LEISTUNGSBERICHT

DIREKTION 6 – IKT&CYBER

2023

EINSATZBEREIT FÜR ÖSTERREICH

BUNDESHEER.AT

UNSER HEER

Bundesministerium für Landesverteidigung

Die Bezeichnungen in diesem Leistungsbericht betreffen Männer, Frauen wie auch nichtbinäre und diversgeschlechtliche Personen gleichermaßen.

Der Begriff "Mitarbeiter" oder "Bediensteter" beinhaltet - so nicht explizit anders angeführt - Soldaten, Zivilbedienstete (Beamte und Vertragsbedienstete) und externes Unterstützungspersonal nach dem Arbeitskräfteüberlassungsgesetz (Leiharbeiter, nachfolgend kurz AÜG).

Das Stichwortverzeichnis dient der besseren Lesbarkeit militärischer und technischer Begriffe, ersetzt exakte Definitionen aus Lexika oder Vorschriften jedoch nicht. Es soll als allgemeines Nachschlagewerk verwendet werden können.

Bundesministerium für Landesverteidigung

Sehr geehrte Leserinnen und Leser!

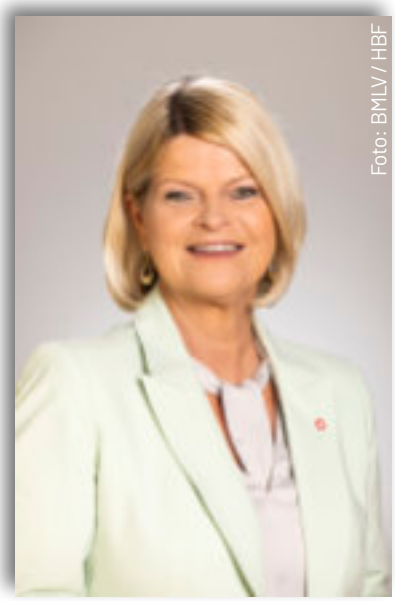


Foto: BMLV / HBF

Mag.ª Klaudia Tanner

Als Bundesministerin für Landesverteidigung ist es mir eine Freude die Digitalisierung des Österreichischen Bundesheers durch die Cyberkräfte im Leistungsbericht für das Jahr 2023 präsentieren zu können.

Mit dem Aufbauplan ÖBH 2032+ entwickeln wir unser Bundesheer mit dem klaren Fokus auf die Kernaufgaben der militärischen Landesverteidigung. In diesem Zusammenhang legen wir ein besonderes Schwergewicht auf die Wahrnehmung von Inlandsaufgaben, um auf jegliche Herausforderungen, die auf unser Land zukommen könnten, vorbereitet zu sein.

Es ist uns gelungen, die budgetären Voraussetzungen für die anstehenden und herausfordernden Aufgaben unseres Bundesheeres im Rahmen des Landesverteidigungsfinanzierungsgesetzes abzusichern. Dies ermöglicht es uns, notwendige Investitionen zu tätigen und die Streitkräfte auf ein höheres Niveau zu bringen.

Uns ist bewusst, dass wir vor personellen Herausforderungen stehen. Es geht dabei nicht nur um die Rekrutierung von neuem Personal, sondern auch um Begleitmaßnahmen für unser bestehendes Personal, um deren Fähigkeiten kontinuierlich zu erweitern und zu verbessern. Die Entwicklung unserer Streitkräfte ist ein ganzheitlicher Prozess, der sowohl die Gewinnung neuer Talente als auch die Förderung und Unterstützung unserer bestehenden Kräfte umfasst.

Die Cyber und Informationskräfte sind mit den sich ständig ändernden und rasch wachsenden Herausforderungen von Desinformation und Fake News, Digitalisierung und künstlicher Intelligenz auf dem modernen Gefechtsfeld konfrontiert.

Der Zulauf von neuem IKT-Gerät ist ein wesentlicher Aspekt, um im Informationsraum wirksam zu agieren und die Sicherheit unserer Nation zu schützen.

Das Bundesheer steht vor der Aufgabe, diese neuen Herausforderungen anzunehmen und Lösungen zu entwickeln, die sowohl die technologische Überlegenheit sichern, als auch die Resilienz unserer Gesellschaft als Ganzes stärken.

Durch die konsequente Weiterentwicklung unserer Cyber- und Informationskräfte gewährleisten wir auch in Zukunft die Sicherheit Österreichs im digitalen Umfeld.

Ich danke allen Soldatinnen, Soldaten, allen Zivilbediensteten des Österreichischen Bundesheers und im besonderen den Cyberkräften, für ihren unermüdlichen Einsatz zum Schutz unserer Heimat.

Es lebe das Österreichische Bundesheer!

Es lebe die Republik Österreich!

Bundesministerium für Landesverteidigung

Sehr geehrte Damen und Herren!

General Mag. Rudolf Striedinger

Als der Chef des Generalstabs des Österreichischen Bundesheers ergreife ich hiermit die Gelegenheit, im Zuge eines Vorworts zum diesjährigen Leistungsberichtes der Direktion 6 - IKT&Cyber ein paar Worte an Sie zu richten.

Dieser Bericht spiegelt nicht nur die bemerkenswerten Leistungen unserer Cyber- und Informationskräfte wider, sondern markiert auch den entscheidenden Weg in die Zukunft, den wir als eigene Domäne der Einsatzführung im Rahmen der Landesverteidigung eingeschlagen haben.

Mit dem Aufbau eines neuen Führungssystems und der Einführung eines fortschrittlichen „IKT-System-Einsatz" bis 2032 setzen wir einen technischen Meilenstein für das Österreichische Bundesheer. Diese Entwicklung ist fundamental für die Erreichung eines domänenübergreifenden Lagebildes in Echtzeit, das unsere Reaktionsfähigkeit und operative Effizienz erheblich verbessern wird.

Resilienz, Redundanz, Autarkie unserer Systeme und die Weiterentwicklung unserer Verteidigungsfähigkeiten im Cyber- und Informationsraum rücken immer mehr in den Fokus, um sich den stetig wandelnden digitalen Bedrohungen effektiv entgegenstellen zu können. In dieser Hinsicht erkennen wir auch neue Herausforderungen, wie die Domäne „Weltraum" mit den modernen Technologien für Kommunikation und Aufklärung, als kritische Bereiche, die in unsere Strategie und Vorbereitung einfließen müssen.

Die Etablierung von Informationskräften gemäß dem Aufbauplan ÖBH2032+ und die Entwicklung neuer Fähigkeiten für ein verteidigungsfähiges Bundesheer stellen einen weiteren Schwerpunkt unserer Bemühungen dar. Diese Strategie wird durch die Durchführung von Planspielen ergänzt, welche die Rolle der Cyber- und Informationskräfte in verschiedenen Szenarien simulieren und analysieren, um unsere Taktiken und Strategien kontinuierlich zu verfeinern.

Dieser Leistungsbericht verdeutlicht das Engagement und den fortgesetzten Einsatz der Cyber- und Informationskräfte für die Sicherheit Österreichs in der digitalen Ära.

Ich möchte der Direktion 6 - IKT&Cyber und den Cyber- und Informationskräften unseres Bundesheeres meinen aufrichtigen Dank und Anerkennung für deren Leistungsfähigkeit und Expertise aussprechen. Damit tragen Sie entscheidend dazu bei, den Schutz und die Sicherheit unseres Landes in einer immer komplexer werdenden digitalen Welt zu gewährleisten. Ich bin zuversichtlich, dass wir gemeinsam den Herausforderungen der Zukunft erfolgreich begegnen werden.

Es lebe das Österreichische Bundesheer!

Bundesministerium für Landesverteidigung

Inhaltsverzeichnis

Bundesministerium für Landesverteidigung

Kommandant der Cyberkräfte
GenMjr Mag. Ing. Hermann Kaponig

Sehr geehrte Damen und Herren,
werte Leserinnen und Leser unseres Leistungsberichts 2023.

Mit großer Freude darf ich Ihnen als „Chief Digital Officer (CDO)", als „Chief Information Officer (CIO)" des BMLV, als Überleitungs-verantwortlicher der Direktion 6 – IKT&Cyber in der Generaldirektion Landesverteidigung (GDLV), als Kommandant der Cyberkräfte des Österreichischen Bundesheeres (ÖBH) und als Leiter des IKT- und Cybersicherheitszentrums (IKTCySihZ), unseren neuesten Leistungsbericht für das Jahr 2023 vorstellen. Voller Stolz darf ich auf die Leistungen unseres Verantwortungsbereichs und auf wichtige Weiterentwicklungen für unser Verteidigungsressort hinweisen.

Wir haben uns 2020 erstmals dazu entschlossen, jährlich einen Leistungsbericht über unser breitbandiges Tätigkeitsportfolio zu erstellen. Vor Ihnen liegt unser insgesamt vierter Leistungsbericht, nun für das Jahr 2023. Um den Umfang nicht überzustrapazieren, wollen wir uns allerdings dabei wieder auf unsere wesentlichen Vorhaben beschränken.

Der Leistungsbericht soll einerseits außerhalb unserer Organisation, wie auch innerhalb unserer Organisation all unseren Mitarbeitern im gesamten Bundesgebiet, die Breite unserer Anstrengungen und unseres Zuständigkeitsbereichs vor Augen führen. Andererseits soll er aber auch interessierten Lesern die Gelegenheit geben, in der Retrospektive zu erfassen, was alles geschafft werden konnte.

Dieses Leistungsportfolio wurde nachhaltig durch die Zusammenführung nahezu aller im Fachbereich nötigen Fachdienststellen ermöglicht. Es ist eine Teamleistung, der noch immer nur virtuell eingenommenen Organisation, der Direktion 6 – IKT&Cyber.

Foto: BMLV / HBF

Mit Erstellung dieses Leistungsberichts Anfang 2024 war die Reorganisation auch unseres Fähigkeitsbereichs im dritten Jahr seiner Bearbeitung nicht abgeschlossen. Nach dem aktuellen Stand der Planungen ist vorgesehen, die Direktion 6 – IKT&Cyber noch bis Mitte 2024 im BMKÖS zu behandeln und neue Organisationspläne mit deren Arbeitsplätzen zu verhandeln. Danach wäre die Überleitung in die neue Struktur vorgesehen.

Die Zielsetzungen der Reorganisation hätten sich für unseren Bereich grundsätzlich bestätigt. Wir sind durch die Zuordnung der Verantwortlichkeiten auf strategischer, operativer, taktischer und der technischen Ebene in die Lage versetzt worden, Vorhaben und Projekte sozusagen aus einer Hand zu planen, zu realisieren und operationell zu setzen.

Dazu kann nicht oft genug darauf hingewiesen werden, dass das auch nur deswegen möglich wurde, weil wir mit dem IKTCySihZ als eigenen IKT-Provider des BMLV, besonders auf die Notwendigkeiten und Eigenheiten unserer Organisation eingehen konnten. Nur mit unseren hervorragend ausgebildeten und erfahrenen Experten sind wir in der Lage, komplexe Vorhaben und umfangreiche Projekte uf höchstem technischen Niveau zur Umsetzung zu bringen.

„Den IKT-Provider im eigenen Haus zu haben, ist ein nicht hoch genug zu schätzender Vorteil."

„Das Schwergewicht der Digitalisierung liegt bei den Einsatzaufgaben."

Dies gilt gerade auch in Zeiten, wo sich in der IKT- und Cyber- Branche wesentliche Veränderungen ergeben und Begriffe wie Sicherheit, Vertrauen, „Secure Supply Chain Manangement" oder „Digital Sovereignty" immer mehr an Bedeutung gewinnen.

Gleichermaßen ermöglicht uns die hohe Qualität unserer Mitarbeiter auch, dass wir externen Dienstleistern oder Produktlieferanten sehr konkrete und machbare Vorgaben geben können. Zudem ist damit auch die Wahrnehmung der wichtigen Güteprüfung und Abnahme im Fachbereich gewährleistet.

Wir haben, was die Bereitstellung von Services betrifft, natürlich gleichermaßen versucht, keine Österreich-spezifischen Services (Ö-Versionen) zu realisieren, sondern immer den Notwendigkeiten der Interoperabilität Rechnung zu tragen. Das hat uns zum Einen sehr gefordert und zum Anderen natürlich stark in die Verantwortung genommen.

Die Mitarbeiter wurden dabei auch 2023 hart an die Leistungsgrenzen geführt. Mein besonderer Dank gilt hier all jenen, die trotz aller organisatorischen Unsicherheiten wieder ihr Bestes gegeben haben.

Somit blicken wir auf ein abwechslungsreiches und durchaus herausforderndes Jahr 2023 zurück. Die Ergebnisse lassen sich ohne Frage herzeigen. Wir können stolz auf die Leistungen unseres Teams sein. Ich kann das mit gutem Grund so behaupten, denn wir brauchen auch den Vergleich mit vielen anderen europäischen Nationen nicht zu scheuen. Trotzdem bleibt viel zu tun. Mit der durchgängigen Digitalisierung der Streitkräfte sind alle gefordert.

Dazu sei aus Sicht der Direktion 6 - IKT&Cyber interessierten Lesern vorweg klar vor Augen geführt; Digitalisierung ist allerorts das Topthema – auch bei uns im Verteidigungsressort.

Für unser Bundesheer heißt das, dass Digitalisierung mit Schwergewicht für die Einsatzaufgaben zur Umsetzung zu bringen ist. Für ein Bundesheer, das wieder seiner Kernaufgabe als einzige bewaffnete Streitmacht im Sinne der Militärischen Landesverteidigung nachkommen können muss.

Schließlich gestalten wir die Rahmenbedingungen für unser neues Bundesheer 2032+ im Rahmen des Aufbauplanes ÖBH2032+. Das bindet massive Kräfte der Direktion IKT&Cyber, weil wir hier jetzt schon die richtigen Weichen und Erstmaßnahmen für unser neues Bundesheer 2032+ stellen müssen.

Wir wollen unseren substanziellen Beitrag zu einer digitalisierten Einsatzarmee leisten, das hinkünftig nicht nur Gefechtshandlungen führen können muss. Vielmehr muss unser Bundesheer in der Lage sein, in einem modernen hybriden Szenario zu bestehen und dabei im Kampf der verbundenen Waffen auch Gefechtshandlungen letztlich gewinnen können. Der Faktor Geschwindigkeit wird dazu immer bestimmender. Die Zeit vom Aufklärungsergebnis über das Lagebeurteilungsverfahren bis hin zum Wirkmittel- Einsatz ist dazu weiter zu optimieren („sensor to shooter acceleration").

Es bedarf hierfür eines leistungsfähigen digitalisierten und redundanten Aufklärungs-, Führungs- und Wirkungsverbundes, der über alle Domänen (Landstreitkräfte, Spezialeinsatzkräfte, Luftstreitkräfte, Cyberkräfte, Weltraum-Services und Informationskräfte) reicht.

Nahezu jedes System, egal ob Sensor oder Wirkmittel, wird dazu im Einsatz vernetzt. Der Cybersicherheit wird hierzu besonderes Augenmerk geschenkt. Voll digitalisierte Lagebilder aller Fähigkeitsbereiche sind in Echtzeit bereitzuhalten. Ein neues eigenes Einsatznetzwerk („IKT-System Einsatz"), ein „Battle Management-System (BMS)" und ein neues Führungsinformationssystem sind beispielsweise dazu zu etablieren.

„Die Weichenstellungen zu einem modernen digitalisierten Bundesheer erfolgen jetzt."

In modernen Bedrohungsszenarien wird letztlich nur der erfolgreich sein, wer

- auf Basis gediegener nachrichtendienstlicher Informationen, Aufklärungsergebnissen und Sensordaten, über ein domänenübergreifendes valides Lagebild in Echtzeit verfügt,
- die eigene Führungsfähigkeit maximal aufrechterhalten und/oder die gegnerische Führungsfähigkeit maximal beeinträchtigen kann,
- auf Basis eines (digitalisierten, KI- gestützten und redundanten) Beurteilungsverfahrens schnell zu einem Befehl gelangt und diesen rasch gesichert weiterleiten kann,
- Waffengattungs- und domänenübergreifend auf Basis von „Multi Domain Operations" oder dem „Kampf der verbundenen Waffen" die jeweils effektivsten Wirkmittel zum richtigen Zeitpunkt, am richtigen Ziel und in der richtigen Mengendimension einsetzen kann

Im Tagesbetrieb und Alltag ist jedoch die Erwartung vieler, prioritär in der Organisation im Verwaltungsbereich zu digitalisieren, zu modernisieren und das Arbeiten im Tagesbetrieb auf den letzten Stand der Technik zu bringen. Vieles, was in den letzten Jahren auf Grund der Budgetengpässe nicht möglich war, soll nun sofort umgesetzt werden. Wir setzen hier klare Prioritäten für den Einsatz und setzen parallel die notwendigen Digitalisierungsmaßnahmen für den Verwaltungsbereich im Rahmen der verfügbaren Ressourcen.

Zur Digitalisierung im Gesamten, muss aber auch klar gesagt werden, dass Digitalisierung nicht nur eine Aufgabe der Direktion 6 - IKT&Cyber oder des CDO des BMLV ist, sondern alle Prozesseigner im Ressort mitgefordert sind .

Und unter Prozesseigner verstehen wir die jeweiligen Verantwortlichen und Zuständigen für die diversen Kern- und Unterstützungsprozesse und nicht nur die Anwenderfachabteilungen für definierte IKT-Services.

Es kann auch nicht oft genug gesagt werden, dass Digitalisierung letztlich einen Mehrwert für die Organisation und deren Prozesse in allen Bereichen und Waffengattungen mit sich bringen muss. Dabei geht es nicht nur um die einfache Umwandlung analoger oder teildigitaler Prozesse (Basic - Basisdigitalisierung) ohne Medienbruch in die digitale Welt.

Basisdigitalisierungsmaßnahmen sind sozusagen die Pflicht, die wir ohnehin zu erledigen haben. Die Kür sind erweiternde und optimierende Digitalisierungsmaßnahmen.Wirklich die Chancen der Digitalisierung zu nutzen, bedeutet gleichzeitig auch bestehende Prozesse zu hinterfragen und gegebenenfalls anzupassen oder gänzlich neu aufzusetzen.

Signifikanten Mehrwert bringen schließlich nur Digitalisierungsmaßnahmen, die vorweg auch Prozessanpassungen (Enhanced-Erweiterte Digitalisierung) beinhalten. Das bedeutet jedoch auch notwendige Anpassungen von Weisungen, Richtlinien und Vorschriften in den Fachbereichen als Voraussetzung.

Dieser Vorgang ist zumeist innerhalb der Organisation mit gutem Willen für Einsatzaufgaben wie auch der Verwaltung umsetzbar, weil das in der Regel Anpassungen innerhalb des Ressorts betrifft.

Den höchsten Mehrwert erzielen jedoch Digitalisierungsmaßnahmen, die gleichzeitig Prozesse gänzlich neu aufsetzen (Optimized - Optimierte Digitalisierung). Das ist aktuell jene Chance, die zu nutzen wäre.

„Digitalisierung ist eine Chance und eine Herausforderung für das gesamte System."

Wir müssen unsere Prozesse im Einsatz neu denken, aber auch, wo zweckmäßig, Verwaltungsprozesse neu aufsetzen. Dieser Vorgang erfordert jedoch in der höchsten Ausprägung die Schaffung neuer Grundlagen und oftmals auch gesetzliche Anpassungen. Optimierte Digitalisierung ist daher in der Umsetzung am Schwierigsten und in zeitlicher Hinsicht am Aufwändigsten.

Digitalisierung bringt also einerseits einen Mehrwert mit sich, erfordert aber auch im hohen Maße, dem Sicherheitsaspekt vermehrten Augenmerk zu schenken. Das bringt zusätzliche Aufgabenstellungen für den Bereich der IKT-Sicherheit und der Cybersicherheit im System mit sich.

Darüber hinaus muss auch klar festgehalten werden, dass ohne Digitalisierung in weiterer Folge keine Nutzung von Künstlicher Intelligenz möglich sein wird! Die Nutzung der Möglichkeiten Künstlicher Intelligenz wird auch im BMLV von wesentlicher Bedeutung werden. Dies gilt in gleicher Weise für unsere Einsatzaufgaben, wie auch für die Verwaltungsaufgaben. Die größte Herausforderung des Jahres 2023 für die Direktion 6 – IKT&Cyber war es, im Bereich der Fähigkeitsentwicklung zum ÖBH2032+ mitzuwirken. Dies deshalb, weil es nicht nur um die Fähigkeitsplanung der Cyber- und Informationskräfte, sondern um den gesamten Bereich des Bundesheeres in den Funktionsbereichen IKT, Cyber, EloKa, Weltraum und Informationsoperationen ging.

Planungsarbeiten, Abstimmungsbesprechungen und Planspiele haben wesentliche Arbeitskapazitäten gebunden. Ohne die temporäre Bildung eines „Cyber-, Informations-, Fähigkeits— Boards (CIFB)" wären die Bearbeitungen so nicht möglich gewesen. Eine Vielzahl von ausgewiesenen Experten haben hier hervorragende Arbeit geleistet. Mein besonderer Dank gilt hier vor allem Herrn Oberst des Generalstabsdienstes Mag. Christoph Tatschl, Herrn Oberstleutnant des Generalstabsdienstes Mag. Christoph Jezek und Herrn Bereichsleiter&CTO Mag. Wolfgang Hacker.

Auf den wichtigen Bereich Zusammenarbeit und Kooperation will ich ganz besonders eingehen. Natürlich sind wir innerstaatlich auf Bundesebene sehr bemüht in allen relevanten Gremien und Arbeitsgruppen mitzuarbeiten. Hier waren und sind wir als Direktion 6 – IKT&Cyber beispielsweise in der CDO-Task Force, den IKT-Bund Sitzungen und BLSG-Sitzungen (Bund-Länder-Städte-Gemeinden) vertreten und nehmen aktiv an gesamtstaatlichen Übungen und Veranstaltungen teil. Auch unsere Zusammenarbeit mit anderen Ministerien, wie auch mit Bildungseinrichtungen und akademischen Stellen seien positiv hervorgehoben. Herausragend erwähnt, soll hier ganz besonders die fruchtbare Zusammenarbeit mit unserer offiziellen Partnerschaft, der HTL Spengergasse in Wien, wie auch mit der HTL Hollabrunn, werden.

Zusammenarbeit und Kooperation im internationalen Kontext bedeutet für uns, auch an den Entwicklungen auf Ebene der Europäischen Union wie auch der NATO, aktiv teilzunehmen.

Hier ist Interoperabilität aller Systeme das Topthema. Nationale Insellösungen sollten der Vergangenheit angehören. Wir arbeiten hier auch bei der Erstellung von Grundsatzpapieren mit, testen und erproben Systeme und Services und üben gemeinsam im internationalen Umfeld. Dies erfolgt institutionell oder aber auch mit unseren Kernpartnern im bi- oder multinationaler Zusammenarbeit. Ganz besonders möchte ich dazu auf unser Erfolgsformat der DACH-Kooperation (Deutschland - Österreich – Schweiz) hinweisen, wo die Zusammenarbeit auf vielen Ebenen als vorbildlich zu bezeichnen ist.
Auf einige internationale Übungsformate hierzu will ich auf der nächsten Seite näher eingehen:

Digitalisierung in drei Qualitätsstufen:
- *Basic*
- *Enhanced*
- *Optimized*

Ein Highlight des Jahres 2023 war unsere Teilnahme an der weltweit größten Cyberverteidigungsübung „Locked Shields 2023". Diese NATO-Übung, welche aus Tallinn in Estland gesteuert wird, findet jährlich statt. Sie wird jedes Jahr wechselweise in multinationalen Teams und rein nationalen Teams durchgeführt. Wir haben diesmal aus Österreich mit einem rein nationalen österreichischen Team mit über 100 Personen aus Cyberexperten des IKTCySihZ (Kader und Cyber-Grundwehrdiener), verstärkt durch Miliz und verschiedensten Experten aus dem Bund und den Kritischen Infrastrukturen, erfolgreich daran teilgenommen.

Die Erkenntnisse aus dieser Übung im Vergleich mit anderen Nationen, haben uns wieder einen weiteren wesentlichen Schritt in der Entwicklung der Cyberkräfte gehen lassen.

Auch unsere Teilnahme an der alljährlich stattfindenden NATO- Übung „CWIX23" (Coalition Warrior Interoperability Exercise) in Bydgoszcz in Polen hat uns wieder einen wesentlichen Beitrag für unsere Streitkräftefähigkeitsentwicklung gebracht. Die CWIX ist das Testevent für multinationale Interoperabilität schlechthin. Nachdem wir uns ebenso der Interoperabilität verschrieben haben, ist eine Teilnahme an dieser Übungsserie auch für Österreich unumgänglich, denn hier wird die Weiterentwicklung der einzelnen nationalen Fähigkeiten hinsichtlich der Umsetzung des sogenannten „NATO Federated Mission Networks" (FMN) anhand von Standards überprüft. Dieser Vorgang ist essentiell für die Entwicklung von Fähigkeiten für „Connected Forces" und damit wesentlich für unsere Weiterentwicklung zum neuen „IKT-System Einsatz" des ÖBH.

Auch 2023 waren wir wieder bei der trinationalen Übung „Common Roof" dabei. Bei der Übung „Common Roof 2023" hatte diesmal Österreich zusätzlich die Funktion der Lead-Nation inne. Die Übungsleitung wurde durch unser Führungsunterstützungsbataillon 1 (FüUB1) hervorragend gestellt.

Auch hier wurden definierte IKT-Einsatz- Services auf deren Interoperabilität geübt. Die gewonnenen Erkenntnisse werden in weiterer Folge beim IKT-System Einsatz im ÖBH umgesetzt. Der Fokus bei dieser Übung lag in der Bereitstellung eines trilateralen Führungsnetzes für beispielsweise Einsätze der grenzüberschreitenden Katastrophenhilfe. Dabei wurden die jeweiligen nationalen Einsatznetzwerke in ein gemeinsames „multinationales Mission Network" zusammengeführt und festgelegte betriebliche Abläufe und Prozesse anhand einem Szenario und einem Ablaufplan geübt und evaluiert.

Das erforderte die Konfiguration der technischen Netz- und IKT- Sicherheitsinfrastruktur sowie die Entwicklung und Beschreibung übergreifender IT-Service Management und IT- Sicherheitsprozesse.

Die im multinationalen Netzwerk verwendeten Services und Betriebsabläufe orientierten sich an den FMN- Spezifikationen. Das letzte Jahr war aber auch neben dem wichtigen Einsatz- und Übungsbetrieb, den Planungsarbeiten, und dem „daily business", höchst abwechslungsreich.

Im Laufe des Jahres 2023 durften wir honorige Personen und Delegationen in unserem Verantwortungsbereich zur Dienstaufsicht oder einem bilateralen Austausch begrüßen.

Dazu zählen unter anderem natürlich unsere Frau Bundesministerin Mag[a]. Klaudia Tanner, unser Herr Generalstabschef General Mag. Rudolf Striedinger, der US- Brigadier General Henry U. Harder, Jr mit einer Delegation der US National Guard aus Vermont, der Herr Staatssekretär für Digitalisierung Florian Tursky, MSc. MBA und unser österreichischer Nobelpreisträger Herr Univ.-Prof. Dr. phil. Dr. h. c. Anton Zeilinger.

Die Herrschaften waren allseits begeistert von unserem breiten Leistungsspektrum von Forschungsthemen über unsere Einsatzaufgaben, bis hin zur Betriebsüberwachung.

„Digitalisierung gilt als Voraussetzung für den Einsatz Künstlicher Intelligenz."

Das Jahr 2023 war aber auch von einigen internationalen Verpflichtungen geprägt. So z.B. war neben einem Besuch des „Kommando Cyber- und Informationsraum (KdoCIR) in Bonn/Deutschland auch die jeweiligen „Cyber Commanders Foren (CCF) in Tallinn/Estland und in Krakau/Polen, wie auch die EU CIS & Cyber Commanders Strategic Conference (CyberCo) in Brüssel/Belgien und Madrid/Spanien zu besuchen. Alles Veranstaltungen, die wesentlich dazu beitragen, dass man internationale Entwicklungen erkennt, wo es möglich erscheint erfolgreiche „Role models" übernimmt, oder Fehler, die andere machen mussten, selbst nicht mehr machen muss.

Bereits 2022 beginnend, wurde im Jahr 2023 eine umfassende Prüfung unseres Fachbereichs durch den Rechnungshof durchgeführt. Der Bericht des Rechnungshofes über die "Koordination der Cyber–Defence"; (Reihe Bund 2023/30) erging im Oktober 2023. Ich darf mich bei dieser Gelegenheit bei den Damen und Herren des Rechnungshofs für deren höchst kompetente und sachlich durchgeführte Prüfungsarbeit auf Basis von Fakten bedanken. Für die umfangreichen Koordinationsarbeiten innerhalb des Ressorts sei ganz besonders Herrn Oberst Erwin Pustelnik gedankt.

Wir nehmen die Empfehlungen des Rechnungshofberichtes sehr ernst und haben dazu bereits Maßnahmen gesetzt. Zudem wird dieser Rechnungshofbericht neuerlich zum Anlass genommen, entsprechende Anträge an die zuständigen Stellen zu richten, um unser Fähigkeitsspektrum im Bereich „Cyber Defence" weiter entwickeln zu können.

Die Funktion des Kommandanten der Cyberkräfte erforderte auch im Jahr 2023, eine Vielzahl von Dienstaufsichten bei unseren Dienststellen im gesamten Bundesgebiet, Teilnahme an verschiedensten Übungen und Veranstaltungen. Damit konnten wieder Eindrücke „von vorne" gewonnen werden, das eigene Lagebild im Fachbereich verdichtet und das eine oder andere Problem rasch gelöst werden.

Vor allem bei Übungen konnte ich mich vom hohen Ausbildungsstand unserer Fachkräfte überzeugen. Mit solchen Experten und Expertinnen ist mir nicht Bange den Technologiesprung in unserem Bundesheer zu gehen.

Besonders erwähnenswert waren im Jahr 2023 auch die Aktivitäten unser IKT&Cyber-Einsatz-Abteilung hinsichtlich der so genannten Notfallkommunikation. Es geht hier darum, dass trotz Resilienz und Redundanz ein Ausfall von IKT- Systemen auch in Zukunft nicht zur Gänze ausgeschlossen werden kann. Das Bundesheer muss als Einsatzorganisation befähigt sein, eine österreichweite Notkommunikation innerhalb kurzer Zeit zur errichten und zu betreiben, um die Führungsfähigkeit und die Handlungsfähigkeit auch in Krisen- und Katastrophenfällen aufrecht zu erhalten. Dazu wurde ein Notkommunikationsnetz festgelegt, um dem ÖBH nach einem längerfristigen großflächigen Stromausfall ein autarkes, erprobtes und datenfunkfähiges Führungsnetz zur Verfügung zu stellen. Das wurde auch in Österreich festgelegt und mittlerweile auch bereits zweimal in Übungen erprobt. Für die Initiative und Umsetzung sei dazu besonders dem Abteilungsleiter Herrn Brigadier Mag. Arnold Staudacher mit seinem Mitarbeiter Herrn Amtsdirektor Regierungsrat Peter Loher herzlich gedankt.

Personell hat sich bei uns einiges getan, weil wir auf Grund der neuen RIVIT- Arbeitsplätze (Richtverwendungen für IT- Fachpersonal) im Organisationsplan des IKTCySihZ endlich in der Lage waren, systemisch vergleichbare Rahmenbedingungen für unsere Mitarbeiter anzubieten.

Damit können wir nun interessierten neuen Mitarbeiter ein interessantes Aufgabenspektrum mit einem durchaus attraktiven Arbeitsumfeld anbieten. Auch konnte mit den neuen RIVIT-Arbeitsplätzen eine Vielzahl von AÜG- Mitarbeiter (Arbeitskräfte Überlassungsgesetz), die auf Basis dieser Leihverträge kurz-bis langfristig bei uns gearbeitet haben, auf RIVIT-Arbeitsplätze übernommen werden.

„Interoperabilität ist das Kernthema."

Wir konnten auch den Frauenanteil in der Organisation steigern. Nicht zuletzt deswegen, weil wir Projekte wie „Frauen in der IT" offensiv beworben haben und damit auch in der Öffentlichkeit das breite Spektrum für weibliche IKT- und Cyber-Expertinnen publik machen konnten.

Die Möglichkeit als Cyber- Grundwehrdiener bei uns den Wehrdienst ableisten zu können, hat sich offenbar in der Community herumgesprochen. Natürlich wird diese Möglichkeit durch das BMLV und auch von uns offensiv beworben.

Mittlerweile kommen nahezu nur mehr Grundwehrdiener als Cyber-GWD zu uns, die bereits einen Fachschul-, HTL-, FH- oder Universitätsabschluss mitbringen.

Und trotzdem verbleiben viele bei uns, weil die Aufgaben höchst interessant und abwechslungsreich sind, Weiterbildungsmöglichkeiten bestehen und man in einem interessanten jungen Team mitarbeiten kann. Auch das ist Bundesheer - Hightech abseits von geschwärzten Gesichtern.

Neben vielen Neuzugängen im Bereich hatten wir leider auch einige Todesfälle im Aktivstand und im Ruhestand zu beklagen. Mit Herrn Amtsdirektor Mag. Klaus Angelis, Herrn Hofrat Gerhard Stachel und Herrn Regierungsrat Klaus Kowalsky sei stellvertretend all jener gedacht, die uns in diesem Jahr verlassen mussten.

Andererseits durften wir uns 2023 besonders darüber freuen, dass unser Herr Gefreiter Benjamin Borenich aus dem IKT&CySihZ, zum „Grundwehrdiener des Jahres 2023 im Befehlsbereich Wien" und Herr Gefreiter Michael Bogensberger von unserem Führungsunterstützungsbataillon 2 zum „Grundwehrdiener des Jahres 2023 im Befehlsbereich Salzburg" gekürt wurde. Zwei Topnominierungen beim „Military Award 2023" haben das sehr erfolgreiche Bild 2023 abgerundet.

Die Steigerung der Cyber-Awareness, aber auch die Informationsoffensive unseren Aufgabenbereich und das breite Spektrum unserer Möglichkeiten publik zu machen, wurde 2023 konsequent weiter betrieben. Endlich haben wir unseren neuen „Cyber Escape Room". Dieses Projekt war mir ein ganz besonderes Anliegen.

An dieser Stelle möchte ich mich ganz besonders für die Unterstützung bei Herrn Oberst des höheren militärischen Fachdienstes Mag. Michael Hafner und Herrn Oberst des höheren militärischen Fachdienstes Mag. Bernhard Obmann bedanken. In der Realisierung dieses Vorhaben sei Herrn Oberst Walter Posch mit seinem Team vom Heereslogistikzentrum Wien und unserem Herrn Amtsdirektor Roland Pachler mit seinem Team herzlich gedankt.

Mit unserem neuen „Cyber Escape Room" konnten wir modern und innovativ junge Menschen für unseren Aufgabenbereich interessieren. Egal ob das beispielsweise im Rahmen des Rahmenprogramms zum Militärmusikfestival in Klagenfurt, der „Level up"- Spielemesse in Salzburg oder im Rahmen des Nationalfeiertags in Wien, war. Der „Cyber Escape Room" ist ein lebendiges Beispiel dafür, was alles in kürzester Zeit geht, wenn alle wollen und kreativ zusammenarbeiten. Und das zu einem Bruchteil dessen, was entsprechende Firmen dazu verlangt hätten.

Mein Vorwort abschließend, möchte ich mich bei allen Kommandanten, Leitern und Mitarbeiterinnen und Mitarbeitern herzlich für die gezeigten Leistungen im Jahr 2023 bedanken.

Der Kommandant der Cyberkräfte des
Österreichischen Bundesheeres

(Generalmajor Hermann Kaponig)

Marsch der Cyberkräfte

Gewidmet Herrn GenMjr Ing. Mag. Hermann Kaponig

Der Marsch der Cyberkräfte wurde anlässlich des 60. Geburtstages des Kommandanten der Cyber- & Informationskräfte, GenMjr Ing. Mag. Hermann Kaponig, und zur musikalischen Repräsentation der Direktion 6 - IKT&Cyber komponiert.

Dank und Anerkennung gebührt der Gardemusik Wien und insbesondere dem Komponisten Peter Josef Hammer.

~ ~ ~

Der Marsch ist in einem flotten 6/8el Takt geschrieben. Schon die Einleitungsfanfare erinnert an das binäre Computersystem, 0 und 1, an und aus, Ton und Pause, welches musikalisch wie ein Computerprogramm dargestellt wird.

Der erste Marschteil ist eine schöne moderne Melodie, welche durch Synkopen und Vierteltriolen an das flotte immer schneller werdende Internet erinnert. Bei der Wiederholung ist ein Zitat der Star Trek Titelmelodie eingebaut.

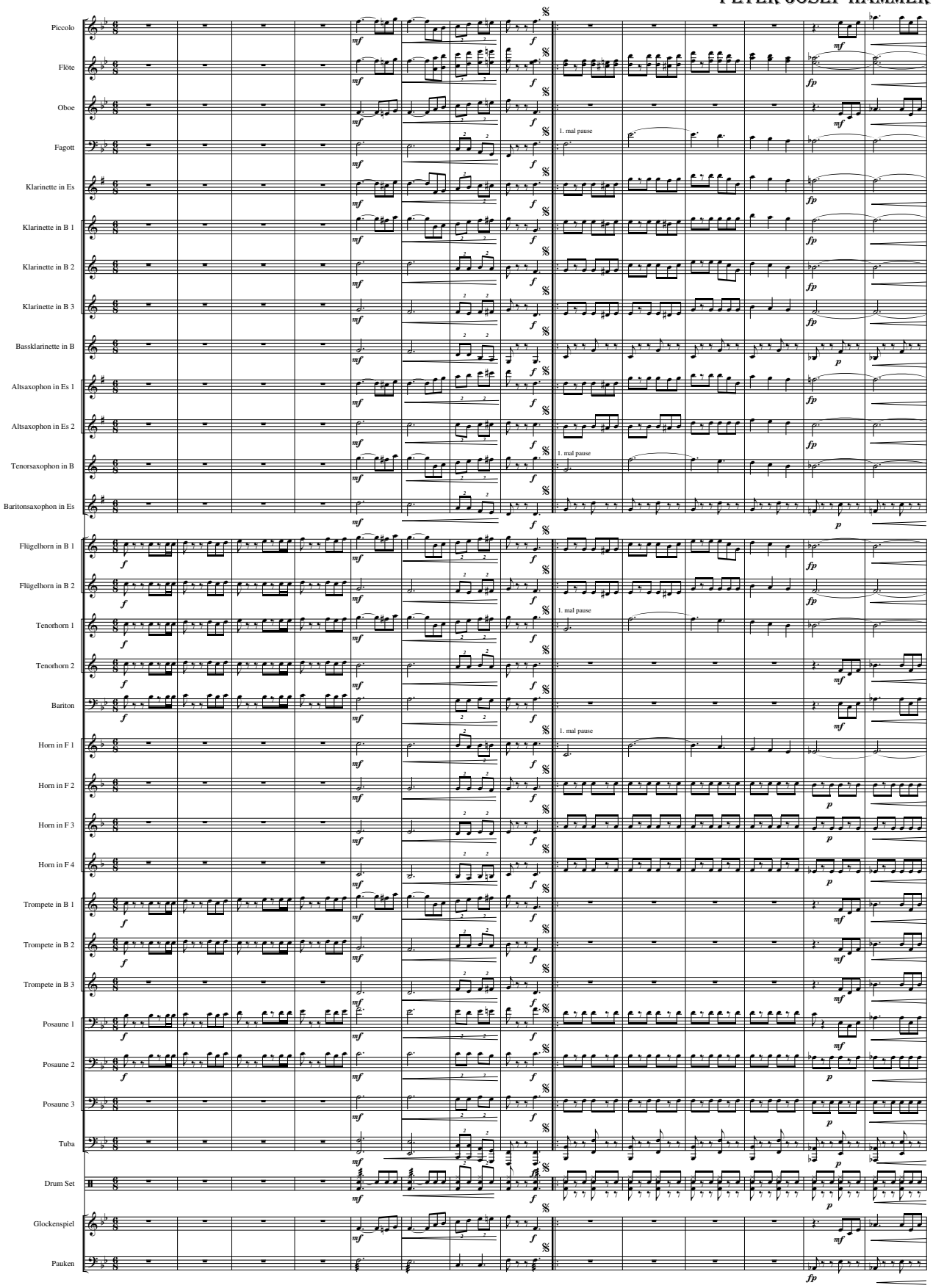
Im zweiten Teil soll das Basssolo mit einer Mollmelodie das Darknet hörbar machen, welches bei der Wiederholung von den Trompeten und Flöten bekämpft wird.

Es folgt nochmals triumphierend der 1. Marschteil welcher mit einem Blackout, dargestellt durch einen Fortissimo Schlagwerksolo, beendet wird.

In der Einleitung vom dritten Teil (Trio) symbolisiert die kleine Trommel mit leisen Schlägen das Blackout, gefolgt von einer traditionellen Melodie. Bei der Wiederholung verbinden die Holzbläser mit einer rhythmischen Gegenmelodie, moderne und Tradition bis der Marsch in einem Grandioso endet.

PARTITUR

PETER JOSEF HAMMER



Bundesministerium für Landesverteidigung

Forschung & Entwicklung

Forschung und Entwicklung spielen im militärischen Bereich eine entscheidende Rolle und sind von großer Bedeutung für die Streitkräfte weltweit. Technologische Innovation und fortgeschrittene Verteidigungsforschung wirken sich nicht nur auf die Effizienz und Effektivität militärischer Operationen aus, sondern haben erhebliche Auswirkungen auf die globale Sicherheitslandschaft.

Moderne Streitkräfte zeichnen sich unter anderem dadurch aus, dass sie:

- Vorteile aus technologischen Fortschritten für sich ziehen,
- flexibel auf Änderungen der Bedrohungslage reagieren können,
- multinational zusammenarbeiten oder
- über Fähigkeiten in der Cyberkriegsführung verfügen.

Sie investieren Ressourcen in die Erforschung, Entwicklung und Produktion von High-Tech-Waffensystemen, um ihre Verteidigungsfähigkeiten zu stärken. Die Bandbreite reicht von konventionellen Waffen bis hin zu hochspezialisierten Systemen wie Drohnen, Cyberwaffen, autonomen Systemen oder Machine-Learning- / Künstlicher Intelligenz-Systemen.

Fortschritte in der Elektronik sowie im Bereich der Kommunikationstechnologie, verschlüsselte Übertragungen und moderne Radarsysteme haben zu Fortschritten in der Militärtechnologie geführt. Moderne Streitkräfte sind in der Lage domänenübergreifend, streitkräfteübergreifend, system- bzw. plattformübergreifend sowie führungsebenenübergreifend Informationen in nahezu Echtzeit sicher auszutauschen. Diese Art von Informationsüberlegenheit ist entscheidend für eine erfolgreiche Operationsführung.

Im Kontext der umfassenden Landesverteidigung muss das ÖBH und somit auch die Direktion 6 - IKT&Cyber auch auf hybrid agierende, vorwiegend irreguläre Gegner reagieren.

Es ist davon auszugehen, dass potenzielle Gegner mit modernsten technischen Mitteln ausgerüstet sind und daher den eigenen Kapazitäten überlegen sein können, indem sie z.B. hochspezifische Cyberwaffen, autonome Systeme, Künstliche Intelligenz (KI) oder Quantentechnologie zur Anwendung bringen. Emergente und disruptive Technologien werden in den Fachbereichen der Direktion 6 - IKT&Cyber sehr genau beobachtet. Die Beteiligung an geförderten, nationalen und europäischen Forschungsprojekten ist nur eine von mehreren Möglichkeiten, wie wir den langfristigen Herausforderungen begegnen wollen.

Expertinnen und Experten der Dion6 sind in nahezu allen strategischen Forschungs- und Entwicklungs-Bereichen (SFB) des BMLV/ÖBH – z.B. Digitalisierung, Cyber und EloKa, Weltraumtechnologie, Robotik und Autonome System – engagiert. Unser Ziel ist es, nach Maßgabe der verfügbaren Personalressourcen, Ergebnisse aus der angewandten Forschung sowie der experimentellen Entwicklung mittelfristig im Regelbetrieb zur Wirkung zu bringen. Wir pflegen die aktive Zusammenarbeit mit Bildungseinrichtungen, indem wir u.a. Diplomarbeiten von Schülerinnen und Schülern sowie Studierenden betreuen.

Nachfolgend werden Beispiele für betreute Diplomarbeiten sowie Forschungsvorhaben dargestellt.

Foto: pixabay.com

Diplomprojekte

LowCode/NoCode-Plattform

Programmierung einer LowCode/NoCode-Plattform für Webapplikationen durch Schülerinnen und Schüler der HTL Spengergasse. Damit soll es möglich sein, dass Anwender ohne Programmierkenntnisse Webapplikationen erstellen können.
Den Anwendern steht dazu eine grafische Oberfläche zur Verfügung, in welcher unterschiedliche Elemente (wie z.B: Texteingabefelder, Textbausteine, Buttons, etc.) zur Auswahl stehen. Diese können mit Hilfe von Drag&Drop zu einer Maske zusammengefügt werden.

Für jede dieser Applikationen wird im Hintergrund eine eigene Datenbank generiert inkl. Berechtigungssystem. Außerdem soll die Applikation eine Schnittstelle zur Verfügung stellen, über welche MS-Excel-Dateien eingelesen werden können.

GeoWeb-Anwendung

Umsetzung einer GeoWeb-Anwendung durch Schülerinnen und Schüler der HTL Spengergasse, welche verlegbare Funkstandorte und deren Verbindungsrelationen für die IKT-Netzplanung erfasst und strategische Daten zum Zweck der Führungsfähigkeit bereitstellt.

Foto: Bundesheer/Dion6

BOOST-Überblick

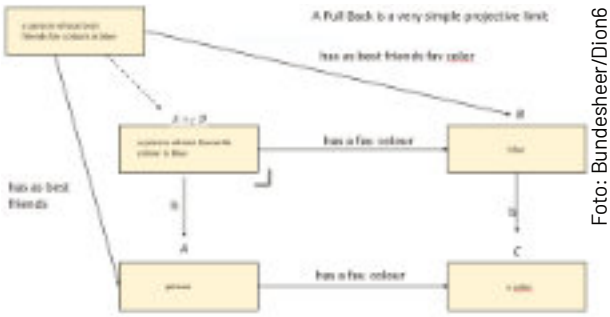


Foto: Bundesheer/Dion6

AGI II Thinking Diagram

Die Applikation wird aus einer interaktiven Landkarte, einem Content Management System und einem Zugriffskontrollsystem bestehen. Für geschultes Fachpersonal wird es möglich sein, die verlegbaren Funkstandorte zu verwalten und neue anzulegen. Die Planung der Funkstandorte erfolgt visuell über die Karte und bietet die Möglichkeit die Daten für den Einsatz, wie etwa das topographische Höhenprofil, Funktypen und Entfernungen zu exportieren. Durch die grafische Unterstützung mit Hilfe einer Landkarte werden die Koordinaten eines neuen Funkstandortes bei der Neuerfassung automatisch mit einem Klick auf die Karte erfasst.

Forschungsprojekt FORTE Projekt BOOST

BOOST (AdaptaBle autOmated intelligence gathering prOcesses for decision SupporT) ist ein kooperatives F&E Projekt, das im Rahmen des Militärforschungsprogramms FORTE von der Österreichischen Forschungsförderungsgesellschaft FFG gefördert wird. Basierend auf den Ergebnissen des Vorgängerprojekts PIONEER erweitert BOOST die Fähigkeiten im taktischen Aufklärungsverbund mittels Integration multimodaler Datenquellen (Audio, Video, Text) und durch maschinelles Lernen. Neben der Nutzung etablierter Methoden, wie der semantischen Repräsentation, wird dabei auch mit aktuellen Verfahren der KI, beispielsweise Large Language Models (LLM) experimentiert, um die Leistungsfähigkeit der automatisierten Nachrichtengewinnung aus unstrukturierten Daten zu verbessern. BOOST orientiert sich konsequent an standardisierten Prozessen und Datenstrukturen gemäß Federated Mission Networking (FMN).

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Artificial General Intelligence

Im Rahmen des Forschungsvorhabens wird versucht, Artificial General Intelligence (AGI) für einen konkreten Anwendungsfall zur Anwendung zu bringen. Die verfügbare KI wird bereits im medizinischen Sektor eingesetzt.

Per Definition zeichnet sich eine AGI dadurch aus, dass sie die Fähigkeit besitzt, jede intellektuelle Aufgabe zu verstehen oder zu lernen, die ein Mensch ausführen kann.

Das Ziel des Vorhabens ist es zu evaluieren, ob das bereitgestellte KI-System mit geringen Datenmengen und auf handelsüblicher Hardware Ergebnisse für den definierten Anwendungsfall – nicht im medizinischen Sektor - liefert. Es wurden ca. 2.400 Datensätze als Basis für das Trainieren der KI zur Verfügung gestellt.

Das Training erfolgte auf einem Server, welcher bereitgestellt wurde.

Cyberlagebild

Das Gefechtsfeld wird komplexer, vernetzter und unübersichtlicher. Sicherheit kann nur gewährleistet werden, wenn ein umfassendes Situtationsbewusstsein durch ein holistisches Lagebild, sichergestellt ist. Daher ist die Erstellung eines Quellen- und ebenenübergeifenden Lagebildes einer der zentralen Schwerpunkte im Rahmen der Forschung und Entwicklung auf nationaler und internationaler Ebene.

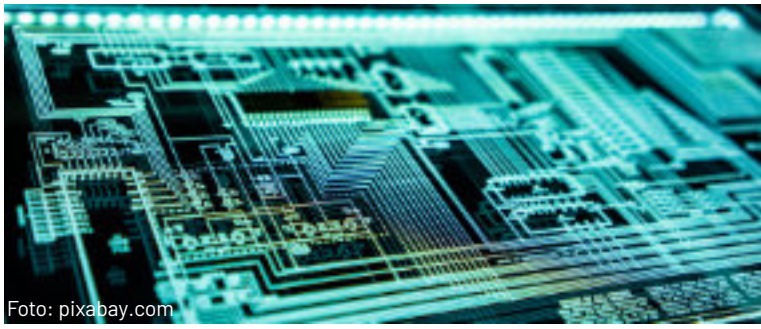


Foto: pixabay.com

Cyber Range

Die Entwicklung und Optimierung von Cyber Range-Plattformen für die Einrichtung eines Cyber-Truppen Übungs Platzes stehen im Fokus, um realistische Trainingsumgebungen für Cyber-Abwehrmaßnahmen zu schaffen. Es sollen die Rahmenbedingungen geschaffen werden, damit Einsatzkräfte optimal auf aktuelle und zukünftige Bedrohungen vorbereitet werden.

Um Interoperabilität mit anderen europäischen Mitgliedstaaten zu gewährleisten, ist auch in diesem Bereich die aktive Teilnahme an EU-Projekten zur Entwicklung gemeinsamer Fähigkeiten sowie zur stetigen Zusammenarbeit besonders relevant.

Security Operations Centers (SOC) & Rapid Response

Die Experten der Direktion 6 - IKT&Cyber arbeiten kontinuierlich an der Verbesserung von Security Operations Centers (SOC) und schnellen Reaktionsmechanismen. Durch effiziente Überwachung und rasche Reaktion auf Sicherheitsvorfälle wird die Widerstandsfähigkeit gegenüber Cyberangriffen gestärkt.

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Hierfür wird einerseits im Bereich des gezielten Einsatzes bedarfsorientierter KI-Modelle zur Erkennung und Analyse von Angriffen geforscht und auf EU-Ebene gemeinsame Lösungen entwickelt.

Andererseits ist die Einrichtung bzw. Weiterentwicklung von Rapid Response Teams unerlässlich. In der Direktion 6 - IKT&Cyber engagiert sich das MilCyZ insbesondere durch die Teilnahme an europäischen Kooperationsprojekten im Bereich Rapid Response, um Erfahrungen und Expertise auszutauschen und damit Synergien mit den nationalen Bestrebungen zu schaffen.

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Cyber Sicherheits-Technik & Security-Framework

Die Forschung im Bereich der Cyber Sicherheits-Technik konzentriert sich auf innovative Lösungen und Technologien zur Absicherung von IKT-Systemen, um fortschrittliche Verteidigungsmechanismen zu entwickeln.

Es wird zudem an der Integration und Anpassung entsprechender Frameworks gearbeitet, um einen robusten Sicherheitsansatz zu gewährleisten.

Post Quanten Kryptographie

Angesichts der Fortschritte im Bereich der Quantencomputing-Forschung beschäftigten sich Spezialisten der Direktion 6 - IKT&Cyber mit der Entwicklung und Implementierung von Post-Quanten-Kryptographie. Hierbei liegt der Fokus auf zukunftsorientierten und sicheren Verschlüsselungsmethoden.

Daher wurde das Forschungsvorhaben zur Entwicklung eines Kryptosystems, welches mit österreichischem Wissen entwickelt und zukünftig im österreichischen Wirtschaftssystem produziert werden soll, ins Leben gerufen. Im Bereich der Cyber-Sicherheit ist die Verschlüsselung der Garant zur Gewährleistung des Schutzziels Vertraulichkeit.

Quantentechnologie

Die Direktion 6 - IKT&Cyber ist sich der potenziellen Auswirkungen von Quantencomputing auf die Sicherheitslandschaft bewusst.

Forschungsaktivitäten in diesem Bereich zielen darauf ab, frühzeitig Strategien zu entwickeln, um mit den Herausforderungen dieser neuen Technologie umzugehen und potentielle Anwendungsbereiche zu eruieren und dementsprechende Fähigkeiten aufzubauen. Unter anderem beteiligen sich Experten der Direktion 6 - IKT&Cyber in europäischen Projekten zur Bereitstellung einer EU Secure Quantum Communication Infrastructure.

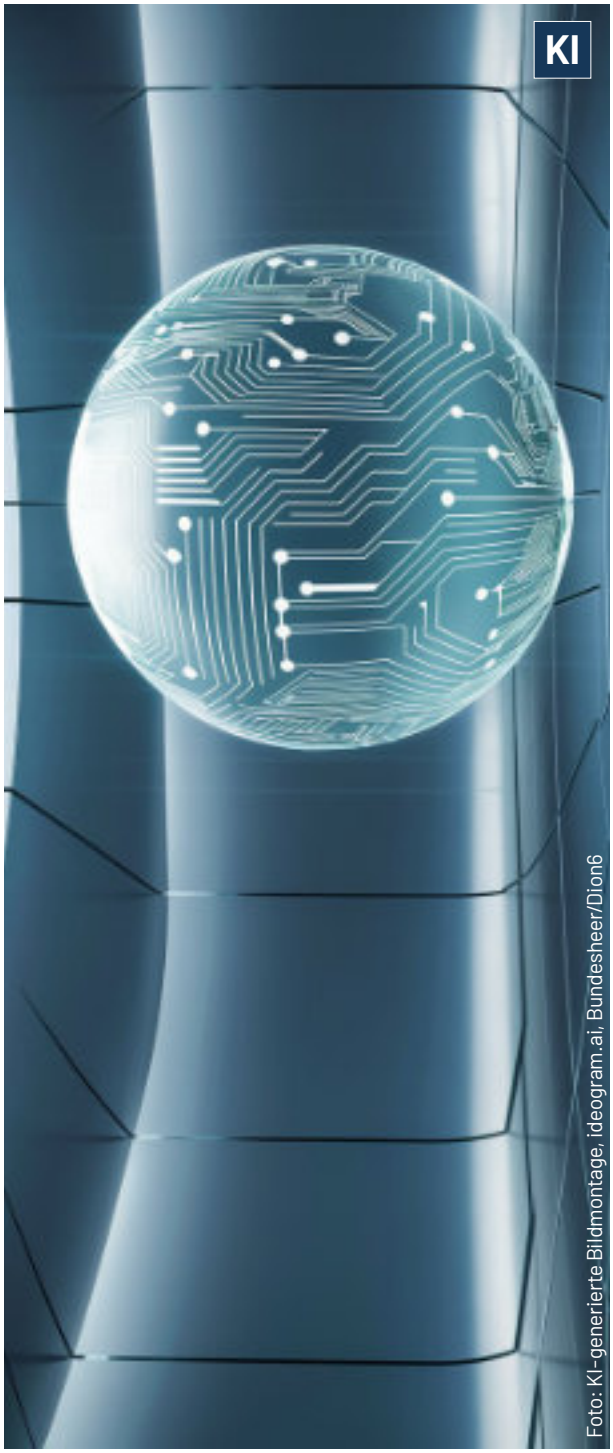


Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Bundesministerium für Landesverteidigung

Fähigkeitsentwicklung & Aufbauplan 2032+

Im vergangenen Jahr lag das wesentliche Schwergewicht in der Weiterentwicklung der Cyber- und Informationsdomäne. Dabei waren einerseits die Fähigkeiten zu definieren und andererseits deren Aufwuchs im Rahmen des Aufbauplans ÖBH 2032+ zu entwickeln. Die zugehörigen Waffengattungen Cyber, EloKa, FüU (vormals IKT), sowie die Kommunikations- und PsyOps- Truppen wurden dabei unter einem zentralen Teilstreitkräftekommando zusammengeführt.

