Desinformatie, manipulatie en destabilisatie uitdagingen voor defensie

Bij hybride oorlogsvoering probeert de vijand politieke processen te beïnvloeden, netwerken te infiltreren of plat te leggen of nepnieuws te verspreiden (bron: ministerie van Defensie).

[tekst] **Ing. Marjolein de Wit-Blok**

Er is in Nederland véél kennis aanwezig met betrekking tot technieken en technologieën waarmee 'desinformatie' is te herkennen en de betrouwbaarheid van het uitwisselen van informatie te maximaliseren. Tijdens het Kooy Symposium dit voorjaar gingen zestien sprekers in op de thema's desinformatie, manipulatie en destabilisatie. Dit symposium, de belangrijkste activiteit van de KIVI afdeling Defensie & Veiligheid, wordt jaarlijks georganiseerd om de Nederlandse technologie op dit gebied te stimuleren en op de kaart te zetten. Een verslag over hybride oorlogsvoering, gaming, cybersecurity en blockchain.

Vanuit Defensie zijn oplossingen om desinformatie te kunnen herkennen onder meer belangrijk in het kader van hybride oorlogsvoering. Kol. Drs. Peter de Boer: "Wanneer de dreiging militair van aard is, is voor iedereen duidelijk wat de rol van defensie is. Wanneer andere opponenten worden aangewend met behulp van verschillende instrumenten, dan spreken we over hybride dreiging. In Nederland hanteren we de definitie: conflictvoering tussen staten, grotendeels onder het juridisch niveau van openlijk gewapend conflict, met geïntegreerd gebruik van middelen en actoren, met als doel bepaalde strategische doelstellingen te bereiken. Met hybride oorlogsvoering

probeert de vijand bijvoorbeeld politieke processen te beïnvloeden, netwerken te infiltreren of plat te leggen of nepnieuws te verspreiden. Het doel is meestal verwarring zaaien."

Bewustwording

"Kenmerkend voor de hybride variant is vooral de inzet van verschillende middelen waarbij zowel nationaal als internationaal veel afstemming plaatsvindt over de wijze waarop we moeten reageren op dreigingen," aldus De Boer. "Daarbij lijkt consensus te bestaan dat moet worden gekozen voor een tweesporenbenadering: enerzijds is het belangrijk om weerbaar te zijn tegen hybride dreigingen, anderzijds is het van belang om de tegenstander te kennen en acties van de tegenstander te onderkennen. Voor beide sporen geldt dat bewustwording van de dreiging de eerste stap is naar een oplossing. Vervolgens moeten publieke en private partijen gezamenlijk verantwoordelijkheid nemen voor oplossingen. De benodigde technologieën zullen moeten ondersteunen bij het in kaart brengen van kwetsbaarheden, het duiden en signaleren van activiteiten en het onderzoeken van statelijke actoren. Een uitdaging voor zowel defensie, het bedrijfsleven als onderzoeksinstituten."

Rol van onderzoeksinstituten

Interessant onderzoek in het kader van desinformatie en manipulatie wordt binnen TNO uitgevoerd en richt zich op de werking van het menselijk brein. Drs. Maj. Maaike Duistermaat zegt hierover: "Het menselijk brein is een neuraal netwerk dat zich kenmerkt door onder andere een gelimiteerde capaciteit en aandacht, blinde vlekken en de neiging om verbanden te leggen. Wat dat betreft zijn onze hersenen zéker niet te vergelijken met een computer. Een groot verschil is dat alle signalen die wij binnen krijgen door middel van onze zintuigen níet of moeilijk zijn te negeren of te deleten. Een computer neemt beslissingen op basis van gegevens waarvan wij zeggen dat hij ze mag gebruiken. Dat is bij een mens niet mogelijk. Dus hoezeer wij ook denken dat we rationeel handelen op basis van feiten...: niets is minder waar."

