Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 190 (2024)

Heft: 9

Artikel: Verteidigungsfähig im Cyberraum

Autor: Besse, Frederik

DOI: https://doi.org/10.5169/seals-1063597

Verteidigungsfähig im Cyberraum

Die Armee muss ihre Verteidigungsfähigkeit auch im Cyber- und elektromagnetischen Raum stärken. Das Kommando Cyber will in diesem Wirkungsraum seine operationellen Fähigkeiten ausbauen. Dazu gehören unter anderem die mobile EKF-Einsatzunterstützung oder offensive Cyberaktionen gegen militärische Ziele.

▲ Die Armee muss sich im Cyber- und elektromagnetischen Raum mit einer komplexen Bedrohungslage auseinandersetzen, die sich stetig verändert und entwickelt.
Bild: Kdo Cyber

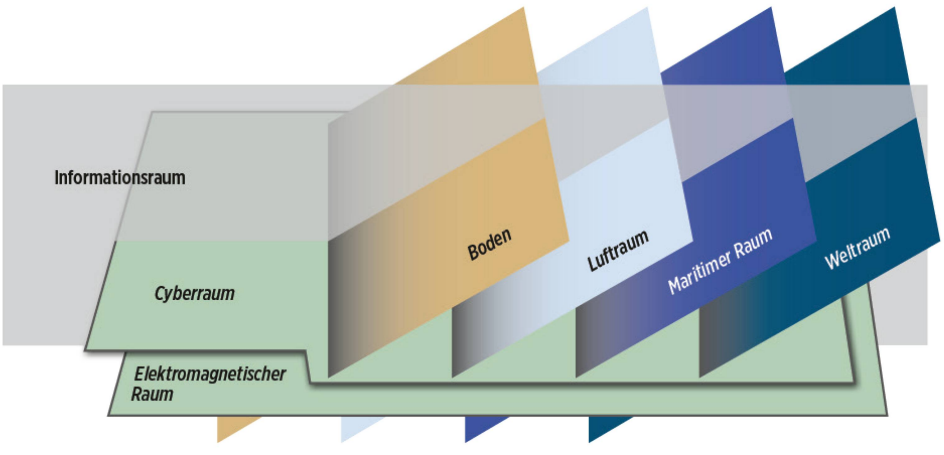
Frederik Besse

Heute finden jeden Tag Angriffe im Cyberraum in unterschiedlichster Art statt. Auch gegen die Schweizer Armee. Sie ist dadurch permanent gefordert und täglich im Einsatz, damit ihre einsatzkritische Informations- und Kommunikationstechnologie-Infrastruktur (IKT) geschützt ist. Der Bericht «Sicherheit Schweiz 2023» des Nachrichtendienstes des Bundes zeigt auf: Cyberangriffe begleiten nicht nur kinetische Angriffe, um deren Auswirkungen zu verstärken, sondern können bereits lange vor einem offenen Konflikt stattfinden, beispielsweise um die kritische Infrastruktur eines Landes zu stören. Auch neutrale Länder können von solchen Aktionen betroffen sein. Im Krieg zwischen Russland und der Ukraine ist diese Entwicklung zu beobachten. Bereits vor der Annexion der Krim 2014 wurden Aktionen im Cyber- und elektromagnetischen Raum verzeichnet und seit der Invasion im Frühjahr 2022 haben sich solche Aktionen aus Russland gegen die Ukraine massiv intensiviert.

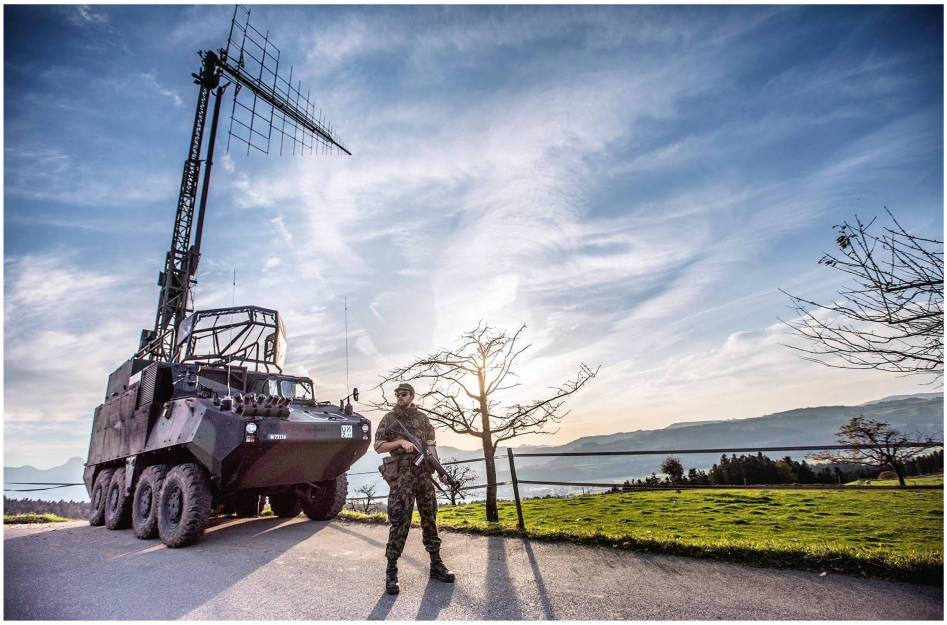
Aktionen im Cyberraum gehören damit zum heutigen Konfliktbild. Sie betreffen auch die Schweiz. Dies bereits im Alltag und nicht erst, wenn ein bewaffneter Konflikt unmittelbar bevorsteht (siehe: Sicherheit Schweiz 2023: Lagebericht des Nachrichtendienstes des Bundes).

