«Wir sind Freiheitskämpfer»

Divisionär Alain Vuitel leitet seit Mai 2021 als Projektleiter das Projekt Kommando Cyber. Er ist verantwortlich für die Führung des Projekts und den schrittweisen Aufbau des Kommandos Cyber der Armee. Er ist direkt dem Chef der Armee unterstellt und ist Mitglied der Armeeführung. Die Rohstruktur des Kommandos soll Ende 2021 erarbeitet sein. Ab 2022 soll das Cyber Bataillon 42 bereit sein.

Oberst Felix Meier

Herr Divisionär, Ihre Laufbahn und Ihre Verwendungen in unserer Armee sind höchst eindrücklich. Welche Erkenntnisse und Erfahrungen nehmen Sie in Ihre neue Funktion mit?

Divisionär Alain Vuitel: Auf meiner Laufbahn als ziviler und uniformierter Angestellter im VBS konnte ich in der Tat wichtige Erfahrungen sammeln. Eine Erkenntnis, die ich bei all diesen Aufgaben gewonnen habe und die mich heute als Projektleiter Kommando Cyber täglich begleitet, ist die Bedeutung des Wissens- und Entscheidungsvorsprungs.

Um die Führungsfähigkeit sicherzustellen, muss eine Führungskraft möglichst umfassendes Wissen über eine Situation erlangen. Nur so kann sie oder er eine fundierte Entscheidung treffen. Daten und daraus gewonnene Informationen sind hier tatsächlich unser wertvollstes Gut. «This is core Business».

Diesen Wissensvorsprung zu erlangen, wird ein Kerngeschäft des Kommandos Cyber sein, nämlich erstens die IKT*-Sicherheit zu gewährleisten, zweitens das Potenzial der Digitalisierung auszuschöpfen sowie drittens die Erlangung der Hand-

Bild: VBS

«Heute gibt es keine militärischen Mittel mehr ohne IKT-Anteil», Divisionär Alain Vuitel, Projektleiter Kommando Cyber.

*IKT: Informations- und Kommunikationstechnologie

lungsfreiheit im Cyber- wie im elektromagnetischen Raum. Es spornt mich ungemein an, hier einen so gewichtigen Beitrag für die ganze Armee leisten zu können.

Welches ist der Zeitrahmen im Projekt-Aufbau, wie wird das Kommando Cyber zusammengesetzt werden, welche Funktionen wird es vereinen und wie wird die Unterstellung sein?

Vuitel: Auf den 1. Januar 2024 soll das Kommando Cyber gebildet sein. Bis dahin ist es eine Projektorganisation. Das Kommando Cyber wird dem Chef der Armee unterstellt, so ist es aktuell auch mit dem Projekt Kommando Cyber. Im Moment sind wir mit rund 30 Mitarbeitenden in der Phase Initialisierung.

Abgeleitet aus den Fähigkeiten geht es darum, die Grundlagen für die nächste Projektphase zu entwickeln. Das zukünftige Kommando Cyber soll ein einsatzorientiertes Kommando sein, in welchem sich Berufs- und Milizpersonal auf hochsichere und robuste IKT (Informations- und Kommunikationstechnologie) ausrichten, sowie Aktionen im elektromagnetischen- und Cyberraum 365/24 führen.

Eine Strategie des VBS und der Armee ist die digitale Transformation. Was will man damit genau erreichen? Die Optimierung militärischer Führungsprozesse muss darauf ausgelegt sein, die Qualität und/oder die Geschwindigkeit in der Entschlussfassung zu erhöhen. Tut dies die Digitalisierung, und wenn ja, können Sie uns konkrete Beispiele nennen?

Vuitel: Wir im Projekt Kommando Cyber und auch in der FUB sind Freiheitskämpfer. Wir wollen die Daten aus den Silos, in denen sie sich befinden, befreien. Heute gibt es tatsächlich für fast jedes System ein eigenes Daten-Silo. Die Systeme generieren auch eine immer grösser werdende Menge von Daten, diese zu fusionieren ist heute sehr aufwendig und träge.

Es geht darum, dass wir Silo-übergreifend Daten fusionieren können, erst so wird es zum Beispiel möglich, dass ein Entscheidungsträger über fundierte Informationen verfügt, welche aktuell und skalierbar sind und in einem verständlichen Lagebild dargestellt werden. So kann ein entscheidender Wissensvorsprung erlangt werden. Die Verfügbarkeit, Vernetzung und Integrität von Daten sind zum Beispiel für das Luftlagebild zentral.

Wie stellt man sicher, dass das enorme Mengengerüst an IT-Mitteln, nämlich die Vielfalt, die Qualität und Quantität, welche man im Cyber-Bereich beschaffen will, tatsächlich unseren polyvalenten Bedürfnissen entsprechen und nach den eher langen Beschaffungsprozessen beim Roll-out nicht bereits veraltet sind?

