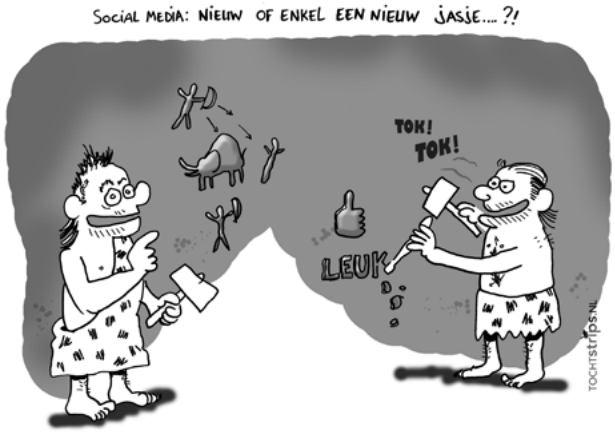
11 Nog meer veranderingen?

Wat kunnen we in de toekomst nog aan nieuwe ontwikkelingen verwachten? In dit laatste hoofdstuk schetsen zes ervaringsdeskundigen, Tony Bosma, Rick de Haan, Roy Johannink, Marco Leeuwerink, Jocko Rensen en Arnout de Vries een aantal ontwikkelingen die mogelijk een positief of negatief effect kunnen hebben op het veiligheidsdomein en van invloed zijn voor de wijze en de vorm waarop sociale media de komende jaren een rol spelen. Bedenk wat de geschetste ontwikkelingen voor de eigen organisatie (gaan) betekenen? Is het een voordeel? Is het een nadeel? En hoe gaan we daar mee om?



11.1 Meer online en mobiele informatie

Via sociale media kunnen gebruikers online of mobiel informatie delen in een sociale omgeving. Hierdoor ontstaat een conversatie. We blijven online en mobiele informatie met elkaar delen. We delen al veel aan informatie, maar de grenzen zijn daarin nog niet opgezocht. Meer gedeelde informatie betekent ook meer zorgen over de waarheid. Om het effect van enkele of verzamelde berichten beter op hun waarde te kunnen schatten of te kunnen toepassen, zullen overheden nieuwe systemen ontwikkelen waarmee ze berichten op sociale media beter kunnen taxeren op impact, waarheid en actualiteit. Systemen als Veri.ly (http://veri.ly) worden verder doorontwikkeld om beter te weten hoe te handelen. Want met een groeiende brij aan data (tot meerdere zetabytes) wordt het steeds lastiger om feiten van fictie en verleden van heden te onderscheiden. Niet alleen gaan criminelen data gebruiken om rookgordijnen op te werpen, ook een argeloze burger kan (on)bedoeld zand in de ogen strooien. Hoe meer informatie zij delen, hoe lastiger het wordt deze te duiden. Desalniettemin neem je deze informatie tot je

en geef je daar vervolgens een eigen interpretatie aan. Het maakt niet uit of hij/zij live aanwezig of thuis via een second screen deze extra informatielaag benut. Iedereen heeft een eigen virtuele informatielaag over hetgeen hij of zij waarneemt. Wie controleert of bepaalt deze laag? Burgers informeren elkaar. De media heeft een eigen rol en het bedrijfsleven wil geld verdienen. En waar is de overheid in dit plaatje?

11.2 Meer emotie in de informatie

Er zijn nog andere mogelijkheden als het gaat om het delen van informatie. Denk dan niet alleen aan de locatie waar je bent, maar ook het gevoel dat je op dat moment hebt. Facebook vraag dit inmiddels ook al; waar ben je, hoe voel je je en met wie ben je? Het delen van emoties zal een nieuwe dimensie geven aan de sociale digitale contacten waarbij we niet alleen met elkaar delen waar we zijn *(Foursquare)*, met wie we zijn en wat we doen? Ook ons 'zijn', met al onze motivaties, verlangens, irritaties, vreugde en walging worden als het ware hier gemixt. Daaruit ontstaat een hele rijke vorm van (nieuwe) informatie en communicatie die voor diverse veiligheidsprofessionals (communicatie, *intelligence*, opsporing, handhaving, preventie, hulpverlening) van onschatbare waarde kan zijn. Doordat je elkaar beter begrijpt (en onderliggende behoeftes en gedragsintenties kunt inschatten) kun je elkaar beter helpen, te woord staan, samenwerken, iets leren, vinden en bedanken.

