Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 98 (2023)
Heft: 7-8

Artikel: Immer einen Schritt voraus sein
Autor: Stirnimann, Stephan
DOI: https://doi.org/10.5169/seals-1052990

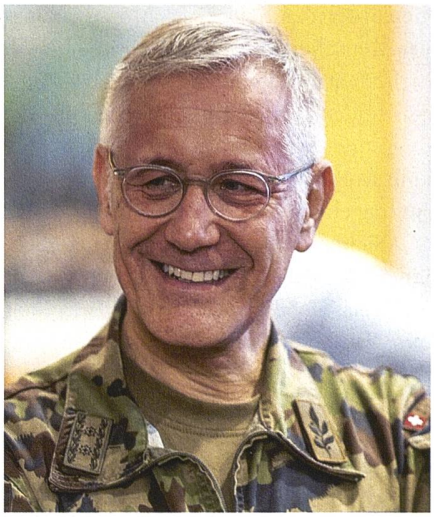
Immer einen Schritt voraus sein

Das Projekt Kommando Cyber nimmt Form an. Ende März führte Divisionär Vuitel der OGZU das Projekt Kommando Cyber ein – ein Thema, das an Aktualität nicht zu überbieten ist. Kaum eine Übung oder ein Einsatz der Armee ist nämlich ohne den Bereich der Informations- und Kommunikationstechnologie (IKT) durchführbar.

Stephan Stirnimann

Die Gesamtkonzeption Cyber dient dazu, die nötigen Massnahmen zur Weiterentwicklung im Bereich des Cyber-Raums, des elektromagnetischen Raums sowie der Informations- und Kommunikationstechnologie anzustossen. Sie schafft eine gemeinsame Vorstellung in diesem Bereich und eine Vorgabe für die Planung der 2020er- bis in die 2030er-Jahre. Der Bundesrat hat die Gesamtkonzeption Cyber Mitte April 2022 zur Kenntnis genommen.

Die Armee muss sich nicht nur ihren aktuellen Aufgaben stellen. Auch künftige Bedrohungen, Herausforderungen und die immer schnelleren Entwicklungen im cyber- und elektromagnetischen Raum müssen sie rechtzeitig antizipieren. Bereits 2022 entschied der Bundesrat, im Rahmen der «Gesamtkonzeption Cyber» bis zu 2,4 Milliarden Franken in die «Cyberarmee» zu stecken. Damit soll sich die Schweizer Armee im Cyber-Raum künftig besser vor Bedrohungen schützen können.



Divisionär Alain Vuitel führt als Projektleiter das Projekt «Kommando Cyber» der Schweizer Armee.

Cyber-Raum als Operationssphäre

Im Kurzreferat im Rahmen der Offiziersgesellschaft Zürcher Unterland (OGZU) vor rund 200 Gästen zeigte Divisionär Vuitel auf, wie der Cyber-Raum zu einer militärischen Operationssphäre geworden ist und immer mehr Staaten bereit sind, diesen zu nutzen und zu verteidigen. Eine solche Entwicklung in Streitkräften erfordert grundlegende Anpassungen in einem Umfang, der wohl nur mit dem Aufkommen von militärisch genutzten Flugzeugen im Ersten Weltkrieg und der anschliessenden rasanten Entwicklung von Flugzeugen vergleichbar ist.

Ausgebildete Spezialisten notwendig

Neben den geladenen Gästen der OGZU befand sich auch eine ganze Offizierschule der Führungsunterstützungsbrigade 41 (FU Br 41) im Saal. Sie ist die Brigade der Informations- und Kommunikationstechnologie der Schweizer Armee und betreibt die Kommunikationsnetze, die Führungsanlagen der Landesregierung und der Armee sowie mobile Systeme für die elektronische Kriegsführung. Die FU Br 41 stellt ebenfalls Dienstleistungen und Systeme für besondere Aufgaben (Informatik, Kryptologie und Sprachspezialisten) bereit.

Brigadier Martino Ghilardi, vorher Chef Militärdoktrin im Bereich Unternehmensentwicklung Verteidigung, ist seit dem 1. April 2023 Kommandant der Führungsunterstützungsbrigade 41. Ein Projektteam arbeitet seit Mai 2021 am Aufbau des Kommando Cyber. Strategische Partnerschaften sollen die notwendige Handlungsfreiheit schaffen, damit sich das Kommando Cyber auf die Kernaufträge der Armee konzentrieren kann. Letztendlich geht es darum, dass die Armee in allen Lagen über den notwendigen Wissens- und Entscheidvorsprung verfügt.

