LEISTUNGSBERICHT

DIREKTION 6 – IKT und CYBER

2024

EINSATZBEREIT FÜR ÖSTERREICH

BUNDESHEER.AT

UNSER HEER

Bundesministerium für Landesverteidigung

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

BM Mag. Klaudia Tanner

Seit dem letzten Leistungsbericht der Direktion 6 – IKT und Cyber im Jahr 2024 ist gerade im Cyber- und Informationsbereich sehr viel passiert.

Wir beobachten weltweit einen zunehmenden und rapiden Wandel der gesellschaftlichen, geopolitischen und sicherheitspolitischen Lage. Der andauernde Krieg in der Ukraine, der Nahostkonflikt aber auch der Einsatz von Informationsoperationen und Desinformation zur Destabilisierung des Vertrauens in demokratische Werte und Einrichtungen stellen Politik und auch Armeen auf der ganzen Welt vor neue Herausforderungen.

Das Erkennen und richtige Reagieren auf Deepfakes und Cyberangriffe auf staatliche Stellen und Unternehmen und die daraus entstehenden Risiken für Europa und unsere Bürgerinnen und Bürger rücken immer weiter in den Fokus.

Auch das Österreichische Bundesheer stellt sich diesen neuen Herausforderungen. Durch den Aufbauplan ÖBH2032+ und die damit verbundenen Beschaffungen gewährleisten wir Stabilität und Sicherheit für die Bürgerinnen und Bürger Österreichs. Durch Verbesserung der Infrastruktur, der notwendigen Beschaffung von Ausrüstung und der konsequenten Weiterführung der Digitalisierung der Streitkräfte schaffen wir die Voraussetzungen dafür, dass Österreich wieder voll verteidigungsfähig wird.

Mit dem Ausrollen des „Tactical Communication Network" ist ein großer Schritt in Richtung modernster Führungsfähigkeit gelungen und die Digitalisierung ist bei unseren Soldatinnen und Soldaten angekommen.

In turbulenten Zeiten werden aber auch neue Partnerschaften geknüpft. Es freut mich besonders, dass wir gemeinsam mit der National Garde von Vermont eine Kooperation geschlossen haben und diese im Rahmen des „State Partnership Program" in den Bereichen Cyber- und Informationsoperationen intensiv leben. Wesentliche Inhalte des Programms ermöglichen beiden Partnern einen Austausch von Fähigkeiten, Erfahrungen und Know-How, wodurch die Leistungsfähigkeit für beide Seiten stetig gesteigert und verbessert wird.

Auch im Rahmen des PESCO „Cyber Rapid Response Team" konnten die Mitarbeiterinnen und Mitarbeiter des Militärischen Cyberzentrums bei der ersten EU-Partnerschaftsmission in Moldau ihr Können unter Beweis stellen.

Durch die konsequente Weiterentwicklung unserer Cyber- und Informationskräfte schaffen wir die Voraussetzungen für die Sicherheit im nationalen und internationalen Umfeld.
Die Verteidigungsfähigkeit und Konkurrenzfähigkeit auf einem modernen Gefechtsfeld sind ohne Digitalisierung nicht mehr denkbar.

Ich bedanke mich für den hervorragenden und unermüdlichen Einsatz zum Schutz unserer Heimat bei allen Soldatinnen, Soldaten, allen Zivilbediensteten des Österreichischen Bundesheers und speziell bei den Mitarbeitern der Direktion 6 - IKT und Cyber für ihr Engagement und den Mut zur permanenten Weiterentwicklung.

Mag. Klaudia TANNER
Bundesministerin für Landesverteidigung

Bundesministerium für Landesverteidigung

Sehr geehrte Damen und Herren!

Auch heuer ergreife ich als Chef des Generalstabes des Österreichischen Bundesheeres natürlich gerne die Gelegenheit, einige Worte im diesjährigen Leistungsberichtes der Direktion 6 - IKT&Cyber an Sie zu richten.

Als oberste Priorität im Aufbauplan ÖBH2032+ wurde die Verteidigungsfähigkeit des Österreichischen Bundesheeres festgelegt. Dies sieht eine ausgewogene Fähigkeitsentwicklung aller Teilstreitkräfte und Waffengattungen in einem Zeitraum von zehn Jahren und darüber hinaus vor. Das Österreichische Bundesheer soll auch im internationalen Umfeld als ebenbürtiger Partner wahrgenommen werden.

Das Zielbild ÖBH2032+ stellt das vorläufige Ergebnis der Streitkräfteplanung dar und beschreibt in der notwendigen Detaillierung, welche Fähigkeiten das Österreichisches Bundesheer bis zum Jahr 2032 erhalten, ausbauen und aufbauen sollte, um die militärstrategische Zielsetzung „verteidigungsfähig" zu erfüllen.

General Mag. Rudolf Striedinger

Im Zentrum der Bemühungen steht also wieder die Verteidigung Österreichs.

Durch unsere nationalen Bemühungen und intensive internationale Zusammenarbeit, wie beispielsweise das PESCO-Projekt "EUCDCC", werden die digitale Verteidigungsfähigkeit gestärkt, Erfahrungen ausgetauscht und dadurch ein gemeinsamer Nutzen erzielt, um gegen Bedrohungen zu kämpfen.

Auch in Österreich hat man erkannt, dass die multidomäne Verschränkung und Wirkung der Schlüssel zum Erfolg in modernen, hybriden Konflikten ist. Daher spiegelt sich diese Absicht auch als CyIDCC (Cyber Information Domain Component Command) im Aufbauplan ÖBH2032+ wieder.
Zur Sicherstellung der Planungs- und Führungsfähigkeit auf der operativen und oberen taktischen Führungsebene wird ein operativ führendes Kommando (FHQ) aufgebaut. Hier wird auch erstmalig die Zelle J10 Informationsoperationen berücksichtigt; dieser Entwicklungsauftrag liegt federführend bei der Direktion 6.

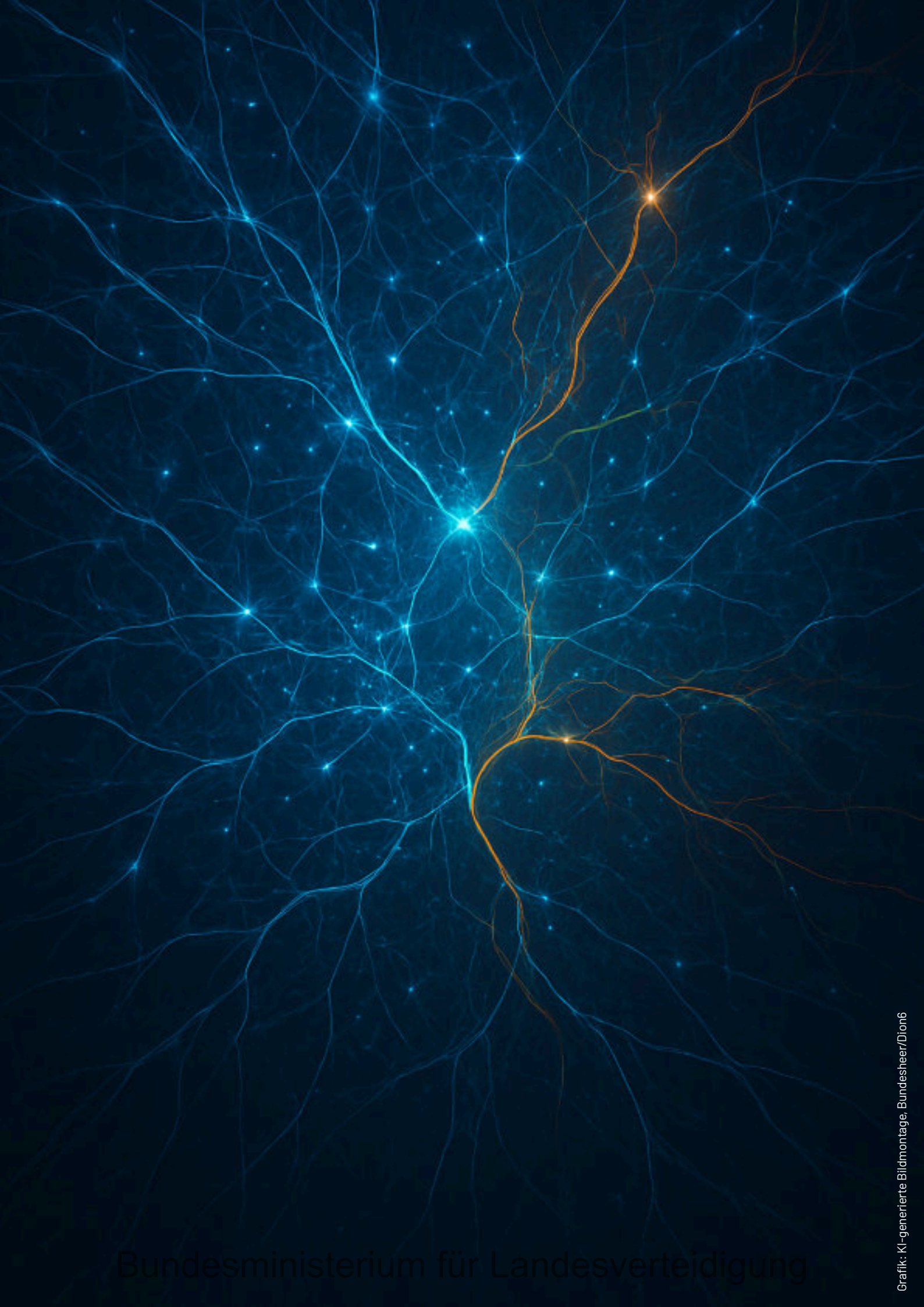
Als Chef des Generalstabes ist es mir ein Anliegen, dass die Kommandanten aller Führungsebenen und deren Stäbe in der Lage sind, die Führungsaufgaben unter den jeweils vorhandenen personellen, materiellen und organisatorischen Bedingungen wahrzunehmen und zu beherrschen.
Die Digitalisierung aller Prozesse ist Voraussetzung für die moderne Führungsüberlegenheit. Erst Digitalisierung macht verteidigungsfähig. Die Aufgabenerfüllung der Direktion 6 IKT und Cyber als Teilstreitkraft im Rahmen der militärischen Landesverteidigung schafft Führungsüberlegenheit im Cyber- und Informationsraum, im elektromagnetischen Spektrum und den zugeordneten Space Services.

Das ÖBH2032+ ist verteidigungsfähig!

Das Österreichische Bundesheer ist dazu befähigt, Österreich gegen jeden militärischen Angriff zu verteidigen und sein Volk zu schützen.

General Mag. Rudolf STRIEDINGER
Chef des Generalstabs

Inhaltsverzeichnis



Bundesministerium für Landesverteidigung

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Direktion 6 – IKT und Cyber

Leiter Dion6: GenMjr Ing. Mag. Hermann KAPONIG

Sehr geehrte Damen und Herren, werte Leser:innen unseres Leistungsberichts 2024.

Wir verfassen seit 2020 jährlich einen Jahresbericht zu unserem Leistungsbereich. Vor ihnen liegt nun unser fünfter Leistungsbericht für den Betrachtungszeitraum 2024. 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 andererseits innerhalb unserer Organisation all unseren Mitarbeiterinnen und Mitarbeiter im gesamten Bundesgebiet, die Breite unserer Anstrengungen und unseres Zuständigkeitsbereichs vor Augen führen. Andererseits soll er aber auch interessierten Leserinnen und Leser die Gelegenheit geben, in der Retrospektive zu erfassen, was alles in Angriff genommen und geschafft werden konnte.

Besonders erfreulich war 2024, dass wir im Rahmen der Reorganisation des Verteidigungsressorts, nach mehrjährigen Bemühen die neuen Organisationspläne für die Direktion 6 – IKT und Cyber endlich zufriedenstellend mit dem BMKÖS ausverhandeln konnten. Damit wurden jene Strukturen zur Verfügung gestellt, die es ermöglichen den neuen Herausforderungen entsprechend entgegen treten zu können.

Die neuen Organisationspläne wurden durch die Organisationsabteilung des BMLV verfügt. Die Altstruktur wurde in die Neustruktur übergeleitet und mit 1. Oktober 2024 auch personell eingenommen. Die neue Struktur der Direktion 6 wurde im Rahmen eines festlichen Antretens von Abordnungen aller Organisationselemente der Direktion 6 entsprechend würdig begangen.


Foto: BMLV/HBF

Die Direktion 6 verfügt damit nun unter anderem mit der Abteilung „IKT Cyber Planung“ (IKTCyPl), mit der Abteilung „IKT Bereitstellung und Nutzungsmanagement“ (IKTBstg&NuMngt) und der Abteilung „IKT Cyber Einsatz“ (IKTCyE), neben dem „IKT Cyber Sicherheitszentrum“ (IKTCySihZ), der „Führungsunterstützungsschule“ (FüUS) und den beiden „Führungsunterstützungsbataillonen“ (FüUB1 und FüUB2), über drei unmittelbare Abteilungen.

Mit der organisatorischen Veränderung erfolgte auch die offizielle Anerkennung der Cyberkräfte als eigene Domäne, wie es schon im Militärstrategischen Konzept (MSK17) festgeschrieben wurde.

Die Cyberkräfte sind damit auch als eigene militärische Teilstreitkraft anerkannt worden. Somit stehen die Cyberkräfte auf gleicher Ebene wie die Landstreitkräfte, die Luftstreitkräfte und die Spezialeinsatzkräfte des Bundesheeres und sind nicht nur mehr Unterstützungstruppe, sondern auch Kampftruppe.

„Die Cyberkräfte wurden als militärische Teilstreitkraft anerkannt und sind nun auf der gleichen Ebene wie Land-, Luft- und Spezialstreitkräfte. Wir stellen das IKT-System des Bundesheeres auf gänzlich neue Beine und etablieren ein truppenorientiertes IKT-System ÖBH2032+.“

Unserem Leistungsbereich sind zudem die operativ taktischen Informationskräfte und in Teilbereichen die Services für den Weltraum zugeordnet worden. Wir sind damit insgesamt für fünf Waffengattungen (Cybertruppe, EloKa-Truppe, FüU/IKT-Truppe, Komm-Truppe, PsyOps-Truppe), für die Ausbildung im Fachbereich und für den IKT-Provider zuständig.

Ich bedanke mich bei dieser Gelegenheit bei all jenen Stellen und Personen, die dazu beigetragen haben, dass unser Leistungsbereich so ausgestaltet werden konnte. Damit brauchen wir auch den internationalen Vergleich nicht zu scheuen.

Unser planerisches Schwergewicht bei den Bearbeitungen des letzten Jahres war es, unsere Beiträge zur Fähigkeitsentwicklung des Ressorts beizutragen. Hier waren massive Planungs- und Beitragsleistungen zum Aufbauplan des ÖBH2032+ und zur Ausgestaltung des Zielbildes ÖBH2032, vor allem in der Handlungslinie Führungsüberlegenheit, zu erbringen.

Dabei wollen wir das IKT-System des Bundesheeres auf gänzlich neue Beine stellen. Wir bauen unser bisher sehr zentral aufgestelltes IKT-System auf ein dezentrales System um und etablieren ein truppenorientiertes „IKT-System ÖBH2032+" auf Basis einer „ÖBH Multi Hybrid Cloud". Mit diesem System wird ein entscheidender Beitrag zur Erreichung der Militärstrategischen Zielsetzung geleistet.

„Das ÖBH2032+ ist verteidigungsfähig. Das ÖBH2032+ ist dazu befähigt, Österreich gegen jeden militärischen Angriff zu verteidigen und sein Volk zu schützen" – geleistet.

Mit der nun existierenden performanten Friedensstruktur sind wir in der Lage, auch unsere Beiträge für die neue Einsatzstruktur des Ressorts, mit dem „Leitungsstab des BMLV" auf strategischer Ebene, dem „Force Headquarter" (FHQ) auf operativer Ebene und unserem neuen „Cyber Information Component Command" (CyICC) auf Taktischer Ebene, zu erbringen.

Unsere Maßnahmen der Einsatzvorbereitungen waren und sind weiterhin das Schwergewicht der weiteren Bearbeitungen.

