Höhere Kaderausbildung und "Cyber" : eine Bestandesaufnahme

Autor(en): **Keller, Daniel / Kuhnen, Stephan**

Objekttyp: **Article**

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

Band (Jahr): **184 (2018)**

Heft 1-2

PDF erstellt am: **03.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-772496

Höhere Kaderausbildung und «Cyber»: Eine Bestandesaufnahme

In den Kaderlehrgängen der HKA werden die Teilnehmer dazu geführt, sich mit dem Thema «Cyber» auseinander zu setzen. Dieses wird abhängig von Führungsstufe und Funktion behandelt, wobei unter «Cyber» in diesem Artikel Cyber-Schutz verstanden wird. Gemeinsamer Nenner über alle Lehrgänge der HKA: «Cyber» ist zwingend in die Aktionsplanung einzubinden – zeitliche Abhängigkeit sowie Wechselwirkung zur eigenen militärischen Aktion werden angesprochen und dargestellt. *AM*

Daniel Keller, Stephan Kuhnen

Der Ausdruck «Cyber» wird umgangssprachlich als Synonym für Datenwelten und Internet verwendet. Der Cyber-Raum beschreibt die Umgebung, in welcher Daten elektronisch rechnergestützt, zeitverzugslos und vernetzt erfasst, gespeichert, verarbeitet und übermittelt werden. Daraus sich ergebende Auswirkungen können sowohl nicht greifbar (virtuell) als auch greifbar (physisch) sein. Es wird von Cyber-Krieg, Cyber-Bedrohung, Cyber-Schutz, Cyber-Verteidigung, Cyber-Ausbildung usw. gesprochen – Begriffe, die umgangssprachlich in wechselnden Kombinationen sowie zu allen möglichen Gegebenheiten verwendet werden. Jeder, der über entsprechende Mittel und Fähigkeiten verfügt, kann im Cyber-Raum agieren und diesen Raum als Aktionsraum nutzen. Umgekehrt gilt es, die eigenen IKT-Systeme und -Infrastrukturen stufengerecht mit geeigneten Massnahmen zu schützen. Im Aktionsplan Cyber-Defence VBS (APCD) vom 09.11.2017 steht: «Die Armee ist für die Verteidigung der eigenen IKT-Systeme und -Infrastrukturen verantwortlich. In Friedenszeiten sind aktive Gegenmassnahmen (Abwehr) der Armee zur Verteidigung ihrer eigenen IKT-Systeme und -Infrastrukturen genehmigungspflichtig.»

Ausgangslage: militärische Herausforderung

Die Führung von militärischen Aktionen im Cyber-Raum ist ausschliesslich Angelegenheit der operativen Stufe und dazu werden bestimmte Spezialisten und Organisationen aus der FUB eingesetzt. Dazu werden Mittel der FUB eingesetzt. Eigene IKT-Systeme und -Infrastrukturen vor gegnerischen Cyber-Aktionen zu schützen, ist aber Aufgabe jedes Benutzers, das heisst von allen unseren Kadern und Mannschaften. Zukünftige Kommandanten und Stabsoffiziere an den Lehrgängen der HKA haben deshalb den Auftrag, verantwortungsvoll mit den eingesetzten IKT-Mitteln umzugehen und möglichen Datenabfluss zu verhindern. Auf diese Weise kann jeder dazu beitragen, das eigene IKT-System vor gegnerischen Cyber-Aktionen zu schützen.

«Zukünftige Kommandanten und Stabsoffiziere an den Lehrgängen der HKA haben deshalb den Auftrag, verantwortungsvoll mit den eingesetzten IKT-Mitteln umzugehen und möglichen Datenabfluss zu verhindern.»

