BESAFE 51

Inspiratie voor uw lokaal veiligheids - en preventiebeleid
JULI 2019

ibz

P708831 | Afgiftekantoor Antwerpen X
Verschijnt 5x per jaar

TECHNOLOGIE

Interview met Claudia De Maesschalck, Chief Disruption Officer

"Om een malafide netwerk te bekampen, hebben we een bonafide netwerk nodig"

In sommige grote organisaties wordt de innovatie geleid door een chief disruption officer. IBZ heeft er sinds kort ook een. De taak van CDO Claudia De Maesschalck spitst zich toe op de nieuwe technologieën die malafide netwerken gebruiken.

U bent aangeduid als de eerste Chief Disruption Officer voor de overheden bevoegd voor Veiligheid, in de eerste plaats voor IBZ, en ingebed binnen de AD Veiligheid en Preventie. Wat houdt deze functie precies in?

Claudia De Maesschalck: "Ik wil graag even de voorgeschiedenis schetsen: enkele jaren geleden was IBZ aanwezig op een congres over hoe snel nieuwe technologieën evolueren en deze de bonafide ecosystemen kunnen ontwrichten indien men zich niet proactief voorbereidt. Denk aan retail en e-commerce, of de Uberisatie van goederen en diensten aan huis. Maar ook – en vooral – in het ecosysteem van de veiligheid kunnen we niet op de lauweren rusten. Malafide netwerken bedienen zich volop van nieuwe technologieën en hebben per definitie niet de remmingen die de essentie uitmaken van het bonafide netwerk, met name: ethische, reglementaire en legistieke grenzen. Men mag daar gerust ook budgettaire grenzen aan toevoegen. Met andere woorden, we moeten disruptiever durven zijn om hun business model – dat sterk tech-driven is – zoveel mogelijk onderuit te halen. Enkele jaren geleden waren de geesten misschien nog niet rijp. Nu wel."

> "In het ecosysteem van de veiligheid kunnen we niet op onze lauweren rusten."

U zegt dat de geesten nu rijp zijn, kan u dat even verder toelichten?

Claudia De Maesschalck: "Peter Hinssen, één van inspirerende tech-goeroes achter Niveau S, stelt duidelijk: 'it takes a network to beat a network', en ook dat de voorbereiding op 'The day after tomorrow' nu moet gebeuren. Terwijl we toch nu – u vergeeft mij de uitdrukking – nog al te veel bezig blijven met het opruimen van brol van de dag voor gisteren. Dit inzicht maakte het Congres Niveau S van 19-20 december van vorig jaar mogelijk. Het werd georganiseerd door IBZ en VIAS en bracht op zeer transparante wijze veiligheidsdiensten, private actoren, kenniscentra en burgers samen om na te denken over hoe we ons samen moeten voorbereiden op de dag na morgen, als een coherent en sterk bonafide netwerk ter bestrijding van de ontwrichting van het maatschappelijk weefsel door malafide netwerken en hun ondermijningsmodel. Het Congres heeft geleid tot een aantal conclusies en aanbevelingen en het is nu mijn opdracht om dit te vertalen in nieuw en duurzaam beleid."

THEMANUMMER

Nieuwe technologieën spelen een alsmaar belangrijkere rol in het veiligheids- en preventiebeleid. Besafe brengt een overzicht.

▶ *vervolg van pagina 1*

Waarom heeft men u gevraagd, toch een buitenstaander vermits u onder de FOD Buitenlandse Zaken valt?

Claudia De Maesschalck: "De beleidsvertaalslag van Niveau S is per definitie transversaal en silo-overschrijdend. In die zin is het een voordeel dat ik zelf niet uit een veiligheidsdienst kom, maar dat ik wel ervaring heb met veiligheidsmateries. Als ex-voorzitter van de Nationale Veiligheidsoverheid, in volle aanslagenperiode, heb ik met de veiligheidsdiensten gewerkt. Overigens heb ik mij gedurende mijn diplomatieke carrière van meer dan 25 jaar gespecialiseerd in wetenschaps- en technologiediplomatie. Dit maakt dat ik naast de overheidsactoren ook een uitgebreid netwerk heb binnen kenniscentra en de tech-industrie."

Nog een vraag over de functie: waarom precies Chief Disruption Officer, en niet Chief Innovation Officer?

