Secondant

THEMA'S:CRIMINALITEITSTRENDSCYBERCRIMEPUBLIEKE VEILIGHEIDSZORGTECHNOLOGIE
RUBRIEK:ONDERZOEK & ANALYSE

HYBRIDE DREIGINGEN ZIJN DICHTERBIJ DAN JE DENKT

Foto: Sandra Uittenboogaart

15 februari 2021
AUTEURS: RICK MEESSEN , MARCEL VAN BERLO

De coronacrisis maakt duidelijk dat hybride dreigingen niet meer weg te denken zijn uit onze samenleving. Ze manifesteren zich overal en in verschillende vormen, en zullen de komende tijd ook onder ons blijven. Alleen een weerbare samenleving kan deze dreigingen enigszins pareren.

Het verspreiden van nepnieuws, complottheorieën en het beïnvloeden van verkiezingen zijn verschijnselen waar we de laatste tijd steeds meer mee zijn geconfronteerd. Daarbij gaat het niet louter om activiteiten van complotdenkers. Vaak is er sprake van ‘hybride conflictvoering’. Bij deze vorm van conflicten gaat het om een gecoördineerde, complexe mix van gebeurtenissen en middelen met mogelijke gevolgen voor de veiligheid, die

vaak ongrijpbaar of zelfs ondefinieerbaar zijn. De middelen kunnen van diplomatieke, militaire, economische en juridische aard zijn. Het kan ook gaan om het verspreiden van desinformatie. De verschillende middelen worden geïntegreerd en over langere termijn ingezet om geopolitieke doelen te bereiken. Denk daarbij aan orkestratie van cyberaanvallen, desinformatiecampagnes, en provocatieve luchtruimschendingen. Het gaat vaak samen met misleiding, ambiguïteit en ontkenning van de acties. Hierdoor is het lastig om de dader(s) aan te wijzen (attributie) en wordt een effectieve respons bemoeilijkt.

China maakt veel gebruik van digitale spionage bij hightechbedrijven

De laatste tijd nemen hybride dreigingen een steeds prominentere plaats in het publieke debat in. De inlichtingendiensten en politie waarschuwen voor de groeiende digitale dreiging (spionage, sabotage) en voor de destabiliserende beïnvloeding door landen als Rusland, China en Iran. Het is hiermee een serieus gevaar voor onze democratie, waardoor het ook op lokaal niveau een forse impact kan hebben. Zo maakt China veel gebruik van digitale spionage bij hightechbedrijven, waarmee ze de concurrentiepositie van die bedrijven ondermijnen, met in potentie schadelijke gevolgen voor deze bedrijven. Dat kan uiteindelijk ook op lokaal niveau tot banenverlies leiden.

CORONACRISIS

Ook tijdens de coronacrisis hebben Rusland en China niet stilgezeten. In een studie die de Spaanse fact checking-organisatie Maldita heeft uitgevoerd, bleek dat desinformatie met name gericht is op 5G als bron van het virus, het gebruik van mondmaskers en vaccinatie. Rusland gebruikt desinformatie over vaccinatie om gevoelens van onveiligheid en polarisatie in het Westen te creëren door het opstoken van anticorona/-vaccinatie-bewegingen.

Ook het creëren van afhankelijkheden en een positief (schijn)imago zijn onderdeel van geregisseerde hybride campagnes. Zo leverden Chinese bedrijven mondkapjes en andere medische goederen. De Chinese overheid buitte dit flink uit met georkestreerde pr-campagnes die de positieve rol van China belichtten. Met de boodschap ‘From Russia with Love’ stuurde Rusland Russische vliegtuigen met medici en hulpgoederen naar Italië. Deze actie bleek echter niet altijd te voorzien in ook daadwerkelijk goed functionerende medische middelen. Maar dat maakte niet meer uit, het imago was al opgepoetst. Het bij- of hoofdeffect van deze liefdadigheid was het versterken van polarisatie binnen de EU, doordat Italië zich in de steek gelaten voelde door zijn bondgenoten.

TECHNOLOGIE ALS HYBRIDE DREIGING

Hybride dreigingen zijn in wezen van alle tijden. Met de snelle technologische ontwikkelingen zijn deze dreigingen echter sneller, beter en breder te verspreiden. Voor hybride actoren is het belangrijk om middelen in te zetten waarmee attributie kan worden voorkomen en die snel een groot deel van de samenleving kunnen raken. Om die reden zijn cyber hacks en desinformatiecampagnes een probaat middel gebleken. We zien dat ook nieuwe technologische ontwikkelingen een arsenaal aan kansen biedt voor hybride actoren. Onze samenleving is erg afhankelijk van satellieten, denk aan navigatie en het financieel betalingsverkeer. Het storen, misleiden of zelfs uitschakelen van satellieten leidt daardoor tot schadelijke en mogelijk zelfs ontwrichtende effecten voor onze samenleving. In een in september 2020 uitgebracht rapport van het Amerikaanse ministerie van defensie wordt China's ontwikkeling van onder meer storingszenders tegen satellieten dan ook als een groot risico geduid.