Vuitel: Die aktuellen Beschaffungsprozesse der Verwaltung sind eindeutig zu langsam für die IKT-Mittel. Dies wurde auch bereits in einem externen Bericht festgehalten, dessen Ergebnisse im Sommer 2020 vorgelegt wurden.

Hier werden nun nötige Massnahmen getroffen, damit wir den technologischen Fortschritt auch für uns nutzen können. Die Armee ist hier jedoch an Vorgaben vom Beschaffungsprozess gebunden und kann nur bedingt etwas dazu beitragen.

Erstaunlicherweise benötigen Cyber-Kräfte gar nicht so grosse Mengen an IT-Mitteln. Die Technologieentwicklung im Cy-

Kolumne

Fokus CdA

Kürzlich habe ich eine Gruppe von Fallschirmgrenadieren getroffen, die vor genau 50 Jahren zusammen brevetiert worden sind. Sie rückten während des Kalten Krieges in die Rekrutenschule ein, drei Jahre nach dem Einmarsch der Truppen des Warschauer Pakts in die Tschechoslowakei. Ihre damalige Ausbildung war komplett einsatzorientiert und praktisch ausnahmslos «im scharfen Schuss». Sie waren extrem fokussiert.

Diese Erkenntnisse sind gerade in Bezug auf Ausbildung und Bereitschaft unverändert gültig. Deshalb möchte ich nicht mehr von Wiederholungskursen reden, sondern von Einsatzvorbereitungen. Bei allen Aktivitäten muss der Fokus auf möglichen Einsätzen liegen. Jeder Tag im Dienst soll eine Vorbereitung auf mögliche Einsätze sein. Und gerade die Kader aller Stufen müssen immer wieder überprüfen, ob ihre Tätigkeiten relevant sind im Hinblick auf Einsätze.

Damit übereinstimmend lautet der erste der vier strategischen Grundsätze der Vision 2030: Denken und Handeln auf den Einsatz ausrichten. Dies wird zum Teil bereits heute konsequent gelebt. Die Sanitätstruppen zum Beispiel haben letztes Jahr im Rahmen des Assistenzdienstes zugunsten des zivilen Gesundheitswesens unter Beweis gestellt, dass sie sich richtig vorbereitet haben. Sie haben mit den Einsätzen in Spitälern während der WKs das Richtige trainiert. Und die Armee hat gezeigt, dass sie bereit ist, wenn es sie braucht.

Wir müssen auch in Zukunft richtig auf Bedrohungen und Gefahren reagieren können. Die Aufgabe der Armee ist es, langfristig Sicherheit zu gewährleisten. Dafür muss sie robust, durchhaltefähig und konsequent auf Einsätze ausgerichtet sein. Und jederzeit und in allen Lagen kämpfen, schützen und helfen können.

Korpskommandant
Thomas Süssli
Chef der Armee

berbereich geht derart schnell, dass hier in der Regel hochwertige zivile Systeme beschafft werden, was den Prozess vereinfacht. Zudem ist das «Schlüsselsystem Cyber» der hochqualifizierte Spezialist und nicht ein «Supercomputer».

Der Schutz vor Cyberangriffen ist der Auftrag des Kommandos Cyber. Können Sie konkret erläutern, was genau geschützt wird (mil Infra, ziv Infra, priv Infra, etc.) und wie der Grundentschluss für diesen Schutz lautet?

Vuitel: Die Armee ist in erster Linie dazu da, die eigenen Systeme zu schützen, damit diese einsatzfähig bleiben. Das Kommando Cyber wird auch zukünftig im Rahmen der Armeeaufgaben subsidiäre Leistungen erbringen, zum Beispiel im Rahmen der Unterstützung von zivilen Behörden.

Eine fachspezifische Unterstützung im Bereich Cyber wird wie jedes Unterstützungsbegehren der Behörden durch die Armee beurteilt und beantwortet. Die Armee kann den Kantonen, dem Sicherheitsverbund oder der Wirtschaft subsidiär nur Unterstützung bieten, wenn die folgenden Bedingungen erfüllt sind: die zivilen Mittel sind erschöpft, geeignete militärische Mittel sind vorhanden und die Bewilligung der politischen Behörden liegt vor. Also gleich wie bei der Corona-Pandemie, ausser dass dann keine Sanitätssoldaten, sondern Cybersoldaten ausrücken.

Wie gestalten sich die Abgrenzung und auch die Kooperation im Bereich Cyberschutz zwischen zivilen Institutionen und dem Militär, und in welcher Ausprägung ist die internationale Kooperation vorgesehen?

Vuitel: Die Cybersicherheit in der Bundesverwaltung basiert auf drei Säulen und ist organisatorisch getrennt, prozessual aber miteinander verbunden z.B. im Bereich der Analyse von Cyberrisiken. Das EJPD ist für die Cyberstrafverfolgung zuständig und kooperiert dabei eng mit den kantonalen Strafverfolgungsbehörden. Im EFD wird durch das Nationale Zentrum für Cybersicherheit (NCSC) das Thema Cybersicherheit behandelt. Das NCSC kooperiert dabei eng mit bundesinternen und -externen Stellen, z.B. dem Nachrichtendienst des Bundes oder Betreibern von kritischen Infrastrukturen. Das VBS ist schlussendlich für den Bereich Cyber Defence zuständig.

