WARUM SICH STAATEN SCHWER TUN, EINE MILITÄRISCHE CYBER-TRUPPE AUFZUBAUEN

Von Max Smeets

Die Entwicklungen im Bereich der Cyberkonflikte sind rasant. Ein Grossteil der wissenschaftlichen Literatur setzt sich damit auseinander, ob Operationen im Cyberraum als Zwangsmittel eingesetzt, einen strategischen Vorteil erzeugen oder durch Normen beeinflusst werden können. Eine grundlegende Frage scheint die Wissenschaft indes weitgehend übersehen zu haben: Sind Staaten überhaupt in der Lage, Cyber-Operationen durchzuführen? Das vor Kurzem erschienene und an der ETH vorgestellte Buch *No Shortcuts: Why States Struggle to Develop a Military Cyber Force* soll diese Lücke füllen.

Der Band bietet zunächst einen empirischen Überblick darüber, welche Entwicklungen Staaten im Cyberbereich gemacht haben. Zu Beginn des dritten Jahrzehnts des 21. Jahrhunderts scheinen sich die Risiken radikal zu verändern. Staaten erkennen den Cyberraum weithin als neue «Kriegsführungsdomäne» an und der «Cyber-Klub» verliert die Exklusivität der frühen 2000er-Jahre. Es ist inzwischen öffentlich bekannt, dass über vierzig Staaten ein militärisches Cyberkommando oder ähnliche Strukturen eingerichtet haben. Gleichzeitig bleibt aber auch vieles beim Alten. Es gibt eine grosse Diskrepanz zwischen der relativ grossen Anzahl an Staaten, die derartige Einheiten eingerichtet haben und der nach wie vor geringen Anzahl an Staaten, die tatsächlich Cyberoperationen mit dem Ziel der Störung, Verleugnung, Beeinträchtigung oder Zerstörung (dem Erzielen einer konkreten Wirkung) durchzuführen imstande sind.

Im Buch wird einleitend aufgezeigt, dass viele Länder, die ein Cyberkommando oder ähnliche Strukturen eingerichtet haben, kaum in der Lage sind, eine effektive militärische Cyberstreitmacht aufzustellen. Es gilt zwar als relativ einfach, zu einem beliebigen Zeitpunkt und ohne strategischen Zweck irgendeinen Cyber-Effekt gegen irgendein System oder Computernetz zu verursachen. Die Verursachung eines präzisen Cyber-Effekts zu einem bestimmten Zeitpunkt, der keine oder

nur geringe unerwünschte Folgen hat und einen spezifischen strategischen Zweck verfolgt, ist hingegen schwierig. Während verschiedene Staaten unter unterschiedlichen rechtlichen, politischen und operativen Zwängen operieren, versuchen die meisten Staaten, welche ein Cyberkommando eingerichtet haben, die zweite Art von Operationen durchzuführen.

Weiter bietet das Buch einen konzeptionellen Rahmen für das Verständnis der Anforderungen eines Staates an die Schaffung und Aufrechterhaltung der Fähigkeit zur Durchführung von Operationen mit Cybereffekten. Der vorgeschlagene Rahmen unterscheidet zwischen fünf Dimensionen: Personen, Schwachstellen, Instrumente, Infrastruktur und Organisation (auf Englisch: *People, Exploits, Tools, Infrastructure, and Organization*).

