DE SCHADUWZIJDE VAN DIGITALISERING

Onderzoeksjournalist bij De Volkskrant Huib Modderkolk schreef in 2019 het boek 'Het is oorlog maar niemand die het ziet'. Hierin beschrijft hij de resultaten van zijn zesjarige zoektocht naar de schaduwkant van het internet waar criminelen, maar ook staten, schijnbaar naar hartenlust hun gang kunnen gaan. Het boek werd een bestseller in Nederland (meer dan 100.000 keer verkocht) en werd vertaald in onder andere het Engels en het Duits. Het was tevens de basis voor de Tv-documentaire *Niemand die het ziet* van BNNVARA begin dit jaar. Centraal thema in de documentaire is de rol die Nederlandse veiligheidsdiensten gespeeld (zouden) hebben bij Stuxnet.

Dit Amerikaanse computervirus was specifiek ontwikkeld om bepaalde Siemens-apparatuur dat gebruikt werd in de ultracentrifuges van het Iraanse nucleaire programma schade toe te brengen. In 2010 was Stuxnet het eerste succesvolle offensieve cyberwapen dat door statelijke actoren is ingezet tegen een andere staat. In zijn boek en documentaire onthuld Modderkolk dat een agent van een van de Nederlandse diensten een cruciale rol heeft gespeeld in deze Amerikaans – Israëlische sabotageactie.

Desinformatie

Met de inzet van Stuxnet als offensief cyberwapen door statelijke actoren is een geheel nieuw tijdperk aangebroken. Naast spionage (meekijken) en criminaliteit (o.a. gijzelsoftware) is sabotage aan het cyberdomein toegevoegd. Daarmee wordt Stuxnet aangemerkt als historische mijlpaal. Een eventueel Nederlandse bijdrage hieraan zou opvallend zijn en Modderkolks fascinatie hiervoor is dan ook eenvoudig te verklaren. In zijn nieuwste publicatie neemt hij de lezer mee in zijn zoektocht naar de identiteit van de Nederlandse agent. Deze begint als hij omslachtig en voorzichtig in contact komt met een agent van de Israëlische inlichtingendienst Mossad. Deze man doet het voorkomen alsof hij de hulp van Modderkolk nodig heeft, maar wil uiteindelijk weten wat de Nederlandse journalist precies weet van de hele affaire en probeert hem te sturen in zijn onderzoek. De Nederlandse bijdrage aan Stuxnet en de interesse van de Israëlische Mossad in deze zoektocht loopt als een rode draad door het boek. Modderkolk wisselt deze hoofdstukken af met andere gevaren achter de schermen van het internet en met name de rol die overheidsinstanties daarin spelen.

'Zijn focus ligt bij Nederlandse activiteiten die zich dikwijls kunnen meten met de cyberkopgroep van de Westerse wereld; de Verenigde Staten, Verenigd Koninkrijk en Israël'

In deze hoofdstukken krijgt de lezer tal van diverse cyber-onderwerpen voorgeschoteld waar naast spionage, sabotage en criminaliteit inmiddels ook beïnvloeden door desinformatie aan het cyberdomein is toegevoegd. Met name de democratische Westerse wereld is erg gevoelig voor deze desinformatie en Modderkolk geeft meerdere voorbeelden waar we ook in Nederland met open ogen zijn ingelopen. Door beïnvloeding vanuit (staatsgesteunde) Russisch orthodox-christelijke instellingen worden van gevoelige onderwerpen in het onderwijs of de LHBTQ+-rechten een probleem gemaakt, waardoor goede intenties van de desbetreffende initiatiefnemers om worden gedraaid naar iets kwaadaardigs. Dieptepunt hierin is het cancelen van kinderboekenschrijver Pim Lammers en de Week van de Lentekriebels. Niet alleen de 'gewone mens' trapt erin, maar ook politici lijken slachtoffer. Of laten zij zich maar wat graag beïnvloeden? Ook in de aanbesteding van de nieuwe onderzeeboten voor de Koninklijke Marine zijn pogingen tot beïnvloeding gedaan. Zo meldt *De Groene Amsterdammer* dat er in 2019 drie artikelen in vakbladen zijn verschenen met een negatieve benadering van de Zweeds-Nederlandse en Duitse kandidaat. De schrijver van het artikel blijkt niet te bestaan en *Defense News* trekt de artikelen in. De Zweedse militaire inlichtingendienst MUST weet Saab-Damen te melden dat een derde partij in de digitale systemen van het Zweeds-Nederlandse bedrijf heeft gezocht naar gevoelige en vertrouwelijke informatie. Niet alleen statelijke actoren bedienen zich van cyber-spionage.

Niet of, maar wanneer

Cyber-spionage en sabotage vormen dan ook het tweede hoofdthema van het boek. Modderkolk vertelt uitgebreid over de activiteiten van Rusland en Iran op het internet. Net als in zijn eerste boek ligt zijn focus bij de Nederlandse activiteiten die zich dikwijls kunnen meten met de cyberkopgroep van de Westerse wereld; de Verenigde Staten, Verenigd Koninkrijk en Israël. De Russische en Iraanse activiteiten worden omschreven als weinig subtiel, lomp en nauwelijks heimelijk, alsof men schiet met een schot hagel. Veel geraffineerder en technisch hoogwaardiger zijn de illegale Chinese activiteiten op het internet. Opvallend is ook hoe Westerse overheidsinstanties en bedrijven reageren als zij een *hack* ontdekken. Een Russische of Iraanse inbraak wordt dikwijls in de openbaarheid gebracht en soms wordt de vondst zelfs als succes gepresenteerd. Chinese *hacks* daarentegen worden bij voorkeur doodgezwegen, *naming and shaming* van China durft men kennelijk niet aan. Somber en ontnuchterend is ook de conclusie van Modderkolk; het is niet de vraag of je wordt gehackt (of de negatieve gevolgen van een *hack* ondervindt), maar wanneer je wordt gehackt en wanneer je de *hack* door hebt.

