UNSERHEER
EINE INFORMATION DES BMLV
BEILAGE ZUR 4. AUSGABE 2023

Die steigende Gefahr durch Klicks und Bytes

Militärische Konflikte werden heute nicht mehr nur mit Kampfjets, Panzern und Sturmgewehren ausgetragen, sondern zunehmend auch mit Maus und Tastatur bestritten. Das **Bundesheer** investiert deshalb aktuell im Rahmen seiner **„Mission Vorwärts“** auch ganz massiv in seine IT- und Cyberfähigkeiten.

Ohne Netz kein Heer Die IKT- und Cyber-Kräfte des Bundesheeres stellen mit ihren Qualifikationen die Ausbildung, Organisation sowie die Lagedarstellung und Führung auf dem Gefechtsfeld sicher.

Foto: Bundesheer/Haiden

IT-Attacken auf staatliche Server, Unternehmen oder Privatpersonen sind heute feste Begleiter unseres Alltags. Aber auch die Computersysteme und komplexen Waffensysteme von Streitkräften sind immer öfter potenzielle Zielscheiben für Hacker und Angreifer. Cyberangriffe können damit „nur“ einzelne Unternehmen und Sparten treffen. Sie haben aber auch das Potenzial, die gesamte Wirtschaft empfindlich zu stören und einzuschränken. In weiterer Konsequenz sogar unsere Gesellschaft und damit letztlich unseren Staat lahmzulegen – das damit verbundene Sicherheitsrisiko ist also enorm.

Für das Bundesheer bedeutet all das: Einsätze werden in Zukunft zunehmend nicht mehr nur zu Land oder in der Luft zu bestreiten sein, sondern immer öfter auch im World Wide Web. Die Landesverteidigung wird digitaler, das Thema Cybersicherheit gewinnt an Bedeutung und wird noch mehr als bisher zum militärischen Thema. IT-Expertinnen und -Experten werden daher zu einer immer wichtigeren Ressource für das Heer. Ein Kampf der verbundenen Waffen ist durch die zunehmende Komplexität und Vernetzung aller Waffensysteme ohne die Querschnittsmaterie Cyber mittlerweile praktisch undenkbar.

Das Bundesheer hat darauf längst reagiert: Fällt etwa die Stromversorgung durch einen überregionalen Blackout aus oder werden die Kommunikationsnetze durch Cyberangriffe lahmgelegt, so ist die Armee schon jetzt in Teilen weiter handlungsfähig und kann darüber hinaus auch Blaulichtorganisationen bei der Aufrechterhaltung ihres Notbetriebs unterstützen. Diese Fähigkeit soll allerdings weiter forciert werden – von der autarken Stromversorgung über die Bevorratung mit Treibstoffen und Lebensmitteln bis hin zu gesondert gesicherten und verschlüsselten Kommunikationsnetzen. Für den Fall der Fälle werden daher aktuell in ganz Österreich zwölf Kasernen so ausgebaut, dass sie im Notfall nicht nur für das Bundesheer, sondern auch für Blaulichtorganisationen als autarke „Sicherheitsinseln“ dienen können. Ziel sind Energie- und versorgungsautarke militärische Liegenschaften, um die Versorgungssicherheit im Land auch im Worst Case sicherzustellen und das staatliche Krisen- und Katastrophenmanagement zu unterstützen.

IT-Offizier: Exzellente Ausbildung mit neuem Studiengang
Für die zivilen Mitarbeiterinnen und Mitarbeiter sowie für die Soldatinnen und Soldaten des Bundesheeres eröffnet die ständige Weiterentwicklung des militärischen Cyber- und Informationsraums eine große Bandbreite an Einsatzmöglichkeiten.

Neben vielfältigen Jobangeboten und der Möglichkeit auch als Zivilperson in den Cyberspace Bundesheer einzutauchen – beispielsweise als Kryptograf, Programmierer, Netzwerktechniker oder IT-Sicherheitsanalyst – gibt es zudem auch die Option, in Uniform „außergewöhnlich“ zu studieren.

