FORSCHUNGS- UND BERATUNGSLEISTUNGEN FÜR DIE ARMEE IM BEREICH CYBERDEFENSE

Von Myriam Dunn Cavelty und Andreas Wenger

Cybervorfälle mit unangenehmen Konsequenzen für einzelne Firmen oder Regierungseinheiten sind weltweit keine Seltenheit mehr. Viele der Cyberattacken sind ausgetüftelter, kostspieliger und gravierender als früher. Eine wichtige Ursache für diese Entwicklung ist die Professionalisierung der Angreifer. Hinzu kommen die anhaltende Digitalisierung und die wachsende Verwundbarkeit der Informationsinfrastrukturen.

Seit einigen Jahren ist bekannt, dass auch staatliche Akteure vermehrt in Cyberaktivitäten strategischer Natur verwickelt sind. Diese Tätigkeiten reichen von Spionage mittels ausgeklügelter Schadsoftware für politische und wirtschaftliche Zwecke über die Entwicklung von «Cyberwaffen» bis hin zu koordinierten Störaktionen «gegnerischer» Webdienste. Meistens können die entsprechenden Akteure ihre Urheberschaft verbergen, weil die Involvierung von Staaten oder patriotischen Hackergruppen in Cyberangriffe schwer nachweisbar ist.

Aufgrund der globalen Natur des Cyberraums ist kein Staat vor diesen Entwicklungen gefeit. Es stellt sich daher auch für die Schweiz die Frage, welche strategischen Entscheide in Bezug auf Verteidigungskonzepte, aber auch auf Angriffsmöglichkeiten zum Beispiel in Kriegszeiten gefällt und welche Arten von Kapazitäten aufgebaut werden sollen. Vor allem: Wie soll die Zusammenarbeit zwischen staatlichen Stellen und Wirtschaft und gegebenenfalls der Zivilgesellschaft strukturiert werden?

CYBERSICHERHEIT IN DER SCHWEIZ

Die Schweiz hat seit 2012 eine nationale Cyberstrategie: die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken, kurz «NCS» genannt.[1] Damit will der Bundesrat in Zusammenarbeit mit anderen Be-

1 Bundesrat, *Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS),* Bern, 27.6.2012; Eidgenössisches Finanzdepartement, *Umsetzungsplan NCS,* Bern, 15.5.2013.

hörden, den Betreibern kritischer Infrastrukturen und der Wirtschaft die Cyberrisiken für die Schweiz minimieren. Die Strategie soll helfen, folgende Ziele zu erreichen: 1) Bedrohungen und Gefahren im Cyberbereich frühzeitig zu erkennen; 2) die Widerstandsfähigkeit von kritischen Infrastrukturen, inklusive der Verwaltungen, zu steigern; 3) Cyberspionage, Cybersabotage und Cyberkriminalität wirkungsvoll zu reduzieren.

Dabei schliesst die NCS den Kriegs- und Konfliktfall explizit aus. Für die Armee wird darin aber ein Teilauftrag formuliert: Sie soll die eigene Einsatzfähigkeit und Handlungsfreiheit über alle Lagen permanent gewährleisten können. Dazu gehören in erster Linie effektive Massnahmen zugunsten der eigenen Informations- und Kommunikationstechnologie (IKT)-Systeme und -Infrastruktur. Darüber hinaus definieren die Strategie und der dazugehörige Umsetzungsplan zwei weitere Aufgaben für die Armee: Erstens erwarten die zivilen Behörden subsidiäre Hilfeleistungen zum Schutz kritischer Infrastrukturen. Zweitens soll die Armee in einem Konflikt- und Kriegsfall die Führung in der Krise mit ausfallsresistenten Infrastrukturen sicherstellen.

Die Schweizer Cyberstrategie schliesst den Kriegs- und Konfliktfall explizit aus.

Einerseits stellen damit zielführende Operationen im Cyberraum, um militärischen Gegnern die Nutzung des Cyberraums zu erschweren oder gar zu verwehren, eine zwingende Fähigkeit der Armee dar. Andererseits soll die Armee, ähnlich wie die Rettungstruppen, Leistungen zugunsten der Wirtschaft und Gesellschaft erbringen, wobei diese Leistungen sicherheitspolitisch bisher unpräzis formuliert sind. Damit ein spezifisch auf die Schweiz zugeschnittenes Cyberdefense-Konzept (Cyberverteidigungskonzept) erarbeitet werden kann, hat der Chef der Armee einen Delegierten Cyberdefence der Armee per Anfang 2013 ernannt.

CYBERSICHERHEITSFORSCHUNG AM CSS

Seit rund 20 Jahren beobachtet das Center for Security Studies (CSS) der ETH Zürich nationale und internationale sicherheitspolitische Entwicklungen im Bereich der Cybersicherheit. Es hat eine Vielzahl von wissenschaftlichen und praxisorientierten Studien in diesem Fachge-

biet publiziert.[2] Ebenso hat das CSS Workshops und Konferenzen organisiert, an denen sich nationale und internationale Fachexperten gewinnbringend über Cyberthemen ausgetauscht haben.[3] Das CSS hat sich dadurch als sicherheitspolitisches Kompetenzzentrum mit Expertise im Bereich Schutz kritischer Informationsinfrastrukturen und Cybersicherheit national und international etabliert und ein ausgedehntes Expertennetzwerk in zahlreichen Ländern aufgebaut.