Claudia De Maesschalck: "Omdat silo-overschrijdende initiatieven meer dan een incrementele aanpak vereisen. Innoveren is een vanzelfsprekende bezigheid. De technologieën die we willen aanboren zijn misschien op zich niet disruptief, maar de manier waarop de overheid ze zal omarmen en integreren binnen veiligheidstoepassingen is dat wel. De oplossingen zullen disruptief zijn, de manieren waarop ze worden aangeboord en gebruikt eveneens. Dit geldt tevens voor de mindset die hiervoor nodig is. Ook hier is disruptie aangewezen, zoniet noodzakelijk."

© FOTO CLAUDIA DE MAESSCHALCK

CDO Claudia De Maesschalck: "We moeten niet alleen het geweer van schouder veranderen, maar ook het geweer zelf is aan vervanging toe."

Welke zijn nu in concreto de werven die u opstart?

Claudia De Maesschalck: "Er zijn meerdere werven; alle hebben eigen finaliteiten maar versterken elkaar tegelijkertijd. Drie springen er uit: in de eerste plaats het oprichten van een duurzaam juridisch kader waarbinnen de vier kwadranten – overheid, privé, kenniscentra en burger – binnen de veiligheidssfeer elkaar op structurele wijze kunnen ontmoeten: om op te schalen, vraag en aanbod as is en to be bijeen te brengen. Zo kan niet alleen gerichter en projectmatig worden samengewerkt, maar wordt ook juridisch vorm gegeven aan het bonafide netwerk. Alle overheidsdiensten kunnen er niet alleen hun inventaris in kwijt van wat al bestaat, maar ook de cartografie aan noden in onderbrengen. Dat moet optimalisatie van wat is en wat moet worden toelaten tussen alle vragers en aanbieders. Zonder overlap, fragmentering, of tegenstrijdige programmatie.

Een tweede werf gaat meer over 'maken'. Er is nood aan tegengaan van versnippering van datagaring en -opslag. Het delen van data moet niet alleen versterkt worden binnen de overheden, – denk aan de aanbevelingen van de parlementaire commissie na de aanslagen – maar moet ook worden nagestreefd met de 'buitenwereld'. De overheid wil geen toegang tot private data, wel integendeel: het behoort tot onze opdracht om die te beschermen. Anderszins is er nog al te veel een tweedeling tussen de integriteit van de fysieke identiteit en die van de digitale identiteit. Wat dit laatste betreft, wil ik verwijzen naar het kaderstukje over data insight sharing verder in dit nummer."

> **"Malafide netwerken bedienen zich volop van nieuwe technologieën en hebben per definitie niet de remmingen die de essentie uitmaken van het bonafide netwerk, met name: ethische, reglementaire en legistieke grenzen."**

En de derde werf?

Claudia De Maesschalck: "Die is in se de transversale: bij alles wat we doen, weze het prioriteiten stellen, nieuwe technologieën stimuleren dan wel unusual suspects samenbrengen, moet dit alles getoetst worden. Niet alleen aan de haalbaarheid en betaalbaarheid, maar ook op wenselijkheid dan wel toelaatbaarheid. Daarom pleit ik sterk voor de oprichting van een pluridisciplinaire raad die hiervoor de werkvork biedt die ons moet begeleiden in het regel- en wetgevend kader. Ook hier is proportionaliteit een rode draad: wil de overheid relevant blijven, dan mogen we niet verworden tot de lastige nonkel die alles vergalt. We moeten ook de leuke nonkel op het feest kunnen zijn, die tevens inspireert en vertrouwen biedt. Zo blijft het feest een plezante publiekstrekker, zonder dat het uit de hand loopt."

Dreigt met die nieuwe technologie niet het doemscenario van big brother of Minority Report?

Claudia De Maesschalck: "Daarom hebben we precies de ethische raad nodig. Evenwel, nieuwe technologie en de mogelijkheden ervan niet omarmen is in se nog onethischer: het geeft de tech-savvy malafide netwerken vrij spel en daarmee zou de overheid precies aan een van haar kerntaken verzaken, nl. de bescherming van het algemeen belang en de veiligheid van en binnen het bonafide netwerk.

We moeten niet alleen het geweer van schouder veranderen, maar ook het geweer zelf is aan vervanging toe. Om die paradigmashift te bewerkstelligen is het daarentegen van belang dat klein wordt gestart. Met laaghangend fruit. Met goed uitgedachte use cases die een olievlek kunnen starten en die door bewezen nut ook andere veiligheidsdiensten en actoren binnen het veiligheidsecosysteem kunnen inspireren en stimuleren. Daarom ben ik ook blij dat binnen alle diensten een SPOC (single point of contact) is aangeduid die dicht staat bij de chefs, en ook het eigen terrein uiterst goed kent om met steun van de hiërarchie goed gefocuste proeftuinen op te zetten. In dit kader wil ik alvast iedereen bedanken voor de samenwerking."