Die taktische Führungsstufe hat folgenden Handlungsbedarf:

- Ausbilden, befehlen und durchsetzen der Cyber-Schutzvorgaben und der regelkonformen Benutzung der IKT-Systeme und -Infrastrukturen im eigenen Verantwortungsbereich;
- Sicherstellen der Führungsfähigkeit des eigenen Verbandes, indem Eventualplanungen für Ausfall oder Beeinträchtigung der IKT-Systeme durch Cyber-Aktionen erstellt werden;
- Erziehen, führen und ausbilden der Unterstellten bei der Nutzung der Social-Medias, insbesondere was Informationen zur eigenen Funktion in der Armee, zu Dienstleistungen, Einsätzen und Übungen betrifft.

Ausgangslage: Fragestellungen bei der Kaderausbildung

Zu folgenden und anderen möglichen Fragen müssen sich die Teilnehmer an den Führungslehrgängen der HKA Gedanken machen.

Können …

- … infolge unberücksichtigt gebliebener Cyber-Schutzvorgaben Teile der Armee ihre Aufgaben gar nicht erst übernehmen (weil diese Teile bereits viel früher unvorsichtig mit Daten umgegangen sind)?
- … infolge unvorsichtigem Umgang mit Zugangsdaten (z.B. SmartCard und persönlicher PIN) Unberechtigte auf das eigene IKT-System zugreifen, sich Daten beschaffen oder gar Geräte und Systeme zeitlich begrenzt oder dauerhaft nicht verfügbar machen?
- … einsatzgegliederte Formationen und Verbände (Personal, Mittel und Ausrüstung) gar nicht am verlangten Ort zusammengeführt werden, weil Mobilisierungs- und Koordinationsverfahren und -abläufe von aussen nachhaltig beeinflusst wurden?
- … im Einsatzfall Schlüsselpersonen ausfallen, weil Einzelne gezielt als wichtige Ziele in Social-Medias ausgesucht und durch die gewonnenen persönlichen Daten mit einfachen Mitteln ausgeschaltet werden?
- … gegnerische Einflüsse in sozialen Netzwerken als Folge von Cyber-Beeinflussungsmassnahmen im Cyber-Raum so dominant sein, dass Teile der Armee ihre Aufgabe nicht mehr wahrnehmen wollen?

- … zum Eigenschutz gehärtete Systeme von Armee und militärischer Verwaltung so stark an Agilität verlieren, dass sie nicht mehr glaubwürdig und effizient eingesetzt werden können oder gar zeitweise ausfallen?

Obwohl nicht alle Fragestellungen auf der taktischen Führungsstufe beantwortet werden können, dienen sie dem Gesamtverständnis und führen die Teilnehmer an die bereits heute sehr reale und bestehende Bedrohung heran. Am Ende von Beurteilen und Planen soll der Teilnehmer im redigierten Befehl unter den besonderen Anordnungen eine konkrete, machbare und durchsetzbare Handlungsanweisung für Unterstellte formulieren.

Erkenntnisse für die Ausbildung an der HKA

Eigenverantwortung

Die Eigenverantwortung des Einzelnen ist hoch. Das Bewusstsein um die Verletzlichkeit der eigenen IKT-Systeme und -Infrastrukturen sowie die daraus folgende mögliche Angreifbarkeit wird durch die HKA in allen Lehrgängen laufend verstärkt. Allfällige Angriffe erfolgen an Orten und in Bereichen, die nicht vorhersehbar sind. Betroffen sind alle Führungsstufen. Sorglosigkeit und Verletzen bestehender Grundregeln können zu echten Schwierigkeiten führen.