Wir stellen uns im Rahmen des Zielbildes ÖBH2032 mit unserem Fähigkeitsbereich Cyber- und Informationsraum für die Einsatznotwendigkeiten auf. Planspiele und Übungen auf nationaler und internationaler Ebene runden unsere Anstrengungen zur Fähigkeitsentwicklung für den Einsatz ab. Besonders hervorzuheben waren hier die Luftraumsicherungsoperation Dädalus24, die Cyber-Übungen (z.B. Locked Shields u.v.am.), die NATO-Interoperabilitätsübung CWIX24, die DACH-Übung „Common Roof 24" oder die Großübung „Schutzschild 24", aber auch die wichtigen Notkommunikationsübungen. Hier haben wir unsere Leistungsfähigkeit überprüfen und uns anhand der gewonnenen Erkenntnisse wesentlich weiterentwickeln können.

Aber auch im Normbetrieb waren unsere Auftragsbücher prall gefüllt. Die Digitalisierung des Ressorts in allen Leistungsbereichen schreitet unaufhaltsam voran. Auch das Thema „Künstliche Intelligenz" gewinnt im militärischen und verwaltungsorientierten Bereich immer mehr an Bedeutung. Hier sind wir sehr stolz darauf, mit dem IKT Cyber Sicherheitszentrum (IKTCySihZ) unseren eigenen IKT-Provider verfügbar zu haben, um den Ressortspezifischen Herausforderungen bestmöglich begegnen zu können. Ergänzend dazu haben wir unsere Kooperationen mit internationalen Partnern und die Zusammenarbeit mit zivilen Dienstleistern nachhaltig verstärkt, um der breit gefächerten Auftragslage entsprechen zu können. Natürlich haben wir unsere Beiträge auch aktiv in den Bearbeitungen des Bundes eingebracht und Entwicklungen auf Bundesebene, wo sie im Verteidigungsressort Sinn machen, mitberücksichtigt.

Ein besonderes Highlight des letzten Jahres war die Übergabe des neuen verlegbaren IKT-Systems TCN (Tactical Communication Network) an die Truppe, welches seine große Feuertaufe bei der Übung „Schutzschild 24" hatte.

Ein große Herausforderung der Digitalisierung für den Einsatz und Normbetrieb, war auch die Gewinnung von entsprechendem Personal. Hier waren und sind einerseits die Abgänge durch Versetzungen oder Ruhestandsabgänge zu kompensieren und andererseits neue Bedarfe für die Steigerung der Leistungsfähigkeit in allen Bereichen zu decken. Dazu brauchen wir sowohl Experten in Uniform wie auch in Zivil.

Vor allem durch die neuen RIVIT-Verträge (Sonderverträge für die IT-Arbeitsplätze) besteht eine ausgezeichnete Grundlage, um entsprechendes Fachpersonal gewinnen zu können. Hier waren wir sehr erfolgreich.

Im militärischen Bereich freuen wir uns über die nunmehr in bereits drei Jahrgängen laufenden Ausbildungen des Fachhochschulstudienganges „Militärische IKT-Führung" (FHStg MilIKTFü) an der Theresianischen Militärakademie (TherMilAk). Im heurigen Jahr wird bereits der erste diesbezügliche Jahrgang zur Truppe ausmustern und damit die Qualität im Fachbereich deutlich verstärken.

Erfreulich war auch der steigende Anteil an weiblichen Mitarbeiterinnen im Bereich der Direktion 6. Mittlerweile ist hier auch öffentlich bekannt, welch breit gestecktes Aufgabenspektrum wir hier im Bereich haben, das auch für weibliche Mitarbeiterinnen von hohem Interesse ist.

Mit Stolz vermerken wir auch das stetig steigende Interesse der jungen Wehrpflichtigen, bei uns als Cyber-Grundwehrdiener (Cyber GWD) ihre Wehrpflicht zu leisten. Erfreulich ist hier zudem der Anteil jener, die sich nach Beendigung ihrer Wehrpflicht dazu entschließen im System zu bleiben und im Bundesheer Karriere machen zu wollen.

Eine weitere Herausforderung für unseren Fachbereich ist die Infrastruktur, die für unseren aufwachsenden Leistungsbereich von entscheidender Bedeutung ist.

Einiges konnte hier bereits erreicht werden. Maßnahmen größeren Umfanges sind vor allem für unsere Organisationselemente in Wien und in Villach in der Planung.

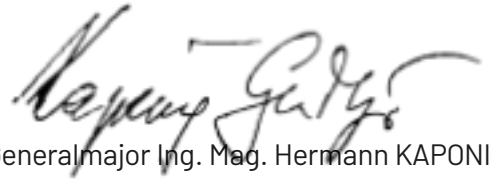
Darüber hinaus möchte ich auch auf Maßnahmen verweisen, die zur weiteren Etablierung unseres Fähigkeitsbereichs beigetragen haben:

- Unser 2023 komponierter und publizierter „Cyber- Marsch", trägt weiter zum Waffenstolz unserer Domäne bei. Der Cyber-Marsch wurde 2024 bei Veranstaltungen, Angelobungen und militärischen Festakten gespielt und hat die Truppe und die Bevölkerung begeistert.
- Wir haben ein neues „Cyber-Leistungsabzeichen" (in Bronze, Silber und Gold) im Bundesheer eingeführt und können nun besondere Leistungen im Fachbereich damit entsprechend würdigen.
- Unser „Cyber Escape Room" war auch bei vielen Öffentlichkeitsveranstaltungen und Tagen der Schulen präsent und ist dabei im Sinne der „awareness" für Cyber-Bedrohungen und der Personalgewinnung sehr gut angekommen. Dass nun auch das Deutsche Kommando Cyber- und Informationsraum (KdoCIR) und das Schweizer Cyber-Kommando ähnliches planen, zeigt uns, dass wir hier am richtigen Weg sind.
- Auch die Würdigungen unserer Arbeit im Rahmen der Veranstaltung „Matinée - Militär des Jahres", wo einzelne Mitarbeiterinnen und Mitarbeiter und Teams vor den Vorhang geholt wurden, zeigt uns die Anerkennung und Bedeutung unserer Leistungen.

Somit blicken wir wieder auf ein abwechslungsreiches und durchaus herausforderndes Jahr 2024 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 weiterhin alle gefordert.

Mein Vorwort abschließend, möchte ich mich bei allen Kommandanten, Leitern, Soldatinnen und Soldaten, Mitarbeiterinnen und Mitarbeitern herzlich für die gezeigten Leistungen im Jahr 2024 bedanken.

Der Kommandant der Cyberkräfte des Österreichischen Bundesheeres:



Generalmajor Ing. Mag. Hermann KAPONIG

Foto: Bundesheer/Dion6

Cyberleistungsabzeichen

Im Heeresgeschichtlichem Museum ist die Auszeichnung der Tel-Truppe ausgestellt. Im Aussehen gleicht es dem Fernmelde-Bewährungsabzeichen, trägt aber als Abschluss nach oben an Stelle des Staatswappen die Kaiserkrone.

Im Österreichischen Bundesheer wurde das FM – Bewährungsabzeichen 1992 letztmalig verlautbart.

Durch die ständige Weiterentwicklung der Fernmeldetruppe in den letzten Jahren hin zu den Cyberkräften und durch die Neuausrichtung des ÖBH nach dem militärstrategischen Konzept zum Aufbau der Cyberkräfte wurde das Fernmelde - Bewährungsabzeichen hierfür zum Cyberleistungsabzeichen modifiziert. Aus Gründen der Tradition und der Bedeutung des Abzeichens innerhalb der Cyberkräfte wurde das grundsätzliche Erscheinungsbild beibehalten jedoch abgestuft in Bronze, Silber und Gold.

Die ersten Cyberleistungsabzeichen in Bronze wurden im Juli 2024 an StWm Stefan DICHTL (MilKdoNÖ) sowie Vzlt Christian KOGLER und Vzlt Hannes TRAUSMÜLLER (beide MilKdoST) für ihre besonderen Leistungen im Fachbereich der Cyberkräfte verliehen.

Das Cyberleistungsabzeichen in Silber wurde im Oktober 2024 am Traditionstag der Cyberkräfte an der FüUS sowie im FüUB1 und FüUB2 an verdiente Kameraden für ihre herausragende Leistungen im Fachbereich verliehen.

Die ersten Cyberleistungsabzeichen in Gold wurden im Dezember 2024 an GenMjr Ing. Mag. Hermann KAPONIG, Bgdr Mag. Christof TATSCHL und Mag. Wolfgang HACKER für ihre außergewöhnlichen Leistungen für die Teilstreitkraft Cyber verliehen.

Grafik: Bundesheer/Dion6

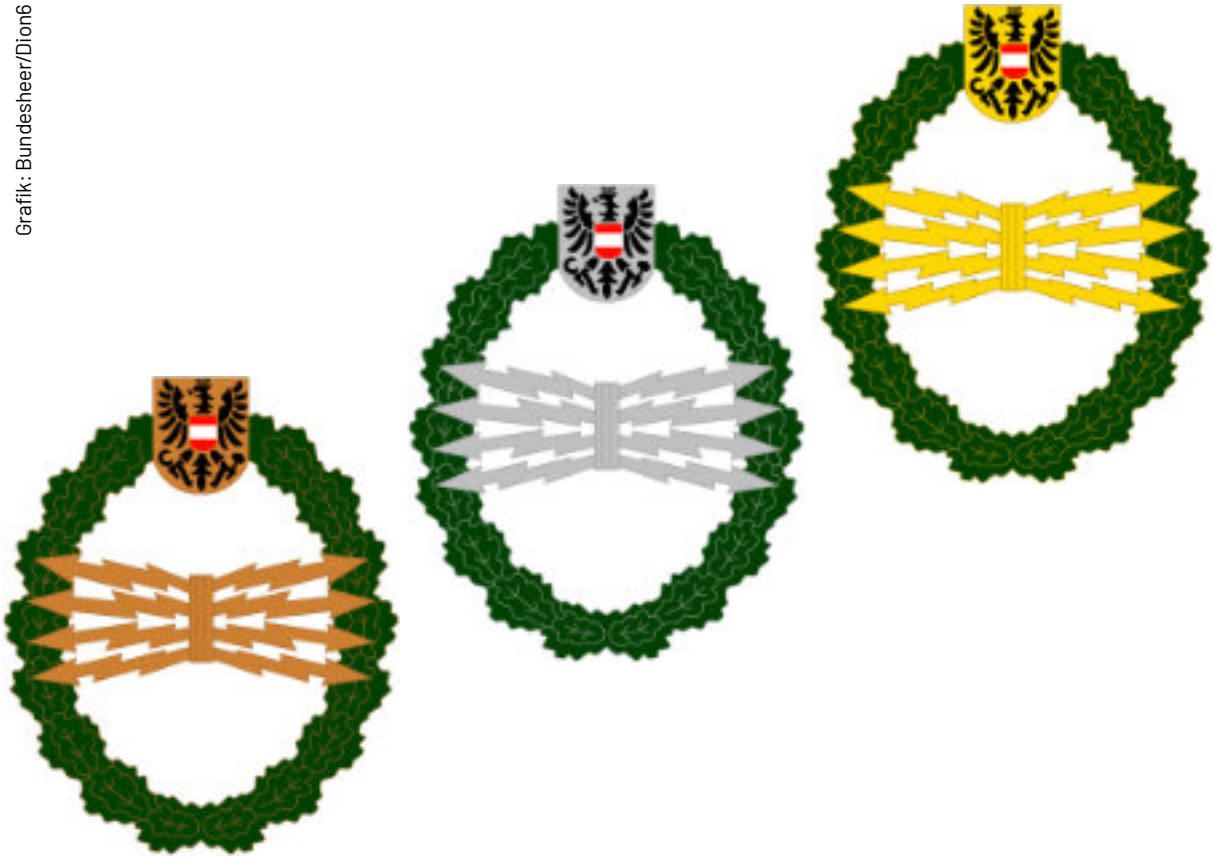


Foto: Bundesheer/Dion6

Die Geschichte des Fernmeldewesens und der Cyberkräfte des Österreichischen Bundesheeres

Die Geschichte des Österreichischen Bundesheeres während der Ersten und Zweiten Republik weist, im Gegensatz zu jener der kaiserlichen Streitkräften vor 1918, deren Aufarbeitung stetig weitergeht, größere Lücken auf. Dies betrifft ebenfalls einzelne Waffengattungen der Streitkräfte der Republik, für die es bis heute keine abschließenden Monografien gibt.

Die Kommunikation innerhalb der Armee, welche durch die technische Weiterentwicklung ab dem Vormärz des 19. Jahrhunderts, vor allem aber im nachfolgenden 20. Jahrhundert sich mit sehr großen Schritten entwickelte, hat für die Zeit nach 1918 noch kein solches Werk vorzuweisen.

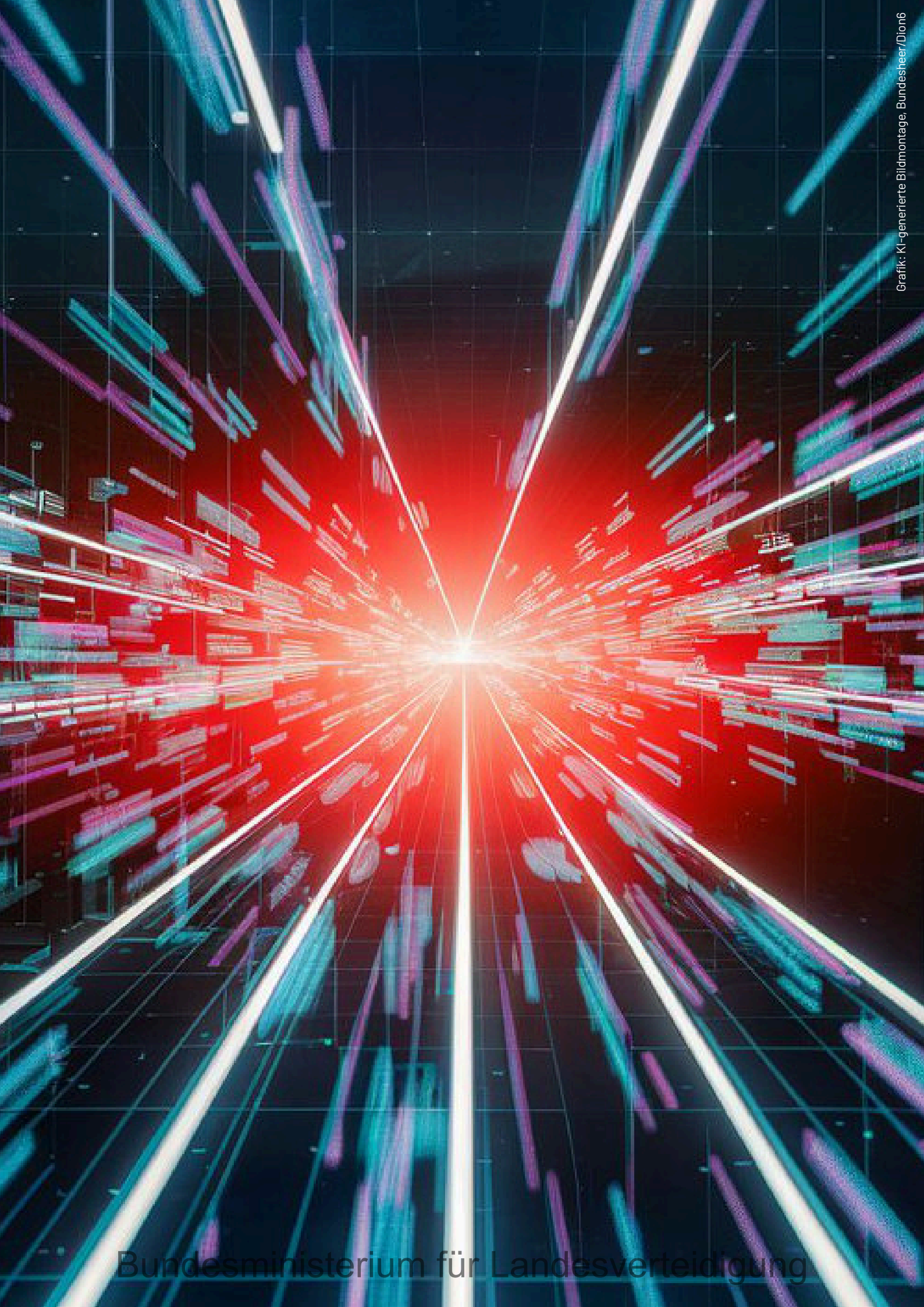
Auf Anweisung des Leiters der Direktion 6 - IKT und Cyber, Herrn Generalmajor Ing. Mag. Hermann KAPONIG, begann im Herbst 2024 die Ausarbeitung eines solchen Standardwerkes, welches in den nächsten Jahren erscheinen soll. Aufgearbeitet sollen hier nicht nur die einzelnen Zeitabschnitte in der Geschichte des Fernmeldewesens und der Cyberstreitkräfte von 1918 bis heute, sondern es werden auch die einzelnen Geräte, welche man beim österreichischen Militär für die Kommunikation verwendete, heereskundlich vorgestellt.