Het Internet of Things: handig bij diefstalpreventie, maar ook voor inbrekers

Niet alleen computers, smartphones en/of tablets kunnen worden aangesloten op het internet. Ook andere apparaten zoals koelkasten, wasmachines en thermostaten kunnen er gebruik van maken.

Langzaam maar zeker zal het Internet of Things (IoT) de wereld om ons heen veranderen. Tegen 2020 zullen er meer dan 20 miljard objecten geconnecteerd zijn met het internet, met elkaar en zeker ook met apps. Het IoT heeft als doel om ons leven makkelijker te maken. Door de connectie met het internet worden domme objecten vaak nuttiger en wellicht breder inzetbaar.

Het bekendste voorbeeld van zo een IoT-toestel is de slimme koelkast: het toestel weet wanneer de houdbaarheidsdatum van producten verstreken is, zet de koeling een standje hoger als er een hittegolf heerst en beheert de voorraad. Dit dankzij sensoren in de koelkast, een internetverbinding en een intelligent systeem dat het verbruik bijhoudt.

Andere slimme toestellen zorgen voor een betere beveiliging van de woning, denk maar aan bewakingscamera's en slimme deursloten die vanop een smartphone met een app kunnen worden bediend. Zo kan de woning nog beter beveiligd worden.

Of toch niet? Er zijn namelijk ook enkele risico's aan IoT. Het internet blijft het Wilde Westen en ontwikkelt zich razendsnel, wat kan zorgen voor een verminderde beveiliging en de mogelijkheid dat het wifi-netwerk overgenomen worden door hackers. Elke verbinding van een slim toestellen met internet is een mogelijk doelwit voor criminelen die deze toestellen willen overnemen om zo bijvoorbeeld het slimme deurslot te kraken en te openen.

Om u hiertegen te wapenen komt u met een goede beveiliging van uw wifi-netwerk en IoT-toestellen al een heel eind ver. Enkele tips:

- voorzie meerdere lagen beveiliging in elk IoT-toestel: een slim slot van uw voor- of achterdeur kunt u bijvoorbeeld via uw mobiele app combineren met een code die u moet ingeven of met een vingerscan.
- beveilig uw draadloze wifi-netwerk altijd met een sterk wachtwoord.

Nuttige links

- www.besafe.be/nl/nieuws/wees-slim-en-beveilig-ook-je-slimme-apparaten
- www.safeonweb.be/nl/gebruik-sterke-wachtwoorden

Van slimme deurbel tot thermostaat en fiets

Het Internet of Things kent ondertussen al heel wat toepassingen die kunnen helpen bij diefstalpreventie.

Neem nu de slimme deurbel. Hiermee kunt u via uw smartphone vanop afstand nagaan wie er voor uw deur staat, kunt u communiceren met deze bezoeker en wekt u de illusie dat u thuis bent. Bent u echter wantrouwig, dan kunt u vanop afstand wat muziek opzetten in de woning. Zo lijkt het alsnog dat u echt thuis bent.

Daarnaast zijn ook de huisthermostaat die op gepaste tijdstippen vanop afstand kan worden bediend en intelligente lampen onderdelen van het Internet of Things. Het automatiseren van de connectie met de lampen in huis kan eveneens aanwezigheid simuleren, ook als er niemand in de woning is. Het is een hulpmiddel in de bestrijding van woningdiefstal. Idem dito voor de rolluiken die vanop afstand kunnen worden aangestuurd, ook als de bewoner op vakantie is.

Tot slot is er in Nederland een slimme fiets ontwikkeld, die voorzien is van een speciale sensor. Deze sensor kan door een fietsendealer met industriële lijm op eender welke fiets worden geplakt. De sensor staat standaard altijd uit, waardoor hij nagenoeg geen energie verbruikt en dus niet kan uitvallen. Wanneer een fiets gestolen wordt, kan de rechtmatige eigenaar van de fiets de sensor activeren via een mobiele app. Eens geactiveerd zendt de sensor de locatiegegevens door naar een opsporingsteam dat zo kan zien waar de gestolen fiets zich bevindt en onmiddellijk in actie kan schieten om deze terug te vinden.

