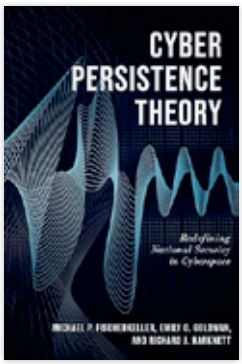


## Cyber Persistence Theory

Redefining National Security in Cyberspace
Door Michael P. Fischerkeller, Emily O. Goldman en Richard J. Harknett
Oxford (Oxford University Press) 2022
266 blz.
ISBN 9780197638255
€ 56,-

De drie auteurs van *Cyber Persistence Theory* weten waarover ze het hebben. Richard Harknett, hoogleraar aan de universiteit van Cincinnati, is een bekend cyberauteur en voormalig US CYBERCOM *scholar-in-residence*. Emily Goldman werkt als strategisch adviseur voor US Cyber Command en was verantwoordelijk voor de US CYBERCOM-visie 2018. En Michael Fischerkeller is IT-onderzoeker bij het Institute of Defense Analysis (IDA), een onderzoeksinstituut gelieerd aan het Pentagon. Samen zijn zij de grondleggers geweest van de *persistent engagement*-strategie van US CYBERCOM sinds 2016.

Al in het eerste introducerende hoofdstuk doen de auteurs hun theorie op hoofdlijnen uit de doeken. Hier bekritiseren ze het heersende paradigma over gewapend conflict, met sleuteltermen als *coercion* (afdwinging) en *deterrence* (afschrikking). Termen die volgens hen in de weg hebben gestaan van een goed begrip van cyberspace. De kern van hun betoog is dat cyberspace moet worden gezien als 'a third strategic environment' met unieke structurele kenmerken, waardoor staten zich er anders gedragen dan in het conventionele en/of nucleaire domein. Conventioneel, nucleair én cyber dus als onderscheiden, maar tevens onderling verbonden handelingsruimtes voor staten om strategische effecten te sorteren: 'States must manage all three of these strategic environments simultaneously…' (blz. 8).

### Cyber als hoofdtoneel

In cyberspace zijn staten er vooral en voortdurend op uit langs digitale weg kwetsbaarheden uit te buiten om strategische voordelen te behalen zonder de drempel van gewapend conflict te overschrijden. 'Each intrusion, hack, or technical action – although not strategically consequential on its own – often cumulatively results in effects that, in past generations, required armed conflict or a threat thereof' (blz. 7). En: 'Whereas security requires states to triumph in war in the conventional environment and avoid war in the nuclear environment, states in the cyber strategic environment may have a true alternative through which to achieve strategically relevant outcomes' (blz 157). Een alternatieve mogelijkheid voor staten derhalve om geopolitieke doelstellingen te bereiken zonder de intrinsieke prikkel – zowel positief als negatief – om door middel van internationale diplomatie tot bilaterale en/of multilaterale samenwerking te komen. Dit gebrek aan internationale coöperatie leidt tot voortdurende competitie tussen landen. Cyberspace is om die reden allang geen zijtoneel meer van de strategische competitie tussen staten, maar volgens de auteurs gepromoveerd tot het hoofdtoneel van deze wedijver: 'Exploitation of cyberspace vulnerabilities and opportunities and not coercion is the primary route toward gain' (blz. 7).

Het gebrek aan een goed begrip van de dynamiek in cyberspace heeft er toe geleid dat veel staten de militaire logica van afschrikken en afdwingen zijn blijven toepassen op een domein dat zich daar niet voor leent. De mogelijkheden van het internet komen slecht overeen met ambities ten aanzien van territoriale verovering en/of afdwinging. Zoals in de eerste bladzijden wordt opgemerkt: 'Cyber 'war' is not likely to serve as the final arbiter of competition in an anarchical world…' (blz. 5). Dit betekent ook dat cyber war niet in de plaats zal komen van conventionele oorlogvoering, ook al voegen cyberoperaties daaraan een belangrijke dimensie toe. De Russische aanval op Oekraïne in 2022 en de huidige oorlog tussen Israël en Hamas lijken het gelijk van de auteurs te bevestigen. Ook in oorlogstijd klopt de stelling dat cyberspace hoofdzakelijk als een exploitatiedomein moet worden begrepen, waarbij statelijke en mogelijk ook niet-statelijke activiteiten in cyberspace onderdeel worden van een politieke en militaire strategie gericht op afdwinging.