Eingebaut werden ebenso vergleichende Texte der DACH-Partner Deutschland und Schweiz über deren Entwicklung ihrer Cyberstreitkräfte. Die Zeit davor wird nur oberflächlich behandelt, da es hierfür bereits ein zweibändiges Werk, geschrieben von Oberst in Ruhe (iR) PRIKOWITSCH, Kurator des Fernmeldemuseums, gibt.

Zielpublikum des Buches ist neben der Fachwelt inner- wie außerhalb des Bundesheeres auch die vielen zivilen Militärenthusiasten und die inner- und außeruniversitären Wissenschaftler, die in ihre Forschungsarbeit dann auch die hier erarbeiteten wichtigen Aspekte der Militär(technik)geschichte einbauen können. Die Veröffentlichung ist abhängig von der Fertigstellung der jeweiligen Artikel für das zweite Halbjahr 2026 geplant.

Foto: Archiv/PRIKOWITSCH

Foto: Archiv/PRIKOWITSCH



Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Bundesministerium für Landesverteidigung

Highlights

SCHUTZSCHILD 24

Im Zeitraum vom 10 06 24 bis 21 06 24 fand die auf dem Szenario Schutzoperation basierenden Großübung (NÖ, OÖ, ST u. K) statt. Bei der Übung war jeder achte von der Direktion 6 gestellt. Aus folgenden Bereichen stammten die Teilnehmerinnen und Teilnehmer aus der Direktion 6 - IKT und Cyber:
IKTCyE, InfoOps&opKomm, MilCyZ und IMG.

(S. 14, 33, 52, 55, 60, 92, 93, 95, 99, 110, 113, 129, 134)

Foto: BMLV/HBF

LOCKED SHIELDS 24

Seit 2012 nimmt das MilCyZ fast jährlich an der Cyberübung teil. Die Übung zielt darauf ab, dass die Reaktionsfähigkeit, Verteidigungsstrategien und das taktisches Handeln gegen reale Cyberbedrohungen geübt wird. Dabei werden groß angelegte Cyberangriffe auf kritische Infrastrukturen simuliert, bei dem über 2.000 Cyberexperten aus 40 Nationen in 20 Team gegeneinander antreten.

(S. 89)

Grafik: Bundesheer/Dion6

Tactical Communication Network + MUV

Die Einführung des Tactical Communication Network (TCN), ein neues verlegbares IKT-System, war eines der Highlights aus dem Jahr 2024. Zusätzlich wurde erstmals der Nachfolger des Fernmelde-Prinzgauers, der IVECO Multirole Utility Vehicle (MUV) „NORIKER" vorgestellt.

(S. 14, 133)

Foto: BMLV/HBF

Foto: Bundesheer/Dion6

COMMON ROOF 24 (CR24) + erster Einsatz TCN

Im September und Oktober fand die siebte Ausgabe der trilateralen Übung statt, welche im DACH-Rahmen (DE, AUT, CH) abgehalten wird. Die CR ist als Betriebsführungsübung konzipiert, welche sich auf die gemeinsame Planung, Errichtung, und den Betrieb von Kommunikations- und Führungsunterstützungssystemen unter realitätsnahen Bedingungen konzentriert. Im Zuge dessen konnte auch das TCN erfolgreich getestet werden. (S. 52, 61, 123)

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Battlefield Management System & Führungsinformationssystem

Durch die vertraglich fixierte Beschaffung eines Battlefield Management Systems (BMS) für die gesamten österreichischen Landstreitkräfte und der Ablöse des veralteten Führungsinformationssystems (FüIS) PHÖNIX wurde ein weiterer positiver Schritt für den Aufbauplan ÖBH 2032+ getan.

(S. 74, 86)

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Medizinische Informationssystem (MEDIS)

Das Medizinische Informationssystem (MEDIS) soll im Rahmen des militärischen Gesundheitswesen mehrere Aufgaben übernehmen, wie z.B. Einhaltung gesetzlicher Vorgaben, Unterstützung der Sanitätsversorgung bei Einsatzvorbereitung und im Einsatz, Datenaustausch mit zivilen Gesundheitsdienstleistern und Bearbeitung aller medizinischen Prozesse in einem System.

(S. 44, 74)

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Fähigkeitsinformations-, planungs- und -steuerungssystem (FIPS)

FIPS dient der Digitalisierung zentraler Prozesse. Ziel ist es ein flexibles IT-Service bereitzustellen, das sämtliche Planungsaktivitäten im BMLV/ÖBH beginnend von der militärstrategischen Planung über die Fähigkeits- und Grundsatzplanung, die Strukturplanung, Beschaffung und Umsetzung in allen Entwicklungslinien bis hin zu Bereitstellung, Betrieb und Aussonderung unterstützt. (S. 75, 81)

Cyber EscapeRoom: Zusammenarbeit mit CIR

Im November 2024 präsentierte InfoOps&opKomm den mobilen Cyber-EscapeRoom der Direktion 6 – IKT und Cyber im Ausbildungszentrum Cyber und Informationsraum (CIR) der Deutschen Bundeswehr (DBW). Im Zuge dieser Präsentation konnte ein vertiefender Einblick in die Funktionsweise und die Wirkung des EscapeRoom gegeben werden. Daraus resultierte die Absicht vonseiten der DBW, ähnliche Modelle zu bauen und diese mit dem unseren zu verbinden. (S. 38)

Foto: Bundesheer/Dion6

KI im ÖBH

Das Thema Künstliche Intelligenz gewinnt im militärischen und Verwaltungsorientieren Bereich immer mehr an Bedeutung. Der Dion6 steht ein eigener Provider zur Verfügung und kann so Ressortspezifische Herausforderungen bestmöglich begegnen. Dazu wurden die Kooperationen mit internationalen Partnern und die Zusammenarbeit mit zivilen Dienstleistern nachhaltig verstärkt, um der breit gefächerten Auftragslage entsprechen zu können. (S. 14, 85)

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Umstellung Liegenschaftsserver + Serverrollout

Nachdem 2023 die Beschaffung und Lieferung der neuen Serverhardware für die Liegenschaftsserver erfolgt ist, konnte 2024 die Zuweisung der Hardware, die Vorkonfektionierung der Serverracks, die Aufstellung/Installation und Inbetriebnahme, der Parallelbetrieb und die Umstellung der Liegenschaftsserver begonnen werden.

(S. 86)

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Basiskurs Space & Sec / Secure PNT & NavWar

Der Kurs vermittelt grundlegendes Wissen zu militärischer Raumfahrttechnologie, beleuchtet strategische Aspekte der Konfliktführung im Weltraum und analysiert internationale Fähigkeiten sowie wirtschaftliche, organisatorische und legislative Rahmenbedingungen. Neben der theoretischen Wissensvermittlung bietet der Lehrgang auch die Möglichkeit, durch die Erarbeitung und Analyse realer Szenarien praxisnahe Fähigkeiten zu entwickeln. (S. 119)

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Grafik: pixabay.com

Bundesministerium für Landesverteidigung

IKT Bereitstellung und Nutzungsmanagement

Stellvertretender Leiter Direktion 6 – IKT und Cyber
Leiter IKTBstg&NuMngt: Bgdr Mag. Christof TATSCHL

Das Jahr 2024 war ein spannendes und produktives Jahr. Es war im wesentlichen gekennzeichnet mit der Vorbereitung der Einnahme der Direktion 6 IKT und Cyber (Dion6). Ein Vorgang welcher mit 01. November erfolgreich abgeschlossen werden konnte. Es konnte die erste Geschäftsordnung der Dion6 erstellt werden, die eine hervorragende Basis für die weitere Schärfung der Abläufe in der Direktion bietet.

Durch die Herausforderungen der Erfüllung des Zielbildes 2032 und die raschen technologischen Entwicklungszyklen befindet wir uns auch nach Festlegung der organisatorischen Rahmenbedingungen in einem andauernden Entwicklungsprozess. Im Rahmen des Entwicklungsprozesses, ist für uns das Zielbild 2032 handlungsleitend.

Ein zentraler Schritt unserer Entwicklung war die Schaffung der neuen Abteilung IKT-Bereitstellung und Nutzungsmanagement. Im wesentlichen kümmern sie sich um die Einsatzkoordination sowie die Einsatzauswertung im Fachbereich, die Steuerung des Betriebs und die Bereitstellung von autarken und sicheren IKT-Services.

Ein weiterer Aufgabenbereich, Informationsoperationen und operative Kommunikation (InfoOps&opKomm), ist verantwortlich für die operative Einsatzführung und Unterstützung der Informationskräfte sowie der operativen Kommunikation im Cyber- und Informationsraum mit der Beitragsleistung zur operativen Planung und Führung von Einsätzen.
Cloud-Technologien, einschließlich modernster Datenmanagement Konzepte und Sicherheitstechnologien, die es dem IKTSysÖBH 2032+ ermöglichen wird eine voll vernetzte, flexible, KI-unterstützte, resiliente Einsatzführung zu gewährleisten, wird das ÖBH im IKT-Leistungsbereich wieder zur Spitze aufschließen und im EU-Rahmen aber auch mit unseren Partnernationen auf Augenhöhe mitarbeiten können.

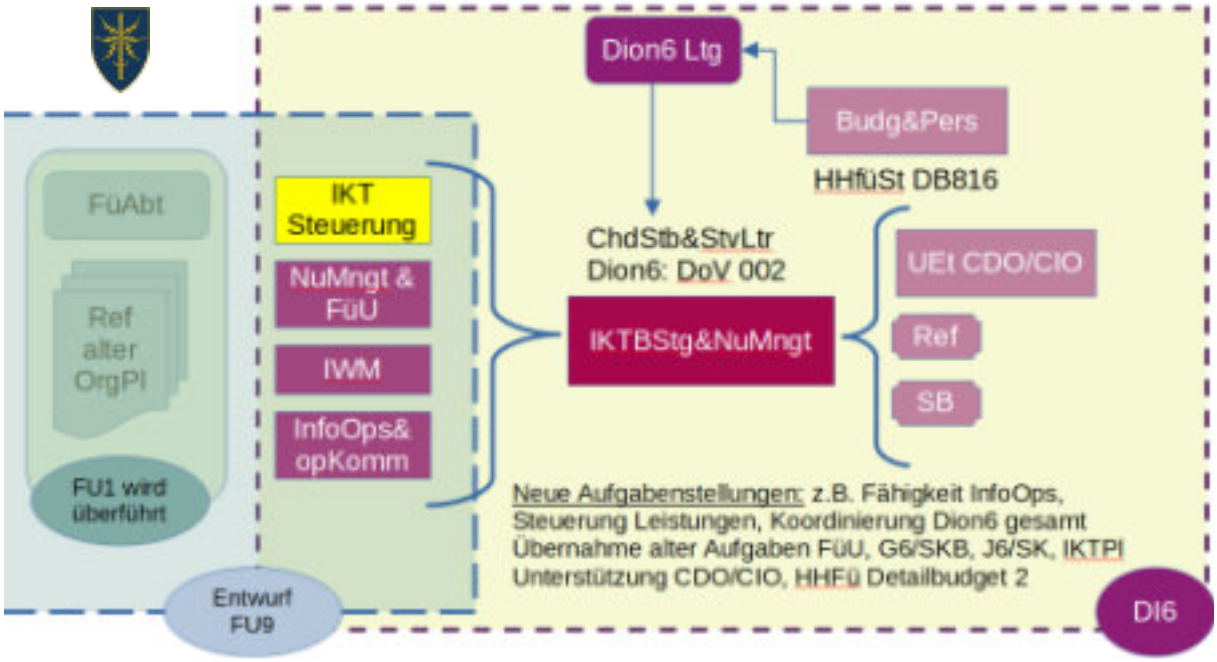
Auf diese Art wird es uns gelingen, eine neue Art von Einsatzführung, abgeleitet von dem derzeitig absehbaren Bedrohungsbildern zu ermöglichen.


Foto: BMLV/HBF

Wir haben mit unseren Partnern im DACH-Rahmen begonnen die Common Roof in Richtung einer Digitalisierungsübung der Streitkräfte weiterzuentwickeln und wollen bereits 2026 gemeinsam mit den Streitkräften an dieser Übungsserie teilnehmen, um Prozesse zu entwickeln und bereits getane Entwicklungsschritte zu evaluieren. Zusätzlich arbeitet die Dion6 intensiv mit zivilen Firmen zusammen, um den Blick auf die Zukunft nicht zu verlieren und das hohe Know-How in Österreich und im EU Umfeld für eine raschere und zielgerichtete Entwicklung nutzen zu können.

Die Waffengattungen Cyber, EloKa und InfoOps werden kontinuierliche weiterentwickelt. Dabei soll besonders auf die im ÖBH nun neu vorhandene Fähigkeit Information Operations hingewiesen werden, durch die es nun möglich sein wird den Einsatz führenden Kommandanten auch in der Umsetzung seiner Ziele im Informationsraum zu unterstützen. Diese Fähigkeit wird, besonders auch in Zusammenarbeit mit der Fähigkeit Cyber Operations, rasant an Bedeutung gewinnen. Die begonnene Arbeit an der Modernisierung und den Aufbau unserer Ausbildungsstätte der Führungsunterstützungsschule, um sie in ein Cyber-Information Truppenschule umzubauen, wird es ermöglichen die notwendige Fachausbildungen für die neuen Fähigkeiten zur Verfügung zu stellen.

Abschließend darf ich mich bei allen Mitarbeiterinnen und Mitarbeiter für Ihre hervorragende Arbeit bedanken und freue mich auch ein weiteres erfolgreiches Jahr.



Grafik: Bundesheer/Dion6

Aufgabenspektrum

Primäre Aufgabenfelder der Abteilung

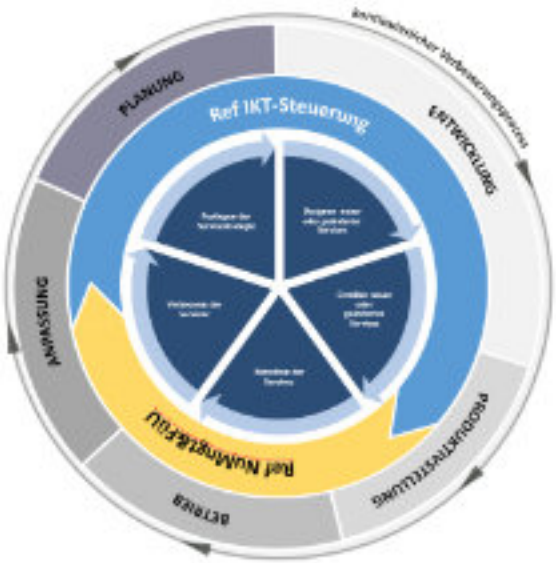
Das Referat IKT-Steuerung, ist dem Element IKT-Cyber Bereitstellung & Steuerung aus der Führungsabteilung der Anfang 2022 finalisierten Version der Dion6 entwachsen und ist in der neuen Struktur als zentrales Referat in der neuen Abteilung IKTBstg&NuMngt eingebettet. Die Bereitstellung von autarken und sicheren IKT-Services im Hinblick auf eine zielgenaue Digitalisierung von Prozessen des täglichen Dienstbetriebes sowie von militärischen Prozessen und Abläufen im Zuge der Einsatzvorbereitung, der Einsatzdurchführung und der Einsatznachbereitung erfordert in einem hohen Umfang Koordinierung, Steuerung und Abstimmung zwischen der Bereitstellung sowie den anderen Organisationselementen innerhalb der Direktion 6.

