Wie sich die Armee vor Cyberattacken schützt

Autor(en): **Kägi, Ernesto**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **189 (2023)**

Heft 7

PDF erstellt am: **09.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-1052752

◀ Blick in das Security Operation Center.
Bild: Jonas Kambli, VBS

Wie sich die Armee vor Cyberattacken schützt

Cyberangriffe durch «hoch professionelle digitale Piraten» auf zivile, wirtschaftliche, öffentlich-rechtliche oder militärische Informationssysteme erfolgen heute jederzeit und überall. So gesehen befinden wir uns in einer neuen Dimension von Krieg.

Ernesto Kägi

Erpressungen im Cyberraum mit hohen Lösegeldforderungen sind an der Tagesordnung. Hacker-Angriffe von gigantischen Ausmassen, ausgeführt mit immer raffinierteren «Tools», können unsere Zivilgesellschaft lahmlegen oder zumindest nachhaltig stören. Dabei beschleicht einen das ungute Gefühl, dass der Verteidiger gegenüber dem Angreifer immer etwas zu spät kommt.

Keine Branche bleibt verschont

Bereits 2016 wurde Ruag gehackt. Darauf wurde der Konzern in einen zivilen und einen militärischen Bereich aufgeteilt. 2021 sollen Hacker erneut ins System der Ruag International eingedrungen sein. 2020 wurde die mit modernsten CNC-Anlagen ausgestattete Thurgauer Fensterfabrik Swisswindows AG durch einen massiven Angriff auf die technischen und kommerziellen IT-Systeme völlig lahmgelegt und in den Konkurs getrieben. 170 Angestellte verloren ihren Arbeitsplatz. Auch die Luzerner Grossgarage Epper, deren gesamte kommerzielle und autotechnische Infrastruktur des Mutterhauses und des verzweigten Filialnetzes in der Innerschweiz, wurde vorübergehend ausgeschaltet. Immer noch am Laufen ist der Grossangriff auf die NZZ und CH-Media Gruppe. Nach Verweigerung einer Lösegeldzahlung wurden erst kürzlich weitere sensitive NZZ-Daten veröffentlicht. Im März 2023 erbeuteten Hacker in der Gemeinde Saxon VS Personendaten von Sozialhilfeempfängern.

Mit diesen fünf Beispielen soll aufgezeigt werden, dass kein Bereich des staatlichen, wirtschaftlichen und sicherheitsrelevanten Lebens vor Cyberangriffen verschont bleibt. Selbst kleinere KMUs sehen sich mit Lösegeldforderungen im hohen fünfstelligen Bereich konfrontiert. Gemäss National Cyber Security Center (NCSC), der Bundes-Meldestelle für Cyberangriffe, haben sich die Hackerangriffe innert zwei Jahren verdreifacht, auf über 30 000 Fälle im Jahr 2022. Eine Pflicht zur Meldung von Cyberangriffen gibt es allerdings bisher nicht.

Bund und Institutionen sind aktiv

In der Frühlingssession 2023 hat das Parlament über eine Cyber-Meldepflicht diskutiert. Für den Bund wäre eine solche insofern wichtig, um damit das Bedrohungsbild besser zu verstehen und um Arten von Angriffen und erkennbare Muster besser zu erkennen. Auch Informationen über Abwehrmassnahmen – welche erfolgreich waren und welche keinen Erfolg hatten – sind wesentliche Kenntnisfaktoren, um Abwehrmassnahmen besser ausgestalten zu können. Eine Meldepflicht für einzelne Unternehmen ist jedoch ein zweischneidiges Schwert, stehen sich doch Unternehmensreputation, weitere Erpressbarkeit und die Gefahr, als Firma an den Pranger gestellt zu werden, diametral mit dem Bundesinteresse nach einer gemeinsamen Cyber-Bekämpfungskultur gegenüber. Hier braucht es vor allem eines: Aufbauarbeit mit viel gegenseitigem Vertrauen.

Der Bund, insbesondere der Bereich Verteidigung des VBS, will sehr aktiv gegen Cyber-Kriminalität vorgehen. Aber auch die anderen Departemente sind nicht untätig. So sind immer mehr Cyberdefence-Mitarbeitende tätig, um die IT-Systeme wirkungsvoll zu schützen. Dabei kommt der gegenseitigen Vernetzung und einem ständigen Informations- und Know-how-Austausch entscheidende Bedeutung zu.