Das erreichte rein planerische Ziel der Direktion 6 - IKT&Cyber im Kalenderjahr 2023 war es, die Waffengattungen im Sinne der Ausrüstung zu modernisieren, leistbare bzw. benötigte Services und Fähigkeiten zu entwickeln, deren Personal zu spezialisieren, adäquate Ausbildungen zu formulieren, die benötigten Strukturen modern und effizient zu definieren und dabei klar die Ziele und Notwendigkeiten für eine moderne Einsatzführung aufzuzeigen.

Das Cyber- und Informationsdomäne Teilstreitkräftekommando [Component Command] (CyIDCC) stellt dabei nicht nur die zentrale Einrichtung zum Führen der nachgeordneten waffengattungsspezifischen Truppenkörper dar, sondern dient auch als oberes taktisches Bindeglied inhärent der fachlichen Expertise zur operativen Ebene im Rahmen der eingeführten Planungsprozesse.

Als Novum und zugleich Herausforderung für den Aufbau und Aufwuchs des Kommandos ist die umfängliche Einbindung der Miliz in allen Bereichen, von der Führung bis hin zu den jeweiligen Spezialisten in den Waffengattungen mit dem Ziel einen unterbrechungsfreien, zeitverzugslosen und unmittelbaren Übergang vom Frieden in den Einsatz sicherzustellen.

Mit der Aufstellung des Kommandos bzw. der Überleitung bestehender Strukturen in die neue Gliederung wird nicht nur eine neue Domäne nun militärische genutzt und für die Einsatzführung zur Verfügung gestellt werden, sondern auch bereits vorab in Friedenszeiten ein wesentlicher Mehrwert für die Früherkennung und Sicherheit geleistet.

Foto: pixabay.com

Im Zuge der Bearbeitungen wurde auch die Cyber- Truppe weiterentwickelt und mit Strukturen hinterlegt, die einen umfänglichen Einsatz im Rahmen einer Schutzoperation ermöglichen.

So sind neben hoch beweglichen Elementen vor allem die Ausbildungs- und Testumgebung, sowie die Cyber- Informationszentren zu nennen, die im Einsatz unerlässliche Ressourcen, Informationen und damit verbundene Einsatz-orientierte Möglichkeiten bereitstellen. Ganz besonders muss hier die internationale Zusammenarbeit erwähnt werden, die im letzten Jahr insofern intensiviert werden konnte, als dass Informationen und Einsatzerfahrungen anderer Armeen aufgenommen und beurteilt werden konnten. Mitunter konnten auch diverse Ausbildungen genutzt werden, die das notwendige Wissen und die Prozesse innerhalb der Cyber Truppe wesentlich ergänzt haben.

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Mit den nun vorhandenen Instrumenten, den mittlerweile angelaufenen spezialisierten Ausbildungen, den etablierten Strukturen und den geplanten Weiterentwicklungen wird gerade die Cyber Truppe in den nächsten Jahren einen immer größeren Stellenwert in der Einsatzführung des österreichischen Bundesheeres erleben und dabei einen immensen Mehrwert darstellen.
Die EloKa- Truppe wird langfristig einen klaren Aufwuchs erfahren, zumal in den letzten Jahrzehnten das elektromagnetische Spektrum immer wichtiger wurde bzw. in der heutigen Einsatzführung nicht mehr wegzudenken ist.

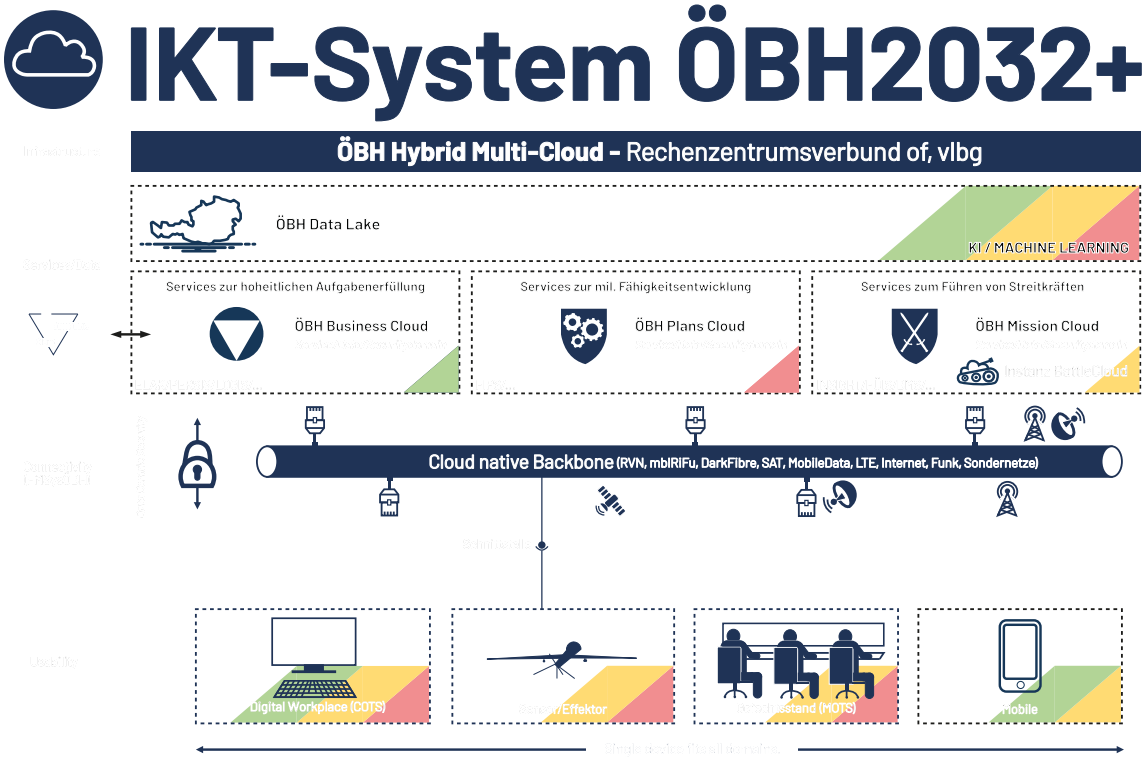


Foto: Bundesheer/Dion6

IKT-System ÖBH2032+

Dabei umfassen die Bereiche nicht mehr nur die frühere Erfassung und Auswertung einzelner Frequenzen zum Zwecke der Aufklärung, sondern vielmehr auch die Optionen zur Manipulation, Verschleierung oder Negierung von Informationsübertragungen im Spektrum. Hinzukommend und damit ein wesentlicher Treiber des Aufwuchs sind die immer stärker genutzten Positionierungssysteme (GNSS) und Kommunikationsservices aus dem Weltraum. Gerade die Symbiose zwischen der EloKa Truppe und den erdunterstützenden Fähigkeiten bzw. Services aus dem Weltraum heraus, stellt hier eine neue Dimension der Einsatzführung und -Unterstützung dar, die zukünftig entscheidend für die Kommandanten sein wird.

Auch konnte noch vor Ende des Jahres ein Workshop hinsichtlich der Ausbildung für Fachpersonal im Space Bereich abgehalten werden, sodass Ende des nächsten Jahres das erste Personal zur Umsetzung der Strukturen im Space Bereich zur Verfügung stehen wird. Mit all diesen Maßnahmen wird damit auch die EloKa- Truppe in den nächsten Jahren nicht nur ihr Einsatzspektrum im passiven Bereich erhöhen, sondern auch mehr Möglichkeiten in der aktiven Mitgestaltung der Einsatzführung erfahren.

Die Führungsunterstützungstruppe, vormals IKT-Truppe, wird technologisch auf den neuesten Stand gebracht. So wird es in erster Linie die Aufgabe der Direktion 6 - IKT und Cyber sein, das neu etablierte, militärische Einsatznetz vollflächig zu implementieren, die dahinter stehenden Services und Rechenzentren zu integrieren und deren Funktionalitäten autark im Verband und resilient im Rahmen der Einsatzführung aufzubauen.

Damit wird nicht nur der wesentliche Baustein für eine vernetzte Einsatzführung im Sinne des friktionsfreien, medienbruchfreien und homogenen Aufklärungs-, Führungs- und Wirkungsverbund mit der umfassenden Integration aller im ÖBH eingeführten Sensoren, Plattformen und Effektoren gelegt, sondern auch die Basis für eine vernetzte, die Einsatzführung unterstützende Datenbasis für zukünftige Modelle künstlicher Intelligenzen gelegt.

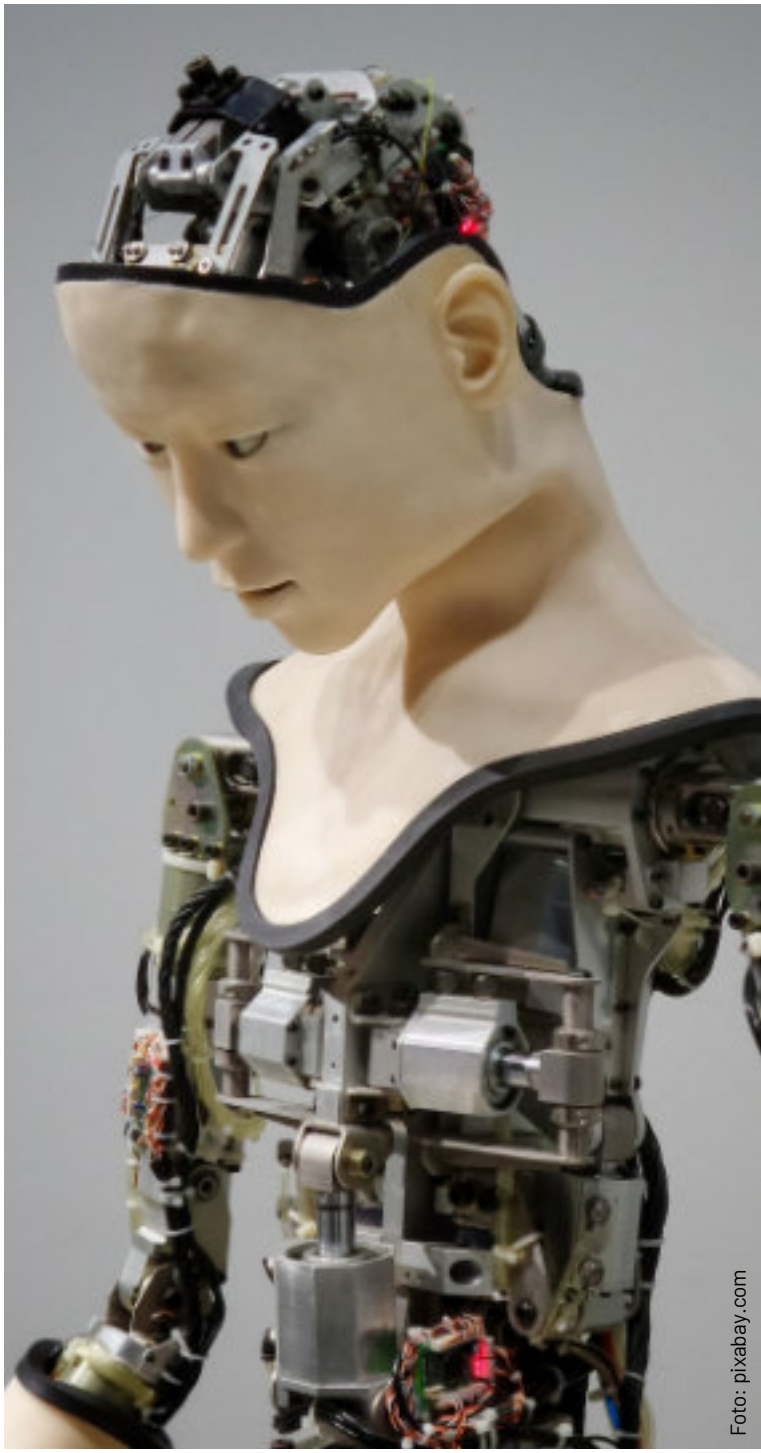


Foto: pixabay.com

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Die mittlerweile fast abgeschlossene Umrüstung der Streitkräfte auf das Tactical Communication Network (TCN) stellt hierbei die Basis für die zukünftigen Systeme dar. Dies ist jedoch erst der erste Schritt hin zu einer vollumfänglichen Neuausrichtung der Vernetzung über alle Ebene hinweg und wird in den nächsten Jahren mittels der jeweiligen Bausteine weiter fortgeführt.

Gerade hier ist der Ansporn im Jahr 2032 eine umfassend vernetzte Systemumgebung bereitzuhalten von derartiger Wichtigkeit, da immer mehr Systeme, im Sinne von Sensoren, Plattformen und Effektoren, nur mehr vernetzt nutzbar bzw. sogar teilweise nur mehr so beschaffbar sind.

Eine friktionslose, rasche und datenzentrierte Einbindung der Waffensysteme in die prozessualen, digitalisierten Abläufe ist somit nicht nur das oberste Ziel der Bearbeitungen sondern in Zukunft auch unumgänglich. Erst mit diesem Schritt wird es zukünftig möglich sein, alle Waffengattungen und deren Systeme auf einem modernen Gefechtsfeld harmonisierend zur Wirkung zu bringen.

Im Zuge der Bearbeitungen wurden die Informationskräfte neu aufgestellt. Gemeinsam mit der Direktion Kommunikation wurde eine Grundsatzstruktur geschaffen, um zukünftig vor allem im Bereich der Informationsoperationen die Einsatzführung auch in dieser Domäne besser aufzustellen.

Dies fängt damit an, dass hoch bewegliche und spezialisierte Truppenteile verfügbar sein müssen und geht bis zur Implementierung von fachlich beratenden Elementen in den jeweiligen Stäben. So wurden hier auch die neuesten Erkenntnisse und Erfahrungen aktueller Konflikte in die Entwicklungen der neu aufzubauenden Fähigkeiten in der Informationsdomäne herangezogen.

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6


Foto: pixabay.com

Wesentlich ist hierbei die umfassende Implementierung der kognitiven Sichtweisen in die stabsdienstlichen Prozesse aller Ebenen unter einem gemeinsamen Narrativ mit der Etablierung einer ständig strukturierten strategischen Kommunikation. Auf der operativen Ebene fügt sich diese gemeinsame Bearbeitung dann in die jeweiligen Spezialgebiete ein, sodass die Informationsdomäne nicht nur einen wesentlichen Mehrwert in der Einsatzführung erfährt, sondern auch eigenständig Effekte generiert, die die strategischen Ambitionen im Anlassfall untermauern.

Nachdem nun die Ausrichtungen klar beschrieben wurden, gilt es nun in den folgenden Jahren deren Umsetzung zu forcieren, das Personal zu rekrutieren, zu schulen und die Strukturen zu implementieren. Es sind aber noch weitere planerische Tätigkeiten vorab der Bereitstellung erster Kräfte nachzuziehen.

So sind die Prozesse der jeweiligen Waffengattungen mit dem des Teilstreitkräftekommando zu harmonisieren bzw. weiterzuentwickeln, aber auch zu erproben und im Rahmen einer operativen Planung zu implementieren.

Dies wird neben den weiteren Bearbeitungen zu Strukturen, Ausrüstung und Ausbildung ein wesentlicher Meilenstein für das Jahr 2024.

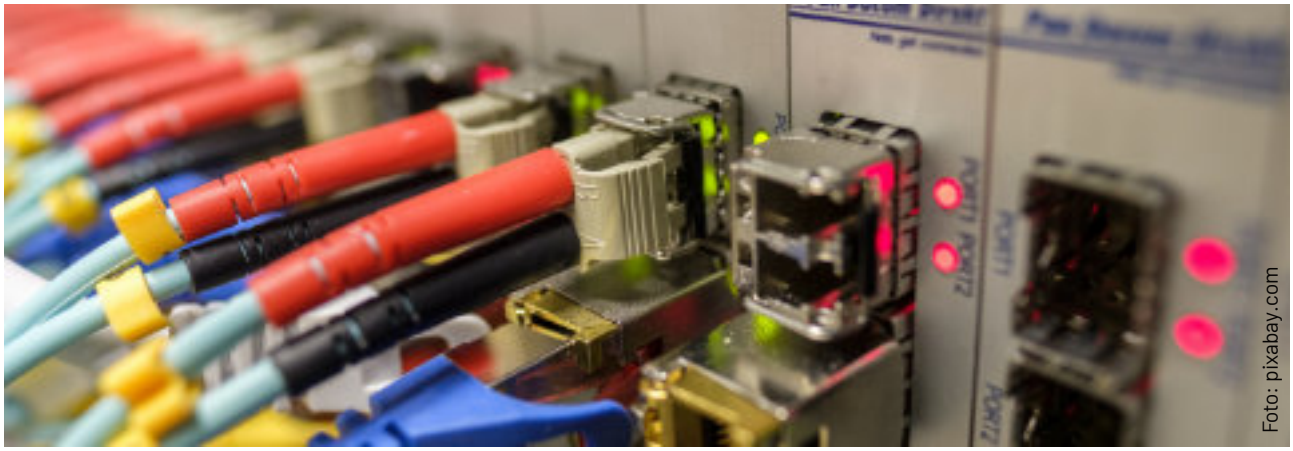


Foto: pixabay.com

Bundesministerium für Landesverteidigung

Digitalisierung & KI

Enterprise Architektur

Ein umfassender Ansatz zur Unterstützung der digitalen Transformation

Um im Zeitalter des digitalen Wandels erfolgreich zu sein, ist es erforderlich, Prozesse der Leistungserbringung von Organisationen zu digitalisieren, nämlich sie an den Möglichkeiten digitaler Technologien auszurichten bzw. an diese anzupassen. Das erfordert im Ressort eine netzwerkorientierte und datengetriebene Denkweise und im Besonderen das Annehmen der Herausforderung der digitalen Transformation.

In einer Welt, die sich kontinuierlich komplexer gestaltet, ist es unabdingbar, dass das Ressort in der Lage ist, schnelle und fundierte Führungs- und Planungsentscheidungen zu treffen. Ein strukturierter und ganzheitlicher Ansatz, wie ihn die Disziplin der Enterprise Architektur bietet, ist hierbei von essenzieller Bedeutung.

Enterprise Architektur stellt einen entscheidenden Baustein dar, um die digitale Transformation im ÖBH voranzutreiben und den Herausforderungen einer modernen, vernetzten Welt zu begegnen. Sie ermöglicht ein umfassendes Verständnis für das komplexe Geflecht aus Anforderungen, Abhängigkeiten und Rahmenbedingungen. Ziel ist es, die komplexe Struktur und Funktionsweise des ÖBH in ihrem Zusammenspiel zu erfassen und in klar verständlichen sowie nachvollziehbaren Modellen darzustellen. Dadurch wird eine planvolle und nachvollziehbare Gestaltung von effektiven und effizienten digitalen Prozessen und Wirkmodellen ermöglicht und so ein wichtiger Beitrag für die digitale Transformation geleistet.

Aufbau der Fähigkeit im ÖBH

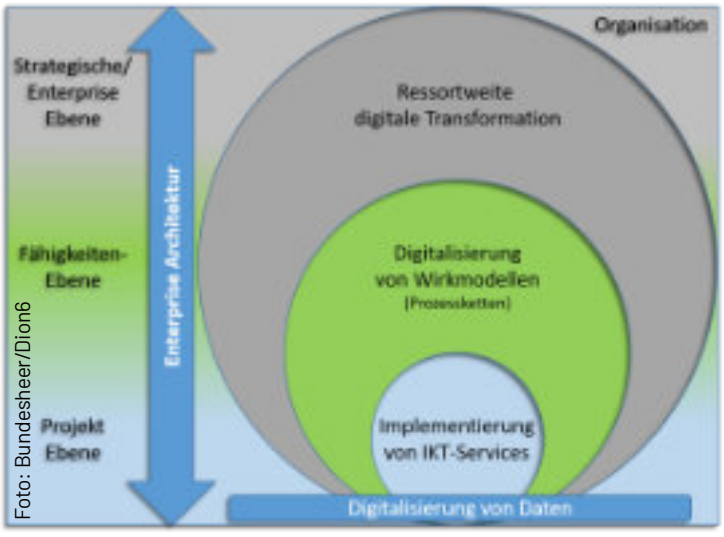
Die Fachdisziplin des Enterprise Architektur Management soll zukünftig im strategischen Unterstützungselement Digitalisierung (SUeD) verortet sein und die Teilbereiche der „Architecture Governance", des „Architecture Managements" sowie der eigentlichen Architektur-Entwicklung abdecken.

Ein notwendiger Personalaufwuchs wird neben Enterprise Architekten auch Business Analysten sowie Informations- und Datenarchitekten umfassen müssen. Technisch wird die Fachdisziplin durch ein datenbankgestütztes Architektur-Repository unterstützt werden, das eine Modellierung, Verknüpfung und Auswertung der entwickelten Architekturen ermöglichen soll.

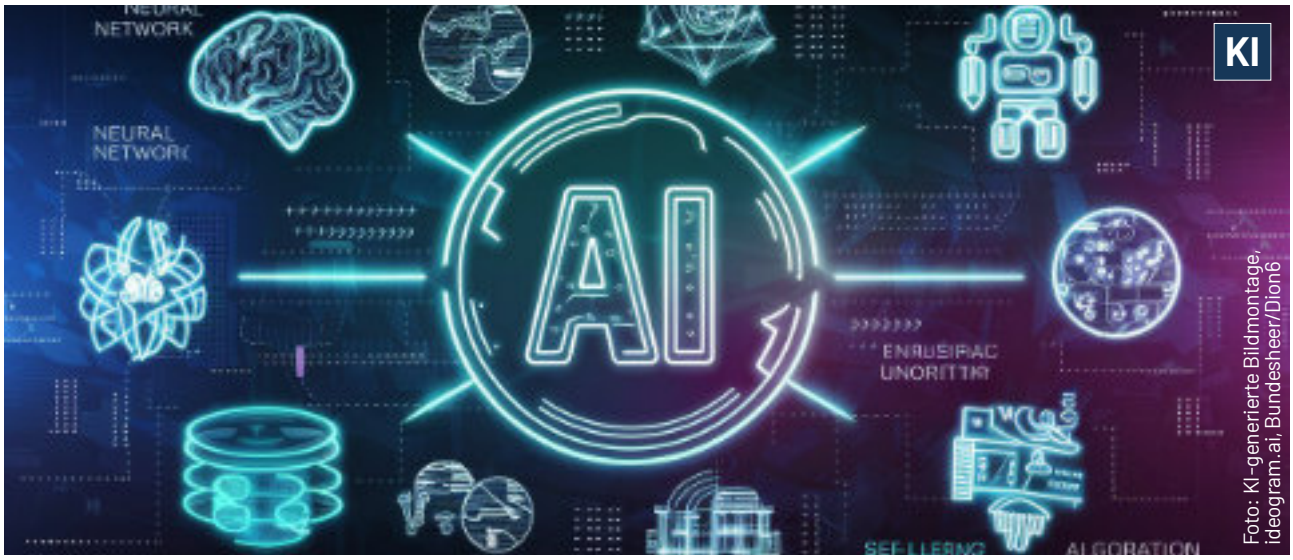
Für die Nutzbarkeit von Enterprise Architektur sowie für die Generierung eines Mehrwerts für die Organisation wird die Einbindung der eigentlichen Bedarfsträger sowie der planenden Dienststellen von entscheidender Bedeutung sein.

Konzeptioneller Aufbau und Nutzung

Die bisherigen konzeptionellen Überlegungen zu Aufbau und Nutzung von Enterprise Architektur im Ressort zeigen bereits deutlich, wie das Österreichische Bundesheer von EA profitieren kann. Die Erfassung und Beschreibung von operationellen Abhängigkeiten und Informationsflüssen schaffen die Grundlage für ressortweite Informations- und Datenarchitekturen. Diese schaffen die Basis für eine effiziente Nutzung der Ressource „Daten" (Analysen auf Basis von Daten und die Fähigkeit zu datenbasierten Entscheidungen).



Enterprise Architektur

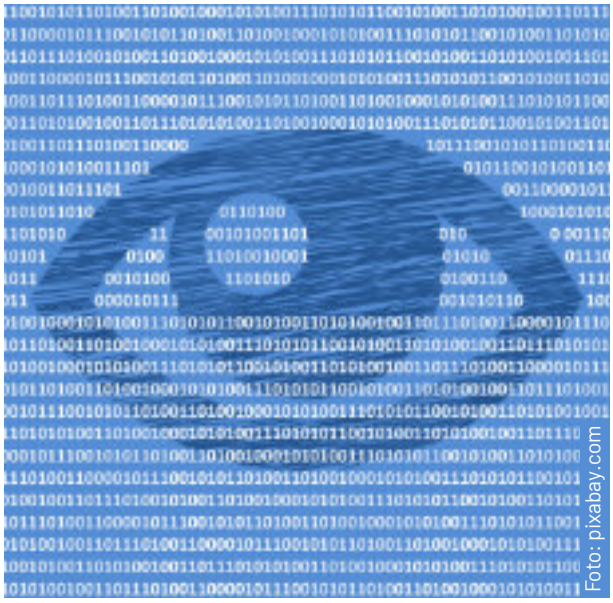


Durch ein ganzheitliches, modellbasiertes Planen und Gestalten digitaler Wirkmodelle wird das Zusammenspiel von Akteuren, Plattformen, Sensoren und Informations- und Kommunikationstechnologie im Aufklärungs-, Führungs- und Wirkungsverbund konkret beschrieben. Diese Zielarchitekturen ermöglichen im Vergleich mit der aktuellen Ist-Situation Ableitungen für erforderliche Vorhaben und Digitalisierungsmaßnahmen in allen Entwicklungslinien.

Durch ein auf die Enterprise Architekturentwicklung aufgesetztes modernes Requirements-Engineering wird eine stringente und nachvollziehbare Ableitbarkeit von Anforderungen aus Zielarchitekturen sichergestellt.

Daten – Der „Rohstoff" der digitalen Transformation

Im Zeitalter der Digitalisierung ist ein Wissens- und Entscheidungsvorsprung entscheidend für eine effektive und effiziente Aufgabenerfüllung. Dieser Vorsprung kann nur durch die umfassende Nutzung von Informationen (Daten) erreicht werden. Moderne Technologien wie das „Internet of Things (IoT)", Sensoren und mobile Geräte haben die Produktion von Daten (Datenerfassung, Verteilung und Bereitstellung) revolutioniert. Datentechnologien ermöglichen, große und komplexe Datenmengen effektiv zu analysieren und daraus wesentliche Erkenntnisse für die Wahrnehmung von Aufgaben zu gewinnen. Fortschritte in der Anwendung künstlicher Intelligenz verbessern die Möglichkeiten der Datenanalyse und ermöglichen automatisierte Erkenntnisse und Vorhersagen.



Daten können inzwischen beinahe in Echtzeit erfasst, verarbeitet und analysiert werden. Das ermöglicht, Entscheidungen schneller zu treffen und Wirkungen rascher und genauer herbeizuführen. Dazu müssen ausreichende Speicherkapazitäten, Rechenleistungen und Analysefähigkeiten dort bereitgestellt werden, wo die für die Analysen und Entscheidungsunterstützungen notwendigen Daten in Echtzeit verarbeitet werden sollen.

Digitale Prozesse und Prozessketten bilden den Kern der digitalen Transformation. Daten stellen den dafür erforderlichen „Rohstoff" dar. Digitalisierung zielt aus Datensicht auf den Aufbau einer datenorientierten Organisation ab, welche datenbasierte (faktenbasierte) Entscheidungen und die Automatisierung von Prozessen ermöglicht. Die Fähigkeit zum Erfassen, Integrieren, Bereitstellen und Nutzen von Daten bildet die Kernkompetenz datenorientierter, digitalisierter Organisationen.

Daten sind keine Nebenprodukte der IT oder „IT-Assets", sondern die Träger von Informationen. In einer zunehmend digitalen Welt hinterlässt praktisch jede Person, jedes Gerät und jede Interaktion digitale Spuren. Durch die zunehmende Vernetzung von Geräten, die Verbreitung von Sensoren und durch die verstärkte Nutzung digitaler Plattformen können aus diesen Daten

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

durch Zusammenführung und Einsatz moderner Analysemethoden und Technologien wertvolle Erkenntnisse für das Ressort gewonnen werden.

Dadurch sollen Entscheidungsprozesse unterstützt, Trends identifiziert, Prognosen erstellt, und Prozesse und Verfahren zur Aufgabenwahrnehmung verbessert werden. Durch professionelle Nutzung von Daten kann Informations- und Wirkungsüberlegenheit in militärischen Einsätzen erzielt werden. Zu diesen Zwecken müssen Informationen (Daten), die in strukturierter oder unstrukturierter Form vorliegen, verarbeitet, analysiert, interpretiert und verwertet werden können.

Daten stellen ein zentrales Asset der Leistungserbringung dar und müssen durch die jeweiligen Prozessverantwortlichen und Entscheider als solches verstanden und gemanagt werden.

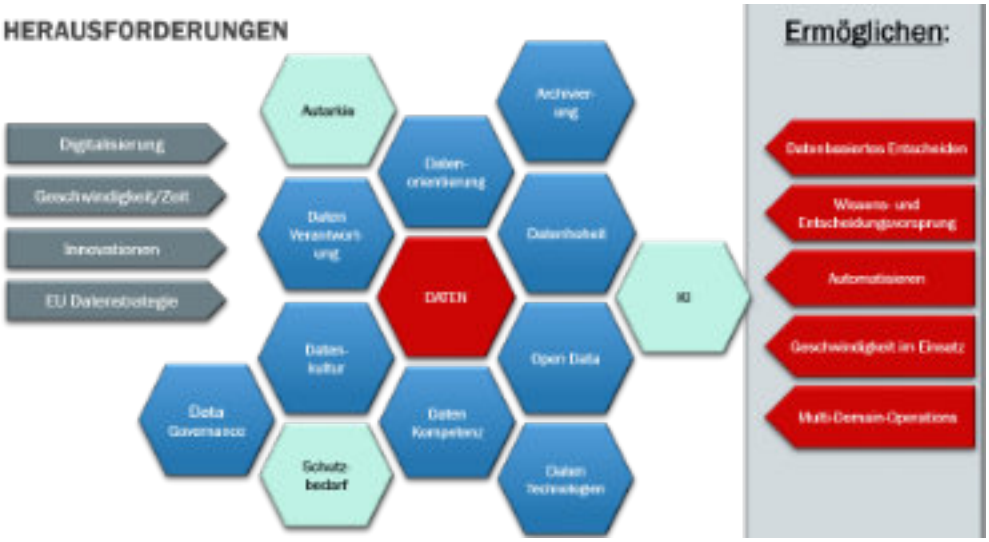


Foto: Bundesheer/Dion6

Herausforderungen der Digitalen Transformation


Foto: pixabay.com

Fähigkeiten sowie die Geschäftsprozesse, mittels welcher Fähigkeiten „realisiert" werden, müssen zu ihrer Digitalisierung datenorientiert geplant und entworfen werden.

Das Ressort unterstützt den digitalen Transformationsprozess, indem es sich zu einer datenorientierten Organisation bekennen muss und sich zu einer solchen auch entwickeln muss. Dazu müssen Daten im Ressort als wertvolles strategisches Gut verstanden und gezielt als Mittel der Entscheidungsfindung eingesetzt werden. Durch die intelligente Nutzung von Daten muss der Transformationsprozess gesteuert und die datenbasierte Optimierung und Neugestaltung von Geschäftsprozessen ermöglicht werden.

Um diesen Herausforderungen gerecht zu werden, wurde im Ressort erstmalig eine Datenstrategie entwickelt. Diese definiert mit den leitenden Prinzipien die grundlegenden Vorgaben im Umgang mit Daten um die erforderliche Basis zum Aufbau einer datenorientierten Unternehmenskultur zu schaffen.

Mit den strategischen Handlungsfeldern wird durch die Datenstrategie ein priorisierter Maßnahmenkatalog festgelegt, um die Fähigkeit zur zielgerichteten Planung und Steuerung der „Domäne Daten" im Kontext der Digitalisierung und Nutzbarmachung von Daten sicherzustellen. Eine erfolgreiche Umsetzung der Datenstrategie im Ressort erfordert darüber hinaus die Sicherstellung begleitender Rahmenbedingungen, welche in Form kritischer Erfolgsfaktoren definiert wurden.

Strategie zur Künstliche Intelligenz im Ressort

Künstliche Intelligenz (KI) ist ein vielschichtiges Thema, welches sich sowohl als Realität als auch als Hype darstellt. Sie durchdringt bereits heute zahlreiche Bereiche des menschlichen Lebens und hat das Potenzial, Alltag und Arbeitswelt zu revolutionieren. KI ist eine transformative Kraft, welche die Art und Weise, wie Aufgaben wahrgenommen werden, insbesondere wie im militärischen Einsatz Wirkungen erzielt werden, grundlegend verändern wird.

Das Anwendungsgebiet von KI umfasst als Technologiegruppe potentiell viele inhaltliche Leistungsbereiche. Der Einsatz von KI im Ressort bedarf der Koordinierung inhaltlicher Aspekte mit Digitalisierungsaspekten sowie die Berücksichtigung ergänzender Vorgaben wie beispielsweise die Datenqualität oder Validierung der Informationen.Es ist zu erwarten, dass KI zunehmend zur Optimierung der Effektivität (Wirksamkeit; Wirkung) und der Effizienz bei der Wahrnehmung vielfältiger Aufgabenstellungen beitragen wird. Somit wird der Einsatz von KI für die Erreichung militärischer Vorteile sowie für die Effizienz und Effektivität von Prozessen zur Wahrnehmung von Aufgaben des Ressorts notwendig werden.

Die Implementierung von KI im Ressort stellt kein IKT-Projekt im eingeschränkten Sinne dar, sondern muss als Organisationsprojekt zwischen zentraler Steuerung und dezentraler Umsetzung im Schnittfeld von prozessorientierten, organisationsorientierten und menschenorientierten Betrachtungsweisen verstanden werden.

Integration und Nutzung von KI bedingen komplexe Prozesse, die eine ganzheitliche Herangehensweise erfordern. Ein strukturierter Planungsprozess zu KI-Projekten muss unter anderem Verfügbarkeit und Qualität der für die beabsichtigte Funktionalität notwendigen Daten, die Gewährleistung der Datensicherheit sowie die erforderliche IKT-Infrastruktur sicherstellen. KI-Systeme müssen nahtlos in die vorhandenen IT-Infrastrukturen und Prozesse integriert werden können.

Die nun fertiggestellte KI-Strategie schließt inhaltlich am Grundlagenpapier zu KI der GDVPol an. Auf strategischer Ebene verfolgt das Ressort folgende Ziele:

- Ziel 1: Das Ressort verankert KI strategisch und wird zu einer AI-ready Organisation, die KI auf allen Ebenen und in allen Leistungsbereichen nutzt.

- Ziel 2: Das Ressort verfolgt einen partnerschaftlichen Zugang zu verantwortungsvoller Nutzung von KI.

Mit der KI-Strategie wurde der Themenbereich breit erfasst und ein Zielbild für das Ressort definiert. Über definierte Handlungsfelder wurden strategische Leitlinien in den Domänen Organisation, Mensch, Kultur und Technologie sowie für unterstützende Bereiche (z.B. Forschung, Innovation) definiert.

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Bundesministerium für Landesverteidigung

IKTCyber-Plan & IKTCyber-Bereitstellung

Leiter: Oberst des Generalstabsdienstes Mag. Christof Tatschl

Hervorzuhebende Aktivitäten

Fähigkeitsentwicklung

Experten im Militär – die Wissensachse zwischen Zivilgesellschaft und Militär

Mittlerweile verstärken 68 Experten im Militär als Milizsoldaten die Fachbereiche der Direktion 6 - IKT&Cyber. Diese Experten setzen sich aus unterschiedlichsten zivilen Wissensbereichen zusammen und sind beim ÖBH fachlich den Bereichen „IKT&CySih&InfoSih", „IKTRiskMngt", „IKT", „Infomngt&WM" und den „GeoWiss" zugeteilt.

Leitstelle ist die Abt IKTCyPl. Für die Expertenbereiche „Radartechnik" und „Radarbetriebsdienst" ist Dion6/FüAbt/Ausb&Miliz Leitstelle. Diese planen, steuern, koordinieren die Experten und verwaltet diese mit Unterstützung des MilKdo WIEN hinsichtlich der Mobilmachungsverantwortung. Die Experten bringen ein hohes Maß an zivilem Wissen ins Militär ein, können sich dort aber auch weiterbilden und netzwerken. 2023 war ein sehr aktives Jahr, hier einige Beispiele.

IKT-Sicherheitskonferenz am 03. und 04. Oktober im Design Center Linz

Aus zarten Anfängen mit einigen Dutzend Teilnehmern hat sich die IKT-Sicherheitskonferenz zur größten Fachkonferenz für IKT-Sicherheit in Österreich entwickelt. Tausende Teilnehmer, Vortragende und Aussteller sowohl aus dem militärischen als auch aus dem zivilen Bereich nutzten die zwei Tage für hochkarätige Vorträge, Fachdiskussionen und die Präsentation neuer Technologien. Begleitet wurde das Ganze durch das Finale der Austrian Cyber Security Challenge und das Halbjahrestreffen der Cybersicherheitsplattform.

Damit war die Konferenz auch ein Pflichttermin für die Experten „IKT und Cyber" des Österreichischen Bundesheeres. Diese fungieren als Bindeglied zwischen militärischer Cyber-Abwehr und ziviler Cyber-Sicherheit.

Cyber Defence und Cyber Security erfordern rasches und effektives Handeln. Dafür sind sowohl entsprechendes Domänenwissen als auch funktionierende Netzwerke erforderlich, um schnell auf unterschiedliche Herausforderungen reagieren und auf verteilte Expertisen zugreifen zu können.

Neben der Teilnahme an den offiziellen Veranstaltungen - sowohl als Zuhörer als auch als Vortragende - nutzten die Experten vor allem auch die Möglichkeit des informellen Informationsaustausches mit anderen Konferenzteilnehmern. Die dabei gewonnenen Erfahrungen werden sowohl im zivilen Beruf als auch im Rahmen ihrer militärischen Funktionen genutzt.

Aus Linz berichtete der Cybermilizexperte (Technologie- und Datenmanagement, Cybersicherheit) Mjr OR Mag. (FH) Christian Zec, MSc.

Wortmeldungen von Experten die bei der IKT-Sicherheitskonferenz 2023 teilgenommen haben:
„Die IKT-Sicherheitskonferenz ist DAS Who-is-Who der österreichischen Cybersecurity-Community. Brandaktuelle und Weltklasse Vorträge, interessante Aussteller und viel Gelegenheit sich zu vernetzen. Ein Fixpunkt für alle, denen IT-Sicherheit nicht egal ist." so der Experte für Cybersicherheit Thomas Steinbrenner, MSc.

„Ich fand die IKT-Sicherheitskonferenz sehr gut organisiert. Auch die Professionalität der Vorträge war bemerkenswert. Wie man an den fast 4000 Teilnehmern sah, gehört die Konferenz zu einer der größten und wichtigsten im DACH-Raum. Ich bin 2024 gerne wieder dabei," so der Experte DI Herbert Mühlburger.

FOTO KK, Experten bei der IKT-Sicherheitskonferenz 2023 in Linz.

Teilnahme an internationalen IT- und Sicherheitskonferenzen

IT-SECX an der FH St.Pölten

FOTO KK, FH-Prof, Dr. Wagner

Der Experte FH-Prof. Dr. Markus Wagner, MSc (designierter Leiter des neuen Josef Ressel Zentrums) lud zur ITSecX Konferenz an der FH St. Pölten. Die IT-SECX (https://itsecx.fhstp.ac.at/) ist eine Plattform für den Austausch von Wissen über IT-Sicherheit, einschließlich aktueller Trends, Technologien und neuester Entwicklungen.

Dabei stellen Experten Forschungsprojekte, Praxisberichte und Best Practices vor, wobei auch mögliche Forschungskooperationen besprochen werden.

Die Teilnahme an dieser Veranstaltung für die militärischen Experten der IKTCyPl sowie weitere interessierte Teile des ÖBH (FüUS, LVAk) wurde durch FH-Prof. Dr. Markus Wagner, ebenfalls IKT-Experte der Direktion 6 - IKT&Cyber, ermöglicht.

CIMIC Konferenz der LVAk 2023

FOTO KK, ObstltdhmfD Mag. Cerne, MBA

Im September 2023 fand die Civil-Military Relations Konferenz „Security through Unity: Europe's Challenges after Ukraine Crisis" – ein Kooperationsprojekt der LVAk mit dem St. Georgs-Orden, statt. Unser Experte, ObstltdhmfD Mag. Cerne, MBA, war bei dieser Konferenz Co-Host, Vortragender und Moderator.

Hauptziel der dreitägigen Konferenz war es, die Herausforderungen, vor denen Europa heute steht zu diskutieren und Wege zu finden, welche Einheit und Sicherheit für die Zukunft gewährleisten. Namhafte Vertreter aus Politik, Militär und Zivilgesellschaft hielten dazu inspirierende Vorträge und präsentierten ihre Forschungsergebnisse.

Zentrale Themen waren eine strategische Kommunikation in Zeiten der Desinformation sowie die Notwendigkeit einer effektiven Planung als Reaktion auf hybride Bedrohungen.

Aus- und Weiterbildung

IKT&Cyber Militär Experten

Im herausfordernden Jahr 2023 kam auch die Ausbildung unserer Experten nicht zu kurz.

Mehr als 20 Experten absolvierten diverse Ausbildungsgänge an der LVAk zum Oberleutnant des Expertendienstes, sowie an der TherMilAk im Rahmen der Militärexpertenbasisausbildung.

Grafik Darstellung der Cyberfähigkeiten

Einige Kameraden haben auch die sogenannte „Grundschulung IT Services" für das Arbeiten mit dem ELAK erfolgreich absolviert.

Ausblick - die Experten-Koordinationsgruppe bestehend aus den Kameraden Cerne, Mühlburger, Wagner und Zec planen bereits gemeinsam mit der Leitstelle IKTCyPl erste Schritte für die BWÜ 2024 und das Jahresprogramm 2024.

Fachspezifische Mitarbeit

Die Experten im Militär leisten ihren Beitrag auch im Rahmen von Zuarbeiten zu fachspezifische Themen wie zum Beispiel KI oder inhaltliche Entwicklung des BaStG an der TherMilAk „Mil-IKTFü".

So wurde mit mehreren Kameraden in verschiedenen Themenfeldern an der innovativen und nachhaltigen KI-Strategie des Ressorts gearbeitet. Dabei wurden auch mögliche Kooperationen mit dem Ökosystem "Innovative Start-Ups" und angewandten Forschungseinrichtungen erörtert.

Fähigkeitsentwicklung Cyber

„Die militärische Landesverteidigung im Cyberraum ist als Teil der Umfassenden Landesverteidigung und somit der gesamtstaatlichen Sicherheitsvorsorge Aufgabe des Bundesheeres. Die Cyberverteidigung ist ein gesamtstaatlicher Prozess unter der Federführung des BMLV und umfasst daher alle Maßnahmen zur Vorbereitung, Aufrechterhaltung und Wiederherstellung der Handlungsfähigkeit im Rahmen einer souveränitätsgefährdenden bzw. -verletzenden Handlung."

Wiewohl Grundlagen zur Entwicklung der Waffengattung Cyber-Truppe, die in der Cyber-Verteidigung eine Hauptrolle spielt, bereits seit mehreren Jahren vorliegen, konnten nunmehr auch die Inhalte der 2021 verfügten Österreichischen Strategie für Cyber-Sicherheit (ÖSCS) berücksichtigt werden. Hier wurden die nationalen Grundlagen geschaffen, dass militärische Fähigkeiten in einen gesamtstaatlichen Ansatz der Republik als Beitrag zur umfassenden Landesverteidigung vorzuhalten sind.

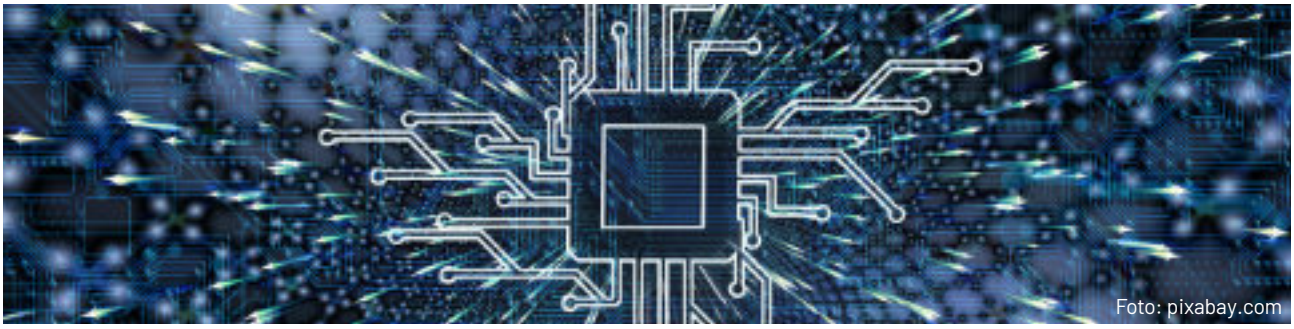


Foto: pixabay.com

Dazu verlangt es rechtliche Rahmenbedingungen, in welchen der Prozess mitsamt den Verantwortlichkeiten und des Zusammenwirkens der jeweiligen Ressorts definiert werden muss. Militärische Landesverteidigung im Cyberraum gem. § 2 Abs. 1 lit. a des Wehrgesetzes 2001 (WG 2001) a ist primär die Nutzung des Cyber-Raumes für militärische Zwecke. Maßnahmen zur Vorbereitung, Aufrechterhaltung und Wiederherstellung der Handlungsfähigkeit im Rahmen von souveränitätsgefährdenden bzw. verletzenden Handlungen im Cyber-Raum außerhalb von Netzen des BMLV gehen über die Kompetenzen des Ressorts hinaus. Eine Zuordnung von konkreten Schutzobjekten der kritischen Infrastruktur an das BMLV und ÖBH bedingt Vorgaben durch das Gremium des Cyber-Koordinationsausschusses.

Unter Berücksichtigung der aktuellen weltpolitischen Lage (Stichwort UKRAINE Krieg 2022) müssen rasch Festlegungen auf militärstrategischer Ebene getroffen werden, die es ermöglichen eine planungsstabile Fähigkeitsentwicklung der Cyber-Truppe vorzunehmen. Der Anlassfall der militärischen Cyber-Verteidigung spielt hier eine bedeutende Rolle, weil nur nach Schaffen der konzeptiven Grundlagen der Bedarf an Fähigkeitsträgern eindeutig abgeleitet und konkretisiert werden kann.

Diese Richtlinie soll zu einer raschen und nachhaltigen Streitkräfteentwicklung der Waffengattung Cyber-Truppe beitragen. Die IKT-Truppe sowie die EloKa-Truppe werden in diesem Dokument nicht explizit angesprochen.

Die Richtlinie soll zu einer weiteren Konkretisierung der Ausgestaltung des gesamtstaatlichen Ansatzes der Republik Österreich beitragen. Die Ausplanung von Strukturen der Cyber-Truppe zur Aufstellung konkreter Fähigkeiten soll auf Grundlage der strategischen Ausrichtung dieses Dokuments erfolgen.

Fähigkeitsentwicklung IT-Sicherheit

2023 wurden Schwergewichtsmäßig die Themen Data Centric Security und Zero Trust in verschiedensten Arbeitsgruppen, sowohl national als auch international, behandelt.

Bei den Federated Mission Networking Multinational CIS Security Management Authority Meetings in Kopenhagen, Canada und Lissabon wurde neben den Leitungsaufgaben (Syndicate 1) Probleme zwischen Federated Mission Networking Policy und dem Data Centric Security Implementierungsplan der NATO behandelt. In Zusammenarbeit mit Syndicate 3 wurden auch erste Analysen für Zero Trust Architekturen durchgeführt.


Foto: pixabay.com

Im Rahmen der DACH Arbeitsgruppe Digitalisierung wurden innerhalb des Fähigkeitsclusters IKT-Sicherheit erste Analyseergebnisse zum Thema Data Centric Security und Zero Trust ausgetauscht. Nachdem der Fähigkeitscluster IKT-Sicherheit beauftragt wurde, eine Lösung für die fehlende Kollaborationsmöglichkeit für Inhalte mit der Klassifizierunsstufe Restricted zu finden, wurde ein Zeitplan und Möglichkeiten für eine DACH Restriced VTC bearbeitet.

Ein Weiteres Thema des Fähigkeitsclusters IKT-Sicherheit war die Bearbeitung der SOC-Prozesse für die Common Roof 2024.

Im Rahmen der Arbeitsgruppe Digitalisierung des BMLV wurde bei der Fertigstellung des IKT-Grundsatzerlasses mitgewirkt. Hauptbearbeitung war ein Beitrag zur IKT-Sicherheitsarchitektur.

Foto: pixabay.com

Zusammen mit Vertretern der Bereiche Technik, Applikation und Sicherheit wurde eine Arbeitsgruppe zur Erstellung eines Analyseberichts für Data Centric Security und Zero Trust gegründet.

Mit 2024 soll ein erster Analysebericht mit Handlungsfeldern und Maßnahmenkatalog für die Transformation zu einer DCS/ZT Architektur erstellt werden.

Nach Verfügung der Vorhabensabsicht wurde die Implementierung zusammen mit Technik, Applikationen, IKT-Sicherheit und IKTS begleitet. Derzeit befinden sich Systeme für eine Testung in Beschaffung sowie technische Absprachen.

Im Rahmen des IKTSysÖBH 2032 wurde der Referent als Verantwortlicher für den Bereich Planungsnetz (aka militärisches Hochsicherheitsnetz – milHSN) eingeteilt. Erste Beurteilungen wurden 2023 bereits abgeschlossen.

Internationale Fähigkeitsentwicklung

Die „Multinational Capability Development Campaign" (MCDC) ist ein multinationales Konzept- und Fähigkeitsentwicklungsprogramm mit dem Zweck, gemeinsam nicht-materielle Lösungen zur Schließung von Fähigkeitslücken für multinationale Einsätze für zukünftige Einsatzanforderungen zu erarbeiten.
Durch die Identifizierung bestehender Fähigkeitslücken und der Erarbeitung möglicher Lösungen, leistet MCDC einen wichtigen Beitrag für die Interoperabilität und die nationale Streitkräfteentwicklung. Bei MCDC sind dzt. 23 Nationen und zwei Organisationen vertreten.

Foto: Bundesheer/Dion6

Logo MCDC

Initiator sind die USA, diese stellen auch das Sekretariat und den Vorsitz, Österreich ist seit 2007 Mitglied.

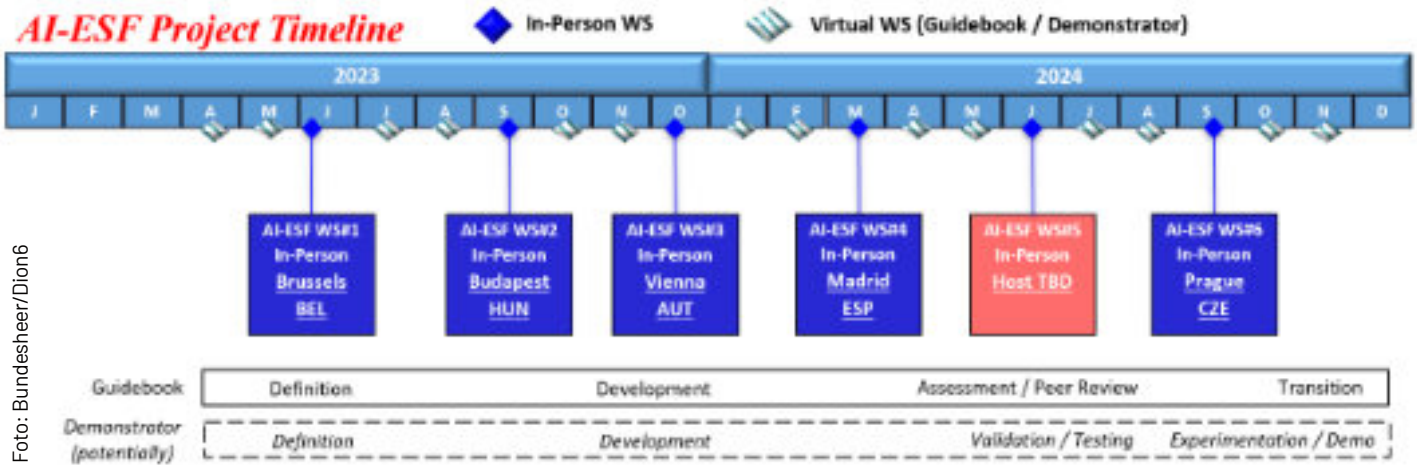


Foto: Bundesheer/Dion6

AI-ESF Project Timeline

Eine Teilnahme an einem MCDC-Projekt kann entweder als „Contributor" (aktive Mitwirkung, wird grundsätzlich gewünscht), als „Observer" (Beobachter, keine aktive Mitwirkung, somit Zugriff nur auf das Endprodukt eines Projektes) oder im Zuge der Projektleitung (PL) erfolgen. Die Teilnahme an mindestens einem Projekt als „Contributor" ist erforderlich, um auch auf andere MCDC-Produkte zugreifen und diese national verwerten zu können.

Im Bereich der Arbeits- und Koordinierungsebene ist AUT, respektive das ÖBH, durch einen „National Director" (ND) vertreten (derzeit Obst Schluyok, MA/MilStrat). Die Entscheidungsebene erfolgt durch Mitglieder der „Executive Steering Group" (ESG; Ebene Brigadier/Generalmajor oder zivil entsprechend; Vorsitz: stvJ7/JS/US; derzeitiger Vertreter des ÖBH: AL MilStrat). AUT beteiligt sich am AI-ESF Projekt als „Contributor".

Die AI-ESF Workshop-Serie (in Summe insgesamt sechs „in-person-workshops" finden ca. alle drei- bis vier Monate statt, zusätzlich pro Monat ein virtuelles Treffen) hat zum Ziel, dass das Kernprojektteam (NATO/SACT), die Mitwirkenden, Beobachter und Fachexperten aus den teilnehmenden Nationen gemeinsam Lösungen entwickeln, die Ergebnisse (d.h. die Endprodukte gem. „Project-Plan") anschließend einem „Peer Review-Prozess" unterziehen und diese ggf. im Rahmen eines Confirmation Events validieren. Die Endprodukte der AI-ESF WG - ein „Guidebook" - und falls realisierbar ein „Demonstrator" - sind Anfang 2025 zu erwarten.

"Sensor fusion is the process of combining sensor data or data derived from disparate sources such that the resulting information has better accuracy and less uncertainty than would be possible when these sources were used individually."