Das Kommando Cyber ist ab dem 1. Januar 2024 operationell. Eine der Schwierigkeiten für das Kommando Cyber sei es, auf dem hart umkämpften Arbeitsmarkt gut ausgebildete und qualifizierte Spezialisten zu finden. «Seit Kurzem nutzen wir nun auch das Potenzial neuer Kanäle, um qualifizierte Fachkräfte für uns zu gewinnen», erklärte Vuitel vor dem geladenen Publikum.

Realistisches Training

In der Übung «Locked Shields» wurden diverse militärische Führungs- und Informationssysteme sowie Systeme kritischer Infrastrukturen (z.B. Wasserversorgung, Finanzdienstleister, etc.) simuliert, welche durch die «Blue Teams» verteidigt werden mussten. Mit «Locked Shields» konnte die Schweizer Armee ihre Cyberabwehrfähigkeiten in einem «realistischen und herausfordernden» Szenario testen, verbessern und ihre Cyberkompetenzen ausbauen.

Im Zentrum der Übung stand die Anwendung technischer Cyberfähigkeiten sowie die Verbandsausbildung der taktischen Stufe und die Kaderausbildung. Die Übungsanlage umfasste hierzu diverse Operationstypen des Cyber-Raums, mit einem Schwergewicht auf defensive Cyber-Operationen.

Cyber-Spezialist-Lehrgang

Mit der Weiterentwicklung der Armee (WEA) wurde eine Cyber-Kompanie in der Elektronischen Abteilung 46 (Elo Abt 46) in der Führungsunterstützungsbrigade 41 (FU Br 41/SKS) zur Unterstützung der Berufsorganisation FUB gebildet. Der Cyber-Lehrgang der Armee dient dazu, Armeeangehörige für diese Kompanie aus-

zubilden. Zweimal im Jahr werden je 20 Teilnehmende ausgebildet (also 40 pro Jahr), und zwar an der Elektronische Krieg-führung-Schule 64 (EKF S 64). Er beinhaltet 800 Stunden Ausbildung und Einsatz im Bereich Cyber. Der Lehrgang kann mit einer Berufsprüfung zum «Cyber Security Specialist» mit eidge-nössischem Fachausweis abgeschlossen werden. Dieses Diplom erfordert noch zusätzliche Arbeitserfahrung nach dem Lehrgang.

Im Interview mit dem SCHWEIZER SOLDAT hat Divisionär Vuitel weitere Fragen beantwortet.

✚ *Wie schaffen Sie es, genügend Nachwuchspersonal im hart umkämpften Arbeitsmarkt zu rekrutieren? Haben Sie eine Kampagne «im Köcher»?*

Divisionär Vuitel: Neben den gängigen Kanälen, die unsere offenen Stellen bewerben, haben wir inhouse eine Ausbildungsstätte aufgebaut: die «ICT Warrior Academy». Diese bietet für bestehende Mitarbeitende wie auch für junge Talente die Lehrgänge ICT-Systemspezialist/-in «Junior» und Cyber Defence (Fokus Security Operation Center) an. Die Lehrgänge dauern bis zu zwölf Monate. Dort haben wir die einmalige Gelegenheit, neue Mitarbeitende auf die Aufgaben im Kommando Cyber spezifisch zu schulen, was uns im hart umkämpften Markt sicherlich hilft.

Ausserdem bilden wir im Cyber-Lehrgang ebenfalls Spezialistinnen und Spezialisten aus, welche im Rahmen ihrer Wiederholungskurse wiederum Berührungspunkte mit uns haben. Genau diese Berührungspunkte wollen wir verstärkt nutzen und diesen Fachkräften aufzeigen, welche Jobs und Chancen das Kommando Cyber als ziviler Arbeitgeber bietet.

✚ *Kürzlich wurden verschiedene Internetseiten von Schweizer Städten gehackt beziehungsweise blockiert. Wie sehen Sie die momentane Bedrohungslage?*

Vuitel: Die Ereignisse der letzten Monate haben beispielhaft gezeigt, dass auch die stark vernetzte Schweiz im Cyber-Raum in den Fokus von international tätigen Gruppierungen gelangen kann. Aktuell sind diese Aktionen zum Glück noch von vergleichsweiser tiefer Intensität und Qualität. Dennoch sollten sie nicht unterschätzt werden. Vielmehr sollten die Ereignisse ein Weckruf sein. Sie zeigen, wie wichtig ein guter Schutz vor Cyber-Angriffen und die Schliessung von Schwachstellen bereits zum Alltag geworden ist.