Mit der Ausbildung zum IKT-Offizier bietet die Militärakademie seit Kurzem einen neuen Ausbildungszweig, der auf die aktuellen Kommunikationsherausforderungen im digitalen Bereich abzielt. Im Rahmen des Studiums werden Expertinnen und Experten für den Einsatz von Informations- und Kommunikationssystemen des Bundesheeres ausgebildet, aber auch der Bereich der elektronischen Kampfführung ist ein großes Thema. Zu den Aufgaben dieser Spezialistinnen und Spezialisten gehört die Planung militärischer Einsatznetzwerke ebenso wie der Betrieb, die Überwachung und die Steuerung von digitalen Netzwerken des Bundesheeres. Informations- und Wissensmanagement stehen dabei im Vordergrund. Die Ausbildung dauert insgesamt vier Jahre. Nach einem Jahr Erwerb der soldatischen Grundfähigkeiten folgen drei Jahre an der Militärakademie. Abgeschlossen wird mit dem Dienstgrad Leutnant und dem akademischen Grad Bachelor of Science.

Das Bundesheer ist Cyber. Du auch?
Um auch zukünftig in der Lage zu sein, neue Sicherheitsprobleme und Angriffsszenarien zu erkennen, abzuwehren und ihnen entgegenzuwirken, entwickelt das Österreichische Bundesheer seine Kompetenzen stetig weiter. Dazu gehört auch die länderübergreifende Zusammenarbeit innerhalb Europas. Seitens der Europäischen Union wurde zum Beispiel das Projekt „OPENQKD“ zur Anwendung von Quantum Key Operations in Angriff genommen. Klingt mystisch, ist es aber nicht. Kurzum ist damit die Vergabe von geheimen Schlüsseln an Partner gemeint, um in der Kryptografie verschlüsselte Nachrichten „entsperren“ zu können.

Auch die Künstliche Intelligenz (KI) entwickelt sich rasend schnell weiter und kommt in den verschiedensten Bereichen in der militärischen Landesverteidigung vor. Das Thema „Machine Learning“, bei dem Computer gezielt trainiert werden, aus Daten und Erfahrungen zu lernen und sich stetig zu verbessern, anstatt dafür programmiert zu werden, spielt dabei schon länger eine entscheidende Rolle.

Fotos: Bundesheer/Kulec, Sebastian Freiler

Auch die rasante Weiterentwicklung der künstlichen Intelligenz, speziell im militärischen Cyberbereich, stellt Armeen vor neue Herausforderungen. Um diesen gerecht zu werden, wurde durch das Militärische Cyber Zentrum ein nationales Forschungsprogramm mit der Fachhochschule St. Pölten umgesetzt. Im Mittelpunkt dabei: Die Analyse der Ziele, Möglichkeiten und Bedürfnisse des Bundesheeres im Hinblick auf einen möglichst effizienten Einsatz von KI. Dabei wurde der Fokus auf die Weiterentwicklung der Technologie gerichtet, um abschätzen zu können, in welche Richtung sich Technologien und Anwendungen weiterentwickeln.

Um den Prozess der Cyberlagebilderstellung zu automatisierten und zu digitalisieren, wird zudem aktuell ein Cyber-Melde- & Informationsservice entwickelt. Dieses Service ermöglicht die automatische Sammlung und Analyse von Daten und bietet eine zentrale Plattform für die Zusammenarbeit und den Informationsaustausch zwischen den beteiligten Stellen. Weiters liefert es eine zeitnahe und umfassende Darstellung der aktuellen Cyber-Situation und ermöglicht Entscheidungsträgern schnell und effektiv auf Bedrohungen zu reagieren.

Karrieremöglichkeiten für Cyber- & IT-Spezialisten
Wer sich also unter anderem für moderne Waffensysteme, Threat Intelligence, Cybersecurity, Cyber Defense, holistische Lagebilder, Pentesting oder Post-Quantenkryptografie interessiert, ist beim Bundesheer genau richtig. Egal ob im T-Shirt oder im Tarnanzug, mit Cap oder Barett, als Frau oder Mann, jung oder alt, als Hacker, Mathematiker oder innovativer Querdenker: Beim Heer sind alle willkommen, die dabei helfen, unsere Armee digital zukunftsfähiger zu machen und den Cyberraum zu schützen.

Worauf noch warten? Informiere dich unter karriere.bundesheer.at über deine Möglichkeiten und werde Teil der Mission! Mach mit uns das Österreichische Bundesheer noch zukunftsfähiger!