Zur Erlangung der (Informations-)Überlegenheit am Gefechtsfeld ist die Fusion von (multinationalen) Sensordaten (zB Radardaten, EloKa, SIGINT, Geodaten, Bild- und Tondateien etc.) von unterschiedlichsten Plattformen (zB Schiff, LFz, gepanzerten Fzg usw.) und Domänen in ein gemeinsames Lagebild, Meldeformat oder dgl. erforderlich (der multinationale Aspekt ist dabei wesentlich!).

Foto: Bundesheer/Dion6

Das - sowie die Auswertung der Daten - soll unter Einsatz von „Künstlicher Intelligenz" (KI) erfolgen, damit relevante Information in der notwendigen Geschwindigkeit aufbereitet und den Entscheidungsträgern nahezu in Echtzeit zur Verfügung gestellt werden können.

Diesbezüglich wurden beim MCDC AI-ESF WS#3 in Wien durch den Ltr IMG/Dion6, Bgdr Dr. Teichmann, im Rahmen eines hochinteressanten Vortrages folgende drei use cases vorgestellt, die bei der weiteren Bearbeitung des Guidebooks berücksichtigt werden:

- **Ground based mobile Recce („military Google street car"):** 360o overlapping videos, IR, LIDAR, Laser and UAV, etc
- **Situational Awareness „waterways":** AIS, GPS/GNSS-signals, Radio-Comms, OS (social media), harbor and shipping lanes IS, videos, etc.
- **Recognized Environmental Picture (REP):** OS GIS data (e.g. OSM), Open GeoData, Sat-Images, UAV and OS (social media), etc.

Welcher Nutzen ergibt sich durch die Teilnahme am Projekt für das ÖBH bzw. BMLV ?

Die Teilnahme des BMLV/ÖBH an der MCDC-Initiative sowie am AI-ESF-Projekt bringt :

- Ideengewinn („insight") für die Ausarbeitung der nationalen KI-Strategie
- Wissenserwerb zum Themenbereich „Sensor-Fusion und AI"
- Wissenserwerb bezüglich Einführung neuer Technologien und die Verarbeitung großer Mengen von Daten unterschiedlichster Sensoren

Die Mitarbeit von AUT im MCDC-Projekt AI-ESF ist von großem Nutzen (i.a. für die Grundlagenarbeit im Themenbereich „AI/KI", Einbringung von Erkenntnissen und Aspekten in die KI-Strategie des Ressorts, Vernetzung mit Wissensträgern, Wissensgewinn, Wissenstransfer, für die Nutzung und Weiterentwicklung von Produkten aus Forschungsprojekten usw.).

MCDC 2023-2024 Workshop

In Österreich weisen u.a. die FORTE bzw. KIRAS-Projekte „PIONEER", „HYBRIS" und „BOOST" AI/KI sowie Sensor-Fusion-Bezug auf.

Die Teilnehmer des BMLV konnten sich bei den bisherigen Meetings aufgrund von Fachwissen in den Bereichen Computerlinguistik, Terminologie, Wissens- und Change-Management sowie praktischer Erfahrung im Projektmanagement (PM) als Beitragsnation sehr gut einbringen. Eine Teilnahme von weiteren AUT-Vertretern (zB aus dem zivilen, technischen, akademischen und/oder militärischen Bereich) im Bearbeitungszyklus ist möglich und ob der Themenlage auch durchaus zweckmäßig (zB für Beiträge im Rahmen der Kapitelbearbeitung „Policy & Responsible Use", im Themenbereiches „Technology Overview" , zB bei den Subkapiteln „AI", „Sensorfusion" etc.).

Brig Mag. Dr. Teichmann MAS, MSc beim MCDC 2023-2024 Workshop

Fähigkeitsentwicklung internationale Übungen

Die jährliche Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise ist die größte Interoperabilitätsübung der NATO und deren Partner.

Vom 5. bis 23.06.2023 testeten am NATO Joint Force Training Center (JFTC) in Bydgoszcz/Polen, am Airfiel der polnischen Luftwaffe in Bydgoszcz und in mehreren weltweit verteilten sogenannten Battle Labs fast 2000 Soldaten und Ingenieure aus 43 Nationen und NATO Organisationen mehr als 400 militärische Informations- und Kommunikationssysteme im multinationalen Verbund.

Das Spektrum der ingesamt mehr als 20000 Testfälle reichte von Experimenten mit neuen Technologien und Schnittstellenspezifikationen (exploration), über die Erprobung und Prüfung neuer Systeme (experimentation bzw. examination) bis zur Übung mit eingeführten Systemen in einem einsatznahen Umfeld unter Abstützung auf die Federated Mission Networking (FMN Richtlinien (exercise).

Lag noch vor wenigen Jahren das Schwergewicht der getesteten Systeme (bzw. "Capabilities", wie sie bei CWIX genannt werden, weil nicht das technische System an sich, sondern die im Zusammenspiel realisierte Fähigkeit im Vordergrund steht) auf Führungsinformationssystemen im weitesten Sinne, so wurde heuer bereits die gesamte IKT-Landschaft moderner Streitkräfte abgedeckt: Netzwerke und Kommunikationssysteme, Battlefield Management Systeme, Waffeneinsatzsysteme, Aufklärungssysteme, Elektronische Kampfführung, Cyber Defence etc.

Der Fokus der österreichischen Teilnahme lag heuer auf der Vorbereitung der Zertifizierung von IKT-Services des Bundesheeres im Rahmen von FMN (Federated Mission Networking), das seit vielen Jahren das Leitprogramm für die Zusammenarbeitsfähigkeit der NATO und ihrer Partner aber auch zwischen Domänen und Waffengattungen für Joint- und Multi Domain Operations ist. Die Teilnahme erfolgte durch ein Core Team vorort am JFTC und einem Team von Experten und Testern im AUT Battle Lab im Objekt 6. Als Nebenaufgabe galt es Informationen und Erkenntnisse für die nationale Fähigkeitenentwicklung insbesondere im Bereich JISR zu gewinnen. Zu diesem Zweck war ein Experte der Abteilung für einsatzorientierte Applikationen eine Woche vorort.

Alle festgelegten Ziele wurden erreicht!

AUT CWIX Core Team und Besucher vorort am NATO JFTC

Veränderungsdienst IT-Materialstruktur

Als eine Konsequenz der laufenden „Reorganisation der ZentrSt des BMLV und der Oberen Führung des ÖBH" kam es 2023 zu einem erhöhten Aufkommen von neu verfügten OrgPlänen und dadurch zu einem erhöhten Bedarf von Anpassungen der IT-MatStrukt. Dieser Trend wird sich 2024 noch einmal verstärken, da dann die OrgPläne der Dion 1,2 und 7 in Kraft treten werden und voraussichtlich auch noch die restlichen OrgPläne der Dion 3 - 6 verfügt werden.

Im Zuge der Einschulung von Obst Löscher in die IT-MatStrukt wurde der dringende Bedarf an einer Überarbeitung („Digitalisierung") der bisherigen „IT-MatStrukt-Tabelle" erkannt und bereits im April 2023 eine erste Besprechung mit Technikern der AppI sowie Vertretern StruktPI und Org einberufen. Nach mehreren Bearbeitungsrunden und Koordinierungsbesprechungen konnte am 20.12. durch AppI ein erster Prototyp der neuen, digitalen IT-Materialstruktur präsentiert und an IKTCyPI übergeben werden. Die Produktivsetzung ist mit 1.Quartal 2024 avisiert.
Der große Mehrwert dabei ist, dass im Zuge von Berechtigungsmanagement nun die Verbände direkt und jederzeit ihre Strukturen einsehen können und damit Transparenz und Planungssicherheit geschaffen wurde.

WLAN Ausstattung Dion 7

Nachdem Dion 7 die Prüfung und ggf. schrittweise Realisierung einer Verdichtung der WLAN Ausstattung (Bereitstellung von „offenem WLAN") bei allen Wohnheimen und Seminarzentren beantragt hat, wurde Dion 6 um weitere Veranlassung ersucht. IKTCyPI hat daraufhin im September 2023 eine erste Besprechung unter Mitwirkung von Dion 7, IKTS, Dion6/IKTCyE und Dion6/IKTBetr durchgeführt und so die Grundlage für alle weitere Bearbeitungen gelegt.

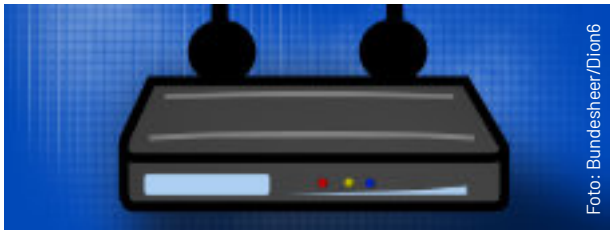


Foto: Bundesheer/Dion6

Dabei hat sich für IKTCyPI der Bedarf an einem eigenem „WLAN Konzept ÖBH" klar gezeigt und dies wird eine weitere Hauptaufgabe des Referats 4 im Jahr 2024 darstellen. Der Bedarf ist allgegenwärtig und betrifft eigene Bedienstete als auch Gäste des Ressorts.

Smartphonekonzept ÖBH

Die durch den Direktor 6 beauftragte Erstellung eines neuen „Smartphonekonzepts ÖBH" wurde im 2. Halbjahr eingeleitet und nach umfangreicher Grundlagenarbeit im November 2023 eine erste Besprechung mit Vertretern IKTTe, IKTBetr, IKTCyE sowie IKTS und LogFü&Trsp durchgeführt. Neben der gemeinsamen Erarbeitung von insgesamt 4 Varianten konnten grundsätzliche Fragen zu den Themenbereichen Technik, Kosten und logistische Maßnahmen erörtert werden. In Abhängigkeit der noch zu verfügenden OrgPläne stellt dieses Projekt eine weitere Hauptaufgabe für das Jahr 2024 dar.

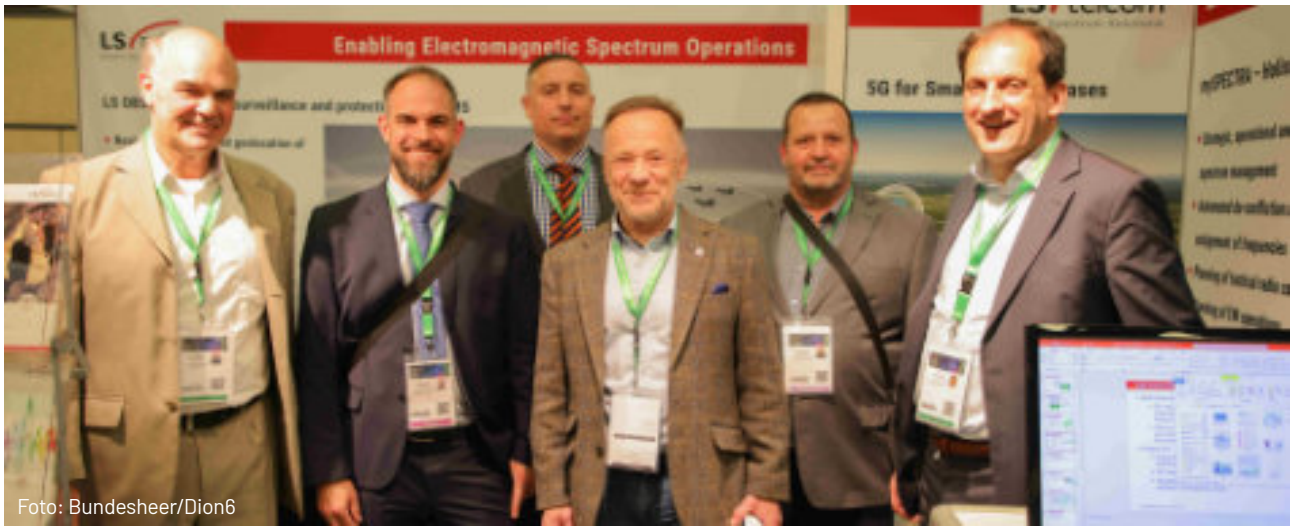


Foto: Bundesheer/Dion6

Mai 2023 – Teilnahme an der AOC Europe Conference&Exhibition in Bonn

IKTCyber-Einsatz
Leiter: Brigadier Mag. Arnold Staudacher

Hervorzuhebende Aktivitäten

Auf das abgelaufene Jahr 2023 zurückblickend, fällt es mir aufgrund der umfangreichen Vorhaben und Projekte, die im Bereich IKTCyE durchgeführt wurden, schwer, im engen Rahmen dieses Berichts nur wenige Highlights hervorzuheben. Die hier dargestellten „Highlights" sind insbesondere unter dem Gesichtspunkt von wesentlichen Weiterentwicklungsschritten, Meilensteinen oder wichtigen Einsatzleistungen der Cyberkräfte und natürlich aus persönlicher Einschätzung entstanden. So möchte ich ganz zu Beginn mit unserer Hauptaufgabe beginnen, nämlich mit der Sicherstellung der Einsätze des ÖBH im In- und Ausland.

Einsatzleistung 2023

Im Inlandseinsatz unterstützten die beiden FüUB1 und 2 mit jeweils 1 Assistenzkompanie die Polizei bei der Bewältigung der Migrationskrise an der südlichen Staatsgrenze in Kärnten. Die Kompanien waren insgesamt 6 Monate vom April bis Ende September im Einsatz und erbrachten somit 50% der Einsatzleistung im Jahr 2023 im Befehlsbereich des MilKdo Kärnten - und das zur vollsten Zufriedenheit der vorgesetzten Dienststellen und der sicherheitspolizeilichen Behörden.

Im Ausland leisteten auch in diesem Jahr wieder zahlreiche Soldatinnen und Soldaten der Direktion 6 - IKT&Cyber ihren Beitrag. Durchschnittlich waren ca. 40 Bedienstete der Cyberkräfte permanent in einem Auslandseinsatz, die Masse als IKT- und S6 Fachpersonal sowie im Bereich MilGeo eingesetzt. Als besonderes Highlight ist dabei die Neuerrichtung der Heimatfunkverbindung zum österreichischen Kontingent UNIFIL auf Basis der neuen Kurzwellenfunkgeräte zu erwähnen. Diese hat eine neue Ära im Kurzwellenfunk des ÖBH mit einem der modernsten und zuverlässigsten Geräte weltweit eingeläutet und das gerade rechtzeitig vor dem nur wenige Wochen später beginnenden Gazakrieg. Bei der Mission KFOR führte die angespannte Lage dazu, dass seit August erstmals 2 CREW Systeme zum Schutz der AUT EOD Truppe zum Einsatz gebracht werden.

Foto: BMLV / HBF

Bei sehr kurzen Vorbereitungs- und Vorlaufzeiten war das UZ EloKa damit konfrontiert, mit relativ geringen Einsatzgrundlagen für eine optimale Konfiguration der Systeme auf einen konkreten Einsatz bezogen (Nutzerforderung, Bedrohungsdatenbanken etc.) zu sorgen. Letztendlich konnten die Zeitvorgaben durch die Zusammenarbeit aller Beteiligten der EloKa Truppe (vor allem EloKaKp/FüUB2, UZ EloKa/MilCyZ) und AUTCON KFOR eingehalten werden und dieser Ersteinsatz der CREW Systeme im Ausland als wesentlicher Meilenstein erfolgreich realisiert werden.

Übungsvorhaben – Fähigkeitserhalt und –entwicklung IKT und Führungsunterstützung

In dieser Kategorie sind insbesondere 4 wesentliche Vorhaben zu erwähnen. Im Bereich der Notkommunikation wurden 2 österreichweite Übungen auf Basis eines Blackout Szenarios im Juni und im September 2023 durchgeführt.

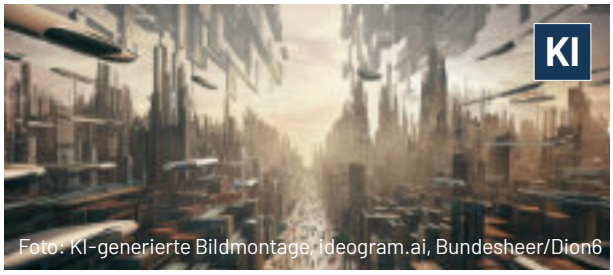
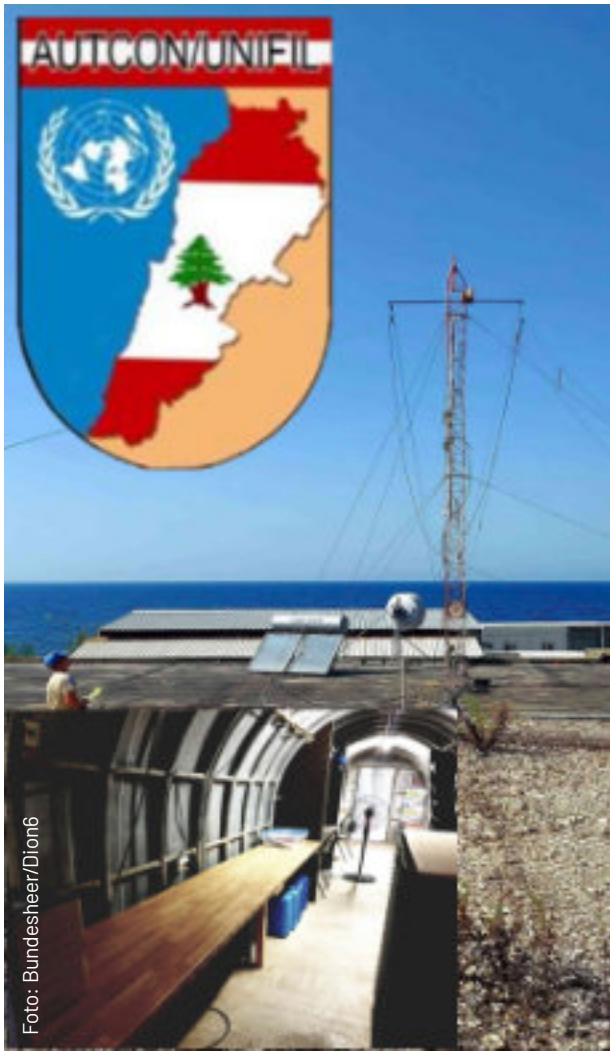


Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6



Taktische Breitband DiPol KW-Antenne, Gerätestandort Shelter,AUTCON UNIFIL

Dabei wurde an 4 Tagen mit 30 bzw. 38 Funkstellen österreichweit unter der Leitung IKTCyE aus der Schwarzenbergkaserne in WALS der Notkommunikationsbetrieb auf Basis einer Datenfunksoftware und Sprechfunk geübt. Während dieser Übungen konnten wesentliche Fortschritte in den Bereichen der Netzkonzeption, der Übungsleitung (Struktur, Leitfunkstelle, Einlagensteuerung und Übungsauswertung) und hinsichtlich der Einsatzbereitschaft der Funktrupps erzielt werden.

Nach nunmehr 3 Übungen dieser Art ist ein Fähigkeitszustand erreicht, welcher als wesentlicher Zwischenschritt und Meilenstein auf dem Weg zum Bundesheer 2032 bezeichnet werden kann. Es bleibt jedoch noch viel zu tun.

Im Oktober 2023 fand unter ff FüUB1 die trinationale D-A-CH FMN Betriebsübung „Common Roof 23" statt.

Nachdem das FüUB1 in diesem Bereich bereits 2022 erste Übungserfahrungen sammeln konnte, wurde in diesem Jahr ein weiterer Meilenstein erreicht, weil nunmehr nicht nur die Teilnahme mit einem nationalen „Subordinate Service Management and Control Operations Element" (SSE) sicherzustellen war, sondern gleichzeitig aus dem Standort Villach über das multinational besetzte „Centralized Service Management and Control Operations Element" (CSE) auch die Gesamtübungsleitung übernommen wurde.

Die sehr zeitaufwändige Übung mit umfangreichen Vorbereitungskonferenzen und –workshops sowie mit einer arbeitsintensiven technischen Instantiierung im Vorlauf an die 3-wöchige Übung bot dem FüUB1 und vielen anderen IKT/ FüU Fachleuten die Möglichkeit, sich mit Partnern auszutauschen, multinational entwickelte FMN Prozesse zu üben und zu validieren und sich auf zukünftige Aufgaben vorzubereiten.

Dies ist sowohl dem FüUB1 als auch den vielen Mitwirkenden der „IKT Community" sehr gut gelungen.

Nach über 10 jähriger Pause konnte das FüUB2 ganz im Sinne von „Mission Vorwärts" endlich wieder den geschlossenen Bataillonseinsatz – zumindest mit Bataillonsstab, einer FüUKp und mit der EloKaKp im Rahmen der Übung „Steinfeld" der TherMilAk üben. Ausgehend von der Übungsleitung an der TherMilAk in Wr. Neustadt wurden die Verbindungen zu den übenden Truppen zur vollsten Zufriedenheit sichergestellt.

Mit der EloKaKp konnten wertvolle Erfahrungen beim Einsatz der neuen Erfassungs- und Ortungssysteme gewonnen werden.


Foto: pixabay.com


Foto: Bundesheer/Dion6

Elektronischer Störeinsatz gegenüber Mini Drohnen, Übung „Alpine Jam", TüPl Hochfilzen

Die Ausbildung des Personals am neuen Tactical Communication Network (TCN), das zu den modernsten Systemen Europas gehört, unter ff FüUS sowie die Auslieferung der Geräte an die Truppe waren eine wesentliche Herausforderung in diesem Jahr, die durch die IKT Truppe des ÖBH erfolgreich bewältigt wurde.

Unter ff IKTCyE und in enger Abstimmung mit der IKTS, der Dion 4, dem IKT&CySihZ sowie mit der Truppe wurde der phasenweise Gerätezulauf sichergestellt und die betrieblichen Einsatzgrundlagen und Richtlinien erstellt.

Im November konnten schließlich die ersten IKT Betriebsübungen durch die 4. PzGrenBrig und durch die LRÜ unter Mitwirkung durch die FüUBs mit dem neuen verlegbaren IKT System TCN durchgeführt werden. Bei diesen Übungen wurden Schwachstellen und Kinderkrankheiten erkannt bzw. beseitigt und so die Voraussetzungen für den Ersteinsatz bei der Luftraumsicherungsoperation „Daedalus 24" Anfang 2024 geschaffen.


Foto: pixabay.com

Fähigkeitserhalt und –entwicklung Elektronischer Kampf & Cyber

Im Fachbereich EloKa wurden neben dem erstmaligen Einsatz von CREW Systemen im Ausland wesentliche Fortschritte beim Einsatz der Erfassungs- und Ortungssysteme erzielt und fanden mit dem Zulauf des zweiten Seriensystems im November 2023 vorerst einen Abschluss.

Die neuen Systeme zur Überwachung und Peilung im elektromagnetischen Spektrum kamen gleich bei mehreren Übungen, u.a. bei der Übung „Steinfeld" und bei der trinationalen D-A-CH Übung „Alpine Jam 23" am TüPl in Hochfilzen zum Einsatz. Es konnten wertvolle Erfahrungen für die Fähigkeitsentwicklung gewonnen werden.

Einen wesentlichen Meilenstein konnte auch das MilCyZ mit der Teilnahme an der diesjährigen Cyberverteidigungsübung „Locked Shields 23" erzielen.

Erstmals wurde im Rahmen dieser weltweit größten technischen Cyberübung gemeinsam mit Experten der nationalen zivilen Schlüsselinfrastruktur sowie mit der Miliz in Wien geübt. Das Blue Team unter der Führung des MilCyZ hatte dadurch die noch nie erreichte Stärke von ca. 120 Cyberexperten.

Die eigenen ca. 90 Bediensteten aus dem ÖBH (inkl. Miliz) wurden durch ca. 30 Experten aus der zivilen Schlüsselinfrastruktur, vor allem aus den Bereichen Energie, Telekom und Bankenwesen unterstützt.

Dieses bis dato einzigartige Event in Österreich wurde durch Besuche der Frau Bundesminister für Landesverteidigung und durch den Herrn Generalstabchef des Bundesheeres entsprechend ausgezeichnet.

Foto: Bundesheer/Dion6

Cyber Experten des MilCyZ bei der Verteidigung des Cyberraumes, Locked Shields 2023

Digitalisierungs-Element

Leiter: Oberst des höheren militärischen Fachdienstes Christian Pacher, MSc. MA.

Hervorzuhebende Aktivitäten

Steuerung und Umsetzung der Digitalisierung

Im Frühjahr 2021 wurde die AG DIKT (Digitalisierung und IKT) eingerichtet und mit der Erstellung jener strategischen Grundlagen beauftragt, welche die verbindlichen strategischen Vorgaben für die systematische Entwicklung der Digitalisierung darstellen sollen.

Im Februar 2022 wurde AG DIKT darüber hinaus mit der konkretisierenden Entwicklung geeigneter Rahmenbedingungen für eine kontinuierliche bedarfsgerechte Steuerung der Entwicklung der Digitalisierung beauftragt. Die daraufhin ergangene Empfehlung der AG DIKT zur Einrichtung eines strategischen Lenkungsgremiums im Ressort wurde durch KBM&GS zustimmend zur Kenntnis genommen.

Die Steuerung der Digitalisierung soll dazu grundsätzlich durch Koordinierung im Rahmen eines strategischen Lenkungsgremiums auf Ebene der Generaldirektoren erfolgen. In der Funktion als Chief Digital Officer (CDO) des BMLV soll der Leiter der Direktion 6 - IKT&Cyber die Unterstützung des strategischen Lenkungsgremiums umfassend sicherstellen und als Bindeglied zur operativen Umsetzung fungieren. Am 14.03.2023 trat das strategische Lenkungsgremium erstmals zusammen. Damit wurde eine erste zentrale Voraussetzung zur Ermöglichung einer digitalen Transformation erfüllt: Die Abbildung einer ressortweiten Steuerung auf Ebene des Top-Managements.

Zur effektiven Wahrnehmung der Aufgaben sowie zur Unterstützung des strategischen Lenkungsgremiums, benötigt der CDO qualitativ und quantitativ ausreichende personelle Ressourcen.

ChGStb erteilte dem CDO den Auftrag ein „strategisches Unterstützungselement Digitalisierung" (Arbeitsbegriff SUeD) zu entwickeln und aufzubauen sowie mit den Bearbeitungen zur Digitalisierung zu starten.

Foto: Bundesheer/Dion6

Auf Basis der Digitalisierungsstrategie und den Bearbeitungen zur Datenstrategie wurde eine „Prozesslandkarte Digitalisierung" entwickelt, sowie abzubildende Aufgabenfelder zur Steuerung der digitalen Transformation festgelegt.

Anfang Juni wurde dem ChGStb ein Strukturvorschlag sowie Arbeitsplatzbeschreibungen für eine mögliche Abteilung Digitalisierung vorgelegt.

Trilaterale Kooperation „Enterprise Architektur"

In Anbetracht der steigenden Komplexität und Dynamik militärischer Fähigkeiten und Bedarfe stellt sich die Disziplin der Enterprise Architektur zunehmend als ein zentraler Ansatz zur Unterstützung der Digitalisierung dar.

Durch einen ganzheitlichen Ansatz, der operationelle und technische Abhängigkeiten sowie Anforderungen transparent und nachvollziehbar macht, ermöglicht Enterprise Architektur eine effiziente und zielgerichtete Entwicklung im Kontext der Digitalisierung und unterstützt dazu beim Beherrschen der zunehmenden Komplexität.
Der Aufbau der EA-Fähigkeit im „Strategischen Unterstützungselement Digitalisierung" (SUeD) wird begleitet durch eine Kooperation mit Deutschland und der Schweiz.

Unter Abstützung auf die DACH-Kooperation „Digitalisierung" findet ein umfangreicher Erfahrungsaustausch zum Thema Aufbau und Nutzung von Enterprise Architektur statt. In diesem Jahr wurde dazu ein eigenes Fähigkeiten-Cluster „Enterprise Architektur" etabliert, in dem gemeinsam mit Deutschland und der Schweiz Architekturgrundlagen sowie praktische Anwendungsfälle erarbeitet werden. Dieser Austausch ist gegenwärtig besonders hilfreich für alle beteiligten Nationen, da neben dem Neuaufbau dieser Fähigkeit im BMLV, in der Schweiz und in Deutschland es aktuell zu einer Neuausrichtung der bestehenden Architekturpraxis kommt.

Die Einführung und Nutzung der Fachdisziplin Enterprise Architektur erfordern nicht nur den Aufwuchs von Personalressourcen innerhalb des SUeD, sondern auch ein breites Verständnis der Fachdisziplin innerhalb des Ressorts. Daher wurden in diesem Jahr mehrere Ausbildungsgänge zum Thema Enterprise Architektur und modellbasiertes Requirements Engineering durchgeführt. Mithilfe der bestehenden DACH-Kooperation „Digitalisierung" konnte man sich bei der Durchführung der Lehrgänge auf Lehrkräfte der Schweizer Armee und deren langjährige Fachexpertise in diesen Anwendungsgebieten abstützen.

Foto: pixabay.com

Energiemanagement, IoT und Nachhaltigkeit

Um die Ziele des Europäischen Green Deals und die nationale Kreislaufwirtschaftsstrategie zeitgerecht umzusetzen, müssen Organisationen und öffentliche Dienststellen ihre internen Prozesse anpassen. Das Internet der Dinge (Internet of Things, IoT) und Long Range Wide Area Network (LoRaWAN) bieten viele neue Möglichkeiten zur Digitalisierung in den Liegenschaften – Stichwörter „Klimaschutz" und „Energieeffizienz". Ein LoRaWAN stellt ein reichweitenstarkes, energiesparendes Funknetzwerk dar. Es eignet sich besonders für das Internet der Dinge und ist dabei vor allem für drahtlose, batteriebetriebene Systeme konzipiert.

Foto: pixabay.com

Neben dem Normalbetrieb haben definierte Kasernen und Sicherheitsinseln die Aufgabe, in Krisensituationen Mindestfunktionalitäten autark weiter bereitzustellen. IoT und LoRaWAN tragen im Ressort zur Modernisierung und Veränderung von Prozessen sowie zur Nutzung der Vorteile der Digitalisierung bei reduziertem Personal bei. Das BMLV nimmt dabei eine Vorreiterrolle ein. Bereits seit zwei Jahren hat die Direktion 6 - IKT&Cyber Digitalisierungsprojekte unter Nachrüstung von LoRaWAN-Sensoren und Aktoren pro Gebäude im Facility Management realisiert.

Foto: pixabay.com

In den Küchen des ÖBH müssen täglich über 600 HACCP-Messpunkte (Hazard Analysis and Critical Control Points) erfasst werden, diverse Energiezähler sind auszulesen – klassische IoT-Anwendungsfälle, die im Endausbau mit über 20 LoRaWAN-Sensoren pro Küche umgesetzt werden sollen.

Ein weiteres Thema ist die automatische Temperaturüberwachung in den Sanitätslagern des ÖBH – sie stellen auch Lagerkapazitäten für das Gesundheitsministerium bereit und dienen als strategische Reserve. Dazu werden diese im Endausbau mit über 30 LoRaWAN fähigen Tiefkühl- und Ultratiefkühlsensoren und Gateways zur Datenübertragung ausgestattet, um eine kostengünstige, lückenlose und autarke Temperaturüberwachung zu garantieren.


Foto: pixabay.com

Digitalisierungsvorhaben

Kommunikationsserver für die Bereiche Stellung und Medizin

In den Stellungshäusern werden verschiedene Geräte (Muskelkraftstuhl, Blutanalysegeräte etc.) zur Eignungstestung der Stellungspflichtigen verwendet. Die Informationen wurden bislang durch manuelle Eingabe zwischen den genützten Systemen ausgetauscht. Im Best Case mit einer Fehlerquote von nur einem Prozent bei der manuellen Datenerfassung, bedeutet das für eine Stellungsstraße mit ca. 500.000 Datensätzen im Jahr, 5.000 Fehleingaben in diesem Zeitraum.


Foto: pixabay.com

Mit Implementierung des Kommunikationsservers „Mirth Connect" als Open Source Lösung wird die manuelle Datenerfassung obsolet und so die Fehlerquote auf null reduziert, weil der Kommunikationsserver künftig als zentrale Drehscheibe und als „Dolmetscher" fungiert. Er ermöglicht die interoperable Einbindung von aktuell ca. 50 unterschiedlichen Geräten und sorgt dafür, dass die Daten untereinander und mit anderen Systemen und Anwendungen automatisiert ausgetauscht werden.

Durch die Nutzung des Kommunikationsservers in den Stellungshäusern wird den geringen Personalressourcen Rechnung getragen.

Mirth Connect „übersetzt" die gesendeten Daten in das Format, welches durch das empfangende System benötigt wird. Über den Netzwerk- und Alarm-Monitor kann der aktuelle Status der Schnittstellen automatisiert überwacht werden.

Mirth Connect unterstützt viele Plugins, die es ermöglichen, die Funktionalität der Plattform an individuelle Anforderungen anzupassen. Somit können bestehende Schnittstellen und Synergien genutzt werden, ohne alles neu zu erfinden, weil mit dem Kommunikationsserver die Nachrichten an das Empfängersystem anpasst werden.

Digitalisierungsvorhaben im Bereich Ausbildung

Das BMLV arbeitet an der Digitalisierung der Ausbildung, indem zukünftig als Lernmanagementsystem eingeführt wird. Moodle ist eine innovative E-Learning-Plattform, die es ermöglicht, den Unterricht und das Lernen auch online gut zu organisieren. Das BMLV nutzt Moodle, um den gesamten Ausbildungsprozess effizienter und flexibler zu gestalten. Lehrende können Lehrinhalte digital bereitstellen. Alle Bediensteten sollen zukünftig, auch von privaten Geräten aus, auf Lerninhalte und Unterlagen zugreifen können.

https://eledia.de/web/image/product.template/1178/image_1920?unique=96b9924

Eine segmentierte (W)LAN-Infrastruktur ermöglicht die sichere Nutzung von privaten Geräten („Bring Your Own Device") an den Akademien und Schulen. Die Nutzer können dabei nur auf die für sie freigegebenen Ressourcen im Netzwerk zugreifen. Dies fördert das selbstständige Lernen und lässt eine individuellere Betreuung zu.

Foto: pixabay.com

Foto: pixabay.com

Die bisher eingesetzte Lösung ist in die Jahre gekommen. Der Einsatz von Moodle eröffnet allen Lehrenden und Lernenden neue Wege für die eigene (Aus)Bildung. Moodle ermöglicht ein Arbeiten und Lernen mit anderen Teilnehmern in Chats, Foren oder Glossaren und auch ein verbessertes blended learning.

Zudem kann die Leistungsfähigkeit einer Moodle-Site durch die Installation von Plugins, mit denen Funktionen oder Funktionalitäten hinzugefügt werden und von denen es schon mehr als 2.000 gibt, erhöht werden.

Moodle ist das weltweit am meisten eingesetzte Learning Management System, wird kontinuierlich weiterentwickelt und ist daher als sehr zukunftssicher einzustufen.

Daneben sorgt das BMLV auch mit der Einführung der sicheren WLAN-Infrastruktur an den Akademien und Schulen maßgeblich für die Modernisierung des eigenen Ausbildungssystems.

Durch die Nutzung von COTS (Commercial Off The Shelf; kommerzielle Massenprodukte) bzw. Open Source Produkten werden Skaleneffekte genützt, die Geschwindigkeit der IT-Servicebereitstellung erhöht und Kooperationen mit anderen Ausbildungsinstitutionen gefördert.

IKT-Betrieb - IKTBetr

Leiter: HR Mag. Peter Binder, M.Sc., MSc.

Hervorzuhebende Aktivitäten

Fliegerübung NATO Tiger Meet

Die österreichischen Luftstreitkräfte nahmen im Zeitraum 26.09.23 – 17.10.23 am NATO Tiger Meet 23 (NTM23) mit insgesamt 3 Luftfahrzeugen „Eurofighter" samt den erforderlichen Versorgungs-, Verwaltungs- und Unterstützungsteilen teil. Neben der traditionellen Abwicklung des „NATO Tiger Meets" war tägliches taktisches Training der Luftstreitkräfte von insgesamt 13 Nationen ein Ausbildungsziel.

Im Rahmen des Trainings befanden sich bis zu 60 Kampfflugzeuge verschiedenster Typen gleichzeitig im zugeordneten Luftraum und simulierten Angriff und Verteidigung in einem täglich veränderten, vorab festgelegten Szenario.

Die Veranstaltung wurde am italienischen Militärflugplatz Gioia Del Colle ca. 50km südwestlich von Bari abgewickelt. Insgesamt waren etwa 1500 Soldaten/Zivilbedienstete in die Übung involviert. Die Arbeitsräume des österreichischen Kontingents befanden sich in Containern direkt am Rand der Flightline.

Diese wurden mit Masse durch das Versorgungsregiment 1 im Mot-Marsch in das Übungsgebiet

Foto: Bundesheer/Dion6

transportiert, einige Container wurden lokal angemietet und durch das Pionierbataillon 1 (PiB1) wurde ein Stromaggregat betrieben, welches die gesamte Versorgung des Containerdorfes einschließlich der Klimaanlagen rund um die Uhr sicherstellte. Die Hauptaufgaben der IKT&Cyberkräfte bei dieser Übung waren unter anderem stabile und sichere Verbindungen nach Österreich aufzubauen, die von EDV-Systemen für Verwaltung, Logistik und luftfahrtspezifische Anwendungen benötigt wurden, um den reibungslosen Ablauf dieser Übung sicherstellen zu können.

Foto: Bundesheer/Olt Markus Grießer

Austria-Kontingent mit Eurofighter

Eröffnungszeremonie

Highlights

Das Konzept des S6/KdoLRÜ sah wie folgt aus: eine leistungsfähige Internetanbindung wurde bei einem lokalen Provider angemietet, als Redundanz waren LTE-Router mit einer österreichischen SIMKarte bzw. ein SAT-Terminal vorgesehen. Die über diese Trägernetze geführten Verbindungen wurden Hardware-verschlüsselt (SINA-Boxen), mit Endpunkten in Wien und Zeltweg. Zwei Mitarbeiter des IKTBetr/BenBe waren ein Teil der in Goia Del Colle eingesetzten IKT-Kräfte.

Ihre Aufgabe war es, eine Verbindung nach Zeltweg für ein für den Eurofighter essentielles System sicherzustellen und diese Verbindung zu betreiben und zu überwachen sowie den S6/KdoLRÜ fachlich und technisch zu unterstützen. Der Eurofighter benötigt wie jedes moderne Luftfahrzeug eine EDV Anwendung zur Verwaltung seiner logistischen Daten.

Die zentrale Datenbank dazu befindet sich in Zeltweg. Um die Luftfahrzeuge aus der Ferne verwalten zu können, wurden einige Workstations in Goia Del Colle an den Heimatserver in Zeltweg angebunden. Da stellt sich natürlich die Frage, ob der Eurofighter immer eine Verbindung zur Heimatbasis benötigt.

Dem ist nicht so! Bei größeren und länger andauernden Verlegungen wird am Standort der Verlegung ein eigenes Server-Client Netzwerk errichtet, die beteiligten Luftfahrzeuge werden „exportiert" und nach Beendigung der Mission wieder in die Heimatliche Datenbank „importiert". Die Anbindung direkt an den Heimatserver bietet vor allem bei kleineren Verlegungen mehr Flexibilität, wenn z.B. während der Mission der Austausch eines Luftfahrzeuges erforderlich ist. Die Anbindung an den Heimatserver wird deshalb vom Bedarfsträger bei Missionen mit maximal 3 Luftfahrzeugen bevorzugt.

EFT Tiger-Bemalung

EFT zum Start

Der Ablauf der Mission stellte sich aus Sicht der IKTKräfte wie folgt dar. Nach einer Erkundungsmission vor Ort und umfangreichen Planungsarbeiten wurde unter der Leitung des S6/KdoLRÜ Anfang September eine Teststellung in der Schwarzenbergkaserne aufgebaut und alle eingesetzten IKTSysteme und Verbindungen getestet sowie Verbesserungen bzw. Anpassungen vorgenommen.

Durch das Referat MilCyZ / Sys-Kopplungen wurden Geräte für Verschlüsselung und Anbindung an das Internet konfiguriert, Anschlusspläne gezeichnet und die Geräte zur Verfügung gestellt. Am 26.09.23 verlegten die IKT-Teile im mot-Marsch Richtung Bari.

Da eine Marschstrecke von ca. 1200 km zurückzulegen war, erfolgte die Verlegung an 2 Tagen mit einer Nächtigung in Cesena. Am Ende des 2.Tages wurde direkt der Militärflugplatz Goia Del Colle angefahren, Gerät abgeladen und verwahrt. Danach wurde die Zeit genützt ums sich ein erstes Bild des Militärflugplatzeszzu machen. Anschließend wurde das 50km entfernte Hotel in Bari bezogen.

Das ortsfeste Richtverbindungsnetz – ofRVN

„Under Construction“, so lautet auch das diesjährige Motto für das ortsfeste Richtverbindungsnetz. Das ofRVN wurde beginnend mit 2003 errichtet. Eineinhalb Jahrzehnte später, im Jahr 2018, hatten die Komponenten des Trägernetzes das „End of Life“ erreicht und seitdem wird das System einem Mid-Life-Upgrade (MLU) unterzogen, wobei wesentliche Hardware-Komponenten zu tauschen sind. Seit annähernd 6 Jahren wird das Trägersystem ofRVN abschnittsweise umgebaut. Bei den Umbautätigkeiten im Jahr 2023 wurden an 8 Standorten in NÖ, OÖ und SBG neue Geräte bzw. Funkstrecken in Betrieb genommen.

Der Fokus in diesem Jahr lag darauf, die sogenannte Nordspange, die von Wien über Linz bis in die EZ/B führt, fertig zu stellen. Zwei Funkstrecken sind davon noch ausständig, diese sind für Anfang 2024 geplant. Mit der steigenden Anzahl an neuen Geräten und den dazu gehörenden Funkstrecken haben sich aber auch Probleme eingeschlichen, von Störungen der Sendeanlage bis hin zu systemweiten Fehlern. Die zum Teil aufwändige Fehlersuche sowie die anschließenden Instandsetzungen fordern das eigene technische Personal als auch Techniker des Auftragnehmers.

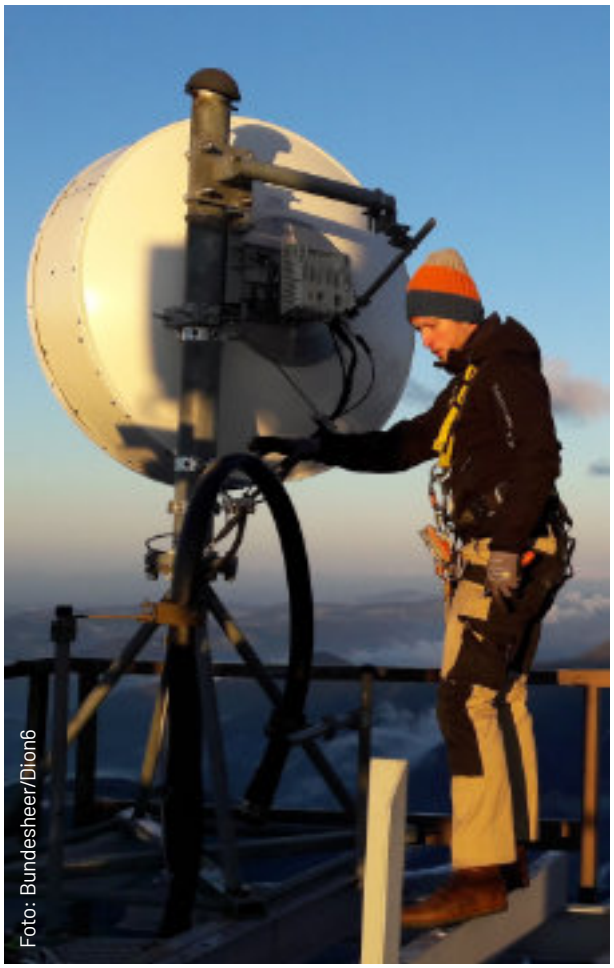
Das Netz in den Bergen

Eine große Herausforderung besteht in der Erreichbarkeit der Stationen im Kontext mit einer exakten Wettervorhersage, die einerseits einen Hubschrauberflug und andererseits einen mehrtätigen Umbau erlaubt.

Containerdorf-Austria

Etwa ein Drittel der Geräte steht auf Höhenstationen, die sich zum Teil im hochalpinen Gelände befinden. Während Geräte mit LWL-Verbindungen innerhalb von ein bis zwei Tagen umgebaut werden können, besteht bei Richtfunkstrecken ein Mehraufwand.

Die Arbeiten in diesem Bereich beanspruchen Zeitfenster von drei bis vier Tagen bei entsprechend passender Wetterlage. 75% des MLUs sind geschafft! Für das Jahr 2024 ist das Schließen der Nordspange, die Fertigstellung der Mittelstrecke zwischen Zeltweg und der Gemeindealpe, sowie der Ausbau der Stichverbindungen in Linz geplant – wir bauen weiter!



Instandsetzung auf dem Muckenkogel

Antennentausch

IKT-Technik - IKTTe

Leiter: Mag. Wolfgang Hacker

Hervorzuhebende Aktivitäten

Tactical Data Radio (TDR)

Das „Tactical Data Radio" (TDR) ist eine Funkgerätefamilie mit 2 Ausführungen, einer Handheld und einer Vehicular Version, welche im Frequenzbereich 30-2500MHz operieren können und über mehrere Wellenformen verfügen, wodurch hohe Datenraten aber auch hohe Reichweiten für Sprache erreicht werden können.

Im Jahr 2021 wurden Leihgeräte des TDR beim BMLV zur Erprobung bereitgestellt und seit dem wurden in enger Zusammenarbeit mit einer zivilen Firma, Firmenschulungen, viele Labortests sowie einige Feldtests durchgeführt, wobei die Reichweiten sowie die realen Sprach- und Datenverbindungen getestet werden konnten.

Für Software Updates das Key Management sowie die Kommissionierung ist das „Tactical Device Management" zuständig, welches auf einem entsprechendem Server läuft.

Foto: BMLV / HBF

Inzwischen wurden erste Geräte beschafft, um das TDR auch im Einsatz in Österreich benutzen und eventuell auch an das Tactical Communication Network (TCN) anschalten zu können. Hierfür ist die Kommissionierung der Geräte ein wichtiger Punkt. Mit der Kommissionierung wird im ersten Quartal 2024 bei den erworbenen Geräten begonnen werden. Danach werden weitere praktische Erprobungen durchgeführt.

Foto: Bundesheer/Dion6

TDR-Gerätesatz

Minerva – eine unternehmensweite Datenbasis

Das Ziel des Projekts *Minerva* ist es, eine umfassende Data-Analytics-Plattform bereitzustellen, welche die Automatisierung der Extraktions-, Lade- und Transformationsprozesse, eine unternehmensweite Daten Plattform, sowie Datenanalyse Funktionalitäten und die digitalisierte Visualisierung der Ergebnisse umfasst.

Bei der Architektur stand der Einsatz von Open Source Lösungen im Vordergrund. Open Source Produkte sind im Vergleich zu kommerzieller Software in vielen Bereichen wesentlich flexibler.

Neben den Kostenvorteilen (und trotzdem oft besseren Support!) sind diese Produkte anpassbar auf unterschiedliche Systeme. Der Fokus liegt auf der Interoperabilität und Erweiterungen mit Plugins und Extensions. Das Know-How für diese Tools wird intern aufgebaut und es kann auf eine aktive Community mit laufenden und schnellen Weiterentwicklungen zurückgegriffen werden. Diese Architektur erlaubt es uns, Daten aus unterschiedlichsten Quellen zu inkludieren und Consumern (Applikationen, Dashboards, Machine Learning Models, ...) bereitzustellen.

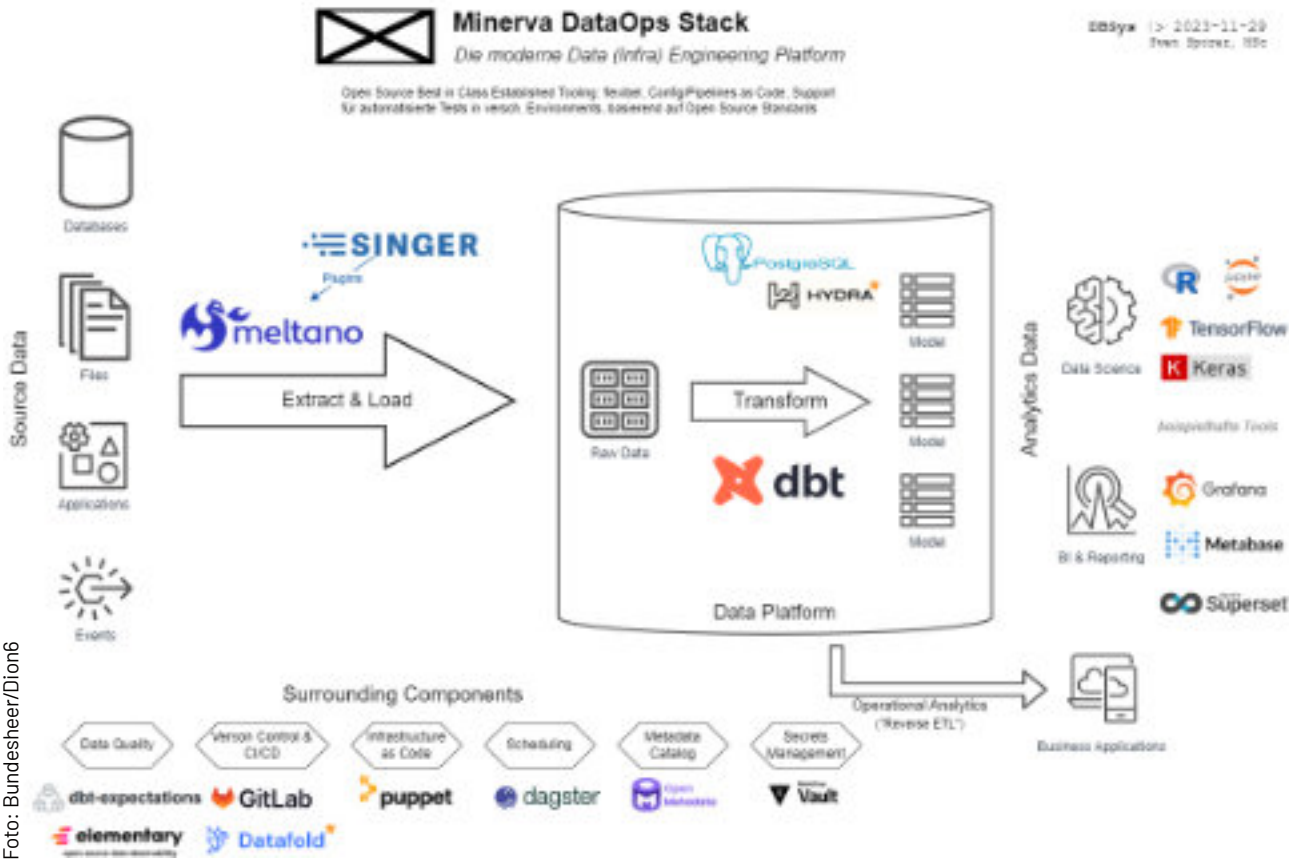


Foto: Bundesheer/Dion6

Minerva DataOps Stack

Sicheres Militärisches Netz (SMN) - Notebooklieferung 2023

Im Jahr 2022 erfolgte die Lieferung der ersten vereinbarten Tranche von 3.000 Stück Lenovo ThinkPad L15 Gen 2, welche im Rahmen eines 2020 durchgeführten „erneuten Aufruf zum Wettbewerb (EAW)" beschafft wurden.

Die Lieferung von weiteren 2.600 Stück wurde für Herbst 2022 festgelegt. Das Modell Lenovo ThinkPad L15 Gen 3 wurde der Dion 6 im Juni 2022 zur Testung zur Verfügung gestellt.

Bei diesem Gerät wurden zahlreiche Mängel festgestellt, zum einen konnte u.a. auf die BIOS Daten nicht automatisiert und ohne Austausch des Motherboards zugegriffen werden, zum anderen waren die Notebooks aufgrund der WebCam unbrauchbar für VTCs, die Krypto-Software konnte nicht installiert und der Akku nicht geladen werden.

Des weiteren wurde festgestellt, dass der verbaute Smardcard Reader inkompatibel mit dem geplanten Chipkartentyp war.

Der Lieferant der Notebooks schätzte die Kosten für die Entwicklung einer Lösung auf ~ € 200.000.

Foto: Bundesheer/Dion6

Lenovo Notebook

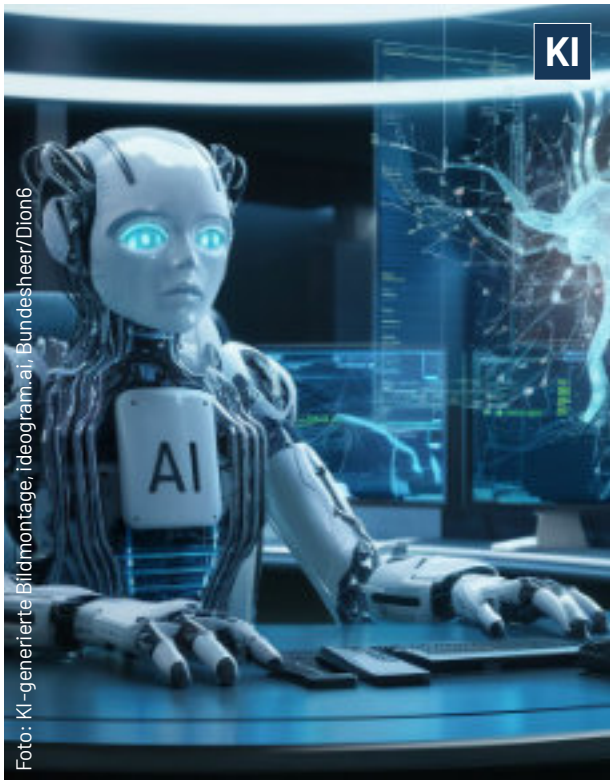


Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Nach Analyse & Recherche durch die Abteilung Dion6/IKTTe/HW&SysSW konnte das Problem durch gezielte Verbesserung des Treibers des Chipkartenlesers um € 10.000,- behoben werden.

Im Zuge des Abrufes wurde die Speicherkapazität des eingebauten SSD Speichers auf zukunftssichere 480GB verdoppelt.

Nach Behebung der festgestellten Mängel und Testung mit mehreren neuen BIOS Versionen und Gerätemodellen, konnte die Freigabe dieses Gerätes im April 2023 erfolgen.

Im Anschluss erfolgte der Abruf der Restmenge inkl. der Option die Bestellmenge auf insgesamt 6.000 Geräte mit Zubehör zu erhöhen.

Die Geräte wurden im HLogZ W übernommen, geklont und seit November 2023 an die Bedarfsträger durch HLogZ ausgeliefert.

SquadNet Soldatenfunkgerät

SquadNet ist das neueste Soldatenradio und wurde speziell für die Bedürfnisse abgesessener Soldaten und der Infanterie entwickelt. Aufgrund der technischen Konzeption als Software Defined Radio (SDR) bietet es eine hohe Flexibilität und erlaubt es je nach Rolle die Konfiguration des benötigten Feature- Sets und Funktionen.

Ferner wurden Headset Systeme mit integriertem Gehörschutz beschafft. Die PTT (Push to Talk) Module haben vielfältige Funktionen und Konfigurationsmöglichkeiten für den Nutzer.

Die Meshed Netzwerk Fähigkeit, mit der automatischen Weiterleitung von Übertragungen, ermöglicht eine Reichweitenerweiterung und sorgt für zuverlässige Kommunikation in Situationen wo eine direkte Sichtverbindung aufgrund der Topologie nicht möglich.
SquadNet ist für den Einsatz in militärischen Umfeld entwickelt und bietet eine entsprechende Mil-Std Qualifikation. Das SquadNet Radio alleine wiegt 154 g, 250 g mit Batterie, welche eine Einsatzfähigkeit von bis zu 24 Stunden ermöglicht.