11.3 Meer snelheid: realtime video

Is in Nederland anno 2014 nog maar net in een paar gebieden het supersnelle datanetwerk 4G uitgerold, in Zuid-Korea wordt nu al geïnvesteerd in een 5G netwerk. Uiterlijk 2020 ligt er een netwerk dat zó snel is, dat een speelfilm binnen een enkele seconde kan worden gedownload. Geen YouTube filmpjes uploaden meer, maar *streaming* (TV) kanalen zien vanaf elke bril of telefoon. En wat als er honderd filmpjes tegelijkertijd voorbij komen? Hoe scheid je dan nog het kaf van het koren? Het gevolg van al die video's en *streamings* is dat mensen live kunnen meekijken met crisis. Beeldvorming wordt *realtime* bepaald. Uitleg door overheid lijkt misschien overbodig, maar wordt eigenlijk des te belangrijker. Want wat ziet men nu eigenlijk? Wat is waar, maar nog belangrijker: wat niet?

11.4 Nieuwe (besloten) sociale omgevingen komen en gaan

Er komen steeds nieuwe platformen bij waar ook meer zal worden gedeeld. Nieuwe platforms waar beslotenheid de norm zal zijn, omdat men door het internet meer details inclusief emoties met elkaar kan delen. De kans is ook groot dat we meer gaan differentiëren. Platforms komen en gaan, maar bepaalde

platforms blijven zeker bestaan. Ook het bloggen en wiki's blijft. Het microbloggen zoals Twitter, het chatten of instant messaging - via Whatsapp of Telegram - zullen hun toepassing behouden in een bepaalde (veiligheids)context. Wat wel gaat veranderen, is de openheid van alle netwerken. Altimeter, een groot Amerikaans onderzoeksbureau, verwachtte eind 2013 dat de toekomst van sociale netwerken vooral gesloten zal zijn. Ze kregen gelijk met WeChat, Snapchat en Tango. Voor overheden betekent dit extra moeite doen om deel te kunnen blijven nemen aan die netwerken en om relevante informatie en de dialoog te blijven opzoeken.

11.5 Intensievere netwerken

Ondanks de besloten netwerken zullen bedrijven, burgers en overheden meer samenwerken. Transparantie en privacy krijgen een nieuwe balans. Burgers en bedrijven krijgen als collectief steeds meer middelen in handen om zelf hun veiligheid te organiseren. De overheid krijgt daarentegen een kleinere, maar wel een essentiële rol. Lessen uit andere delen van het land en de wereld worden beter gedeeld in open en besloten netwerkstructuren van professionals en amateurs. Het bedrijfsleven, de wetenschap en de overheid zijn veel meer met elkaar verweven en multidisciplinair aanwezig in allerlei kruisverbanden. Dit is ook harde noodzaak in een steeds complexer wordende samenleving.

