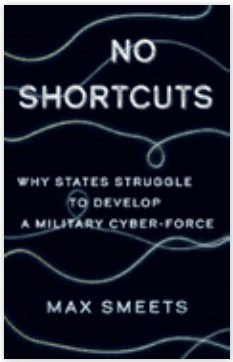

No Shortcuts

Why States Struggle to Develop a Military Cyber-Force
Door Max Smeets
Londen (Hurst) 2022
296 blz.
ISBN 9781787386877
€ 44,99

Rond 2010 zijn meerdere landen bezig met het vraagstuk 'hoe de staat te verdedigen tegen cyberdreigingen', maar ook over het zelf uitvoeren van cyberaanvallen. Maar behalve het Amerikaanse U.S. Cyber Command zijn het in die tijd vooral de inlichtingenorganisaties die zich bezighouden met operaties in cyberspace. In de daaropvolgende jaren richten veel landen separate Cyber Commando's op, zo ook Nederland – initieel met een Task Force Cyber (2012) en later in 2015 het Defensie Cyber Commando (DCC). Maar met een instellingsbeschikking, het inhuren van cybersecuritycursussen of het inschakelen van een pool aan cyberreservisten heb je nog geen offensieve cybercapaciteit; daar is een weloverwogen en zorgvuldig opgebouwd plan voor nodig. Er zijn, aldus Max Smeets in zijn recente boek, 'no shortcuts' om cybercapaciteit op te bouwen.

Aspiraties en middelen

Smeets is een Nederlandse cyberwetenschapper werkzaam bij de Eidgenössische Technische Hochschule in Zürich, directeur van het European Cyber Conflict Research Initiatief en daarnaast verbonden aan het Amerikaanse Stanford en het Britse RUSI. Smeets schreef al eerder over het DCC en ook in *No Shortcuts* is Nederland een van de casestudies. In zijn boek analyseert Smeets diverse cyber commands door statelijke cyberaspiraties af te meten aan de beschikbare middelen en de (opgelegde) operationele beperkingen (blz. 51 e.v.). Sommige landen hebben veel middelen, maar zijn mede door juridische en ethische kaders (zoals Amerika tot 2018 toen een nieuwe cyberwetgeving is aangenomen) beperkt in hun optreden.[1] Andere landen, zoals Rusland, zijn dat niet (type I). Noord-Korea (type II) laat zien dat een actor met weinig middelen nog steeds ellende kan veroorzaken als restricties niet gelden (zie figuur 1). In geval van pech zijn zowel de middelen als het raamwerk waarbinnen optreden mogelijk is beperkt: een zogeheten Paper Tiger, waar niet alleen Nederland, maar ook vele andere Europese cyber commands onder vallen.

Een staat kan enkel strategische waarde hebben ofwel een strategisch effect genereren met een cyber command als de operationele beperkingen niet te groot zijn. Dat betekent dat type III- en IV-staten dus niet in staat zijn strategische effecten te genereren (blz. 74).
Als een staat actief en effectief wil zijn in cyberspace en offensieve acties wenst uit te voeren zal hij met vijf elementen rekening moeten houden. Ten eerste personeel – voor Smeets het belangrijkste element – waarbij het niet alleen gaat om hackers, maar juist ook om taalwetenschappers, ontwikkelaars, juristen en strategen. Om effectief te zijn heeft een staat ook zogeheten *cyberexploits* nodig. Een exploit is software die gebruik kan maken van fouten in programmatuur. De

1 U.S. House of Representatives, 'John S. McCain National Defense Authorization Act (NDAA)', *Congressional Records* 164, No. 1 (2018) 1636-2423.