Foto: Bundesheer/Dion6

SquadNet Soldatenfunkgerätesatz

Applikationen - Appl

Leiter: HR Dipl.Ing. Gerald Hofmeister

Hervorzuhebende Aktivitäten

Informationsmanagement & Büroautomation – Infomngt&BA

In der Abteilung Infomngt&BA ist im Jahr 2023 sehr viel passiert. Für die Großvorhaben IDV-Ablöse, Software-Portfolio Truppe sowie Fähigkeiteninformations-, -planungs- und -steuerungssystem (FIPS) wurden Teams aufgebaut und die Arbeitsbereitschaft hergestellt (Details zu den Vorhaben IDV-Ablöse und FIPS siehe Kapitel Vorhaben&Projekte des Leistungsberichts).

Betreffend BMLV-ELAK wurden drei Major Release-Upgrades mit insgesamt ca. 325 umgesetzten Punkten durchgeführt. Hervorzuheben sind hier der Abschluss der Ablöse des BMLV-ELAK V3.3 durch die Webversion ELAK V4.0 sowie die vollständige Integration des neuen Office-Produkts LibreOffice.

Auch beim Mailmanagement hat sich viel getan, so gab es ein Major Release Upgrade des HCL Notes-Clients von V9 auf V12, für das Internet-Mailing (Webmail) wurde die Mehrfaktorauthentifizierung eingeführt und Mail-Management wurde für das Tactical Communication Net (TCN) bereitgestellt.

Eine große Herausforderung stellte die Erweiterung der Datendrehscheibe Identity Data Hub dar, sodass diese nun die Daten für den neuen Telekommunikationsverbund (TKV) und das elektronische Telefonbuch (ETB) bereitstellt. Eine wichtige Besonderheit dabei ist, dass es möglich ist die gelebten IST-Strukturen abzubilden auch wenn diese in ORGIS und PS-NT noch nicht erfasst sind.

Foto: pixabay.com

Foto: BMLV / HBF

Personal Applikationen – PersAppl

In der Abteilung PersAppl konnten im Jahr 2023 weitere Projekte erfolgreich umgesetzt bzw. gestartet werden. Neben den Leuchttumprojekten „bundesheeronline", „ZAMS" und „PAAN-Zeitmanagement" wurde mit der Umsetzung von „PMSE – Personalmeldesystem Einsatz" gestartet. Ein erster Prototyp vom PMSE soll bereits Ende Jänner 2024 der PMSE-Arbeitsgruppe präsentiert werden.

Als Highlights an gesetzlichen Erfordernissen, die im Jahr 2023 in den Personalapplikationen umgesetzt wurden, sei angeführt: , Grundwehrdienst für Frauen' (Ausbildungsdienst in Chargenfunktion), die Reaktionsmiliz, die Milizausbildungsvergütung, die Umsetzung des dritten Geschlechtes in den Personalapplikationen und vieles mehr. Zu jeder Release wird eine ausführliche Release Notes erstellt und über das Impressum der Personalapplikationen veröffentlicht (erreichbar über alle IKT-Services von PersAppl durch anklicken des PS-NT-Logos). Technische Erneuerungen (ua. ZMR-Schnittstelle, Zusammenlegung dezentrale Oracle-Datenbanken im Stellungsbereich, L2/L3-Trennung) als auch klassische Systemerhaltungsmaßnahmen (ua. Reorganisation des BMLV) wurden in gewohnter Qualität realisiert.

Die Abteilung PersAppl hat Kompetenz im Bereich WEB-Technologie aufgebaut, insbesondere mit dem Hintergrund stark wachsender User-Zahlen (bundesheeronline, PAAN-Zeitmanagement), die nicht im klassischen Sinne geschult werden können. Im Allgemeinen werden neue Projekte bereits in WEB-Technologie in PersAppl umgesetzt.

Bauwesen Applikationen - BauWAppl

Die „Sicherheitszone Militärisches Gesundheitswesen" (SihZo MilGesW) ist eine besonders geschützte Systemumgebung im DGMN für die SanDienststellen des ÖBH. Die Einbindung der proprietären medizinischen Geräte über Schnittstellen und einen Kommunikationsserver vereinfachen die Prozesse und reduzieren Fehlerquellen.
Das „interoperable Zutrittsmanagementsystem" (iZMS) verwaltet und steuert Online- und Offline-Zutritte in den Liegenschaften. Marktübliche Standards ermöglichen den Einsatz von Schlössern beliebiger Hersteller, womit die Abhängigkeit von einzelnen Firmen eliminiert wird.

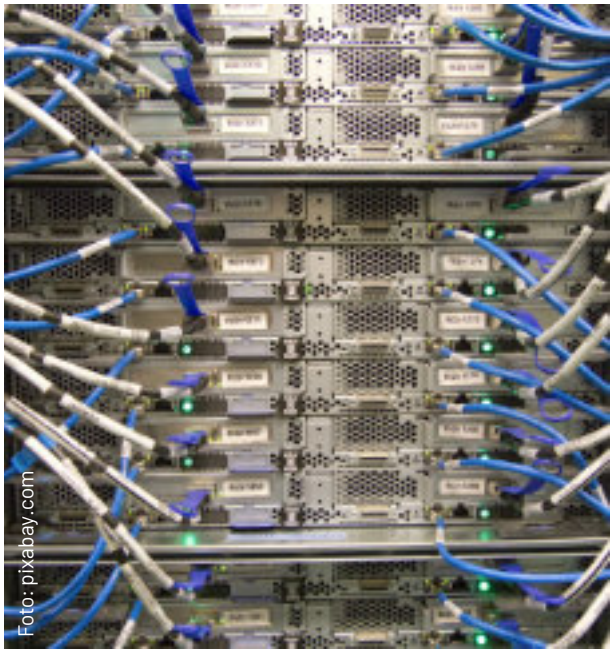


Foto: pixabay.com


Foto: pixabay.com

Im „Energiemanagementsystem" (EnMS) werden Zählerstände automatisch ausgelesen und zentral ausgewertet. Das System ist eine Basis zur energetischen Steuerung der Immobilien.

Mit „Moodle" wird das eLearning im Ressort modernisiert. Das lizenzfreie Produkt ermöglicht die effektive Integration innovativer Lernmethoden und soll SITOS SIX ablösen.

Der „Muskelkraftstuhl" trägt zur Eignungsfeststellung von Stellungspflichtigen bei und ist im DGMN integriert. Stamm- und Messdaten der Probanden können nun über Standard-Schnittstellen automatisiert ausgetauscht werden.

DGMN 2.0 steht u.a. für ein neues Active Directory-Design, das die Mandanten- und Gerätevielfalt, die Funktionsabstufungen, die Zonenbildungen und die Fachexpertise noch granularer unterstützt. Eine Zwei-Faktor-Authentifizierung wird die Basissicherheit erhöhen.

Einsatz Applikationen - EinsAppl

Federated Mission Networking Verification & Validation

Mit dem CFBLNet PoP (Combined Federated Battle Laboratories Point of Presence) hat das Österreichische Bundesheer eine klassifizierte Testinfrastruktur, die heuer erstmals für die formelle FMN Zertifizierung genutzt wurde.

In standardisierten Tests mit CAN, FIN, SWE und NATO wurde die Kompatibilität mehrerer IKT-Services mit der aktuellen Spezifikation FMN Spiral 4 überprüft.

Neben technischen Basisdiensten konnte das für Einsatzapplikationen grundlegende Service "Geospatial Information" erfolgreich zertifiziert werden.

2024 soll dann die derzeit in Entwicklung befindliche neue Version des Friendly Force Tracking getestet werden. FFT wird dann erstmals auch über standardisierte Security Labels als Voraussetzung für Data Centric Security (DCS) verfügen.

Übungseinsatz von mobilen Geräten

Organisations- und Logistik Applikationen - Org&LogAppl

Statusdarstellung der Fähigkeitenentwicklung

Die Anwendung MoSe (Monitor zur Streitkräfte-Entwicklung) soll den Steuerungsverantwortlichen laufend einen Überblick zum Zustand der Fähigkeitenträger des ÖBH und zu deren Entwicklungstrends anbieten.

Dazu werden Daten zu den Fähigkeitsträgern (OE) der mobil gemachten Organisation des Bundesheeres (Mob-Org des ÖBH) aus ORGIS, PS-NT und LOGIS übernommen Kennzahlen zu den nPersonal und Ausrüstung in den Waffengattungen sowie der Heeresstruktur bereitgestellt.

Foto: pixabay.com


Foto: pixabay.com

Flugstundenevaluierung (LFZ-Mgmt-Cockpit)

Im neuen LFZ-Mgmt-Cockpit werden Geräteinformationen aus LOGIS mit manuell eingegebenen Flugdaten ergänzt, verarbeitet und in verschiedenen tabellarischen Auswertungen und Grafiken dargestellt.

Das Service stellt den Fliegerwerften täglich aktuelle Lagemeldungen sowie monatliche/jährliche Betriebsdaten-Auswertungen zur Verfügung, die als vorgefertigter Bericht oder in beliebiger Form an die zu meldenden Stellen weitergegeben werden können.


Foto: pixabay.com

Militärisches Geowesen - IMG

Leiter: Brigadier Mag. Dr. Friedrich Teichmann, MAS, MSc.

Hervorzuhebende Aktivitäten

Das IMG konnte sich sowohl national wie auch international durch eine Reihe von Aktivitäten und Weiterentwicklungen auszeichnen. Getrieben wurden viele dieser Umsetzungen durch die massiv veränderten Rahmenbedingungen im Sicherheitsbereich, die sich insbesondere im MilGeo-Dienst in einer Fokussierung zum klassischen militärischen Einsatz auszeichnet. Im Fokus steht dabei die Beitragsleistung des Fachbereiches MilGeo zum Aufklärungs-, Führungs- und Wirkungsverbund auf allen Ebenen, der insbesondere im Zusammenhang mit der Digitalisierung der Streitkräfte massive Auswirkungen auf den Fachbereich mit sich bringt.

Foto: BMLV / HBF

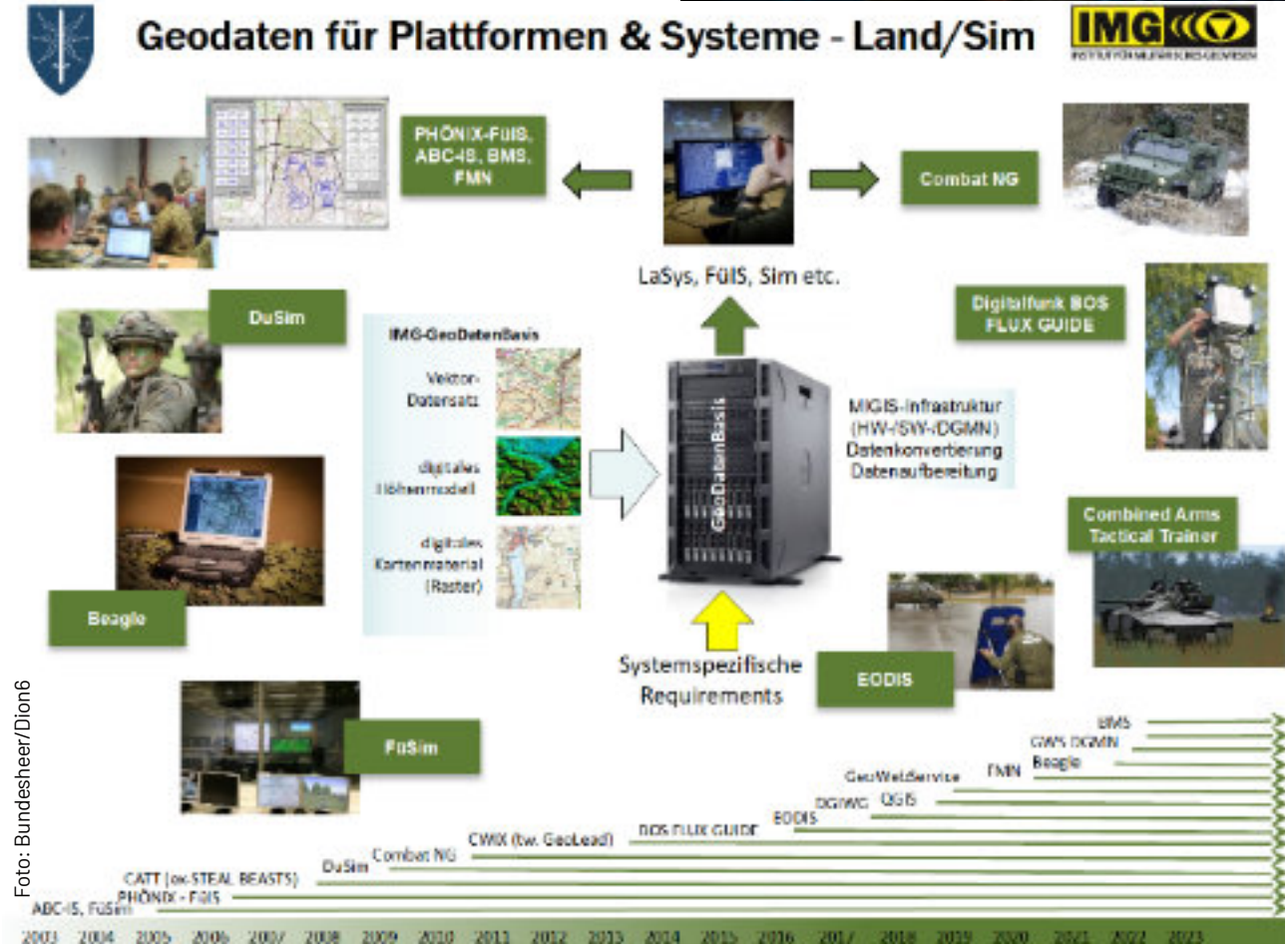


Foto: Bundesheer/Dion6

Geodaten für Plattformen & Systeme - Land/Sim

Der Schlüssel für jeden wirkungsvollen Aufklärungs-, Führungs- und Wirkungsverbund sind die aktuellen GeoInfo-Produkte (von der klassischen Karte auf taktischer Ebene bis zu den Landesbeschreibungen auf strategischer Ebene); diese Produkte müssen kontinuierlich dem Bedarf und den technischen Möglichkeiten angepasst werden. In diesem Zusammenhang konnte das IMG 2023 die Partner aus dem DACH-Verbund für die Festveranstaltung 10-Jahre MGI (Militärische Geo-Informationen) einladen. Daneben gewinnt die direkte Einspielung in GeoDaten in den diversen Plattformen der Land- und Luftstreitkräfte immer mehr Bedeutung. Ohne korrekte GeoDaten funktionieren die meisten modernen Waffensysteme NICHT!

Und diese kontinuierlich wachsende Anzahl der Einsatzsysteme des ÖBH verlangen meistens spezielle Formate bzw. Zusammenstellung der GeoDaten.

Neben den klassischen Geo-Services (von der analogen Karte bis zu den digitalen Waffensystemen) ist eine innovative Weiterentwicklung des Produkt-Portfolios des IMG Voraussetzung für einen „state-of-the-art" Fachdienstes „Militärisches Geowesen", der innerhalb der neuen Direktion - 6 IKT&Cyber, etabliert wurde. Neben der in den letzten Jahren eingeführten VR-Brille (Virtuelle Realität) des IMG's zur Geländeanalyse bzw. Kdt-Beratung konnten kundenfreundliche 3D-Modelle (BORIS) in das modernisierte Repertoire der MilGeo-Produkte aufgenommen werden.

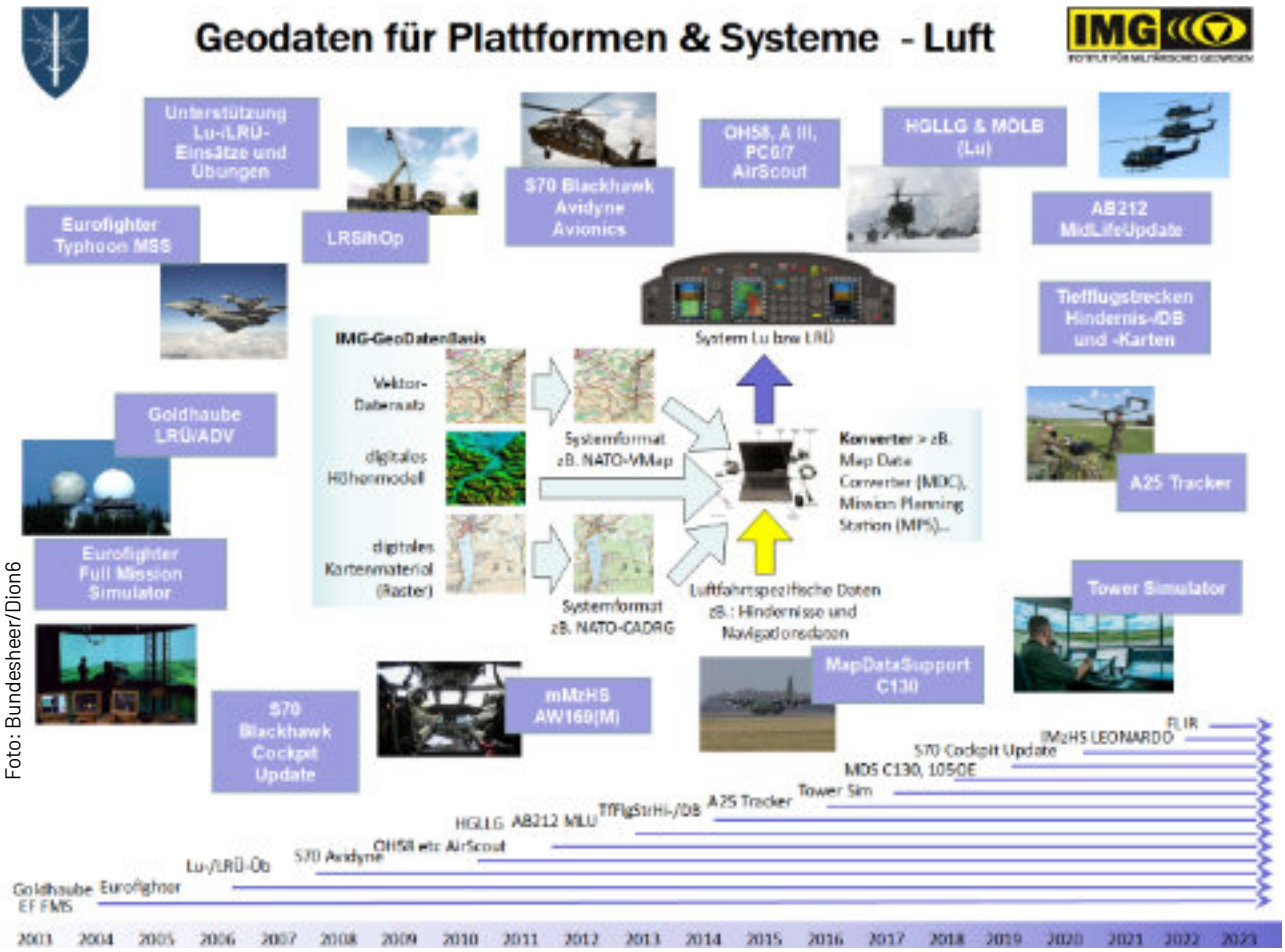


Foto: Bundesheer/Dion6

Geodaten für Plattformen & Systeme - Luft

VR-Handcontroller

Diese Weiterentwicklung gelingt nur dann im Sinne des Kunden (in diesem Fall HQ, Brig, Baon, TF, Stab, Kdt), wenn dies in Übungen direkt mit dem Bedarfsträger entwickelt wird. Daher ist eine umfassende Übungsteilnahme von MilGeo-Teams (z.B. im Brig-Stab) eine „conditia-sine-qua-non". Diese „bottom-uo" Entwicklung komplimentiert die Planungsaufgaben zur Fähigkeitsentwicklung ÖBH 2032 (top-down), die als Vision für den modernen Fachdienst, „MilGeo 2.0," durch die Experten des IMG entwickelt wird.

Die Korrektheit (Unverfälschtheit) von Geographische Koordinaten (sowohl in Karten als auch in den Endgeräten der militärischen Einsatzsysteme) bzw. deren Lage-Richtigkeit sind die Kernaufgabe von Navigation Warfare (NavWar) bzw. Secure PNT (Position-Navigation-Timing). In zwei national und international hochrangig beschickten Testwochen (z.B. durch die NATO NCIA oder die DEU Bundeswehr) am TÜPL Seetaler Alpe (Frühjahr und Herbst 2023) konnten weitere wichtige Entwicklungsschritte sowohl für defensive NavWar (korrekte PNT-Lösungen für die eigenen Systeme) als auch offensive NavWar (durch Jamming und Spoofing die Veränderung der gegnerischen Positionsdaten) gesetzt werden.

Der aktuelle Ukraine-Krieg zeigt schonungslos die dringende Notwendigkeit auf, daß moderne Streitkräfte sowohl über defensive (z.B. für Präzisionswaffen) als auch offensive NavWar Fähigkeiten (z.B. als Drohnenabwehr) verfügen muss, und daß am IMG frühzeitig diese Fähigkeitsentwicklung begonnen hat.

Die enge Verzahnung von MilGeo zu den Space Services (Sat-Images, Sat-Navigation, Sat-Kommunikation) setzte sich auch 2023 in verschiedenen Projekten fort. Besonders eindrucksvoll konnte diese Vernetzung Geo und Space bei der internationalen ISNEX Übung am TÜPL Hochfilzen unter Beweis gestellt werden. Die teilnehmenden Vermessungs-Teams der MN GSG (Multi-Nationalen Geospatial Support Group) wurden neben Schnee und Hochgebirge insbesondere offensiven NavWar-Angriffen ausgesetzt, die ihre hochpräzisen satelliten-gestützten Vermessungssysteme (GPS oder Galileo) umfassend stören und verfälschen konnte, und damit zum Einsatz von back-up Lösungen (z.B. Karten oder Triangulation ohne GPS), ähnlich wie in einem potentiellen Einsatzszenario, zwang.

Auch am internationalen Parkett konnte das IMG 2023 reüssieren: Beim in GRAZ gehosteten DACH Fachdienstmeeting auf Leiter-Ebene wurden erstmals mit einem Strategie-Workshop visionäre Entwicklungen gesetzt; außerdem zeigten sich die Leiter der DEU und CHE GeoDienste über die Fähigkeitsentwicklung Navigation Warfare und den Synergien zu Space Services, die derzeit am IMG entwickelt werden, sehr beeindruckt.

Das internationale Highlight war aber sicherlich das Hosting des EDA CapTech Meetings, bei dem dankenswerterweise FBM Mag.[a] Klaudia Tanner die Begrüßungsrede hielt: in drei Tagen trafen sich alle namentlichen europäischen Militär-Experten zu Forschung und Entwicklung im Weltraumbereich in Wien und konnten gemeinsam mit über hundert Industrie-Vertreter nicht nur die SRA (Strategic Research Agenda) „Military Space" der EU, sondern auch konkrete gemeinsame Weltraum-Projekte sowie Synergien dazu identifizieren.

Der Schlüssel für das erfolgreiche Jahr 2023, aus Sicht IMG, sind jedoch motivierte und qualifizierte Mitarbeiter, die nicht nur die laufenden Anforderungen und Anträge wirtschaftlich und zweckmäßig und im Sinne der Kunden (vom Kabinett der FBM bis zur Miliz-Kompanie) rasch erfüllen, sondern auch die notwendigen Entwicklungsschritte für „stay-in-the-game" für den Fachdienst MilGeo setzen.

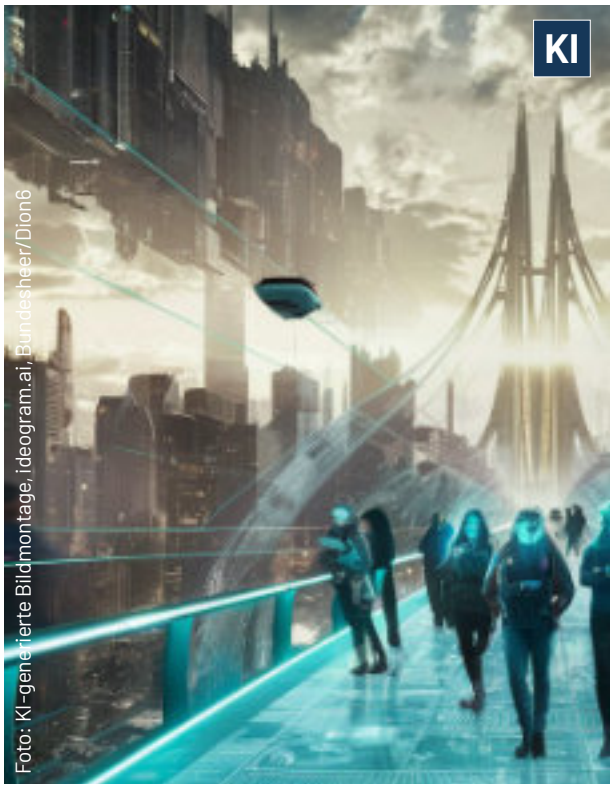


Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6


Foto: pixabay.com

Aber auch der Personalstand das IMG's unterliegt Veränderungen: der Abgang verdienter Mitarbeiter muß langfristig unbedingt durch qualifizierten und motivierten Neuzugang kompensiert werden, um weiterhin die geforderte Leistung des Fachdienstes erbringen zu können. Diese neuen Mitarbeiter sind die langfristige Zukunft des IMG's, sie müssen möglichst harmonisch in das bestehende Team integrieren werden, auf die bestehenden erfolgreichen Prozesse und Wissensbasis aufsetzen können und idealerweise mit zusätzlichen Ideen und Fähigkeiten das IMG bereichern können.

Dieser kontinuierliche Prozess einer qualifizierten „Personalerneuerung" ist, neben der Schaffung bzw. Erhaltung adäquater Arbeitsumgebung und der Modernisierung des Portfolios bei gleichzeitiger Sicherstellung der Services, DIE zukünftige Herausforderung im Fachdienst MilGeo.

Militärisches Cybersicherheitszentrum - MilCyZ

Leiter: Dipl.-HTL-Ing. Lambert SCHARWITZL, MA, MSc.

Hervorzuhebende Aktivitäten

Der Cyberraum hat sich zu einem kritischen Bereich für nationale Sicherheitsinteressen entwickelt, und die Herausforderungen in diesem Bereich sind im vergangenen Jahr weiter gewachsen. Das sich entwickelnde Sicherheitsumfeld bringt eine zunehmende Komplexität und Dynamik mit sich.

Cyberbedrohungen sind in ihrer Intensität und Vielfalt gestiegen, wobei verschiedene Akteure, darunter Cyberkriminelle und staatliche Einheiten, innovative Methoden zur Infiltration von kritischen Infrastrukturen und Institutionen, sowie öffentlichkeitswirksame „Denial of Service "-Angriffe einsetzen. Die fortschreitende Digitalisierung unserer Gesellschaft eröffnet zwar neue Möglichkeiten, birgt jedoch gleichzeitig erhebliche Risiken für die nationale Sicherheit. Der enorme Anstieg der Bedrohungen im Cyberraum durch vermehrte, gezielte Angriffe war auch im Jahr 2023 nicht zu übersehen.

Die Notwendigkeit einer robusten Verteidigung im Cyberraum steht im Mittelpunkt der Bemühungen des Militärischen Cyberzentrums (MilCyZ). Die folgenden Ausführungen geben einen Einblick in die getroffenen Maßnahmen und die erzielten Ergebnisse des MilCyZ im Jahr 2023. Ziel des Zentrums ist es, die Integrität, Vertraulichkeit und Verfügbarkeit der IKT des ÖBH zu gewährleisten und somit die Souveränität sowie Sicherheit Österreichs zu schützen.

Foto: BMLV / HBF

Cybersicherheits-Management

Im Vergleich zu konventionellen Kriegen sind Cyberoperationen kostengünstiger und für Staaten sowie nichtstaatliche Akteure leichter zugänglich. Sie ermöglichen erhebliche Auswirkungen und ermöglichen Kriege ohne physische Konfrontation. Es besteht weitgehende Einigkeit darüber, dass cyberfähige Technologien das internationale und nationale Sicherheitsumfeld zwangsläufig verändern werden. Daher ist die Bedeutung von Forschung und Entwicklung im Bereich der Verteidigung im Cyberraum von entscheidender Relevanz. Die Dynamik des Cyberraums erfordert eine kontinuierliche Innovation, um mit den raffinierten Techniken der Angreifer Schritt zu halten und präventive Maßnahmen zu entwickeln.

Foto: pixabay.com

Die Europäische Union (EU) und ihre Mitgliedstaaten haben dies erkannt und haben daher verschiedene Initiativen gestartet, um in Forschung und Entwicklung in diesem Bereich zu investieren. Österreich ist dementsprechend an zahlreichen European Defence Fund (EDF) - und European Defence Agency-Projekten aktiv beteiligt, um Synergien zu schaffen und somit Interoperabilität zu gewährleisten. Österreich hat im Jahr 2023 zudem seine Bemühungen zur verstärkten Zusammenarbeit in der Cyberverteidigung fortgesetzt und ist proaktiv an zahlreichen Projekten auf nationaler und EU-Ebene vertreten. Das MilCyZ unterstützt sowohl die nationale Strategie zur Cyberverteidigung als auch Maßnahmen der EU Cyber Defence Policy zur Stärkung der Resilienz im Cyberspace der EU.

Aus diesem Grund hat Österreich beschlossen, sich an den beiden Projekten PESCO "Cyber Rapid Response Team" (CRRT) und PESCO Cyber Range Federation (CRF) als vollwertiger Teilnehmer zu beteiligen. Insbesondere die Teilnahme an dem Projekt PESCO CRF stärkt die nationale Umsetzung des Aufbaus eines Cyber Truppenübungsplatzes. Das MilCyZ hat damit begonnen, eine eigene CyberRange für das BMLV/ÖBH zu konzipieren. In dieser technischen Infrastruktur können komplexe Systeme abgebildet und diverse Angriffs- und Verteidigungsszenarien simuliert werden.

Neben der Vorbereitung des Fachpersonals auf Krisen durch spezialisierte Übungen, umfasst die CyberRange die Fähigkeit das Verhalten von Angriffen innerhalb komplexer Systemstrukturen in einer gesicherten Umgebung zu analysieren und neue technische Komponenten in realitätsnahen Szenarien auf ihre Resilienz zu testen. Somit liefert eine CyberRange einen wichtigen Beitrag zur Systembereitstellung für die Verteidigung, sowie den Erhalt und die Erweiterung der personellen und technischen Fähigkeiten im BMLV/ÖBH und die Förderung der gesamtstaatlichen Resilienz.


Foto: pixabay.com

Sicherheitskonzeption & Informationssicherheit

Durch die Ausarbeitung systemspezifischer Sicherheitsanforderungen wurden auch im vergangenen Jahr wieder zahlreiche IKT-Systeme maßgeschneidert und bedarfsorientiert abgesichert und in die IKT-Sicherheitsarchitektur des ÖBH integriert. Die Unterstützungsleistung durch Beiträge der IKT-Sicherheit bereits in der Planungsphase erhöht die Resilienz der Systeme des ÖBH bei gleichzeitiger Senkung des Aufwandes und der Kosten gegenüber nachträglich implementierter Sicherheitsmaßnahmen. Somit werden zahlreiche Systeme gem. eines gesamtheitlichen Sicherheitskonzeptes eingebunden, im Betrieb aufwändige Sonderlösungen vermieden und Vereinheitlichung von Sicherheitsmechanismen und -technologien geschaffen.

Durch die Abwicklung zahlreicher Sicherheitsüberprüfungen im Zuge von anlassbezogenen IKT-Sicherheits-Audits sowie im Zuge von Akkreditierungsverfahren, konnten auch dieses Jahr wieder zahlreiche, teilweise kritische, Schwachstellen in IKT-Systemen und Produkten gefunden und durch geeignete Maßnahmen geschlossen werden, bevor diese durch eventuelle Angreifer zu einer Gefahr werden konnten. Im Zuge der „Responsible Disclosure“ werden die gefundenen Schwachstellen in Produkten vertrauensvoll an den jeweiligen Hersteller gemeldet, um diesem die Möglichkeit zu geben, das Produkt mittels Sicherheitsupdates abzusichern. Im vergangenen Jahr wurden mit diesem Prozess über 15, darunter auch einige hochkritische Schwachstellen identifiziert und an die Hersteller gemeldet. Diese konnten so einer Behebung zugeführt werden, und die Absicherung kommt allen Nutzern dieser Produkte und somit auch dem ÖBH zu Gute.

- Die selbst eingesetzten Produkte werden dadurch sicherer.
- Das ÖBH präsentiert sich gegenüber der Industrie als kompetenter und wertvoller Partner.
- Durch die Beitragsleistung zur Erhöhung der Sicherheit für die Allgemeinheit steigt die positive Wahrnehmung in der Öffentlichkeit.

Cyber-Verteidigung der IKT-Landschaft

Das Gefechtsfeld wird komplexer, vernetzter, unübersichtlicher. Sicherheit kann nur gewährleistet werden, wenn ein umfassendes Situtationsbewusstsein sichergestellt ist. Daher ist die Erstellung eines Lagebildes einer der zentralen Schwerpunkte des MilCyZ im Rahmen der Forschung und Entwicklung auf nationaler/internationaler Ebene. Um ein ganzheitliches Situationsbewusstsein im Cyber- und Informationsbereich für das gesamte ÖBH zu entwickeln, ist ein koordinierter Ansatz zur Cybersicherheit auf allen Ebenen notwendig.

Dies erfordert eine enge Zusammenarbeit zwischen technischen Experten, operativen Entscheidern und hochrangigen Führungskräften sowie Kommunikations- und Informationsaustauschmechanismen. Basis dafür ist ein gemeinsam ausgearbeitetes Konzept, das in ein gesamtheitliches Projekt zur Umsetzung der geteilten Interessen umgesetzt werden kann. Im Rahmen des Vorhabens „Holistisches digitalisiertes Cyberlagebild" werden die notwendigen Grundlagen für ein ebenenübergreifendes, KI-gestütztes, holistisches Lagebild für den Cyberraum eruiert.

Ein weiterer Fokus lag auf dem Ausbau von „Cyber Rapid Response Teams" (CRRT). Dies stellt einen zentralen Bestandteil des BMLV zu gesamtstaatlichen Resilienzbemühungen im Cyberraum dar. Die CRRTs ergänzen die Kompetenzen und Kapazitäten des BMLV um Incident Response als auch Remediation-Anteile. Mit der Verfügbarkeit im BMLV kann hier künftig anlassbezogen im Zuge der Unterstützung (Amtshilfe, Assistenzeinsatz) für andere Behörden und Organe schnell und zielgerichtet agiert und reagiert werden. Mit der vollwertigen Teilnahme an dem Projekt PESCO CRRT unterstreicht Österreich zudem seine aktive Beteiligung an einer gemeinsamen europäischen Krisenreaktionsfähigkeit mit der Vision, das CRRT im EU-Cyber-Ökosystem zu verstärken. Das EU CRRT bietet Unterstützung für Cyber-Resilienz, Reaktion auf Cyber-Vorfälle und Präventiv-maßnahmen und ist somit ein relevantes Werkzeug im Rahmen der EU CyberDiplomacy Toolbox.

Cybersicherheitstechnik

Das Jahr 2023 war für die Abteilung Cybersicherheit Technik geprägt durch die Bereitstellung von Defence Technologien (d.h. die Sensor- und Effektor Anteile der SOC's) und Cyber-Experten für die Abwehr von laufenden oder unmittelbar drohenden Cyber-Angriffen durch das MilCyZ. Diese Aufgabe umfasste den realen Einsatz ebenso wie die durchgeführten Cyber-Übungen, so war die Abteilung der größte „Truppensteller" für die Locked Shields 2023. Daneben ist die Aufrechterhaltung des Betriebs zu wesentlichen Teilen durch die Abteilung zu leisten und eine Mitwirkung in nahezu allen IKT-Projekten des Ressorts gefordert.

Um hier ausgewählte Themen exemplarisch anzuführen, ist etwa das Rollout eines truppentauglichen GEHEIM Systems zu nennen. Die Beistellung von Kryptomaterial und Sicherheitssystemen für das TCN war im Kryptobereich eine feldverwendungsfähige Lösung. Am anderen Ende der Reifegradskala ist der Abschluss eines Forschungsprojektes zu nennen, in dessen Rahmen quantenresistente kryptographische Algorithmen auf einen hardware Security Token implementiert werden konnten. Mit dem Pilotprojekt „MAVE as a service" wurde, in Zusammenarbeit mit Dion 2, erstmals versucht Defence Technologien für einen Betrieb außerhalb der Dion 6 bereitzustellen. Im Kontext des zentralen MAVE Systems konnte 2023 erstmals verschiedene Machine Learning Algorithmen zur Erkennung von Malware zum produktiven Einsatz gebracht und mit großem Erfolg genutzt werden.

Foto: Bundesheer/Dion6

Sicherheitsmeldung von MAVE (Multi Anti Virus Engine)

Neben der Beschäftigung mit den disruptiven Technologien Quantencomputing und künstliche Intelligenz stand das Jahr 2023 im Zeichen der Fokussierung auf die Einsatzerfordernisse des ÖBH und die damit verbunden Cyber-Bedrohungen im Zeichen eines digitalisierten Schlachtfeldes. Diese Schwerpunkte werden die Abteilung Cybersicherheit Technik auch in den folgenden Jahren beschäftigen.

Elektronischer Kampf

Das elektromagnetische Spektrum (EMS) im Allgemeinen sowie im militärischen Kontext das elektromagnetische Umfeld (EMU) ist mit dem aktuellen Konflikt in Europa stark in den Fokus der Betrachtungen gerückt. Die zivile und militärische Nutzung dieser Domäne hat die einsatzkritische Relevanz und die Abhängigkeiten und Erfordernisse für Militär und Gesellschaft in einem Zeitalter der digitalen Kommunikation erneut untermauert.

Es wurde mit dem Aufbau eines digitalen EloKa-Lagebildes begonnen, um künftig für die EloKa-Elemente und die Nutzer von EloKa-Systemen ein Lagebewusstsein zu schaffen und Beiträge für übergreifenden Lagebildern zu leisten. Die derzeitigen Herausforderungen sind die Zusammenführung der Informationen von unterschiedlichen Sensoren und Systemen, der Bearbeitung und der weiteren bedarfsträgergerechten Bereitstellung.

Das internationale Engagement der Abteilung stellt einen wichtigen Teil der Arbeit in dieser technischen Waffengattung dar. Dies erfolgt unter anderem durch stetige nationale Vertreter in technischen Arbeitsgruppen der NATO für Selbstschutzsysteme der Land- und Luftstreitkräfte, und Teilnahme an internationalen Übungen und internationalen Fachmessen und -veranstaltungen. Die Beitragsleistung im Rahmen der Planungen für das ÖBH 2032+ der Dion6 für die Waffengattung EloKa war im vergangen Jahr eine relevante Aufgabe und es konnte eine Grundlage für den weiteren Fähigkeitenaufbau geleistet werden. Diese herausfordernde Aufgabe wird künftig ebenfalls ein einsatzrelevantes Thema in der Abteilung bleiben.

Foto: pixabay.com

Der Erhalt der bereits aufgebauten Expertise erfordert laufende technische und militärische Aus- und Weiterbildungen. Im vergangenen Jahr wurde neben Firmenschulungen im Bereich der Signalanalyse, des Requirement Engineerings und Systemarchitektur auch an Ausbildungen der Carl Cranz Gesellschaft teilgenommen. Im Gegenzug kommt dieses Fachwissen zusätzlich durch das Halten von Vorträgen an der Landesverteidigungsakademie, der Führungsunterstützungsschule und der Flieger- und Fliegerabwehrtruppenschule zur Anwendung.

Cyber-Übungen

Neben zahlreichen einschlägigen Cyber- und EloKa-Übungen ist die jährliche Teilnahme an der international größten live-fire Cyberdefence-Übung der NATO, „LOCKED SHIELDS", besonders hervorzuheben: Das MilCyZ stellt seit 2012 – auch unter Einbindung von Milizexperten - den größten Anteil bei der Bereitstellung der österreichischen Training Audience, die hier den Einsatz eines sog. Cyber Rapid Response Teams zur Bekämpfung eines hybrid agierenden, staatlichen Gegners übt.

2023 war es für das ÖBH die bisher größte Einsatzübung: Knapp 150 militärische und zivile Cyberexperten konnten zwei Wochen lang die kollaborative Cyber-Verteidigung gegen einen virtuellen Gegner üben und neueste Technologien und Prozesse zur Anwendung bringen.

Führungsunterstützungsschule - FüUS

Leiter: Oberst des Generalstabsdienstes Mag. Franz Sitzwohl

Hervorzuhebende Aktivitäten

Innovationszentrum in Elektronischer Kampfführung und Digitaler Kommunikation

Ausbildung Elektronische Kampfführung: Neues Zeitalter der Innovation

EloKa-Lehrgang an der FüUS

Das Jahr 2023 stellte für die Führungsunterstützungsschule (FüUS) einen historischen Wendepunkt dar, insbesondere in der EloKa-Ausbildung. Durch ein beeindruckendes Angebot an hochmodernen Kursen, Seminaren und Übungen, sowohl auf nationaler als auch auf internationaler Ebene, hat die FüUS ihre führende Position in diesem Bereich eindrucksvoll bestätigt. Bei allen Kursen gilt es, das Bewusstsein und das Wissen über EloKa Bedrohungen (Erkennen und Handeln) zu schärfen, um die Awareness dafür zu steigern.

Besonders hervorzuheben ist die erfolgreiche Integration des Störsenders SGS-2000, der als bahnbrechende Innovation in der praktischen EloKa-Anwendung gilt. Dieser Fortschritt demonstriert das Engagement der FüUS, stets an der Spitze technologischer Entwicklungen zu stehen. Unser Ziel für 2024 ist es, die internationale Vernetzung weiter auszubauen und neue, wegweisende Taktikseminare zu entwickeln.

Digitalisierung in der Militärkommunikation: TCN und darüber hinaus

2023 markierte einen Meilenstein in der digitalen Militärkommunikation mit der Einführung des „Tactical Communication Network (TCN)". Diese Initiative transformierte die Kommunikationsfähigkeiten der Streitkräfte und führte zur Anpassung unserer Ausbildungsprogramme. Besonders beeindruckend war die Zahl der Absolventen: Insgesamt ca. 270 Offiziere, Unteroffiziere und zivile Bedienstete durchliefen erfolgreich unsere neu strukturierten TCN-Kurse, was unsere Effizienz und Wirksamkeit in der Ausbildung unterstreicht. Der spezialisierte Lehrgang „Kdt IKTZg", der derzeit entwickelt wird, ist eine weitere Innovation, die auf die anspruchsvollen Herausforderungen im digitalen Einsatzraum abzielt.

Cybersicherheitsübung der Wiener Netze mit Experten der Dion6

Cybersicherheit: FüUS als maßgeblicher Akteur

Die FüUS spielte 2023 eine entscheidende Rolle bei der Cybersicherheitsübung unseres Partners der Wiener Netze. Revident Markus Prosser, ein herausragende Experte für Cybersicherheit aus unseren Reihen, trug wesentlich zum Erfolg dieser wichtigen Übung bei, die die Aufrechterhaltung kritischer Infrastrukturen in Krisenszenarien simulierte. Die Kompetenz und das Fachwissen des FüUS-Mitarbeiters in der Handhabung komplexer Cyber-Bedrohungen verdeutlichten einmal mehr die führende Rolle unserer Schule in der modernen Kommunikationssicherheit. Der gegenseitige Wissensaustausch mit unseren zivilen Partnern hilft, zukünftige Herausforderung gemeinsam zu meistern.

Auswirkungen auf den Ausbauplan 2032+

Im Zuge des Aufbauplans 2023+ erfährt die Führungsunterstützungsschule einen Zuwachs an Kompetenzen, welche sowohl in personeller als auch in materieller Hinsicht große Chancen bietet. Die neuen Institute „Information Operation" und „Geowesen & Space" erweitert die Fähigkeiten der Schule in neuen Waffengattungen, eine zusätzliche Führungsunterstützungskompanie soll den reibungslosen Betrieb, die geforderte Ausbildung und den notwendigen Kaderaufwuchs gewährleisten.

Dadurch kann auch die Einsatzorganisation unterstützt werden. Der Gewinn von qualifiziertem Kader stellt somit eine Priorität für die kommenden Jahre dar um die Herausforderungen der Zukunft im Österreichischen Bundesheer in den vielfältigen Aufgabengebieten meistern zu können.

Foto: pixabay.com

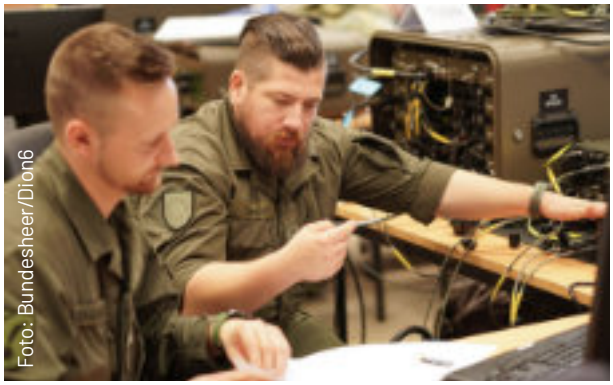


Foto: Bundesheer/Dion6

Übungsnetzwerkaufbau der FüUS

Die benötigte Infrastruktur mit modernsten Ausbildungsanlagen stellt eine Voraussetzung für eine qualitativ hochwertige Fortbildung dar. Die Führungsunterstützungsschule kann dadurch noch mehr Fachwissen in der Ausbildung bereit stellen und das Personal für die anspruchsvolle Arbeit im Fachgebiet vorbereiten.

Ein Jahr des Fortschritts und der Innovation

Das Jahr 2023 war ein Meilenstein in der Geschichte der Führungsunterstützungsschule. Mit beispielhaften Leistungen in der EloKa-Ausbildung, revolutionären Entwicklungen in der digitalen Militärkommunikation und einer Schlüsselrolle in der Cybersicherheit hat die FüUS ihre Stellung als Innovationsführer und Kompetenzzentrum eindrucksvoll unter Beweis gestellt. Wir freuen uns darauf, diese Erfolge in den kommenden Jahren weiterzuführen und die Zukunft der militärischen Ausbildung aktiv zu gestalten.

Führungsunterstützungsseminar für Offiziere

Das diesjährige FüU- Seminar für Offiziere hat neue Maßstäbe in der Weiterentwicklung militärischer Fähigkeiten gesetzt. Im Mittelpunkt standen innovative Entwicklungen in den Bereichen Informations- und Kommunikationstechnologie, Elektronische Kampfführung und Cyber. Das Schwergewicht des Seminars lag dabei auf der Entwicklung neuer Fähigkeiten in diesen Fachbereichen, der Weiterentwicklung des Planungsverfahrens Führungsunterstützung und dem Vergleich der Systeme unserer Partnernationen.

Hotspot: Starhemberg- Kaserne

Generalmajor Hermann Kaponig eröffnete das Seminar mit einem umfassenden Überblick über die Entwicklungen innerhalb der Dion 6, einer Schlüsselkomponente der Cybersicherheitsstrategie des ÖBH. Sein Vortrag betonte die Wichtigkeit der ständigen Anpassung und Verbesserung der Cyberfähigkeiten im Militär. Ein weiteres Schlüsselelement des Seminars war die Herausforderung der Cybertruppe, präsentiert von Milizexperte Marco Petrovic von der ÖBB. Seine Einblicke in die Cybersicherheit, basierend auf seinen Erfahrungen in verschiedenen Großunternehmen, beleuchteten die Komplexität und Wichtigkeit dieser.

Die Einführung des Tactical Data Radio (TDR) durch ObstdG Treiblmaier (IKCyPl) markierte einen entscheidenden Schritt in der Verbesserung der IKT-Fähigkeiten des ÖBH. Die Einführung des TDR ist die nächste Erweiterung im IKT System des ÖBHs und schließt die Fähigkeitslücke der mobilen breitbandigen (Anhalt 1 Mbps) Datenübertragung im taktischen Bereich. In mehreren Workshops mit drei Gruppen wurden praktische Einsatzkonzepte für das TDR entwickelt, die dessen Bedeutung für die mobile Datenübertragung im taktischen Bereich unterstrichen.

Workshop zur Entwicklung des TDR

Internationale Perspektiven wurden durch die Beiträge der Schweizer Armee und der deutschen Bundeswehr ergänzt. Oberstleutnant Christoffel Cadosch und Hauptmann Stefan Meltzner (ITSBw) boten wertvolle Einblicke in ihre nationalen IKT- und Cybersicherheitssysteme, die einen Vergleich der verschiedenen Ansätze und Technologien ermöglichten.

E-Learning in der Deutschen Bundeswehr

Hauptmann Stefan Meltzner von der Deutschen Bundeswehr bot einen Einblick in die Transformation der militärischen Ausbildung im digitalen Zeitalter. Er skizzierte die frühere Trennung von Fern- und Präsenzausbildung sowie die damals begrenzte mobile IT-Ausstattung. Mit dem Jahr 2020 begann ein bedeutender Wandel: Die ITSBw baute eine flexible IT-Infrastruktur auf, erweiterte die Netzinfrastruktur, führte kollaboratives Arbeiten und Videokonferenztools ein und implementierte Lernmanagementsysteme.

Ab 2022 stand die Ausbildung des Lehrpersonals und die Etablierung der neuen Systeme im Mittelpunkt. Hptm Meltzner betonte die Bedeutung einer stabilen IT-Netzinfrastruktur und moderner Anwendungen für die Ausbildung. Besonderer Wert wurde auf ortsunabhängige Verfügbarkeit und die Erstellung moderner Ausbildungshilfsmittel gelegt. Ein Kernpunkt war "Link and Learn" für Soldaten, unterstützt durch verschiedenste Systeme.

Die Förderung lebenslangen Lernens und die Qualifizierung der Ausbilder in Medienkompetenz und digitaler Kompetenz waren ebenfalls zentrale Themen. Hptm Meltzner hob hervor, wie durch E-Learning projektorientierte Szenarien und selbstorganisiertes Lernen bereichert werden. Die ITSBw bietet u.a. Kurse in Bereichen wie IT-Sicherheit, Kryptoverwaltung, Wehrrecht und IT-Management an.

Der Vortrag zeigte die entscheidende Rolle der ITSBw in der digitalen Transformation der militärischen Ausbildung und die Vorbereitung der Soldaten auf moderne Kriegsführung.

Übungsnetzwerk TDR

Digitalisierung der Schweizer Streitkräfte

Die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS), sieht vor, dass alle Beteiligten im Cyberbereich in der Lage sein sollten, sich selbst zu schützen. Oberstleutnant Cadosch von der Schweizer Armee stellte das Programm „Fitania“ vor. Dieses Programm stellt einen Meilenstein in der Digitalisierung der Schweizer Streitkräfte dar und zielt darauf ab, die Armee mit modernen Informations- und Kommunikationstechnologien (IKT) auszustatten. Es ist vorgesehen, dass die Mehrheit der Bataillone und Kompanien in der Lage sein wird, eigenständige Operationen in diesen Bereichen durchzuführen. Sie sollen mit Systemen ausgestattet werden, die leicht zu bedienen sind, um den funkbasierten Informationsaustausch des Feindes in ihrem Operationsgebiet selbstständig zu stören und die Führungskapazität des Gegners auch auf einer taktischen Ebene zu schwächen.

FH-Bachelorstudiengang und Cyber Range

Oberst des Generalstabes Kunovjanek und Oberstleutnant des Generalstabes Treiblmaier stellten den FH-Bachelorstudiengang "Militärische informations- und kommunikationstechnologische Führung" vor und berichteten über erste Erfahrungen aus der Lehre sowie die ersten Eindrücke der Cyber Range.

Als Cyber Range bezeichnet man eine virtuelle Trainingsumgebung, die für den Bereich der Cyber-Sicherheit entwickelt wurde. Sie ermöglicht es, realistische Cyber- Angriffsszenarien zu simulieren und Gegenmaßnahmen zu üben, ohne dabei echte Daten oder Systeme zu gefährden.

Das Besondere hierbei ist, es können sowohl offensive als auch defensive Fähigkeiten trainiert werden, um im Falle eines Cyber-Angriffs schnell und effektiv reagieren zu können.

Die Cyber Range ist eine wichtige Ergänzung für Ausbildungen und militärischesTraining, da der Cyber-Krieg zunehmend eine Bedrohung für die nationale Sicherheit darstellt. Durch die Cyber Range kann die Reaktionsfähigkeit verbessert werden es ermöglicht dem ÖBH, neue Technologien und Taktiken zu testen, bevor sie in der realen Welt eingesetzt werden.

Insgesamt ist die Cyber Range ein wichtiger Bestandteil des militärischen Trainings und ein wesentlicher Beitrag zur nationalen Sicherheit. Es bietet den Soldaten eine realistische und sichere Umgebung, um ihre Fähigkeiten in der Cyber-Verteidigung und -Kriegsführung zu verbessern und das Militär auf die Herausforderungen des modernen Krieges vorzubereiten.

Fazit

Das Seminar endete mit einem Kameradschaftsabend, der den Teilnehmern die Möglichkeit bot, sich in einem informellen Rahmen auszutauschen und Netzwerke zu pflegen. Diese Veranstaltung betonte die Notwendigkeit der fortlaufenden Weiterbildung und Anpassung an neue Technologien im militärischen Bereich, um den sich ständig verändernden Herausforderungen gerecht zu werden.

Die Zusammenarbeit über nationale und institutionelle Grenzen hinweg und die Integration innovativer Ansätze in die militärische Ausbildung sind essentiell in einer Zeit rascher technologischer Fortschritte, wo das menschliche Element ein entscheidender Faktor für die Effektivität und Anpassungsfähigkeit der Streitkräfte bleibt.

Führungsunterstützungsbataillon 1 - FüUB1

Leiter: Oberst Ernst Berthold, MSD

Hervorzuhebende Aktivitäten

Das Jahr 2023 war für das Führungsunterstützungsbataillon 1 in vielerlei Hinsicht ein sehr forderndes. Zusammengefasst kann jedoch resümiert werden, dass die gestellten Aufgaben und Aufträge abgearbeitet und die gesteckten Ziele erreicht wurden.

Ein großes Thema im Bataillon war 2023 die Auslieferung der neuen Systeme für das verlegbare Fernmeldenetz TCN (Tactical Communication Network). Die ersten Kompanien wurden ausgebildet und das Gerät befindet sich im Bataillon. Die letzte Kompanie folgt im ersten Quartal 2024 womit das Bataillon dann voll ausgestattet sein wird. Auch die Arbeiten der Elektronik-Instandsetzung als Vorrüstwerkstätte verlaufen planmäßig. Damit ist dann das Bataillon im Bereich der verlegbaren IKT Systeme auf dem neuesten Stand der Technik und bereit für die Einsätze der nächsten Jahre.

Ein Schwergewicht im Bereich Übung und Einsatzvorbereitung des Bataillons war sicherlich die Durchführung der Multinationalen IKT Übung „Common Roof 23" bei der das Bataillon nicht nur den österreichischen Anteil stellen durfte, sondern auch mit der Gesamtleitung (dem Lead) der Teile der Deutschen Bundeswehr und der Schweizer Armee beauftragt war. Dies bedeutete nicht nur die Vorbereitung, Durchführung und Nachbereitung der vorgesehenen Planungskonferenzen inklusive Lessons Identified und Lessons Learned Prozess wahrzunehmen, sondern auch die multinationale Überwachung und Steuerung der jeweiligen nationalen Netze mittels einer zentralen, multinational besetzten Betriebssteuerungszentrale.

Die Erkenntnisse, welche gewonnen werden konnten, erweisen sich für das zukünftige Servicemanagement, insbesondere im Zusammenhang mit TCN als sehr wertvoll. Der Auftrag an das FüUB1 zur Durchführung der Common Roof 24 wurde bereits erteilt und ich freue mich, die gewonnenen Erfahrungen umzusetzen und den Prozess weiter voran zu treiben.