Cyber-Schutz

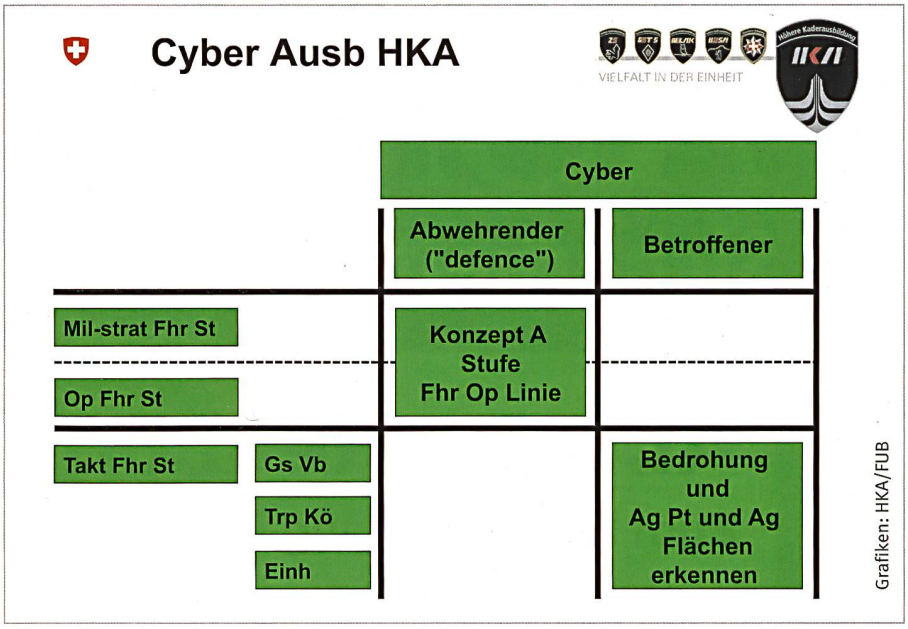
Aufgrund der kritischen Abhängigkeit der militärischen Einheiten zu den IKT-Systemen und -Infrastrukturen muss der Cyber-Schutz in allen Bereichen angewendet und hoch gehalten werden.

Schutz von Informationen

Der Schutz von Informationen ist wichtiger denn je, denn diese, z.B. Identitäten, Listen aller Art (Material, Notfall), Kommandierungen usw. erlauben einem Angreifer, sich ein Gesamtbild zu verschaffen. Sie erlauben, in IKT-Systeme und –Infrastrukturen, von denen die Aktion abhängt, präzise einzugreifen. Sie stellen Ziele (System, Funktion) dar, über die der Angreifer Vertraulichkeit, Integrität und Verfügbarkeit beeinträchtigt.

Antizipation

Der Gegner bereitet seine Aktivitäten im und aus dem Cyber-Raum bereits jetzt und heute vor. Er versucht, aus vielen und unterschiedlichen Quellen Daten und Informationen aller Art zu sammeln sowie sich Zugänge zu verschaffen, um diese später zu verwenden. Das Ziel kann sein, Aktionen, Einsätze und Operationen später zu manipulieren oder sogar zu verhindern. Darum ist es wichtig, sich mit dem Thema Cyber- und Informationsschutz zu befassen, bevor die militärische Auseinandersetzung beginnt. Cyber- und Informationsschutz ist eine permanente Aufgabe, um Absichten des Gegners frühzeitig zu erkennen und zu durchkreuzen.



Konzept Cyber-Ausbildung an der HKA.

Konsequenzen für die Ausbildung an der HKA

Für die Teilnehmer an den Lehrgängen der HKA geht es darum, den Cyber-Raum als gegnerischen und eigenen Wirkungsraum zu erkennen. Der Teilnehmer muss Cyber-Bedrohung als relevanten Teil der Gesamtbedrohung verstehen. Er soll daraus Konsequenzen für die eigene Führungsstufe in Aktionsführung, Ausbildung sowie für das persönliche Handeln ableiten können.

