tekst en foto's: Wim de Goeij

We leven en werken allemaal in de Cyber Age. Internettechnologie is een absolute blijver. Als straks met 5G het internet of things losgaat, is zo'n beetje alles aan elkaar verbonden. Dat betekent nieuwe gemakken, maar ook nieuwe problemen. Zoals cybercriminaliteit, cyberterrorisme, cyberactivisme, cyberspionage en zelfs cyberoorlog. Het bestrijden daarvan was het onderwerp van 'Vechten voor veiligheid in de Cyber Age', een themadag van FNV Veiligheid, het samenwerkingsverband van de NPB, defensiebond AFMP en de Marechausseevereniging.

Cyberbewustzijn moet snel omhoog

NPB-voorzitter Jan Struijs was ook aanwezig op de themadag. 'Zo'n dag als deze helpt om het bewustzijn over de digitale wereld te vergroten. En dat is hard nodig,' stelde hij. 'De digitale vaardigheden van politiemensen moeten naar een hoger niveau. Als politieman of -vrouw moet je ook op het gebied van cyber security weten wat er speelt en wat je te doen staat. Mijn ervaring is dat politiemensen wel willen, het thema leeft zeker, maar dat we te maken hebben met achterstallig onderhoud op dit gebied.'

Volgens Struijs zijn de middelen vaak verouderd en is de parate kennis meestal te laag of zelfs ruim onvoldoende. 'De NPB zal er bij de werkgever op blijven aandringen dat de Nationale Politie op dit gebied orde op zaken stelt. Daarbij is volgens ons kleine stapjes maken niet meer genoeg. Daarvoor gaan de ontwikkelingen te snel. Dus meer techniek en meer scholing. En om te beginnen een veel hoger bewustzijn van de noodzakelijke bescherming van burgers als het gaat om zaken waar het woord cyber aan vast zit. Deze themadag is een mooie aanzet. Nu moeten we doorpakken.'

TIEN MINUTEN GEEN INTERNET

Pieter-Jaap Aalbersberg, de huidige Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), was de eerste spreker op de goed bezochte themadag in Utrecht. Hij sprak uit de betrokkenheid bij het onderwerp van onder andere de aanwezige politiemensen te waarderen. Ook volgens Aalbersberg is een veel groter bewustzijn van digitale criminaliteit dringend noodzakelijk. 'De dreiging van cybercrime is veel omvangrijker dan men denkt. Amsterdam kan tot wel 24 uur zonder stroom, maar tien minuten geen internet ontwricht de samenleving. Dan komt er al veel tot stilstand. En zo zijn er nog veel meer voorbeelden te geven.' Dat realiseert men zich in Nederland nog onvoldoende en daarom stelde Aalbersberg de volgende vragen: 'Hoe kunnen we Nederland maatschappelijk en economische veilig houden? Hoe kunnen we onze weerbaarheid vergroten? Hoe bestrijden we cybercrime als politie, leger en marechaussee?'

Zeven jaar lang was hij als eenheidschef het gezicht van de Amsterdamse politie: Pieter-Jaap Aalbersberg. Na de ramp met de MH17 in 2014 leidde hij de repatriëringsmissie. Nu is hij de NTVC op het ministerie van J&V.

NIEUWE KWETSBAARHEID

Nederland op digitaal gebied veilig houden vraagt verregaande samenwerking tussen met name overheden en bedrijfsleven en overheden onderling. De NCTV levert op nationaal niveau een coördinerende bijdrage en zorgt voor de *cyber-security-agenda*. Aalbersberg verwees naar zijn jongste rapport (zie website nctv.nl): 'We zijn in de nieuwe kwetsbaarheid gerold. Steeds meer sectoren zijn aan elkaar verbonden en de afhankelijkheid van internettechnologie blijft toenemen. Ontwrichting van de maatschappij ligt op de loer en we moeten dus doordenken over hoe we dat kunnen voorkomen.'