11.6 Van lokaal naar globaal

De gelegenheid maakt de dief, dat geldt ook in de toekomst. Alleen zullen die dieven niet per se meer uit de je directe omgeving komen. Cybercrime leert ons dat diefstallen online letterlijk vanuit de hele wereld kunnen gebeuren. Omdat ons leven zich meer en meer digitaal afspeelt en we voortdurend online zijn, kan dit online 'open raam' dat traditioneel de gelegenheid de dief maakt, nu vanuit de hele wereld worden misbruikt. Het maakt de preventie lastig, maar plaatst ook de opsporing en vervolging voor een grote uitdaging. Want hoe vang je een dief die in Singapore woont en slechts virtueel in Nederland aanwezig was? Of misschien nog lastiger: hij pleegt zijn diefstal in een ander land, omdat hier toevallig de software fysiek staat waar een argeloze Nederlander mee te maken krijgt? De verplaatsing van lokaal naar globaal zal ook voor de openbare orde gevolgen hebben. Via een initiatief als Crowdvoice (www.crowdvoice.org) kan iedereen *realtime* wereldwijd meedoen aan protesten. We volgen op deze wijze wereldwijd de meningen van anderen en hechten daar ook steeds meer waarde aan. Nederlandse protestgangers kunnen hierdoor in andere landen voor problemen zorgen en omgekeerd. Daarnaast is het vertrouwen in de klassieke autoriteit (de overheid) die de verbinding met de samenleving lijkt te zijn kwijtgeraakt, ook nog nooit zo laag geweest. Netwerken als Crowdvoice leiden ertoe dat mensen steeds meer zelf de regie nemen en we weten inmiddels waar dat toe leidt. De Arabische landen kunnen hier sinds een paar jaar over meepraten.

11.7 Collaborative Safety

Collaborative Economy oftewel de deeleconomie, is enorm in opkomst. Bij de deeleconomie draait het om gedeeld bezit. Voorbeelden hiervan zijn: Zipcar (gedeeld autobezit), 99Dress (jurken huren van particulieren) en Peerby (spullen lenen van je buren). De deeleconomie draait om een 'gelegenheids-wij', een term die een groep trendwatchers introduceerde in hun trendrede 2013. Een gelegenheids-wij is een groep mensen die wordt verenigd door één gezamenlijk(e) doel of drijfveer. De ene keer gaat het om een groepskorting voor een theatervoorstelling via voordeelcoupons van Groupon, de andere keer om een persoonlijk voordeel zoals Broodfonds, een fonds dat een alternatieve verzekering biedt aan zelfstandige professionals. De groepssamenstelling kan variëren. Deze op het eerste gezicht onlogische lijkende verbanden of netwerken zullen steeds vaker worden geformeerd in de maatschappij, tenminste zolang er een collectief nut of noodzaak mee te behalen valt. Nut en noodzaak gaan ook rond het thema veiligheid ontstaan. Sterker nog: dit bestaat al. Buurtwachten en buurtpreventieteams zijn vaak al gelegenheids-wij's. Door internet zal dit alleen nog maar eenvoudiger worden. Mensen vinden elkaar al via Whatsapp- en Facebookgroepen. Wanneer de onveiligheid of het onveiligheidsgevoel in een wijk over een bepaald thema groot genoeg is, zijn mensen sneller bereid een steentje bij te dragen. Zo werd de succesvolle dienst Airbnb, waar burgers over de hele wereld een *bed & breakfast* kunnen aanbieden, ingezet bij orkaan Sandy om mensen gratis van onderdak te voorzien. Maar het gaat verder via fysieke maatregelen, waarbij iedereen straks een drone kan kopen om een brand in huis te blussen. Maar ook virtuele hand- en spandiensten, van surveilleren tot online beveiligingscamera's bekijken of bewakingsdrones bedienen, de leden van de gelegenheids-wij kunnen en zullen hiermee aan hun eigen veiligheid bijdragen. We kunnen niet meer langer om *collaborative safety* heen. De minder positieve kant van de medaille zou kunnen zijn dat burgers die zelf het heft in eigen handen nemen op het gebied van veiligheid, de kans lopen onschuldige mensen aan te wijzen of digitaal aan de schandpaal te nagelen. Want burgers zullen zelf (overheids)data hergebruiken (zie http://bestwelsnel.nl), maar dat betekent niet dat zij altijd de juiste vaardigheid of kennis hebben om deze data op een adequate manier te interpreteren. Het collectieve belang zal immers groter zijn dan het individuele belang.

