen op straat door bijvoorbeeld slimme camera's (crowd dynamics).
Voorbeeld: Een uitgaansgebied in Eindhoven, 'Stratumseind' is een proefproject gestart. Daar hangen allerlei slimme camera's die bijvoorbeeld bezoekers kunnen tellen en een indicatie van de drukte kunnen geven. Andere camera's reageren op bewegingen of geluid. Er kan dan worden vastgesteld of er wordt gerend, geschreeuwd of geslagen. Er kan op tijd extra politie of meer beveiliging worden ingezet. Ook zijn er sensoren aanwezig die preventief kunnen werken, die 'rustig en kalmerend' licht uitstralen. Een opstootje kan daarmee worden voorkomen. Via gegevens van mobiele telefoons kan ook worden gekeken uit welke woonplaats bezoekers komen. Eventueel rivaliserende groepen supporters kunnen zo snel worden gedetecteerd. Gekoppeld met data uit sensoren die de bieromzet registreren, de temperatuur bijhouden of het aantal auto's in garages tellen, kan een inschatting worden gemaakt of er een verhoogde kans is op ongeregeldheden. Er zijn immers aanwijzingen over de hoeveelheid publiek en (overmatig) drankgebruik. Dergelijk gebruik van sensoren, met als doel om 'meer aan de voorkant' te komen, is vergelijkbaar met '*predictive policing*' dat hetzelfde beoogt [26].

Inbraakvoorspeller
In Utrecht wordt momenteel een oplossing ontwikkeld die voorspelt wanneer en op welke locaties er een verhoogd risico op inbraken is. Dit resulteert in een dynamische heatmap. Tevens wordt inzichtelijk gemaakt welke omgevingsfactoren van invloed zijn op dit risico. Zowel de heatmap als de situatieanalyse kunnen dienen als input voor gerichte interventieactiviteiten of nadere voorlichting. Dankzij de inbraakvoorspeller zijn er minder diefstallen en vernielingen in wijken waar speciale 'flexteams' van handhavers op af worden gestuurd.

Tegengaan overlast gevende jongeren
Utrecht wil ook overlast door hangjongeren tegengaan. Ze houdt informatie bij over het aantal jongens en meisjes dat op straat rondhangt, hun 'leeftijdsopbouw', of het bekenden van de politie zijn, de 'sfeer' en of ze wel of geen overlast veroorzaken. Utrecht combineert en analyseert gegevens uit databestanden om gericht en innovatief toezicht uit te voeren.

4.2 Specifieke kansen van Smart City voor stedelijke veiligheid

De voorbeelden in de vorige paragraaf laten zien hoe verschillende concepten momenteel worden toegepast voor stedelijke veiligheid. De toepassingen adresseren verschillende vraagstukken met betrekking tot stedelijke veiligheid, maar zijn vooral voorbeelden van de inzet van een technologie vanuit één kolom en maken nog beperkt gebruik van Smart City technologie.

Nieuwe mogelijkheden ontstaan (vooral) wanneer data en ook diensten van meerdere domeinen worden gecombineerd. Bijvoorbeeld toepassen van slimme lantaarnpalen met sensoren voor het meten van de luchtkwaliteit, met camera's voor het geleiden van voertuigen naar vrije parkeerplekken en met camera's en microfoons voor detectie van agressiviteit en criminaliteit in uitgaansgebieden. In plaats van verticale silo's per maatschappelijk doel wordt dan de meerwaarde van Smart Cities benut, zoals aangegeven bij de Smart City architectuur geïntroduceerd in hoofdstuk 2. De combinatie van sensoren en data vanuit verschillende domeinen; vanuit de mogelijkheden die de *Smart Infrastructure* biedt én vanuit de uitdagingen op het gebied van stedelijke veiligheid waar de Smart Society om vraagt. Ook bij grotere incidenten (bijvoorbeeld een terroristische aanslag) of evenementen (Olympische huldiging lokale sporter) kunnen sensoren en diensten uit meerdere domeinen hun nut bewijzen. Dat is bijvoorbeeld het geval bij crowdmanagement of (nood-)hulpverlening in situaties die vooraf niet voorzien waren en waar niet in eerste instantie rekening mee is gehouden bij het ontwerpen van de Smart Infrastructure.

Smart City technologie heeft de potentie om een belangrijke bijdrage te leveren aan stedelijke veiligheid, zowel de huidige als de toekomstige. Zoals aangegeven bij de Smart City architectuur in paragraaf 2.3 gaat het hier in eerste instantie dus om een benadering vanuit de maatschappelijke doelen, en niet vanuit de technologische mogelijkheden als primair vertrekpunt.

4.2.1 Kansen voor huidige veiligheidsvraagstukken

Om de nieuwe mogelijkheden voor vandaag en morgen concreet te maken zoomen we in op de in het vorige hoofdstuk aangegeven belangrijke huidige stedelijke veiligheidsvraagstukken: High Impact Crimes, Radicalisering en Polarisatie, Jeugd en Veiligheid en Ondermijning als voorbeeld. Deze vraagstukken zijn tijdens de workshop aan experts voorgelegd, evenals Smart City mogelijkheden. In gezamenlijkheid hebben zij toepassingen bedacht van hoe Smart City technologie zou kunnen worden ingezet voor de veiligheidsvraagstukken, en wat daarvoor nodig is. In bijlage 4 staat de vorm en inhoud van de workshop beschreven. Tabel 4 geeft voor de top vier huidige veiligheidsvraagstukken voorbeelden van de toepassingskansen van Smart City technologie en concepten. Deze worden hieronder nader toegelicht.

	Aanbrengen van infrastructuur en gebruik van data:	Voor de volgende diensten en toepassingen:
High Impact Crimes	· Sensoren/camera's · Buurtcloud (dataverzameling over, uit en van de buurt) · Buurtapps	· Detecteren van verdacht gedrag · Informeren buurtbewoners bij verdacht gedrag · Automatisch aanpassen omgevingsfactoren (licht, geluid) ter afschrikking, beveiliging of beïnvloeding gedrag
Radicalisering en Polarisatie	· Internet · Sociale media	· Herkenning van indicatoren van risicoprofielen en -patronen
Jeugd en Veiligheid	· Sensoren/camera's · Internet · Sociale media	· Vroegdetectie overlast en samenscholing · Herkenning van indicatoren van risicoprofielen en -patronen. · Serious gaming als gedragsinterventie
Ondermijning	· Buurtapps, sensoren (beeld, geluid, geur), afwijkend energieverbruik, verkeerspatronen, patronen mobiele telefonie/ dataverkeer	· Detectie indicatoren van aan ondermijning gerelateerde strafbare feiten · Sociale wijk- en buurtnetwerken om maatschappelijke weerbaarheid te verhogen · Herkenning van indicatoren van risicoprofielen en -patronen.

Tabel 4 **Huidige veiligheidsvraagstukken afgezet tegen Smart City elementen**

High Impact Crimes

Voor het vraagstuk High Impact Crimes is naast repressie en nazorg vooral preventie een belangrijk onderdeel. Relevante componenten daarbij zijn een intensieve informatiegestuurde aanpak (vraagt om historische gegevens en real time data, maar ook kwaliteitsbewaking) en samenwerking met burgers en de verschillende partijen in de veiligheidsketen. Smart City concepten kunnen een bijdrage aan preventie/detectie leveren. Bijvoorbeeld door inzet van mensen en sensoren, waaronder camera's, die verdacht gedrag signaleren en dit doorgeven aan buurtbewoners, bedrijven in de buurt en hulpdiensten. Een voorbeeld hiervan is het Fieldlab Inbraakvrije wijk van DITSS in Rotterdam Lombardijen [27], waar wordt geëxperimenteerd met sensoren voor geluid en beeld met als doel verdacht gedrag te detecteren en het gevoel van veiligheid te vergroten. Het signaleren van verdacht gedrag of incidenten kan op basis van beeld, geluid, beweging, een nood/alarmknop, domotica, etc. Afhankelijk van de dreiging kan bijvoorbeeld via een 'buurtapp' of geautomatiseerd een beslissing worden genomen over de respons: zelf in de buurt oplossen of opschalen naar inzet van politie of andere hulpverleners. De respons op de detectie van verdacht gedrag kan via een automatisch systeem, zoals het aanpassen van de verlichting, het creëren van geluid, via het sturen van gedrag of zoals genoemd via het inschakelen van hulpdiensten. Zo kan een buurtapp worden gebruik om buurtgenoten uit te nodigen de hond uit te laten, zodat inbrekers worden afgeschrikt, of om gericht resources die aanwezig zijn in de omgeving in te zetten.

Om een dergelijk Smart City concept te realiseren is het wenselijk dat er een eigenaar, beheerder, dan wel facilitator is. Dat zou een rol voor de gemeente kunnen zijn, zoals nu samen met de politie bij Burgernet. Vraag is wat die rol precies kan zijn, gezien de nu ook bestaande op dit concept lijkende Whatsapp buurtpreventiegroepen en buurtapps (zoals BuurtApp, MijnBuurtje, NextDoor Veiligebuurt) vanuit private- of commerciële initiatieven. Voor het delen van data kunnen 'dataovereenkomsten' (convenanten) worden afgesloten. Om een dergelijk concept tot succes te brengen is het nodig dat de voordelen voor alle deelnemers duidelijk zijn. Om schaalgrootte en meerwaarde voor de gebruikers te bereiken is het wenselijk dat in het concept een combinatie is op te nemen van verschillende toepassingen. Mogelijke belemmeringen liggen op het gebied van privacy en vertrouwen bij het delen van de data en ook in elkaar (burgers, bedrijven en overheid). Een *afgesproken software framework* en informatiestandaard voor het delen van data is nodig, waarbij de integriteit van de data ook is gewaarborgd. Organisatorisch is het nodig om binnen de gemeente tot een coördinatie- of regiepunt te komen.