### Relevante eenheid van analyse

De drie auteurs hebben, zoals gezegd, een theorie ontwikkeld om

bij te dragen aan een beter begrip van en effectievere strategie in het cyberdomein: de cyber persistence theory. In plaats van afschrikking en afdwinging gaat het volgens de auteurs in cyberspace in de eerste plaats om 'persistence in seizing and maintaining the initiative to set the conditions of security in and through cyberspace in one's favor' (blz. 56). In het belang van digitale veiligheid pleiten zij in het verlengde daarvan voor nieuwe strategieën van volharding die tot uiting komen in de noodzaak tot het creëren van een *campaign mindset* waarbij de autonome handelingsruimte van de tegenstander moet worden ingeperkt. Omgekeerd moet ook het gedrag van de opponent door de lens van langdurige 'campagnes' worden beschouwd in plaats van individuele hacks of losstaande cyberincidenten. De geplande 'campagne' is volgens de auteurs dé relevante eenheid van analyse. Kortom, proactief handelende en initiatiefrijke actoren zijn in het digitale domein een voorwaarde voor veiligheid en stabiliteit (blz. 122-123). Na de eerste vier conceptuele hoofdstukken illustreren de auteurs dit aan de hand van diverse reële casus, waaronder Amerikaanse cyberoperaties tegen de online propaganda-activiteiten van IS, Russische beïnvloeding en ondermijning van Amerikaanse digitale netwerken en Chinese compromittatie van veelgebruikte software als Microsoft en Adobe door middel van de exploitatie van *zero days*, oftewel voorheen onbekende digitale kwetsbaarheden.

**Levensvatbare beleidsopties**

Al met al is *Cyber Persistence Theory*, voorzien van een omvangrijk notenapparaat, een indrukwekkende poging om een nieuw theoretisch kader te creëren dat de alledaagse werkelijkheid in cyberspace kan bevatten. Cyberspace wordt vaak geschaard onder het bredere begrip *grey zone* – het schemergebied tussen oorlog en vrede – waarin sprake is van openlijke en heimelijke strategische beïnvloeding in tal van dimensies. Polemologen hanteren daarvoor ook wel het concept van 'negatieve vrede'; de afwezigheid van oorlog zonder dat van een duurzame vrede kan worden gesproken. Fischerkeller, Goldman en Harknett voegen daaraan een nieuw en relevant vocabulaire toe. Op deze conceptuele kracht kan en moet worden voortgebouwd als het gaat om het ontwikkelen van levensvatbare beleidsopties ten aanzien van het relatief nieuwe cyberdomein. De auteurs begeven zich in deze publicatie niet op dit pad. Zij komen niet verder dan de voorzichtige aansporing om het vigerende internationale recht aan te passen en te komen tot heldere definiëring van verantwoordelijk statelijk gedrag en onrechtmatige daden in het cyberdomein. In de huidige onzekere dynamische geopolitieke constellatie en veiligheidssituatie volstaat het niet om te zeggen dat afschrikking en afdwinging niet meer werken en het vervolgens daarbij te laten. Op basis van het aangereikte theoretische instrumentarium zullen anderen de vertaalslag naar de weerbarstige praktijk moeten maken. Een ware uitdaging, die hopelijk binnen afzienbare tijd zal worden opgepakt. ■

*Dr. S. Reyn en dr. A. Claver, ministerie van Defensie*