Zivile Unternehmen aller Branchen sowie Institutionen wie Swisscom, SBB, Post, Swissgrid (die international stark verknüpfte Schweizer Elektrizitäts-Schaltzentrale) versuchen, sich vor Cyberangriffen auf ihre IT-Infrastrukturen zu schützen. Swisscom, über deren Netze und Systeme eher früher denn später Hacker-Angriffe auf Swisscom-Kunden erfolgen, ist einer der ganz grossen Player im Cyber-Abwehrbereich. Das VBS arbeitet nicht nur mit ihnen, sondern auch mit der ETH, Universitäten, Polizeikorps (siehe Box zur Kantonspolizei St. Gallen) und weiteren Institutionen zusammen.

Eklatanter Fachkräftemangel

Wenn in der Schweiz zurzeit in vielen Branchen von einem grossen Fachkräftemangel gesprochen wird, dann trifft dies für den Bereich Cyber-Sicherheit in besonderem Masse zu. Selbst kleinere KMU-Betriebe müssen

mit Cyberdefence-Spezialisten in der Lage sein, ihre kommerziellen und technischen Systeme immer besser zu schützen. Entsprechende Spezialisten sind absolute «Mangelware». Nebst dem Informatik-Vollstudium an der ETH bieten zurzeit lediglich die Universität Luzern und die berufsbegleitende Fernfachhochschule Schweiz spezifische Cyberdefence-Studienlehrgänge an.

Kommando Cyber löst Führungsunterstützung ab

Dem Projekt Kommando Cyber der Schweizer Armee kommt bereits heute und vor allem in Zukunft eine entscheidende Bedeutung zu. Deshalb hat der Bundesrat die «Gesamtkonzeption Cyber» genehmigt, welche aufzeigt, wie die Schweizer Armee im Cyber- und elektromagnetischen Raum bis Mitte der 2030er Jahre aufgestellt und weiterentwickelt werden soll. Der Projektleiter Kommando Cyber wurde beauftragt, die Option 3 umzusetzen. Im ersten Schritt soll primär der Eigenschutz im Cyber- und elektromagnetischen Raum (CER) weiter ausgebaut werden und die Fähigkeiten zu Aktionen im CER-Raum erhalten beziehungsweise in Teilen weiter ausgebaut werden. In einem zweiten Schritt soll die Resilienz der Kerninfrastrukturen zum CER-Eigenschutz ausgebaut und die Fähigkeit zum dezentralen CER-Eigenschutz und zur Forensik im Einsatzraum aufgebaut werden. Der dritte Schritt schliesslich umfasst den Ausbau der Fähigkeiten der Bataillone und Kompanien zu eigenständigen

ZUSAMMENARBEIT MIT DER KANTONSPOLIZEI ST. GALLEN

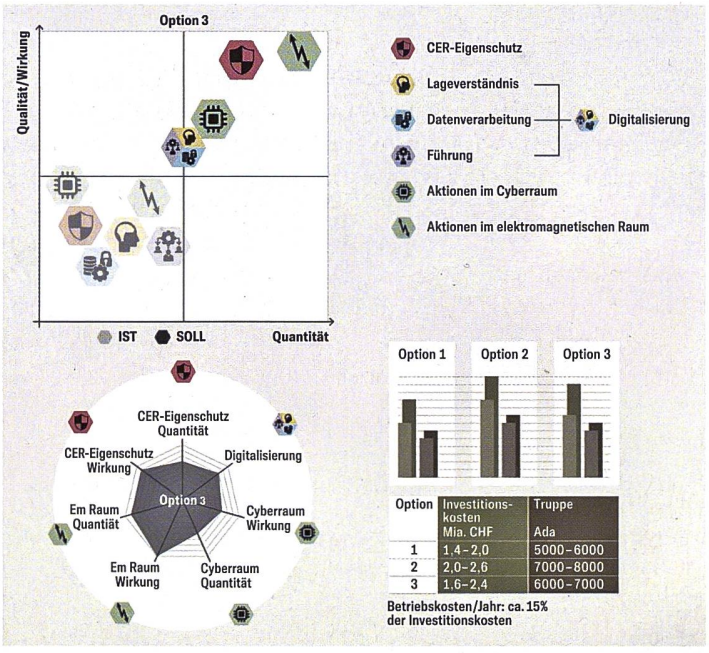
Die Kantonspolizei St. Gallen (Kapo SG) und die Elo Op Schulen 64 haben vereinbart, dass ein 19-jähriger, abverdienender Ostschweizer Wachtmeister seinen praktischen Dienst bei der Kapo SG absolviert. Zuerst wurde er gründlich in die Kapo-Abteilungen IFC (IT, Forensic + Cyber Crime), KAS (Kriminalanalyse) und LNZ (Lage- und Nachrichtenzentrum) eingeführt, um so die Arbeits- und Denkweise der Polizei, insbesondere in der Verfolgung von Cyber-Vorfällen, kennenzulernen. Dann erhielt der junge Cyber-Wehrmann, der nach der Kantonsschule direkt die RS absolvierte und der nach dem Abverdienen des Wachtmeister-Grades an der ETHZ Informatik studieren will, von der Kapo zwei verschiedene Aufträge, deren Lösung die Polizei in zukünftigen Fällen 1:1 einsetzen kann.

