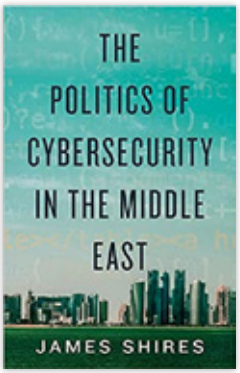

The Politics of Cybersecurity in the Middle East

Door James Shires
Londen (Hurst) 2021
312 blz.
ISBN 9781787384736
€ 41,-

'Never waste a good crisis', zou Churchill hebben gezegd bij de onderhandelingen over de totstandkoming van de Verenigde Naties. Uit een groot kwaad – de Tweede Wereldoorlog – kan iets goeds voortkomen, sterker nog: het is te gebruiken om het eigen belang na te streven. Dit is ook de strekking van *The Politics of Cybersecurity in the Middle East,* een zeer lezenswaardig academisch werk van James Shires, universitair docent Cybersecurity Governance aan het Institute of Security and Global Affairs van de Universiteit Leiden.

Een staat kan meerdere instrumenten van macht toepassen om zijn doelen en belangen na te streven, te verdedigen of te promoten. Los van militaire of diplomatieke middelen kan de staat ook informatie of beeldvorming, bijvoorbeeld rondom een crisis, dusdanig vormen of manipuleren dat zijn acteren – zowel richting de eigen bevolking als richting andere staten – niet meer dan vanzelfsprekend lijkt. Shires noemt dit *moral manoeuvres*, een strategische actie om, onder het mom van een normatief 'juiste' actie, feitelijk een eigenbelang na te streven. Dit geldt niet alleen voor staten, maar ook voor NGO's of grote 'tech'-bedrijven.

In zijn boek geeft Shires geeft aan dat staten, bedrijven of andere belanghebbenden cyber-gerelateerde activiteiten – denk aan de Amerikaans-Israëlische Stuxnet-aanval in 2010 op de verrijkingscentrale in het Iraanse Natanz – *framen* op een wijze die hun eigen interesses en agenda dient: vandaar de 'politics' van cybersecurity. Verschillende frames of paradigma's van cybersecurity dienen een ander doel: een cybergerelateerde actie wegzetten als een cybercrime roept een ander beeld, oplossingsrichting en juridische kaders op dan een cyberoorlog. De keuze is niet belangeloos: ieder label 'attracts significant political and financial capital', aldus Shires (blz. 203).

Vier verschijningsvormen

Shires beschrijft vier verschijningsvormen van cybersecurity (blz. 9), gebaseerd op twee criteria (zie figuur 1). Is cybersecurity gericht tegen een andere staat of op de eigen staat; en gaat het bij cybersecurity om het inbreken op het ICT-systeem of om het beheren en beheersen van informatie? Het boek richt zich op cyberactiviteiten in het Midden-Oosten (met name Egypte en Golfstaten als Qatar, VAE en Saoedi-Arabië), vanwege de combinatie van meer of minder autoritaire regimes, in opkomende regionale digitale economieën, met mondiale financiële netwerken; het is daarmee een analytische lakmoesproef voor acties van landen als Rusland en China.

Cyberconflict is het eerste paradigma waar cybersecurity tegen wapent. De eerdergenoemde Stuxnet-aanval heeft als ongewenst neveneffect gehad dat Iran een militaire cybereenheid heeft ontwikkeld binnen de Revolutionaire Garde. Deze cybereenheid was

	Inbreuk	Informatie
Tussen staten	Cyber Conflict	Buitenlandse Inmenging
Binnen de staat	Mensen-rechten	Informatie Controle

Figuur 1 Vier verschijningsvormen van cybersecurity

verantwoordelijk voor de Shamoon-aanval op de Saoedische oliemaatschappij Aramco. Menig inlichtingen- en veiligheidsdienst in de Golfregio, Europa en de VS heeft deze aanval echter uitgebuit om het destructieve en onbetrouwbare karakter van Iran aan te tonen, om daarmee zelf aan politiek belang te winnen. Ook het (militair-)industriële complex (Raytheon, Dell, BAe) is debet geweest aan het schromelijk overdrijven van de effecten van Iraanse acties, om zo lucratieve contracten met Golfstaten te kunnen afsluiten.