"Deze universeel voorkomende manieren van denken en redeneren noemen we heuristieken en biases. Zij voldoen níet aan de regels van logica, kansberekeningen en rationaliteit en vinden bij vrijwel alle mensen op dezelfde manier plaats. Inmiddels zijn tientallen van deze biases vastgesteld waarvan 'kuddegedrag' een belangrijke is. Verder kennen we allemaal wel het fenomeen dat we liever de 'feiten' horen die ons gedrag of beslissingen bevestigen dan feiten die dit ondermijnen. We selecteren als het ware datgene wat voor ons als mens het gunstigst is. Deze onbewuste denkwijzen beperken in veel situaties de kwaliteit van onze beoordelingen, verklaringen en beslissingen."

Het onderzoek naar deze biases kan helpen bij het herkennen van vormen van desinformatie die mensen op het verkeerde been zetten. 'De tegenstander doorhebben' en inspelen op zijn biases. Ook voor de industrie belangrijk in het kader van bijvoorbeeld veilig handelen (bediening, onderhoud), het omgaan met problemen, het nemen van financiële beslissingen, communicatie met andere afdelingen enzovoorts.

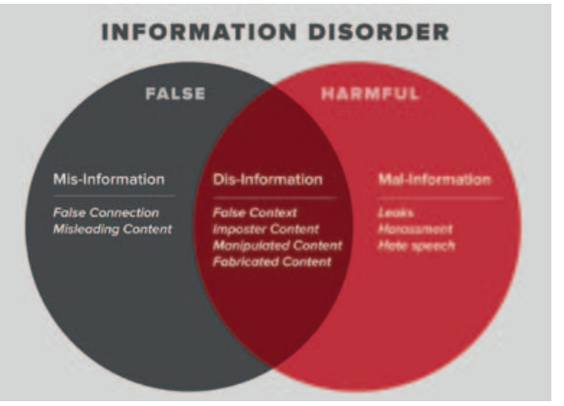
Gaming

Een andere presentatie van TNO ging over de 'games' die het onderzoeksinstituut ontwikkelt om mensen in een gesimuleerde omgeving te laten oefenen met complexe situaties. Hybride dreiging gaat immers over een gecoördineerde, complexe mix van gebeurtenissen, middelen of fenomenen met veiligheidsimplicaties. Vaak ongrijpbaar of zelfs ondefinieerbaar en dus ook niet in een PowerPoint over te brengen om vervolgens – rationeel? – de juiste beslissingen te nemen.

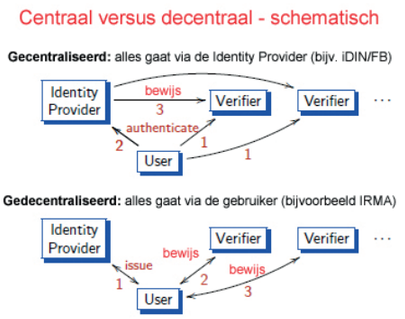
Drs. Rick Meessen: "Hybride dreiging gaat vaak samen met misleiding, ambiguïteit en ontkenning van de acties. Hierdoor worden attributie en effectieve respons bemoeilijkt. Binnen TNO is sinds 2017 het middel 'strategic gaming' toegepast op hybrid conflictvoering, met name om met de relevante actoren in Nederland een beter begrip te krijgen van de aard en effecten van hybride dreigingen en campagnes. Maar ook om te kijken hoe en waarover afgestemd moet worden om de dreigingen snel te kunnen detecteren en duiden en vervolgens de effecten te kunnen mitigeren."

Inmiddels is er een pallet van games

Het spits werd afgebeten door Kol. Drs. Peter de Boer die in 'setting the scene' aangeeft wat het belang is van technische ontwikkelingen in het kader van 'desinformatie, manipulatie en destabilisatie' (foto: Marjolein de Wit-Blok).



Desinformatie onderverdeeld in drie varianten: 'mis-informatie' is niet juist maar heeft verder geen gevolgen, desinformatie heeft wel gevolgen maar nog niet direct ernstig terwijl mal-informatie te beschouwen is als 'het kwaad' (bron: ministerie van Defensie).



IRMA heeft een decentrale architectuur waardoor attributen uitsluitend op een telefoon zijn opgeslagen en niet centraal op een computer (bron: Radboud Universiteit Nijmegen).