Dat hierbij een grote rol weggelegd is voor de politie, mag duidelijk zijn. Aalbersberg: 'Traditionele criminaliteit is verschoven naar het digitale domein. En dat betekent dat we niet meer zonder slimme it'ers als specialisten in de bestrijding van cybercrime kunnen, maar ook dat jong en oud bij de politie op dit gebied moeten bijblijven. Makkelijk is dat niet, maar de digitale veiligheid vraagt dit wel van de politieman of -vrouw in het veld. We kunnen er niet meer onderuit. We hebben zelfs een inhaalslag maken.'

INVESTEREN

Aalbersberg maande zijn voormalige collega's in het politievak daarom op de hoogte te blijven van de kansen en bedreigingen in de digitale wereld. 'Het is een permanent proces. Cybercriminelen zoeken altijd naar het zwakste punt om geld te maken of de samenleving te ontwrichten. Daar investeren ze in. Wij investeren ook, onder andere in het verkrijgen van informatie. Misschien is dat wel een nieuw fenomeen in ons vak. Daar liggen in ieder geval kansen bij de bestrijding van cybercrime. Bijvoorbeeld via artificial intelligence, zelfdenkende computers. Hoe doen we dat op een transparante en ethisch verantwoorde manier? Daarop zal ook de politie een antwoord moeten vinden.'

Bewustwording, weerbaarheid, bijblijven en intensieve samenwerking zijn een paar woorden die bleven hangen na het cyberverhaal van Pieter-Jaap Aalbersberg. Hij stelt tot slot de uitdaging vast: 'Zijn wij voorbereid, en als er wat gebeurt, zijn wij dan in staat om de burger te helpen? Bereid je daar goed op voor, ook via deze themadag.'

Dagvoorzitter Frank Kuiper (rechts, in het dagelijks leven NPB-eenheidsbestuurder) introduceert drie van de vier workshop-sprekers: luitenant-kolonel Edwin Noordzij (KMar), financieel rechercheur Daniel Leon en analist Erik Kroon (Nationale Politie)

De vierde workshop-spreker was ritmeester Jelle van Haaster, de bouwer van een prijswinnende app voor het gebruik van social media tijdens militaire missies.

Vier workshops

Om de deelnemers meer inzicht te geven in specifieke cyberthema's had FNV Veiligheid vier workshops in de aanbieding. Ritmeester Jelle van Haaster besprak het nut van militaire cyberoperaties in conflictgebieden – het onderwerp van zijn promotieonderzoek. Financieel rechercheur Daniel Leon vertelde hoe fenomenen als Bitcoin en Blockchain werken, hoe criminelen daar ge- en misbruik van maken en waar de kansen en uitdagingen voor de opsporing liggen. Luitenant-kolonel Edwin Noordzij van de KMar nam de deelnemers mee naar de virtuele wereld van het dark web: een plek op internet waar je niet kunt komen met zoekmachines als Google, maar waar je met een simpele muisklik illegale zaken kunt kopen. Anoniem! Of toch niet? Analist Erik Kroon zette uiteen hoe de Landelijke Recherche erin geslaagd was één van de grootste dark web-markten – Hansa Market – te infiltreren en neer te halen.

Deze informatieve presentaties maakten in ieder geval duidelijk dat digitale bedreigingen in de handen van het Openbaar Ministerie, de politie, de Marechaussee en het leger ook digitale kansen kunnen zijn. Er zijn genoeg mogelijkheden om de mens achter de cybercriminaliteit aan te pakken. We zijn niet kansloos, maar er moet wel veel voor gedaan worden. Er zijn specialisten voor nodig en vooral veel intensieve samenwerking tussen tal van diensten. Maar het kan. Ook cybercriminelen maken fouten.

De missie van historicus en datajournalist Dimitri Tokmetzis is mensen inlichten over de technologie die ons leven bepaalt. Dat deed hij onder andere in het boek De Digitale Schaduw, een waarschuwing voor de gevaren van een oncontroleerbare digitale identiteit.