		Operationele beperkingen	
		Hoog	Laag
Beschikbare middelen	Hoog	Type III Gentle Giant	Type I Loose Cannon
	Laag	Type IV Paper Tiger	Type II Troublemaker

Figuur 1 Typologie cyberactoren (bron: Smeets, No Shortcuts)

exploit werkt slechts tot het moment waarop een ICT-bedrijf een software-update aanbiedt. Bij de Stuxnet-operatie in 2010 zijn (minimaal) vier exploits gebruikt. Volgens Smeets ligt er te veel nadruk op het bezit en de handel in exploits; het gaat immers om het samenspel tussen de vijf elementen en vooral het cognitieve vernuft van de menselijke gebruikers. Tools zijn – ten derde – ondersteunende softwareprogramma's die nodig zijn om een exploit uit te buiten. Veelal zijn dit bestaande programma's – of de programma's die door de opponent worden gebruikt – om onontdekt te blijven. Om een actie uit te kunnen voeren is een goede infrastructuur nodig tijdens de operatie zelf, maar bovenal in de voorbereiding ervan, denk aan een gesimuleerde internetomgeving of *cyber battlespace*. Tot slot dient de staat al deze elementen organisatorisch goed in te bedden. Een cyber command kan personeel wel werven, maar als er geen structuur is om hen te behouden, te stimuleren of te laten groeien neemt de effectiviteit snel af.

Smeets zet deze denktrant voort als hij de lezer meeneemt naar het vraagstuk over wapenhandel of het beperken van de proliferatie van cybermiddelen. De analogie met nucleaire wapenbeperking of conventionele wapenhandel gaat daarbij mank. Wat is immers 'handelswaar' in cyberspace? Smeets geeft ook hierbij aan dat het niet om 'cyberwapens' zoals payload of exploits gaat, maar om het verkrijgen en behouden van kennis en vaardigheden van cyberexperts, van mensen. Een interessante observatie is dat een offensieve actie van land A (neem Rusland) tegenover land B (Oekraïne) onbedoeld een overdracht van kennis is. Door de offensieve Russische acties sinds 2014 te analyseren komen de Oekraïners er immers achter wat de wijze van optreden en gebruikte vaardigheden zijn, waardoor het defensief in te richten is; een van de oorzaken van de sterke Oekraïense cyberdefensie op dit moment.

Papieren tijger DCC

Wetenschappelijke literatuur over (activiteiten in) cyberspace grijpt vaak terug op bestaande theorie uit het recht, internationale betrekkingen of bestuurskunde. Smeets doet een zeer verdienstelijke aanzet tot theorievorming vanuit cyberspace zelf; sterker nog, hij laat met zijn denken over het overdragen van kennis en vaardigheden zien dat het klakkeloos overnemen van denkbeelden uit de fysieke wereld eerder een valkuil dan een uitkomst is. Alleen al hierom is *No Shortcuts* een lezenswaardig boek. Maar wat het voor Nederland nog interessanter maakt is dat Smeets de Nederlandse case (inclusief het DCC) gebruikt in zijn vergelijkende onderzoek naar capaciteiten en beperkingen van landen, daar waar de focus toch vaak op de VS, Rusland, China of Noord-Korea ligt. Smeets geeft in zijn onderzoek aan dat cyberspace geen *level playing field* is. De cyberpikorde in staten wordt bepaald door beschikbare middelen, maar ook door de aanwezigheid van of het gemis aan een strategische visie, operationele capaciteiten en bovenal door al dan niet zelfopgelegde juridische en ethische beperkingen. Zo ook voor het DCC, want dat heeft een taak toegewezen gekregen tijdens het (gewapende) conflict. Dit mandaat staat in schril contrast tot de beperkingen buiten dat conflict. Smeets legt hier de vinger op de zere plek: het DCC kan en mag zich niet voorbereiden op een inzet omdat er buiten het (gewapende) conflict geen juridisch raamwerk is. Het DCC kan in de gereedstellingsfase niet oefenen en geen mensen stimuleren en uitdagen. Combineren we dit met Smeets' argument dat mensen de primaire kracht van een cyber command zijn, dan heeft het DCC geen mogelijkheden om personeel te behouden, en zonder opgeleid en gemotiveerd personeel blijft het commando een papieren tijger.

Kol dr. Peter Pijpers, NLDA ■