De smartphone, het vertrekpunt om de thermostaat, de deurbel, de rolluiken, de verlichting vanop afstand te besturen.

© FOTO SHUTTERSTOCK

Steeds efficiëntere bewakingscamera's

De bewakingscamera is de tool bij uitstek geworden om zowel de openbare weg als gebouwen of gesloten ruimten (openbaar, privaat of volledig privatief) te beveiligen.

Over beelden beschikken, ze ter plaatse of op afstand kunnen raadplegen, ze in real time of achteraf kunnen bekijken, brengt een geruststellend element met zich mee, een gevoel dat als er iets gebeurt, we de oorzaken kennen en adequaat kunnen reageren. Waar in het begin CCTV-systemen enkel gebruikt werden voor het verzamelen en opnemen van beelden, laat de huidige technologie toe veel verder te gaan. Of het nu gaat om camera's die uitgerust zijn met geluidsdetectoren, warmtedetectoren, bewegingsdetectoren, camera's voor automatische nummerplaatherkenning of camera's met gezichtsherkenning, bewakingssystemen zijn steeds vaker uitgerust met een oplossing voor beeldanalyse, of zelfs uitgerust met AI, om te kunnen melden wanneer er iets gebeurt, beelden te kunnen filteren, te sorteren en te structureren. Deze intelligentie maakt het in ieder geval mogelijk om de efficiëntie van de geïnstalleerde bewakingscamera's te verhogen en helpt de operatoren ook bij het bekijken van beelden in real-time. Daarnaast is ook de kwaliteit van de beelden, evenals de opslagcapaciteit, aanzienlijk verbeterd, waardoor het vaststaat dat beelden een onmisbaar bewijselement worden.

Door de nieuwe onlinetoepassing voor de aangifte van de bewakingscamera's, die in 2018 werd gelanceerd, weten de politiediensten waar bewakingscamera's zijn geïnstalleerd en met wie ze contact kunnen opnemen om toegang te vragen tot de beelden in het kader van hun politietaken. Wanneer er feiten plaatsvinden, vraagt men zich in eerste instantie af of er camera's aanwezig zijn en of er beelden van deze feiten werden gemaakt.

Natuurlijk moet er bij het gebruik van eender welke technologie rekening worden gehouden met de geldende wetgeving inzake de bescherming van persoonsgegevens en de beperkingen van de Camerawet[1], maar het is duidelijk dat bewakingscamera's en zelfs intelligente bewakingscamera's in de toekomst niet meer weg te denken zullen zijn.

Nuttige link

- www.besafe.be/nl/veiligheidsthemas/camera/camerawet

1 Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, die ingrijpend werd gewijzigd door de wet van 21 maart 2018.

Camera's met gezichtsherkenning: er zijn nog privacy-belemmeringen

Acht jaar geleden testte de politiezone RIHO vier digitale camera's met gezichtsherkenning. Die werden toen gebruikt bij de opnames van het televisieprogramma Villa Vanthilt, dat elke avond zo'n 800 mensen naar de grote markt lokte. Dat cijfer werd ook berekend door de slimme camera's. De beelden van de camera's werden via het 3G-netwerk van Belgacom naar de meldkamer doorgestuurd. Roeselare was toen de eerste stad die met dergelijke technologie experimenteerde. "Het was een eenmalig project dat we uittesten in samenwerking met Belgacom, dat ook een deel van de kosten op zich nam," zegt Tineke Verduyn van PZ RIHO. "We hebben bij wijze van proef toen de beelden gelinkt aan een databank met foto's, waaraan enkele personen hun medewerking hadden verleend. Om het project verder te zetten zouden we een ruimere databank nodig hebben gehad, maar daar staken juridische belemmeringen de kop op. Bovendien stond op dat moment ook de technologie nog niet helemaal op punt. Vandaag is die ongetwijfeld beter en zijn de netwerken veel sneller. We hebben ondertussen wel de nieuwe Video Synopsis-technologie aangekocht. Die zorgt ervoor dat onze 128 camera's 'slim' worden. Hierdoor kunnen we zowel in real-time als bij opgeslagen beelden niet enkel gericht zoeken naar personen maar ook naar voertuigen."