(zoals matrix games en dilemma games) ontwikkeld waarmee ervaring is opgedaan voor diverse hybrid conflictvoering scenario's. Het gebruik en de ontwikkeling van deze games staat nog in de kinderschoenen maar hebben inmiddels op zowel kleine als grotere schaal al bijgedragen aan het verbeteren van het bewustzijn van mensen in bepaalde situaties. Wellicht later ook bruikbaar in de industrie om mensen te trainen; bijvoorbeeld in noodsituaties op een chemische plant.

Privacy by design

Vanuit de wetenschappelijke hoek hield onder meer professor dr. Bart Jacobs, Hoogleraar computerbeveiliging van Radboud Universiteit Nijmegen, een presentatie over IRMA. Een Identity platform waarvan de afkorting staat voor: 'I Reveal My Attributes'. Daarbij is een attribuut een eigenschap zoals leeftijd, bankrekeningnummer of opleiding. Jacobs: "Wanneer je een fles whisky koopt moet je volgens de wet bewijzen dat je ouder dan 18 jaar bent. Meer dan dat hoeft de verkoper niet te weten. Via IRMA is het mogelijk om alleen dit ene aspect online via je mobiele telefoon te kunnen aantonen; de rest van je gegevens blijft geheim. Deze privacybescherming zit ingebakken in het systeem en wordt daarom ook privacy by design genoemd. In de meeste recente nationale en Europese wetgeving wordt privacy by design vereist voor nieuwe ICT-systemen. Naast intrinsieke privacybescherming biedt IRMA ook bescherming tegen identiteitsfraude: wanneer je naam of geboortedatum helemaal niet worden genoemd, zijn ze ook niet te misbruiken."

Decentrale architectuur

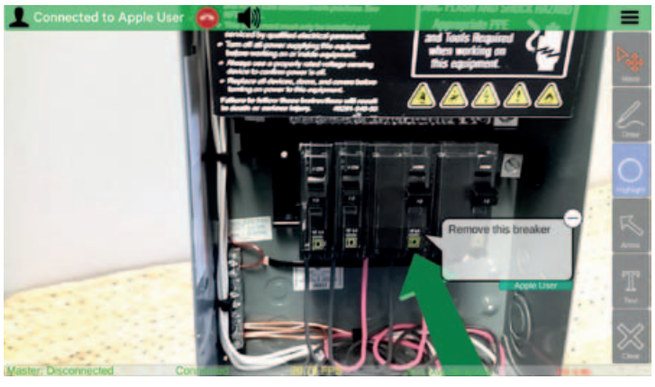
In een notendop werkt het systeem als volgt: De attributen zijn voor iedere gebruiker te downloaden naar de IRMA app op de smartphone. Zij worden uitgegeven door bijvoorbeeld een bank, nationale overheid, webshops enzovoort. De bijbehorende attributen – bijvoorbeeld leeftijd, telefoonnummer, Burgerservicenummer, IBAN en BIC – zijn hier dus reeds beschikbaar. Voordat het attribuut wordt afgegeven dient de betreffende persoon zich eerst te identificeren waarna het wordt verstrekt voorzien van een digitale handtekening. Hiermee is de echtheid en herkomst te controleren.

Het systeem wijkt af van andere systemen omdat het een decentrale architectuur heeft waardoor de attributen uitsluitend op een telefoon zijn opgeslagen en niet centraal op een computer. Hiermee is de privacy geborgd en kunnen andere partijen de gegevens niet misbruiken. Pilots lopen onder andere bij de overheid (invullen van formulieren, huishoudboekje van Utrecht), de gezondheidszorg en in samenwerking met SURF.

