Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 186 (2020)

Heft: 7

Artikel: Die rechtlichen Aspekte der militärischen Cyber-Abwehr

Autor: Vögtlin, Jan E.

DOI: https://doi.org/10.5169/seals-905595

Die rechtlichen Aspekte der militärischen Cyber-Abwehr

Eine juristische Betrachtung eines militärischen Mittels unter Einbezug der spezifischen und allgemeinen nationalen rechtlichen Grundlagen.

Jan E. Vögtlin

Die Armee ist seit längerem in der Lage, einen Cyber-Angriff durchzuführen, es gab jedoch bis vor kurzem keine Rechtsgrundlage für eine solche Massnahme.[1] Diese Lücke füllend und den Gegebenheiten im sich rasch entwickelnden Umfeld von Informatik, Cyber und Cyber-Kriminalität Rechnung tragend, hat das Parlament, mit der Anpassung des Bundesgesetzes vom 18.03.2016 über die Militärverwaltung und die Armee (MG; SR 510.10), den Bundesrat beauftragt, die militärische Cyber-Abwehr zu definieren. Zu diesem Zweck wurde die Verordnung über die militärische Cyber-Abwehr (MCAV; SR 510.921) in Auftrag gegeben und schliesslich am 1. März 2019 durch den Bundesrat in Kraft gesetzt.

Cyber-Abwehr: so wichtig wie Luftraumverteidigung. Bild: nau.ch

Der vorliegende Artikel gibt einen Überblick über die MCAV als juristische Grundlage der militärischen Cyber-Abwehr und behandelt deren Anwendung.[2]

Einleitung

Die Bundesverfassung definiert die Aufträge für die Schweizer Armee klar und abschliessend. Die Armee dient der Kriegsverhinderung, der Friedensförderung und der Selbstverteidigung des Landes und der Bevölkerung. Weiter unterstützt die Schweizer Armee die zivilen Behörden bei der Bewältigung von ausserordentlichen Lagen zur Aufrechterhaltung der inneren Sicherheit.[3]

Zur Umsetzung der Selbstverteidigung definiert das MG die entsprechenden Kompetenzen und Grundlagen. Es werden unter anderem die verschiedenen Einsatzarten und die Ausbildung der Milizangehörigen definiert. Unter der militärischen Sicherheit gemäss Art. 100 MG findet sich die Grundlage für die militärische Cyber-Abwehr.[4]

Diese Norm beauftragt die zuständigen Stellen mit den wahrzunehmenden Massnahmen und somit die Militärverwaltung und die Armee zur Cyber-Abwehr.[5] Ebenfalls werden bereits Anforderungen wie auch Einschränkungen der Anwendbarkeit definiert.

Cyber-Abwehr ist folglich, juristisch betrachtet, die Konsequenz beziehungsweise die Ableitung, aus dem Auftrag der militärischen Sicherheit Angriffe gegen militärische Informationssysteme und Informatiknetzwerke abwehren und unterbinden zu können. Die militärische Cyber-Abwehr ist somit ein Teil des Eigenschutzes und der Selbstverteidigung. Keine militärische Planung, Operation oder Aktion findet heute ohne Informationssysteme statt, daher ist Cyber ein integraler Bestandteil militärischen Handelns. Daraus lässt sich folgern, dass Cyber einerseits ein weiteres militärisches Mittel zur Sicherstellung des Eigenschutzes und der Selbstverteidigung ist und andererseits die Operationssphäre Cyber eine weitere Dimension von militärischen Aktionen.[6]

Übersicht Verordnung über die militärische Cyber-Abwehr (MCAV)

Die MCAV regelt Massnahmen, die Zuständigkeiten zur Umsetzung von Massnahmen im Cyber-Raum, die Aufsicht über die zuständigen Stellen sowie die Forschung in diesem Bereich.[7] Konkret befasst sich die MCAV mit den zu ergreifenden Massnahmen nach einem Cyber-Angriff auf militärische Informationssysteme und Informatiknetzwerke im gesamten Auftragsspektrum der Armee.