Foto: Bundesheer/Dion6

Ein besonderer Meilenstein für das Jahr 2024 wird auch die Großübung „Schutzschild24" im Juni sein, in Zuge derer seit langem wieder im Brigade- und Militärkommandorahmen militärische Verfahren geübt werden können.

Sehr erfreulich ist auch die Tatsache, dass die Athleten des FüUB1 bei militärischen sportlichen Wettkämpfen wieder beachtliche Ergebnisse eingefahren haben, darunter mehrere Heeresmeister- und Vizemeistertitel beim Schießen mit Pistole und Sturmgewehr sowie im militärischen Orientierungslauf.

Im Bereich Personalgewinnung, Personalplanung und Personalsteuerung sind wir in der glücklichen Lage mit einem Besetzungsgrad von über 80% auch in dieser Hinsicht für die Zukunft sehr gut ausgestattet zu sein.

Die Soldaten und Soldatinnen des FüUB1 sind somit für kommende Aufgaben gerüstet und bereit die geforderten Aufträge getreu unserem Motto „schnell-flexibel-sicher" durchzuführen.

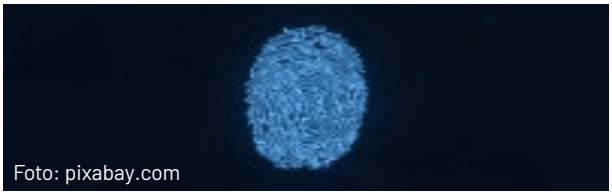


Foto: pixabay.com

Luftraumsicherungsoperation - DAEDALUS23

Ein schon fast traditioneller Jahresauftakt ist die Teilnahme an der Übung DAEDALUS für das FüUB1. Vom 09 01 bis zum 22 01 23 unterstützten die Villacher Cybersoldaten die Luftraumsicherungsoperation.

Vom 16 01 bis 20 01 23 fand das jährliche Treffen der privatrechtlichen Stiftung „World Economic Forum" (WEF) in Davos (Schweiz) statt. Dies bildete das Schwergewicht während der Übung. Insgesamt waren etwa 1000 Soldaten im Einsatz. Diese verteilten sich über das gesamte Bundesgebiet. Das Hauptaugenmerk lag jedoch im Einsatzraum Tirol und Vorarlberg über welchen ein Flugbeschränkungsgebiet errichtet wurde. Das Bundesheer überwachte den Luftraum mit mehreren Luftfahrzeugen die zur Patrouille, als Funkrelais oder als Emergency Response Team (ERTA-Luftbewegliche Ersthelfer) eingesetzt wurden. Weiters war ein ELDRO-Element zur elektronischen Drohnenpeilung und -abwehr in Zeltweg eingebunden.

Eine Verstärkung der passiven Luftraumüberwachung (LRÜ) wurde durch den Einsatz von Aufklärungs- und Zielzuweisungsradaren (AZR), Sensoren der Flugabwehr und eines Visual-Reporting-Team (VRT) erreicht.

Funktrupp bei der DAEDALUS23

Die 3. Führungsunterstützungskompanie erhielt den Auftrag, das angeforderte Netz der Übung zu errichten, zu betreiben und zu halten. Die 3. Kompanie verlegte mit 61 Soldaten in den Einsatzraum und errichtete unter anderem einen Gefechtstand in Tirol. Die eingesetzten Richtfunktrupps und Knotenvermittlung stellten das befohlene breitbandige Datennetz, über welches notwendige Messdaten des AZR für die Luftraumüberwachung und sonstige wichtige Informationen ausgetauscht wurden. Die Cybersoldaten konnten alle gestellte Aufträge friktionslos erfüllen, das Niveau der Vorjahre halten und leisteten damit einen wesentlichen Beitrag zum erfolgreichen Übungsverlauf.

Funktrupp bei der DAEDALUS23

Girls Day

Stillgestanden - hieß es am 27 04 23 für junge Frauen, die sich beim Heerespersonalamt für den Schnuppertag beim Bundesheer - also zum Girls Day - gemeldet haben. Bei wechselhaften Temperaturen und windigem Wetter ließen es sich die angemeldeten Frauen nicht nehmen, den Soldatenalltag und das Kasernenleben aus erster Reihe kennen zu lernen. Der „Girls Day" - eine gezielte Personalwerbeaktion für Frauen, welcher federführend durch das Heerespersonalamt beworben wurde, fand heuer in der Khevenhüllerkaserne in Klagenfurt statt.

Girlsday beim FüUB1

Der Girls Day hat den Zweck, Frauen gezielt über Karrieremöglichkeiten im Bundesheer zu informieren und mögliche Laufbahnen im Offiziers- und Unteroffiziersbereich aufzuzeigen bzw. zu erörtern. Zusätzlich soll ein Impuls gesetzt werden, der eine Trendwende bei der Berufsorientierung von Mädchen unterstützt und ihnen einen neuen Einblick auf die Berufswelt eröffnen soll. Dieser Tag versteht sich mitunter als integrativer Aktionstag, der auf einen sehr handlungs- sowie erlebnisorientierten und damit nicht zuletzt auch emotionalen Zugang setzt und damit Mädchen Mut auf die Eroberung neuer Berufsfelder machen will.

Ergänzend wurden den jungen Damen der militärische Dienstbetrieb und der Soldatenalltag näher vorgestellt, da Frauen normalerweise keinen oder sehr eingeschränkten Kontakt zur Organisation Bundesheer haben.

Beim diesjährigen Girls Day stellten unterschiedliche Waffengattungen ihre Vorzüge den Teilnehmerinnen vor und brachten den jungen Frauen die jeweilige Waffengattung näher.

Die Soldaten des FüUB1 betrieben die Station Führungsunterstützung und vermittelten den Besucherinnen die aktuellen Kommunikationsmöglichkeiten mit verschiedensten Kommunikationsmedien und Kanälen. Somit hatten die Teilnehmerinnen über den gesamten Tag verteilt die Möglichkeit Kommunikationstechnologie auszuprobieren und sich über die Leistungsfähigkeit unseres Cyberverbandes entsprechend zu informieren.

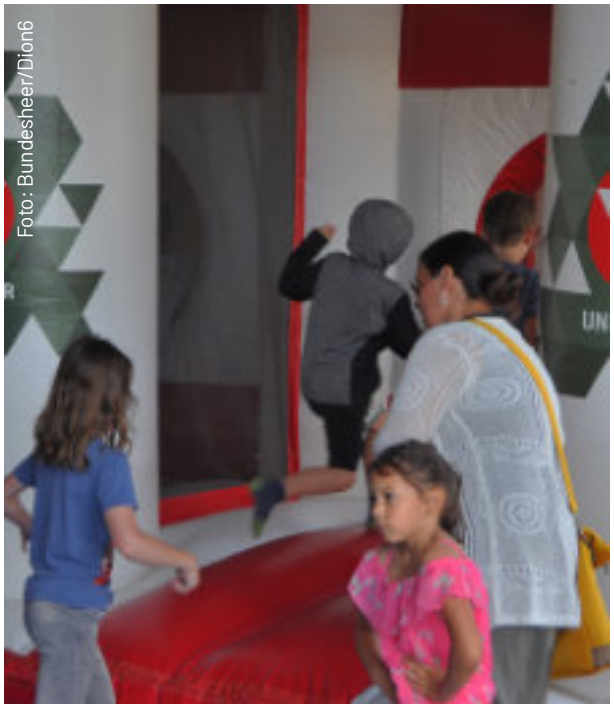
Am Ende des Tages hatten Interessentinnen für den Soldatenberuf die Möglichkeit sich speziell und individuell vom Heerespersonalamt beraten zu lassen.

Stand am Girlsday beim FüUB1

Tag der Schulen beim FüUB1

Auch heuer veranstaltete das Militärkommando Kärnten unter der Federführung der Villacher Cybersoldaten einen Tag der Schulen. Die Schülerinnen und Schüler, sowie das Lehrpersonal bekamen dabei einen Einblick in den Soldatenalltag. Am Dienstag, dem 04 07 23 waren von 0800 bis 1430 Uhr die Türen der Lutschounig-Kaserne in VILLACH geöffnet. Der Tag der Schulen dient dazu, der Kärntner Schuljugend einen Überblick über die Aufgaben, Ausbildung, Ausrüstung und Ausstattung des Bundesheeres zu geben.

Dieser Tag versteht sich deshalb auch als ein Impuls für Schüler bei der zukünftigen Berufsorientierung. Er soll den Besuchern neue, interessante Einblicke in die soldatische Berufswelt und deren Breitbandigkeit eröffnen. Somit versteht sich dieser Tag mitunter als integrativer Aktionstag, der auf einen sehr handlungs- sowie erlebnisorientierten und damit nicht zuletzt auch emotionalen Zugang setzt und damit jungen Menschen Mut auf die Eroberung dieses Berufsfelds machen will.



Parkour beim Tag der Schulen beim FüUB1

Neben diversen Informationsständen zum Thema gab es für unsere jungen Gäste in den Kasernen auch eine Kostprobe aus der Truppenküche. Cybersoldaten inklusive dem System Cybershelter, Infanterie, schwere Lastsysteme, Pioniergerät, Informationen zur umfassenden Lehrlingsausbildung beim Heereslogistikzentrum sowie Leistungssportler des Heeressportzentrums eröffneten einen umfassenden Einblick in viele Tätigkeiten beim Bundesheer.

Die Soldaten des FüUB1 betrieben neben einem Informationsstand Cyber auch das virtuelle Duellsystem Cyber Escape Room, bei dem 8 Spieler gegeneinander interaktiv antreten können, und vermittelten den interessierten Gästen die aktuellen Kommunikationsmöglichkeiten im Kurzwellen, Ultrakurzwellen und Richtfunkbereich mit verschiedensten Kommunikationsmedien und Kanälen.

Somit hatten die Teilnehmer über den gesamten Tag verteilt die Möglichkeit verschiedenste Fernmeldegerätschaften auszuprobieren und sich über die Leistungsfähigkeit des Cyberverbandes entsprechend zu informieren.

Umrahmt wurde die Veranstaltung akustisch von der Militärmusik Kärnten und von einem Stand der Antenne Kärnten, welche den interessierten Schülern die Möglichkeit gab, Livemoderationen durchzuführen somit in die Welt des Mediums Radio näher einzutauchen.

Rätsellösen im CyberEscapeRoom

Führungsunterstützungsbataillon 2 - FüUB2

Leiter: Oberst Johannes Nussbaumer, MSD

Das Jahr 2023 war in erster Linie von einer sehr hohen Auftragslage gekennzeichnet. Bei zahlreichen Übungen und Einsätzen, sowohl im Inland wie auch im Ausland, konnten die Spezialisten des FüUB2 als Force Provider Cyberkräfte im IKT- und im EloKa-Bereich ihre Expertise zur erfolgreichen Auftragserfüllung der Bedarfsträger einbringen.

Von 09 01 – 23 01 2023 war die 1. FüUKp im Rahmen der Luftraumsicherungsoperation DÄDALUS23 im Bundesland Vorarlberg eingesetzt. Anlässlich des Weltwirtschaftsforum in Davos (Schweiz) wurde ein Flugbeschränkungsgebiet über Teilen Westösterreichs errichtet. Mittels mobiler Radarstationen, Feuerleitgeräten und Flugmeldetrupps wurden alle Vorgänge in der Luft vom Boden aus überwacht. Die dabei gewonnenen Daten wurden über die mobilen und verlegbaren Fernmeldesysteme der eingesetzten FüU-Kompanien direkt in die Einsatzzentrale Basisraum nach St. Johann/Pg übertragen. Damit konnte mit unseren präsenten IKT-Kräften eine kompetente Unterstützung zur Bereitstellung des aktuellen Luftlagebildes gewährleistet werden.

Am 10. Mai 2023 wurde dem FüUB2 das staatliche Gütezeichen „familienfreundlicher Arbeitgeber 2022/23" durch Frau Bundesministerin MMag. Dr. Susanne Raab im Palais Berg in Wien verliehen. Das ÖBH steht vor der Herausforderung, sich als Arbeitgeber am Arbeitsmarkt attraktiv positionieren zu müssen, um die qualitative und quantitative personelle Befüllung nachhaltig sicherstellen zu können.

Übergabe des Gütezeichens „Familienfreundlicher Arbeitgeber"

Ein positives Argument im Rekrutierungsprozess ist die Vereinbarkeit von Beruf und Familie, da dies Umfragen zufolge für die aktuelle Generation ein wesentlicher Beurteilungsfaktor in der Auswahl der beruflichen Tätigkeit darstellt. Das Audit „berufundfamilie" ist ein maßgeschneidertes Instrument zur Implementierung, Überprüfung und Weiterentwicklung einer familienbewussten Personalpolitik in Unternehmen aller Branchen. Aufgrund des Standortes abseits eines Ballungsraumes und der steigenden regionalen Lebenskosten steht das FüUB2 vor der Herausforderung, neue Mitarbeiter zu gewinnen und diese in der Organisation zu halten. Ein besonderes Anliegen ist die Erhöhung der Attraktivität für Arbeitskräfte durch eine familienbewusste Personalpolitik, welche die Vereinbarkeit von Familie und Beruf ermöglicht. Diese Zertifizierung wird somit als wichtiges Instrument zur Personalgewinnung angesehen und das FüUB2 wird sich intern und extern als moderner, flexibler und attraktiver Arbeitgeber präsentieren.

Das FüUB2 war im Jahr 2013 letztmalig im Verbandsrahmen in eine Großübung involviert. Mit der Übung STEINFELD 23 bot sich für uns als Force Provider ein perfektes Umfeld um die übende Truppe fachgerecht zu unterstützen. Von 3. bis 14. Juli nahm das FüUB2 mit dem BKdo, Teilen der StbKp, der präsenten 3. FüUKp und der EloKaKp an der Abschlussübung STEINFELD23 der TherMilAk

Foto: Bundesheer/Dion6

in den Bezirken Wiener Neustadt und Neunkirchen teil. Das FüUB2 hat für diese Übung das gesamte Führungsnetz geplant, errichtet und betrieben. Dazu wurden über zwei Truppenanschaltekästen und mittels einer Mehrkanalsatellitenanlage die Übergänge ins ortsfeste Fernmeldesystem sichergestellt und durch den Einsatz von mobilen und verlegbaren Systemkomponenten ein Sprach- und Datennetz für die Führung der eingesetzten Verbände bereitgestellt.

Für die Überwachung des elektromagnetischen Spektrums setzten wir die Experten unserer EloKa-Kompanie ein, welche mit dem neuen Erfassungs- und Ortungssystem den Truppenfunk überwachen, orten und auswerten konnten. Für uns als Force Provider Cyberkräfte ergab sich ein hoher Benefit auf allen Ebenen und wir konnten viele Lessons Identified in Lessons Learned umsetzen. Insbesondere der Einsatz des Systems war enorm wichtig für die Optimierung der Verfahren zur Aufbereitung des elektromagnetischen Umfeldes und der Generierung des Lagebildes.
Die Auswertung der gewonnenen Erfahrungen sind wichtige Meilensteine für die Implementierung des Systems im ÖBH.

Im Zeitraum 23 10 bis 03 11 2023 fand am Truppenübungsplatz Hochfilzen das trinationale Übungs- und Testvorhaben ALPINE JAM 23 statt.

An dieser Übung nahmen Fachkräfte der elektronischen Kampfführung aus Österreich, Deutschland und der Schweiz teil. Das Hauptaugenmerk lag in der Verbesserung der Einsatzbereitschaft der CREW-Systeme (Countering Radio Controlled Improvised Explosive Devices – Electronic Warfare) und dem Austausch von Erfahrung und Wissen der einzelnen Länder und diente auch als Vorbereitung für die Teilnahme an der THORS HAMMER 2024, einer Übung für elektronische Maßnahmen gegen funkgezündete improvisierte Sprengkörper.

Übungsteilnehmer ALPIN JAM

Aufstellung der Truppe

Dadurch konnte unsere EloKa-Kompanie die eigenen Force Protection Systeme weiter optimieren, die Effektivität und Kompatibilität verbessern und Testungen zur Abwehr von Drohnen im Partnerverbund durchführen.
Die EU-BATTLEGROUP 2025 besteht aus einem infanteristischen Kampfverband und einer Medical Task Force unter deutscher Führung, sowie dem Logistikverband (= CSSBN) unter österreichischer Führung. Die 3. JgBrig ist das formierungsverantwortliche (fv) Kommando für das CSSBN und das FüUB2 ist fv Kdo für die FüUKp, in welcher bestens ausgebildete KIOP/K-PE-Soldaten eingeteilt sind.

Diese FüUKp/KPE führte im letzten Quartal noch einige gemeinsame Übungen durch, um die Zusammenarbeit innerhalb der Organisationselemente bzw. die Weiterentwicklung der Fertigkeiten der KPE-Soldaten zu verbessern.

Dazu fand ein TCN-Workshop in der 42.KW, eine Formierungsübung in der 45.KW und eine TCN-Betriebsübung in der 46.KW statt. Die Schwergewichte dabei waren:
Einrichten von Gefechtsständen am COLPRO-Zeltsystem, Netzeintritt über einen Truppenanschaltpunkt (TAP) sowie über Mehrkanalsatellitensystem, Koordinierung und Überwachung durch die Netzsteuerung und Ausbildung im Bereich Kurzwelle.

Durch dieses Training am neuen Gerät und das Üben von gefechtstechnischen und betrieblichen Abläufen wurde die Sicherheit im Umgang mit neuen Systemen geschaffen und die ausbildungsmäßige Einsatzbereitschaft hergestellt.

Rekrut des Jahres Gfr Michael Bogensberger (2.v.l.)

Das FüUB2 stellte mit dem Gfr Michael Bogensberger den Salzburger „Rekruten des Jahres". Er entwickelte für die EloKaKp mit der „Aufbauplatz App" eine digitale Plattform, um Informationen über günstige Erfassungs- und Peilstandorte zu dokumentieren. Die Software ist genau auf die Bedürfnisse der EloKaKp zugeschnitten, ist direkt auf ihren IT-Systemen implementiert und könnte sogar die Bereiche Funk und Richtfunk integrieren. Diese bemerkenswerte Leistung zeigt, wie junge Talente im Bundesheer genutzt und gefördert werden können, um moderne und effiziente Lösungen zu entwickeln, die den täglichen Betrieb und die Sicherheit der Truppen verbessern.

Die Bediensteten des FüUB2 überzeugen nicht nur durch ihre Fachkompetenz im Bereich IKT und EloKa, sondern immer wieder auch in sportlichen Belangen. Frau StWm Sylvia Steiner von der StbKp/FüUB2 beeindruckte die Konkurrenz bei der Weltmeisterschaft im Schießen in Baku. Die Pistolenschützin sicherte sich die Goldmedaille im 50 m Bewerb, nachdem sie bereits eine Bronzemedaille im 25m Bewerb mit der Standard Pistole gewonnen hatte.

Goldmedaille für Frau StWm Sylvia Steiner (Mitte)

Das FüUB2 stellte zwei Mannschaften für die zehnte Auflage des Gebirgswettkampfes „EDELWEISS RAID" von 27 02 bis 03 03 2023 in den Tiroler Tuxer Alpen. Die Edelweiss Raid ist ein internationaler, militärischer Spezialwettkampf für Gebirgsjäger weltweit.

Die teilnehmenden Wettkampfteams kamen aus Bulgarien, China, Deutschland, Polen, Rumänien, Schweiz, Tschechien, den USA und Österreich. Die Soldaten des FüUB2 erreichten dabei den hervorragenden 4. Platz mit der Mannschaft 1 und den 17. Platz mit der Mannschaft 2. Ich bin überaus stolz, solche Leistungsträger in meinen Reihen zu haben.

Foto: Bundesheer/Dion6

Teilnehmer EDELWEISS RAID

Auswirkungen Aufbauplan 2032+

Gemäß Aufbauplan ÖBH 2032+ ist bis 2028 die Aufstellung einer EloKaKp sicher zu stellen. Daher ist der begonnene schrittweise Aufbau der FüUKp(eloKa) weiter fortzusetzen. Für den EloÜbwZg/FüUKp(eloKa) wären vier Erfassungs- und Ortungssysteme, zwei verlegbar in WA-Sheltern und zwei mobile Systeme in gehärteten Fahrzeugen (PANDUR EVO) zu beschaffen. Hier darf angemerkt werden, dass ein Peilverbund aus mindestens drei eingesetzten Erfassungs- und Ortungssystemen bestehen muss!

Mit diesen Beschaffungen kann eine hochqualitative arbeitsfähige, verlegbare Fähigkeit „Initial Operational Capability" der FüUKp(eloKa) bis Mitte 2024 hergestellt werden. Des Weiteren ist mit dem Aufbau von Electronic Attack-Kapazitäten zu starten, leistungsstarke Störsysteme sind zu beschaffen und in gehärtete Fahrzeuge (PANDUR EVO) einzubauen um eine „Full Operational Capability" der FüUKp(eloKa) zu erreichen.

Das verlegbare Fernmeldesystem (vlgbFMSys) erfährt mit der Umsetzung des Vorhabens TCN eine Totalerneuerung. Mit dem TCN steht das ÖBH im internationalen Vergleich im Spitzenfeld der digitalen Vernetzung. Im Zuge der derzeit laufenden Labor- und Feldtests soll ein mit dem TCN kompatibles und international interoperables TDR (Tactical Data Radio) als Ersatz für das in die Jahre gekommene Truppenfunksystem CONRAD „gefunden" werden. Damit soll der Grundstein für die Zusammenführung des mobilen Fernmeldesystems (mbIFMSys) mit dem vlgbFMSys gelegt werden. In weiterer Folge soll damit der Weg zu einer „Tactical Cloud" bzw. den NGN ÖBH (Next Generation Network ÖBH) unter Berücksichtigung der bereits getätigten Investitionen ermöglicht werden. Die nunmehrigen Budgetzahlen erlauben eine zweckmäßige und wirtschaftliche Planung und Realisierung im ÖBH bei den zukünftigen Herausforderungen Digitalisierung, Sensorintegration und militärische Nutzung von künstlicher Intelligenz.

Neben den materiellen Beschaffungen muss besonders das Personal im Fokus des Fähigkeitsaufbaues liegen. Als mittel- bis langfristig problematisch könnte sich jedoch die Personalentwicklung im Bereich des Offiziers- und, im Besonderen, des Unteroffiziersnachwuchses auswirken. Sowohl Einstiegszahlen als auch Ausstiege nach bereits abgeschlossener Grundausbildung haben ein bedenkliches Maß erreicht. Für den Erhalt bzw. den Ausbau der notwendigen Fähigkeiten und den Betrieb der in Beschaffung befindlichen hochtechnologischen Waffensysteme und Ausrüstungsgüter ist die Bereitstellung von hoch qualifiziertem Personal in der erforderlichen Quantität unabdingbar.

Initiativen & Kooperationen

Personalwesen der Zukunft

Da im IT-Bereich ein Mangel an Fachpersonal in allen Bereichen herrscht, ist das Match am Arbeitsmarkt sehr turbulent. Die Direktion 6 - IKT&Cyber hat erkannt, dass die offensive Information von Stellungspflichtigen über die Möglichkeit des CyberGWD, besonders an IT-orientierten Bildungseinrichtungen, von besonderer Bedeutung ist. Deshalb haben wir ab dem Jahr 2019 die Ausbildung von Informationsoffizieren stark forciert und es haben bisher 16 Informationsoffiziere die Ausbildung abgeschlossen.

Die Informationsoffiziere werden auf überwiegend IT-Bildungseinrichtungen entsandt, um über die Möglichkeit des CyberGWDs und den weiteren Verwendungsmöglichkeiten im Rahmen des Arbeitnehmerüberlassungsgesetz (AÜG), Militärperson auf Zeit (MZCh), Vertragsbediensteter (VB) und Richtverwendung IT (RiVIT) zu informieren.

Seit dem Ende der COVID-Pandemie 2021 sind unsere InfoOs bei 45 Info-Veranstaltungen an Informationstagen von HTLs mit Erfolg eingesetzt.

In den Anmeldungen zum Cybergrundwehrdienst ist dieses erweiterte Informationsangebot deutlich merkbar. Zu den Einrückungsterminen im Februar und Oktober gibt es jeweils 4x so viele Anmeldungen wie mögliche Plätze. Durch diese Menge an Bewerbern ist die Möglichkeit gegeben, auf das System „Best of the Best" zuzugreifen. Hier wählen die jeweiligen Bereiche und Abteilungen die Fähigkeiten die sie für ihre Aufgabenbewältigung benötigen genau aus, und entscheiden so welche Cybergrundwehrdiener sie zukünftig als Teammitglieder zur Seite gestellt bekommen.

Informationen Cyberkräfte

E-Mail Cybergrundwehrdienst

Foto: pixabay.com

Referat Personal

Im Jahr 2023 konnte Dion6 IKT&Cyber im Personalbereich einige Erfolge verzeichnen. Die Einführung des neuen Besoldungsschemas RIVIT Richtverwendung zeichnete erste Erfolge mit der Aufnahme von mehr als 40 Mitarbeitern auf einen RIVIT-Arbeitsplatz.

Die Kooperation mit der HTL-Spengergasse und dem Projekt FIT (Frauen in der Technik) erwies sich ebenso als erfolgreich. Im Zuge einer Informationsveranstaltung wurden den Teilnehmern die Möglichkeiten der unterschiedlichsten technischen Arbeitsplätze veranschaulicht. Daraus resultierend konnten nicht nur Ferialpraktikanten gewonnen werden, sondern auch neue Mitarbeiter. Der Frauenanteil in unserer Direktion konnte im letzten Jahr auf über 11 % angehoben werden.

Ein anderer Zugang erfolgte mit der Ausbildungskooperation mit dem BBRZ (Berufliches Bildungs- und Rehabilitationszentrum). Über diese Kooperation konnten ebenfalls mehrere Bedienstete innerhalb der Direktion 6 - IKT&Cyber Fuß fassen. Im Jahr 2023 konnten über 110 Aufnahmen verzeichnet werden. Denen gegenüber stehen ca. 40 Abgänge.
Ein weiterer wichtiger Aspekt der Direktion 6 - IKT&Cyber ist die kontinuierliche Ausbildung des Personals.

Foto: Bundesheer/Dion6

Cyber Experten der Direktion 6 - IKT&Cyber

Ausbildung und Miliz

Die Aus- Fort- und Weiterbildung der Bediensteten der Dion6 ist von enormer Wichtigkeit um permanent auf dem letzten Stand des Wissens und der Technik zu sein und somit die Einsatzfähigkeit hoch zu halten.

Im Zuge dessen besuchten im Jahr 2023 237 Mitarbeiter Ausbildungen an zivilen Ausbildungsstätten im Inland und 70 Mitarbeiter Ausbildungen im Ausland.

Weiters wurden unter anderem an mil. Ausbildungsstätten 23 Ausbildungen in Kooperation mit ausländischen Streitkräften durchgeführt. Man sieht daher, dass die Liste an Ausbildungen und -Ausbildungsmöglichkeiten in der Direktion 6-IKT&Cyber mannigfaltig sind und immer an den aktuellen Stand der Technik angepasst werden.

Öffentlichkeitsarbeit

Die Dion6 war im Jahr 2023 in der Öffentlichkeitsarbeit sehr aktiv und hat eine Vielzahl an Veranstaltungen besucht. Ziel war es, Werbung für den Cyber-Grundwehrdienst zu machen, Personal für die technischen Bereiche zu werben sowie das Image der Cyberkräfte zu fördern. Die Highlights des Jahres waren das Wiener Donauinselfest, die Level-Up Gaming Messe in Salzburg, die IKT-Sicherheitskonferenz in Linz, der Nationalfeiertag und die Auszeichnung des ehemaligen Cyber-Grundwehrdieners Gfr Benjamin Borenich zum Wiener Grundwehrdiener des Jahres.

HTL Besuche

Im Zuge der aktiven Personalwerbung und Präsentation der Direktion 6 - IKT&Cyber als attraktiven und innovativen Arbeitgeber wurden 2023 mehrere HTLs mit IKT-Schwerpunkt in Wien und Umgebung besucht.
Cyber-Grundwehrdiener der Direktion 6 IKT&-Cyber unterstützten bei diesen Veranstaltungen tatkräftig das Team der InfoOps&opKomm und den Informationsoffizieren.

HTL Spengergasse

Die Partnerschaftspflege mit der HTL Spengergasse konnte mit mehreren gemeinsamen Veranstaltungen gepflegt werden. Am Firmeninformationstag 23 der HTL Spengergasse am Donnerstag, 23. März 2023 war das Interesse am Österreichischen Bundesheer und im speziellen der Direktion 6 - IKT&Cyber sowohl von den Schülern aller Abteilungen und dem Lehrpersonal sehr hoch.

Informationskräfte beim FIT HTL Spengergasse

SPENGERGASSE
ausbildung mit zukunft

Foto: HTL Spengergasse

Logo HTL Spengergasse

HTL Hollabrunn Emergency Day 23

Bei dem "Emergency Day" der HTL Hollabrunn wurde der Fokus auf das Thema Blackout gesetzt. Ziel ist, den Schülerinnen und Schülern verschiedene Aspekte eines Blackouts näher zu bringen und die Einsatzorganisationen, deren Ausrüstung und Möglichkeiten bei Blackouts und darüber hinaus vorzustellen.

Neben zahlreichen Blaulichtorganisationen aus dem Umfeld wurde von einer Abordnung des ÖBH aus Mistelbach beim Stationsbetrieb die operative Ausrüstung des Bundesheeres und diverse Karrieremöglichkeiten vorstellen.

Cyber EscapeRooms bei der HTL Hollabrunn

Die Direktion 6 - IKT&Cyber war mit den Cyber-EscapeRooms vertreten, um den Schülerinnen und Schülern spielerisch die Auswirkungen eines Hacker-Angriffs sowie eines darauffolgenden Blackouts näherzubringen. Anschließend wurde bei einer Nachbesprechung auf kritische IKT Fehler im modernen Alltag hingewiesen.

Weiters wurde unter anderem die Firmeninformationstage und Karriere Tage der HTLs Wien West, TGM, Donaustadt, St. Pölten und Wiener Neustadt besucht. Auch dort war das Interesse am Österreichischen Bundesheer und der Direktion 6 - IKT&Cyber sehr hoch.

2023 hat gezeigt, dass die Initiative zur Ausbildung von Cyber-Informationsoffizieren erste Erfolge bringt und es deshalb geplant ist, auch 2024 weitere Informationsoffiziere auszubilden.

Foto: HTL Hollabrunn

htl Hollabrunn

Logo HTL Hollabrunn

Team des Cyber EscapeRooms beim Donauinselfest23

Donauinselfest

Vom 23. - 25. Juni 2023 fand auf der Wiener Donauinsel das "Donauinselfest", das größtes OpenAir-Festival weltweit, zum 40. Mal statt.

Das Bundesheer präsentierte sich in einem eigenen Action&Fun Bereich, die Direktion 6 - IKT&Cyber stellte hierbei die beiden neuen Cyber EscapeRooms einem breitem Publikum vor.

Unter Anderem wurden die Cyber EscapeRooms von FBM Mag.[a] Klaudia Tanner, dem Militärkommandanten von Wien Bgdr Mag. Kurt Wagner, Bundesparteivorsitzender der SPÖ Andreas Babler sowie Wiens Bürgermeister Michael Ludwig besucht und von Info-Offizieren der Dion6 in die Möglichkeiten des Cyber EscapeRooms eingewiesen.

Alle Spielteilnehmer waren vom Cyber Escape Room begeistert, egal ob sie als Sieger oder Zweitplazierte aus dem Spiel gingen.

LevelUp vom 01.07. - 02.07. in Salzburg

Zum zweiten Mal fand heuer im Messezentrum Salzburg die "Level UP" statt. Federführend durch die Direktion 6 - IKT&Cyber war das Österreichische Bundesheer mit dem Cyber-EscapeRoom und zahlreichen weiteren Stationen vertreten. Der Cyber-EscapeRoom war ein Blickfang und das Publikum war begeistert in einem nachgebauten Bunker und Panzer gegeneinander zu spielen.

Die EloKa-Truppe war mit dem Allschutzfahrzeug „Dingo 2" vom FüUB2 vor Ort. Die Besucher konnten in das außergewöhnliche und interessante Fahrzeug einsteigen und Militär-Feeling hautnah erleben.

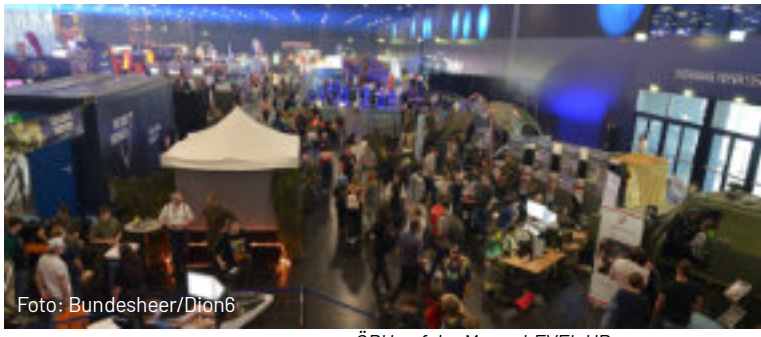
Die Sanitätstruppe der Sanschule war mit dem SanitätsUnimog vertreten. An der Station konnte man mit einer VR-Brille Patienten versorgen und an einer lebensechten Puppe seine Erste - Hilfe Fertigkeiten auffrischen und üben.

Die Militärpolizei, ein Spezialverband des Bundesheeres, war mit viel Ausrüstung vor Ort. Einmal mit Helm und Schutzweste ausgestattet ein Schutzschild zu halten, wurde zum einmaligen Erlebnis und von den Besuchern großartig angenommen. Gezeigt wurde darüber hinaus die Waffenausstattung eines MP-Trupps sowie z. B. ein Reisepasskontrollgerät zum Erkennen von Fälschungen.

Das Pionierbataillon 2 und das ABC-Abwehrzentrum waren mit den Robotern TEODOR und TAUROB, einem Bombenentschärfungsroboter und einem Kampfstoff – Detektierungsroboter vor Ort. Die beiden waren sicher eines der Highlights auf der Ausstellungsfläche des ÖBH. Auch konnte man einen ABC-Schutzanzug und einen schweren Bombenanzug aus nächster Nähe bestaunen und auch anlegen.

Die HTS kam mit einem Schießstand, auf dem mit Pistole oder Sturmgewehr Schnelligkeit und Treffsicherheit unter Beweis gestellt werden konnte. An diesem Stand kam es zu langen Wartezeiten, da der Andrang kaum bewältigbar war.

Das HPA Tirol und das Militärkommando Salzburg waren mit einem Infostand vertreten.



ÖBH auf der Messe LEVEL UP

Um die Kurve zu den Gamern zu finden, wurden wir von 2 E-Heeressportlern tatkräftig unterstützt und das Publikum hatte die Möglichkeit, gegen richtige Profis zu spielen. Eine weitere Unterstützung waren 2 Flugsimulatoren, mit denen man seine Flugkünste testen konnte und auch das Gefühl bekam, selbst ein Flugzeug zu fliegen.

Die Level Up war für das ÖBH ein sehr gelungener Auftritt mit vielen Highlights und die Begeisterung des Publikums, ein Heer zum Angreifen anzutreffen, war sehr hoch. Das Österreichische Bundesheer konnte sich als moderner und attraktiver Arbeitgeber präsentieren und die Besucher nahmen uns mit Begeisterung auf.

Cyberkräfte auf der Messe LEVEL UP

Durch die Teilnahme an all diesen Veranstaltungen und die Arbeit der Informationsoffiziere hat die Dion6 ihre Bekanntheit weiter erhöht und zeigte sich als ein moderner und attraktiver Arbeitgeber. Die Dion6 blickt auf ein erfolgreiches Jahr 2023 zurück und freut sich darauf im Jahr 2024 die bestehenden Initiativen und Partnerschaften auszubauen und weitere innovative Projekte zu betreiben.

Grundwehrdiener des Jahres 2023 - Wien

Benjamin BORENICH wurde am 25.08.2023 im Rahmen der „110 Jahre Heeresbekleidungsanstalt"- Feier der Preis für den „Grundwehrdiener des Jahres 2023 – Wien" überreicht.

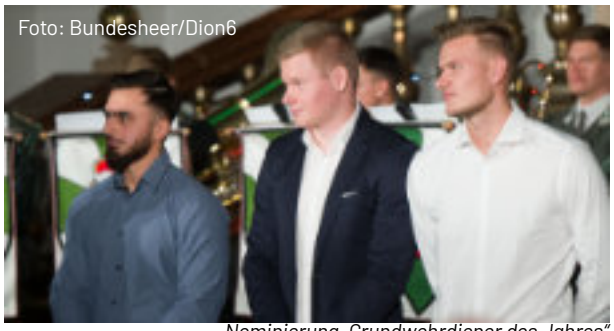
Der Gefreite des Einrückungstermins ET10/22 nutzte seine Grundwehrdienstzeit bei der Direktion 6 - IKT&Cyber im Bereich der Führungsabteilung/ InfoOps&opKomm dafür, in Team- und Alleinarbeit Teile der technischen Planung sowie Umsetzung des Cyber Escape Rooms durchzuführen.

Der Militärkommandant von Wien, Herr Brigadier Mag. Wagner, überreichte Herrn Gfr Borenich im Rahmen seiner Rede den Preis und gratulierte ihm für seine erbrachten Leistungen. Als Vertreter der Direktion 6 - IKT&Cyber gratulierte im Anschluss Herr ObstltdG Mag.(FH) Jezek zum Erhalt des Preises und bedankte sich bei ihm für seine Arbeit und Einsatzbereitschaft an den Cyber Escape Rooms.

Rekrut des Jahres Wien Gfr Benjamin Borenich (Links)

Militär des Jahres - Nominierungen

Der Dion6 gelang es heuer gleich in zwei Kategorien unter den Nominierten zu sein. So wurde Gfr Michael Bogensberger vom FüUB2 für die Erstellung einer Aufbauplatz Datenbank zum "Grundwehrdiener des Jahres" nominiert. Mit diesem Tool ist es möglich erkundete Aufbauplätze für Richtfunkstellen zu erfassen, zu aktualisieren und weiterzugeben. Das ermöglicht eine effizientere Planung von Richtfunkstrecken und erspart die doppelte Erkundung von Aufbauplätzen durch mehrere Einheiten. Da auch die wichtigsten Kontaktdaten erfasst werden, kann die Erkundung und die Absprache nun auch durch einen Telefonanruf oder eine E-Mail erledigt werden.



Nominierung „Grundwehrdiener des Jahres"
Gfr Michael Bogensberger (Mitte)

Auch in der Kategorie "Einheit des Jahres" war die Dion6 mit einer Nominierung mit vertreten. In einer Kooperation zwischen HLogZ Wien und der FüAbt/ InfoOps&opKomm wurden Anfang des Jahres zwei Cyber Escape Rooms gebaut, welche sich zur Steigerung der Cyber Awareness und zur gezielten Personalwerbung vielfach bewährt haben. Bei der Überreichung der Awards dieser Kategorie betonte GenMjr Vodosek die Wichtigkeit von Innovation und Kooperation für das Österreichische Bundesheeer.

Nominierung „Einheit des Jahres" Team mit FBM

Leistungsschau am Nationalfeiertag 2023

Das Österreichische Bundesheer präsentierte sich rund um den Nationalfeiertag mit einer Informations- und Leistungsschau an vier Standorten in der Wiener Innenstadt. Soldatinnen und Soldaten zeigten in 13 Themenbereichen am Heldenplatz, am Hof, am Burgtheater und auf der Freyung ihr Können.

Die Direktion 6 - IKT&Cyber zeichnete sich für die in diesem Rahmen erstmalig gezeigte Themeninsel "Cyber - Forschung - Technik" gemeinsam mit der WFE, dem ARWT, der HTS und der 6. Gebirgsbrigade verantwortlich.

Vorgestellt wurden Innovationen, mit denen sich das ÖBH derzeit beschäftigt. Unter anderem zeigte das ÖBH Projekte aus den Bereichen Weltraum, Drohnendetektion, Fahrzeugtechnik, Robotik und VR-Simulationen.

Auch der Cyber-EscapeRoom fand reges Interesse unter den zahlreichen Besuchern, sodass die vorhandenen Timeslots schnell vergeben waren. Durch das für alle Altersgruppen geeignete Spiel sowie den im Vordergrund stehenden Lerneffekt der Rätsel kamen alle Teilnehmer, egal ob Gewinner oder Zweitplatzierte, mit einem großen Grinsen aus den EscapeRooms und nahmen ihre Preise in Empfang. Vorgestaffelt tummelten sich am 25. Oktober beim der "Tag der Schulen" etwa 800 Schülerinnen und Schüler.

Wir freuen uns über die sehr rege Teilnahme unserer Partnerschule HTBLA Spengergasse und den eng befreundeten HTLs Hollabrunn und Rennweg. Weiters besuchten uns auch folgende HTLs: Wien 10, Wien 16 und St.Pölten. Das Feedback der Schüler und Lehrkräfte war durchgehend sehr positiv und sie zeigten sich überrascht über das breite Ausstellungsspektrum der Themeninsel.

Foto: Bundesheer/Dion6

Cyber EscapeRoom am Nationalfeiertag 23

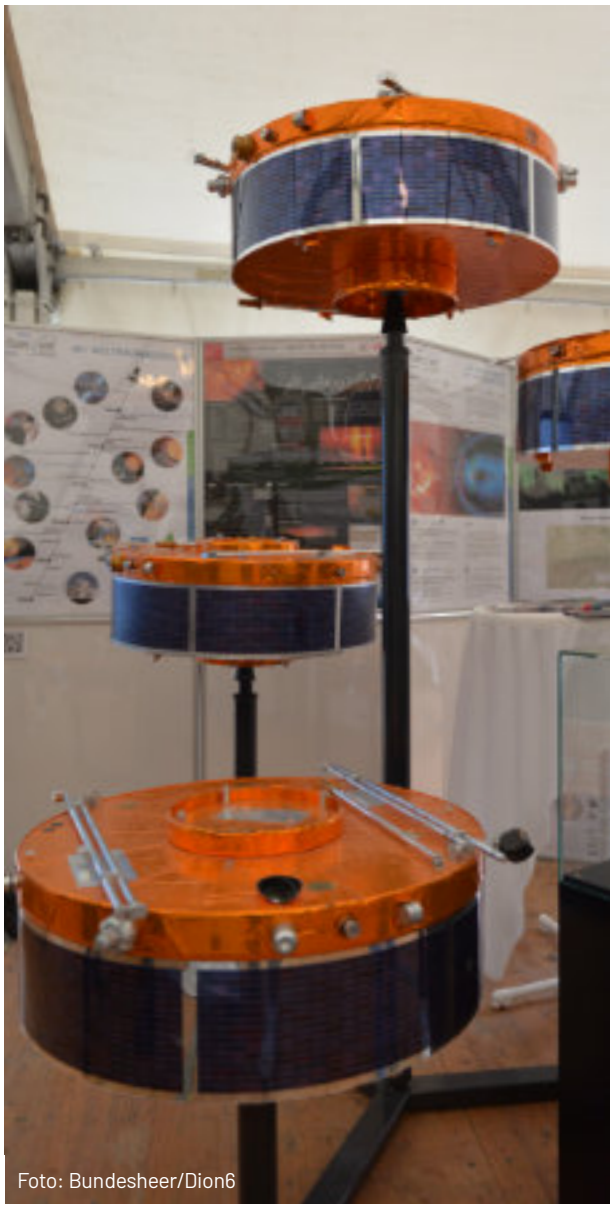
Roboter von SMART INSPECTION

Verteidigungsministerin Mag.ª Klaudia Tanner und Bildungsminister Martin Polaschek nahmen sich ausgiebig Zeit, um sich an unseren Ständen über die aktuellen Projekte zu erkundigen und mit den Betreibern einige Worte zu wechseln. Auch der Rüstungsdirektor GenMjr Harald Vpdosek zeigte reges Interesse an den ausgestellten Prototypen und betonte besonders die Bedeutung der Zusammenarbeit zwischen den Forschungseinrichtungen und dem ÖBH.

Mit durchschnittlich ca. 1000 Besuchern pro Stunde ziehen wir eine positive Bilanz und es zeigte sich, dass wir mit dem Themenbereich "Cyber - Forschung - Technik" ins Schwarze getroffen haben.

FBM im Zelt „Cyber - Forschung - Technik"

Das ist ein Ansporn für die kommenden Jahre und in Kooperation mit der WFE und seinen Forschungspartnern, dem ARWT mit seiner technischen Expertise und der Innovationsmut der MilAk, der HTS und unseren befreundeten HTLs und Bildungseinrichtungen freuen wir uns auf die nächsten gemeinsamen Projekte.



Modellsatelliten

Cyber Escape Room: Cyber-Sicherheit zum Angreifen

Die unsichtbare Front: Cyberangriffe und ihre Auswirkungen

Nicht nur in Zeiten von Homeoffice, „Bring your Own Device“ und hybriden Arbeitsmodellen ist Cybersicherheit immer mehr ein Problem welches das persönliche Umfeld miteinbezieht. Entsprechende Maßnahmen zur Prävention, Schadensbegrenzung und Weiterführung nach einem Schadensfall können jedoch nur dann erfolgreich wirken, wenn man von einem grundsätzlichen Level an Selbstständigkeit und Eigenverantwortung unter den Nutzern eines Systems ausgehen kann. Jede Haustüre in Österreich ist versperrt und das hat einen messbaren positiven Effekt auf die gesamtheitliche Sicherheitslage. Analog ist auch die Absicherung von IT-Systemen zu denken.

So kommt der Cyber Awareness eine ganz besondere Bedeutung zu und es reicht es längst nicht mehr aus, standardisierte Belehrungen herunterzubeten. Es ist vor allem wichtig, das Interesse für Cybersicherheit zu wecken.


Foto: Bundesheer/Dion6

Cyber EscapeRoom bei der IKT-Sicherheitskonferenz


Foto: Bundesheer/Dion6

Teilnehmer im Cyber EscapeRoom

Gamification

Gamification oder auch Gamifizierung ist die Übertragung von spieltypischen Elementen und Vorgängen in spielfremde Zusammenhänge mit dem Ziel der Verhaltensänderung und Motivationssteigerung bei Anwenderinnen und Anwendern. Unter diesem Gesichtspunkt wurde durch die Dion6 und die Dion4 Österreichs erster mobiler Cyber Escape Room entworfen, welcher Cyber-Security in Form von einem Teamwettbewerb näherbringt. Ausgehend von einer Liste an generellen IT-Sicherheitstipps wurde ein Spiel aus mehreren zu lösenden Rätseln erstellt, welche alleine oder in Zusammenarbeit zu lösen sind. Die Spieler sollten aufgefordert werden Sicherheitslücken zu finden und auszunützen. Ziel war es die Spieler auch die Auswirkungen derart schlecht gesicherter Systeme spüren zu lassen.

Custom Inhousing

Die Umsetzung erforderte ein hohes Maß an Innovation und eigener Kreativität. So wurde die technische Infrastruktur von Cybergrundwehrdienern unter Anleitung der Cyberexperten der Direktion 6 - IKT&Cyber aufgesetzt. Gleichzeitig und in enger Abstimmung wurde die Ausgestaltung der mobilen Container im HLogZ Wien mit viel Liebe zum Detail vorgenommen.

Teilnehmer im Cyber EscapeRoom

Die so erarbeitete Lösung geht weg vom klassischen Ansatz eines Escape Rooms, bei dem Rätsel gelöst werden um den Raum verlassen zu können. Hier wurden zwei Räume errichtet in denen zwei Teams gegeneinander spielen. Die Räume wurden ganz im militärischen Stil konzipiert. Einer der Räume stellt den Innenraum eines Bunkers dar, der andere wurde ganz im Stil eines Schützenpanzers eingerichtet.

Hierzu wurden Originalteile aus Beständen liebevoll restauriert und eingesetzt, was ein sehr authentisches Ambiente erzeugt. Angefangen bei dem Panzersessel im Panzer über die Beleuchtung bis hin zu den originalen Bedienelementen wird das Gefühl eines echten Panzers übermittelt.

Im Bunker wurde die Inneneinrichtung eines klassischen Unterkunftszimmers und eines Schutzraumes verkleinert nachgebaut. Besonders die verkleinerten Betten geben dem Raum ein ganz eigenes Flair.

Spielablauf

Mit jedem gelösten Rätsel kann die Haustechnikanlage des jeweilig anderen Teams mehr manipuliert werden. Das spornt einerseits dazu an, die vorbereiteten Sicherheitslücken zu finden und auszunützen, andererseits werden die Unannehmlichkeiten dieser Sicherheitslücken sofort spürbar, wenn das gegnerische Team sie nutzt. Es können verschiedene Videos, Sound- und Lichteffekte eingespielt werden, um den Gegner bei der Lösung der Rätsel zu stören und das Spiel so real wie möglich wirken zu lassen.

Im Spiel lernen die Teilnehmer unter anderem verdächtige E-Mails zu erkennen, was ihnen hilft Phishing-Versuche in ihrem Alltag zu vermeiden. In einem anderen Szenario müssen die Teilnehmer ein Passwort knacken, was die Bedeutung komplexer Passwörter unterstreicht. Auch Installation von Updates, Deaktivierung von Cookies und Überprüfung von Berechtigungen sind Thema.

Das sind einfach umzusetzende Maßnahmen, welche jedoch einen hohen Mehrwert für die Sicherheit bieten.
Um in ganz Österreich einsetzbar zu sein, wurden die beiden Räume auf Anhängern errichtet. Derzeit bezieht sich der Schwierigkeitsgrad auf „Easy", das heißt, dass jeder Spieler der ein Smart Phone bedienen kann mit den gestellten Aufgaben zurechtkommt. Das Spiel ist in deutscher Sprache und geeignet für 2 Teams mit je vier Spielern im Alter von 6-99 Jahren. Die Dauer eines Durchgangs beträgt 20-30 Minuten.

Synergien sinnvoll nutzen

Ein großer Vorteil eines mobilen Cyber Escape Rooms ist die Fähigkeit, gezielt die richtige Zielgruppe anzusprechen. Dies reduziert die Streuverluste erheblich und ermöglicht es darüber hinaus auch aktiv Personalwerbung zu betreiben.

Aufgrund der Einzigartigkeit ergibt sich hier auch die Gelegenheit ganz neue Veranstaltungen zu besuchen. So wurde der Cyber Escape Room beim Besuch des österreichischen Bundesheeres auf der Gaming Messe LevelUp in Salzburg als zentrales Ausstellungsobjekt vom Publikum mühelos an seine Kapazitätsgrenze gebracht.

Teilnehmer im Cyber EscapeRoom

Teilnehmer im Cyber EscapeRoom

Bildungswerkzeug mit Langzeitwirkung

Der mit Abstand wichtigste Aspekt ist die Tatsache, dass Erlebnisse wie ein Escape Room-Spiel oft lange im Gedächtnis bleiben. Wenn die Teilnehmer nach dem Spiel über ihre Erfahrungen sprechen, tragen sie die Botschaft der Cyber Awareness weiter und bringen dies mit dem österreichischen Bundesheer in Verbindung.

Durch die Kombination von Spiel, Spannung und Bildung bietet dieses Format eine einzigartige Möglichkeit, komplexe technische Konzepte auf eine zugängliche und unterhaltsame Weise zu vermitteln. Die Teilnehmer erhalten nicht nur praktische Erfahrungen im Umgang mit digitalen Bedrohungen, sondern entwickeln auch ein tiefgreifenderes Verständnis für die Bedeutung der Sicherheit im digitalen Raum.

Abschließend ist festzuhalten, dass Escape Rooms als innovatives Bildungswerkzeug eine Brücke zwischen Theorie und Praxis schlagen und somit einen wertvollen Beitrag zur Ausbildung und Sensibilisierung in Sachen Cybersecurity leisten. Sie eröffnen neue Wege im Bildungsbereich, fördern kritisches Denken und Problemlösungsfähigkeiten und bereiten uns besser auf die Herausforderungen der digitalen Welt vor.

Zu Besuch bei den Cyberkräften

Projekt Frauenförderung: HTL Spengergasse

Zur Steigerung des Frauenanteils in der Direktion 6 - IKT&Cyber wurde auf Initiative der Personalverwaltung eine Informationsveranstaltung für die Partnerschule HTL Spengergasse organisiert.

Im Rahmen des Projekts Frauenförderung „FIT" (Frauen in die Technik) besuchten am 2. Februar 2023 rund 30 Schülerinnen der HTL Spengergasse die Direktion 6 - IKT&Cyber.

Im Zuge der Veranstaltung wurde den Schülerinnen ein Einblick in den Tätigkeitsbereich der IKT-Technik und in den Bereich der militärischen Cybersicherheit gewährt. Des Weiteren wurde über die vielfältigen Karriere- und Weiterbildungsmöglichkeiten im technischen Bereich informiert.

Zum Abschluss konnte während dem gemeinsamen Mittagessen auf die übrigen Fragen der Schülerinnen eingegangen werden.

Frauenförderung FIT (Frauen in der Technik)

Besuch des BBRZ

BBRZ (Berufliches Bildungs- und Rehabilitationszentrum)

Im Hinblick auf eine mögliche Kooperation erfolgte auf Initiative der Personalverwaltung eine Einladung an eine Delegation des BBRZ (Mitarbeiter sowie Kunden), um einen Einblick in den Tätigkeitsbereich der Direktion 6 - IKT&Cyber zu gewähren.

Am 09.03.2023 empfingen Vertreter der Bereiche IKT-Betrieb, IKT-Technik sowie der Personalverwaltung 36 interessierte Damen und Herren im Kinosaal der Stiftskaserne und brachten den Gästen auf informative und anregende Weise deren Aufgaben näher.

Im Zuge der Veranstaltung wurde über Karriere- und Weiterbildungsmöglichkeiten in den Bereichen Betrieb und Technik sowie im allgemeinen Verwaltungsbereich informiert.

Im Anschluss wurden bereits einige Bewerbungsgespräche geführt und nach wenigen Stunden langten auch noch weitere schriftliche Bewerbungen ein. Die Veranstaltung war für beide Seiten ein großer Erfolg und lässt auf eine künftige gute Kooperation zwischen Direktion 6 - IKT&Cyber und dem BBRZ blicken.

Besuch des Staatssekretärs für Digitalisierung Florian Tursky

Staatssekretärs für Digitalisierung

Am 04.07.2023 besuchte Herr Staatssekretär Florian Tursky (HStS) mit Delegation bestehend aus Büroleiter Wolfgang Ebner, Stv.-Pressesprecher Michael Tögel, Fachreferent Marcus Adamec, sowie Referent Kmsr Lukas Kandlhofer als Vertreter des KBM/GS/BMLV die Dion IKT&-Cyber und den CDO/CIO BMLV.

Im Zentrum stand die Einweisung in den Aufgabenbereich der Direktion 6 - IKT&Cyber, die Digitalisierungsmaßnahmen des ÖBH sowie die Präsentation ausgewählter Projekte aus dem Cyberbereich.

Die Digitalisierungsprojekte "Waste Management" und "Behördenverfahren" wurden eingehend vorgestellt. Last but not least erfolgte eine Einweisung mit Durchgang im Objekt 6 in der STIFT-Kaserne.

Besuch des Staatssekretärs für Digitalisierung Florian Tursky

Nobelpreisträger für Physik o. Univ.—Prof. Dr. phil. Dr. h. c. mult. Anton Zeilinger

Am 6. Dezember besuchte emer. o. Univ.-Prof. Dr.phil.Dr.h.c.mult. Anton Zeilinger die Direktion 6 - IKT&Cyber. Anton Zeilinger ist ein österreichischer Quantenphysiker und Hochschullehrer an der Universität Wien.

Besuch des Nobelpreisträgers Anton Zelinger

Im Jahr 2022 wurde ihm gemeinsam mit Alain ASPECT und John Clauser der Nobelpreis für Physik zuerkannt. Zeilinger erhielt den Nobelpreis für Experimente mit verschränkten Photonen und allgemein verschränkten Quantenzuständen, wobei er unter anderem Quantenteleportation nachwies. Er gilt als ein Pionier der Quanteninformationswissenschaft.