Polarisatie & Radicalisering

Met betrekking tot Polarisatie & Radicalisering is het doel toe te werken naar een leefklimaat waarin iedereen zich verbonden voelt met de samenleving en waar geen plaats is voor onwenselijke gedrag. Het gaat om de gehele veiligheidsketen, van proactie, via preventie, preparatie en respons tot en met nazorg. Smart City concepten kunnen vooral ook bijdragen bij preventie en een bijdrage leveren aan sociale cohesie, samenwerking tussen verschillende betrokken instanties en een informatiegestuurde aanpak: informatie-uitwisseling, samenwerking; mensen en informatiesystemen.

Om ervoor te zorgen dat dit gerealiseerd kan worden moet duidelijk zijn wanneer er waar een melding gedaan kan worden. Ook moet de infrastructuur zodanig zijn ingericht dat de gewenste informatie (real-time) verstuurd kan worden. Voor het door sensoren vaststellen van atypisch gedrag zou in de toekomst AI-*machine learning* kunnen worden ingezet. Een grote rol in het kunnen toepassen hiervan is de AVG. Er wordt informatie vastgelegd en verzonden over burgers en de vraag is of dit zomaar mag en kan. Het is dan ook extra belangrijk dat er gefundeerde redenen zijn om informatie vast te leggen en/of door te spelen over iemand, gebaseerd op valide en betrouwbare profielen. Deze informatie moet vervolgens voldoende beschermd worden in een datawarehouse.

Jeugd & Veiligheid

Voor het veiligheidsvraagstuk jeugd en veiligheid is het doel risicogedrag te voorkomen en het vroegtijdig in kaart kunnen brengen van criminaliteit onder jongeren en criminele netwerkvorming. Dit om tijdig de juiste interventies te kunnen inzetten. Jeugdgroepen zijn tegenwoordig minder zichtbaar als vaste groep. Een vaste hangplek bestaat veelal niet meer; jongeren bewegen zich in los-vaste netwerken en ontmoeten elkaar op social media. De digitale wereld versterkt de onzichtbaarheid en zorgt voor allianties, stadsbreed en daarbuiten. Deze structuren lenen zich goed voor (criminele) netwerkvorming. In de samenwerking met partners worden de fluïde criminele netwerken in beeld gebracht door straat- en systeeminformatie bij elkaar te brengen in een integraal beeld voor een integrale, gebiedsgerichte, groepsgerichte en persoonsgerichte aanpak. Smart City concepten kunnen bijvoorbeeld bijdragen aan preventie en repressie.

Om dit op gang te brengen zal het veiligheidshuis 'herkaderd' moeten worden. Bijvoorbeeld door niet alleen casusgericht, maar ook ontwerpgericht te werken. Verder moet er nagedacht worden over benodigde competenties en bevoegdheden. Om dit voor elkaar te krijgen moet nagedacht worden over incentives om jongeren en bewoners te betrekken. Een mogelijke belemmering vormen de huidige 'ambtelijke structuren'.

Ondermijning
Bij ondermijning is het doel het voorkomen van aantasting van maatschappelijke structuren of een aantasting van het vertrouwen in deze structuren door vermenging boven- en onderwereld. Belangrijk hierbij is het vroeg kunnen signaleren van zwakke signalen om ondermijning tegen te gaan. Een manier om ondermijning aan te pakken met Smart City concepten is via het constateren van afwijkende patronen en/of bewegingen van personen, voertuigen, goederen, etc., gerelateerd aan ondermijning. Voor het signaleren van deze afwijkende patronen zouden buurt-apps, sensoren (beeld, geluid, geur) en analysesystemen kunnen worden ingezet, om het tijdstip, de locatie en/of de beweging te constateren. Dat kan bijvoorbeeld door samenwerking tussen verschillende partijen als gemeente, politie, waterbedrijf/waterschap, omgevingsdienst (o.a. geur), energiebedrijf (afwijkend energieverbruik), Rijkswaterstaat (verkeerspatronen) en telecommunicatie operators (patronen mobiele telefonie/dataverkeer).

Voor het realiseren van een dergelijk Smart City concept zou een wijk of bedrijventerrein als proefgebied (living lab, field lab) kunnen worden geselecteerd om de realiseerbaarheid te beproeven. Het gaat om een samenwerkingsverband *(triple- of quadruple helix)*, met als betrokken partijen: gemeente (gevoel van urgentie & capaciteit, middelen, creëren van draagvlak), bedrijven en bewoners in het gebied, eigenaren van bestaande sensoren, sensorleveranciers, wetenschap (onderzoeksopzet) en veiligheidspartners (politie, RIEC, OM). Om het concept te realiseren zijn afspraken over data-uitwisseling nodig. Een mogelijke belemmering is de verwachting dat dit arbeidsintensief is, ook aan gemeentekant. Daarnaast is het gewenst een sjabloon te hebben, zodat niet elke stad opnieuw het wiel hoeft uit te vinden, en opschaling van succesvolle innovaties zowel binnen als tussen steden.

4.2.2 Kansen voor toekomstige veiligheidsvraagstukken

Nieuwe mogelijkheden voor stedelijke veiligheid met Smart City concepten ontstaan door enerzijds gebruik te maken van bestaande infrastructuur en data en anderzijds van nieuwe Smart City Infrastructuur. Dit via samenwerking tussen verschillende partijen waaronder gemeenten, burgers, politie en andere hulpdiensten, bedrijven, leveranciers en kennisinstellingen en met inachtneming van juridische, ethische en governance randvoorwaarden (zie paragraaf 2.3).

Tabel 5 geeft voor drie toekomstige veiligheidsvraag-stukken voorbeelden van Smart City technologie en concepten. Voor een goed begrip wordt opgemerkt dat het vooral reactieve diensten en toepassingen betreft omdat er – vanwege een kennelijke verstoring van een orde – een veiligheidsvraagstuk is ontstaan. Zouden we in plaats van veiligheids- meer uit leefbaarheids-perspectief kijken, dan zien we dat diezelfde infrastructuur en data vooral faciliterende diensten en toepassingen levert.

Veiligheidsvraagstuk	Infrastructuur en data	Diensten en toepassingen
Sociale ontwrichting door techniek	· Infrastructuur waarmee iedereen bereikt wordt, breed toegankelijk	· Sociale media analyse in combinatie met patroon- en profielherkenning, resulterend in alertering van een sociaal vangnet of participatiemogelijkheden
Persoonlijk leed door klimaatverandering	· Sensoren voor water, lucht, geluids-kwaliteit, druksensoren belasting daken/wegen/riolen, warmtebelasting	· Overschrijding norm Waarschuwingssystemen en actuatoren · Maatwerkadviezen en risicomodellen huiseigenaren
Persoonlijk leed door cybercrime	· Afwijkende patronen en signaturen dataverkeer	· Analyse van sociale media, digitaal berichtenverkeer en betalingsstromen in combinatie met patroon en profiel herkenning · Waarschuwingssystemen

Tabel 5 **Toekomstige veiligheidsvraagstukken afgezet tegen Smart City elementen**

4.3 Bestuurlijke kansen voor stedelijke veiligheid

In de vorige paragraaf is ingezoomd op mogelijke waarde van smart cities voor het oplossen van vier huidige veiligheidsvraagstukken (als voorbeeld) en in het kort op kansen van smart cities voor toekomstige veiligheidsvraagstukken. Deze paragraaf zoomt verder uit naar bestuurlijke meerwaarde van het combineren van Smart City en veiligheid.