Zu diesem Zweck werden bewilligungspflichtige und nicht-bewilligungspflichtige Massnahmen unterschieden (Art. 2 MCAV). Kern der Unterscheidung ist das Eindringen beziehungsweise Nicht-Eindringen[8] in fremde Computersysteme und Computernetzwerke.[9] Folglich unterscheidet der Bundesrat zwischen eigenen und fremden Computersystemen und -netzwerken, wobei ein Eindringen durch die Schweizer Armee in ihre eigene Anlagen nicht möglich ist beziehungsweise die Tathandlung nicht erfüllt wird (vgl. Fussnote 8). Sämtliche Massnahmen, in den eigenen Systemen und Netzwerken der Schweizer Armee, erfolgen in der Verantwortung des Chefs der Führungsunterstützungsbasis (FUB) und unterliegen daher keinen Restriktionen durch die MCAV. Exemplarisch handelt es sich dabei um die Überwachung der eigenen Systeme und Netzwerke und weitere vorsorgliche Massnahmen zur Erhöhung des Schutzes der Systeme und Netzwerke, jedoch auch um den Entscheid, den Zugang zu einem eigenen System oder Netzwerk zu trennen.[10]

«Die MCAV regelt die möglichen Massnahmen und Zuständigkeiten im Falle eines Angriffes auf militärische Informationssysteme und Informatiknetzwerke.»

Sollten demnach nicht-bewilligungspflichtige Massnahmen zur Bewältigung

eines Vorfalles oder Angriffes nicht mehr genügen, wird durch die FUB ein Antrag für eine bewilligungspflichtige Massnahme ausgearbeitet (Art. 3 MCAV i. V. m. Art. 4 Abs. 2 lit. c MCAV) und auf dem Dienstweg dem Gesamtbundesrat zur Bewilligung vorgelegt. Es obliegt anschliessend der FUB, die entschiedenen Massnahmen umzusetzen und zu protokollieren.

Anwendung

Der militärischen Cyber-Abwehr sind durch die MCAV klar definierte Grenzen gesetzt. Cyber-Massnahmen in fremden Systemen und Netzwerken zum Eigenschutz und zur Selbstverteidigung der Armee ausserhalb des Aktivdienstes können nur zur Anwendung gebracht werden, wenn ein militärisches Informationssystem oder Informatiknetzwerk einem Angriff[11] zum Opfer fällt.

Folglich beinhaltet die tägliche militärische Cyber-Abwehr die Erweiterung und Aufrechterhaltung des Schutzes der bestehenden Systeme und Netzwerke durch vorsorgliche Massnahmen. Anders ausgedrückt handelt es sich um Tätigkeiten in den eigenen Systemen und Netzwerken. Darunter fallen nebst sämtlichen technischen Massnahmen auch die Zusammenarbeit mit Partnern im technischen Umfeld und die Ausbildung der entsprechenden Personen aus der Militärverwaltung und der Armee, beispielsweise durch den Cyber-Lehrgang.

Fazit

Durch die MCAV erhielt die Schweizer Armee keine neuen Kompetenzen. Vielmehr erhält damit die Armee den Auftrag, den Eigenschutz und die Selbstverteidigung auch im Cyber-Raum sicherzustellen. Das bedeutet einerseits, dass die Armee für den Schutz der eigenen Systeme und Netzwerke in eigener Verantwortung zuständig ist und andererseits, dass ein weiteres militärisches Mittel zur Wahrnehmung des Auftrages des Eigenschutzes und der Selbstverteidigung zugunsten aller militärischen Operationen zur Verfügung steht.[12]

Es bestehen jedoch klare juristische Einschränkungen für die tägliche Arbeit der militärischen Cyber-Abwehr, die diese auch gewollt erschweren können. So ist es beispielsweise nicht vorgesehen, dass zum Zweck der Erhöhung des Schutzes der eigenen Systeme und Netzwerke präventiv in fremde Computersysteme und -netzwerke eingedrungen werden darf und entsprechende Informationen beschafft werden.

Als verhältnismässig neue und herausfordernde Disziplin benötigt die militärische Cyber-Abwehr zunächst Erfahrung auf allen Stufen und in allen Fachbereichen. Erst mit dieser Erfahrung kann weiterer juristischer Handlungsbedarf ausgewiesen und erarbeitet werden, um die Rahmenbedingungen den jeweiligen Bedürfnissen anpassen zu können.

«Cyber ist integraler Bestandteil militärischen Handelns und für die Auftragserfüllung der Armee heute und in Zukunft zentral.»

Die Herausforderung für die Schweizer Armee besteht nun darin, die entsprechenden Fähigkeiten aufzubauen und vor dem Hintergrund der rasanten technischen Entwicklung aufrechtzuerhalten. Erst so können die Cyber-Fähigkeiten in die Operationen der Armee gewinnbringend eingebracht und als integraler Bestandteil genutzt werden. So kann die Schweizer Armee die Auftragserfüllung auch in Zukunft gewährleisten. ■

1 Vgl. Äusserung von KKdt Philippe Rebord vom 11. April 2017.

2 Der Artikel behandelt das nationale Recht und den Auftrag der Schweizer Armee. Die Grundsätze des Kriegsvölkerrechts gelten auch im Cyber-Raum. Es wird aus thematischen Gründen und zugunsten des Umfanges des vorliegenden Artikels bewusst darauf verzichtet, die Anwendung des Kriegsvölkerrechtes und der Neutralität zu beleuchten.