Simulatie cyberaanval

In de presentatie van drs. Petra Hielkema – divisiedirecteur betalingsverkeer en marktinfrastructuur bij de Nederlandsche Bank – werd een raamwerk uitgelegd dat ontwikkeld is voor het uitvoeren van geavanceerde aanvalstesten in de financiële wereld. Dit raamwerk heet TIBER wat staat voor 'threat intelligence-based ethical red teaming'. De noodzaak voor dit type testen is evident. Niet alleen worden cyberrisico's steeds prominenter en richten de aanvallers zich internationaal in toenemende mate op financiële instellingen in het hoogwaardige betalingsverkeer. Ook de kennis over aanvalstechnieken verspreidt zich mondiaal razendsnel waarbij de aanvallen steeds geavanceerder worden. Ontwikkelingen die niet alleen de financiële sector treffen maar ook andere vitale sectoren in de industrie, zoals de elektriciteitsvoorziening of telecom.

Om de gevoeligheid van de systemen voor cyberaanvallen te testen wordt gewerkt met drie teams. Na een uitgebreid overleg over het 'dreigingslandschap' en het installeren van alle mogelijkheden en middelen volgens 'de laatste stand der techniek', zal het 'aanvalsteam' aanvallen volgens vooraf besproken protocollen. Deze aanvallen zijn zeer geheim en vinden 'in het echt' plaats in de eigen systemen waar mensen mee werken. Het enige verschil is dat het aanvalsteam niet het doel heeft om schade aan te richten maar uitsluitend om te kijken hoe bestendig de systemen zijn tegen aanvallen. Wanneer de aanval niet succesvol is, dan zal een 'support' team 'een deurtje openzetten' waardoor het aanvalsteam tóch naar binnen kan. Op deze manier kan ook worden getest hoe snel indringers zijn op te merken en af te weren. En er is een team dat de instelling verdedigt en van niets weet. In november 2017 is de pilotfase afgerond en zijn de richtlijnen voor het raamwerk gepubliceerd. De testen worden nu uitgevoerd waarna de evaluatie zal uitwijzen wat nodig is om de financiële stabiliteit van Nederland en verder te waarborgen.



Met een 'augmented reality' bril zijn niet alleen personen te identificeren, maar kan ook de onderhoudswereld zijn voordeel doen (foto: Intellecture). Onderhoud aan legervoertuigen gaat volgens heel specifieke eisen (foto: Defensie/René Verleg).

Met de ruim 350 inschrijvingen was de zaal op de Gen. Maj. Kootkazerne in Stroe volledig gevuld (foto: Marjolein de Wit-Blok).

Augmented reality

Rob Frees presenteerde in zijn workshop een intelligente bril die op basis van een foto enkele tientallen gezichtskenmerken kan onthouden en hiermee de betreffende persoon kan herkennen. “In het kader van defensie een mooi hulpmiddel om vriend van vijand te kunnen onderscheiden. Ook in de industriële wereld is ‘augmented reality’ een oplossing die een bijdrage levert aan het vereenvoudigen van onderhoud. Je moet je voorstellen dat je met deze bril een soort tweede laag over de echte wereld legt. Bijvoorbeeld een technische tekening van een machine of een installatieschema van een besturingskast. Ook kun je een infrarood camera inbouwen om direct warmte gerelateerde problemen op te sporen of eenvoudig het telefoonnummer van de leverancier oproepen. De bril is een voorzichtige deeloplossing om het gebrek aan goed opgeleide technische mensen te compenseren en past bovendien bij de huidige generatie die selectiever is om vooraf kennis tot zich te nemen maar zich meer richt op de vraag: waar kan ik het antwoord vinden?”

Blockchain

Het onvermijdelijke thema Blockchain werd behandeld door zowel dr. Oskar van Deventer (Senior scientist blockchain net-

Virtual reality wordt ook ingezet om militairen te trainen. Met SUIT (Small Unit Immersive Trainer) wanen militairen zich in een missiegebied, maar staan gewoon in een grote grijze ruimte (foto: Defensie/Phil Nijhuis).

Inmiddels is er een pallet van games (zoals matrix games en dilemma games) ontwikkeld waarmee ervaring is opgedaan voor diverse hybrid conflictvoering scenario’s (foto: Marjolein de Wit-Blok).

De jongste presentator van de dag Liu Kars vertelt over de 'TigerID': een niet-kopieerbaar identificatiebewijs voor de smartphone (foto: Marjolein de Wit-Blok).

sleutels of laten deze stelen en mensen bij elkaar creëren de historie van een blockchain. In alle gevallen zijn er ongetwijfeld kwaadwillenden aanwezig. Maar dat moet ons er vooral niet weerhouden om de potentiële voordelen van blockchaintechnologie te exploreren."