Durch die Einführung dieses konzeptionellen Rahmens wird argumentiert, dass Organisationen, die Cyber-Operationen mit einem gezielten Effekt durchführen wollen, eine vielfältigere Belegschaft benötigen, als dies oft vermutet wird. Für die Entwicklung einer offensiven Cyber-Fähigkeit sind nicht nur technisch versierte Personen erforderlich, die Schwachstellen suchen und Instrumente entwickeln, sondern auch andere Fachkräfte wie unter anderem LinguistenInnen, AnalystenInnen, ZielsucherInnen, StrategenInnen, RechtsexpertenInnen und einsatzspezifische BeraterInnen. Was die Instrumente und Schwachstellen betrifft, so wurde viel Aufmerksamkeit auf die Anhäufung von sogenannten *Zero-Day-Exploits* und die Entwicklung massgeschneiderter Instrumente durch Staaten gerichtet. In Wirklichkeit können aber auch bereits bekannte Schwachstellen und Instrumente oft sehr effektiv genutzt werden. Die wichtigste Voraussetzung dabei ist, dass der Angreifer die Zielsysteme und -netze genau kennt und weiss, wie sich die von ihm eingesetzten Angriffsmöglichkeiten in dieser Umgebung verhalten. Investitionen in die Infrastruktur – für Zielsuche, Entwicklung, Tests und Schulung – sind eine weitere wesentliche Voraussetzung und können mit hohen Kosten verbunden sein. Schliesslich gibt es auch Kompromisse auf inter- und intra-organisatorischer Ebene. Die organisatorische Integration der militärischen und nachrichtendienstlichen Bemühungen eines Staates ist von entscheidender Bedeutung, um die Effektivität von Cyber-Operationen zu erhöhen, den Wissenstransfer zu verbessern und Überlappungen von Missionen zu verringern. Ein Risiko der organisa-

torischen Integration besteht jedoch darin, dass sie zum Verlust unterschiedlicher operativer Kulturen führen kann, wodurch die Grenze zwischen einer Cyberspionage-Operation und einer wirkungsorientierten Operation weiter verwischt und somit das Dilemma der Cybersicherheit noch verschärft wird. Innerhalb der Organisation müssen offensiv ausgerichtete Cyber-Einheiten einen ebenso schwierigen Balanceakt bewältigen. Einerseits müssen sie einen Weg finden, Routinen zu entwickeln, um die Stabilität zu gewährleisten und die Organisation verantwortungsvoll zu führen, andererseits sollten die Richtlinien es dem Einzelnen ermöglichen, nach eigenem Ermessen Anpassungen vorzunehmen, um die kreative Freiheit zu erhalten, die für Innovationen notwendig ist.

Im Anschluss daran, stellt das Buch Hypothesen darüber auf, wie Staaten ihre Kapazitäten effektiver aufbauen und inwieweit externe Akteure diesen Prozess beeinflussen können. Des Weiteren wird argumentiert, dass drei Komponenten – Lernen, Umfang und Technologie – die Effektivität der Entwicklung und des Einsatzes von Cyberoffensiven verbessern können. Dem steht jedoch der Vorbehalt gegenüber, dass Staaten in der Regel mit einer Reihe von Hindernissen konfrontiert sind, wenn es darum geht, eine offensive Cyberfähigkeit zu optimieren. So ist es für Regierungen nach wie vor schwierig, qualifiziertes und geschultes Personal zu rekrutieren – und vor allem zu halten. Dies bedeutet, dass staatliche Cyber-Einheiten Mühe haben können, ihr institutionelles *Know-how* aufrechtzuerhalten.

No Shortcuts wurde daher mit dem Ziel geschrieben, nicht nur eine wichtige Lücke in der akademischen Literatur zu schliessen, sondern den Lesenden auch Einblicke in wichtige cyberpolitische Fragen zu geben – zum Beispiel über die Militarisierung des Cyberraums, die Grenzen der internationalen Zusammenarbeit, die Durchführbarkeit von Rüstungskontrollinitiativen und die langfristige Zukunft der internationalen Sicherheit. Das Buch stützt sich in erster Linie auf die Literatur aus dem Bereich der internationalen Beziehungen. Erkenntnisse aus anderen Bereichen – wie Unternehmensstrategie und Organisationsmanagement – wurden allerdings ebenfalls herangezogen. Entsprechend bedient sich *No Shortcuts* eines interdisziplinären Ansatzes, um die institutionellen Entwicklungen von Staaten im Cyberbereich zu verstehen.

Letztendlich soll *No Shortcuts* eine nützliche Ressource für Studierende, politische EntscheidungsträgerInnen und militärische Führungs-

kräfte gleichermassen darstellen. Das in dieser Publikation enthaltene Material wurde vom Autoren unter anderem als Grundlage für den Unterricht an der Stanford University, der NATO-Verteidigungsakademie sowie für den Unterricht im Rahmen des ETH-Masterstudiengangs in *Comparative and International Studies* (MACIS) verwendet.