Hauptfelder & weitläufige Aufgabenstellungen

Auch wenn die endgültige Verfügung des neuen Referats in der aktuellen Version noch bevorsteht, wurde bereits eine Vielzahl an Aufgaben mit nicht einmal einer Handvoll Personen 2024 konsequent abgearbeitet.

- Koordinierung und Synchronisierung der Bearbeitungen zum IKT-System ÖBH2032+
- Mitwirkung an allen maßgeblichen Planungsarbeiten zum Zielbild 2032
- Inhaltliche Koordinierung des Providers IKT&CySihZ im Tandem mit Chief Technology Officer
- Koordinierung und Steuerung aller Querschnittsaufgaben in der Direktion
- Wirkungsorientierung, Wirkungssteuerung, Koordinierung des Controllings und maßgeblicher Kennzahlen für die Ressourcensteuerung
- Aufbereiten von wichtigen Entscheidungslösungen in Einzelmaterien und Steuerung wesentlicher operativer Einzelaufgaben des Providers
- umfangreiche Steuerung kollaborativer Bearbeitungen zu Kooperationen, Führungsentscheidungen im Fachbereich
- Koordinierungen im Forschungsmanagement und in der Entwicklung sowohl durch direkte Projektteilnahme als auch durch Aufgabenwahrnehmung im Serviceportfolio

Grafik: Bundesheer/Dion6



Ressourcen-, Ziel- und Leistungsplan

Ausgehend vom gültigen Ressourcen-, Ziel- und Leistungsplan 2024 bis 2027, wurden folgende sehr weitreichendere Ziele im Umfang bereits 2023 entworfen und verfolgt:

- 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

Ziel 1 wurde 2024 teilweise erreicht, wobei für die weitere Roadmap zum Aufwuchs die strukturelle Anpassung, die seit 2023 in Schwebe ist, schon dringend erforderlich wird. Mittlerweile wird der SOLL-Stand des verfügten Organisationsplans des Militärischen Cyberzentrums mit Leiharbeitern gerechnet bereits im IST überschritten.

Ziel 2 wurde mit den Maßnahmen in den Meilensteinen teilweise erreicht, wobei vor allem die nicht verfolgte Aufstellung des strategischen Unterstützungselements für die Digitalisierung schmerzt, weil diese Aufgabenstellungen zwangsläufig in umfangreiche Steuerungsaufgaben münden, die das eigene Referat noch massiver auslasten.

Ziel 3 wurde im Wesentlichen in den Zielen 2024 teilweise erreicht, weil Verzögerungen beim Implementieren der Force Protection CREW entstanden und die Weiterbearbeitung der Planungsansätze für elektronische Kampfführung durch die Versetzung des Sachbearbeiters zunächst auffallend stagnierte.

Ziel 4 wurde mit Ausnahme der Evaluierung der Direktion 6 nicht erreicht, weil weder strukturelle Voraussetzungen noch ausreichende Adaptierung für ein Labor an der Führungsunterstützungsschule und Cyber – Range beim primären Fähigkeitsträger Militärisches Cyberzentrum vorlagen und kein gültiger Organisationsplan für die Aufbauphase 2 erreicht werden konnte.

Projektsteuerung und sonstige Aufgabenstellungen

Nebenaufgaben

Für die internen Bearbeitungen im Provider wurden weiterhin alle Aufträge in der Serviceverantwortung ASECOS I/Fähigkeitserhalt und in der Serviceentwicklung für die Anpassungen der IT-Infrastruktur zum European Operations Wide Area Network (EUOpsWAN) erteilt. Dazu wurde ebenfalls die technische Verantwortung für die Betriebsführung des neuen Netzwerk SUE durch das Referat übernommen.

Entwicklungsprojekte

Einen substanziell wesentlichen Beitrag leistete das Referat durch Oberst PUSTELNIK als Stellvertreter der Expertengruppe TQC (Testing, Qualification & Certification) im Projekt CBRN SaaS, bei welchem die internationalen Testungen und Abschlussarbeiten bis zum Ende der Phase 1 laufend begleitet wurden. Im Zuge der Weiterführung in der Phase 2 beginnend ab Juni 2024 kristallisierte sich nach dem CONOPS Workshop im Juli schnell heraus, dass es einer eigenen Expertengruppe für die Ausprägung eines klaren IKT - Konzepts bedarf.

Diese Rolle wurde im 3. Quartal fliegend als „Brückenkopf" der neu aufzustellenden Expertengruppe Netzwerk & Integration

übernommen und binnen kurzer Zeit wurde im Vorfeld der Konstituierung mit den Vertretern ABC-Abwehrzentrum, Strukturplanung, Abteilung Wissenschaft, Forschung und Entwicklung und den eigenen Experten des IKT&Cybersicherheitszentrums ein verständliches und durchgängiges Setup für die IKT – Architektur des Systems im Oktober entworfen. Damit wurden die vorangegangenen Fragestellungen des Firmenkonsortiums weitgehend aufgelöst und bei der Konferenz in BUDAPEST im November erfuhr der Vorschlag auch ganz klar die internationale Zustimmung.

Mittlerweile befindet sich die Expertengruppe unter der Leitung von Oberst PUSTELNIK in Aufstellung und leitet Anfang 2025 bereits die arbeitsmäßigen Vorbereitungen für Planung und Design sowie Durchführung der Verfahrenserprobung in Phase 2 ein. Die Rahmenbedingungen für die Architektur orientieren sich sehr stark am zukünftigen IKT - System ÖBH2032+ und leisten damit eine gute Basis, um die Firmenprodukte möglichst einfach in das militärische IKT - Umfeld integrieren zu können. Mittlerweile läuft parallel auch bereits ein Nachfolgeprojekt unter der Federführung der Abteilung Wissenschaft, Forschung und Entwicklung mit der Direktion 6 als unmittelbaren Bedarfsträger in der erweiterten Projektgruppe.

Unterstützungselement CDO und CIO

Im Jahr 2024 hat die Digitalisierung weiterhin eine zentrale Rolle in der Transformation von Wirtschaft und Gesellschaft gespielt. Die rasante Entwicklung neuer Technologien und die zunehmende Integration digitaler Lösungen in nahezu allen Lebensbereichen haben sowohl Chancen als auch Herausforderungen mit sich gebracht. Um die Zusammenarbeit der öffentlichen Verwaltung effizienter zu gestalten wurden in den Gremien CDO-Task-Force (CDOs der Ministerien), IKT-Bund (CIOs der Ministerien) und in der Kooperation BLSG (CIOs von Bund, Länder, Städte und Gemeinden) Bearbeitungsschwerpunkte definiert und diese an Arbeits- und Projektgruppen zur Erstellung von Grundlagendokumenten wie Strategien, Leitlinien oder Konventionen zugeteilt.

Die Beitragsleistungen des BMLV wurden durch das UetCDO&CIO koordiniert bzw. durch die Teilnahme in diversen Projekt- und Arbeitsgruppen eingebracht.

Schwerpunkte im Jahr 2024 waren:

- Die Erstellung eines Leitfaden für den Einsatz von Open Source Software in der Bundesverwaltung.

Zweck des Dokuments ist es, die Unterschiede von OSS (Quelloffener Software) vs. proprietärer Software kompakt darzustellen und den IT- Verantwortlichen der Bundesverwaltung Lösungsansätze (Software-Auswahlprozess, Darstellung technischer, betrieblicher und rechtlicher Kriterien) für den Einsatz von OSS anzubieten.

- Implementierung eines Bundessprachmodells für maschinelle Übersetzungen.

Aufgrund einer Initiative des BMLV erfolgten erste Bearbeitungsschritte um KI-basierende Sprachübersetzungen in der öffentlichen Verwaltung ohne Datenabfluss zu ermöglichen. Es wurden die Anforderungsprofile der Bundesressorts erhoben und erste Lösungsvarianten erarbeitet. Das Projekt wird 2025 aufgrund der damit verbundenen Sicherstellung der Datensouveränität weitergeführt.

- Teilnahme BMLV im Redaktionsteam BLSG

Durch das Redaktionsteam (4 Personen) erfolgt die Aufbereitung der BLSG-Sitzungen durch Auswahl der Themenschwerpunkte sowie die Koordination des Wissensmanagements für das Gremium. Für das BMLV ergibt sich dadurch die Möglichkeit aktuelle Herausforderungen der Digitalisierung rechtzeitig zu antizipieren und an vorhandenen Lösungsansätzen zu partizipieren.

Im Rahmen der Implementierung eines Staatsgrundnetzes im Sinne des Digital Austria Act (DAA) erfolgten weitere Bearbeitungen in Zusammenarbeit mit dem Bundesministerium für Inneres. In intensiven Workshops wurde die Aufnahme eines erweiterten Testbetriebs durch das IKT&CySihZ vorbereitet, um technische und betriebliche Lösungsmöglichkeiten für das zukünftige Staatsgrundnetz auszuarbeiten.

Um zukünftigen technologischen Herausfor-

derungen gewachsen zu sein wird durch die Dion 6 auch die Forschung vorangetrieben. Insbesondere in den Themenfeldern der Quantentechnologie wird intensiv mitgearbeitet. Das UetCDO&CIO ist dabei als POC und Mitarbeiter in diversen Arbeitsgruppen beteiligt. Die Forschungsunterstützung zum Aufbau einer sicheren Quantenkommunikationsinfrastruktur waren in diesem Jahr im Fokus.

Informations- und Wissensmanagement

Die neue Organisationsstruktur, die mit Oktober 2024 eingenommen wurde, bedingte eine Umgliederung des Referates und die Umstrukturierung der Aufgabenzuordnungen. Waren bis zur Einnahme des neuen Organisationsplanes noch die Hauptkanzlei an den Standorten WIEN, WALS und GRAZ Teil des Referats, liegt nunmehr die Konzentration alleinig auf dem Informations- und Wissensmanagement für die GDLV. Die nachfolgende Darstellung soll einen Überblick über die erbrachten Leistungen im Jahr 2024 geben:

Bei den Einsätzen/Übungen DAEDALUS24, SCHUTZSCHILD 24 und der AIRPOWER24 wurde das Informationsmanagement geplant, angeordnet, kontrolliert und gesteuert. Hierzu wurde zudem Personal des Referats für die Durchführungsphasen in die Einsatzstäbe abgestellt.

Besonders intensiv waren die Arbeiten für und die Mitwirkung an der Schwergewichts-Übung des ÖBH – der SCHUTZSCHILD24.

Zusätzlich wurde auch die COMMON ROOF 2024 personell unterstützt. In den Nachbereitungsphasen wurden zum Zweck des Wissenserhalts, strukturierte Datensicherungen vollzogen.

Das mit Jänner 2022 begonnene Projekt „Individuelle Datenverarbeitung und individuelle Anwendungsentwicklung (IDV/IAE)" konnte mit Mai 2024 positiv abgeschlossen werden. Nach einer BMLV/ÖBH weiten Bedarfserhebung, der Evaluierung möglicher Entwicklungsumgebungen, der durch Appl nunmehr bereitgestellten Entwicklungsumgebung (IDV-Entwicklungsservice) und der Bereitstellung einer Entwickler-Plattform (durch MilKdo T), fand das Projekt mit der Verfügung der neuen Richtlinie „Individuelle Datenverarbeitung für das BMLV und ÖBH" (die bis dahin gültige RiL war übrigens schon 27 Jahre alt) seinen Abschluss.

Die ebenfalls im Jahr 2022 gestartete Initiative zur Reduzierung der Info-Flut im BMLV-ELAK (in Zusammenarbeit mit Präs, ZGK und Pers-Abt/TrBe), deren Ziel es war und ist, die Masse jener Geschäftsstücke (GStk), die derzeit vielfach im BMLV-ELAK verteilt werden, obwohl sie weder einer Erledigung noch einer Umsetzung bedürfen, sondern lediglich der Info dienen, zentral auf anderen Plattformen nach dem Pull-Prinzip bereitzustellen, konnte heuer erfolgreich abgeschlossen werden.

Der Intranetauftritt der Direktion 6 – IKT und Cyber wurde laufend betreut, sodass aktuelle und valide Informationen über das gesamte Leistungsspektrum der Direktion (und darüber hinaus) abrufbar sind.

Grafik: Bundesheer/Dion6

Als eines der vielen Leuchtturmprojekte in diesem Zusammenhang darf erwähnt werden, dass über diese Seite nun militärwissenschaftliche Arbeiten der letzten Dekade aus dem Fachbereich abrufbar sind – dies soll den Wissenstransfer beflügeln.

Die Ergebnisse der Change Advisory Boards (CABs) für Services, die dem Referat als Anwenderfachabteilung zugeordnet sind (BMLV-ELAK, CMS Liferay und HCL Notes), brachten signifikante Verbesserungen für die Benutzer.

Die Erweiterung der Funktionalitäten und Steigerung der Benutzerfreundlichkeit wird auch im kommenden Jahr die Anwender des gesamten Ressorts bei der Erfüllung gestellter Aufgaben unterstützen.

Durch prozessorientiertes Wissensmanagement, der Modellierung und Verfügbarmachung gelebter Prozesse, soll der Wissenserhalt und -transfer unterstützt werden. Die Ambition, Wissen verfügbar zu machen, indem Aufgaben in Arbeitsschritte geteilt werden und der Ablauf der Tätigkeiten Daten-hinterlegt abgebildet wird, soll verstärkt verfolgt werden. Der erste Schritt wurde hierfür 2024 gesetzt, indem die Prozesse der Referats mittels der Prozessmanagementanwendung ADONIS NP generiert wurden. Nun sollen weitere Organisationseinheiten folgen.

Aufgrund der Vielzahl an Aufgaben, kann nicht jede Leistung (bspw. die Neuerstellung der Geschäftsordnung der Dion6 aufgrund der erfolgten Organisationsänderung, das Postfach-Management im HCL Notes, die Entwicklung und Bereitstellung der Jahres-Vorhabens-Übersicht im HCL Notes OE-Kalender, die auch mit der Neuorganisation zusammenhängenden, unzähligen Rollenvergaben im BMLV-ELAK, die Schulungen und Unterstützungen im Zusammenhang mit dem CMS Liferay, die Unterstützung und Bereitstellung von Vorlagen in LibreOffice, die Ausrollung und Betreuung des BMLV-ELAK bei den Auslandsmissionen, etc.) näher beschrieben werden, die dieses Referat (trotz der nicht besetzten Arbeitsplätze) mit viel Engagement und Eigeninitiative erbracht hat. Zudem wurden bis zur Einnahme der neuen Organisationsplans, die Hauptkanzleien der GDLV (an vier Standorten) geführt, die ein verlässliches, rasches Zuteilen physischer und elektronischer Poststücke gewährleisteten.

InfoOps&opKomm

Öffentlichkeitsarbeit

Die Direktion 6 war im Jahr 2024 in der Öffentlichkeitsarbeit sehr aktiv. Ob bei Messen, Konferenzen, Sportveranstaltungen, beim Wiener Donauinselfest, in Schulen oder beim Nationalfeiertag. Ziel war es, Werbung für den Cyber-Grundwehrdienst zu machen, Personal für die technischen Bereiche zu werben, über Karrieremöglichkeiten aufzuklären sowie das Österreichische Bundesheer als attraktiven und modernen Arbeitgeber zu präsentieren.

HTL Veranstaltungen

Im Zuge des aktiven Rekruting und Vorstellung der Direktion 6 – IKT und Cyber als attraktiven und innovativen Arbeitgeber wurden 2024 das ganze Jahr über mehrere HTLs mit IKT-Schwerpunkt in Wien und Umgebung besucht. Unter anderem wurden die Direktion 6 – IKT und Cyber in folgende Schulen vertreten. Im ersten Halbjahr besuchte unser Team die HTL Spengergasse, die HTL Mödling, die HTL Wien West (Ottakring), die HTL Wiener Neustadt, die HTL Donaustadt und die HTL Rennweg. Im zweiten Halbjahr war es dann ruhiger, da waren wir nur in der HTL Wien 10 und ein zweites Mal in der HTL Rennweg.

HTL Spengergasse

Die HTL Spengergasse ist eine besondere Schule für die Direktion 6 - IKT und Cyber. Es freut uns, dass wir daher auch dieses Jahr unsere Partnerschaft mit der HTL Spengergasse pflegen und stärken konnten.