„Konflikte werden in Zukunft immer unberechenbarer“

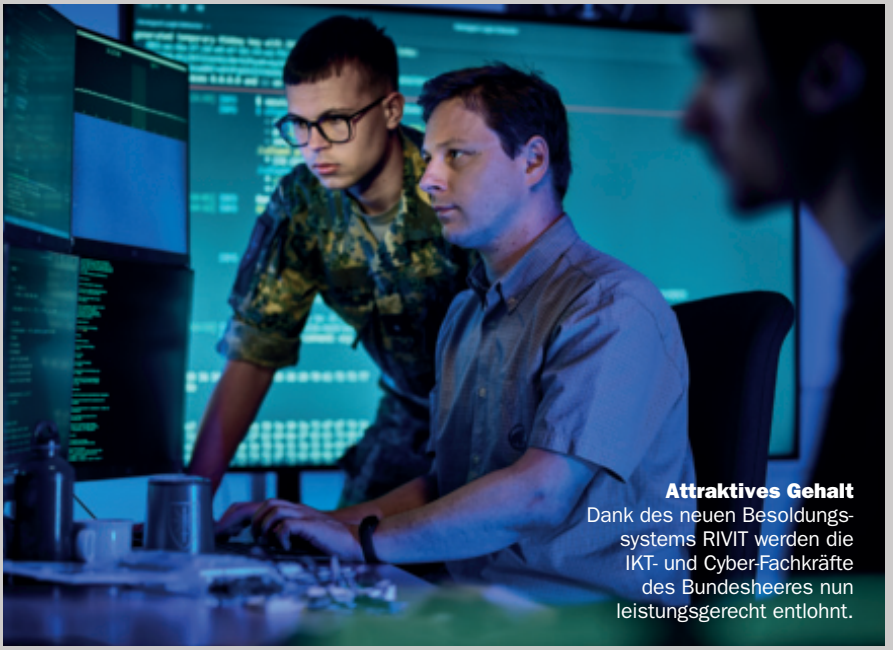
Generalmajor Hermann Kaponig ist seit dem Jahr 2019 Kommandant des IKT und Cybersicherheitszentrum des Bundsheeres. Ein Gespräch über die größer werdende Bedeutung des Cyberraums in modernen Konflikten und geplante Investitionen in die IKT-Infrastruktur und das IKT-Fachpersonal des Bundesheeres.

Herr Generalmajor, in den vergangenen Jahren hieß es, dass ein „Krieg der Zukunft“ hybrid und stark auch auf der Cyberebene geführt wird. Nun sehen wir in der Ukraine klassische Schlachten Mann gegen Mann, mit Schützengräben, viel Artillerie und Panzern. Inwiefern spielt dort aber auch der Cyberbereich eine Rolle?
Die Wirkung der klassischen Waffen ist sichtbar und wird in allen Medien gezeigt. Geplant, geführt, und gelenkt werden Konflikte jedoch im elektromagnetischen Spektrum und im Cyberraum. Jedes moderne Einsatzsystem braucht Standortgenauigkeit, Aufklärungsdaten und Koordination im Zusammenwirken. Durch gezielte Angriffe im Cyberraum, zum Beispiel auf satellitengestützte Verbindungen, können militärische Operationen nachhaltig gestört oder gar verhindert werden. Auch der Konflikt in der Ukraine wird von einem großangelegten Krieg im Cyberraum begleitet. In modernen Konflikten wird oftmals frühzeitig und

ohne Vorwarnzeit versucht, IKT-Systeme, Netzwerke verschiedenster Art, Navigationssysteme, Führungsmittel, aber auch die Energieversorgung von wichtigen Systemen und der kritischen Infrastruktur schon lange vor einem Einsatz konventioneller militärischer Mittel zu beeinträchtigen, zu verfälschen, zu stören oder gar zum Ausfall zu bringen.