3 Vgl. Art. 58 Bundesverfassung der Schweizerischen Eidgenossenschaft (BV; SR 101).

4 Cyber-Angriffe gegen militärische Systeme und Netzwerke verfolgen in der Regel das Ziel, zentrale Prozesse einer Armee zu stören. Der Angreifer will im Zielsystem Informationen gewinnen, Daten verändern (beispielsweise in Logistiksystemen) oder die Verfügbarkeit von Daten unterbinden (beispielsweise durch Verschlüsselung von Datenbanken-Ransomware). Cyber-Abwehr bezweckt daher den Schutz gegen Angriffe, die die Unterdrückung der Führungsfähigkeit einer Armee zum Ziel haben. Es liegt auf der Hand, dass die Sicherstellung der Cyber-Abwehr für die Auftragserfüllung der Schweizer Armee zentral ist.

5 Art. 100 Abs. 1 lit. c MG: Sie ergreifen im Falle eines Angriffes gegen militärische Informationssysteme und Informatiknetzwerke die erforderlichen Massnahmen. Sie können in Computersysteme und Computernetzwerke, die für solche Angriffe verwendet werden, eindringen, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen. Solche Massnahmen bedürfen, ausser im Aktivdienst, der Genehmigung durch den Bundesrat.

6 Die Betrachtung und Beurteilung von Cyber als Operationssphäre ist nicht Bestandteil der vorliegenden Ausführungen.

7 Vgl. Die Sicherheitspolitik der Schweiz, Bericht des Bundesrates vom 24.08.2016 (SIPOL B 16), 7846: «Die Armee muss jederzeit, im Alltag wie in der Krise, ihre eigenen Informations- und Kommunikationssysteme und -infrastrukturen vor Angriffen schützen und Cyber-Angriffe abwehren können. Sie setzt die entsprechenden Mittel so ein, dass sie sich selber schützen und ihren Auftrag erfüllen kann.»

8 Der Vorgang des Eindringens in ein System wird ebenfalls im Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG; SR 121) in Art. 37 erwähnt, jedoch definiert weder die Botschaft zum NDG, zum MG noch die Erläuterungen zur MCAV diese Tathandlung. Aufschluss gibt Art. 143bis des Schweizerischen Strafgesetzbuches (StGB; SR 311.0) beziehungsweise die einschlägigen Kommentare dazu. Als Eindringen wird die Überwindung einer Zugangsschranke (Tathandlung) in eine gegen Eindringlinge besonders gesicherte Datenverarbeitungsanlage (Tatobjekt) definiert.

9 Bewilligungspflichtige Massnahmen bedürfen eines gesamtbundesrätlichen Entscheides (Art. 7 MCAV), wogegen nicht-bewilligungspflichtige Massnahmen in der Kompetenz des C FUB liegen. Der C FUB ist für die Führungsunterstützung und somit auch für sämtliche militärischen Systeme und Netzwerke verantwortlich.

10 Art. 4 Abs. 2 lit. d MCAV. Diese Unterscheidung zeigt zusätzlich auf, dass der Betrieb von Systemen und Netzwerken in der Verantwortung der FUB einen integralen Teil der militärischen Cyber-Abwehr darstellt.

11 Ein Angriff stellt ein völkerrechtswidriges Verhalten eines Staates gegenüber einem anderen Staat dar und verletzt in der Regel die Souveränität oder territoriale Integrität des Opferstaates. Fraglich und stets Einzelfall abhängig, bleibt die Intensität der Massnahme im Cyber-Raum zur Erfüllung der Definition eines Angriffes nach völkerrechtlichen Kriterien.

12 Die Wahl des einzusetzenden Mittels bei einer militärischen Reaktion obliegt dem Bundesrat. Nach einhelliger Meinung im internationalen Umfeld spielt der Angriffsvektor für die Wahl der Gegenmassnahme keine Rolle beziehungsweise jedes militärische Mittel kann als Antwort auf den Einsatz eines anderen legalen militärischen Mittels, unter Wahrung der Verhältnismässigkeit, zum Einsatz gebracht werden.

Hauptmann
Jan E. Vögtlin
MLaw, Rechtsanwalt
Legaladvisor Cyber
VBS FUB ZEO
4532 Feldbrunnen