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Der Firmeninformationstag 24 der HTL SPENGERGASSE am Donnerstag, 22. Februar 2024 war wiederum aus der Sicht Direktion - 6 IKT und Cyber eine gelungene Veranstaltung in allen Belangen.

Die Schülerinnen und Schüler der unterschiedlichen Abteilungen zeigten eine reges Interesse am österreichischen Bundesheer und im speziellen der Direktion 6 – IKT und Cyber.

Da ein großer Teil der Fragen im Zusammenhang mit dem Grundwehrdienst als "CYBER-GWD" gestellt wurden, war es ein sehr großer Mehrwert, wieder Cyber-GWDs zu einer Schulveranstaltung mitzunehmen, da Ihr geringer Altersunterschied zu den Schülern und Ihre Aussagen aus der Praxis den Zugang für die Schüler vereinfachten.

Cyber-EscapeRoom Tage für die HTL Spengergasse vor dem HGM

Im Zuge der gelebten Partnerschaft zwischen der Direktion 6 – IKT und Cyber und der HTL Spengergasse veranstaltete das Team InfoOps&opKomm unter der Leitung des neuen Partnerschaftsverantwortlichen Gerald WOHLKÖNIG zwei Cyber Escape Room Tage vor dem HGM Wien im Arsenal.

Berufs- und Studieninformationsmesse (BeSt) Wien 24

Von 07. März bis am 10. März 2024 war die Direktion 6 – IKT und Cyber, mit mehreren Info-Offizieren und CYBER-GWD`s auf der BeSt Wien 24, in der Wiener Stadthalle auf dem Stand des Österreichischen Bundesheeres mit unter anderem dem Heerespersonalamt (HPA), einem Vertreter des Militärkommando Wien (MilKdoW), dem Jagdkommando, einem Hubschrauberpilot, einem Vertreter von der Luftunterstützung aus LANGENLEBARN und der Militärpolizei (MP) vertreten.

Foto: Bundesheer/Dion6

Im Allgemeinen wurden die Besucherinnen und Besucher zu den Themen allgemeine Wehrpflicht, Stellung, Grundwehrdienst, aber auch Frauen beim Heer.

Aber auch intensive Beratungsgespräche zu dem Thema CYBER-GWD und welche Möglichkeiten die Grundwehrdiener beim ÖBH so haben aufgeklärt.

Ganz besonders hervorzuheben ist, dass sich sehr viele junge Frauen über die Möglichkeiten, sowohl als Soldatin, aber auch als zivile Mitarbeiterin, für das österreichische Bundesheer tätig zu sein, erkundigt haben.

TU-Day: Bundesheer und Cybertruppe an der Technischen Universität Wien

Das Bundesheer und die Cybertruppe präsentierten sich beim TU-Day sehr erfolgreich. Rund 100 interessierte Besucher wurden am Stand der Direktion – IKT und Cyber an ihrem Stand beraten.

Die Messe war ideal, um Bachelor-Studentinnen und Studenten anzusprechen und auf die Option der Teilzeitbeschäftigung hinzuweisen und in weiterer Folge aufgabenspezifisch vertiefend auszubilden. Studienabsolventinnen und Studienabsolventen sind aufgrund der hohen Nachfrage deutlich schwerer zu rekrutieren.

Foto: Bundesheer/Dion6

Tag der offenen Tür in der Liechtensteinkaserne / Allentsteig

Am letzten Maiwochenende öffneten die Soldatinnen und Soldaten des Aufklärungs- und Artilleriebataillons 4 in der Liechtenstein-Kaserne die Tore und luden die Bevölkerung des Waldviertels ein, um sich über das Bundesheer in der Region zu informieren. So nahmen rund 2.500 Besucherinnen und Besucher das Angebot an und strömten in die Kaserne.

Um die Weiterentwicklung im Bereich der Technik zu präsentieren, wurden zusätzlich historische Aufklärungsfahrzeuge, wie der Schützenpanzer "Saurer" und der Jagdpanzer "Kürassier" ausgestellt.

Das Team InfoOps&opKomm war mit dem Cyper-EscapeRoom anwesend. Das neue Spielerlebnis, welches den Fokus auf Cyber-Awareness im Privat- und Berufsleben legt, wurde von den Teilnehmerinnen und Teilnehmer sehr positiv angenommen. Außerdem bestand reges Interesse an den Tätigkeitsfeldern der Direktion 6 – IKT und Cyber sowie dem Cybergrundwehrdienst.

Foto: Bundesheer/Dion6

Heer on Tour 24 / MilMusik 24 Bewerbekonzerte

Im Mai 2024 fanden unter dem Leitthema „Mission vorwärts" die Leistungsschaureihe „Heer on Tour" an fünf Orten in Niederösterreich in Verbindung mit den Bewerbekonzerten des MillMusik Festivals 2024 statt. Durch Mitmachstationen sollten vor allem ein Heer zum (Be-)Greifen die Verweilzeit aller Besucher anheben und so Personal nachhaltiger beworben werden.

Foto: Bundesheer/Dion6

Die Direktion 6 - IKT und Cyber war mit dem Cyber-EscapeRoom bei den Terminen am 15. Mai in St. Pölten, 16. Mai in Poysdorf und am 17. Mai in Mödling vertreten. Besonders in St. Pölten, wo am 15.05. ab 08:30 auch ein Tag der Schulen stattfand, war der Andrang sehr groß.

SCHUTZSCHILD 24 - Aufgaben InfoOps

Bei der durchgeführten Großübung SCHUTZ-SCHILD 2024 wird zum ersten Mal der Informationsraum, gebündelt in der J10/ HICON Zelle, sowohl als „RED-Team" (Gegen-spieler) als auch „BLUE-Team" (Eigene Kräfte) bespielt. Hierfür wurden im Vorfeld eine eigene Intranetseite erstellt, die das Internet sowie diverse Social-Media Plattformen abbildet. Auf dieser Webseite wurden den übenden Teilen Postings zur Ansicht bereitge-stellt. Auf diese galt es dann richtig zu reagieren, sei es eine Meldung an den Vorge-setzten, die zuständige Stelle oder eine offizielle Pressemitteilung.

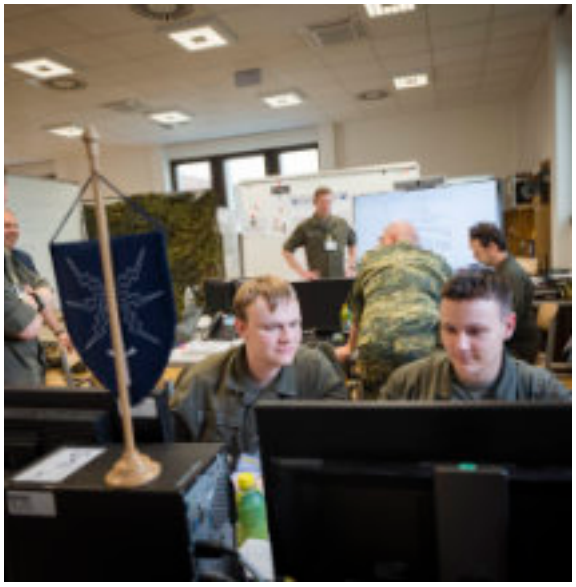


Foto: BMLV/HBF

Cyber Escape Room on Tour "A Hell of a Ride" im Juni 2024

MOTORTAG am Salzburgring

Eine Veranstaltung von Motorbegeisterten für Motorbegeisterte. An beiden Tagen waren um die 20.000 Besucherinnen und Besucher anwesend. An den Spielen Cyber-EscapeRoom nahmen in Summe ca. 180 Personen teil. Diese Veranstaltung wäre zukünftig eine ideale Bühne für Großfahr-zeuge und schweres Gerät.

Foto: Bundesheer/Dion6

Cyber Infotage in der Stiftung Theresiani-sche Akademie in 1040 Wien

Auf Einladung des Theresianums veranstal-tete die Direktion 6 – IKT und Cyber zwei "Cyber-Informationstage" für interessierte Schülerinnen und Schüler. Das Interesse war sehr hoch und es nahmen an beiden Tagen in Summe 300 Schülerinnen und Schüler am Cyber-EscapeRoom teil. Das Feedback war überaus positiv und die Schulleitung freut sich, dieses Event 2025 zu wiederholen.

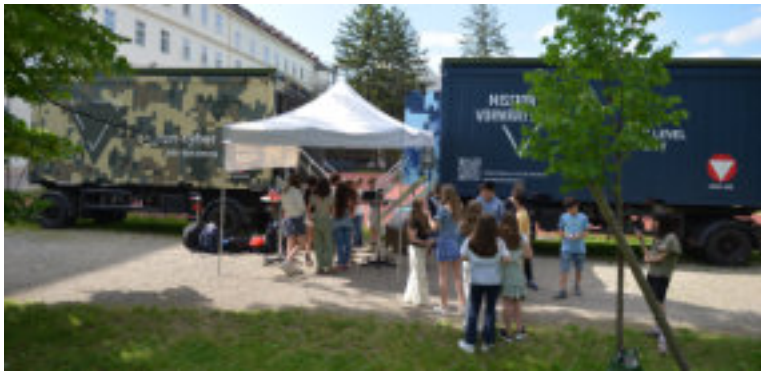


Foto: Bundesheer/Dion6

Tag der Schulen und Tag der offenen Tür in der JANSA Kaserne GROSSMITTEL

Die JANSA Kaserne öffnete am 07. Juni und 08. Juni 2024 ihre Pforten und lud am 07. Juni zum Tag der Schulen und am 08. Juni zum Tag der offenen Tür ein. Besonders am 08. Juni war der Besucheransturm sehr groß und der Cyber-EscapeRoom durchgehend ausgebucht.

Foto: Bundesheer/Dion6

MINT Challenge Finale der Industriellen Vereinigung Salzburg in der RedBull Arena SALZBURG

Die Industriellen Vereinigung Österreich veranstaltete am 13. Juni 2024 in SALZBURG, RedBull Arena die MINT Challenge 2024. Auf Einladung durch die IV nahm die Direktion 6 – IKT und Cyber mit dem Cyber-EscapeRoom daran teil.

Foto: Bundesheer/Dion6

Am Vormittag besuchten 2 Schulklassen mit in Summe 45 Schülerinnen und Schülern den EscapeRoom. Am Nachmittag nahmen Mitarbeiterinnen und Mitarbeiter der IV Salzburg und deren Partner am EscapeRoom teil und waren restlos begeistert von der innovativen Möglichkeit, Cyber Awareness spielerisch zu vermitteln. Es herrschte großes Interesse an weiteren Kooperationen mit der IV und den Bildungsdirektionen Salzburg und Burgenland.

Donauinselfest 2024

Von 20. Juni bis 23. Juni 2024 fand wieder das DONAUINSELFEST in WIEN statt. Es kamen ca. 3 Mio Besucherinnen und Besucher und auch bei der Sportinsel des ÖBH war der Andrang sehr groß. Der Cyber-EscapeRoom war immer ausgebucht.

Foto: Bundesheer/Dion6

Hot in the City Schulabschlussfest

Nach einer Pandemie-bedingten Pause fand 2024 von 25. Juni bis 27. Juni wieder das Schulabschlussfest „Hot in the City" (HitC) im GÄNSEHÄUFEL in WIEN statt.

Zum größten Schulabschlussfest Wiens kamen an den 3 Tagen ca. 14.000 Schülerinnen und Schüler. Davon nahmen in Summe 250 Schülerinnen und Schüler am Cyber-EscapeRoom teil.

Foto: Bundesheer/Dion6

LEVEL UP 24 Gaming & E-Sport Messe im Messezentrum SALZBURG

Von 29. Juni bis 30. Juni fand auch 2024 wieder die Gaming & E-Sport Messe LEVEL UP im Messezentrum SALZBURG statt. Das ÖBH stellte ein 600m^2 Areal mit einem großen Auszug aus allen Cyber, IKT, EloKa und Simulationsbereichen des gesamten Bundesheeres. Die Besucherinnen und Besucher konnten einen Schießsimulator, zwei Flugsimulatoren sowie Geräte und Fähigkeiten des ÖBH erleben. Der Cyber-EscapeRoom war das i-Tüpfelchen und rundete das ÖBH Erlebnis auf der LEVEL UP gelungen ab. An den zwei Messetagen spielten zahlreiche Besucherinnen und Besucher die zweite Spielversion im Cyber-EscapeRoom, welches wie das Vorherige den Fokus auf Cyber Awareness legt.

Foto: Bundesheer/Dion6

Jobmesse Wien – Marx Halle

Am 07. September und 08. September 2024 fand in der Marx Halle Wien die Jobmesse 2024 statt, wo mehrere tausend Besucher gekommen waren um sich bei ca. 120 Ausstellerinnen und Aussteller, bezüglich eines Jobs zu erkundigen. Die Direktion 6 – IKT und Cyber war gemeinsam mit dem Heerespersonalamt (HPA) auf einem Stand vertreten und repräsentierte das Österreichische Bundesheer.

Foto: Bundesheer/Dion6

An beiden Tagen kamen mehrere hundert Besucherinnen und Besucher an den Stand und zeigten sich sehr interessiert an den Angeboten. Hauptsächlich ging es um die Themen „Lehrlinge beim Heer", „zivile Berufsmöglichkeiten" und wofür die Cyberkräfte beim ÖBH zuständig sind und welche Jobmöglichkeiten es gibt.

Besuch der Hochschule des Bundes für öffentliche Verwaltung

Am 10. September 2024 besuchten Studierende der Hochschule des Bundes für öffentliche Verwaltung aus Deutschland die Direktion 6 – IKT und Cyber.

Die Delegation bestand aus einem Dozenten und zehn Studierenden des Fachbereichs Digital Administration und Cyber-Security, deren zukünftige Stammbehörden unter anderem das deutsche Bundeskriminalamt (BKA), das Bundesministerium für Wirtschaft und Klimaschutz (BMWK), das Bundesministerium des Innern und für Heimat (BMI), das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie die Bundeswehr sein werden.

Foto: Bundesheer/Dion6

Das Team InfoOps&opKomm organisierte für den Besuch mehrere Vortragende aus der Direktion 6 die verschiedene Themen vortrugen wie z.B. Tätigkeitsbereiche der Direktion, Cyber Security, Digitale Verwaltung und deren Anwendung und Quanten Kryptografie und Quanten Computing.

Feierliche Übernahme von 118 Leutnanten

Am Samstag, den 28. September, wurden 72 Berufs- und 46 Milizoffiziere, davon 8 Frauen, des Jahrganges „Generalmajor Sommer" an der TherMilAk feierlich in die Truppe übernommen.

Aus dem Jahrgang Generalmajor Sommer mustern 6 Leutnante in die beiden FüUBs und in die FüUS aus. Generalmajor Kaponig nahm persönlich an dem Festakt teil und machte sich ein Bild von den neuen Leutnanten.

Foto: Bundesheer/Dion6

Die Besucherinnen und Besucher konnten im Cyber-EscapeRoom ihre Cyber-Fähigkeiten unter Beweis stellen und sich über die Tätigkeitsfelder der Direktion 6 informieren.

Tag der offenen Tür TüplA/LAGER KAUFHOLZ am 05. Oktober 2024

Die Direktion 6 - IKT und Cyber war mit dem Cyber-EscapeRoom Vorort und hat die Besucherinnen und Besucher dazu eingeladen ihr Cyber-Wissen zu überprüfen und unter Beweis zu stellen. Zeitgleich konnten die anderen Gäste über den breiten Wirkungsbereich der Direktion 6 – IKT und Cyber sowie die Möglichkeit des Cyber-Grundwehrdienstes informiert werden.

Foto: Bundesheer/Dion6

25. Oktober 2024: Tag der Schulen

Die Direktion 6 - IKT und Cyber betrieb im Zuge der Leistungsshows des Bundesheeres zum Nationalfeiertag 2024 AM HOF die Themeninsel "Cyber, Forschung und Technik" in Zusammenarbeit mit fast allen Direktionen der GDVPol. Alle Teile präsentierten Forschungs- und Technikprojekte für das Bundesheer von Morgen.