Nach einer Begrüßung und einer Einweisung durch den Kdt GenMjr Ing. Mag. Kaponig wurden dem renommierten Wissenschaftler ausgewählte Forschungs- und Tätigkeitsfelder vorgestellt und bei einem gemeinsamen Mittagessen mögliche Kooperationen und gemeinsame Problemstellungen diskutiert.

Besuch des Nobelpreisträgers Anton Zeilinger

Organisationsentwicklung

Entwicklung der Leitungsebene

Die Eröffnungsbilanz Anfang 2023 war gegenüber den Entwicklungen 2022 quasi unverändert, was die Umsetzung der Reorganisation betraf und setzte die Direktion 6 - IKT&Cyber in dauerhafte Warteposition. Im Rechnungshofbericht Bund 2023/30 über Koordination der Cyber-Defence wurde der Direktion 6 - IKT&Cyber bescheinigt, dass durch die gemeinsame Führung wesentlicher Elemente die Voraussetzungen für eine effektive Zusammenarbeit der Organisationseinheiten vorliegen. Gleichzeitig wurde auch die Empfehlung abgegeben, die Verhandlungen mit dem BMKöS über die Systemisierung der Arbeitsplätze in der Direktion 6 - IKT&Cyber mit dem Ziel einer Einigung und einer zügigen Umsetzung der Organisationspläne im Verteidigungsministerium rasch wieder aufzunehmen und abzuschließen.

Die Situation, unverändert virtuell weiterarbeiten zu müssen, führte dazu, dass, keine umfangreichen Personalmaßnahmen durchgesetzt werden konnten. Die bedingungslose Weiterführung der Aufträge führte dazu, dass nach Herstellen des Lagebilds Ende 2022 vehement mit Bündelung von qualifiziertem Personal an der Entwicklung der Fähigkeiten im Hinblick auf ÖBH2032+ in Form eines mehrmonatigen Boards zur Erstellung eines Masterplans gearbeitet wurde.

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Foto: pixabay.com

Ganzjährig waren alle periodischen Zuarbeiten zur Finalisierung des Thesenpapiers und Maßnahmen für die Planungen ÖBH2023+ und gleichzeitiger Umsetzung der Realisierung erforderlich. Mittlerweile können aus den Weisungen zu Priorisierung und Realisierung unmittelbare und mittelbare Beiträge der Direktion 6 - IKT&Cyber zu über 80% aller Ziele des Ressorts abgeleitet werden, dieser Anteil entwickelt sich durchgehend ansteigend.

Ende 2023 wurde der Bearbeitungsprozess zur Ausgestaltung des IKT-Systems ÖBH 2032+ gestartet, der im Anteil der Mitarbeit in der Dion6 wiederum breit gefächert angelegt wurde, um möglichst alle Expertisen umfassend bündeln zu können.

Trotz stagnierender Entwicklung der Reorganisation 2023 und ungemein hoher Belastung der Leitungsebene wurden herausragende Leistungen erzielt, die sich auf eine unverändert hohe Motivation der Mitarbeiter zurückführen lassen. Das ist angesichts der verlaufenen Perspektiven 2023 mehr als bemerkenswert und unterstreicht auch den hohen Reifegrad der noch immer virtuellen Organisation, mit Veränderungen und Herausforderungen für die Zukunft umzugehen.

Entwicklung der technischen Bereiche

Mit der Umstellung der Sonderverträge auf Richtverwendungen für IT-Personal wurden die ursprünglichen Organisationspläne der vier technischen Bereiche Applikationen, IKT-Technik, IKT-Betrieb und Militärisches Cyberzentrum von 2020 Mitte 2023 mit neuem Umfang verfügt. Daraus entstanden 7,29% mehr Arbeitsplätze, was im Grunde den Strukturumfang für drei Bereiche zunächst verbesserte. Für das Militärische Cyberzentrum wurde aber zeitgleich mit Blickrichtung auf die definierten Kennzahlen im Aufwuchs (dargestellt mit der Kennzahl 14.1.1. im Wirkungsziel 1) ein neuerlicher Antrag mit Erhöhung der Arbeitsplätze gegenüber der verfügten Struktur um 56,8% vorgelegt, um alle Zielwerte der Folgejahre abdecken zu können.Während die neuen RIVIT - Einstufungen durchwegs markante Verbesserungen enthalten, bleiben etliche noch ungelöste Fragen offen, die für die spezifischen Anforderungen im eigenen Ressort nicht so leicht zu lösen sind und wahrscheinlich einer Evaluierung in der Tiefe bedürfen. Das ist eine logische Ableitung, weil sich das an der Einsatzvorbereitung orientierte Spektrum von technischen Mitarbeitern von reinen „Verwaltungsressorts" doch sehr deutlich unterscheidet, indem z.B. auch Techniker zwangsläufig an Übungen und auch in Einsätzen mit signifikant erhöhtem Zeitaufwand mitwirken müssen.

Zusammenfassung, Empfehlungen

Zusammenfassend war 2023, was die Erfüllung der Personalziele betrifft, durchwegs erfolgreich, weil die Personalstärke in der Direktion 6 - IKT&Cyber gegenüber dem Planungsziel 2023 übertroffen wurde. Dieser Umstand ist auch einem enormen Aufwand an positiven Impulsen zur Personalgewinnung durch die Direktion 6 - IKT&Cyber selbst zu verdanken und wurde mittelbar auch durch eine weitreichende Unterstützung der IKTS aus dem Budget der Leiharbeiter begünstigt. Mitte 2023 verzeichnete die Direktion 6 - IKT&Cyber im Vergleich der letzten 7 Jahre einen historischen Höchststand an Leiharbeitern, die es auch ermöglichten, viele Arbeitsplätze in den neuen Organisationsplänen im 2. Halbjahr zu besetzen und damit für einen weiteren Aufschwung zu sorgen.

Die FüUBs blieben unterjährig in der Personalzahl stabil, die FüUS war 2023 zwischenzeitig auf einen Besetzungsstand knapp unter 70%, konnte aber minimal wieder zulegen.

- Eine Neugestaltung der Ausprägung für das gesamte Leistungsvolumen der Direktion 6 - IKT&Cyber insgesamt kann sich erst mit Wirksamwerden der gesamten neuen Struktur für die Gesamtteile der Direktion entfalten und wurde für Ressourcen und Ziele 2024 – 2027 im Plan bereits ausgerichtet.

- Für die gesamte Direktion 6 - IKT&Cyber muss die gesamte Struktur schnellstens weiterentwickelt werden und aufwachsen, weil sonst eine Umsetzung der Ziele der Realisierung in der Tiefe in weite Ferne rücken. Die Verzögerungen wurden vor allem beim Militärischen Cyberzentrum am stärksten spürbar, schlagen sich aber letztendlich auf alle Organisationselemente durch.

- Während z.B. die Applikationen leichter Personal gewinnen können, ist der Vorgang für das spezialisierte Cyberpersonal oder Techniker für die IT-Infrastruktur wesentlich schwieriger, weil es Defizite an Spezialisten in diesem Marktsegment gibt. Die Ziele zum Aufwuchs ab 2024 müssen wirklich vehement verfolgt werden, sonst ist der Auftrag langfristig überhaupt nicht mehr umsetzbar. Die Ressourcenzuordnung befindet sich in den Kernbereichen speziell bei IKT-Technik und beim Militärischen Cyberzentrum im Betrieb bereits deutlich über 90% zu Ungunsten der Serviceentwicklung, die aber exponentiell mit enormen Steigerungsraten anwächst und gleichzeitig bei jeder neuen Beschaffung in Zusammenhang mit Prüfungsvorgängen sowie Zertifizierungen und Audits verstärkt wird.

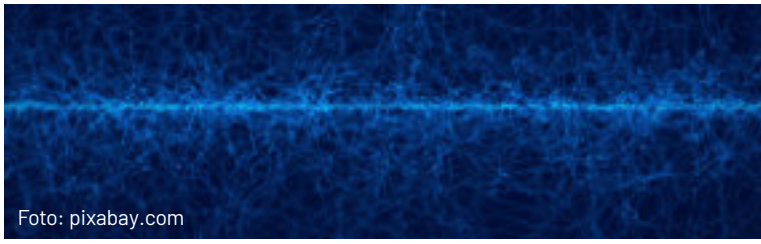


Foto: pixabay.com

Investitionen und Budgetentwicklung

Ressourcen-, Ziel- und Leistungsplan

Während die Reorganisation ins Stocken geriet, wurde 2023 bereits die neue Budgetstruktur mit Ausrichtung auf die Gliederung der Reorganisation etabliert. Damit folgte die Direktion 6 - IKT&Cyber in der Verantwortung direkt dem bis Ende 2022 weitergeführten Detailbudget „Kommando Führungsunterstützung und Cyber Defence" in der neu geplanten Struktur der Direktion 6 - IKT&Cyber nach. Damit war zumindest gewährleistet, dass die Direktion in ihren Ressourcen, Zielen und Leistungen - unabhängig vom unverändert virtuellen Ausgangsstand der Leitungsebene – autark arbeiten konnte.

Von 2022 ausgehend wurde zunächst für 2023 abgeleitet von den Wirkungszielen als einziges und Primärziel der personelle Aufwuchs des spezialisierten Cyberpersonals verfolgt, das trotz schwieriger Rahmenbedingungen im Wirkungserfolg teilweise erreicht werden konnte. Das war immerhin eine Erhöhung von 10,32% im Zielwert gegenüber 2022. Im Laufe des Jahres 2023 wurde - begünstigt durch die Planungsfortschritte ÖBH 2032+ - ab Ende des III. Quartals der Ressourcen-, Ziel- und Leistungsplan 2024 bis 2027 erstellt, der im Umfang wesentlich weitreichendere Ziele für die Folgejahre vorsieht:

- Personeller Aufwuchs des spezialisierten Cyberpersonals
- Weiterentwicklung IKT-System ÖBH und Unterstützung der Digitalisierung
- Sicherstellen der Fähigkeit der EloKa-Truppe zur elektronischen Kampfführung
- Weiterentwicklung der Waffengattung Cyber und Informationsumfeld

Hinter diesen Zielen stehen einzelne Maßnahmen im Detail, die unmittelbar mit dem Aufbau der Fähigkeiten und den Rahmenbedingungen zum ÖBH 2032+ zusammenhängen und ein breites Spektrum an Mammutaufgaben für die nächsten Jahre bilden.

Die gut fundierte Analyse einer Ausgangsleistung dazu konnte bereits Anfang 2023 über die Bearbeitungen im Cyber & Informationskräfte Fähigkeiten Board der Direktion gelegt werden.

Investitionsplanung in die Tiefe

Für die Bearbeitungen zum ÖBH 2032+ wurde Ende Mai 2023 in einer kurzen Klausur gemeinsam mit IKTS für die Autarkie und Nachhaltigkeit das notwendige Investitionsvolumen im Detail für die Anteile Führung & C4I, Cyber und EloKa errechnet, das sich zu diesem Planungszeitpunkt bereits etwa im Umfang von 1,15 Milliarden bewegte.

Budgetentwicklung in der Basisleistung

Trotz weitreichender zusätzlich notwendiger Budgetierungen - z.B. wurde ab 2023 der gesamte Handverlag für die Auslandsvorhaben über das eigene Detailbudget abgerechnet – konnten insgesamt alle Ausgaben für Betrieb, Ausbildung und Repräsentation der Finanzstellen ausreichend und zufriedenstellend bedeckt werden. Bereits frühzeitig wurde der Bedarf für eine Budgetreserve vermittelt, die im IV. Quartal auch tatsächlich angesprochen werden konnte. Die informelle Zusammenarbeit mit dem Haushaltsleitenden Organ Generalstab und der Budgetabteilung funktionierte dazu durchgehend reibungslos. Im Vergleich zu den letzten Jahren konnte 2023 der Trend zur Erhöhung der Basisleistung speziell in der qualifizierten, externen Ausbildung der Mitarbeiter weiter unterstützt werden.

Foto: pixabay.com

Damit wurde zum bereits dritten Mal der wirklich hohe jährliche Bedarf zum überwiegenden Anteil erfüllt. Im Bezug auf die Leistungen im Personalaufwand ist besonders erwähnenswert, dass bei Belohnungen und Prämien deutlich mehr als ursprünglich veranschlagt ausgezahlt wurden, was im Hinblick auf die ausgesprochen hohe Belastung des Personals 2023 doch einen beträchtlichen Mehrwert darstellt, der den herausragenden Mitarbeitern in Form dieser Wertschätzung zurückgegeben werden konnte. Wurden im Ergebnishaushalt 99,97% des Voranschlags verbraucht, so überstiegen im Finanzierungshaushalt die Ausgaben den Voranschlag.

Der Löwenanteil des Mehraufwands daraus entspringt den Ausgaben zum Personal im Sachaufwand (hauptsächlich Kosten für Wehrpflichtige), ein Teil stammt aus dem Personalaufwand, zu geringem Teil entstanden die übrigen aus den Sachausgaben und wurden durch die zugewiesene Budgetreserve mehr als ausreichend abgedeckt.

Die Betriebsbudgetierung für 2023 hatte einen höheren Budgetansatz verglichen mit 2022, die erforderlichen Umschichtungen wurden bereits frühzeitig geplant und vorgemerkt. Für die weitere Entwicklung in den Folgejahren wird ein noch wesentlich höherer Ansatz zu erwarten sein, weil sehr viel in die Ausbildung neuer Mitarbeiter und auch für einen weiteren Bildungsweg von Mitarbeitern investiert werden muss, um konkurrenzfähig zu bleiben.

Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Für das Ressort gedacht, wird es auch notwendig sein, in der Etappe der Streitkräfte technisches Wissen zu fördern, um in der Digitalisierung fit zu bleiben. Im Bereich der externen Ausbildung sparsam vorzugehen, wäre eine gravierende Fehlentscheidung, weil diese Art der Förderung durch Verfügbarkeit qualifizierter Ausbildung bei den Mitarbeitern keine unwesentliche Motivation ist, im Job zu bleiben und sich selbst weiterzuentwickeln.

Das BMLV muss sich diesen herausgearbeiteten Vorsprung unbedingt erhalten, weil das ein unbedingtes Qualitätsmerkmal in der Personalentwicklung darstellt.

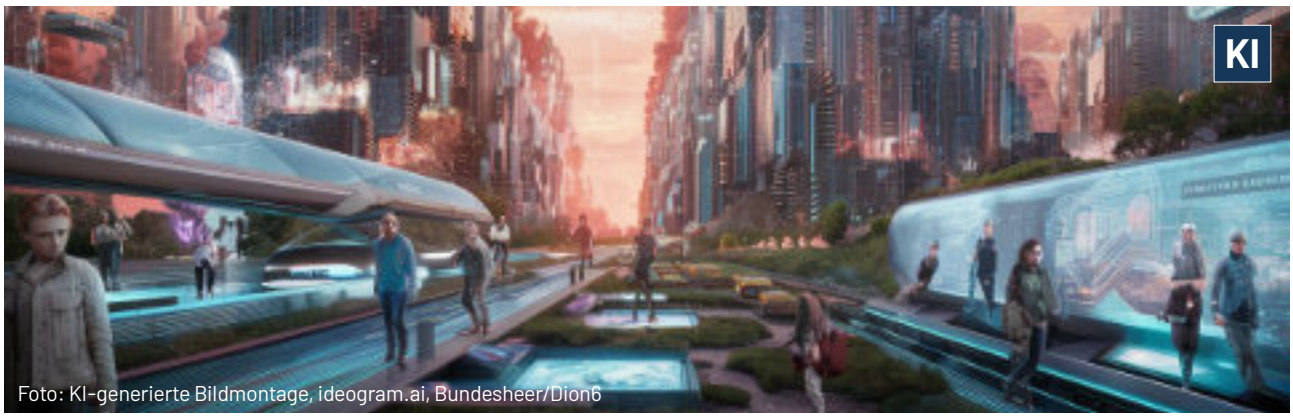


Foto: KI-generierte Bildmontage, ideogram.ai, Bundesheer/Dion6

Kooperation Deutschland-Österreich-Schweiz DACH Digitalisierung – Beschluss für 2023/24

Von 18.-20.10.2023 fanden die DACH Gespräche der DACH Kooperation „Digitalisierung" auf Ebene Steering Board im Raum Villach statt. Generalmajor Hermann Kaponig begrüßte dazu Generalmajor Dr. Michael Färber, den Abteilungsleiter Abteilung Planung und Digitalisierung im Kommando CIR der Deutschen Bundeswehr und den designierten Kommandanten des Kommandos Cyber der Schweizer Armee Oberst i Gst Simon Müller.

Oberst i Gst Simon Müller wird mit Einnahme der neuen Organisationsstruktur am 01.01.2024 zum Divisionär befördert.

Die im Jahre 2014 neu gegründete DACH Kooperation hat sich das Ziel gesetzt vor allem operationell nutzbare Resultate zu schaffen. Die DACH Kooperation zielt dabei auf die Fähigkeit ab ein gemeinsames multinationales Mission Network planen, errichten, betreiben und schützen zu können. Die gemeinsame Fähigkeitenentwicklung setzt auf den Vorgaben des Federated Mission Networking (FMN) auf, validiert diese und entwickelt diese weiter.

Zeitgleich mit den DACH Gesprächen fand die Übung COMMON ROOF in Villach, Murnau (DEU) und Murain (CHE) statt. Diese trinationale Betriebsführungsübung ist zentraler Bestandteil der DACH Kooperation. Sie dient der Weiterentwicklung, Validierung und Auswertung der Prozesse und Verfahren für Planung und Betrieb eines multinationalen Mission Networks. Durch den Übungsleiter Oberst Ernst Berthold wurde die Generalität in die Übung eingewiesen und die wesentlichen Erkenntnisse dargestellt.

Mit Unterzeichnung des DACH Beschlusses wurden die Ziele und Aufträge für das Folgejahr gemeinsam festgelegt. Durch die Generalität wurde die hohe Bedeutung der Kooperation sowohl für die multinationale als auch für die jeweils nationale Fähigkeitenentwicklung herausgestrichen.

Im Zeitraum 06.11. bis 10.11.2023 und 20.11. bis 24.11.2023 wurden zwei Ausbildungsblöcke im Themenbereich „Enterprise Architektur" durchgeführt. Konkret wurden das „Requirements Engineering" am Beispiel der Schweizer Enterprise-Architecture-Modelling Methode, der Ansatz „Systemlandkarte" (umfassende Modellierung der aktuellen IKT-Systemlandschaft) und das „NATO-Architecture-Framework V4" ausgebildet. Diese Kurse wurden im Rahmen der D-A-CH Kooperation durch CHE-Gastlehrpersonal durchgeführt. In Summe wurden 30 Teilnehmer des Ressorts geschult. Die CHE hat in der Architekturentwicklung und der dafür erforderlichen Methodenkompetenz bereits 10 Jahre Erfahrung. Architekturentwicklung ist in der Schweiz im Armeestab (Steuerung) im neu aufgestellten Kdo Cyber sowie dezentral in den Domänen und Fachbereichen (Business Architekten) abgebildet.

Die Kursteilnehmer konnten von der langjährigen Erfahrung und der hohen fachlichen Kompetenz profitieren. Neben diesen Ausbildungsgängen wurde im DACH Rahmen auch eine eigene Arbeitsgruppe etabliert, welche sich mit dem Thema Enterprise Architekturentwicklung im Kontext der Digitalisierung sowie der multinationalen Zusammenarbeit beschäftigt. Da sich das BMLV erst im Aufbau von eigenen Ressourcen befindet, ist die Kooperation mit der Schweiz und Deutschland im Themenbereich Enterprise Architektur für AUT sehr wertvoll.

Kursteilnehmer „Enterprise Architektur"

Tacticla Communication Network (TCN) – Einführung und Herstellen der Verwendungsreife

Einer der Projekt-Schwerpunkte 2023 für die BenBelT-West war und ist in Zusammenarbeit mit der Abt BetrFü in IKTBetr, sowie Abt und Ref von IKT-Technik und IKTCyE, die Einführung bzw. Herstellen der Verwendungsreife des TCN-Systems für die Auslieferung an die Truppe.

Erstes großer Step des Jahres war, der TCN-Systemtest an der FüUS, welcher mit dem positiven Ergebnis „System Einsatzfähig" abgeschlossen werden konnte. Für die einzelnen Teillieferungen an die Truppe wurden in Zusammenarbeit mit HLogZ Wien die TCN-Server (~125 Stk) in der Server-Klonstraße vorgeklont. Mit Beginn der Auslieferung an die Truppe mit Juni 2023 begann auch für die BenBelT-West der Mil. IKT-Support für das System mit den Erstinbetriebnahmen der Vermittlungseinheiten bei der Truppe.

Bei den FMBetrÜbungen „HANDWERK23 & DÄDALUS24" wurde das TCN-System erstmals in einem größeren Übungs&Einsatz-Senario als Netzwerk eingesetzt. Dabei konnten viele gute Erfahrungen gesammelt und noch einige Probleme/Fehler erfasst und behoben werden.

Dem ersten Real-Einsatz bei der DÄDALUS 24 dürfte somit nichts im Wege stehen.

Übungsaufbau des TCN in der FüUS

SPACE - the final frontier

Der Weltraum hat sich in den letzten Jahrzehnten als eine entscheidende Domäne für den Fortschritt und das tägliche Leben auf der Erde erwiesen. Die Bedeutung des Weltraums für den Menschen ist enorm, nicht nur für zivile, sondern auch für militärische Anwendungen.

Der Weltraum spielt auch für das Österreichische Bundesheer eine immer bedeutendere Rolle. Die drei Säulen "space-based earth observation", "satellite navigation" und "satellite communication" sind dabei von besonderer Relevanz. Wobei "space-based earth observation" entscheidende Daten für Lageanalysen sowie thematische Karten liefert, "satellite navigation" präzise Positionierung und Standortbestimmung gewährleistet, während "satellite communication" die unverzichtbare Kommunikation in entlegenen Gebieten sicherstellt. Diese Weltraumtechnologien sind somit integraler Bestandteil der Sicherheitsstrategie und ermöglichen dem ÖBH eine effektive Reaktion auf potenzielle Bedrohungen im digitalen Zeitalter.

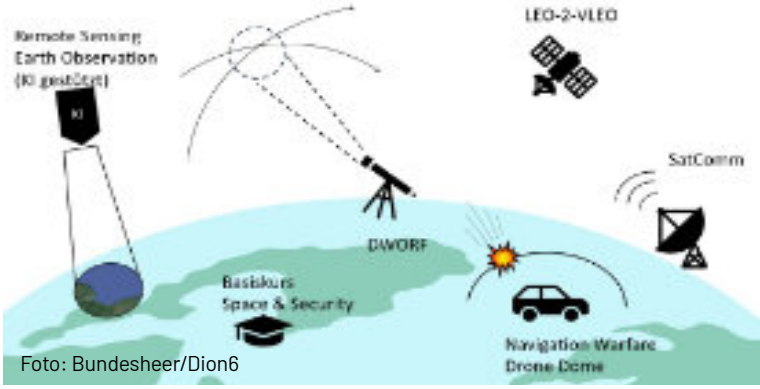


Foto: Bundesheer/Dion6

Weltraumtechnologien - Space Services

Im Zuge einer Umstrukturierung positioniert das österreichische Bundesheer das Ressort gezielt im Bereich "Space" breiter und nachhaltiger und ist Teil der integrierten Fähigkeitsentwicklung BH2032+. Vereinfachte lässt sich sagen: Dion 2 übernimmt die Zuständigkeit für Space Operations, während sich Dion 6 auf Space Services konzentriert. Dieser klare Fokus soll die Effizienz und Vielseitigkeit des ÖBH im modernen Sicherheitskontext stärken.

Foto: Bundesheer/Dion6

Foto: pixabay

Der Masterplan für die umfassende Nutzung des Weltraums ist auf mehreren Ebenen konzipiert, um eine strategische und effiziente Ausrichtung zu gewährleisten. Dieser Masterplan ist in der untenstehenden Abbildung dargestellt. Auf Ebene 1 liegt der Fokus auf der Optimierung des Einsatzes von Weltraum-Services auf operativer und taktischer Ebene. Der nächste Schritt beinhaltet die Ausarbeitung und die interne Veröffentlichung der Österreichischen Militärischen Weltraumstrategie 2035+.

Ebene 3 vertieft diese Strategie mit dem „operativen Entwicklungsplan der Fähigkeiten" für den Weltraum. Innerhalb dieses Plans sind verschiedene Unterebenen integriert, darunter SDA-SSA (Space Domain Awareness und Space Situational Awareness), die Payload-Entwicklung, der Satellitenbetrieb und Space Operations.

In der untenstehenden Grafik sind einige wegweisende Projekte visualisiert. Dazu zählt die Entwicklung eines Pilot-Curriculums für einen Basiskurs „Space & Security", der Einblick in die Thematik Weltraum und den damit verbundenen Hürden und Risiken geben soll. Die Remote Sensing Earth Observation fokussiert sich auf künstliche Intelligenz gestützte Satellitenbildklassifizierung, während man sich in Drone Dome mit der Abwehr von Drohnenschwärmen mittels großflächiger Störung der GNSS-Signale beschäftigt.

Im CatB Projekt „LEO-2-VLEO" wird länderübergreifend ein Satellit gebaut, mit dem Ziel Daten und Information beim Orbit-Wechsel zu generieren. Bei SatComm handelt es sich um ein distributed payload processing Konzept, für eine weltraumtaugliche vernetzte Rechner-Plattform für Satelliten. Diese Projekte verdeutlichen die strategische Umsetzung des Masterplans und unterstreichen die Vielseitigkeit der angestrebten Weltraumaktivitäten.

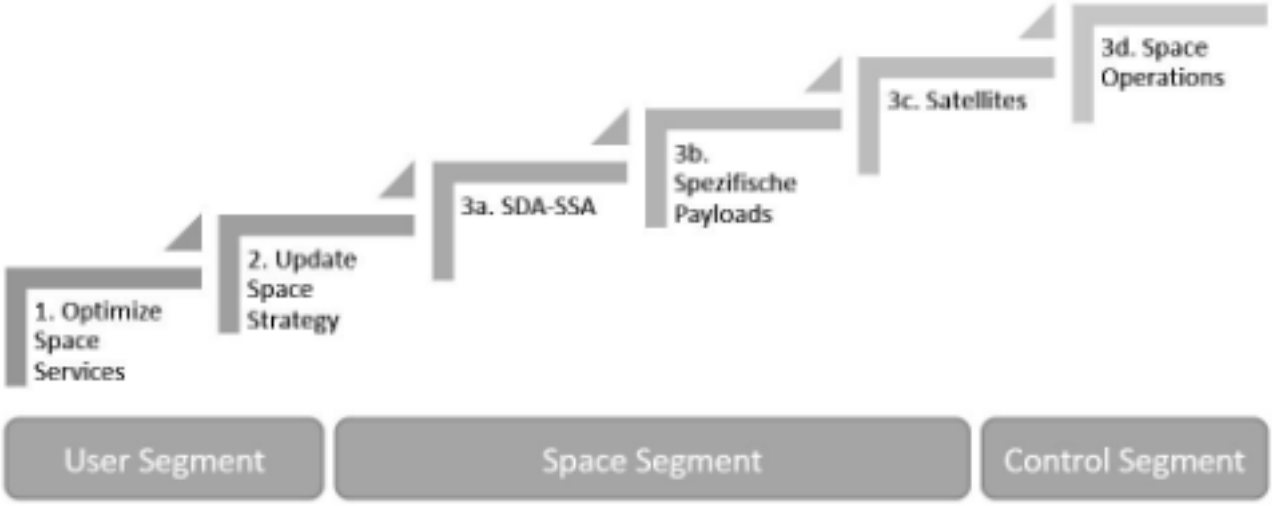


Foto: Bundesheer/Dion6

Österreichische Militärische Weltraumstrategie 2035+

Bundesministerium für Landesverteidigung

Übungen & Einsätze

Planspiele ÖBH 2032+

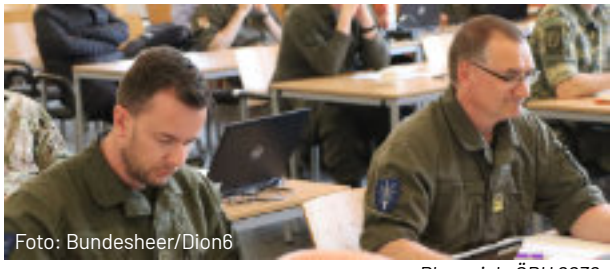
Die Einführung eines Cyber Informations Fähigkeiten Board (CIFB) in der Dion6 prägten das erste Halbjahr 2023 in der Abteilung IKT&CyPl. Mit der thematischen Aufteilung von Entwicklungsbereichen wurden die Aufgaben der Abteilung der Waffengattungen EloKa, Cyber, PsyOps, Komm und der Digitalisierung nun unmittelbar innerhalb der Dion6 aufgenommen.

In den querschnittlichen Kernbereichen KT und IT erfolgte das Zusammenwirken in der Fähigkeitsentwicklung weiterhin direkt mit der Abt StruktPl. Dabei wurden in erster Phase über 40 Vorhaben identifiziert, deren Mitwirkung die fachlichen Kompetenzen der Abteilung IKT&CyPl erforderten.

Die Absprachen zu den Beiträgen im KT und IT Bereich konnten unmittelbar mit den Experten der Strukturplanung getätigt werden. Diese gemeinsamen Anstrengungen wurden auch bei diversen Besprechungsformaten der Fähigkeiten- und Realisierungsplanung dargestellt. Ziel sollte sein möglichst rasch vorhandenes Geld ansprechen zu können und einen Mehrwert für die Truppe zu generieren.

Vom 12.04 bis 14.04 2023 fand in der Schwarzenbergkaserne die Generalstabsklausur zum Aufbauplan 2032+ Bearbeitung des Thesenpapiers statt. Seit Sommer 2022 arbeitet die Abteilung IKT&CyPl aktiv an diesem Papier der Dion Fä&GSPl mit und liefert die Beiträge für die Waffengattungen der Domäne Cyber und Informationsumfeld.

Zur Vorbereitung dieser Klausur wurden vier Fragen gestellt, die in jeweils einer Arbeitsgruppe diskutiert und bearbeitet wurden.



Planspiele ÖBH 2032+

Der Dion6 wurde federführend die Arbeitsgruppe Führungsunterstützung übertragen. In den anderen AG erfolgte eine Mitwirkung der Offiziere der Dion6. Die IKTCyPl wirkte bei der Bearbeitung des Themenbereiches „Ersatzorganisation" mit dem stellvertretenden Abteilungsleiter tatkräftig mit.

In Vorbereitung zu diesem Workshop wurden die Unterfragen innerhalb der Abteilung aufbereitet und während der Diskussionen inhaltlich eingebracht. In Summe konnte festgehalten werden, dass die qualifizierte Weiterführung der Ausbildung im Falle der Mobilmachung eine zu bewältigende Herausforderung für die Waffengattungen und die Schule darstellen.

Die Umsetzung der Ergebnisse dieses Workshops wurden ein Monat später in der Dion6-internen Klausur weiterbearbeitet und die Beiträge zum Thesenpapier vervollständigt.

Im Herbst folgte ein Wargame unter Leitung des ChGStb, indem die Führungsebene und stabsdienstlichen Abläufe diskutiert und dargestellt wurden.

In Summe prägten die Bearbeitungen zum ÖBH 2032 die Masse der Abteilung über das ganze Jahr hinweg. Der Ausblick auf 2024 stellt ein ähnlich intensiven Planungs- und Arbeitsaufwand dar, um die Weiterentwicklung in den Streitkräften sichtbar zur Wirkung bringen zu können.

FüU-Seminar 2023: Meilensteine in Militärtechnologie und Innovation

Das FüU-Seminar 2023 setzte neue Standards in Schlüsselbereichen der Militärtechnologie, besonders in Informations- und Kommunikationstechnologie (IKT), Elektronischer Kampfführung (EloKa) und Cybersecurity.

Ein zentrales Highlight war die Einführung des Tactical Data Radio (TDR), das eine bedeutende Erweiterung der IKT-Fähigkeiten des Österreichischen Bundesheeres darstellt.

Internationale Beiträge aus Deutschland und der Schweiz sowie die Vorstellung des neuen FH-Bachelorstudiengangs und der Cyber Range unterstrichen die strategische Rolle der Führungsunterstützungsschule (FüUS) in der Cyber-Verteidigung. Ein Kameradschaftsabend rundete das Seminar ab, betonte die Wichtigkeit von kontinuierlichem Lernen und internationaler Kooperation in einer sich schnell entwickelnden Militärtechnologie.

Multinationale Übung - Common Roof 2023

Im Zeitraum von 02 10 23 bis 20 10 23 fand in der Lutschounig-Kaserne die multinationale Übung Common Roof 23 (CR23) statt. Diese Übung zielte auf die Interoperabilität innerhalb der Deutschland-Austria-CH (Schweiz) Arbeitsgruppe ab und der Fokus lag in der Bereitstellung eines trilateralen Führungsnetzes für Einsätze im Rahmen der grenzüberschreitenden Katastrophenhilfe und der gemeinsamen Abwehr von Bedrohungen im Cyber Raum. Dabei wurden die jeweiligen nationalen Einsatznetzwerke in ein gemeinsames multinationales Mission Network zusammengeführt und festgelegte betriebliche Abläufe und Prozesse anhand eines Szenarios und eines Ablaufplanes geübt und gleichzeitig evaluiert.

Die Überwachung und Steuerung dieser Teilnetze in den teilnehmenden Ländern erfolgte gesamtheitlich durch das multinational besetzte Zentrale Service Management (CSE Central Service Management & Control Operations Ele-ment) in der Lutschounig-Kaserne in Villach. Nationale Teilnetze betrieben die jeweilig nachgeordneten Zentralen ebenfalls in der Lutschounig-Kaserne in Villach, Murnau (Deutschland) und Murain (Schweiz).

Foto: Bundesheer/Dion6

Die im multinational Netzwerk verwendeten Services und Betriebsabläufe orientieren sich an den vorgegebenen Spezifikationen.

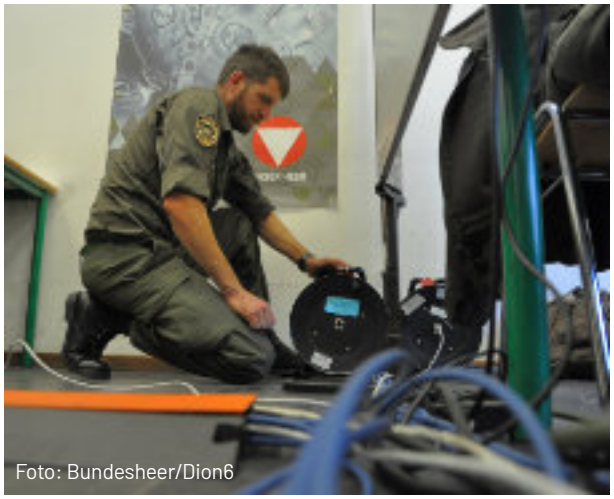
Foto: Bundesheer/Dion6

Übung COMMON ROOF23

Die bei der CR23 gewonnene Erkenntnisse werden in weiterer Folge im Rahmen des laufenden Lern und Optimierungsprozesses in den designierten Gremien des FMN (Federated Mission Networking) eingebracht und beim IKT-System Einsatz im ÖBH umgesetzt.

Die Verantwortlichkeit der Übungsdurchführung für alle Nationen der CR23 lag heuer auch multinational ungeteilt bei FüUB1 bei dem die Übungsleitung inklusive der Netzwerküberwachung im multinationalen Netzwerk lag.

Die Villacher Cybersoldaten hatten den Auftrag die CR23 mit österreichischer Übungsleitung, einem multinationalen CSE sowie mit dem österreichischen SSE (Subordinated Service Management & Control Operations Element) zur Netzwerküberwachung des nationalen Anteiles im multinationalen Netzwerk, durchzuführen. Durch das Errichten und Betreiben eines der zuvor angeführten nachgeordneten Zentralen am Standort in Villach (CSE und SSE), führten die Soldaten die beabsichtigten Erprobungen gemeinsam mit Deutschland und der Schweiz durch und überprüften somit alle interoperablen Fähigkeiten in den Bereichen Betriebsführung, Netzsteuerung und Netzwerküberwachung eines nationalen Einsatznetzes in einem multinationalen Verbund.



Übung COMMON ROOF23

Ebenfalls wurden Datenfunktrupps/Kurzwelle zur Notfallkommunikation für Sprache und Daten an allen Standorten der CR23 eingesetzt, ein verlegbares Einsatzrechenzentrum aufgestellt, Teile zur Einlagensteuerung sowie ein Evaluierungsteam in der Übungsleitung zur Dokumentation der Prozesse gebildet.

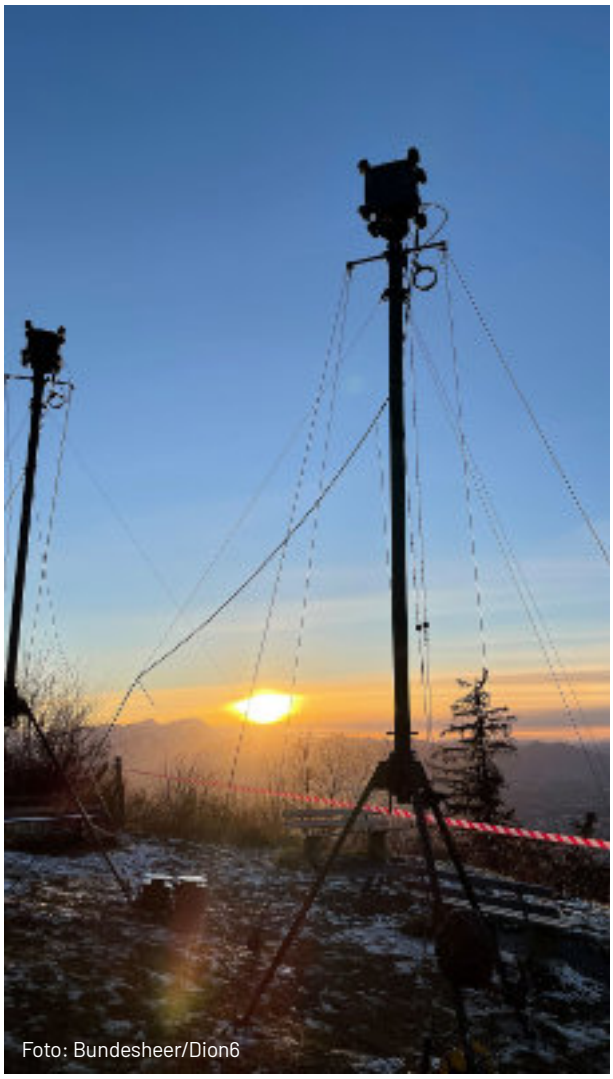
FÜUB 2 unterstützt die Luftraumsicherungsoperation DAEDALUS23

Am Montag dem 09. Jänner 2023 verlegte die 1. Führungsunterstützungskompanie des Führungsunterstützungsbataillon 2 aus St. Johann im Pongau in das westlichste Bundesland Österreichs – nach Vorarlberg.

Grund für die Verlegung war das Ansuchen der Schweizer Bundesregierung an die Republik Österreich, den Luftraum über Westösterreich im Rahmen des Weltwirtschaftsforums 2023 in Davos zu sichern.
Der Betriebszug wurde mit dem Einrichten der Gefechtsstände des Radarbataillons, des ERTA-Teams (Emergency Response Team Air) sowie dem Gefechtsstand der eigenen Kompanie beauftragt. Der Netzzug errichtete sämtliche Fernmeldestellen im nordwestlichen Vorarlberg, um die Verbindung innerhalb der Teile des Radarbataillons sicherzustellen.

Der Lichtwellenleitertrupp hatte den Auftrag, von der Fernmeldestelle im nordwestlichen Bregenzerwald das Aufklärungs- und Zielzuweisungsradar (AZR) des Radarbataillons mittels Lichtwellenleiterkabel in das Fernmeldesystem einzubinden.

Es gelang, sämtliche Aufträge zeitgerecht und korrekt zu erfüllen und einen nahtlosen Übergang in die „scharfe Phase", die mit dem Beginn des Weltwirtschaftsforums 2023 in Davos startete, zu gewährleisten.



Richtfunk-Relaisstelle am Pfänder bei der LRSiOp Daedalus23

Weltweite Cyberübung „Locked Shields 23“

Auch 2023 nahm wieder ein österreichisches Team an der weltweit größten militärischen Cyber-Verteidigungsübung teil. Die Spezialistinnen und Spezialisten üben dabei den Schutz von Systemen der Informations- und Kommunikationstechnologie sowie von kritischen Infrastrukturen gegen Cyberangriffe.

Die Cyberübung „Locked Shields 23“ ist die größte und komplexeste Cyberverteidigungsübung der Welt, mit insgesamt 2.800 Cyberexperten aus 38 Nationen. Auch das Bundesheer nahm 2023 wieder Teil, erstmals gemeinsam in Zusammenarbeit mit zivilen Experten und Milizsoldaten.

Die Organisation der Übung wird vom „Cooperative Cyber Defense Center of Excellence“ (CCDCOE) der NATO in Tallinn, Estland, durchgeführt. Das Training ist eine einzigartige Gelegenheit für militärische und auch für zivile Cyberexperten - die Verteidigung und den Schutz von Systemen der Informations- und Kommunikationstechnologie und kritischen Infrastrukturen gegen Cyberangriffe realitätsnah und gemeinsam zu üben.

„Die Gefahren der heutigen Zeit zeigen, dass Österreich sich auf hybride Bedrohungen, also zum Beispiel Cyberangriffe von außen, vorbereiten muss. In dieser Cyber Verteidigungsübung müssen militärische Systeme wie das IT Netz der Luftraumüberwachung und Führungsinformationssysteme im Cyberraum verteidigt werden, oder und Angriffe auf Kommunikationssysteme, wie 5G-Netze und Satellitenkommunikationsanlagen und abgewehrt.

Auch Szenarien im Informationsumfeld, wie zum Beispiel Desinformationskampagnen müssen bewältigt werden. Mit dieser fordernden Übung stärken wir unsere Fähigkeiten in der Cyberverteidigung, um beispielsweise Ausfälle von Militärnetzen oder öffentlichen Netze in Krisensituationen zu verhindern“, sagte Verteidigungsministerin Mag.[a] Klaudia Tanner bei ihrem Besuch.

Foto: Bundesheer/Dion6

Übung Locked Shields 23

„Locked Shields 23“ größte multinationale Cyber-Übung

„Locked Shields 23“ fand 2023 vom 11.04 bis zum 21.04 statt. Nach einer Woche des Teambuildings und der Verteidigungsvorbereitung folgt die Übungsphase, in der die Teams unter zeitlichem Druck einer ausgeklügelten und intensiven Serie von Cyberangriffen entgegenwirken. Die Verteidiger müssen in Echtzeit Cyberangriffe erkennen, abwehren und eroberte IT-Systeme wieder zurückgewinnen.

Staatssekretär für Digitalisierung und Telekommunikation Florian Tursky betont die Bedeutung der multinationalen Cyber-Übung "Locked Shields" für den Schutz kritischer Infrastrukturen: „Als eine der größten Cyber-Übungen der Welt, bietet Locked Shields die Möglichkeit, unsere Cyber-Verteidigung in realistischen Szenarien zu testen.“ Die Soldatinnen und Soldaten des Bundesheeres werden in der Übung durch Cyber-Angriffe herausgefordert, die zu schwerwiegenden Störungen des simulierten Betriebs von Regierungs- und Militärnetzen, dem Bankenwesen, einem Satellitensystems sowie des Luftverteidigungssystems führen.

Besuch FBM Mag.ª Klaudia Tanner bei der Übung Locked Shields 23

Erstmals mit einem gemischten militärischen und zivilen Team stellte sich das Österreichische Bundesheer mit dem militärischen Cybersicherheitszentrum und der Miliz den Herausforderungen und stärkte damit seine Fähigkeiten im Bereich der Cyberverteidigung enorm.

Besuch ChdGStb General Mag. Striedinger bei der Übung Locked Shields 23

Einsatz im Rahmen der Übung STEINFELD23

Am 27. Juli 2023 verlegte die 3. Führungsunterstützungskompanie einschließlich Teile des Bataillonskommandos in den Einsatzraum Wiener Neustadt zur Unterstützung der Abschlussübung der Theresianischen Militärakademie „STEINFELD23".

Der I. IKT-Zug hatte dabei den Auftrag, in der Vorwoche der Großübung den Gefechtsstand der Übungsleitung und jenen des Führungsunterstützungsbataillons 2 zu errichten und zu betreiben. Während der eigentlichen Übungsphase in der 27. und 28. Kalenderwoche wurde der IKT-Zug dem Akademikerbataillon der Theresianischen Militärakademie unterstellt. Sofort nach dem Erreichen des Gefechtsstandes in der Volksschule Lanzenkirchen, begann der IKT-Zug mit dem Aufbau des Gefechtssandes.

Das Errichten des Vermittlungssystems Großer Verband, das Herstellen der Stabsanschlüsse und die Einbindung der Richtfunksysteme mittels Lichtwellenleiter konnte in kürzester Zeit sichergestellt werden. Der IKT-Zug unterstützte während der gesamten Übung die TOC (Tactical Operations Center) und Meldesammelstelle mit Kaderpersonal sowie Grundwehrdienern. Eine zusätzliche Einbindung in das ortsfeste Fernmeldenetz mittels Mehrkanal-SAT konnte ebenfalls zeitgerecht hergestellt werden.

EloKa-Übung ALPINE JAM II

Am 24. Oktober 2023 begann für Teile der FüUKp (eloKa) die zweiwöchige internationale Übungsserie ALPINE JAM II am Truppenübungsplatz Hochfilzen in Tirol. Bei herbstlichen Bedingungen begrüßten die österreichischen Soldaten die weiteren Übungsteilnehmer aus Deutschland und der Schweiz.

Ziel der Übung sollte es sein, von anderen Nationen in Bezug auf CREW Systeme – CREW bedeutet Counter Radio controlled improvised explosive device - Electronic Warfare, also das elektronische Unterdrücken von ferngezündeten improvisierten Sprengsätzen – zu lernen.

Verschiedenste Bedrohungsszenarien wurden simuliert und die Störsysteme auf Herz und Nieren überprüft. Auf den Teststrecken Asten, Schipfl- und Schüttachalm konnten tragbare Systeme, sowie Systeme welche fix in Fahrzeuge eingerüstet sind, getestet werden.

Der internationale Austausch ist speziell in diesem Themengebiet von bedeutender Wichtigkeit, da jede Nation andere Erfahrungswerte und Systeme besitzt und im Rahmen dieser Übung der persönliche Kontakt und Dialog besonders gepflegt wird.


Foto: *BMLV/Daniel Trippolt*

Antreten Steinfeld23

Allschutz-Transport-Fahrzeug „DINGO" des EloKa-Elementes

Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX)

CWIX ist die größte IKT-bezogene Veranstaltung der NATO und ihrer Partner. 2000 Teilnehmer aus 43 Nationen testeten mehr als 400 militärische IKT-Systeme im multinationalen Verbund am Joint Force Training Center in Polen und in weltweit verteilten Battle Labs. Das Spektrum reichte von Experimenten mit neuen Technologien und Schnittstellenspezifikationen, über die Erprobung neuer Systeme bis zur Übung mit eingeführten Systemen in einem einsatznahen Umfeld unter Abstützung auf FMN (Federated Mission Networking).

FMN ist das Leitprogramm für die Zusammenarbeitsfähigkeit der NATO und ihrer Partner sowie zwischen Teilstreitkräften und Waffengattungen bei Joint und Multi Domain Operations. Der Fokus der österreichischen Teilnahme lag auf der Vorbereitung der FMN Zertifizierung von IKT-Services. Dazu wurden mehrere netzwerktechnische und sicherheitsrelevante Basisdienste sowie das

Geospatial Information Service gemäß aktueller FMN Spezifikation implementiert und aus dem Interoperabilitäts- und Testzentrum in Wien über das CFBLNet (Combined Federated Battle Laboratories Network) mit Systemen von 16 Nationen, darunter unseren Nachbarn Schweiz, Deutschland, Italien, Kroatien, Slowenien und Tschechien, verbunden und getestet.

Dem Bundesheer bietet sich bei CWIX alljährlich die Möglichkeit, am Erfahrungsschatz anderer Armeen teilzuhaben und in einem gesicherten Umfeld eigene unbezahlbare Erfahrungen zu machen ohne die eine "Digitalisierung der Streitkräfte" nicht realisiert werden könnte.

Katastropheneinsatz - Austrian Forces Disaster Relief Unit (AFDRU) - Einsatz Türkei 2023

IMG unterstützte das österreichische AFDRU-Element in der Türkei als Datenprovider, Backbone und mit einem Mann vor Ort.

Nach den verheerenden Erdstößen am 06. Februar 2023 im Bereich der SO-Türkei und N-Syrien wurde AFDRU zur Hilfeleistung alarmiert. Das Katastrophenhilfeelement AFDRU und das IMG verbindet seit Jahren eine enge Zusammenarbeit, das in der letztjährigen, gemeinsam abgehaltenen Übung am Übungsplatz Tritolwerk gipfelte.

So war es eine logische Konsequenz, dass das IMG am Vormittag prompt um Unterstützung ersucht wurde.

Umgehend wurde mit der Recherchearbeit begonnen: Der vermutliche Einsatzraum wurde grob abgegrenzt, der zivile Markt nach vorhandenem Kartenmaterial durchforstet und natürlich die IMG-internen Datenbanken abgeglichen bzw. gesichtet.

Schließlich begannen Kartographen mit der Herstellung von Kartenblättern und Geographen mit der MilGeo-Beurteilung vom in Frage kommenden Raum.

Vorbereitung MilGeo-AFDRU

Der Militärgeologe des IMG, Kontrollor Leutnant Gerhard Herda, MSc wurde - als bei AFDRU-Beorderter - unmittelbar von Korneuburg aus zur Teilnahme angefragt. Er sagte aus dem Urlaub heraus spontan zu, rückte aber zuerst direkt zum IMG ein und nahm das vorerst "quick and dirty"-produzierte Material in Empfang. Danach wurde mit Unterstützung des IMG prompt zu AFDRU verlegt. So konnte eine Erstaustattung von aktuellem und verifiziertem Datenmaterial für die Helfer bereits am Abend sichergestellt werden. Leutnant herda fungierte weiter als POC vor Ort, um eine bestmögliche, unmittelbare Koordinierung zum Bedarfsträger sicherstellen zu können.

08. Februar 2023

Nach Landung in der türkischen Stadt Adana wurde AFDRU der Einsatzraum Hataya mit der Hauptstadt Antakya , dem antiken Antiochia, zugeteilt.

Die BOO (Base of Operations) wurde am unzerstörten EXPO-Gelände im NW der Stadt bezogen. Die Berge- und Rettungsmaßnahmen fanden v.a. im Stadtzentrum statt.

Daher lag das Schwergewicht auf der Herstellung von großmaßstäbigen Satellitenbild-Karten von Antakya (auf Basis der optischen Satelliten "Pleiades" mit einer Auflösung von 50cm), Straßen- und Übersichtskarten von der Provinz Hataya. Nach Fertigstellung wurden die Produkte digital an das Lagezentrum BMLV sowie analog / digital per Kurier nach Korneuburg versandt und nach Etablierung einer Datenverbindung auch mittels Server direkt im Einsatzraum verfügbar gemacht.

Folgende Produkte konnten bereits innerhalb weniger Stunden bereitgestellt bzw. produziert und dem Kontingent vor Abflug am 07. Februar 2023 in analoger und digitaler Form zur Verfügung gestellt werden:

- 32 Atlas-Blätter im Maßstab 1:25.000 (jeweils 10 Stück)
- 4 Kartenblätter in den Maßstäben 1:250.000, 1:750.000 und 1:1.000.000 (jeweils 6 Stück)

Diese wurden in bester und bewährter Zusammenarbeit vom ReprZ Wien im Erdgeschoss der LVAk gedruckt.

- Länderinfos Türkei, Syrien
- Geoinformationen für den Militärdiplomatischen Dienst: Syrien (IMG, 2021)
- Geoinformationen für den Militärdiplomatischen Dienst: Türkei (IMG, 2018)
- Aktuelle Geoinformation Syrien (ZGeoBw, 2019)
- Aktuelle Geoinformation Türkei (ZGeoBw, 2019)
- Munzinger Online/Länder - Internationales Handbuch: Auszug Syrien (Munzinger Archiv GmbH, 06.02.2023)

MilGeo-AFDRU

- Munzinger Online/Länder - Internationales Handbuch: Auszug Türkei (Munzinger-Archiv GmbH, 06.02.2023)
- Übersichtskarte Syrien A4-Format (ZGeoBw, 2009)
- Übersichtskarte Türkei A4-Format (IMG, 2017)

08. Februar 2023

(alle unten angeführten Karten sind als Download unter "Geoinformationen Türkei" zu finden!)

- Satellitenbildkarten Provinz Hatay und Stadt Antakya vor und nach dem Beben
- Satellitenbild-Atlas Stadt Antakya 1:2.000 (Pleiades, 07.02.2023 nach dem Beben)
- Straßenkarte Provinz Hatay 1:25.000 (vor dem Beben)
- Satellitenbildkarten Stadt Antakya (Pleiades, 08.02.2023)

09. Februar 2023

- Satellitenbildkarte Stadt Antakya USAR-Zone AFDRU 1:5.000 (Pleiades, 08.02.2023)

Multinationale MilGeo-Vermessungsübung iSNEx23

Von 17. bis 27. April 2023 fand unter der Leitung des IMG erstmalig in Österreich die "iSNEx 23" („international Survey Networking Exercise 2023“ / Multinationale MilGeo-Vermessungsübung) am TÜPl Hochfilzen / Tirol statt.

Dabei übten elf Vermessungsteams aus neun Mitgliedsnationen der MN GSG („Multinational Geospatial Support Group“ mit Sitz in Euskirchen / Deutschland) der EU und/oder NATO in Österreich unter - heuer NEU - einsatznahen Bedingungen. Dafür wurde am TÜPl H der Luftraum gesperrt und auch die Verwendung von Spoofern und Jammern freigegeben.

Eine fiktive Demarkationslinie (nach Erfahrungen aus UN-Einsätzen am Golan oder aus Zypern) musste quer durch den TÜPl auf einen Meter genau im Gelände festgelegt und vermessen werden. Anfangs noch unter friedensmäßigen Bedingen, später auch unter aktivem Einsatz von "Elektronischer Kampfführung" (EloKa) und von "Elektronische Kampfführung zur Drohnenabwehr" (ELDRO).

Das führte nach einem ersten Staunen zu einem Umdenken bei der Verwendung von digitalen Vermessungsgeräten und Drohnen. Alternative Lösungen mussten unter Zeitdruck erdacht werden und wurden auch gefunden. Das April-typische Wetter (von 30cm Neuschnee bis zu 15 Grad plus) tat sein übriges, um die Teams weiter zu fordern. Zwei überraschend durch die Übungsleitung "gelegte" Minenfelder bildeten den krönenden Abschluss der Einlagen.

Am Visitor's Day am 25. April wurden die einzelnen Vermessungsteams einem gemischten Publikum aus dem In- und Ausland vorgestellt und im Rahmen einer realen Sprengung eine Roadside-Bomb simuliert.
Danach wurde der Bombenkrater innerhalb kürzester Zeit unter Einsatz zweier Drohnen, eines Radpanzer EAGLE mit Laserscanner und unter Schutz zweier EloKa-DINGO millimetergenau aufgezeichnet.

Das dabei entstandene 3D-Modell sowie alle während der Übung produzierten Karten konnten den Besuchern noch während der Veranstaltung präsentiert werden. Die am TÜPl stationierten Tragtiere (Haflinger-Pferde und Esel) waren generell sehr gefragt, erwiesen sie sich wiederum als verlässliche Unterstützung der Teams im unwegsamen Gelände und wurden den Gästen auch mit "speziellen Packlasten" (wie dem "DJT") vorgeführt.

