‘Een ongekende digitale wapenwedloop’

Huib Modderkolk over internet, privacy en spionage

FOTO BENJAMIN KOTEK IN PAKHUIS DE ZWIJGER

Huib Modderkolk: ‘Als staten dagelijks andere landen digitaal aanvallen, dan is dat geen conflict meer, maar oorlog’

Internet is allang geen vrijplaats meer waar staten ooit geen autoriteit hadden. Grote bedrijven en overheden proberen het internet juist te controleren en hebben zicht op de data van miljarden mensen. De individuele privacy is ernstig in het geding, terwijl veiligheidsdiensten dagelijks bezig zijn cyberaanvallen op vitale doelen af te slaan en zelf doelwitten in kaart te brengen. Door internet lijkt de algehele veiligheid in de wereld eerder afgenomen te zijn. Ligt er een taak voor de politiek om het toezicht te verscherpen? En doet Nederland genoeg voor zijn digitale veiligheid?

Frans van Nijnatten

Terwijl de grote zaal van Pakhuis de Zwijger in Amsterdam volstroomt voor de presentatie van het boek *Het is oorlog maar niemand die het ziet*[1] van Huib Modderkolk, glimlachen mensen om de stem die door de luidsprekers klinkt: ‘U kunt staatsgeheimen horen’, en: Niets wat u hier hoort mag u aan derden vertellen, hier binnen geldt strikte geheimhouding.’ Maar als moderator Sheila Sitalsing begint te spreken en haar collega-journalist Modderkolk introduceert op het podium, is de toon al snel ernstig. Modderkolk, onderzoeksjournalist bij *de Volkskrant*, legt uit dat hij een tijd nagedacht heeft over de titel van zijn boek. ‘Oorlog is een beladen woord. Voor oorlog duik je weg. Maar Nederland wordt dagelijks digitaal aangevallen. En als staten dat doen, dan is dat geen conflict meer, maar oorlog.’

1 Huib Modderkolk, *Het is oorlog maar niemand die het ziet* (Amsterdam, Uitgeverij Podium, 2019. ISBN 9789057599804). Gepresenteerd op 4 september 2019 in Pakhuis de Zwijger, Amsterdam.

Modderkolk baseerde zijn boek, waarin hij op zoek gaat naar de gevaren van internet en probeert de wereld van de digitale spionage te begrijpen, op gesprekken met bronnen, onder wie (oud)medewerkers van de AIVD, MIVD en NCTV, ambtenaren van ministeries en beveiligingsonderzoekers. Daarnaast gebruikte hij staatsgeheime documenten, vertrouwelijke politieke stukken, ambtelijke notities, jaarverslagen van de inlichtingendiensten en openbare rapporten van publieke en private instanties. De AIVD en MIVD lazen voor publicatie delen van het boek, en via een rechtszaak lukte het de AIVD bepaalde details uit het boek verwijderd te krijgen.
Omdat hij zijn bronnen niet openlijk kan noemen zegt Modderkolk te beseffen dat hij het nodige vraagt van het vertrouwen van de lezer. Hij schrijft over zaken die inlichtingendiensten zelf niet naar buiten brengen en onthult dat de AIVD betrokken zou zijn geweest bij het naar binnen brengen van het Stuxnet-computervirus in het Iraanse nucleaire complex in Natanz in 2007.

Kantelmoment

'Als ik met bronnen spreek noemen zij het jaar 2015, waarin de MIVD ontdekte dat de Russische militaire inlichtingendienst via een server in Meppel virussen loslaten richting Oekraïnse elektriciteitscentrales en media, een kantelmoment. Het is nu 2019 en de inzet van digitale wapens kan alleen maar beter en meer georganiseerd zijn geworden. Bedenk dat alleen al China dagelijks duizenden hackers inzet', aldus Modderkolk. De MIVD loopt 'digitaal hopeloos achter' vergeleken met de AIVD, concludeert Modderkolk op basis van zijn onderzoek. Hij beschrijft in zijn boek ook het volgens hem moeizame proces van de diensten voor nauwere samenwerking.