WAS IST DER WIRKUNGSRAUM CER?

Der Begriff CER bezeichnet den Cyber- und den elektromagnetischen Raum und umfasst damit ebenfalls den gesamten IKT-Bereich der Schweizer Armee. Der Teil Cyber im Wirkungsraum CER umfasst alle Daten und Informationen, die durch die IKT-Systeme der Armee bearbeitet werden. Der elektromagnetische Raum dient zur physikalischen Übertragung von Informationen durch funkbasierte Signalübertragung, zur räumlichen Ortung von Objekten mittels Radar und Funkortung sowie zur elektronischen Kriegsführung (EKF) durch elektromagnetische Wellen verschiedener Frequenzen.



Der Cyber- und elektromagnetische Raum (CER) im Zusammenhang mit allen weiteren Wirkungsräumen.
Bild: Kdo Cyber



Die elektronische Kriegsführung fällt auch in die Zuständigkeit der FU Br 41. Bild: EKF Abt 52

Den Bedrohungen Rechnung tragen

Die Bedrohungslage im Cyber- und elektromagnetischen Raum ist komplex. Neue Technologien werden laufend weiterentwickelt, ebenso deren technische Anwendungen. Dies schafft ständig neue Abhängigkeiten. Damit und mit der Digitalisierung wachsen im CER die Verwundbarkeit und das Missbrauchspotenzial. Risiken und Bedrohungen im Cyberraum sind vielfältig: Sie reichen von kriminellen Aktivitäten über Spionage, Manipulation und Desinformation bis hin zum Einsatz offensiver Cybermittel in einem bewaffneten Konflikt.

Die Schweizer Armee hat die Chancen und Risiken, die der CER bietet, erkannt und im Grundlagenpapier «Gesamtkonzeption Cyber» aufgezeigt, wie sie mit den Bedrohungen umgeht und ihren Auftrag langfristig in allen Lagen erfüllen wird. Die Armee muss sich umfassend vor Angriffen aus dem Cyber- und elektromagnetischen Raum schützen und auch aktive Massnahmen weiterentwickeln, um Bedrohungen angemessen abzuwehren.

Im Zuge der Umsetzung der Gesamtkonzeption Cyber wurde das einsatzorientierte militärische Kommando Cyber aufgebaut. Die Fähigkeiten des Kommando Cyber richten sich konsequent auf die Aufgaben der Armee aus. Seit Anfang 2024 ist das Kommando Cyber operationell und besteht aus einem rund 700-köpfigen Team. Es vereint unzählige Talente, die weit über «Cyber» hinausgehen. Neben seinen Spezialistinnen und Spezialisten sowie dem Berufsmilitärkorps verfügt es mit der Führungsunterstützungsbrigade 41 über das Wissen und Können von rund 11 500 Milizangehörigen.

◀ Aus der Gesamtkonzeption Cyber: eine vereinfachte Darstellung der operationellen Fähigkeiten im CER. Bild: Kdo Cyber

Eigenschutz als Grundvoraussetzung

Voraussetzung für die Einsätze der Armee ist die Fähigkeit, ihre Systeme vor Bedrohungen aus dem CER schützen zu können. Dieser Eigenschutz im Cyber- und elektromagnetischen Raum umfasst alle Fähigkeiten, die es braucht, um armeeeigene Verbände, Systeme, Infrastrukturen, Daten, Informationen und Netze gegen Bedrohungen im CER zu schützen. Teil des CER-Eigenschutzes ist das integrale Sicherheitsmanagement. Es umfasst technische, organisatorische und betriebliche Massnahmen, um die IKT zu schützen. Ein wichtiges Element dabei ist das sogenannte IKT-Schwachstellenmanagement. Es dient dazu, allfällige Verwundbarkeiten zu erkennen und vorsorglich zu beheben.