Nieuwe denkmodellen

Walter Bril noemde een toepassing van blockchain in de logistieke keten. "De blockchaintechnologie biedt ons voor het eerst de mogelijkheid om serieus na te denken over het aanpassen van onze huidige denkmodellen waarbij we traditioneel nieuwe technologie toepassen in bestaande kaders. De focus zou moeten komen te liggen op het organiseren van vertrouwen, met als gevolg het verminderen van frictie wanneer vraag en aanbod bij elkaar worden gebracht. Het gaat immers om (tijdelijk) organiserend vermogen en niet zozeer om organisaties als duurzame (juridische) entiteit. Het nastreven van volledige werkgelegenheid zou in deze context daarom wel eens in een heel ander daglicht komen te staan. Voer voor managers."

Virtuele identiteit

Dr. Hans Henseler, CEO Tracks Inspector behandelde het thema 'Cyber Agent Technology'. "Het virtuele karakter van sociale media maakt het lastig om feit van fictie te onderscheiden. Virtuele identiteiten, elektronisch geld en fakeberichten zijn ongrijpbaar en worden niet gehinderd door firewalls of andere technische veiligheidsmaatregelen. Het bespioneren van ongewenste groeperingen en het ontregelen van bedreigingen blijft vooralsnog mensenwerk. Om zulke operaties te vereenvoudigen en te coördineren ontwikkelt Tracks Inspector een prototype voor Cyber Agent Technology (CAT). Door te werken met een 'virtuele' identiteit is het mogelijk ongezien sociale media te verkennen en confrontaties met verdachte identiteiten aan te gaan met als doel om ze te ontmaskeren of om hun plannen te saboteren."

Liu Kars – oprichter en CEO van Ticketguard – sloot het blok 'Excellente technologieën' af met een oplossing om eenvoudiger, slimmer en veiliger toegang te verlenen tot een locatie, materieel, webpagina enzovoorts. Deze oplossing is de 'TigerID'; een niet-kopieerbaar identificatiebewijs voor de smartphone waarmee personen zich kunnen identificeren op ieder gewenst moment. Vanuit een account-based systeem is flexibel te bepalen en te verifiëren waar een persoon recht op heeft. Kars: "De oplossing is in eerste instantie ontwikkeld om fraude bij de verkoop van concertkaarten te voorkomen, maar is uiteindelijk toepasbaar voor ieder 'toegangsprobleem'." AT

www.kooysymposium.nl

working bij TNO) als Walter Bril (CSM bij Elements.cloud). Van Deventer ging in op zowel de goede als slechte kanten van blockchain. "Op langere termijn wordt blockchain wellicht een vitale infrastructuur en zal dus goed moeten worden beveiligd. Hoewel het nog niet zo ver is, kunnen we ons maar beter goed voorbereiden. Cryptomunten zijn bijvoorbeeld vaak deflationair, net als goud, wat destabiliserend kan werken bij grootschalig gebruik. Bovendien zijn er voldoende problemen te benoemen op de kortere termijn. De hype lokt bijvoorbeeld consumenten in dubieuze investeringen, en vereenvoudigt drugshandel en witwassen. De verwachte voordelen van blockchaintechnologie zijn minder bureaucratie, lagere administratieve lasten en betere dienstverlening. Deze verwachte voordelen worden momenteel geëxploreerd in vele industriesectoren en bij de overheden. Daarbij wil ik wel benadrukken dat het slechts een technologie is en dat mensen deze moeten laten werken. Mensen maken transacties aan en ondertekenen deze, mensen verliezen hun

Inmiddels is het Kooy Symposium de belangrijkste activiteit van de KIVI afdeling Defensie & Veiligheid waarbij de organisatoren afkomstig zijn uit de 'gouden driehoek': Defensie, onderzoeksinstituten zoals TNO en het bedrijfsleven (foto: Marjolein de Wit-Blok).