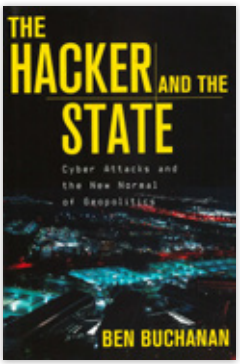

The Hacker and the State

Cyber Attacks and the New Normal of Geopolitics
Door Ben Buchanan
Cambridge (Harvard University Press) 2020
412 blz.
9780674987555
€ 24,-

Voor diegenen die geïnteresseerd zijn in de combinatie van cyber en geopolitiek is het nieuwste boek van Ben Buchanan een aanrader. In *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics* beschrijft hij op een redelijk technische, maar zeer toegankelijke wijze, hoe cyberaanvallen geopolitieke ontwikkelingen beïnvloeden en vormgeven. Ben Buchanan komt uit de school van Thomas Rid en schreef zijn proefschrift bij hem op King's College in Londen. Rid is een van de eerste onderzoekers die het debat over cyberoorlog voorzag van structuur en conceptuele helderheid met zijn boek *Cyber War Will Not Take Place* (2013).
Buchanan loopt zijn onderzoek naar cyberoperaties aan vanuit de academische discipline internationale betrekkingen, en in zijn eerste boek *The Cybersecurity Dilemma* (2017) legde hij overtuigend uit hoe het veiligheidsdilemma (*security dilemma*) verscherpt wordt door de unieke kenmerken van het cyberoptreden. Doordat offensieve en defensieve cyber dicht bij elkaar liggen en voor vijandelijke staten vaak moeilijk van elkaar te onderscheiden zijn, neemt het onderlinge wantrouwen alleen maar verder toe. Buchanans boek *The Hacker and the State* heeft een bredere opzet: het geeft een gedetailleerd overzicht van alle grote (bekende) cyberoperaties tot nu toe en plaatst de casuïstiek in de context van algemeen geopolitiek optreden.

The new normal

The Hacker and the State bevat voor niet-ingewijden waardevolle analyses die vervlochten zijn in het geheel. Een eerste constatering is dat cyber niet goed vergeleken kan worden met kernwapens. Veel analisten en onderzoekers hebben in het verleden cyber juist vanuit het nucleaire paradigma benaderd, als een digitaal equivalent van kernwapens: enorm vernietigend, maar zeldzaam. Buchanan toont aan dat dit onterecht is. Cyberaanvallen zijn inmiddels niet zeldzaam meer, maar juist *the new normal*. Er gaat immers geen week voorbij zonder nieuws van een grote hack, een datalek of ontdekte gevallen van cyberspionage of cybersabotage. Cyberaanvallen, schrijft hij, 'have become a low grade yet persistant part of geopolitical competition' (blz. 3). Juridisch en sociologisch gezien is wellicht de term oorlog hier niet passend, maar staten blijken aanhoudend met elkaar in een digitale strijd te zijn verwikkeld. Deze strijd speelt zich af buiten het zicht van het publiek en wordt vaak niet goed begrepen door traditionele veiligheidsexperts (en politici).
Een tweede rode draad is dat natiestaten geen monopolie hebben op operaties en activiteiten in cyberspace. Bedrijven en criminele organisaties zijn minstens even belangrijke actoren in de zogeheten mêlee, en dit compliceert het toepassen van traditionele theorieën uit de discipline van internationale betrekkingen.

Het conceptuele kader van het boek is eenvoudig. Landen voeren geopolitiek door middel van *signaling* en *shaping*. Onderzoek in internationale betrekkingen richt zich nog voornamelijk op het eerste en dit omvat hoe staten signalen afgeven om hun standpunten en hun intenties duidelijk te maken. Nucleaire wapens geven bijvoorbeeld een afschrikwekkend signaal af en het mobiliseren of ontplooien van militaire eenheden kan eveneens een duidelijke boodschap geven aan potentiële tegenstanders. Shaping daarentegen betreft het direct beïnvloeden of smeden van het gedrag van de ander, door deze bijvoorbeeld te destabiliseren door bedrog, sabotage of andere heimelijke activiteiten. Buchanan past dit conceptueel kader vervolgens toe op een reeks casussen van cyberoperaties. De essentie van zijn argument is dat het cyberinstrumentarium niet geschikt is voor signaling, maar wel erg effectief is op het gebied van shaping. Dit wordt nader uitgewerkt in de drie delen van het boek – spionage, aanval en destabilisatie. Deze delen omvatten elk meerdere hoofdstukken, alle gecentreerd rond een aantal bekende incidenten of cyberoperaties die in detail worden weergegeven.