Modderkolk wijst er op dat de westerse open samenlevingen kwetsbaar zijn, terwijl burgers schijnbaar moeiteloos data over zichzelf afstaan waarmee hun gedrag bijna volledig in kaart gebracht kan worden. Die constatering zit verwerkt in de ondertitel van zijn boek. 'We zien alleen de glimmende kant van internet. Het is moeilijk te begrijpen, zelfs voor experts, wat er

FOTO BENJAMIN KOTEK IN PAKHUIS DE ZWIJGER

'We zien alleen de glimmende kant van internet', zegt Huib Modderkolk op een vraag van moderator Sheila Sitalsing over het blinde vertrouwen in de techniek

binnen in de netwerken gebeurt.' Het blinde vertrouwen in de techniek en internet kan er volgens Modderkolk toe leiden dat de burger vrijheden inlevert en dat niet doorheeft. Data die bedrijven verzamelen, zouden ook in staatshanden kunnen vallen. 'En uiteraard zouden ook criminelen ze kunnen gebruiken als ze er de hand op weten te leggen.'

Als plotseling het licht in de zaal uitvalt en het even donker blijft, ontstaat er niet meteen paniek onder het publiek. Al snel maken Modderkolk en Sitalsing duidelijk dat de blackout bij de presentatie hoort. 'Maar zo kan het wel gaan bij een hackaanval.'

Schemergebied

Voor de research van zijn boek werkte Modderkolk de afgelopen zes jaar in een schemergebied en in die periode publiceerde hij er ook regelmatig over. 'Je kunt inlichtingenbronnen niet zomaar bellen, je moet andere wegen kiezen. In een geval is het mij gelukt via het sociale netwerk LinkedIn en daarop volgend verder speurwerk een bron te lokaliseren. Maar namen noemen kan ik natuurlijk nooit. Schrijven zonder bronnen open te leggen legt enorme beperkingen op, er moeten goede argumenten tegenover staan.' De bescherming van mensen is zo'n argument en Modderkolk kan daarin meegaan en neemt bijvoorbeeld nooit gesprekken op, want audiobestanden zouden verkeerd terecht kunnen komen. Hij zegt met zijn boek

‘de best leesbare versie van de werkelijkheid’ te hebben willen schrijven, en wijst er op dat de inlichtingendiensten zelf nooit zullen zeggen of iets klopt of niet.