Ook Kortrijk tast met die technologie de grenzen van de mogelijkheden af. Die software slaat alle objecten op die in het beeld van de camera's komen en filtert die op basis van karakteristieken zoals het geslacht of de kledij van personen. De software kan ook gezichten herkennen, maar omdat er daaromtrent nog wettelijke beperkingen zijn, wordt die functionaliteit in Kortrijk nog niet gebruikt.

Slimme camera's kunnen personen in een massa filteren op basis van karakteristieken zoals het geslacht of de kledij.

© FOTO BELGAIMAGE

Drone: van Unidentified Flying Object (UFO) naar Unmanned Aerial Vehicle (UAV)

U heeft mogelijk al eens een drone of UAV zien voorbijvliegen. We kennen ze vooralsnog als technologisch tienerspeelgoed of, recenter, als bewakingsmiddel voor de politie. Maar drones zijn intussen veel meer dan dat.

Drones kunnen uitgerust worden met een gewone beeldcamera, dat wist u ongetwijfeld wel al, maar ook met thermische camera's, sensoren, een navigatiesysteem om autonoom te kunnen vliegen, zelfs met een elektronische nummerplaat om ze te identificeren. Zo kunnen ze nu ook worden uitgerust met AI in het kader van anti-drone operaties.
Er zijn talloze toepassingen die voortkomen uit de dronetechnologie:

- bewaking van publieke evenementen en bedrijvenzones;
- onderhoud van bedrijven en (offshore) windturbines, waarbij drones de installaties nakijken door er al filmend over te vliegen terwijl een technicus aan land deze beelden ontvangt en analyseert;
- Google en Amazon ontwikkelen leverdiensten met autonome drones;
- wanneer in Antwerpen een brand uitbreekt, vliegt een autonome drone van de brandweerzone uit naar de brandhaard. Deze drone filmt de brand en stuurt de beelden live door naar de brandweerwagen, nog voor deze aankomt. En drones kunnen zelfs al bosbranden detecteren in afgelegen gebieden.

Toch zijn er ook enkele niet te onderschatten risico's. Zo is het risico op een panne vele malen groter dan bij een vliegtuig. Technologie is per definitie neutraal en kan zowel voor bonafide als malafide doeleinden gebruikt worden. Daarom spelen we als overheid in op nieuwe evoluties en waken we erover het gebruik voor malafide doeleinden te bestrijden. Zo is het belangrijk om weten dat drones onderhevig zijn aan heel wat regelgeving, afhankelijk van de toepassing, waaronder in de eerste plaats het KB drones. Voor bewakingsdrones die zijn uitgerust met een camera (mobiele camera's) gelden bovendien de Camerawet en de GDPR-wet voor verwerkingen van persoonsgegevens. De Wet op het Politieambt regelt tot slot het gebruik van drones door de politie.
Op die manier zijn drones voortaan ook voor u geen UFO's meer.

Nuttige link

- www.besafe.be/nl/veiligheidsthemas/camera/gebruik-van-cameras-door-politiediensten/d-welke-cameras-wanneer-en-waar

PZ CARMA gebruikt onderwaterrobot voor speurwerk

Politiezone CARMA (As, Bocholt, Bree, Genk, Houthalen-Helchteren, Kinrooi, Oudsbergen, Zutendaal) nam in 2016 een ROV of 'remotely operated underwater verhicle' in gebruik. De ROV beschikt over verlichting en camera's en kan ingezet worden voor doelgericht speurwerk onder water. De politie kan zo sneller handelen bij vermissingen of in het kader van gerechtelijke dossiers. De zone ontwikkelde de onderwaterrobot in eigen beheer in samenwerking met enkele experts. De ROV is een klein en wendbaar toestel, dat vanop de waterkant of vanop een boot bestuurd wordt met een afstandsbediening. De beelden die door de camera in de ROV gemaakt worden, kunnen live gevolgd worden op een monitor. Het toestel kan geen voorwerpen manipuleren of boven water brengen. De politie blijft dus een beroep doen op een duikersteam van de brandweer of van de Civiele Bescherming zodra iets verdachts aangetroffen wordt, of als het gaat om zoekopdrachten op te grote duikdiepte of over een te grote oppervlakte.
"We gebruiken het toestel voor gerichte opdrachten," zegt woordvoerder Marleen Smeyers. "Omdat we het snel kunnen inzetten, kan het ons al een beeld geven vóór de gespecialiseerde diensten ter plaatse zijn. Daarnaast heeft het ook voordelen ten opzichte van duikers: het veroorzaakt minder wervelingen onder water, waardoor het zicht van de camera's niet vertroebelt door wervelingen in het water en opstuivend zand. Doordat we het toestel ook kunnen inzetten in combinatie met een boot, kan een groter gebied doorzocht worden."