11.8 Grote conversaties: de wereld doet steeds meer mee

Het klein houden van incidenten was altijd al moeilijk. De netwerksamenleving groeit echter door. Iedereen kent wel iemand die zich op de plaats incident bevindt of anderzijds betrokken is. Verder wordt het allemaal internationaler, waarbij sociale media tijdslijnen automatisch of door de *crowd* worden vertaald en verder geleid. Steeds vaker zijn dat beelden die voor zich spreken. De wijk is de wereld geworden en de wereld de wijk. Dat wat vanmiddag aan de andere kant van de

wereld gebeurt, is het gesprek van de dag aan de eetkamertafel. Het vroegere fotomomentje, het plaatje dat je kon vertellen vanuit een stilstaand perspectief, is niet meer. De wereld beweegt sneller dan voorheen en de foto is een livestream geworden, waarvan niet altijd een 'uitzending gemist' beschikbaar zal zijn. Dit beïnvloedt ook het onderzoeken van incidenten en ervaringen. Onderzoek zal het omgaan met veranderende werkelijkheden moeten gaan verwerken. En hoe ga je om met de collectieve intelligentie en collectieve besluitvorming?

11.9 Meer invloed: de gebruiker bepaalt steeds meer

De wereld gaat steeds sneller, techniek en adoptie ervan lopen in snel tempo uit elkaar. De overname van Whatsapp door Facebook heeft in sneltreinvaart ertoe geleid dat een nieuwe app werd geïntroduceerd, 'Telegram'. Dit zijn onvoorspelbare en grillige ontwikkelingen, omdat de groepsdynamiek in de moderne maatschappij snel is. Heb je net een Whatsapp-buurtgroep opgestart om elkaar te alerteren, is de rest van de wereld bezig met Telegram. De vraag is dan ook hoe een nationaal opererende organisatie hierop inspeelt als door het hele land inmiddels verschillende diensten worden gebruikt. Het verschil in ontwikkelingstempo van mens (gebruiker) en techniek wordt alleen maar groter. Dit leidt tot een grotere kloof in de maatschappij zelf en met de overheid.
Er zijn grote maatschappelijke reacties mogelijk als de (informele) afspraak met de gebruiker van bijvoorbeeld een app wordt geschonden. Ontwikkelingen die gebeuren binnen de macht van marketingreuzen. Hyves is overgenomen door de Telegraaf-groep en vervolgens verdwenen. Whatsapp is overgenomen door Facebook en de eerste opzeggingen in het gebruik ervan steken al de kop op. Burgers realiseren zich dat hun data geld waard is. De burger wil de baas zijn over zijn eigen bytes. Het businessmodel van het verkopen van de data die gemerkt en ongemerkt produceren, wordt deels omgedraaid . De burger krijgt meer invloed en controle en neemt op gebied van veiligheid ook steeds meer het heft in eigen handen. De gebruiker bepaalt steeds meer en wil ook steeds minder bemoeienis van of meekijken door de overheid.

11.10 Meer mogelijkheden voor organisaties

Sociale media ontwikkelen zich ook als (extra) signaleringskanaal waarin patronen kenbaar worden omdat emoties zich opbouwen, gedragspatronen uit berichten zichtbaar worden en cyberpesten, radicalisering of uitbarstingen en protesten vroegtijdig worden gesignaleerd. De gevoelstemperatuur van de maatschappij als collectief wordt vanaf de buitenkant zichtbaarder en beter voorspelbaar. Niet per individu, omdat hiervoor betere privacyregels zijn ingesteld. Als de druk (lees: onveiligheid) op bepaalde plekken op de digitale snelweg te hoog wordt, kan een intensievere samenwerking met bedrijven en burgers ontstaan. Dit alles biedt kansen voor preparatie en preventie en zorgt voor nieuwe mogelijkheden

om eerder in te grijpen. Voorspellende modellen bieden echter nog steeds geen garantie: menselijk gedrag blijft nu eenmaal onvoorspelbaar. Maar vroegtijdige en *realtime* inzichten bieden mogelijkheden om niet te gaan wachten op het uitkomsten van een voorspelling. Dit tijdige handelen stelt tegelijkertijd nog hogere eisen aan een organisatie die zich snel en flexibel moet aanpassen (*lean & mean*).