Ein weiterer wichtiger Bestandteil des Eigenschutzes ist das Erkennen und Abwehren von Angriffen auf die IKT der Armee. Ist der Angriff abgewehrt, muss der entstandene Schaden festgestellt und das Vorgehen des Angreifers analysiert werden.

Zahlreiche Sensoren und Waffensysteme der Armee nutzen den elektromagnetischen Raum. Die Handlungsfreiheit im elektromagnetischen Raum ist darum für die Führung und den Waffeneinsatz in anderen Wirkungsräumen entscheidend, insbesondere am Boden und in der Luft. Entsprechend zentral ist der Eigenschutz. Er beruht im Wesentlichen darauf, gegnerische elektromagnetische Aktivitäten zu erfassen, eigene Truppen zu warnen und wenn notwendig Gegenmassnahmen einzuleiten. Im elektromagnetischen Raum geht es weiter darum, die eigenen Emissionen zu kontrollieren – also das eigene elektromagnetische Strahlungsbild. Dies erlaubt es, sich der gegnerischen Funkaufklärung zu entziehen oder diese zu täuschen. Weiter gilt es zu verhindern, dass sich eigene Sensoren und Effektoren im elektromagnetischen Raum gegenseitig stören.

Die Wichtigkeit der Miliz

Die Milizkomponente des Kommando Cyber besteht aus der Führungsunterstützungsbrigade 41 (FU Br 41) sowie dem Milizstab und den beiden Fachstäben Cyber und Telecom. Die FU Br 41 befindet sich derzeit in einer intensiven Phase der Weiterentwicklung. Im Zentrum steht die Stärkung der Verteidigungsfähigkeit.

Die FU Br 41 verfügt über einzigartige Fähigkeiten im Bereich der Führungsunterstützung, der Übermittlung sowie in der elektronischen Kriegsführung. Mit seinen drei Hauptquartier-Bataillonen verfügt die FU Br 41 beispielsweise über Fachspezialisten für den Betrieb von geschützten Anlagen. Die Milizkomponente des Kommando Cyber ist für Führungsanlagen verantwortlich, baut krisenresistente Telekommunikationsnetze auf und betreibt diese ebenso wie Rechenzentren. Sie ermöglicht zudem die permanente Überwachung des Luftraums mittels Radar.

Die FU Br 41 will sich mit dem Schutz vor Bedrohungen konsequent auf die Stärkung der Verteidigungsfähigkeit ausrichten. Die Bedrohung für die Verbände der FU Br 41 umfasst grundsätzlich alle Formen der Angriffe – also aus der Luft, aus dem CER sowie von Bodentruppen. Diesen Bedrohungen können die Formationen der FU Br 41 mehrheitlich nicht mit direkten Gegenmassnahmen begegnen. Die Alternative: Man entzieht sich durch Tarnung, Täuschung und Bewegung. Dies wird seit Anfang Jahr intensiv mittels neuer Einsatzverfahren trainiert.

Bei den Einsatzverfahren geht es im Wesentlichen darum, sich generell, insbesondere aber im elektromagnetischen Raum maximal zu tarnen. Zudem gilt es sich durch eine hohe Beweglichkeit der gegnerischen Aufklärung und dem gegnerischen Feuer zu entziehen. Dabei ist in möglichst kleinen Verbänden vorzugehen, um so Massierungen zu vermeiden.

Rasche Informationsverbreitung entscheidend

Für den Erfolg von Armeeeinsätzen entscheidend ist, wie schnell Informationen für die Führung nutzbar gemacht werden können. Wer schneller entscheidet und agiert als ein Gegner, behält die Überhand. International spricht man in diesem Zusammenhang vom OODA-Loop. In der Schweizer Armee ist die Rede vom Sensor-Nachrichten-Führungs-Wirkungsverbund (SNFW-Verbund).

Es handelt sich dabei um eine Entscheidungsschleife mit dem Ziel, schneller Wirkung zu erzeugen als ein Gegner. Dies wird erreicht, indem die vier Schritte Beobachten (Observe), Beurteilen (Orient), Entscheiden (Decide) und Handeln (Act) möglichst rasch durchlaufen werden. Dies schneller und besser als der Gegner. Weiter kann ein Gegner aktiv durch den Einsatz von Cyber- oder EKF-Mitteln beeinträchtigt und verlangsamt werden.