De onderwaterrobot van PZ CARMA is klein en kan daardoor snel worden ingezet.

© FOTO PZ CARMA

Data insight sharing: een nieuwe generatie van data delen

Gezien data niet meer behoren tot het monopolie van de overheden, ontstaan er nieuwe verantwoordelijkheden voor alle 'houders' van data en data-inzichten: overheden, private sector en de burgers.

De veiligheidsoverheden kunnen immers nog steeds buigen op het monopolie van het geweld, maar het monopolie op informatie is al geruime tijd verdwenen. Dat is op zich geen ramp, maar de overheden moeten er wel over kunnen waken dat de integriteit van de digitale identiteit, of beter nog, identiteiten, want deze zijn verspreid over verschillende platformen, verzekerd blijft. Dit is in het belang van zowel de overheden, de private actoren en, opnieuw, in het bijzonder de burger.
Een platform 'van de nieuwe generatie' voor het delen van data en data-inzichten moet verwezenlijkt worden. Deze nieuwe architectuur zal ongetwijfeld van hybride aard zijn, met een ruggengraat, maar ook met elementen van blockchaintechnologie van de 3e of 4e generatie.
Hierbij moeten we, middels een volwassen databeheer, een gepast evenwicht vinden tussen een adequate beeldvorming en proportionaliteit. Verschillende initiatieven hieromtrent zijn al in ontwikkeling of worden weldra opgezet op verschillende gezagsniveaus, inclusief door de Europese Commissie, die zich voorbereidt op een nieuwe visie op datadeling gebaseerd op het concept van self souvereign identity, dat een nieuwe macht geeft aan de burger over de manier waarop zijn eigen digitale data worden gedeeld en gebruikt.

PZ Brasschaat registreert verkeersovertredingen met smartphone

De medewerkers van de dienst verkeer van de politiezone Brasschaat werken al sinds 2016 met handhelds waarmee verkeersovertredingen eenvoudig en snel vastgesteld kunnen worden. Via een aangepast softwareprogramma worden alle gegevens meteen op straat geregistreerd en afgewerkt. "De agenten nemen een foto van de overtreding, registreren de nummerplaat van het voertuig en vullen de bijhorende gegevens in. In het commissariaat worden de gegevens daarna automatisch gedownload naar het politienetwerk. Dat gebeurt volledig automatisch. Dankzij de smartphones kunnen de agenten en inspecteurs meer op straat aanwezig zijn", verduidelijkt hoofdinspecteur Werner Hoogsteyns, verantwoordelijke verkeer, van de PZ Brasschaat.
De Android-smartphones zijn door de firma Tradelec, die gevestigd is in Genk, ontwikkeld op maat van de politie en op basis van bevindingen op het terrein. Voor een vlotte en correcte verwerking van identiteitsgegevens kan de barcode van een identiteitskaart gescand en toegevoegd worden. De toestellen zijn verstevigd ('ruggedized') en hebben een hoge graad van waterdichtheid.
"We hebben momenteel 4 toestellen in dienst", voegt Werner Hoogsteyns toe, "maar door het grote succes voegen we daar binnenkort nog 2 toestellen aan toe."

© FOTO PZ BRASSCHAAT

Werner Hoogsteyns: "De handhelds passen in het beleidsplan van het bestuur om meer blauw op straat te krijgen. De politie moet zich kunnen concentreren op de kerntaken en er dient een verdere ontlasting te gebeuren van de administratieve werklast door het vereenvoudigen van de bedrijfsprocessen en het digitaliseren ervan."