Generell war die Übung ein großer Erfolg, konnten doch viele neue Aspekte und LI aufgezeigt werden:

Vermessen bei Schneelagen, Einsatztauglichkeit der eingesetzten Spezialfahrzeuge bei winterlichen Bedingungen, Synchronisierung der unterschiedlichen Geräte, Umgang mit aktiven Jammern und Spoofern, realitätsnahes Training der Einsatz-Vermessungsteams, taktische Kartierung, Vernetzen der MilGeo-Famile, bis hin zu einem Update des MN GSG Survey Handbooks.

Ein paar abschließende Kennzahlen: Teilnehmer: 9 Nationen mit insgesamt 11 Vermessungsteams:

Deutschland (2 Teams), Großbritannien, Kanada, Litauen, Niederlande, Österreich, Polen, Spanien (2 Teams), Tschechien

Nationen mit Beobachtern:
Griechenland, Kanada, Niederlande, USA

Ebenso anwesend: Österreich, Vertreter SHAPE (NATO), Leiter und Generalsekretariat MN GSG Ehrengäste am 25. April 2023 aus: Deutschland , Frankreich, Großbritannien, Lettland, Litauen, Österreich, Spanien, Ungarn und vom zukünftigen MN GSG-Mitglied Schweiz.

Insgesamt konnten also 15 Nationen mit ca. 50 Übenden, plus ca. 25 Beobachtern und ca. 20 VIPs begrüßt werden.

Foto: Bundesheer/Dion6

Truppe der iSNEx23

Die Exercise-Direktoren Bgdr Dr. Friedrich Teichmann und Kapitän zur See Uwe Frey sprachen dem Exercise-Directorate MN GSG als Übungsleitung Obstlt Sebastian Telzer (DEU) und Obst Mag. Maximilian Göttlich (AUT) höchste Anerkennung und ihren Dank für die einzigartige und professionelle Umsetzung dieses Vorhabens aus.

Ein spezieller Dank des IMG für die herausragende Unterstützung ergeht an: TÜPl H, StbB6 / Tragtierzentrum (TTZ), Dion6, HTS, FlFlaTS, JgB8, LzA, LVAk, Fernmeldebehörde der Republik Österreich

Und nicht zuletzt: Der TÜPl H ist jetzt der bestvermessenste Übungsplatz, most likely weltweit! ;-)

Auslandseinsätze

Die IKT-Sicherheitsüberprüfung in den Auslandseinsätzen ist ein Prozessschritt in der Cyber-Sicherheit um klassifizierte Daten und Systeme vor Bedrohungen zu schützen.

Durch regelmäßige Überprüfungen können potenzielle Schwachstellen identifiziert und behoben werden, um Sicherheitslücken zu minimieren.

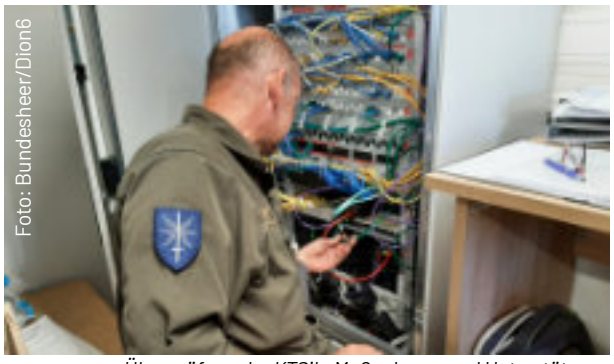
Eine effektive IKT-Sicherheitsüberprüfung gewährleistet die Einhaltung von nationalen und internationalen Compliancemaßnahmen. Eine proaktive Sicherheitskultur im Bundesheer gewährleistet die Resilienz von IKTSys und Services gegenüber Bedrohungen.

Das Referat IKTSih&BedrLCy innerhalb der Abteilung IKTCyE hat den Auftrag die periodischen IKT-Sicherheitsüberprüfungen bei den Missionen des ÖBH durchzuführen. In der Leitlinie zur IKTSih im Ressortbereich des BMLV ist die Überprüfung der technischen, organisatorischen, infrastrukturellen und personellen Absicherungsmaßnahmen angeordnet. Zu diesem Zweck wurden 2023 vier IKT-Sicherheitsüberprüfungen bei den Missionen KFOR, EUFOR/ALTHEA (halbjährlich) und UNIFIL (einmal im Jahr) durchgeführt.

Weiters werden auch diverse Aufbauarbeiten von IKT Systemen bei Auslandsmissionen (z.B. EUTMLI) begleitet. Im Zuge der Überprüfungen wurde das Fachpersonal vor Ort bei der Umsetzung der Maßnahmen unterstützt und bestehende Mängel sofort behoben.

Im Zuge der Absicherung von IKT-Systemen und Schutz der Informationen wurden auch Kryptosysteme für Vertraulich und Geheim österreichweit und in allen Missionen ausgetauscht.

Damit entsprechen die Systeme dem Stand der Technik und stehen den Benutzern für die Verarbeitung von klassifizierten Informationen ab Vertraulich zu Verfügung.



Überprüfung der KTSih-Maßnahmen und Unterstützung des Fachpersonals

IKTSih-Maßnahmen vor Ort

Cyberübung - Crossed Swords 2023 (XS23)

Das CCDCOE veranstaltet jährlich zwei Übungen, an denen die Direktion 6 - IKT&Cyber teilnimmt: Crossed Swords und Locked Shields. Dabei handelt es sich um interaktive, realistische Simulationen, die den Experten für Cybersicherheit der Allianz ermöglichen, ihre Fähigkeiten im Schutz kritischer Infrastrukturen zu verbessern.

Crossed Swords baut auf Locked Shields auf und konzentriert sich auf offensive Cyberoperationen. Über 20 Länder, darunter NATO- und Nicht-NATO-Mitglieder, nehmen mit 400 Systemen teil. Die Übung bietet technisches Red-Teaming-Training für Penetrationstester, Forensikexperten und Awareness Spezialisten.

Die XS23 zielt darauf ab, Cyberexperten in der Durchführung von vollständigen offensiven Cyberoperationen zu schulen. Die Teilnehmer, darunter Operatoren, Forensikexperten und Führungskräfte, trainieren in einem fiktiven Konfliktszenario zweier Nationen und simulieren entsprechende Operationen im Cyberbereich.

Die Übung integriert akademische und industrielle Partner, um Authentizität und realitätsnahe Herausforderungen zu gewährleisten. Ziel ist die Planung und Durchführung taktischer und technischer Operationen, die Cyberangriffe umfassen und digitale forensische Fähigkeiten integrieren.

Die Übung fördert die Zusammenarbeit von Verbündeten und Partnern, stärkt das Verständnis und die Partnerschaften durch taktische und technische Koordination während einer Cybermission.

Cybersicherheitsübungen MIC23 und MICNET

In den vergangenen Jahren führte die Direktion 6 - IKT&Cyber im Rahmen eines EDA-Projektes Live-Fire-Cyber-Defence-Übung durch, die speziell der Verbesserung der europäischen Zusammenarbeit zwischen den nationalen militärischen Computer-Notfallteams (CERTs) der Mitgliedstaaten diente.

An der Übung nahmen mehr als 200 Experten aus 15 EDA-Mitgliedstaaten und der Schweiz teil, die alle von ihren Arbeitsorten aus miteinander verbunden waren.

Die Veranstaltung bestand sowohl aus einem technischen Teil, in dem das Vorfallmanagement (hier insbes. die Erkennung und das Teilen von Informationen mit den anderen Teams) im Vordergrund stand, als auch aus einem operativen Teil, in welchem die internationale Kooperation zwischen der Leitungsebene der milCERTs diskutiert wurde.

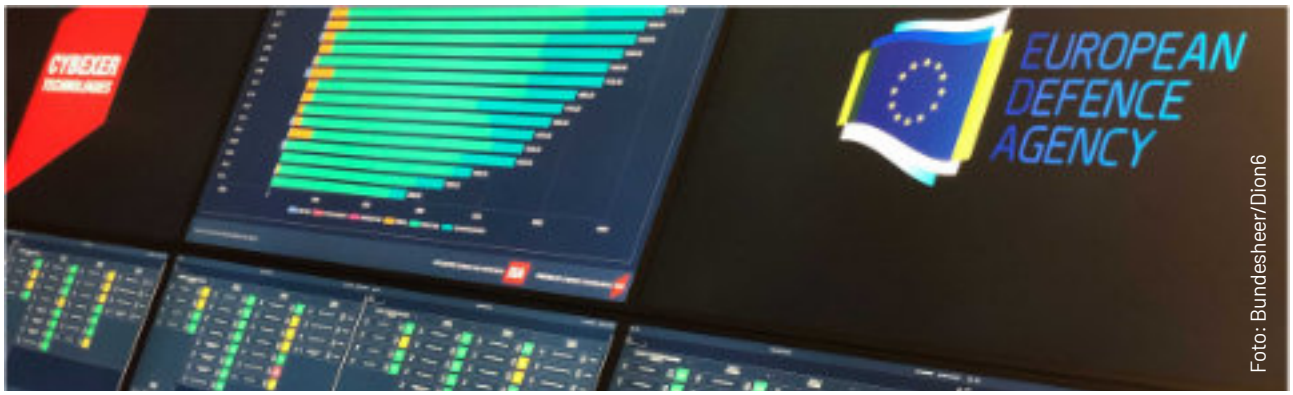
Österreich erreichte dabei den 4. Platz in der Gesamtwertung, sowie in der Sonderwertung „bester SitRep" (Bericht über die „Situational Awareness" in der Übung) zum 3. Mal in Folge den ersten Platz. Zudem stellte das österreichische milCERT das kleinste Team der gesamten Übung mit letztendlich 5 aktiven Teilnehmern.

Das Ziel der Übungswoche war es unter anderem, militärische CERTs zusammenzubringen und die Dynamik des Vorfallmanagements zu beobachten. Wobei der besondere Schwerpunkt auf dem Informationsaustausch, einem Schlüsselfaktor der modernen Cyberverteidigung lag.

Während die europäischen Länder bei der Einrichtung von Mechanismen und Verfahren für den Informationsaustausch zwischen zivilen CERTs weit vorangekommen sind, sind solche Kooperations- und Kommunikationskanäle im militärischen Bereich viel weniger entwickelt, auch aufgrund der hohen Sensibilität der Informationen.

Angesichts dessen haben viele Beteiligte die Notwendigkeit geäußert, die in zivilen Kreisen angewandte Praxis des Informationsaustauschs auch auf militärische CERTs und deren Operationen auszuweiten.

In der neuen EU-Cybersicherheitsstrategie, die im Dezember 2022 veröffentlicht wurde, wird hervorgehoben, dass diese Initiative dazu beitragen würde, die Zusammenarbeit zwischen den Mitgliedstaaten erheblich zu verbessern.



Scoreboard der MIC23

Daher beteiligt sich die Direktion 6 - IKT&Cyber an dem EDA-Cat A Projekt „Military Computer Emergency Response Team Operational Network (MICNET)", welches im November 2023 von 19 Nationen unterschrieben wurde.

Weitere Mitgliedstaaten haben bereits ihr Interesse bekundet.

Elektronischer Kampf - Übung Waveform Development Olympiad 2023 (WDO23)

Das Begegnen der Gefahr von Radio Controlled Improvised Explosive Devices (RCIED) für unsere Soldaten erfordert stetiges Engagement,

Im Bereich der Elektronischen Kampfführung (EloKa) geschieht dies unter anderem durch technischen Maßnahmen mit Force Protection (FP) Systemen, beispielsweise mit sogenannten Counter RCIED Electronic Warfare (CREW) Systemen.

Der Umfang dieser technischen Bedrohungen erstreckt sich einerseits von RCIED und andererseits bis zu small Unmanned Areal Vehicles (sUAV) als elektromagnetisch beeinflussbare Systeme im Kontext der RCIEDs.

Foto: Bundesheer/Dion6

Neben nationalen Anstrengungen beteiligt sich Österreich auch an internationalen Aktivitäten, um eine bestmögliche Wirksamkeit gegen diese globalen Bedrohungen zu erreichen.

Konkret geschieht dies mit einer multinationalen Kooperation im NATO Team of Experts on Electronic Countermeasures for RCIED.

Eine der vielen Aktivitäten ist die regelmäßige Durchführung der sogenannten „Waveform Development Olympiad" (WDO).

Bei dieser, bis dato in verschiedenen europäischen Ländern durchgeführten, technischen Veranstaltung liegt der Arbeitsfokus auf dem Wissensaustausch zu neuen Bedrohungen und den erforderlichen Gegenmaßnahmen, des gegenseitigen Kennenlernens der unterschiedlichen CREW-Systeme und Synchronisationsverfahren, der Verbesserung der Mess- und Testverfahren sowie von erforderlichen Testaufbauten und ebenfalls auf der Signalanalyse zur weiteren Bedrohungsanalyse.

Heuer nahm zum zweiten Mal eine österreichische Delegation von technischem EloKa-Fachpersonal des Unterstützungszentrums EloKa (UZEloKa) des Militärischen Cyberzentrums der Direktion 6 - IKT&Cyber an der WDO 2023 in Deutschland teil.

Im November 2023 waren insgesamt neun Nationen (Deutschland, Niederlande, Belgien, Frankreich, Dänemark, Norwegen, Schweden, Luxemburg und Österreich) zu Gast in Greding.

Neben der Teilnahme an der nächsten geplanten WDO mit österreichischem EloKa-Fachpersonal ist die Durchführung einer eigenen Mess- bzw. Teststation zur Signalanalyse durch österreichische Spezialisten der Abteilung UZEloKa geplant.

Cyber-Übung des MilCyZ CRX

In diesem Jahr veranstaltete das Militärische Cyber-Zentrum der Direktion 6 - IKT&Cyber erstmalig eine eigene Cyber-Übung für fortgeschrittene Cyber-Experten. Durch Zuhilfenahme einer externen Cyber Range Infrastruktur und Trainern über die Kooperation mit Estland, konnte eine Schulung mit anschließender Blue- und Red-Team Übung stattfinden.

Im Zuge dieser Übung wurden Cyber-Verteidigungs- und Angriffssimulationen unter Ausbildungsbedingungen absolviert.

Neben dem Training für österreichische Kräfte, wurden im Zuge der internationalen Zusammenarbeit Cyber-Experten der Schweiz eingeladen, um am Training teilzunehmen.

Bundesministerium für Landesverteidigung

Vorhaben & Projekte

Battlefield Management System (BMS)

Das BMS ist eine essentielle Komponente im Aufklärungs-Führungs-Wirkungsverbund. Es vernetzt die gefechtstechnischen Führungsebenen für die Erfassung, Verteilung und Darstellung ebenengerechter Führungsinformation.

Es dient der Positionsbestimmung und Orientierung, der Darstellung eigener und feindlicher Kräfte, der graphischen Befehlsgebung und unterstützt Zielerfassung und Wirkung. Im ÖBH wird seit einigen Jahren beim JaKdo ein BMS erfolgreich eingesetzt. Zur Vorbereitung der Einführung in den gesamten Landstreitkräften wurde bereits 2021 eine Verfahrenserprobung beim JgB18 in Zusammenarbeit mit HTS und der Abteilung IKTS durchgeführt.

Ein entsprechendes Beschaffungsvorhaben wurde eingeleitet. Zuschlag, Güteprüfung und Beginn der Einführung sind 2024 geplant.

Foto: Bundesheer/Dion6

Battlefield Management System (BMS)

Materialstammdatenverwaltung BMLV (MatS)

Die Materialstammdatenverwaltung (MatS) des BMLV wurde als erstes großes Service auf eine moderne WEB-Applikation umgestellt.

Das Service MatS umfasst jedoch nicht nur die Verwaltung von Artikeln und allen dazu notwendigen Attributen und Strukturinformationen wie Satznormlisten, Soll-Strukturen und Ersatzteilkatalogen, sondern auch weitere für die Artikelverwaltung notwendige Module wie Firmen-, Nation- , Währungsverwaltung und einige mehr.

Foto: Bundesheer/Dion6

LOGIS-Auszug

Ferner wird der Datenabgleich mit dem Natokodifizierungssystem NCORE aus MatS angestoßen. Ein weiterer Teil ist der digitale Datenimport für Massendatenänderungen bzw. der Datenlieferungen von externen Systemen (Firmen, Industrie).

Die Daten werden zentral gehalten und können somit für alle Systeme des BMLV bereitgestellt werden. Derzeit werden im Service MatS über 1 Million Artikel verwaltet!

Smart Waste

IoT und Long Range Wide Area Network (LoRaWAN) bieten viele Möglichkeiten zur Digitalisierung in den Liegenschaften. Sie tragen zur Prozessmodernisierung und zur Nutzung der Vorteile der Digitalisierung bei.

Zur Erreichung des UN-Ziels, die Lebensmittelabfälle bis 2030 zu halbieren, wurde eine entsprechende Strategie postuliert (Reduktion des manuellen Arbeitsaufwands, Aufbereitung valider Steuerungskennzahlen).

Das BMLV hat für die Erfassung der Lebensmittelabfälle in der Verpflegung das Pilotprojekt Smart Waste gestartet. Die Unterstützung für die digitale Umsetzung kommt von BauWAppl.

Foto: Bundesheer/Dion6

LoRaWAN-Netzwerklösung

Zentral im Projekt ist eine LoRaWAN-Netzwerkserverlösung (on premises), die den BMLV-Sicherheitsvorgaben entspricht. Dabei werden LoRaWAN-Sensoren und Qualitätsaktoren verwendet.

Das System besteht aus vier Ebenen:

- Endgeräte (Sensoren, Aktoren)
- Gateways (Basisstationen)
- Netzwerk-Server
- Anwendung bzw. IoT-Plattform

bundesheeronline – Digitalisierung der Behördenverfahren

Am 29.6.2023 wurde ein neues Kapitel im digitalen Außenauftritt des österreichischen Bundesheeres aufgeschlagen.

Unter der Leitung von FBM Mag.[a] Klaudia Tanner und Herrn Digitalisierungsstaatssekretär Florian Tursky fand eine Pressekonferenz zum Thema "Digitalisierung der Behördenverfahren im österreichischen Bundesheer" statt.

Neben den Informationen über den aktuellen Stand der Digitalisierung im österreichischen Bundesheer und der Notwendigkeit der Veränderungen im Zuge dieses Vorganges, stand die Präsentation der neuen Plattform "bundesheeronline" im Vordergrund.

Mittels eines LIVE Einstieges über das neu geschaffene BMLV Bürgerportal (https://citizen.bmlv.gv.at) und der Nutzung der digitalen Identifizierung mittels ID-Austria, konnten durch Mag. Herbert Binder (Abteilungsleiter PersAppl) die neuen "bundesheeronline" Services vorgestellt werden. Erstmals wurden über diesen Wege voll digitalisierte und transformierte Verfahrensprozesse den Bürgern durch das BMLV angeboten.

Im Zuge der Umsetzung des Vorhabens "Digitalisierung der Behördenverfahren" - technische Verantwortung und Entwicklung durch die Abteilung PersAppl und fachliche Begleitung durch das Heerespersonalamt (HPA) - wurden aufwändige, umfangreiche und komplexe Formularanträge in digital einfach verwendbare und auf allen technisch nutzbaren Devices digital transformiert.

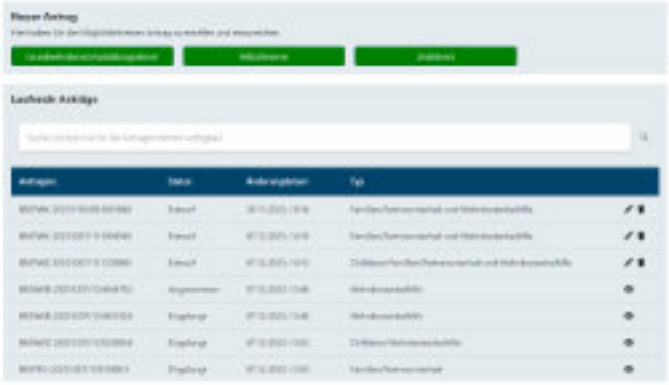


Foto: Bundesheer/Dion6

BundesheerOnline

Abteilungsleiter PersAppl Mag. Peter Binger

Durch Nutzung von neuen Technologien und Methoden (Usability) werden nun über die Serviceplattform "bundesheeronline" moderne digitale Prozesse und Formulare angeboten, die von verschiedensten Personengruppen (Miliz, Grundwehrdienst, etc.) genutzt werden können. Aufwändige Papierverfahren mit langen Durchlaufzeiten sind mit der Einführung dieser Services Geschichte.

FBM Mag.ª Klaudia Tanner mit Digitalisierungsstaatssekretär Florian Tursky

Schnelle und unkomplizierte Antragseinbringungen, jederzeitige Informationen über den Antragsstatus, direkte und moderne Kommunikation mit dem jeweiligen Fachbereich und Verfügbarkeit der Services rund um die Uhr (24/7) stehen nun im Vordergrund.

Laufend werden zu den bereitgestellten Verfahren die Nutzungszahlen erhoben und diese Zahlen dokumentieren eindrucksvoll den Bedarf an "bundesheeronline": Über 6.000 Personen nutzen bereits die Möglichkeit der Selbstauskunft bzw. die Kontrolle der im BMLV hinterlegten Daten.

Über 2.300 Mal wurde "bundesheeronline" in diesen wenigen Wochen zur Aktualisierung des IBAN's durch die digital identifizierten User genutzt (Stichtag 30.11.2023) und führten so zu einer erheblichen Reduktion von einlangenden Papierformularen in den jeweiligen Fachbereichen (bereits bis zu 80 % weniger Anträge).

Aufwändige Antragseinbringungen (Familien-/ Partner- und Wohnkostenbehilfen) von früher bis zu 50 Papierseiten werden mit der Einführung der neuen Services voll digitalisiert durch den Antragsteller eingebracht und können durch die zuständigen Fachbereiche ohne Medienbrüche in den jeweiligen Zielsystemen nachvollziehbar weiterverarbeitet werden.

Auch in diesen Fällen wurden schon mehrere hundert Anträge mit ca. 1.300 Anhangsdokumenten (zuvor per Papier) eingebracht und verarbeitet.

Dieser Weg hat aber erst begonnen! Bereits Mitte Nov. 2023 wurde ein weiteres Verfahren (Entschädigung auf Einkommensentgang) freigeschalten.

Und es werden noch viele weitere Verfahren in den nächsten Wochen, Monaten und Jahren (Stichwort Präsenzdienstzeitbestätigung, Antragstellungen durch Zivildiener, Milizausbildungsvergütung) digitalisiert.

Der Weg in der Modernisierung der Behördenverfahren des Österreichischen Bundesheeres konnte erfolgreich gestartet werden. Ein wichtiger Schritt in die Digitalisierung wurde mit der Bereitstellung von "bundesheeronline" gesetzt - das BMLV ist ab sofort ein wichtiger und starker Partner im österreichischen E-Government!

Zentrales Ausbildungsmanagementsystem - ZAMS

Ein Großteil der aktuellen Ausbildungsplanung erfolgt durch Nutzung bestehender Standardapplikationen wie z.B. Microsoft EXCEL, ACCESS, etc. Der notwendige Austausch von Ausbildungsinformationen zwischen den zuständigen Organisationen erfolgt zum überwiegenden Teil mittels Versendung von Tabellen bzw. durch Einarbeitung dieser Daten mittels selbsterstellter Makros bzw. Informationsweitergabe durch den ELAK.

Alle diese genannten Verarbeitungsschritte sind aktuell zeit- und ressourcenaufwändig.

Die Abteilung PersAppl wurde dazu als technischer Umsetzer eines neuen ZAMS beauftragt. Zum Einen, weil schon jetzt alle abgeschlossenen Lehrgänge im PERSIS zu den Personen gebucht werden, zum Anderen, weil in dieser Abteilung durch die Umsetzung von "bundesheeronline" alle notwendigen technischen Voraussetzungen zur Schaffung einer zentralen Lösung geschaffen wurden.

Erster Umsetzungsschritt ist die Ablöse von KURSIS auf eine neue, zentral verfügbare Webapplikation. Mitte Dez. 2023 wurde der Startschuss zu einem benutzereingeschränkten Probebetrieb gegeben.

Die Planung sieht eine Ausrollung des zukünftigen Web-KURSIS bis Ende Jänner 2024 für alle Nutzer vor. Dieser erste kleine Baustein ermöglicht bereits einen ersten Ausblick auf das künftige ZAMS. Neben der Integration von Rollen und Rechten bzw. der Struktur der Ausbildungsorganisationen, sind auch bereits Funktionen für die zukünftigen Planungsprozesse vorgesehen.

Der Umsetzungsprozess für ein ZAMS ist gestartet und wird 2024 konsequent fortgeführt.

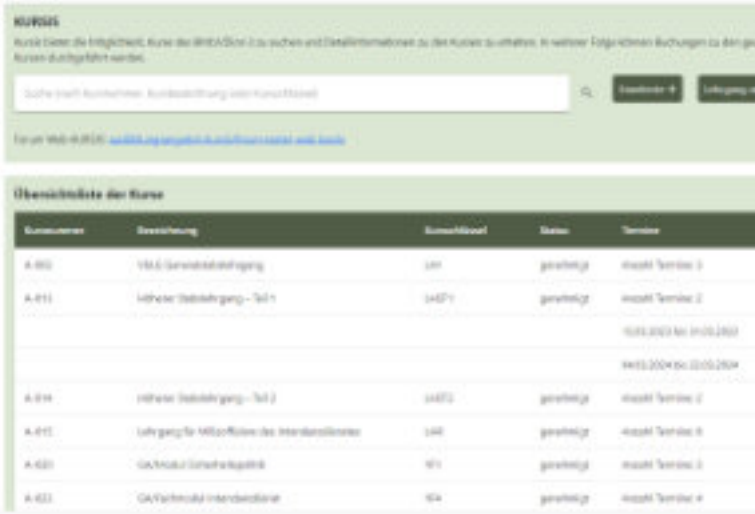


Foto: Bundesheer/Dion6

Auszug Web-KURSIS

Zeitmanagement-PAAN

Ziel von PAAN-Zeitmanagement ist eine allumfassende Digitalisierung und Integration der Zeiterfassung und der erforderlichen Genehmigungswege im österreichischen Bundesheer. Gleichartige Informationen sollen nur noch einmal erfasst und dann in den jeweiligen Teilapplikationen weiterverarbeitet werden.

Dazu wurde bisher das Antragswesen, die WEB-Standesliste und KRONOS-Zeitkarte umgesetzt. Viele Dienststellen und Anwender nutzen bereits Teile von PAAN-Zeitmanagement im Probebetrieb, allein KRONOS-Zeitkarte wird mittlerweile durch über 10.000 Anwender tagtäglich genutzt.

Foto: Bundesheer/Dion6

Logo KRONOS/PAAN/StaMe/Persis

Das gewählte Entwicklungsvorgehen ist evolutionär, PAAN-Zeitmanagement wird daher Schritt für Schritt erweitert bzw. verbessert.

Als Highlights des Jahres 2023 sei daher das Massengenehmigen im Antragswesen oder die Reporting-Funktionalität in der Zeitkarte angeführt.Die Priorisierung der Anforderungen erfolgt durch die PAAN-Arbeitsgruppe, eine für die BMLV-Organisation repräsentative User-Group unter Federführung der Abteilung AllgPersAng.

Die aktuell gültigen Zeitordnungen werden durch die zuständigen Abteilungen GstbAbt und Präs entsprechend angepasst und voraussichtlich im 1. Quartal 2024 verfügt werden.

Die nächsten großen Ausbauschritte wird die Umsetzung des elektronischen Genehmigungsprozess für die Zeitkarte sowie die Integration der Zeitkarte mit der WEB-Standesliste sein. Künftig soll auch PAAN-Zeitmanagement über das BMLV-Stammportal verfügbar sein.

Zukunft der individuellen Datenverarbeitung im BMLV/ÖBH

IDV-Entwicklungs-Service und IDV-Entwickler-Plattform

Zur Unterstützung der Entwicklung von IDV-Anwendungen durch die Truppe bzw. Mitarbeiter des BMLV/ÖBH werden seitens Dion6 ein IDV-Entwicklungs-Service und eine IDV-Entwickler-Plattform zur Verfügung gestellt:

Das IDV-Entwicklungs-Service beinhaltet alles, was erforderlich ist um IDV-Anwendungen zu entwickeln.

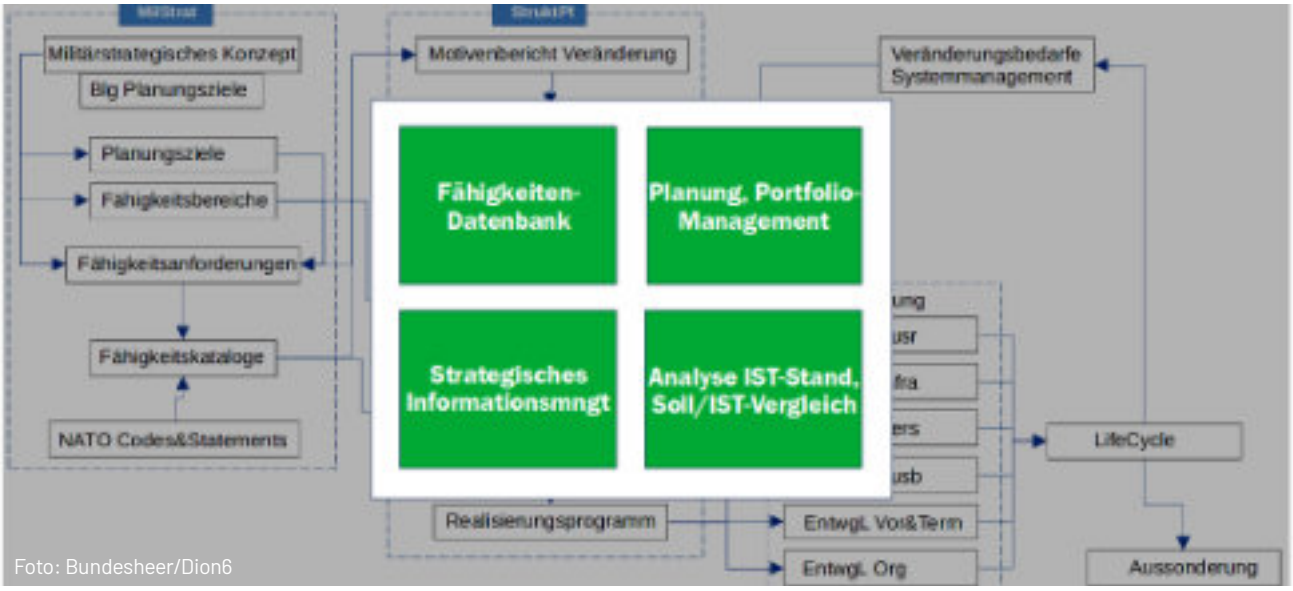
Erstellt werden können Web-Applikationen, als Programmiersprachen kommen für das Backend Java mit dem Spring-Framework und für das Frontend Typescript mit dem Angular-Framework zum Einsatz.

Das IDV-Entwicklungs-Service ist ein Service der Dion6 und wird laufend verbessert werden um die Anforderungen der Entwickler von IDV-Anwendungen optimal zu erfüllen.

Die IDV-Entwickler-Plattform im Intranet ist als zentrale Stelle geplant, auf der sämtliche Informationen, die für die Entwickler von IDV-Anwendungen relevant sind, gefunden werden können.

Foto: Bundesheer/Dion6

IDV-Entwicklungs-Service & Plattform



Fähigkeiteninformations-, planungs- und steuerungssystem (FIPS)

Fähigkeiteninformations-, planungs- und steuerungssystem (FIPS)

Ziel des Fähigkeiteninformations-, planungs- und -steuerungssystems (FIPS) ist die vollständige Digitalisierung der zentralen Prozesse der Landesverteidigung.

Dazu werden 4 Module bereitgestellt:
Die Fähigkeitendatenbank beinhaltet alle relevanten strukturierten (Basis)daten, von den Planungszielen bis zu den Fähigkeitskatalogen und Realisierungszielen.

Das Planungs- und Portfolio-Management-Modul stellt ein klares Bild über den Planungsstand des ÖBH und den Umsetzungsstand der Planungen sicher.

Über das strategische Informationsmanagement sollen hinkünftig sämtliche relevanten Dokumente und Inhalte zentral bereitgestellt werden und einfach gefunden werden können.

Das Modul zur Analyse des IST-Stands und Soll/Ist-Vergleich ermöglicht einen Vergleich zwischen dem geplanten Soll (z.B: 2032+) und dem aktuellen SOLL bzw. dem aktuellen IST.

Telekommunikationsverbund-TKV

Im derzeit laufenden Projekt „TKV" (TeleKommunikationsVerbund) wurden im Jahr 2023 umfangreiche Planungs- und Umsetzungsarbeiten in den Teilbereichen „Ausbildung" sowie „Support/betriebliche Organisation" durchgeführt.

Der TKV ist die Ablöse des derzeit noch aktiven, aber in die Jahre gekommenen NVÖ (NebenstellenVerbund Österreich), also die Modernisierung des gesamten Telefoniesystems des ÖBH. Der NVÖ wird in den nächsten Jahren schrittweise auf TKV umgestellt. Dieses neue System bietet state-of-the-art features im Bereich Telefonie, neue Möglichkeiten im Bereich des Supports (Contactcenter, Telefonzentrale, IVR* und vieles mehr). Im Laufe des Jahres 2023 wurden bereits ca. 15 Liegenschaften im Bereich des ÖBH (MilKden NÖ, OÖ, K, Stmk) von NVÖ auf TKV umgestellt, 2024 werden weitere mind. 15 Liegenschaften folgen. Die Umstellungen konnten durch die ausgezeichnete Zusammenarbeit zwischen IKTS, den involvieren Bereichen DION6, DION4, den betroffenen MilKden und der Auftragsfirma in sehr guter Qualität und mit hoher Effizienz durchgeführt werden.

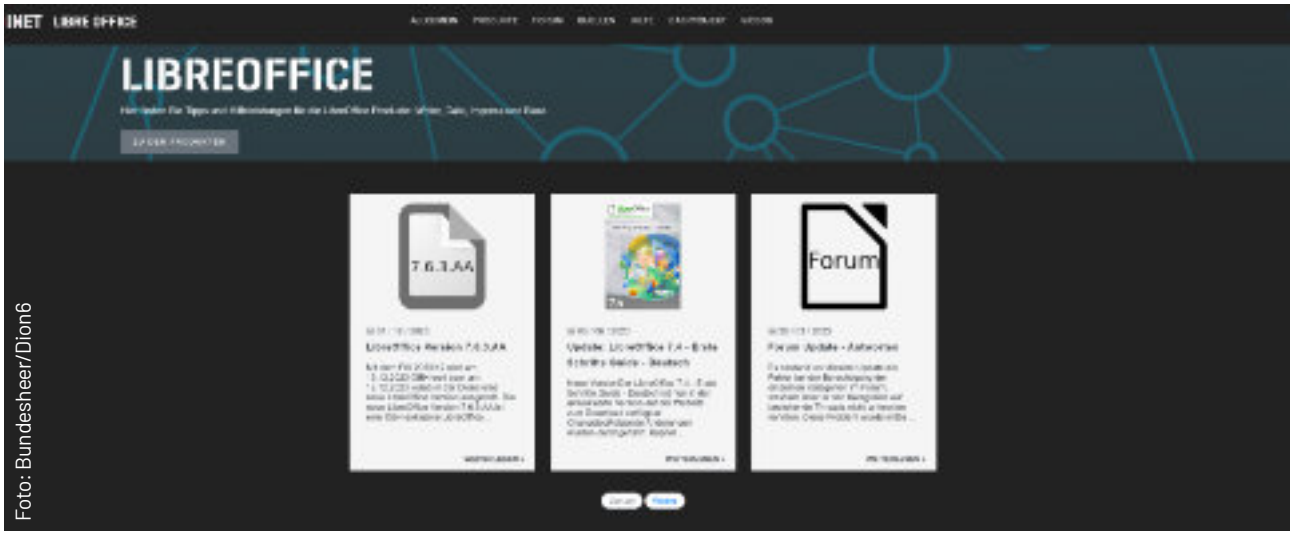


Foto: Bundesheer/Dion6

LibreOffice Intranet-Site

Parallel dazu mussten die wesentlichen Prozesse (Incidentmanagement, Service-Requests, Betriebsprozesse ua.) adaptiert werden und in Abstimmung mit den Bedarfsträgern umgesetzt werden.

Einige kritische Erfolgsfaktoren im Zuge der Realisierung 2023 waren die Umstellung alter Komponenten auf erforderliche neue systemrelevante Komponenten (z.B. Umstellung ETB-Wartungstool auf IDH).

Ausblick 2024:
Im Jahr 2024 ist geplant, zumindest weitere 15 Liegenschaften von NVÖ auf TKV umzustellen, das Contactcenter im Bereich des Supports in Betrieb zu nehmen sowie die Telefonzentrale BMLV (dislozierte auf 6 Standorte) auf TKV umzustellen. Weiters ist die Ausbildung des Betriebs- Techniker- und Supportpersonals weiter voran zu treiben.

Einführung LibreOffice

Zur Erreichung einer digitalen Souveränität des ÖBH wurde durch die oberste Führung des BMLV die Einführung von LibreOffice im SMN angeordnet. Ziel ist die cloud- und herstellerunabhängige Zusammenarbeit innerhalb des BMLV/ÖBH auf Basis von LibreOffice.

Als besonderer Meilenstein wurde mit 1.8.2023 der BMLV-ELAK erfolgreich auf die Open Source Office Suite umgestellt. Seither wurden bis Anfang Dezember 2023 über 500.000 Dokumente mit LibreOffice erstellt. Ein weiterer wichtiger Schritt zur Einführung war die Errichtung eines Vertrages zur Wartungs- und Weiterentwicklung der freien Office Software.

Im April 2024 werden die ersten von Benutzer vorgeschlagenen Verbesserungen bereitgestellt werden, weitere Anpassungen folgen im SMN-Fix-Rhythmus. Alle Mitarbeiter werden eingeladen sich am Weiterentwicklungsprozess zu beteiligen z. B. über das Forum auf der LibreOffice Intranetsite.

Mit LibreOffice wird die Bereitstellung völliger neuer Funktionen möglich. 2024 wird beispielsweise LibreOffice als WebBrowserApplikation u.a. in den BMLV-ELAK integriert, damit wird das gemeinsame, zeitgleiche Bearbeiten von Dokumenten, Tabellen und Präsentationen als ÖBH interne Lösung möglich.

LibreOffice
The Document Foundation

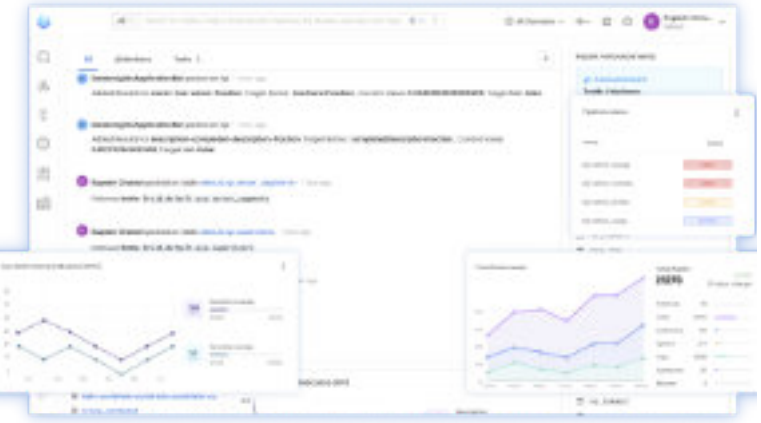
Foto: LibreOffice Foundation

Logo LibreOffice

OpenMetadata–Data Catalog und Datenlandkarte

Die Menge und Komplexität der anfallenden Daten steigt ständig. Bisher gab es nur wenige Möglichkeiten, einen Überblick über potentielle Datenquellen zu erhalten und deren Struktur zu verstehen.

Foto: Bundesheer/Dion6



OpenMetadata-Data Catalog

Im Referat DBSys wurde daher erfolgreich OpenMetadata, eine leistungsstarke Metadatenmanagement-Plattform eingeführt.

Das Ziel von OpenMetadata ist es, Standards und Best Practices für die Verwaltung von Metadaten zu schaffen, um die Zusammenarbeit und Integration zwischen verschiedenen Systemen und Tools zu erleichtern.

OpenMetadata adressiert diese Herausforderungen mit einer umfassenden Lösung. Es bietet eine einheitliche Plattform an, die es ermöglicht, Metadaten unabhängig von der Datenquelle oder dem Speicherort zu erfassen und zu verwalten.

Damit die Effizienz im Umgang mit Daten steigt, bietet OpenMetadata eine breite Palette von Funktionen.

OpenMetadata erleichtert die schnelle Identifikation von Metadaten, fördert die Zusammenarbeit zwischen den Teammitgliedern, verbessert die Datenqualität durch klare Definitionen von Bedeutung und Besitz, ermöglicht detaillierte Einblicke in Datenstrukturen und erleichtert die Nachverfolgung von Datenänderungen über die Zeit. Umfassende Berechtigungsfunktionalitäten regulieren den Metadatenzugriff und gewährleisten die Sicherheit sensibler Daten.

IFF Mode 5 Zertifizierung (Freund/Feind Kennung)

Zur eindeutigen Identifikation (detektiert wird ein Luftziel im ÖBH durch das Primärradar) und verlässlicher Bedrohungsbewertung (IFF) von LFZ im international überwachten Luftraum innerhalb der Reichweite der ÖBH Long Range Radarsensoren (ca. 450 km vorwärts der Staatsgrenze) müssen die Radargeräte des ÖBH zusätzlich mit einer SSR/IFF Mode 5 Funktion im SSR-Empfänger ausgestattet sein.

Dabei wird elektronisch verschlüsselt das Luftfahrzeug abgefragt und durch eine verschlüsselte Antwort vom abgefragten Luftfahrzeug klassifiziert, ob das detektierte Luftfahrzeug grundsätzlich der Bedrohungsstufe friend or foe (IFF) entspricht.

Radaranlage

Die Ortsfesten Radarstationen FADR (Fixed Air Defense Radar) und die verlegbare Radarstation DADR (Deployable Air Defense Radar) „EMMA" sind nach dem bereits abgeschlossenen Upgrade technisch Mode 5 fähig. Um den Mode 5 betreiben zu können, sind elektronische Betriebsschlüssel notwendig. Um diese funktionellen Betriebsschlüssel zu erhalten, müssen die einzelnen Sensorplattformen durch die US/NSA Prüfstelle AIMS zertifiziert werden. Diese „Schlüssel" sind weltweit für einen bestimmten Zeitrahmen einmalig gültig und werden ausschließlich von der NSA/NATO vergeben.

Für die Zertifizierung der Ortsfesten Radarstationen und der verlegbare Radarstation „EMMA" wird das ÖBH bei den umfangreichen Prüfungen für die Zertifizierung durch die Herstellerfirma der Radarplattformen, unterstützt. Ein Zertifizierungszyklus besteht aus „Ground Certification" und der „Flight Certification". Diese wird unter Aufsicht vor Ort von AIMS/NSA durchgeführt und bewertet.

Der Abschluß der Zertifizierung der Sensoren ist für 2025 geplant.

Cyber Truppenübungsplatz & Cyber Range

In einer Welt, die zunehmend von Technologie geprägt ist, stehen militärische Organisationen vor der Herausforderung, sich auf die stetig wachsende Bedrohung durch Cyberangriffe vorzubereiten. Eine innovative Antwort auf diese Herausforderung ist die Einführung von Militärischen Cyber Ranges – hochspezialisierte Trainingsumgebungen, die es ermöglichen, Fähigkeiten im Umgang mit Cyberbedrohungen zu verbessern und sich auf mögliche Szenarien vorzubereiten.

Eine Militärische Cyber Range ist im Wesentlichen eine virtuelle Umgebung, innerhalb derer sowohl Cyberangriff und Cyberverteidigung geübt, als auch neue Technologien erprobt werden können, ohne produktive Systeme zu gefährden. Diese Plattformen bieten realistische Simulationen von Ereignissen im Cyberraum und ermöglichen es so, reale Einsatzsituationen zu simulieren. Der Fokus liegt dabei auf der Entwicklung von Abwehrstrategien, der Erkennung von Angriffen und der Verbesserung technischer und personeller Fähigkeiten.

Foto: Bundesheer/Dion6

Gesamtsystem Cyber-Range + Ausbildungs-Lab im ÖBH

Neben der Beteiligung an mehreren einschlägigen Forschungsprojekten, unterstützt das MilCyZ auch bei der Durchführung multinationaler Übungen, wie der Locked Shields. Bisher können allerdings nur Cyber Ranges von Drittanbietern benutzt werden. Naturgemäß können dadurch nicht alle Anforderungen des Österreichischen Bundesheers abgebildet werden. Daher wurde mit der Entwicklung einer Cyber Range des Österreichischen Bundesheeres im MilCyZ, welche auf militärische Erfordernisse ausgerichtet ist, begonnen.

Neben der Darstellung einer militärischen Netzwerk- und Applikationsumgebung, soll die Cyber Range insbesondere auch Möglichkeiten bieten, externe Hardware aus dem EloKa- (Drohnen, Radar, ...), IoT- und SCADA-Bereich zu integrieren. Didaktisch soll sowohl eine kollaborative Analyse und Evaluierung von Cyberangriffen und Verteidigungsmaßnahmen möglich sein, als auch die Abbildung von Übungsszenarien für die Truppe.

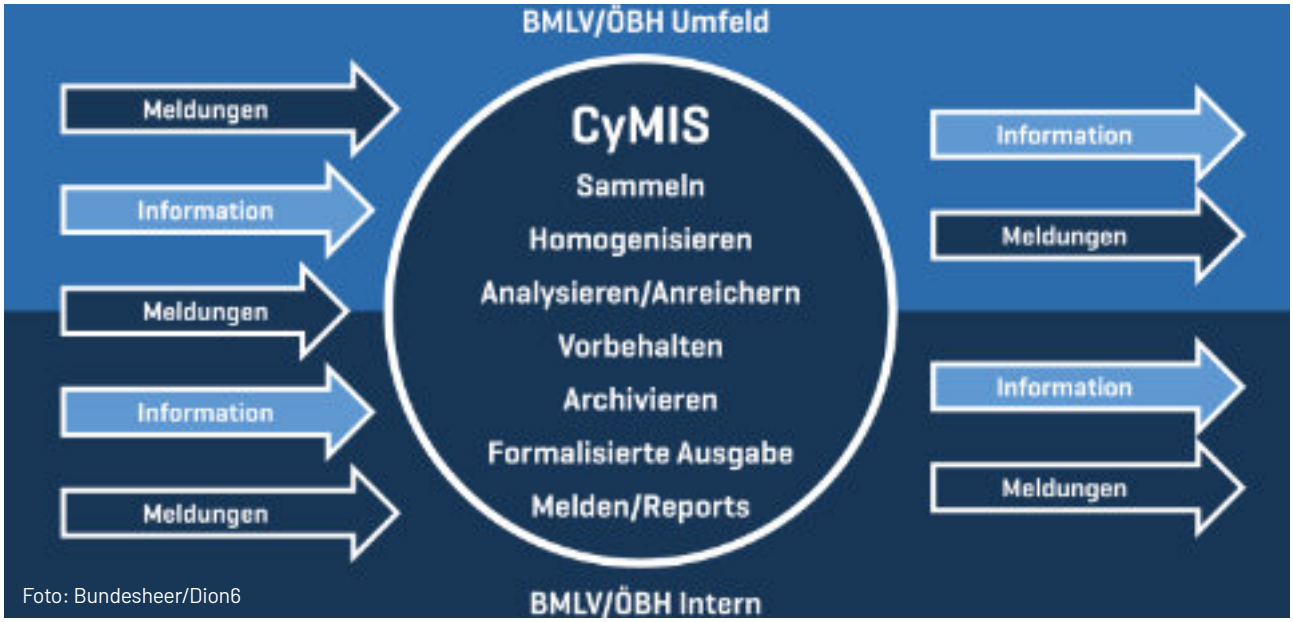
Insgesamt spielen Militärische Cyber Ranges eine entscheidende Rolle in der Vorbereitung auf heutige und zukünftigen Herausforderungen im Cyberraum und bilden eine Ergänzung/Erweiterung zu Cyber-Ausbildungslabors, wie die der FüUS und MilAk.

Sie bieten nicht nur eine sichere Umgebung für Training und Simulation, sondern fördern auch die Zusammenarbeit und den Wissensaustausch im internationalen Kontext. Angesichts der ständig wachsenden Bedrohungen durch Cyberangriffe sind Militärische Cyber Ranges ein unverzichtbares Instrument für jede moderne Streitkraft, welche ihre Fähigkeiten im Cyberraum stärken und sich erfolgreich gegen Cyberbedrohungen verteidigen möchte.

CyMIS – Cyber Lagebild: Digitale Transformation im Dienste der Sicherheit

Im Jahr 2023 hat das ambitionierte Vorhaben "Cyber Lagebild" entscheidende Fortschritte bei der Unterstützung des Schutzes der BMLV/OEBH-IKT-Infrastruktur im Cyber-Raum gemacht. Das noch in der Entwicklung befindliche BMLV/OEBH-Services CyMIS (Cyber-Melde- & Informations-Service) hat einen Meilenstein erreicht, indem es erstmals den kompletten Lagebildprozess in einer Entwicklungsumgebung abgebildet hat.

Dies markiert einen bedeutenden Schritt in Richtung einer sinnvollen Digitalisierung des Erstellungsprozesses.



Cyber-Melde-& Informations-Service - CyMIS

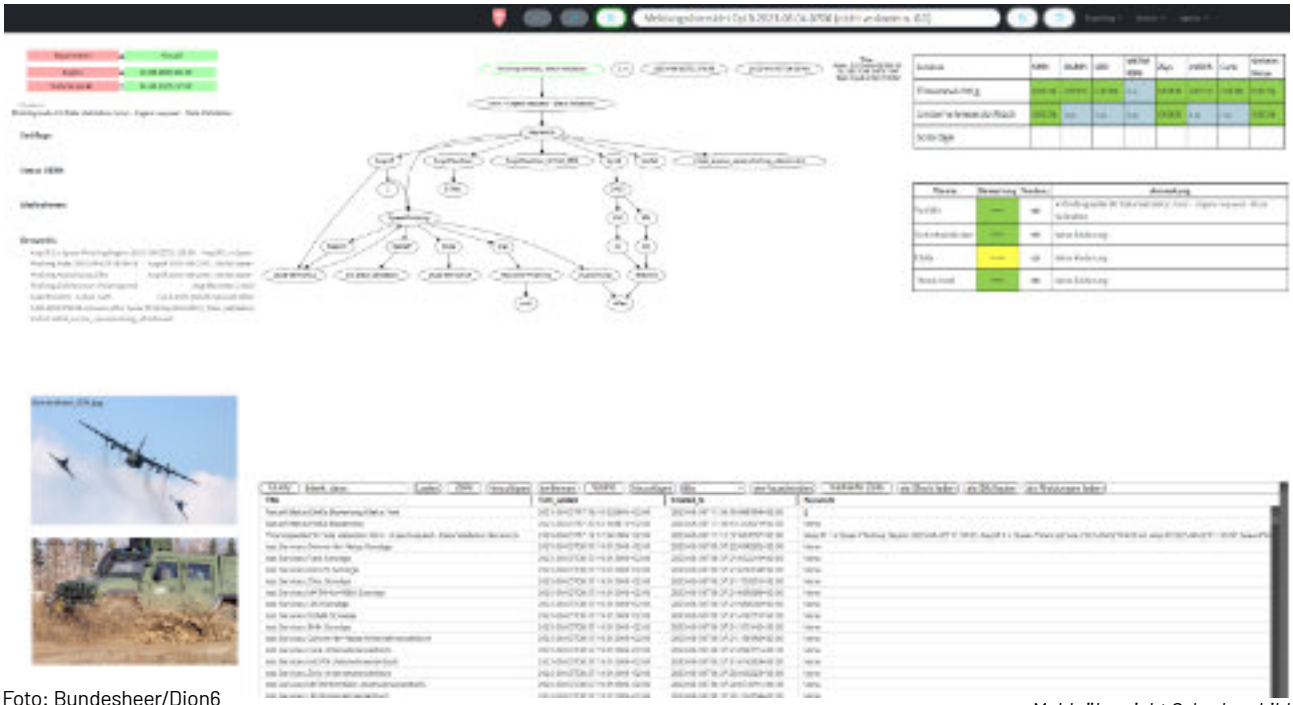


Foto: Bundesheer/Dion6

Meldeübersicht Cyberlagebild

1. Generische Aufbereitung und Verarbeitung von Informationen
CyMIS verfolgt das Ziel, die Aufbereitung und Verarbeitung von Informationen möglichst generisch und einfach zu gestalten. Speziell angepasste Software-Agents, programmiert vom mil-Cyber-LZ-Team, ermöglichen die Anbindung von Informationsquellen. Die homogenisierten Daten werden als generische Meldungen gespeichert und über eine Webapplikation für weitere Verwendung, Analyse, Bewertung, und Erstellung von Lagebildern in Form von Dashboards und Reports bereitgestellt.

2. Einfache Meldungserfassung und Zuordnung
CyMIS erleichtert die Erfassung und Zuordnung von Meldungen sowie die flexible Gestaltung von Lagebildern in Dashboard- und Reportform. Durch einfache Markierung von Meldungen und die Auswahl von Funktionen in der Anwendung können neue Meldungen erfasst und Inhalte vielseitig dargestellt werden, sei es als Bilder, Dokumente, Wissensgrafiken oder zeitabhängig in Form eines GANTT-Diagramms.

3. Einpflegen und Aktualisieren von Strukturen
Erstmals ermöglicht CyMIS das Einpflegen und up-to-date-Halten von Strukturen wie IKT-System-Topologien und Organigrammen mittels Meldungen. Der aktuelle Zustand der eingemeldeten Objekte wird durch (Status-) Meldungen erfasst, wodurch eine Auswertung und Analyse aufgrund der in CyMIS erfassten Beziehungen zwischen den Meldungen möglich ist. Grafische Visualisierungen unterstützen dabei die rasche Erfassung dieser Abhängigkeiten.

4. Integration von ML und KI
Die Integration von Machine Learning (ML) und Künstlicher Intelligenz (KI) steht im Fokus der Weiterentwicklung von CyMIS. Diese Hilfsmittel sollen dem Benutzer in der ersten Phase Vorschläge unterbreiten, die nach Kontrolle rasch übernommen werden können. Dies umfasst die Zusammenfassung von Texten, Beschlagwortung, Erstellung von Trainingsszenarien, situative Meldungsbausteine und das Erfassen von Strukturen aus Texten, Tabellen und Bildern. CyMIS unterstützt auch das Training von ML & KI.

Foto: Bundesheer/Dion6

Meldeerfassung und Übersicht Cyberlagebild

5. Zukunftsausrichtung von CyMIS

Zusammenfassend stellt CyMIS ein zukunftssicheres Werkzeug zur Erfassung von Meldungen und Informationen sowie deren Zusammenhänge in digitalisierter Form dar. Die erste Produktiv-Version soll 2024 im BMLV/OEBH in Betrieb gehen und zunächst im MilCyZ für die Erstellung und Weitergabe der Cyberlage dienen. In weiterer Folge ist die Anpassung für den Einsatz in anderen Organisationseinheiten geplant, um den individuellen Bedarf zu decken und einen ganzheitlichen Schutz der IKT-Infrastruktur zu gewährleisten. CyMIS positioniert sich somit als essenzielles Instrument im Dienste der Sicherheit im digitalen Zeitalter.

Cyber Threat Intelligence (CTI) in der Cyber-Security

Die digitale Landschaft unterliegt ständigen Veränderungen, wobei Cyberangriffe zunehmend komplexer und raffinierter werden. Um dieser Herausforderung effektiv zu begegnen, ist die Nutzung von Cyber Threat Intelligence (CTI) von entscheidender Bedeutung. Neben bereits im Einsatz befindlichen Werkzeugen wurden im letzten Jahr erfolgreich Erweiterungen umgesetzt.