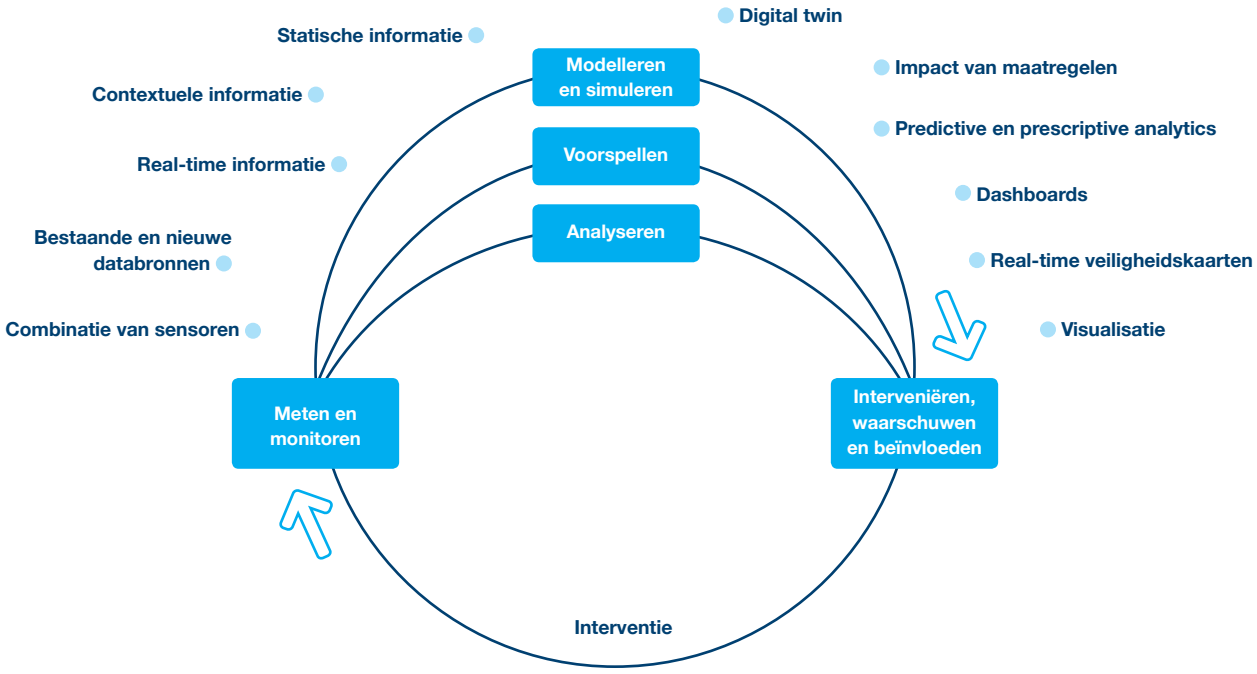
Toepassing van Smart City technologieën en concepten biedt stakeholders in stedelijke veiligheidsvraagstukken de mogelijkheid om verschillende situaties en ontwikkelingen te meten en te monitoren en op basis van een analyse daarvan, of op basis van een voorspelling of via modellering en simulatie, tijdig de juiste interventies te plegen, het effect daarvan te meten en monitoren, etc. Dit met als uiteindelijke doel de stedelijke veiligheid te vergroten. Deze Smart City lus is in figuur 6 weergegeven.

Smart City technologie en ontwikkelingen bieden daarmee op de onderstaande terreinen kansen voor verbetering van de besturing van stedelijke veiligheid, waarbij de mogelijkheden tevens aansluiten bij de huidige benaderingen voor het aanpakken van veiligheidsvraagstukken (zie ook figuur 7).

Informatie-gedreven werken en besturen[2]

De combinatie van data vanuit de infrastructuur-laag biedt de mogelijkheid tot meer en betere inzichten op basis waarvan gericht acties kunnen en beslissingen kunnen worden genomen: informatie-gedreven aanpak en beslissingsondersteuning. Dit is iets anders dan een puur data-gedreven aanpak. Naast de operationele meerwaarde vergroot dit ook de feitelijke onderbouwing en in potentie de consistentie en transparantie van beleid en besluitvorming.

2 In dit verband is de betekenis van ‘intelligence’ als ‘actionable information’ ook van toepassing.



Figuur 6 **Smart City lus**

Vergroten effectiviteit en efficiëntie van preventie, bewaken & beveiligen en handhaving
De effectiviteit en efficiëntie van de operationele veiligheidsprocessen is te verhogen door toepassing van technologie en concepten die (real-time) inzicht geven in een situatie of ontwikkeling. Dit geldt voor preventie, bewaken & beveiligen en handhaving. Hiermee kan meer veiligheid en tegen lagere kosten gerealiseerd worden.

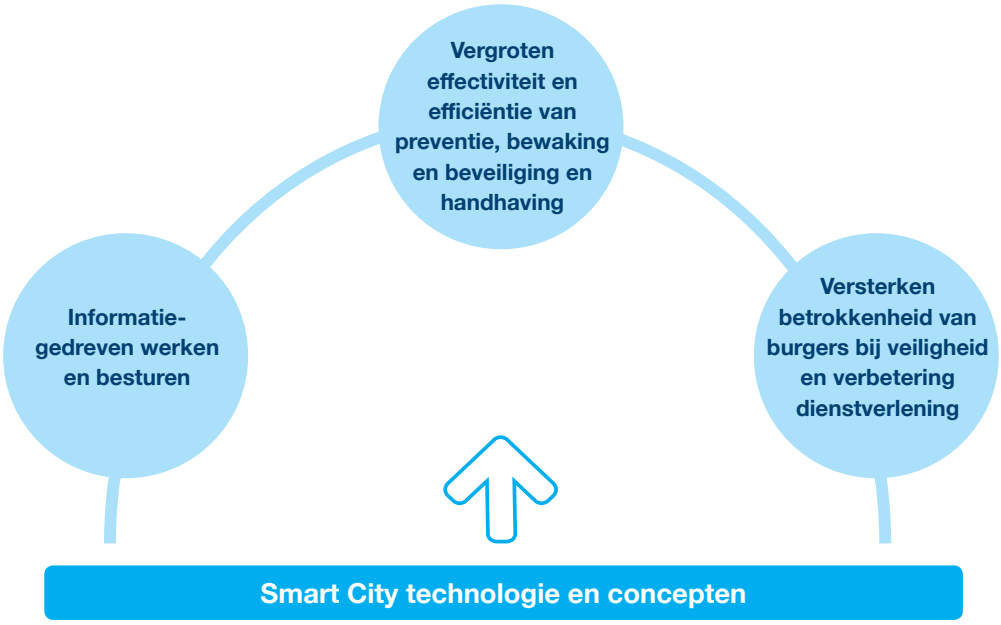
Versterken betrokkenheid van burgers bij veiligheid en verbetering dienstverlening
Samenwerking is een kernpunt bij de Smart City ontwikkeling. Daarmee bieden Smart City concepten ook de mogelijkheid tot het versterken van samenwerking tussen ketenpartners op het gebied van veiligheid én voor het versterken van de betrokkenheid van burgers en bedrijven bij stedelijke dienstverlening. Tevens biedt o.a. de informatie-uitwisseling binnen Smart City concepten de mogelijkheid de dienstverlening vanuit overheden naar burgers te verbeteren.

Naast bovenstaande zijn Smart City initiatieven ook een verandertraject binnen en tussen gemeentelijke functies. Dit kan ook gezien worden als een bestuurlijke kans, maar raakt primair de gemeentelijke organisatie en pas in tweede instantie andere organisaties en richt zich niet op het doel van stedelijke veiligheid. Daarom is het in bovenstaande opsomming niet meegenomen. Er is bij het starten van Smart City-projecten binnen gemeenten ook een risico dat bestaande organisatieonderdelen niet voldoende worden betrokken of eigenaar zijn. In plaats van een verbindend onderwerp kan dan een nieuw organisatieonderdeel ontstaan zonder verbinding die oplossingen ontwikkeld die niet geïmplementeerd worden.

4.4 Benutten van Smart City kansen voor stedelijke veiligheid

Uit de uitwerking van de specifieke voorbeelden voor High Impact Crimes, Polarisatie & Radicalisering, Jeugd & Veiligheid en Ondermijning tijdens de workshop (zie bijlage 4) zijn stappen geïdentificeerd voor het benutten van de kansen van Smart City ontwikkelingen voor stedelijk veiligheid. Bij onderstaande formulering van de aanpak om kansen te benutten voor stedelijke veiligheid hebben we tevens gekeken naar de aanpak vanuit de NL Smart City strategie [10] en naar eerdere ervaringen bij het ontwikkelen van Smart Cities [28].

Bestuurders moeten (Smart City) technologie als nieuwe pijler van stedelijke ontwikkeling omarmen
Veel steden zien de Smart City ontwikkeling nog niet als integraal onderdeel van hun stedelijke ontwikkeling. Echter deze publicatie heeft (mede) aangetoond dat (Smart City) technologie verbindt en overstijgt op de diverse domeinen van stedelijke veiligheid. Er is dus een belangrijke rol voor steden en gemeenten weggelegd om van stedelijke technologie, net als fysieke, economische en sociale componenten [29], via een gestructureerd



Figuur 7 **Bestuurlijke kansen voor stedelijke veiligheid met Smart City technologie en concepten**

strategisch proces integraal onderdeel te laten worden van stedelijke planning. Instituten en autoriteiten hebben als taak om (financiële) middelen uit publieke en/of private bronnen beschikbaar te krijgen om samen met burgers invulling te geven aan (toekomstige) behoeften. Door de inwoner centraal te stellen wordt gewerkt aan hun veiligheidsperceptie, betrokkenheid en weerbaarheid. Ethische en privacyvraagstukken worden natuurlijker en eerder besproken en kloofvorming kan worden voorkomen in de route naar een Smart Resilient City.

Bouw aan de Smart City architectuur
Een data gedreven stad vereist het opbouwen van de Smart City architectuur en competenties zoals beschreven in hoofdstuk 2. Het gaat dan om het aanleggen van infrastructurele voorzieningen zoals een internet-communicatienetwerk, de technologie om data te bewaren, beheren en beveiligen, en tools en technologie om (real-time) data-analyses uit te kunnen voeren. Veel steden stellen data openbaar beschikbaar zodat andere partijen hiermee nieuwe toepassingen kunnen ontwikkelen.