Verdachte gebeurtenissen worden nog te weinig gedeeld

Een ander voorbeeld van het gebruik van nieuwe technologie als hybride dreigingsmiddel is de snelle ontwikkeling van het Internet of Things (IoT). Met de invoering van 5G-netwerktechnologie zal het huidige aantal van 26 miljard gekoppelde apparaten wereldwijd binnen 5 jaar verdrievoudigen. Op straat en in huis zal het IoT dan ingeburgerd en verankerd zijn, en daarmee ook onze afhankelijkheid daarvan. In december 2019 meldden voor het eerst gebruikers van Amazon Ring, gekoppelde slimme hardware voor huisbeveiliging, dat externen illegaal toegang hadden gekregen tot apparaten die aan Amazon Ring waren gekoppeld. Het bedienen van apparaten op afstand is niet alleen voor criminele actoren interessant. Sommige criminele organisaties zijn een verlengstuk van een statelijke actor, en ondersteunen zo hybride campagnes.

DE STAAT VAN NEDERLAND

In Nederland is inmiddels bij enkele ministeries het besef van de ernst en schade die hybride dreigingen kunnen veroorzaken, voldoende ingedaald. Maar door de gecombineerde en geregisseerde inzet van middelen in hybride campagnes zit de zwakte van ons systeem in de verbinding. Verdachte gebeurtenissen worden nog te weinig gedeeld. Het zogenoemde 'connecting the dots' is daarom een van Nederlands belangrijkste uitdagingen. Dit vereist een goede detectie- en monitoringfunctie over de volle breedte van onze samenleving (zowel nationaal als regionaal/lokaal), waarin ook private partijen betrokken moeten worden.

Aangezien we niet alles tijdig kunnen detecteren, dienen we ook onze weerbaarheid te versterken

Aangezien we echter niet alles tijdig zullen en kunnen detecteren, dienen we ook onze weerbaarheid te versterken. Educatie in het gebruik en de effecten van desinformatie is daar een voorbeeld van. Maar ook investeren in fact-checking. Zo is inmiddels een alliantie (International Fact-Checking Network) van meer dan 100 fact checking-organisaties uit 70 landen en in 40 talen ontstaan, die samen de strijd aan gaan tegen desinformatie over COVID-19.

EUROPESE ONTWIKKELINGEN

Als (middel)klein land is het voor Nederland van belang om aan te haken bij ontwikkelingen van onder meer de EU en NAVO. Een van deze ontwikkelingen betreft het EU-HYBNET-consortium, dat vanaf 2020 een 5 jaar durend onderzoeksprogramma voor de EU uitvoert.
Voor Nederland zijn hierbij NCTV, het ministerie van Defensie en TNO aangesloten. Een belangrijke doelstelling van dit project is het identificeren en realiseren van nieuwe en aanvullende capaciteiten tegen hybride dreigingen. Een voorbeeld daarvan is het versterken van onze democratische processen, en de weerbaarheid van burgers en vitale sectoren. Capaciteiten die daarbij een rol spelen zijn cyberverdediging, het tegengaan van desinformatie en adequate communicatie en informatievoorziening naar onze burgers. Dit is niet alleen een taak van de centrale overheid maar ook van gemeenten, die staan immers dichter bij de burgers.

PROACTIEF HANDELEN

Om hybride dreigingen het hoofd te kunnen bieden is veel nodig, op zowel nationaal als lokaal/regionaal niveau. Het ontwikkelen van kennis en bewustzijn, het ontwikkelen van technische en organisatorische capaciteiten tegen hybride dreigingen, en het genoemde ‘connecting the dots’ zijn daar voorbeelden van. Maar bovenal is proactief handelen gevraagd. Een belangrijke element hierin is het anticiperen op nieuwe trends en dreigingen in het hybride speelveld. Een voorbeeld hiervan is de recent geformuleerde kabinetsbrede strategie tegen desinformatie. Maar ook technologieverkenningen en gaming spelen daarin een rol.
Middels ‘hybrid games’ worden nieuwe scenario’s en dreigingen doorgespeeld. Met als uiteindelijke doel om meer bewustzijn te ontwikkelen, inzichten in effecten van hybride dreigingen met elkaar op te bouwen en samen na te gaan welke handelingsperspectieven mogelijk zijn. Een belangrijke volgende stap hierbij is het steeds meer betrekken van

lokale/regionale en private actoren. Alleen met een brede maatschappelijke aanpak maken we kans om hybride dreigingen te kunnen pareren. <<

Finland: expertise over hybride dreigingen

Finland heeft een lange geschiedenis als kleine staat die naast een groot en assertiever buurland leeft: Rusland. Daardoor is Finland zich bewust van hybride dreigingen en treft het land ook adequate maatregelen tegen die dreiging. Voorbeelden zijn een goed functionerende publiek-private samenwerking voor snelle respons acties (rondom cybersecurity) en het 'total defence concept', waarbij alle sectoren van de overheid en de economie betrokken zijn bij de defensieplanning. In 2017 is het **European Centre of Excellence for Countering Hybrid Threats** in Helsinki opgericht, zij zijn ook initiator van het EU-HYBNET-project. Tijdens de looptijd van het project kunnen ook nieuwe partners toetreden. Vul hiervoor dit **application form** in of ga naar deze **webpagina** voor meer informatie.

Rick Meessen en Marcel van Berlo zijn werkzaam bij TNO, respectievelijk als Principal Adviseur Defensie en Veiligheid en Programma Coördinator EU en Nationale Veiligheid . De auteurs zijn bereikbaar voor vragen en discussies via e-mail: rick.meessen(at)tno.nl en marcel.vanberlo(at)tno.nl.