Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 189 (2023)

Heft: 7

Artikel: "Wir bilden die digitale Wirbelsäule der Armee"

Autor: Kägi, Ernesto / Vuitel, Alain

DOI: https://doi.org/10.5169/seals-1052753

«Wir bilden die digitale Wirbelsäule der Armee»

Divisionär Alain Vuitel ist überzeugt, dass das Kommando Cyber dank permanenter Lageverfolgung, intensiver Zusammenarbeit zwischen Key-Playern, gut ausgebildeten Cyberdefence-Spezialisten und dem Einsatz der geeignetsten Tools als erste Verteidigungslinie die einsatzkritische IKT-Infrastruktur der Schweizer Armee wirkungsvoll schützen kann. Und im Interview weist der Projektleiter auf die epochale Bedeutung des Cyber-Kommandos hin.

Ernesto Kägi im Gespräch mit Alain Vuitel

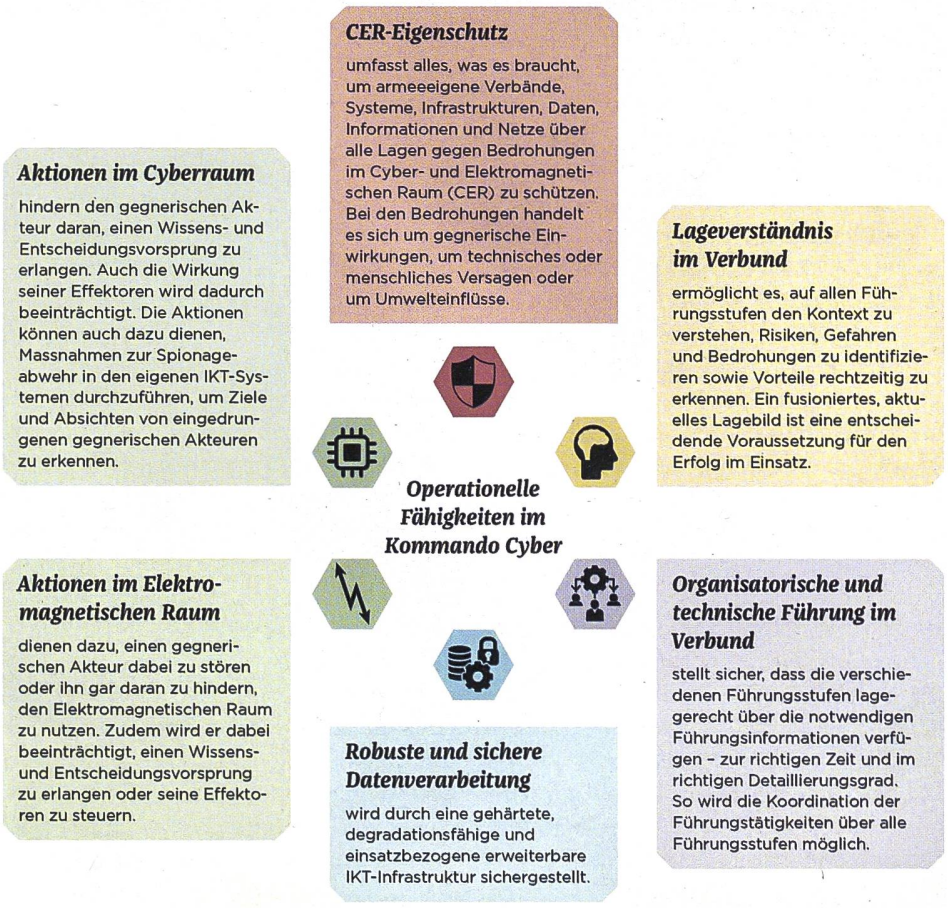
Der Bundesrat hat Ihnen den Auftrag gegeben, die Option 3 der Gesamtkonzeption Cyber weiter zu bearbeiten. Welches ist für Sie der wesentlichste Auftrag aus diesem Konzept und gilt dieser nur fürs VBS?
DIVISIONÄR ALAIN VUITEL: Das Kommando Cyber wird vier Kernaufgaben haben. Zunächst stellt es den Schutz der eigenen Infrastruktur und der Systeme im Cyber- und elektromagnetischen Raum sicher. Dann schöpft es das Potenzial der Digitalisierung aus. Dabei geht es darum, einen Wissens- und Entscheidungsvorsprung für unsere Kommandanten zu erlangen, um die richtigen Mittel am richtigen Ort und zur richtigen Zeit einsetzen zu können. Drittens gilt es, die Handlungsfreiheit im Cyber- und elektromagnetischen Raum sicherzustellen. Und viertens gehört die kontinuierliche Lageverfolgung und -aufbereitung rund um die Uhr, an 365 Tagen im Jahr, dazu.