Cross-sectorale discussie over data
De kern van Smart Cities is dat data uit verschillende bronnen gebruikt worden voor analyses en besluiten op diverse vraagstukken. Het vereist een ecosysteem waarin alle sectoren met publieke en private partners regelmatig samenzitten om te bezien welke data beschikbaar is, of beschikbaar komt en in welke mate deze tot oplossingen voor vraagstukken kan dienen. Bespreek met elkaar in welke mate combinaties mogelijk zijn om infrastructurele kosten met elkaar te delen of elkaars resources te benutten. Maak daarbij duidelijke afspraken over het databeheer en toegang.

Ontwikkel met een Agile mindset en delende attitude
Een iteratieve of agile benadering waarin we stapje voor stapje vooruitkomen en vooruitgaan lijkt een betere benadering dan de meerjarige blauwdrukken vanwege de dynamische veiligheidsdreigingen en technologische vooruitgang. Gelijktijdig moeten we leerervaringen van en in steden delen en met de verschillende stakeholders in een leercyclus terecht komen waarbij we sneller en beter van elkaar leren en op elkaars innovaties doorbouwen. Bijvoorbeeld door het ontwikkelen van kaders, ‘sjablonen’ voor aanpak (observeren, proeftuin, interventies), delen van blauwdrukken die door andere gemeenten als inspiratiebron gebruikt kunnen worden. Hierbij kan een goede en belangrijke rol weggelegd zijn voor de Vereniging Nederlandse Gemeenten (VNG).

Voorkom de ‘pilot tragedie’ door vanaf het begin te focussen op opschalen
Het is de ervaring met Smart City projecten dat ze erg gericht zijn op pilots en bottom-up (kleine) initiatieven. Pilots zijn gericht op leren en experimenteren en hebben volgens deelnemers van de workshop een relatief hoog succes gehalte. Het is echter veel lastiger en veel minder voorkomend dat een succesvolle pilot ‘uitgerold’ of breed inzetbaar/beschikbaar komt voor het groter stedelijke gebied of andere steden. Zoals gememoreerd in de expertworkshop vereist het dat een pilot een bepaalde schaalgrootte moeten hebben voor politie, bedrijven en burgers om er ook toekomstig succes van te maken. Ook is het de ervaring dat de financiële of zelfs de maatschappelijke business case alleen haalbaar is wanneer technologische investeringen gedeeld worden over meerdere (veiligheids)vraagstukken. Denk bijvoorbeeld aan de business case voor Smart Public Nodes [30]. Dit impliceert dat er toekomstgericht en integraal naar vraagstukken gekeken moet worden. Niet alleen met een publieke veiligheidsbril, maar ook met een economische: welke ketenpartners, kennisinstellingen en bedrijven gaan de succesvolle pilot verder brengen en hoe ziet het inkooptraject eruit. Welke facilitator deelt de kennis en brengt de triple-helix bij elkaar, hoe kunnen inkoopmechanismen voor innovatie benut worden.

Werk samen met alle stakeholders, op alle onderwerpen en met alle bronnen
Toekomstige veiligheidsvraagstukken zijn technologie georiënteerd, grijpen op diverse veiligheidskernwaarden in en zullen meer en meer gericht zijn op verstoren van sociale cohesie en legitimiteit van instituties. Dit onderwerp aanpakken vraagt de samenwerking met veel partners binnen het gehele publieke domein, met private partners en inwoners. Om vraagstukken ook haalbaar en betaalbaar te maken moet naar kansen en mogelijkheden op diverse onderwerpen gekeken worden en is flexibiliteit om te wisselen of aan te sluiten op een bestaande ontwikkeling vereist. Het vraagt dat er gekeken wordt naar reeds bestaande databronnen, publieke en private sensoren die er al zijn en het slim (real time, op maat en veilig) delen van deze informatie.


CO-WO
SPACES

5 – Conclusies en aanbevelingen

5.1 Conclusies

Smart Cities

In een Smart City wordt de stad bestuurd op basis van data afkomstig uit sensoren en andere (open) databronnen. De stad wordt slim door informatie uit diverse bronnen te combineren voor het verkrijgen van inzichten en het nemen van beslissingen. Dit met als doel een bijdrage te leveren aan maatschappelijke doelen, waaronder die op het gebied van stedelijke veiligheid.

Naast kansen zijn er ook dreigingen en daarmee randvoorwaarden. De verwevenheid van de digitale wereld en de afhankelijkheid van infrastructuren bij Smart City concepten vragen om maatregelen ter voorkoming van verstoringen en/of ter beperking van de effecten daarvan. Betrouwbaarheid van data en vertrouwen in de partijen die data opslaan en verwerken is vereist. Transparante en ethisch verantwoorde ontwikkeling van Smart City concepten vraagt om verantwoorde waardecreatie.

Het mooie van Smart Cities is dat stedelijke opgaven cross-sectoraal kunnen worden aangepakt doordat verzamelde informatie voor meerdere domeinen meerwaarde kan hebben. Het biedt de mogelijkheid voor een stedelijke gemeenschap om zich te ontwikkelen naar een *Smart Resilient City,* een slimme stad met het vermogen te overleven, zich aan te passen en te groeien, ongeacht de soort tegenslagen. Dit vraagt van het gemeentebestuur (college, gemeenteraad en ambtelijke organisatie) daar integraal en in partnership met burgers en het bedrijfsleven richting aan te geven en een holistisch ontwikkelmodel waarin zowel maatschappelijke doelen als de daarvoor benodigde elementen vanuit de technologie samenkomen.

Stedelijke veiligheid

Bij stedelijke veiligheid gaat het om de mate (van ervaring) waarin de kernwaarden van een gemeenschap weerbaar zijn tegen dreigingen. Kernwaarden zijn: lichamelijke integriteit, welvaart, sociale cohesie, effectieve en legitieme politieke instituties, culturele vrijheden, hoogwaardige infrastructuur en databescherming en privacy [16]. De meest voorkomende actuele (2019-2022) stedelijke veiligheidsvraagstukken uit de momenteel beschikbare integrale veiligheidsplannen van gemeenten liggen op het gebied van: High Impact Crimes, Polarisatie & Radicalisering, Jeugd & Veiligheid en Ondermijning. Dit wordt meestal aangepakt door: 1. specifieke aanpakken gericht op gebieden, personen, groepen, branches of thema's; 2. informatie gestuurd werken; of 3. beleidsintegraliteit door samenwerking tussen bijvoorbeeld het veiligheids-, economisch- en sociaal domein. Deze aanpakken maken in meer of mindere mate (al) gebruik van Smart City mogelijkheden. In de toekomst kunnen de Smart City mogelijkheden nieuwe innovatieve aanpakken voor stedelijke veiligheidsvraagstukken tot stand brengen.

Toekomstige veiligheidsvraagstukken ontstaan door klimaatverandering, verdere verstedelijking, verdergaande digitalisering van kritieke infrastructuur, toenemende sociale ongelijkheid, toenemende verwevenheid tussen interne en externe veiligheid, verdergaande automatisering en cybercriminaliteit. Ook blijven in de toekomst vragen spelen rondom de digitale bescherming wat betreft het delen van gegevens. Toekomstige veiligheidsvraagstukken zijn meer technologie gedreven of veroorzaakt. Het veiligstellen en weerbaar zijn tegen verstoringen van publieke, private en individuele ICT zal een belangrijke veiligheidsprioriteit voor de (nabije) toekomst moeten worden.

Smart Cities en stedelijke veiligheid

Huidige Smart City concepten voor veiligheid zijn vaak nog toepassingen specifiek in het veiligheidsdomein waarbij geen gebruik wordt gemaakt van data en/of of technologie uit andere stedelijke domeinen. Ook gaan ze slechts in op een beperkt aantal componenten van stedelijke veiligheid. Nieuwe mogelijkheden voor stedelijke veiligheid met Smart City concepten ontstaan door enerzijds gebruik te maken van bestaande infrastructuur en data en anderzijds van nieuwe Smart City Infrastructuur. Dit via samenwerking tussen verschillende partijen waaronder gemeenten, burgers, hulpdiensten, bedrijven en kennisinstellingen en met inachtneming van juridische, ethische en governance randvoorwaarden. Daarbij is het belangrijk dat de maatschappelijke doelen het uitgangspunt zijn voor de innovaties.

Voor vier veelvoorkomende stedelijke veiligheidsvraagstukken zijn toepassingskansen van Smart City technologie en concepten beschreven. Om bestaande en nieuwe initiatieven succesvol te maken zijn proefgebieden nodig, *triple-helix* consortia, afspraken over data-uitwisseling en voldoende capaciteit ook aan gemeentezijde. Daarnaast is het gewenst een sjabloon te hebben, zodat niet elke stad opnieuw het wiel hoeft uit te vinden, en opschaling van succesvolle innovaties zowel binnen als tussen steden te organiseren. De bestuurlijke kansen die er liggen zijn op het gebied van informatiegedreven werken en besturen; vergroten effectiviteit en efficiëntie van preventie, bewaken & beveiligen en handhaving; en het versterken van burgerbetrokkenheid bij veiligheid en verbetering van dienstverlening. In de doorontwikkeling naar een *Smart Resilient City* ligt het eigenaarschap van de stad ook bij de burgers en daardoor ook het eigenaarschap of gebruiksrecht over burger- en stadsdata.