Beschrijving grootste cyberaanvallen
Het boek is alleen al waardevol omdat het een overzichtelijke beschrijving biedt van de grootste cyberaanvallen van de afgelopen tien jaar. Veel van deze zijn al uitvoerig elders beschreven, zoals de beroemde Amerikaans-Israëlische Stuxnet-cyberaanval op de uraniumverrijkingsinstallatie in Natanz, Iran. Buchanan vat de bekende verhalen beknopt samen en voegt de meest recente informatie toe, zoals de *scoop* van *Volkskrant*-journalist Huib Modderkolk bij Stuxnet. Modderkolk meldde dat het een agent van de AIVD was die het virus door middel van een USB-stick overbracht naar het Iraanse netwerk en daarmee de *air gap* overbrugde (waarmee het lokale netwerk van het internet gescheiden was). Andere bekende voorvallen zijn de reeks van Chinese operaties om intellectueel eigendom te stelen (bedrijfsspionage), de Sony-hack, de Noord-Koreaanse digitale beroving van verschillende banken, de Wannacry- en NotPetya-aanvallen, Sandworm en de Oekraïense energiecentrales: allemaal passeren ze uitgebreid de revue. Ook wijdt Buchanan een hoofdstuk aan de Russische inmenging in de Amerikaanse presidentsverkiezingen van 2016. Dit omvatte zowel een *hack & leak*-element waarbij e-mails van de Democratic National Committee werden gelekt, als een uitgebreide campagne waarbij desinformatie werd verspreid.

Shadow Brokers
Voor het eerst in de cybersecurity-literatuur heeft Buchanan de casus van de Shadow Brokers uitgewerkt en opgeschreven. Tussen najaar 2016 en lente 2017 bracht een onbekende groep die zichzelf de Shadow Brokers noemde een aantal *exploits* van de Amerikaanse National Security Agency (NSA) naar buiten. Dit betrof verschillende zeer geavanceerde *hacking tools* die kwetsbaarheden in onder meer Windows uitbuitten. De bekendste van deze heette ETERNAL BLUE. Nadat de Shadow Brokers dit 'cyberwapen' op internet zetten, werd het door Noord-Koreaanse en Russische hackers geïntegreerd in hun eigen cyberaanvallen (in respectievelijk Wannacry en NotPetya). Het NSA-'wapen' was zo krachtig dat Microsoft-president Brad Smith het vergeleek met de diefstal van een paar Tomahawk-kruisraketten uit het Amerikaanse arsenaal. Zo heeft de NSA ongewild een belangrijke bijdrage geleverd aan de NotPetya-aanval die uiteindelijk wereldwijd meer dan 10 miljard dollar aan schade aanrichtte. Het is nog steeds niet duidelijk wie achter de Shadow Brokers zat, maar Buchanan vermoedt – waarschijnlijk terecht – dat de Russische inlichtingendiensten een rol hebben gespeeld. Dit lek was uiteindelijk vele malen schadelijker dan dat van Edward Snowden enkele jaren eerder.

Naming and shaming
Zoals elk boek kent *The Hacker and the State* ook enkele onvolkomenheden. Het theoretisch kader is minder robuust dan in Buchanans eerdere boek. Zo passen bijvoorbeeld spionage en inlichtingenvergaring, waar het gros van statelijke cyberoperaties onder valt, niet altijd goed in de categorie shaping. Sommige hoofdstukken beschrijven weliswaar goed de gekozen cyberoperaties, maar geven slechts een summiere analyse hoe ze zich verhouden tot de theorie. Ook blijkt het lastig te categoriseren tussen inlichtingendiensten die criminele activiteiten ontplooien om geld te verdienen voor hun regime (Noord-Korea); zij die vervlochten zijn met de georganiseerde misdaad (Rusland); of zij die hackers in dienst hebben die er naast hun dagtaak een eigen cyber-zzp'tje op nahouden (Rusland en China). Inhoudelijk worden sommige van Buchanans conclusies ook niet gesteund door de feiten. Zo meent hij bijvoorbeeld dat het veelvoud aan FBI-*indictments* (dagvaardingen) maar weinig geopolitiek effect heeft gehad (blz. 99 en 305). Maar er is wel degelijk bewijs dat *naming and shaming* werkt. Op operationeel vlak hebben statelijke hackers vaak hun digitale aanvalsinfrastructuur moeten opgeven nadat deze door de FBI of IT-bedrijven werd ontmaskerd. Nieuwe tactieken en technieken moesten dus worden ontworpen omdat de oude verbrand waren. Ook op het diplomatieke vlak hebben China en Rusland aanzienlijke reputatieschade geleden. Vooral China was woest dat de VS in 2014 grote WANTED-posters verspreidde met Chinese militairen afgebeeld in uniform. Dit heeft, samen met het dreigement om sancties toe te passen, in 2015 geleid tot een akkoord tussen China en de VS om geen cyberbedrijfsspionage meer uit te voeren. Het akkoord heeft overigens niet lang standgehouden; inmiddels is het weer schering en inslag op dit gebied.

Ondanks deze kleine punten is *The Hacker and the State* een zeer lezenswaardig boek dat een plek verdient in de boekenkast. Als ouderwetse hardcopy natuurlijk, want alles wat digitaal is betekent kennelijk een risico. ■

Sergei Boeke, politiek adviseur NAVO-hoofdkwartier Joint Support & Enabling Command (JSEC) Ulm