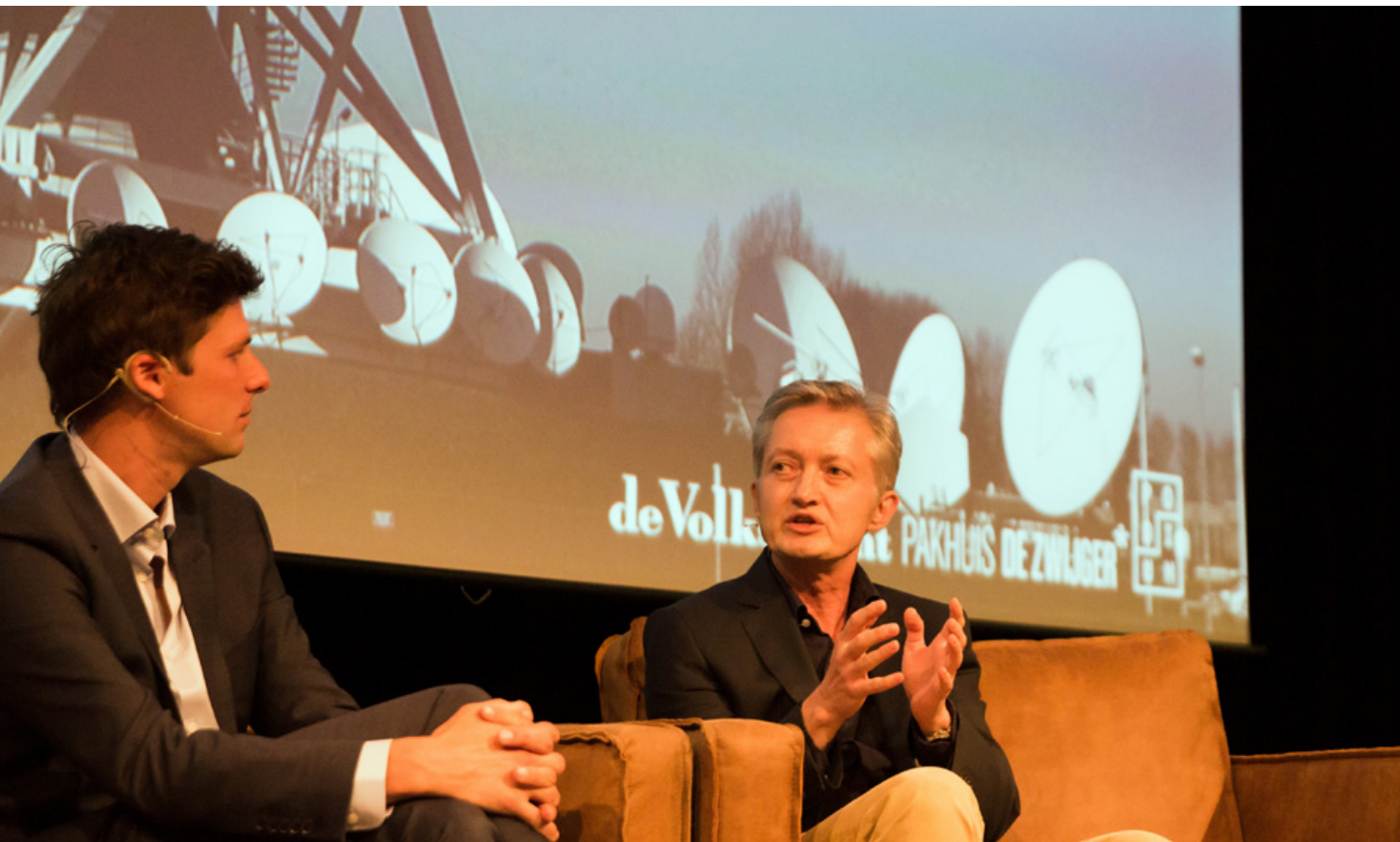
In zijn boek noemt hij de Nederlandse veiligheidsdiensten een stuk geslotener dan bijvoorbeeld de Amerikaanse CIA of FBI, die door hun omvang moeten werken met gedetacheerd personeel, meer politieke strijd moeten leveren en een opener cultuur hebben. Dat zou eerder lekken in de hand werken, waardoor gevoelige informatie op straat kan komen te liggen. Een voorbeeld is Edward Snowden, de Amerikaan die tienduizenden geheime documenten bij de National Security Agency (NSA) meenam en aan journalisten gaf. Daarmee werd ook bekend dat bedrijven als Google en Facebook data aan de NSA afstaan. Als Modderkolk via een journalist zelf Snowden-documenten onder ogen krijgt, blijken die veel technische termen te bevatten en voelt hij zichzelf onwetend. Maar het is geen beletsel om verder te werken en te onderzoeken.

Zo stelt hij de vraag hoe ver inlichtingendiensten mogen gaan met ‘dataminen’ en waar de grens met privacyschending ligt.

‘Het verzamelen van data betekent al snel het profileren van groepen. Het is daarom zorgelijk dat het vertrouwen in data zo groot is’, zegt Maxim Februari, schrijver en rechtsfilosoof en panellid tijdens de boekpresentatie. ‘Wat in deze oorlog wegvalt is het rechtssysteem, doordat algoritmen op basis van data zelfstandig besluiten nemen.’ Die zorg delen zijn medepanelleden Alexander Klöpping, media-ondernemer, en Marietje Schaake (D66), oud-lid van het Europees Parlement. Volgens Schaake laat het toezicht op het handvol bedrijven dat voor talloze mensen het informatie-ecosysteem managet te wensen over. ‘Het gaat om ongecontroleerde macht, waarbij bedrijven zich verschuilen achter handelsgeheimen. Dat is wat mij betreft onhoudbaar, de kernprincipes van de rechtsstaat moeten gehandhaafd blijven.’ Klöpping vindt ook dat er verantwoordelijkheid