5.2 Aanbevelingen

Om de kansen van Smart City te kunnen benutten voor de huidige of toekomstige maatschappelijke doelen op het gebied van stedelijke veiligheid volgt hieronder een aantal aanbevelingen. In de kern gaat het om het *samen creëren van een win-win situatie: gemeenten, burgers, bedrijven, veiligheidsorganisaties en kennisinstellingen.* Bij de combinatie van Smart City en stedelijke veiligheid zijn allerlei partijen betrokken: gemeenten, burgers, bedrijven en veiligheidsorganisaties, met verschillende expertises en met soms verschillende belangen. Het is belangrijk om met elkaar vast te stellen hoe de partijen elkaar kunnen versterken, welke rol en belangen iedere partij heeft (o.a. wie de probleemhouder(s) is/zijn), hoe een win-win situatie gecreëerd kan worden en hoe kan worden opgeschaald.

Ontwikkel een aantrekkelijke business case voor bedrijfsleven én overheid

Nu start een initiatief vaak in een specifieke stad. Dat betekent dat die stad de projectkosten draagt, inclusief de kosten van de benodigde externe expertise en technologische oplossingen. Soms ontvangt de gemeente en/of het bedrijfsleven daar een stimuleringssubsidie voor. Na dat specifieke project trekt het bedrijfsleven weer verder en de stad sluit de projectboekhouding. Het verspreiden van oplossingen c.q. het opschalen daarvan is in Nederland vanwege de bestuurlijke versnippering en het ontbreken van centrale regie op de Smart City ontwikkelingen niet eenvoudig. Ergo, het wordt ervaren als één van de grotere problemen. Om die reden is het goed om een business case te ontwikkelen die werkt als incentive voor opschaling en op hoofdlijnen het volgende kan behelzen: Na afsluiting van het project – feitelijke een Smart City – pilot – berust maximaal eigenaarschap van alle (intellectuele) onderdelen bij de gemeente. De gemeente sluit een overeenkomst – om niet – voor het gebruik daarvan met geselecteerde leveranciers. Deze leveranciers gaan actief acquireren bij andere gemeenten. Mochten er contracten uit voortvloeien dan wordt daar een percentage 'pilotprojectkosten' in opgenomen ten behoeve van de oorspronkelijke pilotgemeente. Hierdoor verdient die gemeente de oorspronkelijke projectkosten terug.

Op deze wijze is het aantrekkelijk voor gemeenten om te investeren in deze projecten en wordt er gebruik gemaakt van de acquisitiekracht van het bedrijfsleven voor verdere opschaling. De Vereniging Nederlandse Gemeenten kan hier een belangrijke rol in spelen.

Combineer initiatieven op het gebied van stedelijke veiligheid met andere domeinen

Buiten de 'directe belanghebbenden' moeten ook de 'indirecte belanghebbenden' niet vergeten worden. Dat zijn de partijen vanuit andere domeinen dan het veiligheidsdomein die bijdragen aan andere maatschappelijke doelen. Zij kunnen mogelijk al data of diensten ter beschikking hebben of juist zelf baat hebben bij gelijksoortige data of diensten. Maar anderzijds zouden ze ook last kunnen ondervinden van de opgezette diensten en toepassingen. Daarom zullen de Smart City concepten domein overstijgend moeten worden bezien in plaats van als separate programma's per domein en is er een cross-sectorale samenwerking nodig.

Aan de ene kant kunnen andere domeinen betrokken worden door hen actief te betrekken bij ideeën die zijn ontstaan op het snijvlak van Smart City en stedelijke veiligheid. Andersom kan het ook functioneel zijn om aan te sluiten bij andere domeinen waarin al gewerkt wordt aan Smart City toepassingen die instrumenteel kunnen worden voor veiligheid. Zo kan er gebruik worden gemaakt van sensoren, netwerken en data die er al zijn of al worden ontwikkeld. Door samen te werken met andere domeinen kan er gebruik gemaakt worden van combinaties van diensten en toepassingen. Domeinen waarin huidige toepassingen het meest voorkomen zijn die binnen milieu en verkeer. Per gemeente zal dit anders zijn, en daarom is het goed binnen de eigen gemeente te achterhalen waar er al partijen bezig zijn met deze toepassingen en daar bij aan te sluiten.

Creëer ook voor stedelijke veiligheid draagvlak vanuit gemeenten en bewoners
Het hoofddoel van Smart City concepten is bij te dragen aan maatschappelijke doelen. De potentie is veelbelovend en deels al bewezen. Maar juist omdat er (cross-sectorale) samenwerking nodig is en het niet altijd even duidelijk is vanuit wie het initiatief moet komen, zullen gemeenten samen met de bewoners zelf deze samenwerkingen ook moeten stimuleren of randvoorwaardelijk maken. Dit met name voor bewustwording over kansen voor stedelijke veiligheid met gebruik van Smart City concepten. En daarnaast om veiligheid mee te nemen in alle Smart City initiatieven.

Voor het benutten van deze kansen die Smart City concepten bieden voor stedelijke veiligheid zullen bestuurders (Smart City) technologie moeten omarmen als nieuwe pijler van stedelijke ontwikkeling. Ook zal er gezamenlijk gebouwd moeten worden aan een Smart City architectuur, zodat deze in te zetten is voor toepassingen in verschillende domeinen. Cross-sectorale discussies zullen gevoerd moeten worden over samenwerking en over het gebruik en het nut van data voor de verschillende vraagstukken.

Werk Agile: experimenteren en leren
Een Agile manier van werken en een 'delende attitude' zijn passend bij het bedenken en verbeteren van Smart City concepten; ook voor stedelijke veiligheid. Dit houdt in dat het ontwerp van toepassingen zodanig is opgezet dat er makkelijk veranderingen kunnen worden aangebracht, dingen aan kunnen worden toegevoegd of opgeschaald kan worden. In het kader van domein overstijgend samenwerken is dit zeer nuttig. De uitdagingen in de stad zijn aan veranderingen en onzekerheden onderhevig, daarom kan deze manier van werken goed helpen omdat het iteratief, incrementeel en adaptief is.

Samenwerken is *key*. Het betrekken van alle stakeholders op alle rakende onderwerpen en alle bruikbare bronnen. Die integraliteit bestaat er ook uit dat je publiek-privaat innoveert. Waarbij de overheid/gemeenten de vraagkant vertegenwoordigen die, bijvoorbeeld ondersteund door een triple-helix facilitator (zoals HSD en DITTS), met bedrijven en kennisinstellingen tot vraagarticulatie, consortia of aanbesteding komen. Dat kan door middel van gerichte kennissessies, matchmaking en marktconsultaties. Door het inzetten van innovatieve inkoopmechanismen, zoals bijvoorbeeld het innovatiepartnerschap, kunnen opschaalbare oplossingen worden ontwikkeld.

Zorg voor open interfaces en mechanismen voor gezamenlijke analyse
Binnen Smart Cities wordt 'informatiegericht' gewerkt. Allerlei data wordt gebruikt om uiteindelijk positief bij te dragen aan maatschappelijke doelen. Omdat dezelfde data en/of diensten voor meerdere doelen en voor meerdere domeinen (in de toekomst) relevant kunnen zijn, is het wenselijk deze informatie te kunnen delen. Dit is wettelijk gezien niet altijd zonder meer mogelijk. De techniek opzetten met open interfaces en mechanismen voor het gezamenlijk analyseren van data zonder deze inhoudelijk te delen (zoals *secure multi-party computation*) dragen bij aan een werkbare oplossing.

Zorg voor borging van beveiliging, privacy en ethisch verantwoord handelen
Te allen tijde moet rekening gehouden worden met de randvoorwaarden rond privacy, dataopslag, -toegang en -verwerking. Privacy waarborging, goed belegd eigenaarschap van data, het kunnen afleggen van politiek-bestuurlijke verantwoording en intervisie op ethisch verantwoord handelen zijn belangrijk bij de samenwerking en het delen van informatie: ga uit van *Responsible Design*. Net als in de fysieke wereld zullen er ook in de digitale wereld democratische wetten en regels opgesteld worden, zodat er geen sprake zal zijn van discriminatie, uitsluiting, onrechtmatig data-gebruik of onwaarheden. Zo zal de digitale stad zijn menselijke kant behouden.

Organiseer een structuur om te experimenteren, leren en delen.
Al zal het accent op de veiligheidsvraagstukken binnen verschillende gemeenten net wat anders liggen, het zal nuttig zijn te kijken en te leren van andere gemeenten. Smart City concepten zijn redelijk nieuw en vaak nog in een experimenteerfase. Soms is er ook sprake van mislukking [31]. Het is goed om daarom als gemeenten en leveranciers apart én met elkaar leren: wat werkte wel, wat niet? Bij de gemeenten is het daarbij belangrijk om leerkringen te hebben voor bestuurders (college) én voor de ambtelijke organisatie. Wat zou beter kunnen, wat zijn de randvoorwaarden voor succes? Er zou dus specifiek voor wat betreft Smart City toepassingen voor veiligheid leerkringen opgezet kunnen worden vanuit een landelijke organisatie. Voorbeeld hiervan is hoe er tussen de vijf grote gemeenten (G5) al kennis wordt gedeeld op dit thema. Een dergelijke leerkring kan 'lessons learned' of dynamische blauwdrukken voor andere gemeenten opleveren en een advies- en coachingsrol naar bestuurders. Voor verschillende partijen die landelijk

opereren, zoals bedrijven en de politie, is zicht op schaal van toepassingen voor stedelijke veiligheid nodig. Het door gemeenten toepassen van eenzelfde sjabloon, dat ruimte biedt aan individuele verschillen, kan hieraan bijdragen.