Gerade in diesem Bereich fehlt in der Schweiz in einigen Bereichen noch ein wenig das Bewusstsein für die Bedeutung eines guten Schutzes im Cyber-Raum. Auf nationaler Stufe wurden diese Herausforderungen erkannt.

Die Aufwertung des NCSC zu einem Bundesamt im VBS, die Schaffung eines Kommando Cyber als erste Verteidigungslinie der Armee im Cyber-Raum sowie die Aufstellung eines Staatssekretariats zeigen, dass diese Entwicklungen ernst genommen werden. Die Abwehr von Cyber-Angriffen ist dabei immer auch eine Verbundsaufgabe und erfolgt deshalb in enger Abstimmung mit allen involvierten Stellen innerhalb des Sicherheitsverbunds Schweiz.

✚ *Herr Divisionär, vielen Dank für Ihre Zeit.* ✚

Wer sich bereits vordienstlich intensiver mit dem Thema Cyber-Security auseinandersetzen möchte, kann sich im Talent-Programm «SPARC» einschreiben

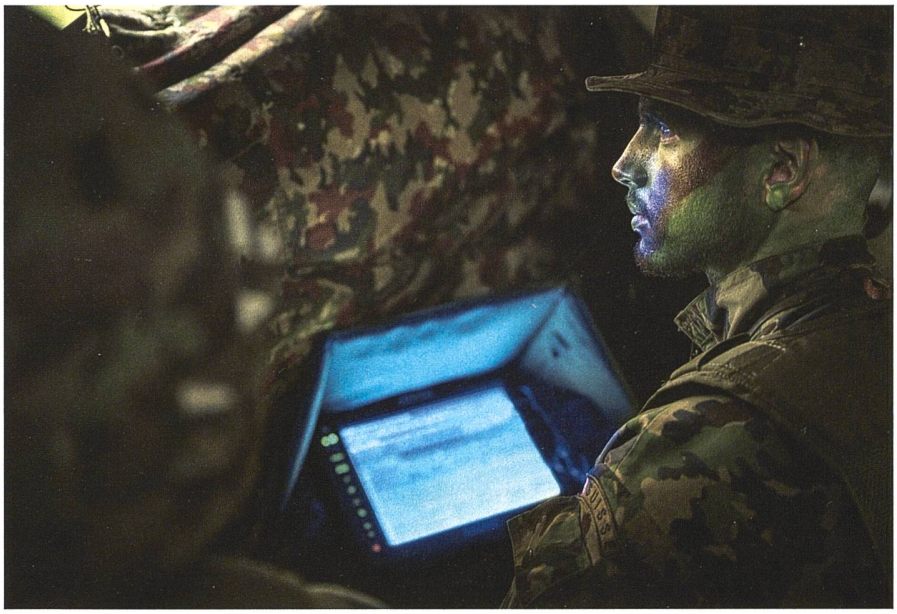


Bild: VBS

In der internationalen Cyberübung «Locked Shields 2023» musste die Armee ihre Infrastruktur gegen Cyberangriffe verteidigen (Symbolbild).

Internationale Militärübung unter Schirmherrschaft der NATO

Im April dieses Jahres hat ein Detachement der Schweizer Armee an der internationalen Cyberübung «Locked Shields 2023» in Estland teilgenommen.

An der Übung beteiligten sich Angehörige des Cyber-Bataillon 42, ziviles Berufspersonal aus dem Projekt Kommando Cyber und Mitarbeitende von Betreibern kritischer Infrastrukturen.

Die Übung «Locked Shields» ist eine internationale Cyberübung, welche vom «Cooperative Cyber Defence Center of Excellence (CCDCOE)» in Tallinn organisiert wird, dem unter der Schirmherrschaft der NATO stehenden Kompetenzzentrum für die Aus- und Weiterbildung ziviler und militärischer Cyberspezialistinnen und Cyberspezialisten. Die Übung simulierte einen hybriden Konflikt, in welchem die Teilnehmerinnen und Teilnehmer ihre Infrastruktur gegen Cyberangriffe verteidigen mussten.

Um die Interoperabilität zu trainieren, bildete die Schweizer Armee dieses Jahr gemeinsam mit Estland und Belgien ein «Joint Blue Team».