Eine der beiden Aufgabenstellungen bestand darin, aus einer Unzahl von Provider-Rückmeldungen die analysierten und brauchbaren Informationen einerseits für die weitere Cyber-Ermittlung der Polizei und andererseits für die später mit diesem Fall beschäftigten Gerichte aufzuarbeiten und darzustellen.

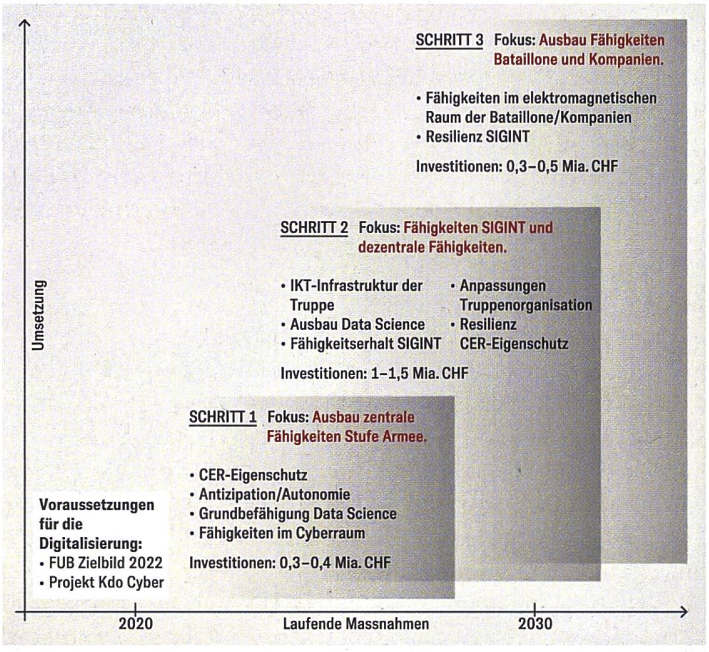
Der Lösungsansatz sah so aus: Gefälschte Ware, welche über einen gefälschten Instagram-Account (Fake-Account) angeboten wird und welche mit einer nichtssagenden E-Mail-Adresse verknüpft ist, führt zum Provider Google, der gegenüber der Polizei auskunftspflichtig ist. In einer ersten Runde erhält die Polizei eine Unmenge von Detaildaten, die für einen Laien nur schwer lesbar und verständlich sind. Mittels einer selbst entwickelten Software, welche auf IT-Tools wie «Tyson» und «Maltego» basiert, schafft es der Cyber-Wachtmeister, erste Ordnung in die Daten zu bringen. Irgendwo versteckt stösst die Software auf eine Gmail-Adresse, mit welcher die Polizei bei Google eine zweite Such- und Informationsanfrage startet. Aus diesen Daten kann mit der selbst entwickelten Software möglicherweise identifiziert werden, zu welchem Land die IP-Adresse gehört. Allenfalls stösst die Software auch auf eine Handynummer, auf einen Namen oder Hinweise, von welchem geografischen Raum aus der Fake-Account betrieben wird. Dies sind alles für die weitere polizeiliche Ermittlungsarbeit oder fürs Gericht sehr wertvolle Daten, welche aus einer Flut von Datensätzen durch die vom Cyberdefence-Spezialisten entwickelte Software herausgefiltert werden können.