Leer pilot-overstijgend
Er zijn al verschillende ervaringen opgedaan met Smart City projecten. Er wordt maar beperkt gebruik gemaakt van elkaars ervaringen, instrumenten en innovaties. Daardoor ontstaan een heleboel maatwerkoplossingen en die kunnen effectief zijn. Maar schaalvoordelen zoals continue verbetering, onderhoud en kostenefficiëntie worden niet behaald. Een risico is dat er sommige aspecten niet voldoende aandacht krijgen die latere toepassing of opschaling in de weg gaan zitten. Door binnen pilotprojecten het gebruik en het delen van elkaars ervaringen, instrumenten en innovaties als randvoorwaarde mee te geven worden meer pilots duurzaam succesvol. Als hulpmiddel daarbij kan een checklist voor succesvolle implementatie van Smart City concepten voor stedelijke veiligheid worden gehanteerd. Bijlage 3 geeft een aanzet voor een dergelijke checklist, de verdere ontwikkeling en borging is aan de gebruikers en coördinerende/faciliterende instituties.

5.3 Hoe verder

Handvatten voor ontwikkeling van Smart City concepten
Bovenstaande aanbevelingen geven handvatten voor de ontwikkeling van Smart City concepten voor stedelijke veiligheid. Maak daarvan gebruik bij het ontwikkelen van nieuwe concepten vanuit een gezamenlijke behoefte op lokale, regionale of landelijke schaal dan wel gestimuleerd vanuit een nationale regierol. Maak gebruik van synergie tussen verschillende domeinen.

Smart Flying Squad
Bij de workshop bleek dat er een groot enthousiasme is om in gezamenlijkheid met verschillende partijen (gemeenten, veiligheidsorganisaties, burgers, bedrijven en kennisinstellingen) na te denken over mogelijkheden van Smart City toepassingen voor stedelijke veiligheid, en ook dat er behoefte is aan meer van dat soort bijeenkomsten. Het is bleek nuttig om vanuit beide kanten na te denken: vanuit zowel de stedelijke veiligheidsvraagstukken, als ook vanuit de mogelijke Smart City toepassingen. Juist door samen te komen kunnen er makkelijker ideeën ontstaan waar elke partij baat bij heeft. Het samenkomen en enthousiasme delen werkt als een accelerator. De aanbeveling is dus om op gelijksoortige manier samen te komen en een '*Smart Flying Squad*' te vormen, waarin gemeenten, bedrijven, politie/hulpdiensten en kennisinstellingen samenkomen en in een soort *pressure cooker challenge* huidige stedelijke maatschappelijke vraagstukken met Smart City concepten conceptueel oplossen als start van een project of programma.

De in dit rapport beschreven toepassingskansen van Smart City technologie voor vier veelvoorkomende stedelijke veiligheidsvraagstukken zijn daarbij een goed startpunt. Het kan ook in lopende projecten om nieuwe kansen te ontwikkelen of knelpunten op te lossen of voor omgevingen als mainports (luchthavens, zeehavens) waar economische, milieu en veiligheidsbelangen bij elkaar komen.

Op deze manier is het mogelijk massa en beweging te creëren via een gezamenlijk lerend systeem voor de ontwikkeling van Smart City concepten voor stedelijke veiligheid via incrementele innovatie: slim delen en samen leren.

Literatuurlijst

[1] Europees innovatiepartnerschap voor slimme steden en gemeenten - strategisch implementatieplan; 2014; Europese Commissie. Geraadpleegd van http://ec.europa.eu/eip/smartcities/files/sip_final_en.pdf; bekeken op 19 februari 2019.

[2] Smart Cities: Digital solutions for a more liveable future; juni 2018; McKinsey Global Institute.

[3] The EU Resilience Prospectus; 2017; 100 Resilient Cities.

[4] 12 Examples of Climate Resilient Solutions; Geraadpleegd van https://stateofgreen.com/en/partners/state-of-green/news/12-examples-of-climate-resilient-city-solutions/; bekeken op 2 maart 2019.

[5] Smart City, Safety and Security; 2017; Maroš Lacinák, Jozef Ristvej.

[6] Chicago launches Smart911 to improve emergency response. Geraadpleegd van https://www.smartcitiesdive.com/news/chicago-launches-smart911-to-improve-emergency-response/533446/; bekeken op 22 maart 2019.

[7] The Sustainable City; 2017; Steven Cohen.

[8] Greenest City: 2020 action plan; 2018; City of Vancouver. Opgehaald van https://vancouver.ca/files/cov/greenest-city-action-plan-implementation-update-2017-2018.pdf; bekeken op 22 maart 2019.

[9] Sleepy in Songdo, Korea's Smartest City; 22 juni 2018; Linda Poon. Geraadpleegd van https://www.citylab.com/life/2018/06/sleepy-in-songdo-koreas-smartest-city/561374/.

[10] NL Smart City Strategie; The future of living; 2017; Jack Mikkers.

[11] Helmond is nu 'twee slimme kruispunten' rijker; 12 september 2018; Guus Puylaert. Geraadpleegd van https://www.verkeerinbeeld.nl/nieuws/120918/helmond-is-nu-twee-slimme-kruispunten-rijker.

[12] GSMA Smart Cities Guide: Crowd Management; 15 augustus 2016; GSM Association.

[13] CITYkeys Deliverable D1.2, Overview of the Current State of the Art; 2015; CITYkeys.

[14] VWData: Verantwoorde Datacreatie met Big Data; 7 juli 2017; R.L. Lagendijk. Opgehaald van https://wetenschapsagenda.nl/programma/startimpulsprogramma-verantwoorde-waardecreatie-met-big-data-vwdata/.

[15] Kernbeleid Veiligheid 2017: Handreiking voor gemeenten; augustus 2017; VNG.

[16] 'Naar een Visie op Amsterdamse Stedelijke Veiligheid'; The Hague Centre for Strategic Studies; 2015; Tim Sweijs, Pim ten Haaf, Stephan de Spiegeleire, Maarten Gehem, Matthijs Maas, Paul Sinning.

[17] Veiligheidsmonitor CBS 2019; CBS. Opgehaald van http://www.veiligheidsmonitor.nl/Publicaties/Rapportages; bekeken op 22 maart 2019.

[18] Jaarrapport 2018 Landelijke Jeugdmonitor CBS; CBS. Opgehaald van https://www.cbs.nl/nl-nl/publicatie/2018/48/jaarrapport-2018-landelijke-jeugdmonitor.

[19] Grote bewegingen, Grote impact; The Hague Centre for Strategic Studies; 2017; Reinier Bergema, Erik Frinking, Karlijn Jans, Paul Sinning, Tim Sweijs, Alice van de Bovenkamp.

[20] Veiligheid in de toekomst; Stichting Toekomstbeeld der techniek; 2018; Carlijn Nabel.

[21] Hoe YouTube rechtse radicalisering in de hand werkt; Volkskrant; 9 februari 2019; Hassan Bahara, Annieke Kranenberg, Dimitri Tokmetzis. Opgehaald van https://www.volkskrant.nl/kijkverder/t/2019/radicalisering-youtube/.

[22] Predictive policing: lessen voor de toekomst; februari 2017; Bas Mali, Carla Bronkhorst-Giesen, Mariëlle den Hengst.

[23] Vuurwerkhandhavers krijgen hulp van sensoren en app; beveiligingsnieuws.nl; 30 december 2018; opgehaald van https://beveiligingnieuws.nl/nieuws/vuurwerkhandhavers-krijgen-hulp-van-sensoren-en-app.

[24] Scanauto's helpen voortaan ook bij opsporen gestolen voertuigen; 28 december 2016; Marc Kruyswijk; https://www.parool.nl/amsterdam/scanauto-s-helpen-voortaan-ook-bij-opsporen-gestolen-voertuigen~a4440732/.

[25] Ik ben veilig; Rode Kruis; opgehaald van https://www.ikbenveilig.nl/ikbenveilig; bekeken op 22 maart 2019.

[26] Sensing door de politie en publiek-private samenwerking: operationele noodzaak; Tijdschrift voor de Politie; 2016; Bart Engberts, Frans Copini.

[27] DITSS Programma Inbraakvrije Wijk; 2018; opgehaald van www.inbraakvrijewijk.nl, bekeken op 22 maart 2019.

[28] Characteristics of Smart Sustainable City Development: Implications for Project Management. Smart Cities, 1(1), 75-97.; 2018; Schipper, R., & Silvius, A.

[29] Opgehaald van https://decentrale.regelgeving.overheid.nl/cvdr/images/Groningen%20(Gr)/i36179.pdf; bekeken op 19 februari 2019.

