Cyberspace

**Lillian Ablon/Anika Binnendijk/Quentin E. Hodgson/
Bilyana Lilly/Sasha Romanosky/David Senty/Julia
A. Thompson:** Operationalizing Cyberspace as a Military
Domain. Santa Monica, Cal.: RAND Corp., Juni 2019

Besprochen von **Dennis G. Hennecken**, Mitglied im
Arbeitskreis Junge Sicherheitspolitiker der BAKS

<https://doi.org/10.1515/sirius-2020-2026>

Die Autoren beschreiben in ihrer Studie den Weg zur Operationalisierung des Cyberspace in drei Schritten. Zunächst analysieren sie aus der NATO Vergangenheit heraus, wie die NATO auf neue Herausforderungen reagiert hat. Anschließend besprechen sie, inwiefern die NATO zum jetzigen Zeitpunkt die Integration des Cyberspace als operationelle Domäne umgesetzt hat. Schließlich wollen die Autoren anhand einer Fähigkeit, *indications and warning* (I&W), aufzeigen, wie die NATO eine effektive militärische Präsenz im Cyberspace aufbauen und gewährleisten könne.

Bei der Analyse der NATO Vergangenheit fokussieren sich die Autoren auf die Reaktion auf chemische, biologische, radioaktive und nukleare Bedrohungen (CBRN). Ausgangspunkt des Fähigkeitsaufbaus sei hierbei die Aufstellung eines graduellen Entwicklungskonzeptes und dessen schnelle Umsetzung gewesen. Begleitet worden sei dies durch ein robustes Programm an Übungen. Ein weiterer Faktor sei der Ausbau der gezielten Nutzung von Expertise in Schlüsselstaaten gewesen, die nicht nur eigene Experten zur Verfügung gestellt, sondern ihr Wissen innerhalb der NATO auch weitergegeben hätten. Schließlich habe die Integration von CBRN in die NATO Doktrinen und den Planungsprozess die Anstrengungen abgerundet. Die Autoren kommen zu dem Ergebnis, dass die aufgezeigte Entwicklung zu CBRN als Blaupause für eine Reaktion auf Fähigkeitslücken im Cyberspace genutzt werden könne. Der Cyberspace sei zudem keine geographische, sondern eine technische Domäne.

In der Analyse des IST-Zustands der Implementierung von Cyber in der NATO zeigen die Autoren auf, dass bereits zahlreiche Nationen sich die Stärkung ihrer eigenen Cyberfähigkeiten vorgenommen hätten, sowohl im privaten wie im öffentlichen Sektor. Wichtig sei es, sich zunächst der Hauptfunktionen der NATO zu vergewissern, welche für das Operieren und Verteidigen im Cyberspace notwendig sind. Das bedeute, dass die NATO den Cyberspace in ihre strategische und operationelle Planung einbinden müsse. Hierzu sei es notwendig, *command and control* über Cybertruppen in *joint operations* zu üben. Allerdings müsse zuerst ein gemeinsamer Grundstandard für Cyber-

sicherheit innerhalb der NATO etabliert werden. Dies sei wichtig, da jede Nation für ihre Ausrüstung selbst verantwortlich zeichne und dafür bedarf es gemeinsamer Standards. Als nächstes müsse geklärt werden, wie weit die Aufgaben der NATO reichen. Solle sie nur das Monitoring des NATO Netzwerkes betreiben, oder auch der Netzwerke aller NATO Staaten überprüfen?

Die Verfasser weisen darauf hin, dass sich die Integration von Cyber in den Planungsprozess von Operationen schwierig gestalte. Ursache seien die Diversität und der hohe Geheimhaltungsgrad im Bereich der Cyberfähigkeiten. Das kontinuierliche Training und Inübenhalten sei ein weiterer Schritt, um Cyber in NATO Operationen zu integrieren und bei den Planern ins Bewusstsein zu rufen. Es gäbe bereits zahlreiche Formate in denen Cyber beübt werde, sodass hier weiter angesetzt werden solle. In Frage käme etwa die erweiterte Bereitstellung einer NATO Cyber Range, wobei abzuwägen sei, ob diese sich auf einen kommerziellen Anbieter abstützen solle oder ob die NATO diese besser selbst betreibt. Am Beispiel der USA und deren derzeitigen Pilotprojekten mit der Integration von Cyberpersonal zeigen die Autoren auf, dass sich der Integrationsprozess stetig weiterentwickle. Schließlich sei Personal ein wichtiges Element. Dabei komme es darauf an, dass das ausgewählte Personal nicht nur die technischen Aspekte des Cyberspace verstehe, sondern auch wie es zum Gelingen von NATO Operationen beitragen kann.

Im letzten Schritt legen die Autoren anhand I&W dar, inwieweit Cyber Bedrohungen durch die NATO begegnet werden kann. Die Autoren statuieren, dass die NATO mit ihrem I&W System über ein funktionierendes System verfügt, welches für Bedrohungen des Cyberspace nutzbar gemacht werden kann. Sie wandeln dabei das I&W Modell von INSA für den Cyberspace ab. Dieses müsse schrittweise aufgebaut werden: Schritt 1 sei die Identifizierung und Priorisierung von missionskritischen Assets; Schritt 2 das Aufstellen und Aktualisieren einer Liste mit den Haupt-Cyberbedrohungen; Schritt 3 die Konstruktion von Szenarien mit dem Potential für Cyberattacken; Schritt 4 die Umwandlung der Szenarien in überwachbare Indikatoren; Schritt 5 die Einrichtung von Datenerfassungsmethoden und das Definieren von Informationsbedarfen; und schließlich Schritt 6 die Festlegung von *standard operating procedures* und das Üben von Befehlsketten unter verschiedenen Szenarien. Sie kommen dabei zu dem Ergebnis, dass die NATO über einen sehr robusten Ansatz für *situational awarness* verfügt, weshalb sie die tiefergehende Integration von Cyberspace in diesen Ansatz empfehlen.

Insgesamt zeigen die Autoren auf, dass die NATO mit den bereits zur Verfügung stehenden Instrumentarien eine wirksame Implementierung des Cyberspace als operationelle Domäne erreichen kann.

<https://www.rand.org/pubs/perspectives/PE329.html>