Samenvatting ICSS Onderzoeksagenda

De maatschappelijke doelstelling die de Impact Coalitie Safety & Security (ICSS) wil behalen is het vergroten van de stedelijke veiligheid. Door de toepassing van innovatieve technologieën in de stad kunnen veiligheidsproblemen worden aangepakt. 'Smart City' technologieën ontwikkelen zich in een rap tempo, waarbij de achterliggende infrastructuur van netwerken, dataverzamelingen en data-analyses steeds belangrijker wordt voor effectieve toepassing. De implementatie van technologie brengt enerzijds nieuwe kansen voor de stad, zoals de toepassing van sensoren en camera's voor veiligheid op straat, crowd management bij evenementen, het tegengaan van georganiseerde ondermijnende criminaliteit en digitale dreigingen. Anderzijds roept de toepassing van technologie ook nieuwe ethische, juridische en privacy vragen op. Toepassing van technologie kan leiden tot een extra risico: ze leidt tot een groter aanvalsoppervlak voor cybercriminelen en maakt de afhankelijkheid van technologie groter.

Vraagstukken variëren van 'Hoe kan bijvoorbeeld de burger beschermd worden tegen privacy schendingen en onveilige technologie?' en 'Welke data vinden partijen verantwoord om te delen en voor welk doel?'. En, 'welke technologische interventies zijn het meest effectief en efficiënt om tot veilige en leefbare gemeenten te komen?'. Het beter benutten van de technologie van de Smart City vraagt om een innovatieve, multi-partner benadering bij de aanpak van veiligheidsproblemen, waarbij zowel de overheid, het bedrijfsleven, de kennisinstellingen, als burgers samen moeten werken om technologieën op een cyberveilige, ethische en wetmatige manier te implementeren in de stad. Het bereiken van een gezonde balans tussen maatschappelijke leefbaarheid en technologietoepassing staat daarom centraal binnen ICSS Smart City projecten.

Door middel van de ICSS onderzoeksagenda worden Smart City projecten, onderzoeksthema's en onderzoeksvragen gebundeld om zodoende beter zicht te krijgen op huidige ontwikkelingen in het Smart City onderzoeksveld en de onbenutte kansen voor de ICSS. De complexiteit van elk veiligheidsvraagstuk is groter dan elke gemeenten op zich kan verwerken, en digitalisering en criminaliteit zijn grens overstijgend. Daarom pleit de ICSS om de krachten te bundelen met de onderzoeks- en innovatiegemeenschap, gemeenten, politie, bedrijven, burgers en andere actoren om technologie op een effectieve en efficiënte wijze in te zetten voor veiligheid. Het benutten van geïdentificeerde kansen is alleen haalbaar als gemeenten, politie en hun partners in de komende jaren samen optrekken door: elkaars experimenteerruimte slim te benutten; de samenwerking te richten op innovatie, implementatie èn opschaling; het actief delen van kennis en ervaring; gezamenlijke programmering; (inter)nationale profilering en leren met én van elkaar. Zodoende creëren we een Smart City ecosysteem waar technologie op een effectieve en verantwoorde wijze wordt ingezet om veiligheidsproblemen op te lossen. De eerste interne versie van de onderzoeksagenda is in 2021 opgesteld. In 2024 heeft er een grondige revisie plaatsgevonden om zodoende de actuele thema's, onderzoeksbehoeften en resultaten te vertalen naar de agenda voor 2025 en verder. Dit document dient als een samenvatting van deze gereviseerde onderzoeksagenda van de ICSS.

Maatschappelijke veiligheidsproblemen

Nederlandse gemeenten en politie kampen met een verscheidenheid aan maatschappelijke veiligheidsproblematiek. Meerdere overkoepelende veiligheidsproblemen zijn op dit moment zichtbaar in de veiligheidsagenda's van politie en gemeenten binnen de ICSS. De benoemde veiligheidsproblemen staan niet op volgorde van gemeentelijke en politionele prioriteit. De