[30] Smart Public Nodes: De smart city business case bewezen; 2017; Herman Pals.

[31] Assen in wurggreep van Sensor City; 30 december 2016; Dagblad van het Noorden. Opgehaald van https://www.dvhn.nl/drenthe/Assen-in-wurggreep-van-Sensor-City-21886666.html?harvest_referrer=https%3A%2F%2Fwww.google.com%2F.

Bijlagen

Bijlage 1 – Overzicht van geanalyseerde integrale veiligheidsplannen

Steden en Gemeenten zijn verplicht om minimaal één keer per vier jaar een Integraal VeiligheidsPlan (IVP) op te stellen. Deze vier jaarlijkse periode liep eind 2018 af. Daarom zijn in de periode tussen 18 december 2018 en medio januari 2019 via het CCV de nieuwe, geaccordeerde IVP-en van de G40 opgevraagd die betrekking hebben op de periode 2019 tot 2022. De IVP-documenten van de G4 waren helaas nog niet beschikbaar en zijn daarom ook niet betrokken in de analyse.

Stad	Integraal VeiligheidsPlan
Almere	Actieplan veiligheid 2019-2022. Afdeling Bestuur, Veiligheid, Leefbaarheid en Strategie, 17-12-2018
Alphen aan de Rhijn	Integraal veiligheidsbeleid 2019-2022
Assen	Integraal Veiligheidsbeleid, Gemeente Assen 2016-2020 Veiligheidsprogramma Gemeente Assen 2019
Breda	Plan van Aanpak Meerjarenprogramma Veiligheid, “Veiligheid breng(t) je samen. Analyseren, Anticiperen en Activeren.”
Den Bosch	Integraal Veiligheidsplan 2019-2022, Gemeente ‘s-Hertogenbosch ‘De basis verstevigd, inwoners en ondernemers in positie’
Enschede	Integraal veiligheidsbeleid Gemeente Enschede 2017-2020. Veiligheid is een verantwoordelijkheid van ons allemaal
Gouda	Concept Kadernota Integraal Veiligheidsbeleid 2019-2022, Gemeente Gouda, Versie ter bespreking in de GASD, 11 december 2018
Haarlem	IVH 2019-2022, Integraal Veiligheids- en Handhavingsbeleid, 01.01.2019, Veiligheid & Handhaving, VEILIGHEIDSANALYSE 2018
Haarlemmermeer	Raadsvoorstel 2018.0042518, Kadernota Integrale Veiligheid 2018-2022. Kadernota Integrale Veiligheid 2018-2022 Haarlemmermeer, Haarlemmerliede en Spaarnwoude. Versie: 4 juli 2018
Leeuwarden	Veiligheidsagenda 2019 – 2023 en geïntegreerd uitvoeringsprogramma 2019 - 2020
Tilburg	Tilburg… je bent er veilig, integraal Veiligheidsplan Tilburg, Periode 2019 t/m 2022, november 2018
Zaanstad	Integraal veiligheidsplan 2019 – 2022, Zaanstad, Oostzaan en Wormerland Openbare orde en veiligheid, 07 november 2018
Zandvoort	Integraal Veiligheids- en Handhavingsplan 2019-2022, Veiligheid & Handhaving, Gemeente Zandvoort, Registratienummer: 2018 789780, Vastgesteld in college dd. 20-11-2018
Zoetermeer	Kadernota Integraal Veiligheidsbeleid Zoetermeer 2019-2022, geactualiseerd

De IVP-en zijn geanalyseerd op de gestelde prioriteiten en bijbehorende aanpakken. Voor de leesbaarheid en overzichtelijkheid zijn in de diverse IVP-en clusters van prioriteiten aangebracht. Hierbij hanteren steden en gemeenten uiteraard een eigen en daardoor verschillende categorisatie. Daarom zijn de prioriteiten op een zo laag mogelijk niveau geïdentificeerd. In totaal zijn 49 prioriteiten in deze IVP-en geïdentificeerd en deze zijn vervolgens gescoord op het aantal keer dat een onderwerp in een van de onderzochte IVP-en voorkomt. Hieruit is een top 10 samengesteld, die in volgorde van scores er als volgt uitziet: High Impact Crimes, Polarisatie & Radicalisering, Jeugd & Veiligheid, Ondermijning, Leefbaarheid, Verwarde personen, Huiselijk geweld, Cybercrime, Drugs en Evenementen.

Codering	Aantal voorkomen
High Impact Crimes	11
Radicalisering en polarisatie	11
Jeugd en Veiligheid	10
Ondermijning	10
Leefbaarheid	8
Verwarde personen	8
Huiselijk geweld	6
Cybercrime	4
Drugs	4
Evenementen	4
Zorg en Veiligheid	4
Regionale prioriteiten	3
Woonoverlast	3
Bestuurlijke ondermijning	2
Brandveiligheid	2
Criminaliteit	2
Criminele samenwerkingsverbanden	2
Kwetsbaren minder zelfredzaam	2
Outlaw Motorcycle Gangs	2
Veilig ondernemen	2
Veilige publieke taak	2
Verkeersveiligheid	2
Woon- en adresfraude	2
Zorgfraude	2
Cameratoezicht	1

Codering	Aantal voorkomen
Crisisbeheersing	1
Crisisorganisatie	1
Ex-gedetineerden	1
Horeca & Coffeeshops	1
Informatieveiligheid	1
Kamerverhuur	1
Knooppunten	1
Loverboyproblematiek	1
Nachtopvang	1
Overlast	1
Personen licht verstandelijke beperking	1
Prostitutie & Mensenhandel	1
Straatoverlast	1
Veelplegers	1
Veilig uitgaan	1
Veilig werken	1
Veilig winkelen	1
Veilige scholen	1
Veranderende samenleving	1
Vermogenscriminaliteit	1
Verouderde bedrijventerreinen	1
Vluchtelingen	1
Zedendelinquenten	1
Zwerfafval	1

Bijlage 2 – **Specifieke aanpakken per prioriteit**

Onderstaande tabel geeft de specifieke aanpakken uit de integrale veiligheidsplannen voor de veiligheidsvraagstukken: High Impact Crimes, Polarisatie & Radicalisering, Jeugd & veiligheid en Ondermijning.

	High Impact Crimes	Polarisatie & Radicalisering	Jeugd & Veiligheid	Ondermijning
Integrale aanpak			· Flankerende maatregelen op het vlak van onder meer vrijetijdsbesteding, openbare ruimte, onderwijs en werk en jongerenvoorzieningen · Een brede aanpak op het gebied van jeugd, zorg en onderwijs	· Op plekken en in branches waar risico's samenkomen een integrale handhaving met publieke en private partners op lokaal, regionaal en landelijk niveau.
Gebiedsgerichte aanpak	· Extra toezicht hotspots en hottimes · Hotspots aanpak van kwetsbare punten zoals snoeien en verlichting. · Veilig ontwerp' bij (her)inrichting en gebiedsontwikkeling · In wijken waar verschillende bedreigingen bij elkaar komen een integrale, gebiedsgerichte aanpak. Veiligheid is daarbij één van de componenten, naast onder meer zorg en welzijn, openbare ruimte, inrichting/infrastructuur en economie.		· Concentreert zich op de hotspots in wijken van de stad waar sprake is van overlast. · Veiligheid in en om scholen en op sportparken	· In specifieke wijken werken gemeente, politie en woning-corporatie samen aan verbeteringen op het gebied van wonen, fysiek, sociaal, veiligheid en leefbaarheid. Beide gebieden vragen een gebiedsgerichte aanpak
Persoonsgerichte aanpak	· De top X-aanpak richt zich daarbij zowel op de dader als zijn of haar omgeving	· Persoonsgerichte aanpak voor personen die (dreigen te) radicaliseren · Casus tafel	· Personen in de stad die herhaaldelijk voor zware overlast en criminaliteit zorgen worden opgenomen in de persoonsgerichte aanpak · Top X-aanpak van het Veiligheidshuis	

	High Impact Crimes	Polarisatie & Radicalisering	Jeugd & Veiligheid	Ondermijning
Groepsgerichte aanpak			· Bij problematisch groepsgedrag van een (jeugd)groep, wordt deze groep bij het jeugdinterventieteam (JIT) ter bespreking ingebracht	
Branche gerichte aanpak				· Ja, zoals bijvoorbeeld horeca, evenementen, vastgoed en prostitutie
Thema gerichte aanpak				· Het vergroten van de bestuurlijke, maatschappelijke en/of sociale weerbaarheid · Signalen van ondermijning worden door interne en externe partners gemeld bij het meldpunt ondermijning · Topics zijn drugs, OMG, mensenhandel, prostitutie, woon- en adresfraude (i.v.m. voedingsbodem voor ondermijning).
Repressie en preventie	· Heterdaadkracht		· Inzet op preventie op het voorkomen van nieuwe aanwas van jongeren die overlast veroorzaken en/of in het criminele circuit terechtkomen. · Alcohol- en drugsgebruik onder 18-minners	· Door middel van het opwerken van ondermijningssignalen en analyses kan besloten worden tot een bestuurlijke, strafrechtelijk, civiele aanpak of combinatie daarvan.
Samenwerking en informatie deling	· Burgerparticipatie: hang- en sluitwerk en verlichting, algemene alertheid, sneller melden, weerbaarheid, eigendom registratie · Samenwerking met partijen in keten: politie, KMar en OM. · Het ondersteunen en faciliteren van de buurtpreventieteams	· Samenwerking met instellingen en maatschappelijke partners · Parate en bekwame hulpverlening- en crisisorganisatie	· Integraal dus een continue integrale samenwerking nodig, zowel intern (met o.a. het zorg- en sociale domein) als extern (met ketenpartners als politie, OM en sociale teams). · Inwoners en ondernemers denken en doe mee en worden partner in oplossingsgerichte acties.	· Vindt binnen de gemeente plaats met lokale partners. Bij opschaling en betrokkenheid van landelijke (opsporings- of toezichts-)partners via het RIEC-LIEC stelsel.