Foto: Bundesheer/Dion6

Die Schwerpunkte dieses Jahr waren neben technischen Neuerungen aus den Bereichen KFZ und Infantriewaffen vor allem Drohnen sowie Drohnenabwehr, Desinformation und KI. Neben den statischen Forschungsständen gab es auch viele Mitmachstationen für die Besucherinnen und Besucher. Im Außenbereich der Themeninsel wurden der Cyber-EscapeRoom, ein Darkroom zum Ausprobieren der neuesten Nachtsichtgeräte, ein Drohnenkäfig für Flugvorführungen präsentiert. Im Drohnenkäfig konnte man sich selbst als Drohnenpilotin und Drohnenpilot beweisen.

26. Oktober 2024: Nationalfeiertag 2024

Bereits zu Beginn der Leistungsschau um 9 Uhr wurden zahlreiche Interessierte auf der Themeninsel begrüßt. Dabei konnten sie sich über die neuesten Entwicklung im Bereich der Cyberabwehr informieren, einschließlich des kürzlich eingeführten Tactical Communication Network, welches bereits sehr erfolgreich bei der Truppe getestet und eingeführt wurde.

Außerdem wurde im Zuge der Präsentation die Wichtigkeit der Zusammenarbeit zwischen dem Österreichischen Bundesheer und zivilen als auch staatlichen Einsatzorganisationen im Bereich der elektronischen Kampfführung und der Cyberabwehr deutlich. Ein besonderer Fokus lag auf der Kompetenz der schnellen und zuverlässigen Bereitstellung von Informationen und daraus resultierenden Reaktionen auf sich ändernde Bedrohungslagen und die Art und Weise, wie die einzelnen Bereiche miteinander kooperieren.

Foto: Bundesheer/Dion6

Die Mitmachstationen, wie zum Beispiel das Testgelände der Nachtsichtgeräte oder der Cyber-EscapeRoom sorgten für Anreize und Unterhaltung für Jung und Alt und waren während des gesamten Tages sehr gut besucht.

27. Oktober 2024: Leistungsschau Light

Dieses Jahr wurde das Programm der Leistungsschau auf den Sonntag ausgedehnt. Daher war die Themeninsel "Cyber, Forschung und Technik" weiterhin für Besucherinnen und Besucher geöffnet und bot erneut die Gelegenheit, sich in einem etwas entspannteren Ambiente zu informieren und die Unterhaltungs- und Schulungsangebote wahrzunehmen.

Foto: Bundesheer/Dion6

Lehrlingssporttage 2024 am TÜPL HOCHFILZEN

Von 29. Oktober bis 31. Oktober 2024 fanden die durch das HPA durchgeführten Lehrlingssporttage für alle Lehrlinge im Bundesheer am Truppenübungsplatz Hochfilzen statt.

Daran nahmen 170 Lehrlinge sowie bis zu 50 Lehrlingsbeauftrage des Bundesheeres aus ganz Österreich teil. Dabei soll die Attraktivität der Lehrlingsausbildung im ÖBH gesteigert und ein Kennenlernen und Netzwerken innerhalb der Lehrlinge gefördert werden. Die Direktion 6 - IKT und Cyber war mit dem Cyber-EscapeRoom vertreten.

Hier konnten die Lehrlinge ihre Cyber Awareness unter Beweis stellen und kleine Überraschungen gewinnen. Die Lehrlinge mussten in Teams zusammenarbeiten und sich den fordernden Cyber-Aufgaben stellen.

Foto: BMLV/HBF

Foto: BMLV/HBF

Foto: BMLV/HBF

Präsentation des Cyber-EscapeRooms beim Ausbildungszentrum CIR

Von 04. bis 06. November 2024 präsentierte InfoOps&opKomm den mobilen Cyber-EscapeRoom der Direktion 6 – IKT und Cyber im Ausbildungszentrum Cyber und Informationsraum (CIR) der Deutschen Bundeswehr (DBW) in der General-Fellgiebel-Kaserne in PÖCKING.

Im Zuge dieser Präsentation konnte ein vertiefender Einblick in die Funktionsweise und die Wirkung des EscapeRoom gegeben werden.

Daraus resultierte ein reger Informationsaustausch und die Absicht vonseiten der DBW, ähnliche Modelle zu bauen und diese mit den österreichischen Cyber-EscapeRoom zu verbinden.

Ziel ist es, ortsunabhängig beide Systeme gegeneinander antreten zu lassen und somit den Auftrag, Cyber Awareness in der Bevölkerung weiterzuentwickeln, weiter voranzutreiben und auszudehnen.

Foto: Bundesheer/Dion6

Tag der offenen Tür des Jägerbataillons 18 in ST. MICHAEL IN DER OBERSTEIERMARK

Am Freitag, den 08. November 2024, fand der Tag der offenen Tür des Jägerbataillons 18 in ST. MICHAEL IN DER OBERSTEIERMARK statt. Die LANDWEHR-Kaserne präsentierte viele Fahrzeuge und soldatisches Gerät. Vor allem die neu beschaffte Ausrüstung und das neue Erkennungsmerkmal der 7. Jägerbrigade, das beige Barett und das Abzeichen „JAGDKAMPF" standen im Fokus.

Foto: Bundesheer/Dion6

Die Direktion 6 – IKT und Cyber stellte den Cyber-EscapeRoom zur Schau. Die Möglichkeit, sein Cyber-Wissen auf die Probe zu stellen, wurde sowohl von den Kameradinnen und Kameraden des Jägerbataillon 18, als auch von den Besucherinnen und Besuchern genutzt.

IT Futures Wien

Am 15. und 16. November 2024 fand im Vienna Austria Center die IT Futures 24 statt.

Die IT Futures ist eine Gelegenheit für Unternehmen, talentierte IT-Expertinnen und IT-Experten zu finden, und für Jobsuchende, ihren beruflichen Horizont zu erweitern. Die Direktion – IKT und Cyber war gemeinsam mit dem HPA auf einem Stand vertreten und repräsentierte das Österreichische Bundesheer als attraktiven Arbeitgeber mit vielfältigen beruflichen Perspektiven, Ausbildungs- und Aufstiegsmöglichkeiten.

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Vor dem Austria Center standen die Cyber-EscapeRoom und die Besucher der Messe hatten die Möglichkeit, ihre Cyber Skills unter Beweis zu stellen. Diese Messe war eine tolle Möglichkeit, die Direktion 6 - IKT und Cyber als IT Arbeitsgeber bei Jobsuchenden der IT - Branche vorzustellen.

FutureConvent im Toscana Congress Gmunden

Am 13. November 2024 fand im Toscana Congress Center in GMUNDEN ein großer HTL-Event mit circa 1.000 Besucherinnen und Besuchern statt. Es wurden HTL-Schülerinnen und Schüler der dritten bis fünften Klassen aus OBERÖSTERREICH und SALZBURG eingeladen, um sich weiterzubilden und beruflich zu informieren.

Abschließend dankt das Team InfoOps&op-Komm allen teilnehmenden Soldatinnen und Soldaten, Zivilbediensteten sowie externen Partnern für die hervorragende Zusammenarbeit bei den zahlreichen öffentlichkeitswirksamen Veranstaltungen.

Foto: Bundesheer/Dion6

Nutzungsmanagement und Führungsunterstützung

Österreichische Offiziere als DACOS CJ6 im OHQ EUNAVFOR ASPIDES

Die anhaltende Bedrohung der Schifffahrt aus dem von der Huthi-Miliz kontrollierten westlichen Teil des Staates JEMEN - insbesondere im südlichen Roten Meer, im GOLF VON ADEN und in der dazwischen liegenden Meerenge BAB AL-MANDAB - führte mit Beginn am 19. Februar 2024 zur Implementierung einer weiteren EU-Marineoperation mit der Bezeichnung EUNAVFOR ASPIDES (altgriechisch: „Schilde") zur Wahrung der Freiheit der Schifffahrt im dortigen Raum.

Foto: Geleitschutz ziviler Frachtschiffe, EUNAVFOR/Media

Als OHQ wurde dazu das EL EUOHQ (Hellenic EU OHQ) in LARISSA bestimmt, in dem ab 11. März 2024 die Position des DACOS CJ6 durch ÖSTERREICH besetzt wurde. Auf ein Jahr begrenzt vorgesehen, hatten bis Februar 2025 drei österreichische Offiziere diese Funktion inne.

Eine neu ins Leben gerufenen Operation bietet naturgemäß interessante Möglichkeiten, sich gerade auch im Führungsgrundgebiet 6 in vielerlei Hinsicht einzubringen.

Die geringe Zeit, die zur Planung und Vorbereitung der Operation verfügbar war, forderte eine rasche Lösung zur Bereitstellung der erforderlichen Kommunikationsmöglichkeiten innerhalb der Operation und mit relevanten externen Stellen.

Foto: Geleitschutz ziviler Frachtschiffe, EUNAVFOR/Media

Insbesondere zum Austausch von bis zu EU SECRET klassifizierten Informationen musste ein ASPIDES Mission Network (AMN) von Grund auf entwickelt und realisiert werden. In dieses sind zur Führung der Operation nicht nur das OHQ, ein Support Element vor Ort, sowie auf See das FHQ und alle weiteren beteiligten Schiffen eingebunden. Über das AMN wird auch der Kommunikationsbedarf mit anderen Kommanden und Organisationen, die im Operationsgebiet präsent sind (so auch EUNAVFOR ATALANTA und das Flottenkommando der Italienischen Marine), sowie mit Stellen zur Koordinierung des internationalen Seeverkehrs abgedeckt. Dieses Netzwerk erstreckt sich so von GRIECHENLAND aus über FRANKREICH, SPANIEN, ITALIEN, DSCHIBUTI bis BAHRAIN und die Schiffe der Operation auf See und deckt die Services VoIP, E-Mailing, Chat, VTC, File Server und Translation ab.

Foto: Geleitschutz ziviler Frachtschiffe, EUNAVFOR/Media

Da diese laufend wechseln, ist die Planung und Durchführung der Installation des Netzwerkes vor deren Eintreffen im Operationsgebiet bzw. dessen Deinstallation nach Verlassen der Operation eine permanente Aufgabe bei CJ6.

Ein wesentlicher Beitrag wurde auch zum Ausbaus der IKT-Infrastruktur im OHQ selbst geleistet. Die Hauptarbeitsumgebung im OHQ ist ein EU SECRET Netzwerk mit Verbindung in das EU Operations WAN. Eine ausreichende Bereitstellung von Internet-Rechnern zum Informationsaustausch insbesondere mit externen Stellen und Telefonen bedingte eine Erweiterung der IKT-Infrastruktur. Nach deren umfassender Neubeurteilung konnten im Herbst 2024 die dazu erforderlichen Arbeiten begonnen werden.

Regelmäßig wurde der Bedarf formuliert, im klassifizierten OHQ-Arbeitsnetzwerk Wörterbücher als Hilfestellung zur Übersetzung von Texten bereit zu stellen. Nach CJ6-interner Beurteilung von Möglichkeiten, gelang es ab Herbst 2024 sowohl in diesem, als auch im AMN eine Eigenentwicklung der CJ6-Abteilung zur maschinellen Übersetzung von Texten zwischen allen Sprachen der an der Operation teilnehmenden Nationen zu implementieren. Damit wird auch wirksam der Versuchung entgegnet, sensible Inhalte auch nur auszugsweise mittels funktionsgleicher Anwendungen im Internet zu übersetzen.

Zur Darstellung und Verfolgung des Schiffsverkehrs müssen bislang mehrere, verschiedene Services/Dienste genutzt werden, denen Daten unterschiedlicher Quellen zugrunde liegen. CJ6 erhob Möglichkeiten für ein Recognized Maritime Picture (RMP), in welchem relevante, auch klassifizierte Daten verschiedener Quellen implementiert und zusammengefasst werden können.

Durch CJ6 wurde initiiert, dazu das EDA-Projekt MARSUR III (MARSUR Networking - Operational Support and Development; MARSUR: Maritime Surveillance), welches diesen Bedarf künftig abdecken können soll, bei EUNAVFOR ASPIDES in einer Demo-Version vorzustellen und möglichst zeitnah im Einsatz zu testen. Nach noch erforderlichen vorbereitenden Maßnahmen seitens der Projektleitung, soll dies ab Frühjahr 2025 nunmehr für alle EUNAVFOR-Operationen realisiert werden.

Grafik: Übungsgebiet, wikipedia.org

Im Februar 2025 erfolgte dazu eine internationale Präsentation des Projektes beim OHQ EUNAVFOR MED IRINI in Rom.

Die Wahrnehmung der Funktion als DACOS CJ6 bei EUNAVFOR ASPIDES bot im Umfeld einer neu begonnenen Operation nicht nur generell umfangreiche Möglichkeiten, im Fachbereich und darüber hinaus wertvolle Erfahrungen zu sammeln. Insbesondere konnten dabei in wesentlichem und umfangreichem Ausmaß Ideen nicht nur eingebracht, sondern auch erfolgreich umgesetzt werden. Die erwähnten Lösungen für das ASPIDES Mission Network und das Hilfsmittel zur Übersetzung von Texten in klassifizierten Netzwerken werden künftig möglicherweise für bzw. in allen EU Einsätzen zur Anwendung kommen.

Foto: Geleitschutz ziviler Frachtschiffe, EUNAVFOR/Media

Foto: Bundesheer/Dion6

IKT und Cyber Plan

Leiter IKTCyPl: ObstdG Mag.(FH) Mag. Norbert KLEIN

Das Jahr 2024 war aus personal- und dienstrechtlicher Sicht durch die Einnahme des Organisationsplanes IKTCyPl mit Wirkung vom 1.10.2024 geprägt. Vorgestaffelt mussten im Frühjahr und Sommer 2024 die Arbeitsplatzbeschreibungen mehrmals überarbeitet und vorgelegt werden. Über den Sommer erfolgten die Personalgespräche, die Einteilungen auf die neuen Arbeitsplätze und für manche Mitarbeiterinnen und Mitarbeiter die Bewerbungsverfahren. Dies war eine große Herausforderung für die Abteilungsleitung über die Sommermonate die Terminfristen einzuhalten und die seriöse Bearbeitung der Personaleinsatzpläne sicherzustellen, um die Wünsche aller Mitarbeiterinnen und Mitarbeiter erfüllen zu können. Aufgrund von Arbeitsplatzidentitäten und Wertigkeitserhalt ist eine Organisationsplanwahrheit noch nicht gegeben. Des weiteren mussten wir auch einige Mitarbeiterinnen und Mitarbeiter aus der Abteilung verabschieden, die in den wohlverdienten Ruhestand übergetreten sind oder sich im Wege einer Versetzung weiterentwickeln konnten. Leider konnten mangels Personal nicht alle Arbeitsplätze in der Abteilung besetzt werden. Dies wird eine wesentliche Aufgabe für das Folgejahr darstellen. Zumal die Bewertung der Arbeitsplätze durch das zuständige Ressort sehr gut ausgefallen sind. Die meisten Arbeitsplätze sind militärisch und setzen ein technisches Studium voraus.

Im Bereich der inhaltlichen Aufgaben, der Fähigkeitsentwicklung in der Domäne Cyber und Informationsumfeld, standen die Bearbeitungen zum Zielbild ÖBH 2032. Das Schwergewicht des Jahres 2024 stellten die Erstellung der Motivenberichte der Waffengattungen IKT-Truppe (Tr), EloKa-Tr und Cyber-Tr dar sowie der Motivenbericht des zentralen IT-Providers. Als querschnittliche Bearbeitungserfolge können die Erstellung der Vorhabensabsicht MEDIS (Medizinisches Informationssystem), das Konzept zum Informations- und Wissensmanagement, das Smartphone-Konzept oder die Materialstrukturapplikation hervorgehoben werden.

Auch im Bereich der (Miliz-)Experten im Militär konnten personelle Weiterentwicklungen verzeichnet werden. Die Honorierung der Leistungen dieser gipfelte in der Verleihung des Awards an einen langverdienten Mitarbeiter in der Miliz.