11.11 Privacy: wel of niet opzij zetten

Het privacybelang wordt steeds vaker ondergeschikt gemaakt aan het algemene of persoonlijke nut: door media en maatschappij. Of dit terecht is bepaalt de rechter. Juist op momenten van incidenten en crises zetten mensen graag hun privacy aan de kant voor de goede zaak. Sommige gebruikers zetten hun locatie aan en filmen er op los. Zij schuwen daarnaast niet om man en paard te benoemen en dit ook nog eens op allerlei manieren te duiden. Thuiszitters krijgen dit alles ongefilterd via hun netwerk keihard en rauw binnen, terwijl ramptoeristen als bijen op de honing afkomen. Er zijn gelukkig ook ontwikkelingen waarbij het privacybelang uitgaat boven het belang van veiligheid. Zo bepaalde het Europese Hof op 8 april 2014 dat de huidige bewaarplicht voor telefoon- en mailverkeer inbreuk maakt op de fundamentele rechten van Europese burgers. Maar aan de andere kant mogen nu wel drones worden ingezet en krijgen inlichtingendiensten misschien zelfs meer bevoegdheden. De maatschappij zal dus ook de komende decennia constant in beweging zijn om haar balans te vinden tussen privacy en veiligheid.

11.12 Meer risicovermijding

We accepteren steeds minder risico's in onze maatschappij. De veiligheid mag dan verbeteren, het veiligheidsgevoel neemt niet echt toe. We willen steeds meer door het nemen van allerlei maatregelen (zelfs kleine) risico's uitsluiten en zien de technologische ontwikkeling als oplossing daarvoor. Dat dit ten koste gaat van gemak of het individu nemen we op de koop toe. We organiseren onze veiligheid op de uitzondering, niet op de regel. Voorkomen is het devies. Slimme camera's gaan agressie opmerken, nog voordat de agressie überhaupt plaatsvindt. Overal hangen camera's en vliegen drones in het rond die alles in ons leven vastleggen, zodat elke misdaad op beeld staat. Doordat mensen in verbinding staan met het internet, weten we altijd wie waar en wanneer is. En gaat er dan toch iets fout, dan moet de onderste steen boven komen om te zorgen dat die steen nooit meer onderop komt te liggen. Een risicovrije maatschappij, kan dat wel?