Uitrol politie-app FOCUS@GPI van start

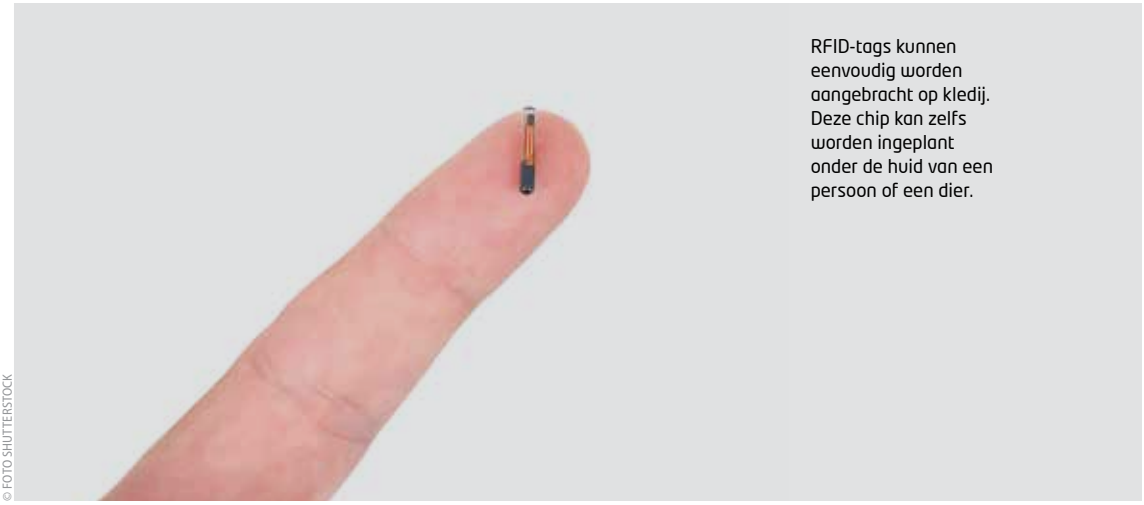
Sinds februari van dit jaar kunnen politiemensen via een smartphone snel en eenvoudig toegang kunnen krijgen tot het Strafregister, het Rijksregister en de databank met nummerplaten. Dat gebeurt via de politie-app Focus@GPI. Via dezelfde app kunnen ze ook een proces-verbaal opstellen of andere nuttige informatie bekijken. Doordat persoonsgegevens rechtstreeks via de app kunnen worden opgevraagd, worden de medewerkers van de dispatching voor een stuk ontlast.
In eerste instantie werd de app ter beschikking gesteld van de vier Vlaamse politiezones Druivenstreek, Voorkempen, Westkust en Antwerpen, de federale wegpolitie Antwerpen, de twee Brusselse zones Polbruno en Marlow, en de drie Waalse zones Namur, Mons-Quévy en Weser-Göhl. In de loop van dit en volgend jaar wordt het systeem verder uitgerold naar de andere politiezones en eenheden van de federale wegpolitie.
Met de app krijgen de politiemensen dan wel via hun telefoon toegang tot de databanken, maar dat gebeurt uiteraard binnen een duidelijk afgebakende regels. Databanken kunnen pas worden geconsulteerd indien dat past binnen de functie of de operationele rol die de betrokken politieman of -vrouw vervult. Gebruiksrechten voor de mobiele toepassingen worden ook gepersonaliseerd toegekend en alle uitgevoerde opzoekingen worden gelogd. De eenheden kiezen zelf in welke politiebasisfunctionaliteiten Focus@GPI wordt gebruikt.

RFID-technologie helpt personen en goederen te traceren

RFID (Radio Frequency IDentification) wordt gebruikt om vanop afstand personen of voorwerpen te lokaliseren en te identificeren. Dat gebeurt via radiosignalen.

Het systeem maakt gebruikt van etiketten of tags die worden aangebracht op de personen of voorwerpen. Die tags zijn voorzien van een elektronische chip en een antenne. De tags zenden signalen uit op een bepaalde radiofrequentie die dan worden opgevangen door een lezer. Elk voorwerp met een RFID-tag heeft een identiteit of een uniek nummer dat zo naar een lezer wordt gestuurd. Door hun elektronische chip hebben ze meer mogelijkheden dan barcodes. Die zijn immers alleen leesbaar als ze binnen de optische straal van het scantoestel vallen.
Tags kunnen passief zijn en de vorm aannemen van een kleefetiket, bv. op een pakket, of een implantaat dat onder de huid van een levend wezen kan worden geplaatst. Actieve tags vertienvoudigen de mogelijkheden van passieve tags en worden gevoed door autonome batterijen.
RFID wordt hoofdzakelijk gebruikt in distributie om de identificatie, de inventaris en de lokalisering van producten te vergemakkelijken. RFID zit bijvoorbeeld ook in vervoersbewijzen, toegangsbadges en in onze paspoorten. Vermits RFID-technologie dus ook individu-gebonden kan zijn, is privacybescherming belangrijk.
Anderzijds kan deze technologie uiterst gepast zijn om kledingstukken, waaronder uniformen, te beveiligen. Dat is nu al het geval in industriële wasserijen, of op cruiseschepen en andere omgevingen waar personeel een uniform draagt. Zo kunnen die kledingstukken gelokaliseerd worden als ze ontvreemd of oneigenlijk gebruikt worden.
Zo'n tag kan echter vrij gemakkelijk worden uitgesneden of verwijderd wanneer deze wordt ingebracht in textiel. Daarom worden de mogelijkheden onderzocht om deze RFID technologieën in het textiel te weven. Met andere woorden: het textiel zelf is dan een wearable RFID-tag.