Een ander thema is de negatieve keerzijde van digitale systemen. Wellicht zijn ze met de beste bedoelingen bedacht, toch kunnen ze ook een bedreiging vormen. Goed voorbeeld is het Nederlandse Travel Information Portal (TRIP). In 2013 werkt de Europese Commissie in het kader van terrorismebestrijding aan een plan om luchtvaartmaatschappijen te verplichten om vooraf passagiersgegevens te verstrekken. Nederland werkt dit plan uit en krijgt uiteindelijk Europese subsidie om TRIP op te zetten. De portal heeft tot doel om met behulp van de passagiersgegevens een risicoanalyse te maken zonder dat de passagiers daar hinder bij ondervinden. TRIP wordt echt effectief als in een latere versie ook de digitale gegevens van de magneetstrip uit het paspoort worden toegevoegd. Met de juiste risico-indicaties kan de douane zeer gericht te werk gaan en is er geen noodzaak om alle passagiers in persoon te bevragen. De veiligheid neemt toe en het ongemak van lange wachtrijen voor passagiers neemt af. Als andere Europese landen zonder TRIP kwetsbaarder lijken, zoals bij de aanslag op het Belgische vliegveld Zaventem in 2016, is Nederland snel bereid TRIP te delen. Een veiliger Europa is immers in het belang van Nederland. TRIP wordt gratis buiten Europa geëxporteerd en vervolgens, wederom voor niets, aan de Verenigde Naties aangeboden. De VN krijgen zelfs de IP-rechten. Maar waarom hebben sommige landen inmiddels seksuele geaardheid en vakbondlidmaatschap in een open veld toegevoegd aan dit systeem? Wat heeft dit met terrorismebestrijding te maken?

'Dit wil je écht niet weten' is duidelijk een boek geschreven door een journalist. Wie een academische studie verwacht komt bedrogen uit. Modderkolk lepelt tal van voorbeelden op en deze zijn vrijwel allen interessant om te lezen. Wat de onderlinge relatie is van deze voorbeelden is lastiger te bepalen. De ondertitel suggereert dat de schaduwzijde van de digitalisering het onderlinge verband is, de rode draad – de zoektocht naar de identiteit van de Nederlandse agent - gaat echter over activiteiten van inlichtingendiensten en dan vooral de Nederlandse diensten en de Mossad. De schrijver geeft, zoals het een goed onderzoeksjournalist betaamt, aan waar hij hoor en wederhoor heeft toegepast en voorziet zijn hoofdstukken van verwijzingen. Door zijn journalistieke schrijfstijl blijft het toegankelijk voor een breed publiek. Hij heeft in zijn zoektocht van vier jaar voor dit boek meer dan 100 mensen gesproken. Specifiek over de identiteit en acties van de Nederlandse agent heeft hij 43 mensen gesproken in binnen- en buitenland. In totaal kwamen 19 van deze contactpersonen van de AIVD en MIVD. Zij hebben anoniem een bijdrage geleverd aan dit boek. Hiermee geeft het de lezer, naast inzicht van de schemerzone van het internet, ook een aardig inkijkje in het werk van de Nederlandse diensten. Modderkolk stelt dat hij het boek voor publicatie heeft aangeboden aan de beide diensten. De AIVD heeft drie keer inhoudelijk gereageerd en had verder geen commentaar. De MIVD heeft gereageerd met de opmerking dat zij nooit inhoudelijk over operaties uitspraken zullen doen en dus niets kunnen bevestigen noch ontkennen.

'Wie een academische studie verwacht komt bedrogen uit'

Ten slotte

De rode draad van het boek en het hoofdthema zijn niet als vanzelfsprekend aan elkaar verbonden. Toch is het evident dat het werk van inlichtingendiensten met de komst van het internet de laatste 30 jaar significant is veranderd. Wet- en regelgeving in het cyberdomein is nog niet 'volwassen', vrij ruim opgezet of bestaat nog niet. Dat maakt handhaving bijzonder lastig. Niet voor niets maken de meeste inlichtingendiensten gebruik van deze *grey zone* om hun doelen te bereiken. Tel daarbij op dat de digitalisering in snel tempo blijft doorzetten en dat steeds meer mensen zich in het cyberdomein begeven – bewust of onbewust. Het ongemak dat Modderkolk heeft is voelbaar. De digitale mogelijkheden lijken onbegrensd, de dreigingen en kwetsbaarheden zijn amper te overzien. Wegkijken lijkt dan zo gek nog niet.

BRIGGENMARNS Rob de Wit

Dit wil je écht niet weten
Over de onvoorstelbare wereld achter je scherm

Auteur	Huib Modderkolk
Uitgever	Uitgeverij Podium, Amsterdam (2024)
Omvang	288 blz
Prijs	€ 20,99
ISBN	9789463812160