afgelopen jaren zien we een significante toename in het aantal digitale dreigingen (zoals phishing, hacks, oplichting en afpersing) waardoor de nationale veiligheid in het geding komt. Tot op heden hebben maatschappij ontwrichtende cyberincidenten zich in Nederland (nog) niet voor voorgedaan. Daartegenover staat vast dat de uitval van digitale processen, als gevolg van een cyberincident, zich relatief vaak voordoen. Digitalisering en technologische ontwikkelingen zorgen niet alleen voor meer (digitale) veiligheid, maar functioneren ook als katalysatoren voor toenemende digitale dreigingen die complexer en dynamischer van aard zijn. De toenemende onderlinge verbondenheid van systemen kan leiden tot onvoorziene kwetsbaarheden van (vitale) processen, veiligheidsketens en ecosystemen, waar statelijke en criminele actoren misbruik van kunnen maken. Er is nog veel onbekend op digitaal vlak, waarbij niveauverschillen tussen gemeenten op het gebied van digitale weerbaarheid en informatieveiligheid zichtbaar zijn.

Georganiseerde- en ondermijnende criminaliteit en high-impact crime vormen in toenemende mate een bedreiging voor de maatschappij, waarbij democratische rechtsorde en sociale cohesie onder druk komen te staan. Liquidaties, drugscriminaliteit, mensenhandel en aanslagen op woningen zijn veelvoorkomend in Nederland. Vandaar dat het belangrijk is om minder weerbare gebieden en gelegenheidsstructuren van inbrekers, drugsdealers en mensenhandelaren aan te pakken. Ondermijning is geen nieuw fenomeen en zal lokale overheden op de kort en lange termijn voor uitdagingen plaatsen. Daarnaast zien we ook dat ongewenste buitenlandse inmenging, bijvoorbeeld in de vorm van hybride dreigingen, is toegenomen. Dreigingen en aanvallen worden veelal geïnitieerd vanuit statelijke actoren zoals Rusland en China. Hybride dreigingen ondermijnen de territoriale soevereiniteit van Nederland, waarbij de scheidslijn tussen oorlog en vrede steeds verder vervaagd. Gezien de positie van Nederland als ‘kennisland’ en (digitaal) knooppunt (datacenters en zeekabels), zal Nederland een interessant doelwit blijven van ongewenste buitenlandse inmenging.

Het beschermen en weerbaar maken van vitale infrastructuur en het tegengaan en voorbereiden op crisis- en grootschalige incidenten blijven belangrijke thema’s voor gemeenten en politie. Zowel de Operationele Techniek- als Informatie Technologie van (vitale) infrastructuur kan worden beschadigd door malafide actoren, waarbij lekken van privacygevoelige gegevens en ransomware aanvallen op de loer liggen. Het beschadigen van vitale infrastructuur kan zorgen voor ontregelingen in de maatschappij, door bijvoorbeeld de uitval van elektriciteitsnetten, uitval van drinkwatervoorzieningen en verstoring van communicatiekanalen van hulpdiensten. Verder zien we dat maatschappelijk ongenoegen, (online) maatschappelijke onrust, polarisatie en anti-overheidssentiment, met name sinds de COVID-19 pandemie, significant is toegenomen. Maatschappelijke spanningen uiten zich bijvoorbeeld in het belagen en bedreigen van politici, uit de hand gelopen demonstraties, ophitsing en rellen (zoals tijdens de ingestelde avondklok). Het aanpakken van maatschappelijke onrust, (anti-institutioneel) extremisme, radicalisering, jeugdcriminaliteit en straatintimidatie zijn daarnaast voorbeelden van onderbelichte onderzoeksthema’s waar de ICSS op kan inspelen.

Op technologisch gebied zien we de afgelopen jaren een stijging van het gebruik van onbemande systemen, waardoor er een toenemende druk is ontstaan op veiligheid, privacy en milieu. Ondanks de risico’s van drones, kunnen onbemande systemen ingezet worden om goederen en mensen te vervoeren (Urban Air Mobility) en om veiligheidscalamiteiten (zoals natuurbranden en crowd managementproblematiek) op te helpen lossen. De technologische basis van onbemande systemen

wordt versterkt door innovaties op gebieden zoals Artificial Intelligence (AI), augmented- en artificial reality, big data, U-Space (gezamenlijk luchtruim en onbemande luchtverkeermanagementsystemen), vliegen buiten het zichtveld van de drone operator (BVLOS) en digital twin toepassingen. Daarnaast zien we dat er, met name tijdens de COVID-19 periode, veel Smart City toepassingen ontwikkeld zijn binnen het thema crowd management. Een technologische toepassing, zoals de Crowd Safety Manager, is na de pandemie verder ontwikkeld en is in staat om een digitale 3D kaart te tonen waarop te zien is hoe druk het ergens is. Daarnaast gebruikt de tool meerdere informatiebronnen om te voorspellen waar drukte kan gaan ontstaan. Zodoende kunnen er slimmere beslissingen gemaakt worden over politie-inzet en inrichting van de fysieke publieke ruimte.