> **"RFID kan uiterst gepast zijn om kledingstukken, waaronder uniformen, te beveiligen."**



RFID-tags kunnen eenvoudig worden aangebracht op kledij. Deze chip kan zelfs worden ingeplant onder de huid van een persoon of een dier.

"En nu?"

Zoals blijkt uit bovenstaande kaderstukjes brengt iedere technologie zowel voordelen als nadelen. Per definitie zijn deze moeilijker in te schatten in het geval van nieuwe disruptieve technologieën: zullen ze hun beloften waarmaken? En welke neveneffecten, ten goede en ten kwade, kunnen we verwachten? Vooral dat laatste maakt de oefening gevoelig, want wellicht zijn niet alle schadelijke neveneffecten en hun impact nu reeds in te schatten.

"We hebben een Ethische Raad nodig, maar we moeten ook voor onszelf de afweging blijven maken rond kosten en baten, weze het letterlijke kosten en baten, dan wel die van morele en deontologische aard."

We mogen ons ook niet laten vangen door nieuwe technologieën als doel op zich te zien. Het moeten middelen blijven, in ons geval tot een bepaalde finaliteit binnen de onderscheiden veiligheidsopdrachten.
Bij deze oefening die we allen aangaan is het dus de evenwichtskunst van het wenselijke, het haalbare, en het toelaatbare. Daartoe hebben we een Ethische Raad nodig, maar moeten we ook voor onszelf de afweging blijven maken rond kosten en baten, weze het letterlijke kosten en baten, dan wel deze van morele en deontologische aard. En bij dit alles ligt die evenwichtskunst in het verzekeren dat we als overheid een stimulerende en relevante speler blijven die niet alleen verbiedt maar ook een gepast onderzoeks- en investeringsklimaat aanlevert, zonder evenwel de ethische aspecten uit het oog te verliezen.

We bevinden ons grotendeels op braakliggend terrein. Ook dat heeft voor- en nadelen. We hebben geen last van remmende voorsprong, maar we hebben evenmin brede ervaring waarop we kunnen terugvallen in geval van twijfel. Daarom verdient het aanbeveling om klein te starten, met duidelijk omschreven proeftuinen.

Hierbij zal ook de vraag moeten gesteld worden of binnen bepaalde proeftuinen en projecten geen bijzonder juridisch regime moet worden voorzien waarbij bepaalde uitzonderingen kunnen worden voorzien op voorwaarde dat deze duidelijk zijn omschreven, proportioneel zijn in het licht van het doel, en het toezicht erop gepast en voldoende is. Dit is een open vraag, maar een die niet uit de weg mag worden gegaan, net zo min als andere "taboevragen" die het debat kunnen doden nog voor het wordt opgestart. En dit debat willen we met u aangaan. Na dit themanummer zullen disruptie en innovatie terugkerende items zijn, op basis van de interactie die hierover met u in dit nummer wordt ingezet.

Hebt u nog andere ideeën of een mogelijke oplossing voor een bepaald probleem in het kader van innovatie en disruptie binnen de overheidssector? Verstuur uw suggesties naar onze e-ideeënbus DisGover@ibz.fgov.be

Colofon
Abonnement en redactieadres: FOD Binnenlandse Zaken, Algemene Directie Veiligheid en Preventie, Waterloolaan 76, 1000 Brussel, 02 557 35 98 **Verantwoordelijke uitgever:** Philip Willekens, directeur-generaal Veiligheid en Preventie, Waterloolaan 76, 1000 Brussel **Teksten en realisatie:** Wolters Kluwer **Redactieraad:** Caroline Atas, Patrick Barbé, Bianca Boeckx, Claudia De Maesschalck, Matthias Finet, Johan Geldhof, Thomas Gijs, Mathieu Kasiers, Christian Nicolet, Eric Valerio, Bea Vossen, Gaetan Willems www.besafe.be