Die HKA leitet für ihre Ausbildung deshalb daraus ab, dass Teilnehmer prüfen müssen,…

- … wie und wann sie sich in Funktion und Verantwortungsbereich durch konsequentes Umsetzen der Cyber- und Informationsvorgaben vor Angriffen und Beeinflussungen aus dem Cyber-Raum schützen;
- … wie sie selbst noch führen können, wenn IKT-Systeme, von denen sie abhängen, nicht mehr zur Verfügung stehen;
- … wie sie selbst und ihr militärischer Führungs- und Verantwortungsbereich mit Social-Media umgehen (z.B. Facebook-Auftritt des eigenen Verbandes, führen während Verbandsübungen über whatsapp);
- … in wie weit sie sich durch die Nutzung nicht-armeeeigener Geräte ausserhalb der Vorschriften bewegen und sich einem Angriff oder einer Beeinflussung aus dem Cyber-Raum aussetzen;
- … wie bei Dienstleistungen, Lageverfolgung und Aktionsvorbereitung auf jederzeit und einfach verfügbare «Ersatz»-Netze (z.B. Mobile Phone von privaten Anbietern) ausgewichen werden kann und wie Daten über wenig oder gar nicht geschützte Netze oder Kommunikationslinien ausgetauscht werden können;
- … wie der allgemein übliche Umgang mit Computern (PC, Smartphone usw.) das missbräuchliche Sammeln («Absaugen») schützenswerter Daten unterstützt;
- … wie Vorgaben bezüglich Daten- und Informationsschutz durchgesetzt werden, wie Fehlverhalten in diesem Bereich in der normalen Lage als Bedrohung erkannt und daher sanktioniert werden will und kann.

Fazit: Schwachstelle Mensch

Die heute eingesetzten militärischen IKT-Systeme und -Infrastrukturen sind zwar geschützt oder gehärtet, können aber jederzeit durch fähige Angreifer mit ge-

+ASMZ
Sicherheit Schweiz

Abo-Bestellcoupon ASMZ
Zum Monatsanfang in Ihrem Briefkasten

Bitte Zutreffendes ankreuzen

Preise inkl. MwSt.