Maxim Februari licht toe hoe het rechtssysteem volgens hem onder druk komt te staan door het vertrouwen in data en algoritmes

FOTO BENJAMIN KOTEK IN PAKHUIS DE ZWIJGER



bij de burger zelf ligt. ‘Algoritmes brengen overzicht voor ons aan in een datachaos. Dat Twitter bepaalt wat we interessant vinden, vinden we fijn.’ Mensen zouden zelf vaker verbindingen met een virtual private network (VPN) kunnen leggen of encryptie zou toegankelijker gemaakt kunnen worden voor grotere groepen.

Volgens Modderkolk is het inmiddels duidelijk dat er een taboe op afluisteren is weggevallen. Zo vertelde zijn bron 'Robin', die voor een Australisch bedrijf nietsvermoedend opnames uitschreef, dat ze tot haar schrik plotseling ook de stem van haar eigen vriend hoorde. Inlichtingendiensten verschaffen zich toegang tot computernetwerken en nemen gegevens van webfora onder de loep. Bedrijven en onverheidsinstanties krijgen door alle data inzichten en opsporingsmogelijkheden die voorheen ondenkbaar waren en waarmee ze mensen ‘zo goed als live kunnen volgen’. Dat het ook om kwetsbare systemen kan gaan legt Modderkolk uit als hij beschrijft hoe de 17-jarige hacker Edwin toegang weet te krijgen tot de gegevens van miljoenen KPN-klanten.

FOTO BENJAMIN KOTEK IN PAKHUIS DE ZWIJGER

Alexander Klöpping en Marietje Schaake wijzen op het handvol bedrijven dat de informatiestromen in handen heeft; maar ook de burger zelf heeft een verantwoordelijkheid

Mensen achter de data

‘Het boek van Huib humaniseert: er zitten mensen achter die data’, merkt Klöpping op. Modderkolk laat in zijn boek zien hoe hackers optreden en hoe personen reageren op hacks en incidenten, zoals rond de affaire bij de certificaatautoriteit Diginotar in Beverwijk in 2011, waar een Iraanse hacker toegang wist te krijgen. Modderkolk noemt dit een duidelijk voorbeeld van de ‘ongekende digitale wapenwedloop’ die in gang is gezet toen het Westen in 2007 Iran als doelwit koos. Een ander voorbeeld is de ‘digitale veldslag’ tussen Russische hackers en de FBI, CIA en NSA in 2016, toen het Amerikaanse ministerie van Buitenlandse Zaken en het Witte Huis werden aangevallen. De AIVD en MIVD konden hackers van Cozy Bear volgen en Amerika waarschuwingen geven. Cozy Bear effende het pad voor het aan de Russische militaire inlichtingendienst gelieerde Fancy Bear, dat er in slaagde servers van de Democratische Partij te kraken en e-mails van Hillary Clinton te stelen en openbaar te laten maken.

Door zijn onderzoek en publicaties geldt Modderkolk als goed ingevoerd en vroegen vrienden en collega’s hem in 2017 bij het referendum over de ‘sleepwet’ of de democratie onder druk kwam en ze voor of tegen moesten stemmen. Modderkolk wist het ook niet: ‘Hoe beter ik internet en de risico’s ken, hoe ingewikkelder het dilemma is geworden. Om de samenleving te beschermen tegen spionage en aanvallen van buitenaf hebben veiligheidsdiensten bevoegdheden nodig die een vrije samenleving onder druk zetten.’ Hij wijst op het bijkomend probleem dat voor conventionele oorlogen internationale regels bestaan, maar ‘voor digitale aanvallen niet.’ En waarschuwt tegelijkertijd dat de Nederlandse overheid veel te weinig investeert in digitale veiligheid. Dat is een ernstig verwijt, maar Modderkolk meent het serieus. De sticker op de cover van *Het is oorlog*, met Arjen Lubachs aanbeveling ‘Wie vroeger de wereld wilde begrijpen, las de Bijbel. Wie de wereld van nu wil begrijpen, leest dit boek’, komt dan eigenlijk iets te frivool over. ■