Foto: BMLV/HBF

Bei der Masse der Aufgaben wurde die Abteilung allerdings fremdgesteuert, durch die Vorhaben der Abteilung Strukturplanung beziehungsweise der Direktion Fähigkeiten- und Grundsatzplanung. Bei der Mitwirkung an den Wargames zur Entwicklung der Anforderungen zum Zielbild ÖBH 2032 war nicht nur umfassendes Fachwissen gefragt, sondern auch der querschnittliche Blick über den Tellerrand, um die Bedarfe der anderen Direktionen zu erfassen und in die eigenen Planungen aufnehmen zu können. Die Zusammenarbeit mit der Abteilung Strukturplanung erfolgte hervorragend, auch wenn uns die vielen eingeforderten Beiträge vor so manche terminliche Herausforderung stellten, da in der Abteilung IKTCyPl immer auf die selben Mitarbeiterinnen und Mitarbeiter mit ihrer Fachexpertise zugegriffen wurde. Im Wege der Fähigkeitsentwicklung galt es, so rasch als möglich die Planungsdokumente zu erstellen, um das reichlich vorhandene Budget ansprechen zu können und um einen sichtbaren Mehrwert in der Truppe generieren zu können.

Mit der selben Schlagzahl geht es nun weiter in das Folgejahr. Die Vorhaben werden immer konkreter. Die Abteilungsleitung steht vor der Herausforderung neues Personal zu lukrieren, die vorhandenen Mitarbeiterinnen und Mitarbeiter zu motivieren und die Fülle an Aufgaben zu koordinieren und abzuarbeiten. In Summe prägten die Bearbeitungen zum Zielbild ÖBH 2032 die Masse der Abteilung über das ganze Jahr hinweg. Der Ausblick auf 2025 stellt einen noch intensiveren Planungs- und Arbeitsaufwand dar, um die Weiterentwicklung in den Streitkräften sichtbar zur Wirkung bringen zu können.

Coalition Warrior Interoperability Exercise - CWIX 2024

Die CWIX 2024 war für AUT sehr erfolgreich, alle Übungsziele wurden erreicht. Besonders hervorzuheben ist die erstmalige Teilnahme von Milizexperten mit sehr gutem Feedback und wertvollen Beiträgen zum Lessons Learned Prozess. Es erfolgte auch ein Proof of Concept für einen Prototypen eines Messanger Dienstes, der das Matrix Protokoll verwenden kann.

Nach langer Wartezeit und vielen Interventionen wurde endlich der Zuschlag für die Beschaffung eines Battlefield Management System (BMS) und der neuen Führungsinformationssystem (FüIS) Software erteilt, deren Planung federführend im Referat 2 stattgefunden hat. Das ÖBH wird also nach abgeschlossener Implementierung unter Federführung der IKTS über ein modernes, interoperables Tool zur Unterstützung der Führungsprozesse von der Ebene Zug bis auf die strategische Führungsebene verfügen.

Medizinisches Informationssystem (MEDIS), Sicherheitszone Militärisches Gesundheitswesen im Dynamisch Gesicherten Militärnetz (DGMN) mit der Integration medizintechnischer Systeme

MEDIS" soll im Rahmen des Militärischen Gesundheitswesens folgende Aufgaben unterstützen und die Einhaltung nachstehender Vorgaben ermöglichen:

- Einhaltung der gesetzlichen Vorgaben in Frieden und Einsatz
  - Dokumentationspflicht gem. med. Organisations- u. Berufsgruppengesetze
  - Einhaltung datenschutzrechtlicher Vorgaben
  - Einbindung/Betrieb aller med./techn. IT-Systeme (31), Geräte, Modalitäten (RIS/PACS, LIS, CAT, EKG, CT, usw.)
- Unterstützung der Sanitätsversorgung bei der Einsatzvorbereitung und im Einsatz
- Kompatibilität mit zivilen Gesundheitsdienstleistern (Datenaustausch)
- Bearbeitung aller medizinischen Prozesse in einem System

Grafik: Bundesheer/Dion6

Die Systemarchitektur MEDIS ist auf möglichst hohe Ausfallsicherheit und Resilienz ausgelegt. Dies umfasst sowohl das IT-Service selbst als auch alle für die Sicherstellung des Betriebs erforderlichen Maßnahmen (z.B. Notstromversorgung der San-Einrichtungen mit deren Endgeräten). Ziel ist es sicherzustellen, dass jedes Militärspital (SanZ, FAmb) auch bei Ausfall aller Datenverbindungen die medizinische Versorgung vor Ort erfüllen kann.

Anfang 2016 wurde eine Vorhabensabsicht zur Einführung eines „Medizinischen Informationssystems - MEDIS" genehmigt, eine zeitnahe Umsetzung erfolgte jedoch nicht. Zwischenzeitlich wurde im Auftrag des damaligen Leiters der S III mit der „elektronischen Patientenverwaltung - ePAT" eine fachspezifische Eigenentwicklung beauftragt, welche seit 2023 flächendeckend in Österreich in allen medizinischen Einrichtungen (TaA, TaS, SanZ, FAmb) im Einsatz ist.

Seit 2023 erfolgte in enger Zusammenarbeit der Dion8, der Dion6 und der FAmb die Ausarbeitung eines Anforderungsdokuments zur Beschaffung eines handelsüblichen „Medizinischen Informationssystems - MEDIS" für die Leistungsbereiche 1 und 2-4 in militärischen medizinischen Einrichtungen.

Dieses soll in die eigens zum Schutz personenbezogener medizinischer Daten geschaffene „Sicherheitszone Militärisches Gesundheitswesen" im DGMN integriert werden, in welcher alle medizintechnischen IT-Services (Laborinformationssystem – LIS, Radiologeninformationssystem RIS/PACS, ...) und Geräte (Modalitäten) zusammengefasst betrieben werden.

„Sicherheitszone Militärisches Gesundheitswesen" – Zielarchitektur (Großformat)

Die für die medizinische Versorgung (Stellung, Truppenarzt, San-Zentren) erforderlichen personenbezogenen Daten werden über eine Schnittstelle aus der „Komponente Person" (Teilapplikation in PS-NT) importiert, relevante Informationen (Ergebnisdaten über diese Schnittstelle wieder an PS-NT (Stellung-NT, Eignungsprüfung - EPR, ...)) übergeben.

Parallel dazu erfolgte durch die Fahrzeuge, Geräte und persönliche Ausrüstung (FGP) die Erneuerung der medizintechnischen Geräte (Röntgen, Labor, Anästhesie, Muskelkraftstuhl, ...) und der erforderlichen Anwendungssoftware (RIS/PACS, CHA, ...), welche systemisch ebenso in die „Sicherheitszone Militärisches Gesundheitswesen" im DGMN integriert werden.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Damit können künftig die medizintechnischen Geräte an das MEDIS direkt angebunden und Daten automatisiert auf Basis von Standards (HL7, DICOM, Fire) ausgetauscht werden.

Weiters können die Themenbereiche der Fernbefundung, Telemedizin sowie der Datenaustausch mit externen Gesundheitsdienstleistern und zu externen IT-Systemen (Epidemologisches Meldesystem [EPISYS1], Impfregister, grüner Pass, ...) abgebildet werden.

Beschreibung MCDC

Die „Multinational Capability Development Campaign" (MCDC) ist ein multinationales Konzept- und Fähigkeitsentwicklungsprogramm mit dem Zweck, gemeinsam nichtmaterielle 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 (s.u.). Initiator sind die USA, diese stellen auch das Sekretariat und den Vorsitz, AUT ist seit 2007 Mitglied.

Teilnehmer MCDC:

AUS, AUT, BRA, CHE, CAN, COL, CZE, DEU, DNK, ESP, EUMS, FIN, FRA, GBR, HUN, ITA, JPN, KOR, NATO-ACT, NLD, NOR, POL, ROU, SWE, USA.

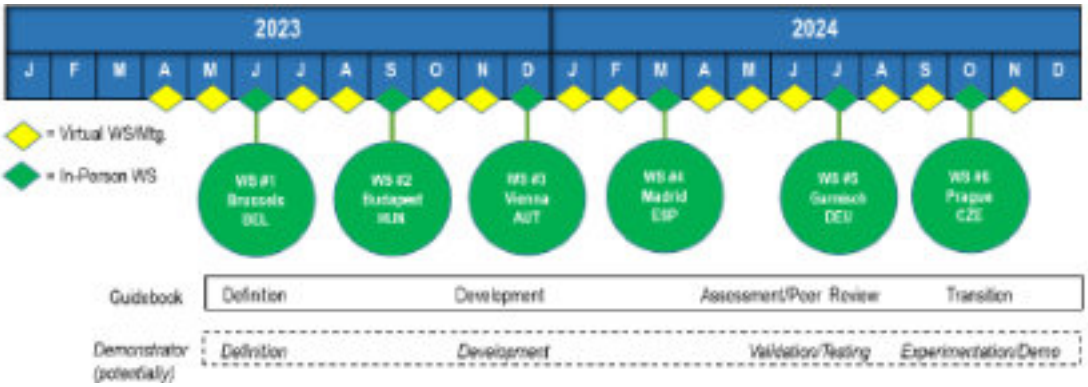
Eine Teilnahme an einem MCDC-Projekt kann entweder als „Contributor" (aktive Mitwirkung, wird grundsätzlich präferiert), als „Observer" (Beobachter, keine aktive Mitwirkung, somit Zugriff nur auf das Endprodukt eines Projektes) oder im Zuge einer Projektleitung (PL) erfolgen. Die Teilnahme an mindestens einem Projekt als „Contributor" ist erforderlich, um auch auf andere MCDC-Produkte (wie z. B. das „Military Uses of Artificial Intelligence, Automation & Robotics Guidebook" (MUAAR) aus der MCDC 2019/20 Campaign Guidebook") zugreifen und diese national verwerten zu können. Im Bereich der Arbeits- und Koordinierungsebene ist AUT, respektive das BMLV, durch einen „National Director" (ND) vertreten (derzeit Obst SCHULYOK, 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 BMLV: Bgdr MMag. DDr. STUPKA/MilStrat). AUT beteiligt sich am AI-ESF Projekt als „Contributor".

Nachstehend die Beschreibung der MCDC-Initiative aus dem „AI-ESF-Guidebook":

„The Multinational Capability Development Campaign (MCDC) is an initiative led by the United States Joint Staff (J-7) designed to develop and assess non-material (non-weaponry) force development solutions, through collaborative multinational efforts, to meet present and future operational needs associated with conducting joint multinational and coalition operations. It contributes to multinational interoperability by identifying and evaluating potential solutions to joint multinational and coalition capability gaps. MCDC focuses on multinational force development with a global community of interest made up of both traditional and non-traditional partners."

Grafik: MCDC, Deckblatt AI-ESF-Guidebook



Grafik: MCDC, AI-ESF Zeitleiste

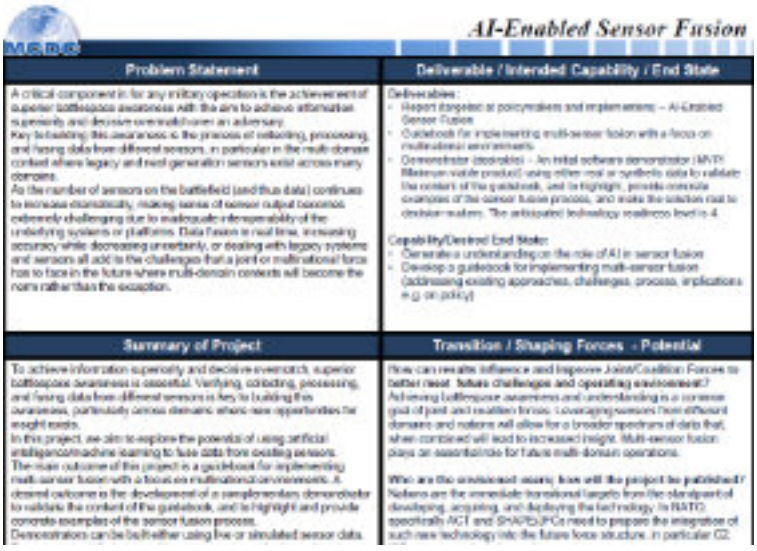
„The MCDC partner-centric development mode enables a broad range of multinational subject matter experts with diverse backgrounds and experience to aggregate and focus on multinational force development solutions. Each contributing member has the ability to invite representatives from their national networks of public, private, and academic institutions as well as functional expertise from other centers of excellence and communities of practice. This reach-back feature of the program is instrumental in producing innovative and non-traditional solutions."

Durchführung

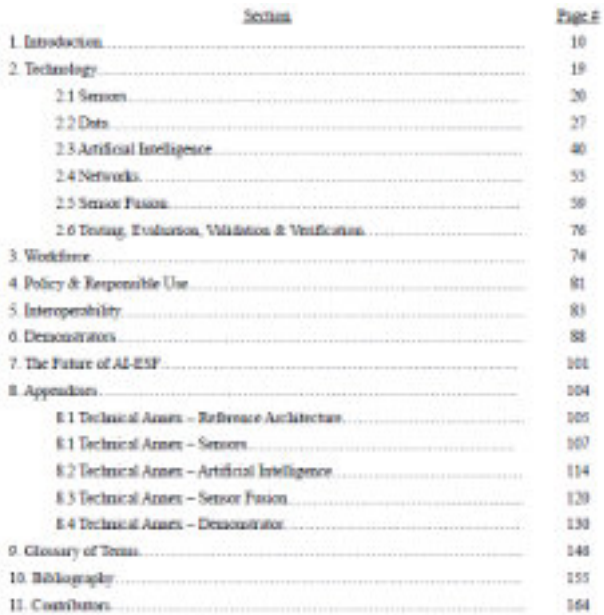
Die AI-ESF Workshop-Serie (in Summe insgesamt sechs „in-person-workshops", diese fanden im Zeitraum von Juli 2023 – Oktober 2024 ca. alle drei- bis vier Monate statt, zusätzlich war pro Monat ein virtuelles Treffen anberaumt; siehe Abbildung unten, „AI-ESF Project Timeline") hatte zum Ziel,

- dass das Kernprojektteam (NATO/ACT) und die Mitwirkenden, d.s. Beobachter und Fachexperten (SME) aus den teilnehmenden Nationen, gemeinsam Lösungen entwickeln,
- diese Ergebnisse, d.h. die Endprodukte gem. „Project Plan" (siehe Abb. 3) anschließend einem mehrstufigen „Peer-Review-Prozess" (intern und extern) unterziehen und
- diese ggf. im Rahmen eines „Confirmation Events" (z. B. CWIX25) validieren.

Das Endprodukt der AI-ESF WG - ein „Guidebook" (inkl. Demonstrator-Konzept; Gesamtumfang ca. 160 Seiten) - liegt Mitte Dezember 2024 in der Endfassung vor (Auszug aus dem Inhaltsverzeichnis des Final-Draft (siehe Abbildung unten)



Grafik: MCDC, AI-ESF Project Plan



Grafik: MCDC, Inhaltsverzeichnis AI-ESF-Guidebook

Kurzinfo zum AI-ESF-Projekt

Definition gem. AI-ESF Project Plan:

"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 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). Die Fusionierung – wie auch 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.

Zweck des Guidebooks (Auszug aus dem AI-ESF-Guidebook):

„This guidebook aims to provide readers with a fundamental understanding of AI's role in sensor fusion, including the technology involved, and to present the existing approaches, challenges, process, and policy involved in the implementation of AI-ESF. Furthermore, this guidebook emphasizes the role of multinational cooperation and provides multiple vignettes and use cases that highlight the application of AI-ESF in multinational contexts."

„The guidebook aims to inform military and political leaders, who need to understand how AI can fuse sensor data, with a view to implement it in military command and control capabilities. It is also intended for policy makers and strategist who need to understand the implications and operational benefits of AI-ESF. Operational and tactical planners will find it useful for understanding how AI-ESF can enhance decision-making and operational effectiveness. Additionally, educational and training staff can use the guidebook in support of creating AI literacy programs for military students".

Vorgehensweise bei der Erstellung des AI-ESF-Guidebooks (Auszug aus dem AI-ESF-Guidebook):

„The creation of this guidebook began with the formulation of the military problem, development of a project plan, and outlining the guidebook though a brainstorming session. Over two years, 18 participating MCDC nations assigned subject matter experts (SMEs), researched the subject matter using a wide range of sources, and developed the guidebook chapters through a series of workshops.

Thorough internal reviews refined the content for clarity and accuracy, followed by a rigorous review by peers from participating governments, academia, industry, and militaries. The peer review process provided diverse feedback which was carefully considered to finalize the guidebook."