11.13 Nieuwe soorten van criminaliteit

De criminaliteit is door de jaren heen veranderd. Dit zal de komende jaren alleen nog maar meer veranderen. Met de technologische ontwikkelingen als grote drijver verandert niet alleen de maatschappij. De afgelopen jaren is cybercrime erg in opkomst. Cybercrime kan het best worden omschreven als criminaliteit met technologie als middel en als doel. Meer technologie in onze maatschappij kan dus betekenen meer criminaliteit, maar juist de massale adoptie ervan betekent dat het verschuift van technologisch middel naar een sociaal middel, waarmee bijzonder veel narigheid kan worden uitgehaald. En met de adoptie van '*internet of things*' in opkomst wordt dit nog veelomvattender, omdat een netwerk van dingen tot en met de huiskamer inclusief je eigen lijf via het internet verbonden zijn aan elkaar. Een koelkast die zelf een bestelling doet bij een online supermarkt als de melk (bijna) op is. Niet alleen dingen zullen in de toekomst met elkaar verbonden zijn, ook mensen zullen met elkaar en met dingen verbonden worden. De FBI noemt cybercrime één van de grootste bedreigingen van onze maatschappij. Misschien hebben ze daar gelijk in, maar er komt meer aan. Een echt gevaar voor onze maatschappij gaat gevormd worden door biocrime. Biocrime zijn misdaden die worden gepleegd met een mens als middel of doel. Als je denkt: 'dit is wel heel erg ver van mijn bed', de eerste hack van een pacemaker met dodelijke afloop is reeds op afstand gepleegd. Drie redenen maken dat biocrime nog meer impact gaat hebben op onze maatschappij. Ten eerste zijn steeds meer mensen verbonden met netwerken, via onder andere medische toepassingen (zoals een ingebouwde insulinepomp die op afstand je dokter informeert over je gezondheid). Ten tweede zal ons lichaam steeds meer robotonderdelen krijgen. Een zelfdenkend kunsthart, een 3D geprinte kunstheup of een microscopisch oog. Niet alleen vanuit medische overwegingen, ook esthetisch of puur ter verbetering wordt het toegepast. Ten derde willen we steeds meer aan onze DNA veranderen. Op dit moment is in Amerika al een doe-het-zelf DNA-analyse kit (23andme) beschikbaar. Voor 99 dollar heb je al zo'n kit in huis. Al deze ontwikkelingen maken biocrime steeds aantrekkelijker voor criminelen. Je breekt letterlijk bij iemand in of dreigt ermee. Het is niet alleen een middel om iemand te doden, maar ook om iemand onder controle te krijgen. Waarom de identiteit van iemand stelen, als je die persoon gewoon kan manipuleren om een bank te beroven?

11.14 Nieuwe wetgeving noodzakelijk?

Met de steeds sneller wordende technologische ontwikkelingen neemt de druk op wetgeving alleen nog maar verder toe. Wij zien het aan de zelfrijdende auto's: niet de technologie, maar de wetgeving is de reden dat deze 'pas' rond 2020 in onze maatschappij te zien zijn. De wetgever bepaalt immers dat er iemand achter het stuur zit, let wel: met zijn handen aan dat stuur. En mag je eigenlijk wel rijden met Google Glass op? Met één oog gericht op het internet ben je minder bezig met de verkeersveiligheid. Terwijl de makers van zelfrijdende auto's juist claimen

veel veiliger te zijn dan met een mens achter het stuur. Wat wordt het verschil tussen mens en machine op gebied van veiligheid? Volgens voorspellingen zijn rond 2017 machines (of robots) slimmer dan mensen. Betekent dit als robotten fouten maken, ze wettelijk aansprakelijk kunnen worden gesteld? Wat als ze zelfdenkend zijn, volgens de laatste kunstmatige intelligentie, kun je dan wel de eigenaar of de maker verantwoordelijk houden? Over kunstmatige intelligentie gesproken, wat te denken als deze intelligente software wordt gebruikt om recht te spreken? Anno 2014 zijn er al softwaresystemen in gebruik die rechters in Amerika helpen om tot een vonnis te komen. Zijn rechters straks overbodig? Of worden wetten door kunstmatige intelligentie gemaakt, dus een Wetgevingsrobot of een Rechtspraakrobot? En welk effect heeft 3D- of 4D-printing op auteursrecht en intellectueel eigendom? Letterlijk alles kan immers met één druk op de knop worden nagemaakt. Wetgeving heeft de komende jaren in ieder geval een uitdagende klus. Zeker met de aanstaande (commerciële) ruimtereizen in het verschiet; welke regels gelden in de ruimte?

Tijd voor discussie!
Wat is er nodig om in het veiligheidsdomein om te gaan met al deze veranderingen? We hopen in elk geval dat deze handreiking een discussie op gang brengt over hoe we met elkaar blijvend aandacht kunnen geven aan en inspelen op deze veranderingen.