Welche Ableitungen lassen sich daraus ziehen?
Konflikte der Gegenwart und der Zukunft werden aufgrund der Komplexität der eingesetzten Mittel und handelnden Gruppen immer unberechenbarer. Der Cyberraum gewinnt hier immer mehr an Bedeutung und ist mittlerweile ein eigener Bereich der Einsatzführung geworden. Die derzeitig aktuellen Konflikte haben uns gezeigt, wie rasch und mit welcher Wucht ein scheinbar friedlicher Alltag gestört werden kann. Wir müssen uns deshalb auch in Österreich im Cyberbereich auf den aktuellsten Stand bringen. Cyberangriffe können souveränitätsgefährdend sein, wenn sie auf militärische IKT-Systeme sowie auf kritische Infrastrukturen und/oder verfassungsmäßige Einrichtungen Österreichs wie Behörden sowie Strom-, Gas- und Wasseranbieter, wirken. Mit neuen Technologien, Techniken, Internet, Digitalisierung, Machine Learning und künstlicher Intelligenz sind dafür völlig neue Möglichkeiten entstanden. Wir müssen uns auf die Cyberverteidigung in Netzwerken vorbereiten. Dies umfasst alle militärischen Maßnahmen im Cyberraum zur Abwehr und Beendigung von Cyberangriffen. Diese Aufgaben werden beim Bundesheer von den Cyberkräften wahrgenommen, die gemeinsam mit den Land- und Luftstreitkräften die Souveränität Österreichs sicherstellen.

Das heißt, das Bundesheer muss seine Anstrengungen auch in diesem Bereich intensivieren?



Attraktives Gehalt
Dank des neuen Besoldungssystems RIVIT werden die IKT- und Cyber-Fachkräfte des Bundesheeres nun leistungsgerecht entlohnt.

Die schnell voranschreitende Digitalisierung stellt Streitkräfte weltweit vor neue Herausforderungen. Die Anstrengungen des Bundesheeres müssen zukünftig alle Maßnahmen für die Sicherheit der Informations- und Kommunikationstechnologie umfassen. Das bedeutet den permanenten Schutz der militärischen IKT-Systeme und Informationen, 24 Stunden am Tag, 365 Tage im Jahr. Dies gilt für das gesamte Bundesheer im In- und Ausland. Ziel muss es sein, das volle Spektrum des Kampfes in der Cyberdomäne zu beherrschen, das heißt vollständige Informationshoheit und Kontrolle über die eigenen Systeme sicherzustellen. Der Kampf der verbundenen Waffen ist wegen der zunehmenden Komplexität und Vernetzung moderner Waffensysteme ohne die Querschnittsmaterie Cyber undenkbar.

Was braucht es dafür vor allem? Investitionen in Hardware oder in gut ausgebildetes Personal?
Modernste Hard- und Software kann nur durch hervorragend ausgebildetes Personal im vollen Spektrum zur Wirkung gebracht werden. Daher liegt unser Fokus auf Personalgewinnung und Ausbildung. Die derzeitige Budgetlage ermöglicht es uns jedoch, nicht nur den Investitionsstau der letzten Jahrzehnte auszugleichen und die IKT-Infrastruktur auf den neuesten Stand zu bringen, sondern auch zukunftssichernde Maßnahmen zu finanzieren.

Beim Personal steht das Bundesheer im harten Konkurrenzkampf mit der Privatwirtschaft. Was kann das Heer Mitarbeiterinnen und Mitarbeitern bieten, was sie anderswo nicht bekommen?
Mit dem neuen Besoldungssystem RIVIT wurde eine an das Lohnniveau in der Privatwirtschaft angeglichene und durchaus attraktive Möglichkeit zur leistungsgerechten Entlohnung geschaffen. Da wir das gesamte Spektrum der IKT abbilden, können wir innovative und attraktive Tätigkeitsbereiche bieten. Diese sind dank eines abwechslungsreichen Technologie-Stacks sehr vielfältig und aufgrund der militärischen Anforderungen im Hard- und Softwarebereich einzigartig. Besonders die Arbeit mit modernen Waffen- und Einsatzsystemen ist ein Alleinstellungsmerkmal. Darüber hinaus bieten wir unseren Mitarbeiterinnen und Mitarbeitern hochwertige Aus-, Fort,- und Weiterbildungen, die in diesem Ausmaß und Qualität anderswo kaum zur Verfügung stehen.

Impressum: Amtliche Publikation der Republik Österreich / Bundesministerium für Landesverteidigung. Medieninhaber, Herausgeber und Hersteller: Republik Österreich / Bundesministerium für Landesverteidigung, Roßauer Lände 1, 1090 Wien. Erscheinungsjahr: 2023. Druck: Heeresdruckzentrum 18-101010100.

Foto: Bundesheer/Haiden