WAKE-UP CALL

De laatste lezing van de dag werd gegeven door Dimitri Tokmetzis, historicus en datajournalist, onder andere voor De Correspondent. Hij is co-auteur van het boek 'Je hebt wél iets te verbergen: over het levensbelang van privacy'. Aan het eind van de dag kreeg iedereen dat boek mee naar huis. In het streven naar meer bewustwording was dat een perfecte zet van de NPB, want de lezer zal toch menigmaal moeten vaststellen dat de digitale wereld nóg verontrustender is dan gedacht. Het boek is een absolute aanrader voor wie wakker geschud wil worden over wat digitaal allemaal mogelijk is en wel of niet gewenst is. De schrijvers bieden geen oplossing, maar stellen vast. Ze geven de situaties bij overheden, commerciële partijen en cybercriminelen weer. Ter informatie. Eén ding is duidelijk: de cyberwereld blijft en zal hard blijven groeien.

Onderzoeksjournalist Tokmetzis is een bijtertje, zo werd duidelijk in zijn betoog, waarin hij ook vertelde wat er met internettechnologie allemaal aan moois mogelijk is. Maar je zou niet alles moeten willen doen, is een van zijn conclusies. Zeker niet als je politieman of -vrouw, marechaussee of militair bent. Dan ben je extra digitaal en fysiek kwetsbaar voor kwaadwillenden. Denk bijvoorbeeld na over welke apps je gebruikt en waar je zo'n app (of smartphone) toestemming voor geeft. Weet in ieder geval dat je héél veel sporen nalaat via de digitale wereld.

DE FITNESS-APP POLAR

Tokmetzis wist het publiek te boeien met een uitgebreid en spannend verslag over hoe de op zich onschuldige, en voor hardlopers zeker nuttige, fitness-app Polar kon uitgroeien tot een groot veiligheidsprobleem voor mensen die bezig zijn met het bewaken van de veiligheid van burgers en van ons land als geheel. Tot vorig jaar kon iedereen met deze app de namen en adressen achterhalen van duizenden militairen en geheim agenten! Uhh...? Dat kan toch niet? Wel dus en Tokmetzis legde uit hoe dit allemaal – legaal – te doen was. Zijn journalistieke team was te goeder trouw. Ze waren uit op onthulling en voorkoming van ellende als gevolg van onzorgvuldige generatie en zichtbaar maken van data. Maar criminelen, met een geheel andere agenda, kunnen dit ook. En als ze het zelf niet kunnen, dan huren ze eenvoudig via het dark web slimme it'ers in. Keuze genoeg!

De grote hoeveelheid aanmeldingen had al duidelijk gemaakt dat er veel belangstelling was voor een themadag met volop cybercrime stories. Toen Sven Schuitema, de voorzitter van de Marechausseevereniging, de dag opende, zat de zaal dan ook helemaal vol.

Het kostte heel wat moeite, mensen en overheidsinstanties om de bouwer van de app te bewegen al die min of meer vrij toegankelijke data van het internet te verwijderen. Lees daarover de verhalen op de website van de correspondent, onder *project polar.* Daar is ook informatie te vinden over hoe je jouw privacy kunt beschermen in andere fitness-apps. Uit de reacties van de deelnemers aan de themadag bleek dat het Polar-app-verhaal het bewustzijn van gebruikers van deze app flink groter had gemaakt. In zover was het dus een geslaagd evenement te noemen. Nu nog de rest van de overheidsdienaren bij de Marechaussee, defensie en politie.

POLITIE SAMENWERKEN MET EXTERNEN

Tokszmetzis besloot met een tip voor de Nationale Politie: 'Misschien moet de politie meer samenwerken met externen. De cyberwereld is zo complex dat meer kennis nodig is. Gebruik deskundigen – journalisten bijvoorbeeld.' Zo'n samenwerking geeft inderdaad meer kansen op effectieve bestrijding van cybercrime en andere cybertermen. Want de digitale wereld is niet alleen een bedreiging. Het kent vele mooie en nuttige toepassingen EN biedt de nodige kansen om kwaadwillenden aan te pakken. Het is en blijft echter vechten voor veiligheid in de Cyber Age. ■

'Helaas is het digitale bewustzijn van politiemensen vaak zo laag dat bijvoorbeeld burgers die aan de balie komen met een probleem inzake cybercriminaliteit zich niet goed geholpen voelen. Het kan ook zijn dat belangrijk digitaal bewijsmateriaal niet of onvoldoende wordt veiliggesteld. Dat moet beter kunnen. De *cyber awareness* bij de politie moet echt omhoog!'

NPB-voorzitter Jan Struijs