Dies sei ganz wichtig, denn «immer mehr Delikte verlagern sich von der Strasse in den Cyberraum», wie sich Kapo-Medienssprecher Florian Schneider in einem Zeitungsbericht zitieren lässt. Für die St. Galler Kantonspolizei bedeutet dieses neue Cyber-Analyseprogramm, welches künftig eingesetzt wird, nebst hervorragenden Kerninformationsübersichten vor allem auch eine grosse Zeitersparnis.

Bei der Präsentation war der ASMZ-Autor beeindruckt, mit welcher sachlichen, unaufgeregten Art der 19-jährige Cyber-Wachtmeister vor Politikern, Vertretern der Justizdirektion, Polizeispezialisten, Armeevertretern und Journalisten seine sehr wertvolle Arbeit vortrug. Ein Beispiel, das hoffentlich in anderen Polizeikorps oder beim Zoll und der Grenzwache in enger Zusammenarbeit mit den Elo Op Schulen 64 Schule machen wird.



Die Option 3 aus der Gesamtkonzeption Cyber wird nun realisiert. Grafiken: Kdo Cyber



Die Option 3 der Cyber-Gesamtkonzeption wird in drei Phasen umgesetzt.

Aktionen im elektromagnetischen Raum bis auf ihre gefechtstechnische Führungsstufe.

Divisionär Alain Vuitel hat im Mai 2021 mit einem kleinen Team mit dem Aufbau des Kommandos Cyber begonnen. Inzwischen arbeiten bereits über 400 Personen in diesem kontinuierlich grösser werdenden Bereich. Die sieben Abteilungen des Kommandos Cyber (ab 1. Januar 2024) werden folgende Hauptfunktionen haben:

→ **Stab:** Plant und führt Aktionen durch und erstellt das integrale Lagebild im Cyber- und elektromagnetischen Raum sowie im Bereich der Informations- und Telekommunikationstechnologie 7/24/365. Die koordinierte und eingespielte Zusammenarbeit über das gesamte Kommando ist dabei zentral.

→ **Langfristige Entwicklung:** Dazu gehören die Verfolgung von langfristigen Trends sowie die technologische Entwicklung, die Steuerung der Fähigkeitsentwicklung, das Ressourcenmanagement inklusive des Frequenzmanagements und weiteren Querschnittsbereichen.

→ **Einsatzkritische Infrastrukturen und Luftwaffensysteme:** Zusammenfassung von sämtlichen einsatzkritischen IT-Strukturen, welche heute in der Armee im Einsatz sind.

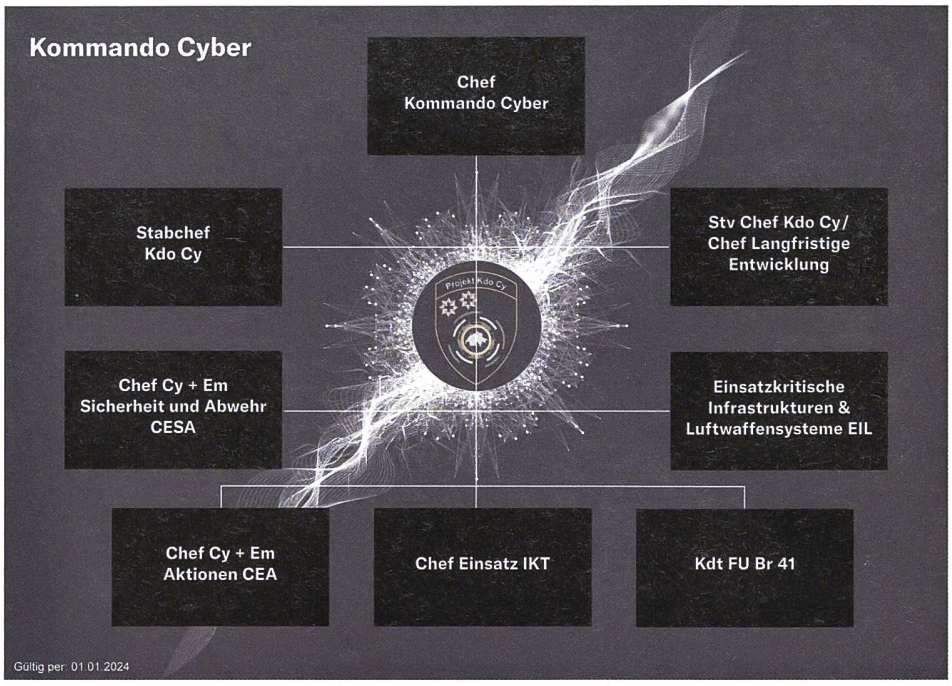
→ **FU Br 41:** Ausbildung und Führung sämtlicher HQ-, Ristl- und EKF-Bataillone.