Het tweede paradigma bevat twee enigszins tegenstrijdige moral manoeuvres gekoppeld aan mensenrechten en 'targeted surveillance'. Mensenrechtenorganisaties geven aan dat het gebruik van *surveillance* softwareschendingen van mensenrechten oplevert. Daar staat tegenover dat softwarebedrijven (zoals de NSO Group, bekend van de Pegasus software) gerichte surveillance juist als een vorm van cybersecurity betitelen, omdat het een emancipe-rende werking zou hebben. Het waarborgen van veiligheid is niet langer een machts- en repressiemiddel van de staat, want met gerichte surveillance kan een burgercollectief of een organisatie als Bellingcat of CitizenLab ook de staat in de gaten houden. Zowel mensenrechtenorganisaties als softwarebedrijven gebruiken het mensenrechtenparadigma om meer aandacht en invloed te krijgen.

Informatiecontrole is de derde vorm van cybersecurity. Ging het vorige paradigma vooral over het gericht inbreken en/of meekijken in ICT-systemen, hier gaat het om de controle over digitale informatiestromen. De combinatie van regelgeving van socialemediaplatforms en van de staten levert voor de burger echter een onwenselijke situatie op. Immers, socialemediaplatforms (bijvoorbeeld Facebook) stimuleren het delen van data, omdat persoonlijke data en surfgedrag rendabele handelswaar is. Staten daarentegen eigenen zich het recht toe om data op grote schaal te monitoren en te filteren op specifieke (strafbare of ideologisch ongewenste) content. Deze trends versterken elkaar en zijn ongunstig voor de burger, zeker als de staat geen kritiek of vrije meningsuiting duldt. Onder het mom van cybersecurity verschuift zo de regulering van informatie van socialemediaplatforms naar het controleren van de eigen burgers door de staat, zeker in meer autoritaire systemen.

Cybersecurity is niet alleen te gebruiken om je te wapenen tegen een interne dreiging – en dus het controleren van de eigen burgers. Cybersecurity behelst ook het beschermen tegen kwaadwillende invloed van buiten, ook door rivaliserende staten. Shires behandelt drie technieken van buitenlandse inmenging: het lekken van data, desinformatie, en controle over mediabedrijven. Lekken van data, zoals ook tijdens de Amerikaanse verkiezingen van 2016 (#DCLeaks), is niet direct aan te duiden als een ontwrichting van de nationale veiligheid. Dit is wel het geval als een staat informatie lekt over dissidenten, diaspora of de gezaghebbende media in andere staten.

De vraag is verder of desinformatie – 'false, inacurate or misleading information designed, presented and promoted to intentionally cause public harm or for profit'[1] – propaganda is en een discours over tegengestelde waarheden, of dat het deel uitmaakt van *information warfare* en daarmee een cybersecurity-vraagstuk is. In zijn Cyber Security Assessment van 2019 volgt Nederland de laatste rationale.[2] Tot slot: in autoritaire systemen vallen mediabedrijven vaak onder toezicht van de staat. Al Jazeera (Qatar) is daardoor in Egypte en Saoedi-Arabië geboycot, uit vrees dat het een satelliet van buitenlandse staatsinvloed is; soortgelijke overwegingen gelden voor het Russische RT of Sputnik. Het toewijzen van uitzendrechten of overname van mediabedrijven is daarmee een veiligheidsvraagstuk en onderdeel van cybersecurity tegen 'foreign interferences'.

'People do use cybersecurity with different meanings in mind'.[3] Dit geeft de kern van het boek van Shires goed weer. Hij maakt expliciet wat we impliciet wel weten: het betitelen van trend, thema of ontwikkeling als een cybersecurity-vraagstuk is niet waardenvrij. Want zelfs als een actie gebracht wordt als een *normative action* in het algemeen belang, is het goed mogelijk dat deze moral manoeuvre eigenlijk een *strategic action* met een hoge mate van eigenbelang is. ■

Kol. dr. B.M.J. Pijpers, NLDA

1 European Comission, High Level Group on Fake News and Online Disinformation 'A Multi-Dimensional Approach to Disinformation' (2018).
2 Netherlands National Cyber Security Centre, 'Cyber Security Assessment Netherlands – CSAN 2019' (2019).
3 Shires, *The Politics of Cybersecurity in the Middle East*, 198-199. Shires parafraseert hier een van de geïnterviewden.