Unser originärer Auftrag ist der Schutz der einsatzkritischen Infrastruktur und der Systeme der Schweizer Armee. Aber subsidiär können wir auch für andere einsatzkritische Institutionen unsere Leistungen erbringen, etwa für das Bundesamt für Bevölkerungsschutz. Diesem werden wir unser Führungsnetz Schweiz zur Verfügung stellen. Leistungen für andere Departemente sind ebenfalls möglich.

Beeindruckend ist die angestrebte dreifache Win-Situation, in der die Armee junge Leute gratis und franko zu Cyberdefence-Spezialisten ausbildet, die zivil der Wirtschaft den eklatanten Fachkräftemangel in diesem Bereich lindern helfen und die in den anschliessenden WKs der Armee immer wieder zusätzliches Cyber-Know-how zurückbringen. Sind sie sicher, dass dieses Dreieck gut funktionieren wird?
Absolut sicher! Ich konnte gerade kürzlich in der Cyber Commander Conference der EU in Brüssel unser Cyber-Ausbildungsprogramm und das Milizsystem der Schweizer Armee präsentieren. Dieses ist in Europa einzigartig und ich spürte, dass unser Milizsystem auf grosses Interesse stösst. In der Tat ist es so, dass im Cyberdefence-Bereich der Milizgedanke – vielleicht abgesehen von Piloten und teilweise den Genietruppen – am eindrücklichsten greift: Jemand ist Soldat und in seinem Berufsleben macht er genau das Gleiche. Der gegenseitige Nutzen ist enorm. Dass wir als Armee junge Leute, auch solche aus dem Berufsleben und ohne Matura, innert zehn Monaten konzentriert zu Cyberdefence-Spezialisten ausbilden, welche anschliessend operationell einen entsprechenden Beruf in der Wirtschaft ergreifen können, macht uns stolz.

Als Arbeitgeber hat das Kommando Cyber nicht den Anspruch, dass unsere Angestellten ihr ganzes Berufsleben bei uns arbeiten. Ich denke, eine berufliche Durchlässigkeit zwischen Wirtschaft und Sicherheitssektor ist wichtig, also dass zum Beispiel jemand, der den Cyber-Lehrgang absolviert hat, bei uns im Kommando Cyber eine Festanstellung erhält und eine gewisse Zeit für uns arbeitet. Vielleicht arbeitet diese Person dann fünf oder zehn Jahre in der Wirtschaft oder in einem Polizeikorps und kehrt dann wieder zu uns zurück – mit wertvollen neuen Impulsen, Kenntnissen und anderen Sichtweisen.