→ **Einsatz IKT:** Verantwortet die Neue Digitalisierungsplattform NDP der Armee. Unter NDP wird die robuste, hochsichere und resiliente IKT-Plattform verstanden, auf welcher der Armee einsatzkritische Anwendungen zur Verfügung gestellt werden. Neben den eigentlichen Plattformkomponenten (Rechenleistung, Speicher und Ähnliches) gehören weitere Bestandteile wie Endgeräte, Sicherheitselemente, Kollaborationsdienste, Integrationsservices für den integralen Datenaustausch oder der Aufbau der Betreiberorganisation inklusive der dafür notwendigen Strukturen und Prozesse dazu.

→ **Cy + Em Aktionen CEA:** Ist das Kompetenzzentrum für elektronische Operationen, betreibt die dazu notwendige Forschungstätigkeit und unterhält die entsprechenden Kontakte. Es betreibt die verschiedenen CER-Sensoren im Rahmen der gesetzlichen Vorgaben.

→ **Cy + Em Sicherheit und Abwehr CESA:** Im Zentrum steht die IKT- und Cyber-Sicherheit aller Systeme der Armee.

Die Arbeiten laufen auf Hochtouren. Auf Anfang 2024 hin wird die heutige FUB von einer breitgefächerten Führungsunterstüt-



Das ab dem 1. Januar 2024 gültige Organigramm des Kommandos Cyber. Grafik: Kdo Cyber

VORDIENSTLICHE SPARC-AUSBILDUNG

«Interessierst du dich für Cyber Security? Mach mit beim Programm SPARC – auch ohne vorhergehende IT-Kenntnisse.», heisst es auf einem mehrsprachigen Flyer, der unter www.armee.ch/sparc zu finden ist und vor allem Junge ansprechen will. Ansprache und Auftritt erinnern an die fliegerische Vorschulung, welche unter dem Namen Sphair seit Jahren Pilotenanwärter im gleichen Alterssegment anspricht.

Wer bei Sparc dabei sein will, muss die Schweizer Staatsbürgerschaft haben, mindestens 16 Jahre alt sein und über gute Englischkenntnisse verfügen – und die Anmeldung muss vor dem RS-Start erfolgen. Willkommen sind Lernende, Gymnasiasten, Autodidakten und Begeisterte aus allen Horizonten. Die Sparc-Ausbildung ist kostenlos und soll junge Frauen und Männer optimal auf die Selektion Richtung Cyber-Lehrgang vorbereiten. Im Sparc-Programm wird die Arbeit individuell zu Hause erledigt. Dazwischen werden «Erlebnistage» durchgeführt, an welchen die Teilnehmenden ihre Sparc-Kollegen kennenlernen. Dort erhalten sie komplexe Aufgabenstellungen, welche in Gruppen gelöst werden müssen. So kann sich ein Team gegenseitig kennenlernen und die Lehrkräfte können die Teilnehmenden bezüglich Fähigkeiten, Teamverhalten und letztlich bezüglich Eignung beurteilen. Wichtige Lernschritte werden durch Prüfungen abgeschlossen.

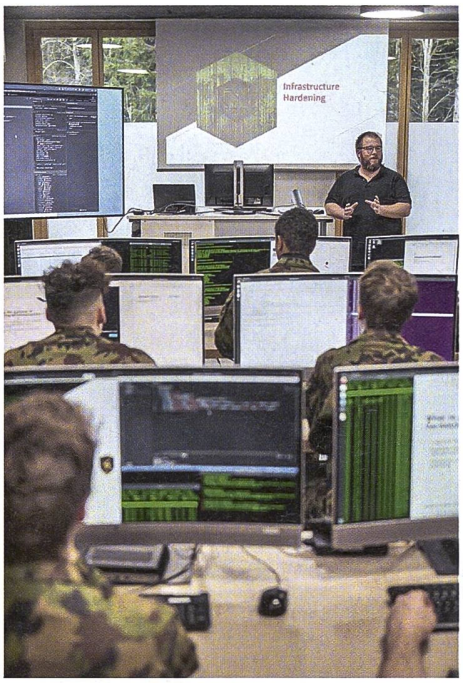
Zurzeit laufen in verschiedenen Schweizer Städten Informationsveranstaltungen. Am ersten derartigen Anlass in der ETH Zürich waren rund 140 junge, interessierte IT-affine Interessenten und Interessentinnen. Rund 100 davon haben sich gleich für den Sparc-Lehrgang eingeschrieben.