I. Hintergrund und Herausforderungen

Die zunehmende Vernetzung und Digitalisierung militärischer Infrastrukturen haben die Angriffsfläche für Cyberbedrohungen erheblich erweitert. Traditionelle Sicherheitsmaßnahmen reichen nicht mehr aus, um den fortgeschrittenen Bedrohungen ständig standzuhalten.

Daher war – zusätzlich zu Anpassungen der Cyber-Defence-Systeme – die Einführung eines umfassenden CTI-Programms notwendig, um auf Bedrohungen reagieren und die Verteidigungsfähigkeiten stärken zu können. Zudem ermöglicht dieses Vorhaben Verbesserungen in der Cyber- und Bedrohungslage, sowie verbesserte Zusammenarbeit über die diversen Dienststellen hinweg.

II. CTI-Plattformen

Seit längerem kommt MISP, die „Malware Information Sharing Platform", als Standardwerkzeug für den Austausch von CTI-Informationen innerhalb der CERT-Community im Allgemeinen, aber auch im BMLV/ÖBH im Speziellen, zum Einsatz.

MISP ermöglicht nicht nur einen strukturierten Datenaustausch, sondern fördert auch die Zusammenarbeit. Es ist im BMLV/ÖBH bereits seit Jahren im Einsatz, ermöglicht die Integration von CTI in die täglichen Abläufe und somit eine zügige Reaktion auf neue Bedrohungen. Dennoch erwies sich diese Plattform und die enthaltenen Daten als nicht leistungsfähig genug. Zudem sind die Community-Daten wichtig, stellen jedoch oft nur ein Bruchteil der relevanten Inhalte dar.

Bild: https://www.misp-project.org

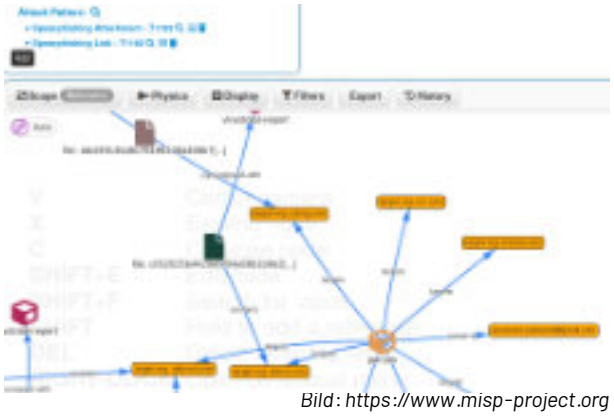


Bild: https://www.misp-project.org

Aus o.g. Grund wurde bereits Ende 2021 begonnen, nach Ergänzungen zu suchen.
Eine sorgfältige Auswahl und Integration von (kommerziellen) Datenfeeds und geeigneten Threat Intelligence Platform (TIP) ermöglicht künftig die vollständige Automatisierung von Prozessen zur umfassenden Nutzung (CTI-Zyklus) der vielfältigen Daten und verbesserte die Effizienz der Cyberabwehr.

Weitere Integrationen in zusätzliche Sicherheitssysteme, sowie Verbesserungen der Prozesse und Zusammenarbeit zum größtmöglichen Nutzen für den Eigenschutz des BMLV/ÖBH sind geplant.

IV. Erfolge und Lessons Learned

Die erfolgreiche Implementierung von CTI in der Cyber Defence des BMLV/ÖBH führte zu signifikanten Erfolgen

- Verbesserte Reaktionszeiten: Die automatisierte Integration von CTI ermöglicht eine schnellere Erkennung und Reaktion auf Bedrohungen, wodurch negative Auswirkungen von Cyber-Angriffen minimiert werden.

- Effektivere Bedrohungsabwehr: Die Kombination von MISP und TIP verbesserte die Gesamteffizienz der Cyberabwehr. Die automatisierte Anwendung von Sperrlisten und proaktive, Kontext-unterstützte Bedrohungsaufklärung tragen laufend dazu bei, Angriffe abzuwehren, bevor sie größeren Schaden anrichten können.

Neben Erfolgen gibt es auch wesentliche LI/LL

- Das komplexe System, als auch die ständig verändernde Bedrohungslandschaft, erfordern kontinuierliche Schulungen und Weiterbildungen der Cyber-Experten, um mit den neuesten Entwicklungen Schritt zu halten.

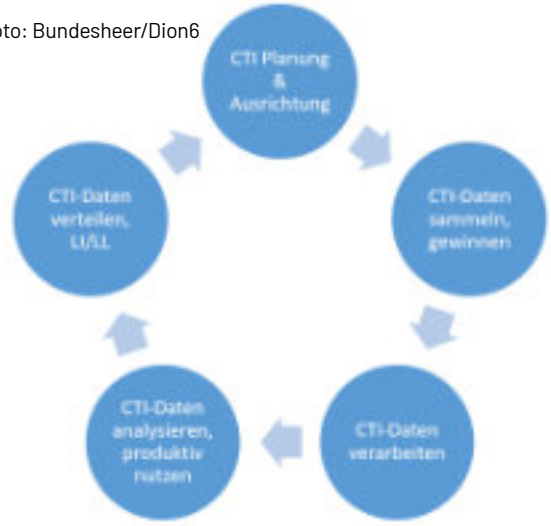
- Die Qualität und Relevanz der ausgetauschten CTI-Informationen sind entscheidend. Eine kontinuierliche Überprüfung und Validierung sind erforderlich, um sicherzustellen, dass die Daten zuverlässig und aktuell sind.

- Die Leistung der eingesetzten TIP sowie der Datenfeeds muss regelmäßig evaluiert werden, um sicherzustellen, dass sie auch neue Anforderungen und Bedrohungen standhalten.

V. Fazit und Ausblick

Die Kombination von MISP und TIP erweist sich als effektiv. Mit den CTI-Daten führt dies zu einer erheblichen Stärkung der Sicherheitsmaßnahmen. Kontinuierliche Anpassung und Weiterentwicklung sind entscheidend, um mit den sich ständig verändernden Bedrohungen Schritt zu halten und eine nachhaltig erfolgreiche Cyberabwehr für das BMLV/ÖBH zu gewährleisten.

Foto: Bundesheer/Dion6



Cyber treat Intelligence CTI

Navigation Warfare Übung GNSS

2023 war ein besonders umtriebiges Jahr für das Referat Navigation des IMG. Über insgesamt sechs Wochen verteilt, fanden mehrere Navigation Warfare (NAVWAR)-Übungen auf den Truppenübungsplätzen des BMLV statt.

Die Kampagnen erstreckten sich über verschiedene Termine, darunter die Messkampagnen vom 03. bis 07. April 2023 am TÜPl SA, welche primär dazu dienten das eigene Gerärt zu vermessen. Gleich anschließend wurde im Rahmen der "International Survey Networking Exercise 2023" (iSNEx23) (17. bis 28. April 2023), organisiert durch das Ref Grundlagen, das Thema NAVWAR den internationalen Vermessungsexperten nähergebracht.

Dabei führte das Referat Navigation während dieser Übungen Vorführungen zu den Themen NAVWAR bzw. Jamming/Spoofing durch, um das Bewusstsein der Teilnehmer für diese wichtigen Themen zu schärfen und die realen Auswirkungen auf ihre Vermessungsgeräte zu beobachten.
Eine weitere Maßnahme umfasste das elektromagnetische Vermessen des TÜPl SA durch Miliz-Anteile des IMG, sowie diversen DSt vom 28. August bis 01. September 2023. Diese großangelegte Übung mit Zuhilfenahme von diversen Lfz (212, Drohen) stellt die Grundlage für zukünftige Übungen dar.

In der darauffolgenden Woche fand dann wie gewohnt der zweite Teil der „Seetaler Fesselspiele“ statt, bei welcher eine beachtliche Anzahl nationaler als auch internationaler Teilnehmer diverse Mess- und Versuchsreihen durchführten.

Diese NAVWAR-Übungen tragen dazu bei, die Fähigkeiten im Umgang mit PNT-Technologien zu verbessern und die Sicherheit gegenüber Störungen und Manipulationen zu gewährleisten.

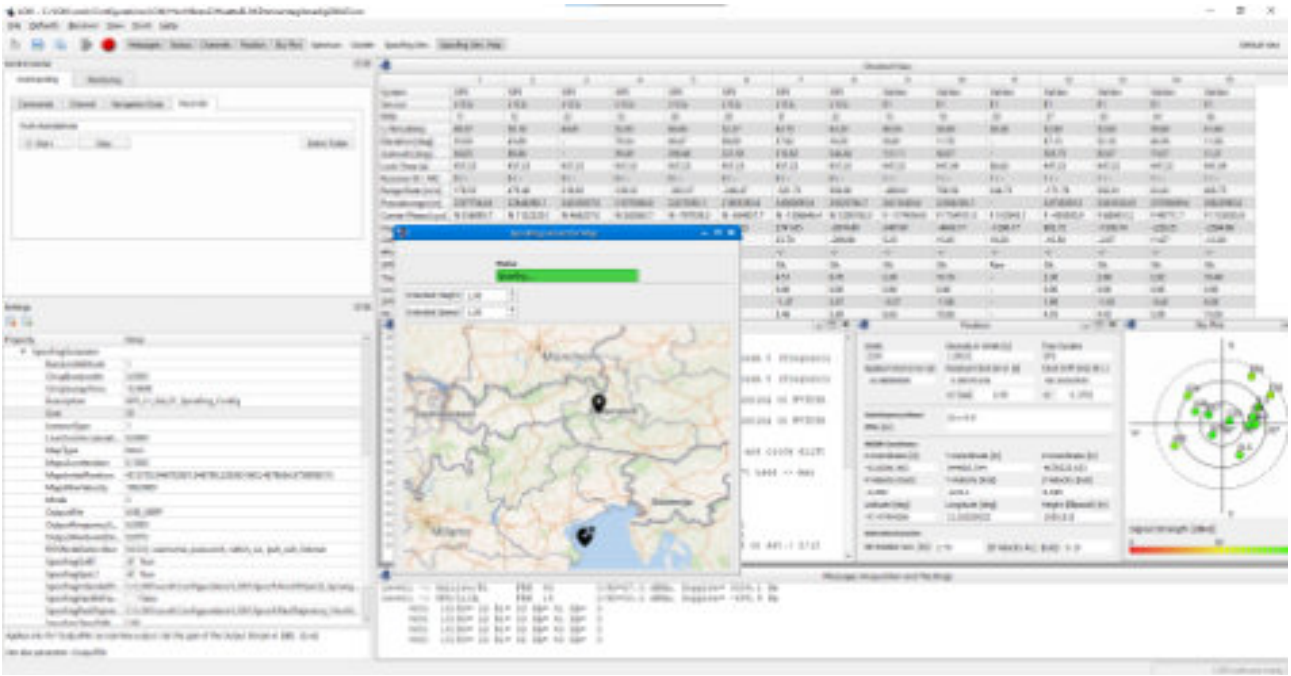


Foto: Bundesheer/Dion6

NAVWAR Jamming/Spoofing

ÖBH-GIS-Tage in Salzburg im Zeichen der Digitalisierung im ÖBH

Von 23.11. bis 24.11.2023 haben die 2. ÖBH-GIS-Tage in Salzburg stattgefunden. Der Leiter des geographischen Fachdienstes im ÖBH und des Institutes für Militärisches Geowesen (IMG) und sein Stellvertreter, Bgdr Dr. Teichmann und ObstdhmtD Dr. Eder, konnten rund 60 Teilnehmer, die sich in ihrem dienstlichen Umfeld regelmäßig mit Geographischen Informatiossystemen (GIS) und Digitalisierung räumlicher Daten beschäftigen im Namen des IMG begrüßen.

Die Veranstaltung diente zum persönlichen Kennenlernen und zum umfassenden Erfahrungsaustausch in dieser sehr aktiven GIS-Community, die mittlerweile zahlreiche Dienststellen des BMLV und ÖBH umfasst.

In über 20 abwechslungsreichen Impulsvorträgen wurde eindrucksvoll gezeigt, wie der Einsatz von GIS-Software den zeitgemäßen Arbeitsalltag bereichern und vielfach sogar entlasten kann.

Das breite Spektrum der Vortragsthemen reichte dabei vom Einsatz von GIS auf Truppenübungsplätzen über Anwendungen in den Luftstreitkräften bis zu 3D-Visualisierungen für internationale Einsätze.

Das positive Feedback zum Einsatz von GIS-Software im ÖBH bestätigt das GIS-/Geo-Support-Team des IMG, bestehend aus OR Mag. Kautz, OR Mag. Fürpass und ADir Pruzsinszky Akad. Geoinf., mit seiner Unterstützung auch weiterhin der aus rund 350 Usern bestehenden GIS-Community des ÖBH mit fachlicher Kompetenz zur Verfügung zu stehen.

Als Grundlage zur Nutzung von GIS-Software dient das Nutzungskonzept „MilGeoWesen Software; Bereitstellung von QGIS (Open-Source GIS) in den gemanagten Netzen und auf "stand alone" Arbeitsplätzen des Ressorts;

Für Informationen und Anfragen steht das GIS-GeoSupport Team des IMG unter: gis@bmlv.gv.at zur Verfügung.

ÖBH-GIS-Tage in Salzburg

Teilnehmer ÖBH-GIS-Tage

Benutzerbetreuung

Die Abteilung BenBe ist das Aushängeschild der Dion6 und der Erstkontakt für Anwender, welche Hilfe in Zusammenhang mit Ihrer I(K)T-Ausstattung benötigen.

Hierbei ist die Abteilung BenBe regional in drei Benutzerbetreuungen (Wien, Graz, Salzburg) unterteilt, welche alle Endanwender-Support betreiben, aber zusätzlich noch spezielle Ausprägungen besitzen (z.B. Support der Zentralstelle durch Wien, TCN durch Salzburg, VKS durch Graz).

Darüber hinaus gibt es noch speziellen Support für wichtige Services bzw. Anwendungsgebiete, welche durch sogenannte Serviceschwerpunkte (SSPs) abgedeckt werden. Hier sind das SSP-ZentrS (ELAK), SSP-MTM, SSP-Eurofighter, SSP-ZAbl und SSP-Internet zu nennen.

Das Jahr 2023 hat wie die Jahre zuvor mit Aufgaben, mannigfaltigsten Problemstellungen und Projekten (als ein Beispiel sei hier das öweite LAN-Druckerrollout-/Ablöse erwähnt) begonnen, welche aber trotz Personalnot bei gleichzeitig wachsendem Aufgabenspektrum alle erfolgreich umgesetzt werden konnten.

Foto: pixabay.com

Foto: pixabay.com

Support der Zentralstelle

Im Bereich Wien wurde der Support der Zentralstelle unverändert gut wahrgenommen, es konnten alle Anfragen bzw. Wünsche zur Zufriedenheit der Anwender beantwortet bzw. umgesetzt werden.

Zu den Highlights gehören hier sicherlich die Einführung von LibreOffice (vorerst in ELAK) als Ablöse des MS Office-Pakets und des Bereitstellens des Supports für die vier LibreOffice Applikationen Writer, Calc, Impress und Base.

Das ganze Jahr über war neben dem Anwendersupport fast im Hintergrund und unbemerkt die Mitarbeit am Projekt „Erneuerung der Liegenschafts-Server" (Testaufbau eines neuen Servers im dafür vorgesehenen Rack samt Verkabelung in der Kaserne Arsenal, Errichtung einer Klonstrasse für die zukünftigen Server im Kommandogebäude Heckenast-Burian, Testdatensicherung aus einer Teststellung in der Militärischen Liegenschaft Breitensee).

Ein weiteres großes Projekt ist der TKV (TeleKommunikationsVerbund), welcher den NVÖ ablösen wird. Hier wurden weitere Liegenschaften umgestellt und die Prozess- und Supportinfrastruktur aufgebaut. Ebenso wurde bereits mit den Schulungen für das Vorort- und Servicedesk-Personal begonnen.

Foto: pixabay.com

Unsere IT-Hotline

Der Bereich Salzburg war neben dem Militärischen Support durch die Systemeinführung im Bereich TCN geprägt. Nach dem erfolgreichen Systemtest im Februar 2023 wurde mit der Auslieferung an die Truppe begonnen.

Videokonferenzsysteme stark in Gebrauch

Beim „VKS" (Videokonferenz System) wurde die darunterliegende Serverinfrastruktur erneuert, um ein noch besseres, stabileres und leistungsfähigeres System zur Verfügung stellen zu können.
Ebenso wurde der Support der Auslandslokationen durch Personalentsendungen sichergestellt (2x Libanon, 2x Kosovo).

Darüber hinaus wurde auch der Support für die „Airpower 2023" gestellt.

Serviceschwerpunkt-Internet

Zurverfügungstellung eines leistungsfähigen WLANs im Rahmen der „IKT Sicherheitskonferenz 2023" für das Veranstaltungsteam und selektive Präsentationen.
Weiters wurden 2 Mitarbeiter zu Service-/Wartungs- und Verbesserungstätigkeiten betreffend das soziale Internet des österreichischen Kontingents im „Camp Naqura im Libanon" entsendet.

Ausblick in die Zukunft

Beginnend mit dem Jahr 2024 wird mit der Umsetzung des Projektes „Erneuerung der Liegenschafts-Server" begonnen. Diese soll/wird mit so wenig Ausfallzeit wie möglich für die Enduser umgesetzt werden. Der große Gewinn hierbei ist nicht nur eine garantiebedingte Firmeninstandsetzung im Fehlerfall, sondern vor allem der lange benötigte Speicherplatzzuwachs auf den Liegenschafts-Servern.

Getreu dem Motto – „bei uns ist jeder richtig", wird die Abteilung BenBe auch in Zukunft alle Anfragen und Anliegen zur vollsten Zufriedenheit der Anwender umsetzen.


Foto: pixabay.com

Bundesministerium für Landesverteidigung

Abbildungsverzeichnis

Bundesministerium für Landesverteidigung

Stichwortverzeichnis

1-9

1st Level Support	Erste Anlaufstelle für IKT-Probleme
2nd Level Support	Zweite Ebene für spezifischere IKT-Probleme
24/7	24 Stunden am Tag, sieben Tage die Woche

A

AAB	Aufklärungs- und Artilleriebataillon 3
AAG21	„Air to Air Gunnery" (Luft-Luft Schieß-Übung)
ABCIS	Atomar-Biologisch-Chemisches Informationsssystem
ABNA	Airgapped Bastion Network Austria (physisch isoliertes Netzwerk)
AbwA	Abwehramt
Accesspoints	Zugangspunkte zu Netzwerken
AddOn	Erweiterung
AI	Artificial Intelligence (künstliche Intelligenz)
AIT	Austrian Institute of Technology (Außeruniversitäre Forschungseinrichtung in Österreich
All Flash	Schnelle Speichertechnologie (nichtflüchtig, behält Speicher trotz Abschaltung)
AMZ	Arbeitsmedizinisches Zentrum
APEX	Application Express (Webbasierte Softwareentwicklungs-umgebung)
Appl	Abteilung Applikation
Application Level Firewalling	Netzwerksicherheitskomponente auf Anwendungsebene
Arbeitsplatzfixes	Fehlerbehebungspunkte von Softwareproblemen
ArcGIS	Geoinformationssystem-Software
ARWT	Amt für Rüstung und Wehrtechnik

ASECOS	System zur verschlüsselten Übertragung von Daten
AssE	Assistenzeinsatz
Audit	Überprüfung
AÜG	Arbeitskräfteüberlassungsgesetz
AUT	Austria
AUTCON	Austrian Contingent (Kontingent im Auslandseinsatz)
AUVA	Allgemeine Unfallversicherungsanstalt

B

Backbone	Rückgrat (Hauptleitungen) von Netzwerken
BACnet	Building, Automation and Control Networks (Netzwerkprotokoll für Gebäudeautomation
BACtwin	Building, Automation and Control Twin (Digitaler Zwilling)
BandlibrarySystem	Bandbibliothek zur Datenspeicherung auf Magnetbändern
BatchFenster	Konsolenfenster des Betriebssystems
BBG	Bundesbeschaffungsgesellschaft
BenBe	Benutzer-Betreuung
Big Data	Große komplexe Datenmengen
Bitbox	Browser in the Box (Browser in virtueller Maschine, um Angriffe auf das Host-System zu verhindern)
BK/C	Bundeskriminalamt/Abteilung Cyber Crime and Competence Center
BKA	Bundeskanzleramt
Blackhawk	Transporthubschrauber S-70 der Firma Sikorsky
BlueScreen	Fehleranzeige nach schwerwiegendem Problem im Betriebssystem
BMDW	Bundesministerium für Digitalisierung und Wirtschaftsstandort
BMEIA	Bundesministerium für europ. und intern. Angelegenheiten
BMI	Bundesministerium für Inneres

BMLRT ▶ Bundesministerium für Landwirtschaft, Regionen und Tourismus

BMLV ▶ Bundesministerium für Landesverteidigung

BMS ▶ Battlefield Management System

BOS ▶ Behörden und Organisationen mit Sicherheitsaufgaben

Bruteforce ▶ Methode, unerlaubten Zugriff auf IT-Systeme zu erlangen

BRZ ▶ Bundesrechenzentrum

BV Meldung ▶ Meldung Besonderer Vorfälle

BVT ▶ Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

BVT/CSC ▶ BVT/Cyber-Security-Center

BWÜ ▶ Beorderten-Waffenübung

C

C4 ▶ Cyber Crime and Competence Center (nationale Koordinierungs- und Meldestelle zur Bekämpfung von Cyberkriminalität)

CAD ▶ Computer-Aided-Design (Rechnerunterstütztes Konstruieren)

Carrier-Ethernet ▶ Erweiterung von Ethernet für Telekommunikation

CCI ▶ Controlled cryptographic Item

CFBLNet ▶ Combined Federated Battle Laboratories Network (Netzwerk zum simulieren von Trainingsumgebungen)

ChangeManagement ▶ Laufendes umfassendes Veränderungsmanagement

Chat ▶ digitale Umgebung zum Nachrichtenaustausch

ChdStb ▶ Chef des Stabes

Chipkarte ▶ Mittel zur Authentifizierung

CIO/CDO ▶ Chief Informational Officer/Chief Digital Officer (strategische Position in der Führungsebene im Bereich IT)

CIRP ▶ College International pour la Recherche en Productique (Internationale Akademie für Produktionstechnik)

CISDefence ▶ Computer and Information Systems Defence

CKM ▶ Cyberkrisenmanagement

CKMS	Chipkarten-Management-System
CMS	Content Management System
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CO-IServices	Community of Interest Services (Interessensgemeinschaft)
COMEX	Communication Exercise 20
COMMON ROOF	Internationale Übung für Interoperabilität im DACH Raum
COMSEC	Communication security
Content Disarm and Reconstruction	Technologie um Schadsoftware aus Daten zu entfernen
Core-Services	Kerngruppe wichtiger Anwendungen (z.B. E-Mail, VPN, etc.)
Covid-19	SARS CoV-2 Virus („Corona-Pandemie")
CR	Common Roof (Übung)
CST	Custodial Support Team
Custom App	Angepasste Applikation
CWIX	Coalition Warrior Interoperability Exercise
Cybär	Maskottchen IKT&CySihZ
CyberTruppe	Militärisches Element zur Beherrschung des vollen Spektrums des Kampfes in Computernetzwerken
Cyberabwehr	Abwendung von Attacken auf Netzwerke und Computersysteme
Cyberangriff	Gezielte Attacke auf größere Rechnernetzwerke, spezifisch wichtiger Infrastruktur
Cyberbedrohung	Bedrohungen im Cyberraum (Cyber Kriminalität, Identitätsmissbrauch, Cyberangriffe oder der Missbrauch des Internets)
Cyberdomäne	Dimension der militärischen Einsatzführung, wie Land, Luft, See oder Weltraum
Cyberkoordinator	Steuerungsorgan der Cyberdömane des BMLV auf strategischer Ebene
Cyberkräfte	Teilstreitkraft des ÖBH zur Beherrschung sämtlicher taktischen Maßnahmen zum Schutz der militärischen Netze
Cyberkriminalität	Straf- oder verwaltungsstrafrechtlich relevante, normierte Angriffe aus dem Cyberraum

Cyberkrise	Eskalationsstufe von Cybervorfällen, ausgerufen durch den BMI (NISG §3 Abs.22, §24)
Cyberlage	Darstellung der Eigenlage des ÖBH im Cyberraum und als Teil des militärischen Gesamtlagebildes
CyberOps	Cyber-Operations (Handlung im Cyberraum)
Cyberraum	Der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab
Cybersicherheit	Gesamtheit aller Technologien, Prozesse und Vorgehensweisen , die Netzwerke, Computer, Programme und Daten vor Angriffen, Schäden oder unerlaubten Zugriffen schützen sollen
Cyberverteidigung	Gesamtheit aller Maßnahmen zum Schutz vor Cyberangriffen und zur Erhöhung der Cybersicherheit
Cybervorfälle	Böswilliges oder versehentlich herbeigeführtes Ereignis, das die Cybersicherheit eines Informationssystems oder die Sicherheit der verarbeiteten Informationen gefährdet oder Sicherheitsrichtlinien, Sicherheitsprozesse oder Nutzungsbedingungen verletzt

D

DACAN	distribution and accounting agency NATO
DACH	Deutschland-Österreich-Schweiz
DADR	Deployable air defence radar
DAEDALUS	Luftraumsicherungsoperation
Datenfunksoftware	Software zur Übertragung von Daten über Funk
Dashboard	Visualisierung von Daten
Data Loss Prevention	Maßnahme zum Schutz der Vertraulichkeit von Daten
DBMS	Datenbank Management System
DDoS	Distributed Denial of Service
DGIWG	Defence Geospatial Information Working Group
DGMN	Dynamisches gesichertes Militärnetz
DhFMO	Diensthabender Fernmeldeoffizier
DhSys	Diensthabendes System
Dienstenetz	Logische Segmentierung des Trägernetzes (Leitung, Router) Netzwerkverkehr wird für unterschiedliche Kunden über ein und dieselbe Netzinfrastruktur logisch von einander getrennt und geroutet. Für jeden Kunden wird das Netz spezifisch abgesichert und verschlüsselt. Es werden somit mehrere Kundenentze zur Verfügung gestellt.

Digitaler Zwilling	▶ Digitale Repräsentanz eines materiellen oder immateriellen Objekts/Prozesses aus der realen Welt in der digitalen Welt
Digitalisierung	▶ Umwandlung von analogen Werten in informationstechnisch verarbeitbare Daten
dpi	▶ Dots per inch (Drucktechnische Auflösung)
DSB	▶ Datenschutzbeauftragter

E

E-Mail	▶ Electronic Mail (Digitale Post)
early life support	▶ Lösung von operativen Problemen während der Anlaufphase
EDA	▶ European Defence Agency
EDRS	▶ Endpoint Detection Response System
EFA	▶ Europäisches Forum Alpbach
Ego-Perspektive	▶ Ansicht, als wäre man die jeweilige Person
Einsatz	▶ Tätigwerden des ÖBH zur Erfüllung seiner verfassungsgesetzlich verankerten Aufgaben lt. §2 Abs.1 Wehrgesetz
ELAK	▶ Elektronischer Akt (unterscheide BMLV-ELAK und ELAK im Bund)
EloKa	▶ Elektronische Kampfführung
EloKa-Truppe	▶ Elektronische Kampfführungs-Truppe
Emotet	▶ Computer Schadsoftware
EOW	▶ EU Operations WAN (Europaweites gesichertes Netzwerk)
ePAT	▶ Elektronisches Patienten Informations System
EPR	▶ Eignungsprüfung
ERGIS	▶ Ergänzungsinformationssystem
ESS	▶ Employee Self Service
ETB	▶ Elektronisches Telefonbuch
Ethernet	▶ Kommunikationsstandard für Software und Hardware in einem kabelgebundenen Netzwerk
EU Battle Groups	▶ European Union Battle Groups

EUBG	European Union Battle Groups 2020
EUCH	European Challenge 2020 (Cyber-Übung)
Eurofighter Typhoon	Abfangjäger des Österreichischen Bundesheeres
EUTM	European Training Mission
Explore AI	Forschungsprojekt über den Einfluss von künstlicher Intelligenz auf das Militärwesen im österreichischen Kontext
Extranet	Erweiterung des Intranets, welches nur für eine festgelegte Gruppe an Nutzern zugänglich ist

F

Fauna	Tierwelt
FEG	Forterhaltungsgebühr
Fertigungsklausel	Festlegung von Unterschriftsberechtigungen und Formulierungen
FFT Proxy	Friendly Force Tracking Proxy
FGP	Abteilung für Fahrzeuge, Geräte und persönliche Ausrüstung
Fibre	Glasfaser
Firewall	Netzwerksicherheitskomponente
First-Line-of-Defence	Erste Verteidigungslinie
FM-Planung	Fernmelde-Planung
FMN	Federated Mission Networking
FMSysÖBH	Fernmeldesystem ÖBH
FNMS	Funknetzmanagementsystem (Software)
Force Provider	IKT-Fähigkeiten des ÖBH, die Bedarfsträgern nicht zur Verfügung stehen, sind zentral beim IKT&CySihZ bereitzuhalten
FORTE	Österreichisches Verteidigungsforschungsprogramm
FORTE CADSP	Forschungsprojekt Cyber Attack Decision and Support Platform
FOSSGIS	Free & Open Source Software for GeoInformationSystems
Frq&SchlW	Frequenz- und Schlüsselwesen

Führungsmittel	Systeme, Geräte und technische Verfahren mit denen erforderliche Informationen gewonnen, verarbeitet, gespeichert und übertragen werden, um die eigene Führung sicherzustellen und die gegnerische zu beeinträchtigen
FüSim	Führungssimulator
FüU	Führungsunterstützung
FüUB	Führungsunterstützungsbataillon

G

G6	Generalstabsabteilung 6
GA-Funktionsliste	Gebäude-Automations Funktionsliste
Galileo-PRS	Galileo Public Regulated Service
Gebäudeautomation	Überbegriff für Überwachungs-, Steuer- und Regelungseinrichtungen in Gebäuden
GeoMetOc-Syndicate	Geospacial Meteorological and Oceanographic Syndicate
GeoOps	Geographic Operations (Geooperationen)
GIS	Geografisches Informations System
Global Mapper	GIS Software-Komplettlösung
GNSS	Global Navigation Satellite System
GOB	Geschäftsfallorientierte Bearbeitung
Goldhaube	Passives Element der österreichischen militärischen Luftraumüberwachung (primär und sekundär)
GovCERT	Governmental Computer Emergency Readyness Team
GovNetBox	Hochsichere VPN-Lösung für bestimmte Geheimhaltungsstufen
GPS	Global Positioning System
Grafana	Programm zur graphischen Darstellung von Daten
Grundwehrdienst	Pflicht eines jeden österreichischen Staatsbürgers, der als tauglich eingestuft ist
GStb	Generalstab
GUI	Graphical User Interface (grafische Benutzeroberfläche)

GWD	Grundwehrdiener/-dienst
GWS	GeoWebService

H

Hardware	Physische Komponenten in der IT
Headset	Kopfhörer mit Mikrofon
HF	High Frequency (Hohe Frequenz)
HGG	Heeresgebührengesetz
HGLLG	Hochgebirgslandelehrgang
HLogZ	Heereslogistikzentrum
HNaA	Heeresnachrichtenamt
Homeoffice	Büroarbeit am Wohnort
Hotline	Heißer Draht (Telefonischer Auskunfts- und Beratungsdienst)
HPA	Heerespersonalamt
HTBLVA	Höhere technische Bundes Lehr- und Versuchsanstalt
HTS	Heerestruppenschule
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hybride Bedrohungen	Einsatz von konventionellen und unkonventionellen Methoden durch staatliche und nichtstaatliche Akteure in koordinierter Weise, ohne die Schwelle eines offiziell erklärten Krieges zu erreichen.

I

i3VE-Smartphone	iPhones speziell gesichert für das sichere militärische Netz
Identity Awareness	Identitätsbewusstsein
IDU	Integrated Display Unit (Displayeinheit für Luftfahrzeuge)
IFC	Industry Foundation Classes (ISO-Standard zur digitalen Beschreibung von Gebäudemodellen)
IFF	Identification Friend/Foe (Freund-Feind-Erkennung)

IKDOK	Innerer Kreis der operativen Koordinierungsstruktur
IKT	Informations- und Kommunikationstechnologie (Überbegriff aller computer- und netzwerkbasierten Technologien, als auch der verbundenen Wirtschaftsbereiche)
IKT-Truppe	Truppenteil der Cyberkräfte
IKTBetr	IKT-Betrieb (Bereich des IKT&CySihZ)
IKTCyPl	Planungsabteilung IKT&Cyber für die GDLV
IKTPl	Abteilung IKT-Plan im BMLV
IMM	Informationsmodul Miliz
Inbound	Eingehend (Datenübertragung)
Incident	Vorfall
Incident Handling Process Post Incident	Bewältigung von Vorfällen
Incident Response	Reaktion auf Vorfälle
InfluxDB	Datenbankmanagementsystem
Information Protection Node	Lösung zum Klassifizieren und/oder zum Schutz von Daten
INMARSAT	Satellitenkommunikationssystem
InstFl/FlFlATS	Institut Flieger/Flieger- und Fliegerabwehrtruppenschule
Intrusion Detection and Prevention	System zur Erkennung und Verhinderung von Angriffen
IP-Netzwerke	Internet Protocol Netzwerke
IRIDIUM	Satellitenkommunikationssystem
ISK	Informationssicherheitskommission
ISMS	Information Security Management System
IT	Informationstechnologie
ITSM	IT-Service-Management
iZMS	Interoperables Zutrittsmanagementsystem

J

J5	Abteilung für Planung auf Ebene höherer Kommanden
J6	Abteilung für IKT-Belange auf Ebene höherer Kommanden
Jamming	Stören von Signalen (Störsender)
JGSWG	Joint Geospatial Working Group
JITSI	Open Source Videokonferenzsoftware

K

Karten	Darstellung eines räumliches Gebildes auf einer Fläche
KBC	Kapsch Business Com (Unternehmen)
KdoFüU&CD	Kommando Führungsunterstützung und Cyber Defence
KdoSK	Kommando Streitkräfte
KdoSKB	Kommando Streitkräftebasis
KFOR Chief Geo	Kosovo Forces (Höchster Geograph der KFOR)
KI	Künstliche Intelligenz
Klon	Identische Kopie (des Betriebssystems)
Klonstraße	Aufreihung vieler Geräte auf denen das geklonte Betriebssystem installiert wird
Krypto	Kryptographie (Wissenschaft der Verschlüsselung von Informationen; Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind)
KURSIS	Kursinformationssystem
KUWEL	Kurzwelle Land

L

Labelling	Markieren/Beschriften von Daten/Objekten
LAN	Local Area Network (Lokales Netzwerk)

Legic	Chipkartentechnologie
Leonardo	Leichter Mehrzweck-Hubschrauber des ÖBH
LFG	Luftfahrtgesetz
LI/LL	Lessons Identified/Lessons Learned
Liferay DXP	PuMa-Ablöse (neues CMS)
Loadbalance	Lastverteilung in Netzwerken
Lockdown	Eine Ausgangssperre oder Absperrung bzw. Versiegelung von Gebäuden und Bereichen
LOD	Low Altitude Danger (Unterer Luftraum, Flugbeschränkungsgebiet)
Log	Dokumentationsdaten von Änderungen/Ereignissen
LOGIS	Logistikinformationssystem
Look-and-Feel	Aussehen und Bediengefühl
LOR	Low Altitude Restricted (Unterer Luftraum, Flugbeschränkungsgebiet)
LRR	Long Range Radar
LRSiOp	Luftraumsicherungsoperation
LSF	Liste staatlicher Funk
LTE	LongTermEvolution (Mobilfunkstandard 3.9)
Lu/Lu Schießen	Luft-Luft-Schießen
LuAufklESt	Luft Aufklärungseinsatzstelle
LVId	Landesverteidigungs-Identifikationsnummer
LWL	Lichtwellenleiter
LZ	Lagezentrum

M

Malware	Schadsoftware
Matchbox	Virtueller Übungsraum

MAVE	Antischadsoftware-Programm
mblGeoEt	Mobiles Geo-Element
MD	Military Domain (Netzwerk im ÖBH)
Metadaten	Strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten
Metrics Collection	Metadaten-Sammlung
Metrik	Kennzahlen/Metadaten
Memorandum of Understanding	Vereinbarung zwischen zwei oder mehreren Parteien
MGI	Militärische Geoinformation
Mifare	Chipkartentechnologie
MIGIS	Militärisches Geoinformationssystem
MilAk	Militärakademie
MilCERT	Military Computer Emergency Readyness Team
milCPS	military Cyber-Protection System (Militärisches Cybersicherheitssystem)
MilGeo	Militärisches Geowesen
milGeoVA	Militärisches Geowesen Virtual Analysis
MILIS	Militärisches Informationssystem
Miliz	Streitkräfte, die zum größten Teil/vollständig aus Wehrpflichtigen im Bedarfsfall aufgestellt werden
Milizexperten	Experten aus verschiedenen Wissensgruppen aus dem Milizstand
MIMZ	Militärisches Immobilien Management Zentrum
MISP	Malware Information Sharing Platform (Plattform für Bedrohungsinformationsaustausch)
Mission Network	Einsatznetzwerk
MissionPlanningSystem	System zur Planung von Einsätzen
MLB	Militärische Landesbeschreibung
MLU	Midlife Upgrade
Mode S/Mode 5	Modus selektiv/Modus verschlüsselt (Sekundärradar)

Motion-Sickness	Bewegungskrankheit
Mountain Training Initiative	Europäische Ausbildungsinitiative zur Verbesserung der Gebirgseinsatzfähigkeit
MoVe	Mobilität in der Verwaltung (Zentrale Steuerung aller Dienstkraftfahrzeuge der Ministerien)
Moving-Map-Systeme	Navigationssystem (Aktuelle Position wird immer in der Mitte der Karte anstatt als Koordinaten angezeigt
MPC	Mid Planning Conference
MPH FTCN	Future Tactical Communication Network
MPR	Microwave Packet Radio
MSK17	Militärstrategisches Konzept 2017
MSS	Microwave Service Switch
MTM	Mail- und Termin Management
Multiplexing	Prozess des MUX
MUX	Multiplexer analoge/digitale Selektionsschaltung, bei der aus mehreren Eingängen ein Ausgang geschaltet werden kann

N

NAFRA	national radio frequency agency
NATO	North Atlantic Treaty Organization
NavWar	Navigation Warfare (Kriegsführung über Navigation)
NCAS	National Crypto Algorithm System (Verschlüsselung von international klassifizierten Daten zur Übertragung)
NDA/MoD	National Distribution Authority/Ministry of Defence
Network Deception Lösung	Sicherheitsstufe in Netzwerken zusätzlich zu Firewalls
NGIF	NATO Geospatial Information Framework
NISG	Netz- und Informationssystemsicherheitsgesetz
NSA	national security agency
NVÖ	Nebenstellenverbund Österreich

O

ÖBH	Österreichisches Bundesheer (Streitkräfte der Republik Österreich, dem die militärische Landesverteidigung obliegt und nach den Grundsätzen eines Milizsystems einzurichten ist)
ObstdG	Oberst des Generalstabsdienstes
ODU	Outdoor Unit (Außeneinheit)
OE	Organisationseinheit
Öffentlichkeitsarbeit	Management der öffentlichen Kommunikation von Organisationen gegenüber ihren internen/externen Anspruchsgruppen
ofFMSys	Ortsfestes Fernmeldesystem
ofRVN	Ortsfestes Richtverbindungsnetz
OGC	Open Geospatial Consortium
ÖMKFL	Österreichische Militärkarte Flieger
Open Source	„Offene Ressource" (Software für jedermann lizenzfrei zugänglich, Quellcode öffentlich verfügbar)
OpKoord	Operationskoordination
Oracle	Amerikanisches Soft- und Hardwareunternehmen
ORF	Österreichischer Rundunk
Org	Organisation (Abteilung im BMLV)
ORGIS	Organisationsplan Informationssystem
Orgplan	Organisationsplan
ORS	Ortsfeste Radarstation
Orthofotos	Verzerrungsfreie und maßstabsgetreue Abbildung der Erdoberfläche aus Luft- oder Satellitenbildern abgeleitet
Outbound	Ausgehend

P

PAAN	PERSIS Automationsunterstützte Abrechnung von Nebengebühren
Pandemie	Neue, zeitlich begrenzte, weltweite, starke Ausbreitung einer Infektionskrankheit mit hohen Erkrankungszahlen

PersA	Personalabteilung A im BMLV
PersAppl	Personal Applikationen
PERSIS	Personalinformationssystem
PGBACKREST	Post Gre Backup Restore
Phishing	Beschaffung persönlicher Daten anderer unwissender Personen
PIONEER	InteroPerability and DIgitization Of INtelligencE GathEring PRocesses ;]
PKI	Public Key Infrastructure (System, das digitale Zertifikate ausstellen, verteilen und prüfen kann)
Plug and Play	Anschließen und loslegen
PM-Bund	Personalmanagement des Bundes mit SAP
PostgreSQL	Freies objektrelationales DBMS
PrK	Präsidentschaftskanzlei
ProofofConcept	Funktionsbeweis eines ersten Prototypen
PS-NT	Personalsysteme Neue Technologie
PTC	Pre Travel Clearance
PTMP	Point To Multi Point
PTT	Push to Talk (Direktsprechverbindung im Funksprechverkehr)
PuMa	Publish Manager

Q

QGIS	Freies Open Source Geographisches Informationssystem der Firma QGIS
QR-Code	Quick-Response Code (zweidimenionale Darstellung der binären Codes von ASCII-Zeichen)

R

Radar	Radio Detection and Ranging (funkgestützte Ortung und Abstandsmessung)
RadStlg	Radarstellung
Ransomware	Schadprogramm mit Verschlüsselungsfähigkeit

Rasterbildform	Pixelbasiertes Bild
RCID	Resistive Capacitive Identification
RCIED	Radio Controlled and improvised explosive Device (funkausgelöste improvisierte Sprengkörper)
Rechenzentrum	Gebäude/Räumlichkeit in dem/der die zentrale Rechentechnik einer oder mehrerer Unternehmen/Organisationen untergebracht ist
redundant	Mehrfach vorhanden
Release	Veröffentlichung
Reputationsdatenbanken	Datenbank vertrauenswürdiger Quellen
Requests for Change	Anfrage für Änderungen
RHEL	Red Hat Enterprise Linux (Linux basiertes Betriebssystem)
RiFu	Richtfunk
Ripple	Sammlung mehrerer Schwachstellen in einer weit verbreiteten Architektur von Kommunikationsprotokollen
RIPTIDE	Resilient Position Navigation and Timing Testing for Defence
Rollout	Veröffentlichung neuer Softwareproduklte und die Verteilung an Kunden sowie die Integration in bestehende Systeme
Router	Netzwerkgerät, das Daten zwischen mehreren Netzwerken weiterleitet (trennt Netzwerke)
Routing	Wegfindung im Netzwerk zur nächsten Station eines Datenpaketes
ROZ	Restricted Operation Zones
RRT	Rapid Response Team (Schnell einsatzbereites Team)
RSM	Resolute Support Mission
rugged und tempest NB	Gehärtete Notebooks
RüstPol	Abteilung für Rüstungspolitik im BMLV
RWARE	Retrieval Ware (Metadatensuchmaschine)
RZ	Rechenzentrum
RZL-Plan	Ressourcen-, Ziel- und Leistungsplan

S

SAA	Security Accreditation Authority (Akkreditierung von Informations- und Kommunikationstechniksystemen)
SAN	Storage Area Network
Sandbox	Software-Testumgebung; Isolierter Bereich ohne Auswirkung auf die Umgebung
Schlüsselarbeitskräfte	Für den Betrieb essentielle Arbeitskräfte
Schlw	Schlüsselwesen
SCPC Mode	Single Channel per Carrier Mode (Ein Kanal pro Gerät)
SD4MSD	Single Device for Multiple Security Domains (Ein Endgerät für verschiedene Sicherheitsstufen)
SDH	Synchrone Digitale Hierarchie
SecOps	Security Operations
Security Patches	Sicherheits-Updates
selWLANRekr	Selektives WLAN für Rekruten (IKT-Service)
SIEM	Security Information and Event Management (Echtzeitanalyse von Sicherheitsalarmen; lokal oder als Cloudservice)
sihpolAssE	Sicherheitspolizeilicher Assistenzeinsatz
Silentel	App für sichere mobile Kommunikation (NATO zugelassene Lösung für klassifizierten Sprach- und Datenaustausch)
SIM-Karte	Subscriber Identity Module Karte (Chipkarte, die zur Identifikation des Nutzers in ein Mobiltelefon eingesteckt wird)
SK	Streitkräfte
SKB	Streitkräftebasis
SMIR	Spectrum Management Repository (Software)
SMN	Sicheres Militärisches Netz
SMN.mobile	Ablöse der GovNetBox; mobiler VPN-Zugang in das SMN
SMS	Short Message Service (Kurznachrichtendienst)
Software	Sammelbegriff für Programme und die zugehörigen Daten
Spam	Unerwünschte, massenhaft per E-Mail oder auf ähnliche Weise versandte Nachrichten

Spoofing	Verschleierung oder Vortäuschung; Täuschungsmethoden zur Verschleierung der eigenen Identität
Sport	Körperliche Betätigung
SSD	Solid State Drive (schnelle Festplatte ohne bewegliche Teile)
SSP	Service Schwerpunkt
SSP ZABL	SSP zentrale Anwenderbetreuung LOGIS
SSP ZS	SSP zentrale Services
SSRS	System Specific Security Requirements (Systemspezifische Sicherheitsanforderungen)
Stammportal	Plattform zur Selbstverwaltung für Mitarbeiter des Bundes
STANAG	Standardisation Agreement - NATO
standalone	Alleinstehendes (IT-)Produkt
SUB	Sicherheitsunbedenklichkeitsbescheinigung
SW	Software
SWIFT BLADE	Multinationale Hubschrauber-Übung
Switch	Umschalter, Weiche (Kopplungselement in Rechnernetzwerken)

T

TA	Technical Agreement
Tablet	Tragbarer flacher, leichter Computer mit Bildschirm der durch Eingaben mit den Fingern reagiert
Tachymeter	Gerät zur Horizontalrichtung- Vertikalwinkel- und Schrägstreckenbestimmung
TAP	Truppenanschaltpunkte
TCN	Tactical Communication Network
TDM	Time Division Multiplexing (Methode zur Übertragung von Datenströmen)
te/tak Fähigkeiten	Technische/Taktische Fähigkeiten
TEC	Technologiegespräche Forum Alpbach
TechnologieStack	Datenökosystem (Liste aller Technologiedienste zum Erstellen/Ausführen einzelner Anwendungen)

Teilmobilmachung	Teilmobilisierung der Streitkräfte (Einberufung von Teilen der Miliz)
Teiltauglichkeit	Ableistung des Grundwehrdienstes mit leichten körperlichen Einschränkungen, „Grundwehrdienst nach Maß“
Teleworking	Regelmäßiges Arbeiten an einem anderen Arbeitsplatz als das Gebäude des Arbeitgebers
TFS	Truppenfunksystem
Threat Intelligence	Informationsbeschaffung über Bedrohungen und Bedrohungsakteure im Cyberraum
Threat Response	Erkennung, Untersuchung und Reaktion auf Schadsoftware im Netzwerk
TIGER MEET	NATO Luftraumüberwachungsübung, an der nur Einheiten mit Tiger im Namen oder Wappen teilnehmen dürfen
Timeseries Database	Zeitreihendatenbank (Datenbank für das Speichern und die Analyse von Zeitreihen wie z.B. Sensordaten)
TKV	Telekommunikationsverbund
TLZ	Technisch logistisches Zentrum
TN	Truppennummer
topographisch	Natürliche Erdoberfläche mit ihren Höhen, Tiefen, Unregelmäßigkeiten und Formen
Tracker	Drohnensystem des ÖBH
Tunneling	Virtueller abstrahierter Übertragungsweg
TÜPl	Truppenübungsplatz
TvZ	Test vor Zuschlag

U

UHF	Ultra High Frequency (Ultra hohe Frequenz)
UNFICYP Force Cartographer	United Nations Peacekeeping Force in Cyprus (Militärkartograf im Auslandseinsatz auf Zypern)
UNIS	IT-Unterstützung der Auslandseinsatz-Planung, Verwaltung und Besoldung
Updates	Software-Aktualisierungen
URL	Uniform Resource Locator (Standard für die Adressierung einer Website)
UseCase	Anwendungsgebiet
USV	Unterbrechungsfreie Stromversorgung

UZEloKa	Unterstützungszentrum EloKa

V

VbÜb	Verbandsübung
VersNr	Versorgungsnummer
VFR/IFR	Visual Flight Rules / Instrument Flight Rules (Sichtflug-regeln / Instrumentenflugregeln)
VHF	Very High Frequency (Sehr hohe Frequenz)
Visual Computing	Grafische Datenverarbeitung
Visualisierung	Umwandlung abstrakter Daten in eine grafische, visuell erfassbare Form
VKS13	Videokonferenzsystem 13
vlgbFMSys	Verlegbares Fernmeldesystem
vlgbRZ	Verlegbares Rechenzentrum
VM	Virtuelle Maschine (virtuelle Umgebung zur Simulation von IT-Geräten, PC am PC)
VO Funk	Vollzugsordnung für den Funkverkehr
VPN	Virtual Private Network (gesicherte Netzwerkverbindung mithilfe von Tunneling)
VR	Virtual Reality (Virtuelle Realität - meist mit Vollvisierbrille)
VR-Sickness	Überkeit hervorgerufen durch die Verwendung einer VR-Brille (vergleichbar mit Seekrankheit)
VSAT	Very Small Aperture Terminal (Satellitenempfänger und Sender mit Antennen für satellitengestützte Kommunikation)
VTA	Verpflegsteilnehmer-Erfassung und bargeldlose Abrechnung
VTC	Video-Tele Conference (Videokonferenzsystem)
VULN	Vulnerability (Verwundbarkeit)
Vulnerability Monitoring	Überwachung von Schwachstellen

W

WAF	Web Application Firewall (Netzwerksicherheitskomponente gegen Angriffe aus dem Internet)
WarRoom	Kommandozentrale

Warfare	Operationen von Streitkräften
Web	„Netz" (meist Internet)
WEBEX	Videokonferenzsoftware
Webproxy	Vermittelnde Kommunikationsschnittstelle in einem Netzwerk
Webshop	Einkaufsplattform im Internet
Windows 10	Microsoft Betriebssystem
WLAN	Wireless-LAN (Kabelloser Zugang zu Netzwerken über Access-Points)
World in miniature navigation	Navigation des Standpunktes durch Verschieben der Person im Modell
WPTT	Wireless Push-To-Talk (Drahtlose Sprechtaste)
WSM	Abteilung Waffensysteme und Munition

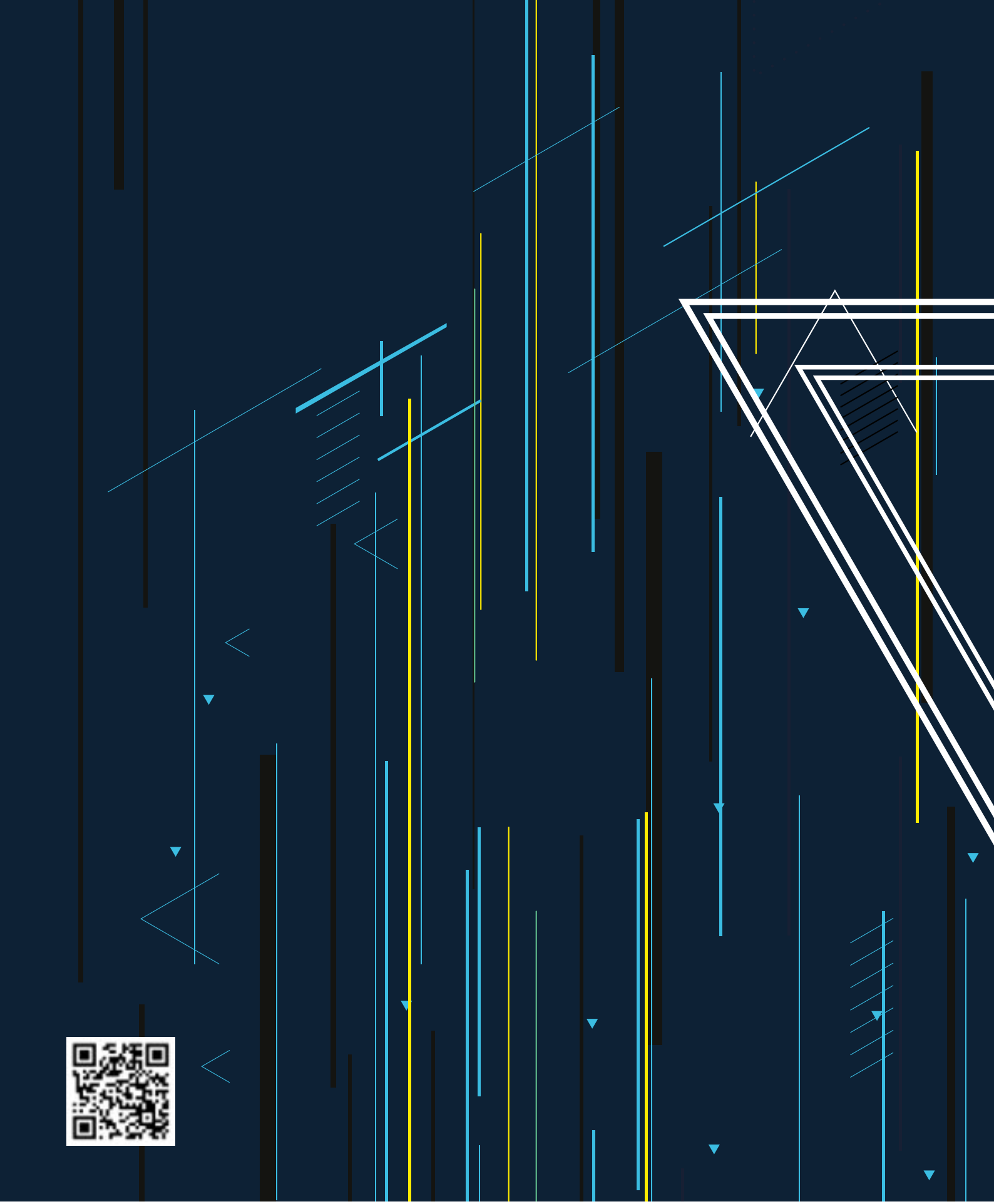
X

XIRIS	Extended Integrated Reporting Infrastructure System (Anwendung zum Erstellen von Auswertungen von Daten aus anderen Anwendungen)

Z

ZBS	Zentrales Berechtigungs System
ZEDVA	Zentrale-Elektronische-Daten-Verarbeitungs-Anlage
ZentDok	Zentraldokumentation
Zerologon	Software-Schwachstelle
ZGeoBW	Zentrum der Geoinformationen der Bundeswehr
zIaaS	Zentrale Infrastructure as a Service
ZMS	Zutrittsmanagementsystem
ZTA	Abteilung im BMLV für Zentrale Technische Angelegenheiten

Bundesministerium für Landesverteidigung



IMPRESSUM:

Amtliche Publikation der Republik Österreich
Bundesministerium für Landesverteidigung

Medieninhaber, Herausgeber und Hersteller:
Bundesministerium für Landesverteidigung
Roßauer Lände 1, 1090 Wien

Inhalt und Redaktion: Direktion 6 - IKT&Cyber
Idee, Konzeption und Gestaltung: Roland Pachler, Michael Kriehebauer, Ben Gratzl
Layout: Roland Pachler, Michael Kriehebauer, Ben Gratzl
Satz: Michael Kriehebauer, Ben Gratzl
Fotos: Bundesheer, Direktion 6 - IKT&Cyber, soweit nicht ausdrücklich anders gekennzeichnet
Druck: Heeresdruckzentrum, 1030 Wien

Produziert nach den Richtlinien des Österreichischen Umweltzeichens

Platzhalter für Zertifizierungslogo