Aufgrund dieser Expertise haben der Führungsstab der Schweizer Armee, die Führungsunterstützungsbasis der Armee und das CSS beschlossen, eine längerfristige Zusammenarbeit spezifisch für den Bereich der Cyberverteidigung aufzubauen. Durch eine Serie von Unterstützungsleistungen in den nächsten vier Jahren wird das CSS dazu beitragen, dass die Armee die in der NCS-Strategie formulierten Ziele erreichen kann. Dabei wird es sich um Unterstützung vor allem bei der Bearbeitung von spezifischen sozialwissenschaftlichen, sicherheits- und verteidigungspolitischen und risikorelevanten Fragestellungen sowie bei der Ausarbeitung von damit zusammenhängenden Ausbildungs- und Übungsinhalten handeln. Ein zentraler Punkt wird sein, gewonnenes Wissen mittels geeigneter Ausbildungssequenzen bei den relevanten Entscheidungsträgern und Interessenvertretern zu verankern.

DIE ZUSAMMENARBEIT

Um ihre Einsatzfähigkeit und Handlungsfreiheit jederzeit und über alle Lagen sicherzustellen, will die Schweizer Armee permanent Cyberbedrohungen erkennen, sich vor Angriffen schützen und diese abwehren können. Zu diesem Zweck muss die Armee neben Führungs-, Präventions- und Reaktionsfähigkeiten auch über Antizipationsfähigkeiten verfügen: Entwicklungstendenzen, Bedrohungen und Verwundbarkeiten im Cyberraum sollen frühzeitig erkannt werden. Die Zusammenarbeit zwischen Führungsstab und CSS umfasst Produkte in fünf Bereichen, die diesen Fähigkeiten dienen werden:

2 Thierry Balzacq / Myriam Dunn Cavelty, «A Theory of Actor-network for Cyber-security», in: *European Journal of International Security* Nr. 1/2 (2016), 176–198; Myriam Dunn Cavelty, *Cybersecurity in Switzerland, Springer Brief* (Berlin: Springer, 2014); dies., «A Resilient Europe for an Open, Safe, and Secure Cyberspace», in: *UI Occasional Papers* Nr. 23 (2013).

3 CSS Evening Talk, *Brauchen wir eine Cyber Grand Strategy?,* ETH Zürich, 9.6.2016.

Allgemeine und sektorielle Trendanalysen: Aktuelle und relevante sicherheits- und militärpolitische Themen im Cyberraum werden systematisch aufgearbeitet und in thematischen Trendanalysen festgehalten und bewertet. Themen umfassen etwa die Entwicklungen und Konzeptionen von Cyberwaffen, Fragen von internationalen Normen und ihren Auswirkungen, technologische Entwicklungen allgemein sowie Entwicklungen der nachrichtendienstlichen Kultur.

Hot-Spot-Analysen: In Fallstudien sollen sicherheitspolitisch und militärisch relevante Cyberoperationen zusammengestellt werden, unter besonderer Berücksichtigung der involvierten Akteure, verwendeten Methoden und unterschiedlichen Auswirkungen (politisch, wirtschaftlich, gesellschaftlich, technologisch). Diese Fallstudien werden in einem zweiten Schritt analytisch ausgewertet, sodass Trends in Bezug auf Akteure, Angriffsmotive und Abwehrmassnahmen identifiziert werden können.

Best-Practice-Analysen: Eine Übersicht über militärische Cyberdefence-Dispositive und -Strategien soll erarbeitet werden. Diese Dispositive und Strategien werden anschliessend nach einheitlichen Kriterien ausgewertet, sodass ein Vergleich bezüglich Best Practices stattfinden kann.

Berichte zu Sensibilisierung und Ausbildung: Es werden Unterstützungsleistungen für die Ausbildung und Sensibilisierung im Bereich der militärischen Massnahmen im Cyberraum ausgeführt. In einem ersten Schritt werden zwei Berichte verfasst: 1) ein Bericht über existierende Sensibilisierungs- und Ausbildungskampagnen, unter Berücksichtigung der Form und der Effektivität dieser Kampagnen; 2) ein Bericht über existierende Cyberszenarien und War Games, unter Berücksichtigung der Inhalte und der verwendeten Methoden. Die Resultate dieser Berichte unterstützen die Erarbeitung relevanter und stufengerechter Ausbildungsinhalte und Szenarien für die Armee.

Dialog: Alle erarbeiteten Resultate dieser vier Teilaufträge werden in Seminaren und Workshops mit der Armee und weiteren relevanten Experten diskutiert, um einen optimalen Wissenstransfer sicherzustellen.

Die erarbeiteten Produkte werden der breiten Öffentlichkeit über die CSS-Webseite zur Verfügung stehen. Sie werden alle auf der Basis von öffentlich zugänglichen Informationen und von selbst durchgeführten Interviews gemäss wissenschaftlichen Recherchekriterien erstellt.