Drei externe Unternehmungen, welche ein Konsortium bilden, sind zusammen mit dem Kommando Cyber für das Sparc-Programm verantwortlich:

→ **ICT Berufsbildung Schweiz** ist die nationale Organisation der Arbeitswelt für das Berufsfeld der Informations- und Kommunikationstechnologie (ICT). Der Verband ist zuständig für sämtliche eidgenössischen Berufsabschlüsse in der Informatik und Mediamatik und ist Prüfungsinstanz für fünf eidgenössische Fachausweise und zwei Diplome der ICT – darunter der eidgenössische Fachausweis Cyber Security Specialist (diese Prüfung kann nach dem Cyber Lehrgang Armee absolviert werden) und das eidgenössische Diplom ICT Security Expert.

→ **TIE International** ist ein führender Anbieter von Ausbildung im Bereich der ICT.

→ **Cybercon** ist mit seiner mehrjährigen Erfahrung im Finanz- und Verteidigungssektor befähigt, in den verschiedenen Domänen der Cyber-Sicherheit, des Cyber-Incident-Managements, der Härtung von IT-Infrastruktur, dem Sammeln und Auswerten von Security Logs sowie der Bekämpfung von Malware oder der kontinuierlichen Verbesserung ihrer Abwehrmassnahmen zu unterstützen.



Armeeangehörige werden in der Cyber-Abwehr ausgebildet. Bild: Clemens Laub, VBS

zungs-Organisation zu einem militärischen Kommando Cyber weiterentwickelt, das sich künftig auf die einsatzkritischen Leistungen fokussiert.

Elo Op Schulen 64 und Cyber Bat 42

In den Elo Op Schulen 64 werden, zusammen mit den Funkaufklärern, auch die Cyber-Spezialisten ausgebildet. Zurzeit sind es rund 40 pro Jahr; die Zahl soll ab 2025 kontinuierlich auf 80 Cyber-Spezialisten pro Jahr erhöht werden. Die militärischen Cyber-Spezialisten werden technisch wie auch im Bereich Leadership ausgebildet. So werden alle im Rahmen ihrer Ausbildung zu Unteroffizieren im Grad eines Wachtmeisters. Der Cyber-Lehrgang bietet allen Beteiligten einen Nutzen: Die Armeeangehörigen lernen in der Armee etwas, das sie für ihre berufliche oder akademische Laufbahn nutzen können. Die Privatwirtschaft profitiert von gut ausgebildeten Fachkräften, welche direkt im Arbeitsmarkt bestehen können. Die Armee profitiert durch das Milizsystem von stetig besser werdenden Cyberdefence-Spezialisten.

Die Ausbildung der militärischen Cyber-Spezialisten basiert auf einer engen Zusammenarbeit zwischen dem Kommando Ausbildung und dem zukünftigen Kommando Cyber. Im Rahmen der Cyber-Ausbildung kooperiert die Armee auch erfolgreich mit den Partnern aus dem Sicherheitsverbund Schweiz und den Betreibern kritischer Infrastrukturen. So besteht die Möglichkeit für die Teilnehmenden, während der Phase des praktischen Dienstes ein Praktikum bei einem Betreiber einer kritischen Infrastruktur oder bei einer Strafverfolgungsbehörde zu machen. Das Interesse der Partner für solche Praktika übersteigt den Bestand an Teilnehmenden im Lehrgang bei Weitem. Dies zeigt, dass die Cyber-Ausbildung der Armee in der Wirtschaft und bei anderen Partnern bereits heute sehr gut etabliert ist.