Ist das zukünftige Kommando Cyber eine Art erste Verteidigungslinie im Cyber- und elektromagnetischen Raum?
Das ist korrekt. Weil die Informatik so essenziell geworden ist, müssen wir sie



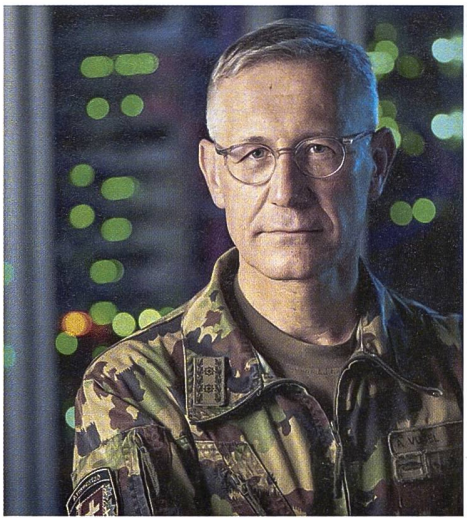
▶ **Die Gesamtkonzeption Cyber sieht sechs operationelle Fähigkeiten vor.** Grafik: Kdo Cyber

wirksam schützen. Eine moderne Luftwaffe ohne sichere Informatik- und Kommunikationsmittel taugt ebenso wenig wie ein Heer ohne ein funktionierendes Führungsinformationssystem. So soll es sein und ich begründe dies wie folgt: Die Informatik ist dermassen essenziell, dass man sie wirksam schützen muss.

Gerne verwende ich eine Analogie, um die Relevanz des Kommandos Cyber greifbar zu machen: Wir bilden die digitale Wirbelsäule der Armee. Uns Menschen hält unsere Wirbelsäule aufrecht, trägt uns und verbindet unsere Gliedmassen mit unserem Hirn. Wir spüren unsere Wirbelsäule grundsätzlich nicht; für unsere Beweglichkeit und Agilität ist sie aber von entscheidender Bedeutung. Genau das ist das Kommando Cyber für die Schweizer Armee: Ohne funktioniert das Gesamtsystem nicht. Aber dies bedingt zwingend, dass die Wirbelsäule nicht blockiert oder weh tut.

Gilt der Ausdruck «In Krisen Köpfe kennen» auch für den Cyber-Bereich?
Auf jeden Fall. Wir sind mit diversen anderen Akteuren rund um systemrelevante IKT-Infrastrukturen im Austausch. Dies sind beispielsweise die Swisscom, Post, Swissgrid, ETH und Universitäten, Polizeikorps usw. Alle haben ihre eigenen Sensoren und agieren im Rahmen ihrer gesetzlichen Möglichkeiten. Das Schöne an der kleinen Schweiz ist, dass man sich kennt und sich vertraut. Die ETH ist übrigens weltweit führend im Bereich Kryptologie. Auch hier arbeiten wir zusammen.

Der Mensch scheint im Cyber-Bereich, nebst seinen IT-Fähigkeiten, besonders wichtig zu sein. Warum ist das so?
Die Fähigkeiten eines Cyber-Spezialisten gehen über die Bedienung eines Waffensystems hinaus. Der Ukraine-Krieg zeigt, dass Soldaten neue Waffen in Rekordzeit kennenlernen und bedienen können. Beim Cyber-Spezialisten verhält sich dies anders. Eine Ausbildung, die ihn befähigt, einsatzkritische IKT-Infrastrukturen wirkungsvoll schützen zu können und evtuell sogar Gegenangriffe auszuführen, dauert sehr viel länger. IKT-Spezialisten gelten gemeinhin als Einzelkämpfer im stillen Kämmerlein. Das ist ein völlig falsches Bild. Sie müssen ein grosses Mass an Teamfähigkeit mitbringen. Deshalb müssen sie beispielsweise beim Eintritt ins Talentprogramm Sparc nicht zwingend IT-Cracks sein, denn Wissen kann man sich aneignen. Ganz wichtig sind



Divisionär Alain Vuitel ist der Projektleiter des Kommandos Cyber. Bild: Philipp Schmidli, VBS.

uns aber Charaktereigenschaften wie Teamgeist und eine kommunikative Sozialkompetenz, denn Cyber ist ein absoluter Teamsport. Wir brauchen ein eingeschworenes Fussballteam und keine Einzelkämpfer.