Kansen voor de slimme stad

De aanpak van veiligheidsproblemen wordt lastiger door toezicht- en handhavingsproblemen bij gemeenten en politie. Naast de additionele inzet van personeel is het noodzakelijk om 'slimmer' te handhaven. De inzet van technologie in de stad kan de lasten van gemeenten en politie potentieel verlichten en daarmee de heterdaad- en slagkracht vergroten. Als gevolg worden Smart City initiatieven steeds vaker geïnitieerd vanuit gemeenten en politie. Ook zien we dat het aantal sensoren toeneemt vanwege brede toepasbaarheid en relatief lage kosten. Door data uit sensoren te gebruiken en te combineren kunnen politie en gemeenten efficiënter te werk gaan.

Daarnaast nemen Smart City initiatieven met het doel om publieke veiligheid te verbeteren in hoog tempo toe. De afgelopen jaren komt Smart City onderzoek steeds meer tot stand, veelal geïnitieerd vanuit gemeenten en politie. Veel gemeenten maken in toenemende mate gebruik van technologie en (publieke en private) data voor de uitvoer van veiligheidstaken en -beleid. Een van de valkuilen van het toenemende aantal Smart City initiatieven is dat het gefragmenteerd plaatsvindt, waardoor lokale initiatieven soms onzichtbaar blijven en een (nationaal) overzicht niet is opgezet. Ook al wordt kennis steeds vaker gedeeld tussen betrokken partijen en worden lessen gemakkelijker ingezet bij andere gemeenten of benut door bedrijven, blijft het vanwege de lokale fragmentatie een uitdaging voor gemeenten om van elkaar te leren. Door meer integraal, en in co-creatie en in afstemming met onderzoekers, richting en sturing aan te brengen in de onderzoeksactiviteiten verwachten we ze effectiever en efficiënter te maken. Hierdoor kunnen publieke en private partijen kansrijke Smart City initiatieven breder inzetten, benutten en opschalen.

Werkpakketten, thema's en sub-thema's

De onderzoeksagenda hanteert drie werkpakketten, elk uitgesplitst in meerdere sub-thema's met desbetreffende onderzoeksvragen. Werkpakket twee, "veilige en geïntegreerde Smart City toepassingen", en werkpakket drie, "maatschappelijk verantwoorde en duurzame ontwikkeling" zijn randvoorwaardelijk voor werkpakket één "gebiedsgericht beveiligen met behulp van Smart City toepassingen". Het eerste werkpakket richt zich op thema's en onderzoeksonderwerpen die bijdragen aan oplossingen om veiligheidsproblematiek in de openbare ruimte op te lossen. Hierbij wordt als eerste stil gestaan bij veiligheidsprioriteiten van gemeenten en politie, zoals crisis- en grote incidenten, ondermijning en digitale dreigingen, maar ook aandacht besteed aan onderbelichte veiligheidsonderwerpen, zoals jeugdcriminaliteit, discriminatie en (anti-institutioneel) extremisme. Sensoren, camera's en andere technologische innovaties, in combinatie met algoritmen, kunnen als oplossing dienen om problematiek in de stad aan te pakken. Een sensor heeft namelijk de capaciteit om bewegingen waar te nemen, te beoordelen en vervolgens data te

presenteren voor de eindgebruiker. Hoe pas je deze technologische innovaties toe op een verantwoorde manier in de stad, bijvoorbeeld ten behoeve van de thema's crowd management en drones, waarbij er rekening wordt gehouden met privacy, en ethische en juridische randvoorwaarden? Een solide beleids- en bestuursarchitectuur is essentieel om mee te nemen bij de toepassing van technologie in de stad.