	High Impact Crimes	Polarisatie & Radicalisering	Jeugd & Veiligheid	Ondermijning
Informatie-gestuurd werken	· Inzichten in welke aspecten een onveilig en veilig gevoel creëren bij inwoners	· Opbouwen signaleringsnetwerk inclusief meldingen van inwoners en ondernemers. Duiding door professionals · Niet alleen de politie, maar ook de gemeente kan informatie uit de samenleving kan halen. · Onderzoek naar de aard en omvang van onwenselijke polarisatie	· Verkrijgen van een integraal beeld van de (jeugd)groep o.a via de 'groepsscan' · Aanwezig in de wijken en buurten, volgen en 'kennen' jeugdgroepen, in het bijzonder de meer problematische groepen · Vroegsignalering via het veld en via burgers	· Investeren in analysemogelijkheden en het slim combineren van databronnen de aanpak van ondermijning naar de voorkant verplaatsen. · Via toezicht en handhaving signaleren, interveniëren én voorkomen. Snel en efficiënt handelen. · Risico gestuurd werken (branches en beroepsgroepen, logistiek en locaties, bedrijfsmatige activiteiten, kwetsbare groepen inwoners) · Informatieknooppunt ontwikkelen om tactisch-operationeel en strategisch de juiste beslissingen te nemen. · Uitwisseling en analyse van data onmisbaar.
Voorlichting	· Voorlichtingscampagnes, inbraakpreventie adviseurs	· Trainingen voor professionals · Voorlichting aan en bewustwording van haar inwoners		· Preventief communiceren
Technologie	· Cameratoezicht tegen bijv. straatroven/geweld in de binnenstad · Digitaal Opkopersregister (DOR), het Digitaal Opkopersloket (DOL) en 'track and trace'-methodes · Het veiligheids-informatiesysteem (VIS) Buurtinformatienetwerk (BIN), buurtapps, (WhatsApp-groepen), burgernet, Meld Misdaad Anoniem			

Bijlage 3 – Checklist ten behoeve van succesvolle implementatie

Om ervoor te zorgen dat Smart City concepten succesvol geïmplementeerd worden hebben we aan de hand van deze studie een eerste versie van een checklist opgesteld. Deze checklist kan gebruikt worden wanneer één of meerdere partijen bij elkaar zijn voor het opzetten van Smart City concepten ten behoeve van stedelijke veiligheid. Het zijn aandachtspunten waar over nagedacht moet worden.

Doelstelling

- Wat is de maatschappelijke uitdaging?
- Wat is gewenst te bereiken vanuit de uitdagingen op het gebied van het geïdentificeerde veiligheidsprobleem?
- Welke doelen, rollen en belangen hebben verschillende partijen hierbij? En zijn deze in balans te brengen, zodat er meerwaarde voor elke partij is?

Conceptontwikkeling

- Wat zijn vanuit de uitdagingen de mogelijkheden van Smart City technologie?
- Hoe kan gebruik gemaakt worden van (bestaande) Smart City technologie en concepten; ook uit andere domeinen?
- Welke rol heeft elk van de betrokken partijen bij de realisatie van het concept?
- Hoe kan het concept worden getest?

Samenwerking

- Zijn afspraken over de samenwerking tussen, gemeenten, bedrijven, veiligheidsorganisaties en kennisinstellingen duidelijk gemaakt?
- Hoe kunnen ketenpartners, burgers en bedrijven betrokken worden bij veiligheid en verbeterde dienstverlening?

Kwetsbaarheden

- Hoe wordt cybersecurity gewaarborgd?
- Hoe zit het met de kwetsbaarheid van infrastructuur?
- In hoeverre hebben private platformbedrijven invloed op de (toekomstige) veiligheid in de stad en valt dit te reguleren?
- Wie is in welke gevallen aansprakelijk waarvoor? Hoe kan deze aansprakelijkheid worden gewaarborgd?

Randvoorwaarden

- Zijn de randvoorwaarden voor gezamenlijke ontwikkeling geborgd?
  - Bestuurders moeten (Smart City) technologie als nieuwe pijler van stedelijke ontwikkeling omarmen;
  - Bouw aan de Smart City architectuur;
  - Ontwikkel met een Agile *mindset* en delende attitude;
  - Voorkom de ‘pilot tragedie’ door vanaf het begin te focussen op opschalen;
  - Werk samen met alle stakeholders, op alle onderwerpen en met alle bronnen.
- Zijn de randvoorwaarden voor beveiliging, privacy en ethisch verantwoord handelen geborgd?
  - Ga uit van *Responsible Design*.

Data

- Welke informatie is aanwezig in de infrastructuur laag, op basis waarvan (door combineren) beslissingen en acties genomen kunnen worden?
- Wie is de eigenaar van benodigde data en/of bij wie zou je dat moeten willen beleggen? Zijn alle betrokkenen het daar mee eens? (Cross-sectoraal)
- Hoe wordt gezorgd voor de betrouwbaarheid van data?
- Zijn er afspraken gemaakt over de uitwisseling en het gebruik van data?
- Hoe lang en waar wordt data opgeslagen?
- Wat is de waarde van data?

Techniek

- Welke mogelijkheden biedt techniek om de gewenste doelstelling te halen?
- Hoe kan toepassing van technologie (real-time) inzicht geven in een situatie of ontwikkeling t.b.v. preventie, bewaking, beveiliging en/of handhaving?

Bijlage 4 – **Vorm en inhoud workshop implementatie**

Op 17 januari 2019 zijn materiedeskundigen vanuit gemeenten, bedrijfsleven en kennisinstellingen bij elkaar gekomen, om in gezamenlijkheid na te denken wat Smart City kan betekenen voor de veiligheid in de stad. Tijdens de presentatie is er dieper ingezoomd op de definitie en elementen van Smart City en zijn bestaande relevante voorbeelden besproken. Ook is er dieper ingegaan op Stedelijke Veiligheid en de huidige veiligheidsvraagstukken.

Tijdens de workshopronde zijn er 4 groepen gemaakt. In elk van de groepen werd een veiligheidsvraagstuk uit de top 4 behandeld, namelijk: High Impact Crimes, Radicalisering en Polarisatie, Jeugd en Veiligheid en Ondermijning.

De opdracht uit de eerste ronde was als volgt:

- Bedenk gezamenlijk een aantal mogelijkheden van hoe Smart City technologie zou kunnen worden ingezet voor dit thema.
- Geef per idee antwoord op de volgende vragen:
  - Welke informatie uit welke sensoren gebruik je?
  - Welke beslissing(en) volgt/volgen uit deze informatie?
  - Welke partij(en) is/zijn hierbij betrokken?
  - Wat/wie help je ermee?
  - Hoe draag je bij aan het vraagstuk/wat lost het op?

In de tweede ronde is er voor de bedachte mogelijkheden dieper ingezoomd op het plan van aanpak, waarbij de volgende opdracht voor hetzelfde team werd uitgewerkt:

- Maak voor het gekozen idee een plan van aanpak:
  - Welke stappen moeten er gezet worden?
  - Welke partijen zijn daarvoor nodig en wat is hun rol?
  - Hoe kan je ervoor zorgen dat het gerealiseerd wordt?
  - Welke belemmeringen verwacht je?

Publicatie informatie
Smart Cities en stedelijke veiligheid

Een publicatie van
The Hague Security Delta (HSD)
Wilhelmina van Pruijsenweg 104
2595 AN Den Haag
T + 31 (0)70 204 5180
Info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL

Auteurs
Hans van Vliet (TNO)
Corine Bonte (TNO)
Ron Schipper (Van Aetsveld)
Peter van Dusseldorp (Van Aetsveld)

Begeleider
Mark Ruijsendaal (HSD)

Opmaak
Studio Maartje de Sonnaville naar een
ontwerp van Studio Koelewijn Brüggenwirth

Print
Drukkerij Edauw + Johanissen

Deze studie is mede tot stand gekomen op basis van gesprekken met en bijdragen van verschillende partijen (naast TNO en van Aetsveld), waarvoor wij hen hartelijk bedanken. Het betreft onder andere: Vereniging Nederlandse Gemeenten, Politie, Gemeente Den Haag, Gemeente Utrecht, DITSS, Siemens, Veiligheidsregio Midden- en West-Brabant, uCrowds, CCV, Strateq, Institute for Future of Living, SIM-CI, Axis, Saxion Hogeschool en collega's van The Hague Security Delta Foundation.

Together we Secure the Future

www.thehaguesecuritydelta.com