Wir haben das Glück, dass das Interesse am vordienstlichen Sparc-Lehrgang bei 16- bis 20-jährigen jungen Leuten sehr gross ist. Das erlaubt uns, dass wir im Sinne eines langen Assessments während Sparc und in der RS die Besten auswählen können. Was bei Sparc und beim Cyber-Lehrgang ebenfalls zum Tragen kommt: Anders als beispielsweise bei der Infanterie müssen unsere Cyber-Talente nicht die gleichen physischen und sportlichen Komponenten mitbringen. Wir möchten dies stärker fördern, damit auch Menschen mit einer körperlichen Beeinträchtigung Dienst leisten können.

Was ist das ganz Spezielle am Cyber- und elektromagnetischen Raum?
Im Cyberraum verschwinden die geografischen Grenzen und Distanzen, was bedeutet, dass wir jeden Tag rund um die Uhr im Einsatz sind. Denn der Gegner ist dies ebenfalls. Es ist eine völlig andere Operationssphäre; das ist der grosse Unterschied zu anderen militärischen Operationen.

Hat ein Cyber-Wachtmeister auch die Möglichkeit, anschliessend Offizier zu werden?
Ja, gegenwärtig erhalten etwa vier Wachtmeister pro Schule den Offiziersvorschlag und absolvieren dann die Offiziersschule im Lehrverband Führungsunterstützung. Dort lernen sie die Armee ausserhalb von Cyber kennen und lernen führen. Bisher haben wir eine Kompanie von Cyber-Spezialisten. In ein paar Jahren wird das Cyber-Bataillon 42 voll alimentiert sein. Dann brauchen wir auch mehr Kader.

Was sind für Sie als Projektleiter Kommando Cyber persönlich die grössten zukünftigen Herausforderungen?
Die ganze Informations- und Kommunikationstechnologie lebt von und mit Menschen. Unser Personal ist das A und O. Man spricht heute viel von «artificial intelligence», «ChatGPT», künstlicher Intelligenz usw. Es ist in der Tat unglaublich, was auf diesem Gebiet bereits alles passiert ist und noch geschehen wird. Aber am Ende ist es der Mensch, der mit einem guten Riecher und über sein Bauchgefühl alles steuert. Meine Herausforderung ist es, die richtigen Fachkräfte zu finden. Menschen, die nicht nur gut ausgebildet sind und nicht nur für Geld arbeiten, sondern auch den tieferen Sinn ihrer Arbeit sehen, nämlich die Sicherheit der Schweiz sicherzustellen.

Die zweite Herausforderung ist, das Mindset so zu verändern, dass wir in der Armee das Potenzial der Digitalisierung ausschöpfen. Das ist ein Paradigmenwechsel und nicht mehr Normalbetrieb à la «wie immer». Man muss in Zusammenhang mit einer wirksamen Cyberdefence bereit sein, Altbewährtes infrage zu stellen und neue Ansätze zu akzeptieren. Ein anschauliches Beispiel ist die Entwicklung des Smartphones in den letzten 30 Jahren. Die industrielle Revolution hat rund 200 Jahre gedauert, von der Entwicklung der ersten Dampfmaschine bis heute. Die IT-Revolution läuft seit zirka 30 bis 35 Jahren.

Was heisst diese rasante Entwicklung für den Einsatz einer Armee? Was heisst das für die Ausbildung einer Milizarmee? Was bedeutet das für die Rekrutierung einer modernen Armee? Das hat durchaus revolutionären Charakter. Mit der Bildung des Kommando Cyber schreiben wir Geschichte. Das letzte Mal, als die Armee ein völlig neues Element kreiert hat, war 1914 mit der Schaffung unserer Luftwaffe. Und 2024, genau 110 Jahre später, schaffen wir ein neues Kommando Cyber, welches in einem völlig neuen Umfeld arbeitet. Und damit werden ganz neue Möglichkeiten eröffnet. ■

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