Het voorkomen dat innovatieve oplossingen en technologieën voor nieuwe onveiligheid zorgen in de stad staat centraal in het tweede werkpakket. Het voorkomen van onveiligheid begint met het implementeren van principes, zoals security-by-design en privacy-by-design, voor veilige OT, IT en IOT-systemen. Hierbij moeten afwegingen worden gemaakt welke hard- en software als basis kunnen dienen voor de technologische innovatie; welke cybersecurity risico's naar voren komen; en hoe cybersecurity risico's gemitigeerd kunnen worden door het gebruik van bijvoorbeeld risicomanagement en risicokaarten van het digitale domein. Daarnaast is de bestuurs- en beleidskant van cybersecurity belangrijk, waarbij er secuur moet worden nagedacht over organisatorische verantwoordelijkheden en processen. Cybersecuritywetgeving en cybersecuritystandaarden spelen een essentiële rol binnen de bestuurs- en beleidskant van cybersecurity.

Samenwerking, ethiek, privacy en de inrichting van de (digitale) sociale infrastructuur zijn essentiële onderwerpen die naar voren komen binnen het derde werkpakket. Bij elk Smart City project is het noodzakelijk om na te denken over de organisatorische inrichting, waarbij afwegingen moeten worden gemaakt welke partijen (burgers, bedrijven, kennisinstanties, overheidsorganisaties) betrokken moeten worden bij het proces. Welke samenstelling van actoren leidt tot het gewenste resultaat, en hoe kan succesvolle innovatie leiden tot implementatie en opschaling naar andere gemeenten? Bij de uitvoering van Smart City projecten is het daarnaast van belang om ethische en privacyoverwegingen mee te nemen rondom de verwerking van persoonsgegevens, effectieve datadeling, data-minimalisatie, de rol van autonome systemen en transparantie bij de toepassing van Smart City technologieën. Welke data is noodzakelijk om tot het gewenste resultaat te komen, en vinden we het acceptabel om Smart City technologieën meer autonomie te geven? De functionaliteit en weerbaarheid van de (digitale) sociale infrastructuur is daarnaast belangrijk voor veiligheids- en innovatieketens om op een verantwoorde wijze Smart City projecten uit te voeren.

De werkpakketten, onderzoeksthema's en onderzoeksvragen geven richting en sturing aan onderzoeksactiviteiten die ondersteunend zijn aan de doelen en projecten van de ICSS. De onderzoeksagenda is een handreiking naar kennisinstellingen vanuit de vraagstukken uit het gemeentelijk veld. Daarnaast kunnen actoren vanuit het Smart City veld, zoals andere gemeenten, bedrijven, maatschappelijke organisaties en overheidsinstanties de onderzoeksagenda als basis gebruiken om nieuwe Smart City projecten op te zetten, om samenwerkingen aan te gaan met lopende projecten of partijen en om subsidiegelden aan te vragen. Als laatste fungeert de onderzoeksagenda als een 'call to action' voor partijen die een samenwerking willen aangaan met de ICSS. De ICSS staat open voor geïnteresseerde partijen die willen bijdragen aan (onderzoeks)projecten en is te bereiken via het email adres: info@veiligesmartcities.nl of de website: www.veiligesmartcities.nl.

Bibliografie

Gemeente Almere. (2023). Veiligheidsagenda Almere 2023-2026.

Gemeente Amsterdam. (2023). Regionaal Veiligheidsplan 2023-2026.

Gemeente Apeldoorn. (2023). Concept Integraal Veiligheidsplan Apeldoorn 2023-2026.

Gemeente Den Haag. (2023). Integraal Veiligheidsbeleid 2023-2026.

ICSS. (2024). Uitvoeringsagenda 2024.

Nationale Politie. Visie op sensing.

NCSC. (2023). Cybersecuritybeeld Nederland 2023.

NCTV. (2023). De Veiligheidsstrategie voor het Koninkrijk der Nederlanden.

NLR. (2021). Strategische Ambitie Drones – Executive Summary.

TNO, ICSS. (2022). Smart Cities voor Publieke Veiligheid: Geleerde Lessen uit de Praktijk van Crowdmanagement – Managementsamenvatting.

VNG, Stichting Maatschappij en Veiligheid, Tilburg University. (2022). Essay: Lokaal Veiligheidsbeleid in 2030.