☐ Jahresabo Fr. 78.– / Ausland Fr. 98.–

☐ Einzelausgabe Fr. 8.– / Ausland Fr. 12.–

☐ Probeabo (nur Schweiz)
3 Ausgaben Fr. 20.–

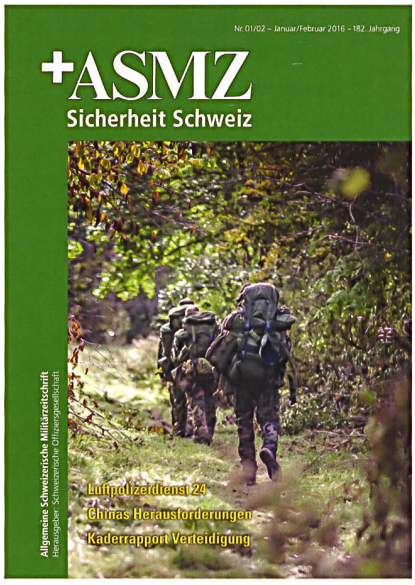
Name: _____ Vorname: _____

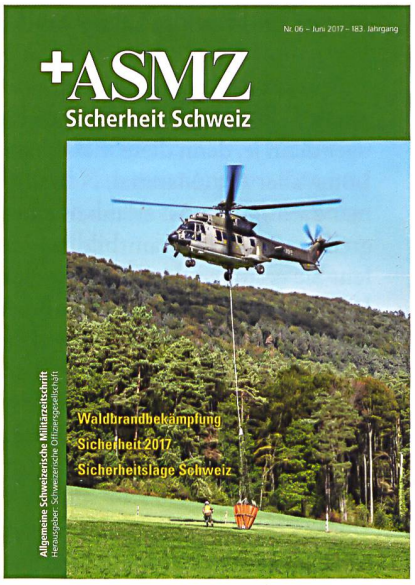
Strasse: _____ PLZ/Ort: _____

Telefon Nr: _____ E-Mail: _____

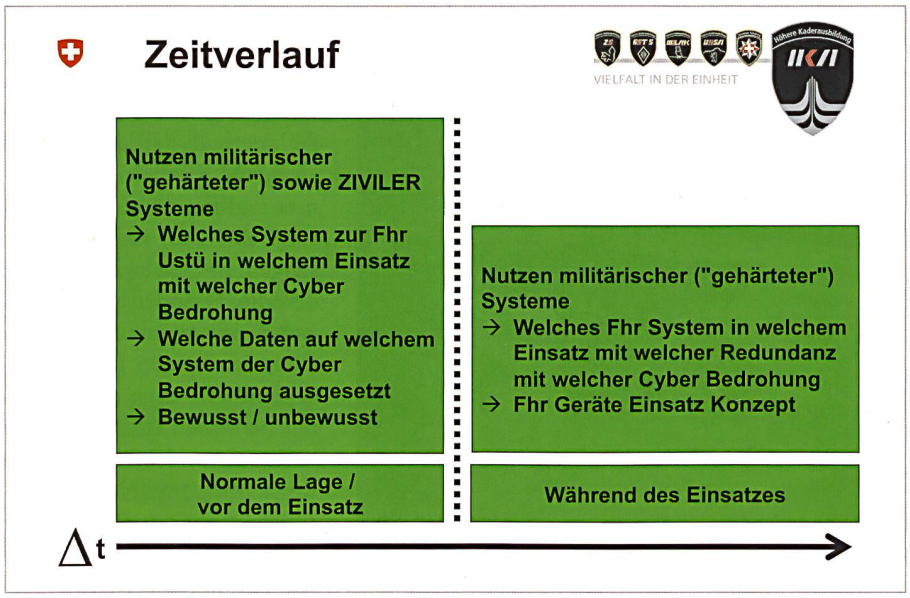
Datum: _____ Unterschrift: _____

Verlag Equi-Media AG
Brunnenstrasse 7
Postfach 732
8604 Volketswil
Telefon 044 908 45 65
Fax 044 908 45 40
abo@asmz.ch
www.asmz.ch





Allgemeine Schweizerische Militärzeitschrift
Herausgeber: Schweizerische Offiziersgesellschaft



Fragestellungen Cyber im Zeitverlauf.

eigneten Mitteln kompromittiert werden. Anzunehmen, dass im Einsatz IKT-Systeme und -Infrastruktur ohne Einschränkung funktionieren, ist zu simpel und sogar gefährlich. Plötzlich befindet man sich unvorbereitet in einer solchen Situation. Es geht darum, sich im Rahmen von Eventualplanungen mit Eingriffen gegen Daten und Informationen, die System- und Leistungsausfälle provozieren können, auseinanderzusetzen und sich darauf vorzubereiten.

Der Einzelne bleibt während aller Vorbereitung, in Ausbildung und im Einsatz eine bedeutende Schwachstelle: Cyber-Bedrohungen mutieren zur realen Gefahr, wenn Bediener sich grundsätzlich falsch verhalten (z.B. Daten ungeschützt lassen) oder die Verbindungen im Hintergrund nicht kennen, nicht realisieren, negieren. Diese erkannte Schwachstelle anzusprechen, sie anzunehmen und mögliche Auswirkungen auf die eigene Aktionsführung zu reduzieren, liegt in der Verantwortung des Einzelnen und noch verstärkt bei den Kadern für ihren Führungs- und Verantwortungsbereich.

Die HKA will – in Zusammenarbeit mit allen Verantwortlichen innerhalb des VBS, insbesondere der FUB – die Auszubildenden, Kommandanten und Stabsoffiziere, darauf vorbereiten, dass durch den Cyber-Raum alle Einsatzvorbereitungen bereits in der normalen Lage real und jederzeit vor, während und nach dem Ausbildungsdienst gestört, verändert oder aufgeklärt werden können. Daher beginnt die Verantwortung und die Arbeit jetzt und bei uns. ■

Autoren:
Divisionär Daniel Keller,
Kdt HKA / SCOS / Stv C Kdo Ausb
Oberst i Gst Stephan Kuhnen,
Chef Ausbildung und Doktrin HKA