Die Armee nimmt regelmässig an internationalen Cyberübungen teil. Da findet ein wichtiger Wissensaustausch statt, und die Erfahrungswerte, welche dabei gesammelt werden, fliessen wieder zurück in die eigene Organisation.

Eine Armee ist ein Gesamtsystem. Das Zusammenwirken sphärenübergreifender Mittel zur Auftragserfüllung ist essentiell. Das Gros unserer heutigen Mittel ist am Boden und in der Luft. Wird es 2030 so sein, dass die Mittel im Cyberraum überwiegen und nicht zuletzt auch aus Budgetgründen die Sphäre Boden nur noch über leichte Mittel verfügen wird?

Vuitel: Die Gewichtung der Fähigkeiten ist auch eine politische Frage. Sie wird regelmässig über die Rüstungsplanung gemacht. Die Ressourcen sind immer eine Herausforderung. Umso mehr geht es darum, dass sich Fähigkeiten und nicht zuletzt Mittel gegenseitig ergänzen und miteinander eine Gesamtwirkung erbringen. Im Fokus steht immer die Bedrohung. Wie die Priorisierung im Jahr 2030 aussehen wird, kann ich nicht beantworten. Die Bedrohung im Cyberraum markiert aber auf jeden Fall eine neue Verteidigungslinie, an der die Armee noch stärker gefordert ist.

Die Beschaffung neuer Kampfflugzeuge und Bodluv-Mittel stehen vor der Türe. Können Sie uns erläutern, wie diese aktuellen Rüstungsgeschäfte mit dem Bereich Cyber verknüpft sind und was der Auftrag des Kdo Cyber im Bereich der integrierten Luftverteidigung in Zukunft sein wird?

Vuitel: Heute gibt es keine militärischen Mittel mehr ohne IKT-Anteil. Aus diesem Grund konzentrieren wir uns insbesondere im Projekt Kommando Cyber darauf, mit dem Aufbau der neuen IKT-Plattform die idealen Voraussetzungen zu schaffen, damit die verschiedenen Mittel zusammen ihre volle Wirkung entfalten können. Diese IKT-Infrastruktur ermöglicht der Armee den Schritt in die Digitalisierung und die Schaffung eines zeitgemässen Wissens- und Entscheidungsvorsprungs. Jedes neue System und auch Informationen über das System müssen auch vor den Bedrohungen aus dem Cyberraum geschützt werden können. Dies gilt auch für neue Kampfflugzeuge und Systeme der BODLUV. Eine gut funktionierende Cyber Security ist darum unabdingbar und zwar über alle Bereiche der Instandhaltung, des Betriebes und des Einsatzes der Systeme und über alle Lagen.

Nicht zu Land, zu Wasser oder in der Luft, sondern immer mehr auch im virtuellen Raum finden die Kriege der Zukunft statt. Vom Cyber-Krieg ist warnend die Rede. Die NATO hat deshalb die Cyber-Verteidigung ganz oben auf ihre Prioritätenliste gesetzt. Das Cyber-Verteidigungszentrum der NATO liegt in der estnischen Hauptstadt Tallinn, also am nordöstlichen Rand der mächtigsten Militärallianz der Welt. Hier werden Cyber-Angriffe simuliert und Abwehrmassnahmen geprobt, aber auch Cyberwar-Spezialisten ausgebildet. Es werden Strategien ausgeheckt und die völkerrechtlichen Konsequenzen für virtuelle Kriege diskutiert. Gemäss einer Mitteilung von SRF im Jahre 2013 soll sich die neutrale Schweiz möglicherweise schon bald am NATO-Kompetenz-Zentrum für Cyber-Abwehr im estnischen Tallinn beteiligen. Eine Partnerschaft werde geprüft, bestätigte damals das Aussendepartement zu Recherchen von SRF. Wie ist der Stand dieser möglichen Partnerschaft?

Vuitel: Diese Partnerschaft ist heute sehr lebendig. Im Rahmen des vom Bundesrat verabschiedeten Ausbildungsprogramms nehmen wir regelmässig an Übungen des Cooperative Cyber Defence Center of Excellence (CCDCOE) teil. Der Austausch ist sehr wertvoll und die Erkenntnisse aus den Übungen fliessen direkt in unser Tagesgeschäft ein. Zudem wird schon bald eine Mitarbeiterin aus dem Kommando Cyber gemeinsam mit einem Mitarbeitenden der Armasuisse für zwei Jahre beim Cooperative Cyber Defence Centre of Excellence in Tallinn (Estland) arbeiten und in diversen Arbeitsgruppen mitwirken.

Herr Divisionär, wir danken Ihnen herzlich für dieses Gespräch.