Nach dem Cyber-Lehrgang der Armee haben Absolventen die Möglichkeit, zusätzlich den Fachausweis zum «Cyber Security Specialist» zu erlangen. An ausgewählten Hochschulen und Fachhochschulen wird ihnen zusätzlich die Ausbildung in der Armee mit ECTS-Punkten angerechnet. Alle Wachtmeister des Cyber-Lehrgangs werden nach abgeschlossener Ausbildung ins Cyber Bataillon 42 eingeteilt. Dieses Bataillon, welches seit Anfang 2022 besteht, hat die Berufsorganisation Kommando Cyber in den Bereichen Eigenschutz und Abwehr, Aufklärung und Wirkung sowie in den militärischen Führungsprozessen zu unterstützen ebenso wie die Fachstelle Kryptologie im Kommando Cyber in der Kryptologie-Leistungserbringung fachlich und personell.

Das Cyber Bataillon 42 erbringt seine Leistungen ganzjährig im Detachements-Betrieb. Somit stehen dem Kommando Cyber permanent Cyber-Spezialisten für die Auftragserfüllung zur Verfügung. Dies ist insofern sehr wichtig, da die Herausforderungen im Cyberumfeld bereits heute komplex und herausfordernd sind. Dieser Truppenkörper vereint das Beste aus Wirtschaft und Wissenschaft, wenn es ums Thema Cyber geht. Die Angehörigen des Bataillons sind nicht nur technische Spezialisten, sondern auch innovative und kreative Problemlöser, welche sich durch eine überdurchschnittliche Motivation auszeichnen. Das Bataillon ist ständig auf der Suche nach jungen Schweizerinnen und Schweizer, welche sich für das Thema Cyber interessieren. Interessierte Quereinsteiger finden weiterführende Informationen auf der Homepage www.cyberdefence.ch ■

Oberst Ernesto Kägi
Ehem. DC Kdo FAK 4
Pz Br 11 und Inf Br 7
8965 Berikon

INFORMATIONSRAUM

Korpskommandant Thomas Süssli
Chef der Armee

«Stehen wir der Beurteilung einer militärischen Lage gegenüber, denken wir uns neben den bewährten Punkten wie Auftrag, Mittel, Gelände und Feind mit Vorteil in die Lage des Gegners hinein.» Diese Zeilen, geschrieben von Major Stäuber in der ASMZ vom Januar 1958, zeigen: Es gibt Strategien, die Jahrzehnte (wenn nicht sogar Jahrhunderte) gleichbleiben. Was sich aber sehr wohl und immer schneller ändert, sind die Einsatzfelder.

Heute ist es von zentraler Bedeutung, sich Wissens- und Entscheidungsvorsprung zu verschaffen. Die Schweizer Armee muss zum Beispiel heute und in Zukunft in der Lage sein, ihre Informatiksysteme gegen Cyberangriffe zu schützen. Auch muss die Armee in den Operationssphären elektromagnetischer Raum und Cyberraum Wirkungen entfalten können.

1958 strich Major Stäuber die Bedeutung der Parlamentszustimmung zu einem Panzerübungsplatz in der Ajoie heraus. Neue Truppenübungsplätze sind für uns im Jahr 2023 noch immer wichtig, genauso wichtig ist jedoch das Kommando Cyber mit der elektronischen Abteilung 46 geworden.

Wir müssen uns auch im Alltag gegen Akteure mit kriminellen und nachrichtendienstlichen Absichten schützen. Dieser Schutz im eigenen Cyberraum bedeutet für die Armee, Cyberangriffe jederzeit zu erkennen und die Angreifer in der Erreichung ihrer Ziele stören zu können. Das heisst: Wer beispielsweise schneller entscheidet, wo Verbände oder Waffenwirkungen zum Einsatz gelangen, behält die Oberhand. Daraus resultiert das Ziel, den eigenen Truppen einen Wissens- und Entscheidungsvorsprung zu verschaffen. Gleichzeitig soll der gegnerische Akteur mit einem Wissens- und Entscheidungsrückstand zu kämpfen haben, um ihn in die Rolle des Reagierenden zu zwingen.

Mit solchen Angaben hätte Major Stäuber vor 60 Jahren wohl nicht viel anfangen können. Folgende Aussage hätte er aber sofort unterschrieben: Die Schweizer Armee muss agil bleiben, um sich auf immer wieder ändernde Gefahren einstellen zu können.