Das Kommando Cyber schafft die Voraussetzungen, um diesen Wissens- und Entscheidungsvorsprung der Armee zu ermöglichen. Ein eigener Wissensvorsprung entsteht beispielsweise dann, wenn Daten aktueller und besser verfügbar sind, wenn ihr Wahrheitsgehalt gewährleistet ist oder wenn sie rascher ausgewertet werden können.

Drei Einblicke in die Zukunft

Mit der Gesamtkonzeption Cyber hat die Schweizer Armee ein Grundlagenpapier erarbeitet. Dessen Umsetzung erfolgt schrittweise über mehrere Jahre hinweg. Nachfolgend sind drei Vorhaben und Projekte beschrieben, welche darauf einzahlen, die Verteidigungsfähigkeit der Armee zu stärken.

(R)evolution in der elektronischen Kriegsführung: Nicht nur der Schutz der eigenen Systeme ist zentral, sondern auch die Fähigkeiten, eigene Aktionen im Cyber- und elektromagnetischen Raum durchführen zu können. Das Kommando Cyber verantwortet die Planung sowie die fachliche Führung von Operationen und Einsätzen der elektronischen Kriegsführung. Dies beispielsweise mit der Ortung von gegnerischen Systemen, welche Funksignale versenden, oder mit der Störung der Kommunikationsinfrastruktur eines potenziellen Gegners.

Eine neue Fähigkeit wird im Bereich der mobilen EKF-Einsatzunterstützung von Kampfverbänden aufgebaut. Die Schweizer Armee will in Zukunft Verbände auf Stufe Einheit mit tragbaren EKF-Systemen ausrüsten. Damit erhalten die Kommandanten die Möglichkeit, in ihrem Raum die gegnerische funkbasierte Führung zu bekämpfen. Dies mit der Wirkung, gegenüber einem Gegner den Wissens- und Entscheidvorsprung durch die Verlangsamung und Störung seiner Systeme zu erlangen. Gleichzeitig können diese Systeme auch einen Beitrag zum Eigenschutz leisten, beispielsweise gegen funkgesteuerte Kleindrohnen. Damit hätten Einheiten eine effiziente und kostengünstige Lösung, um sich gegen kleine Flugobjekte zu schützen. Erste Versuche sind in Vorbereitung.

Cyberaktionen gegen militärische Ziele: In diesem Jahr wurden die Arbeiten zum Aufbau der Fähigkeit für Cyberaktionen gegen militärische Ziele aufgenommen. Damit soll die Schweizer Armee die Fähigkeit erlangen, sowohl im elektromagnetischen wie auch im Cyberraum in gegnerische Führungs- und Feuerleitsysteme einzudringen. Dies basierend auf den rechtlichen Grundlagen des Militärgesetzes. Ab Beginn 2026 wird im Cyberlehrgang der Armee eine entsprechende Fachrichtung ausgebildet werden.

Potenzial der Digitalisierung zugänglich machen und nutzen: Mit der Entwicklung der Neuen Digitalisierungsplattform (NDP) stellt die Schweizer Armee zentrale Weichen für ihre Ausrichtung und Fähigkeiten in der Zukunft. Die Digitalisierung macht vor der Armee nicht halt und bietet grosse Chancen, welche die Armee zu ihrem Vorteil nutzen will. Die NDP ist ein wichtiges Element dieser Bemühungen. Diese Plattform wird als zentrales Nervensystem der Armee in Zukunft einen standardisierten und bedarfsgerechten Datenaustausch innerhalb der verschiedenen Teilstreitkräfte und mit externen Partnern des Sicherheitsverbunds Schweiz ermöglichen, um ein gemeinsames Lageverständnis zu erreichen.

AUSGERICHTET AUF STÄRKUNG DER VERTEIDIGUNGSFÄHIGKEIT

Wie sich die Armee weiterentwickelt, ist ausführlich in der «Gesamtkonzeption Cyber» sowie im Bericht «Die Verteidigungsfähigkeit stärken – Zielbild und Strategie für den Aufwuchs» skizziert. Mit den drei strategischen Stossrichtungen adaptive Weiterentwicklung der militärischen Fähigkeiten, Nutzung von Chancen aufgrund des technologischen Fortschritts und intensivere internationale Kooperation soll die Verteidigungsfähigkeit der ganzen Armee verstärkt werden. Für das Kommando Cyber erfolgen die Umsetzung sowie der Aufwuchs im CER-Bereich schrittweise bis in die 2030er-Jahre.

Maj Frederik Besse
Leiter Kommunikation
Kommando Cyber
Journalistoffizier Stab Ter Div 4
3000 Bern