Wichtigste Erkenntnisse aus der Teilnahme am AI-ESF -Projekt bzw. Empfehlungen:

Das Projekt wurde planmäßig gem. Projektplan und MCDC-Vorgaben innerhalb des zweijährigen Cycles abgeschlossen. Alle Projektziele wurden erreicht, ein Endprodukt liegt vor.

AUT hat an der AI-ESF-WS-Serie aktiv bei den Guidebook-Kapiteln „Workforce" und „Policy & Responsible Use" mitgearbeitet und war ff. bei der Ausarbeitung des Kapitels „Terminologie" bzw. „Glossary of Terms".

Die Mitarbeit von AUT im MCDC-Projekt AI-ESF war/ist (bzw. sollte) von großem Nutzen (sein)

- für die nationale Grundlagenarbeit im Themenbereich „AI/KI" (u.a. zur Auswertung/Interpretation von bereits vorhandenem internationalen Grundlagenmaterial, wie Strategien und Konzepten, welche zB die grundlegende Implementierung von AI in Organisationen beschreiben etc.),
- bei der Umsetzung der KI-Strategie des Ressorts,
- für die Vernetzung mit externen Wissensträgern,
- für den Wissensgewinn und Wissenstransfer.

Die Teilnehmer des BMLV/ÖBH konnten sich bei den Meetings aufgrund von Fachwissen in den Bereichen Computerlinguistik, Terminologie, Wissens- und Change-Management, Workforce sowie praktischer Erfahrung im Projektmanagement (PM) als Beitragsnation sehr gut einbringen. Die Zusammenarbeit innerhalb der WG war stets von Respekt, Kameradschaft und Wertschätzung geprägt.

Eine Teilnahme von AUT-Vertretern an AI-Folgeprojekten im nächsten MCDC-Cycle 2025/2026 wird empfohlen, da MCDC einen sehr guten Rahmen für die nationale Fähigkeitenentwicklung in unterschiedlichsten Bereichen bietet.

Erstmals Teilnahme von Miliz-Experten im Militär an der CWIX

Foto: Bundesheer/Dion6, CWIX-TN

2024 wurden erstmals Milizoffiziere zur NATO Übung CWIX (Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise) mitgenommen. Sie arbeiteten in verschiedenen Focus Areas im Joint Force Training Centre (NATO) in der Ortschaft BYDGOSZCZ/POLEN als auch in ÖSTERREICH. Zweck der Übung war die Verbesserung der Interoperabilität multinationaler technischer Systeme.

Hier ein Auszug aus dem der Erfahrungsbericht zur Interoperabilitätstestung technischer Systeme im Zeitraum vom 3. Juni 2024 bis einschließlich 21. Juni 2024.

„Über einen Zeitraum von drei Wochen wurde die Fähigkeit zur Zusammenarbeit in einem multinationalen Team in zwei Focus Areas (JISR Focus Area und FFT Focus Area) evaluiert und gestärkt.

Die CWIX 2024 hat gezeigt, dass technische und organisatorische Herausforderungen durch eine strukturierte Herangehensweise und effektive Kommunikation überwunden werden können. Zukünftige Übungen sollten auf diesen Erkenntnissen aufbauen, um die Interoperabilität weiter zu stärken.

Meine Tätigkeit als Analyst hat mir Einblicke in den Ablauf einer multinationalen Übung gewährt, die ich persönlich und auch für das österreichische Bundesheer als sehr positiv empfinde und zielführend für weitere Aktivitäten nutzen kann. Die bereits erlangten militärischen, organisatorischen Fähigkeiten und technische Kenntnisse haben dazu beigetragen, dass ich die gestellten Aufgaben erfüllen konnte und darüber hinaus auch Tätigkeiten durchführen konnte, welche Senior Analysten vorbehalten sind. Auftretende Probleme, wie beispielsweise die falsche Bedienung der Tools, welche zu 549 weiteren Testfällen innerhalb 24 Stunden geführt hat, konnten aufgrund der bekannten militärischen Problemlösungskompetenzen nun im multinationalen Umfeld umgesetzt werden. Die Lösung mit Hilfe von Koordination, Identifizierung, Varianten unterschiedlicher Lösungsansätze hat entscheidend zur Behebung des Problems, zur Akzeptanz der eigenen Person und zur Teambildung innerhalb der Focus Area beigetragen."

Miliz-Experten als Lehrpersonal und Lehrgangsentwickler am BaStG „MilIKTFü"

Foto: Bundesheer, SCHLOSSERN

Auch als wesentlichen Bestandteil zeigen sich einige unserer Miliz-Experten beim Bachelor Studiengang an der TherMilAk. Die Mitarbeit bereits während der Akkreditierungsphase und dann auch als Lehrpersonal und bei der inhaltlichen Erstellung der Curricula, sind einige unserer Miliz-Experten eine wesentliche Stütze für die Fachbereiche der Waffengattungen IKT und Cyber.

Aufbauend auf die Akzeptanzanalyse als Beitrag für die Entwicklung und Akkreditierung des FH-Bachelorstudienganges „MilIKTFü" (2020-2021) und die Ausgestaltung der Informatik Curricula des ersten Studienjahres, v.a. der Lehrveranstaltungen Programmieren I und II (2022-2023). 2023-2024 wurden im die Informatik Curricula des dritten bis fünften Semesters ausgestaltet, insbesonders die Lehrveranstaltungen Datenmanagement I und II mit insgesamt 195 Lehrveranstaltungsstunden pro Studienjahr. Damit ist auch eine enge Rückkopplung von der Planung bis zur Praxis des Unterrichts gewährleistet.

Naturgemäß werden an der TherMilAk Lehrende mit militärischem Hintergrund besonders gut angenommen, weshalb der Unterricht durch einen Milizoffizier als Experte im Militär eine besonders gelungene Synthese aus ziviler Expertise und militärischem Bezug darstellt. Der Unterricht wurde von den Fähnrichen auch entsprechend positiv bewertet.

Die Evaluierung der Bewerbungslage des FH-Bachelorstudienganges „MilIKTFü" (Jän/Feb 2023) sowie Beobachtungen und Impulse anhand der Teilnahme des ÖBH an der multinationalen NATO-Übung CWIX 2024 wurden ebenfalls für die Direktion 6 - IKT und Cyber erstellt.

Einsatz lohnt sich

Dieser unermüdliche Einsatz von Obstltd hmtD GÖSCHKA für die Ausbildung an der TherMilAk, für die Bereitschaft auch kurzfristig immer wieder in der Dion 6 zu unterstützen und die kompetente und erfolgreiche Unterstützung des AUT Team an der NATO-Übung CWIX 2024, haben zur Nominierung als Soldat des Jahres 2024 geführt – eine besondere Anerkennung und Würdigung stellvertretend für die Tätigkeit vieler Miliz-Experten im Militär der Dion 6.

Foto: BMLV/HBF

Befohlene Waffenübung (BWÜ) der Miliz-Experten 2024

Vom 18. bis 22. November 2024 fand planmäßig die BWÜ der Miliz-Experten mit 50 Teilnehmern, welche in den Expertenpools der Direktion 6 beordert sind, statt.

Zweck dieser BWÜ war die Mitarbeit der Miliz-Experten in den jeweiligen Fachbereichen auf Basis ihrer Expertisen, die weitere Optimierung der Zusammenarbeit Miliz und aktives Personal sowie die Erbringung von Laufbahnvoraussetzungen für die Milizexperten.

Das Ziel der BWÜ ergab sich in der Analogie der Fortsetzung des Zieles der BWÜ 2022, nämlich der Abstimmung und Zusammenführung der Bedarfe an Expertenwissen der unterschiedlichen Fachbereiche der Direktion 6 mit dem aktuellen Know-how der Miliz-Experten.

2022 wurde dazu ein sogenanntes „Skills Matching" zwischen Miliz-Experten und Aktivpersonal durchgeführt und dieses Mal wurde auf Basis des damaligen Ergebnisses der fachlichen Zuordnung direkt bei den Fachbereichen zu konkret gestellten Aufgaben gearbeitet.

Es hat sich bereits zwischen diesen beiden Übungen eine sehr gute und qualitativ hochwertige Zusammenarbeit zwischen Miliz-Experten und Fachbereiche weiterentwickelt, die mit der BWÜ´24 wesentlich optimiert werden konnte. Ein wesentlicher Aspekt dafür

ist, dass in den Fachbereichen konkrete gleichbleibende PoCs (Point of Contact) festgelegt sind, welcher als kompetente Ansprechpersonen in fachlicher Hinsicht für die Miliz-Experten fungieren. Dieser PoCs sind auch die Schnittstellen zwischen den Miliz-Experten, den Fachbereichen und der Leitstelle IKTCyPI.

Die BWÜs 2022 und 2024 sowie die gewachsene Zusammenarbeit zwischen Miliz-Experten, Fachbereichen und Leitstelle hat gezeigt, dass das System des Expertenwesens gerade in so spezialisierten Bereichen wie in der Direktion 6 funktioniert und damit einen wesentlichen Mehrwert für beide Seiten darstellt.

Das Expertenwesen ist ein „High Value Asset" - aber nur dann, wenn es fachlich kompetent, prozessual konsequent und in der Sache flexibel und innovativ genutzt wird.

Fähigkeitsentwicklung Materialstruktur

IT- Materialstruktur-Applikation

Mit der Fertigstellung des ersten Prototyps der „IT-MatStrukt-App" konnte im Dezember 2023 ein wesentlicher Meilenstein zur Digitalisierung der IT-Materialstruktur erreicht werden und dadurch auch die Ablöse der bisher genutzten „IT-MatStrukt-Tabelle" eingeleitet werden.

Foto: Bundesheer/Dion6, Das IT-MatStrukt-Team bei einem Workshop

Foto: Bundesheer/Dion6, Die Qualität der Applikation wurde verbessert

Im Laufe des Jahres 2024 konnte im Rahmen von zahlreichen Besprechungen und Workshops die Qualität und Nutzbarkeit der Applikation laufend verbessert werden. Durch die Verfügung von zahlreichen neuen Organisationsplänen (z.B. Direktionen 1–8) im Zuge der Strukturanpassung der Zentralstelle und Kommanden obere Führung, konnten Obst Löscher und sein Team wertvolle Erfahrungen bei der praktischen Arbeit mit der Applikation sammeln.

Zusätzlich wurde die App für einzelne, ausgewählte User im Ressort freigeschaltet, um so die Benutzertauglichkeit auch außerhalb der IKTCyPI im täglichen Dienstbetrieb testen zu können.

Als Konsequenz der intensiven Arbeit und der laufenden App-Optimierungen kann ab dem 1. Quartal 2025 die IT-MatStrukt-App offiziell für alle Bedarfsträger im Ressort freigeben werden.

Fähigkeitsentwicklung Cyber-Truppe

Planung zur Fähigkeitenentwicklung der Cyber-Truppe in Abstimmung mit dem Zielbild ÖBH2032, im Umfeld der Cyber-Kräfte zur Finalisierung des Motivenberichts Cyber-Truppe, ua in Workshops mit Stakeholdern der Dion6 im April in SEEBENSTEIN sowie mit StruktPI zur Abstimmung mit der Dokumentenlandschaft der Dion FäH&GSPI. Dies wird folgenden Strukturbedarf ergeben:

Foto: Bundesheer/Dion6

Teilnahme an der Conference on Cyber Conflicts (CYCON) in TALLINN/EST als nationaler Vertreter zum Steering Committee des Cooperative Cyber Defence Centre of Excellence (CCDCoE), mit dem Ziel aktuelle Bedrohungen und Lageentwicklungen im internationalen Umfeld zu erfassen und Grundlagendokumente in die Fähigkeitenentwicklung für die Cyber-Truppe einzubringen:

Foto: Bundesheer/Dion6

Teilnahme an der Übung SCHUTZSCHILD24 im FHQ/CJ6 als Stabsoffizier CyOps. Gesteuert wurde der Einsatz des Cyber Rapid Response Teams zur Abwehr eines Cyber-Angriffs im Übungsszenario am FHQ, die Verlegung des OrgE erfolgte per Hubschrauber-Transport in den Einsatzraum an der TherMilAk:

Teilnahme beim Kurs des European Security and Defence College (ESDC) „Contribution of Cyber in Hybrid Conflicts" am Hybrid Center of Excellence in HELSINKI/FIN. Ziel war das Schaffen des Verständnisses über das Wirken der Domäne Cyber in allen strategischen Dimensionen, gesteuert in einer TTX als Stabsspiel zur Simulation des Umfelds der EU:

Übung „COMMON ROOF 2024"

Vom 30.09.2024 bis 18.10.2024 fand die bereits siebte Ausgabe der trilateralen Übung „COMMON ROOF" statt. Diese Übung wird traditionell im DACH-Rahmen (Zusammenarbeit der IT-Truppen aus DEUTSCHLAND (D), ÖSTERREICH (A) und der SCHWEIZ (CH)) durchgeführt und stellt derzeit, zumindest für die österreichischen Teilnehmer, die einzige Möglichkeit einer Betriebsführungsübung im geplanten Übungsaufkommen dar.

Leitung und Austragungsorte

Im jährlichen Wechsel der Übungsleitung lag diese Verantwortung heuer bei DEUTSCHLAND, wobei der zentrale Übungsstandort beim Informationstechnikbataillon 293 (ITBtl 293) in MURNAU am Staffelsee in BAYERN disloziert war.

Der Standort dieses Bataillons bot optimale Rahmenbedingungen für die Durchführung der technisch und organisatorisch anspruchsvollen Betriebsführungsübung und für den Platzbedarf, den ein Einsatz eines Subordinated Service Management and Control Operations Element (SSE; heuer in Form einer verlegbaren Variante ausgebracht) und des Central Service Management and Control Operations Element (CSE; ortsfest in den Räumlichkeiten des Ausbildungs- und Testzentrums des Bataillons) erfordern.

Die beiden Standorte der SSE´s von ÖSTERREICH und der SCHWEIZ befanden sich beim FüUB1 in VILLACH und in einer Fernmeldeeinrichtung der Schweizer Armee nordöstlich von BERN in MURAIN.

Ziel und Szenario

Die COMMON ROOF ist als Betriebsführungsübung konzipiert, welche sich auf die

gemeinsame Planung, Errichtung und den Betrieb von Kommunikations- und Führungsunterstützungssystemen unter realitätsnahen Bedingungen konzentriert. Das diesjährige taktische Szenario sah ein Verzögerungsgefecht im Dreiländereck der drei beteiligten Staaten vor, welches die Übungsteilnehmer sowohl vor technische, organisatorische als auch betriebliche Herausforderungen stellte. Dieses robuste militärische Szenario wurde durch eine multinationale Betriebsführungsorganisation mit föderierten IT-Services unterstützt bzw. reali-

Foto: Bundesheer/SEDLMAIER

siert. ÖSTERREICH hat dazu unter anderem den Service „HF-Funk" für alle Partner bereitgestellt; diese Verbindungsrelation gilt als eine rasche und flexible Möglichkeit der Kommunikation – wurde aber sowohl aus taktischen wie technischen Besonderheiten (Einschränkungen) lediglich als Redundanz-Relation herangezogen. Ziel war es, die Interoperabilität der eingesetzten Systeme (gemäß Standards nach Federated Mission Networking [FMN]) und die – vor allem prozessuale –Zusammenarbeit der IT-Truppen weiter zu verbessern.

Übungsablauf

Im Rahmen der Übung wurden erforderliche IT-Services den sogenannten Role-Playern zur Umsetzung des „taktischen Spieles" im Sinne des definierten Szenarios bereitgestellt. Dabei war es trotz diverser Störungen (sowohl real als auch durch die Einlagensteuerung provoziert) erforderlich den durchgehenden IT-Betrieb für die Bedarfsträger aufrecht zu erhalten. Die durch die DACH-Arbeitsgruppen gemeinsam erarbeiteten und angewendeten Grundlagen und Dokumente konnten evaluiert und verbessert werden. Diese Erkenntnisse wurden und werden von FMN-Gremien dankbar entgegengenommen und fließen sowohl in die Bearbeitung von Standards im Rahmen des FMN-Spiral-Developments als auch in die nationale Fähigkeitenplanung ein.

Erkenntnisse und Fazit

Die Übung lieferte wertvolle Erkenntnisse zur Weiterentwicklung der betrieblichen und operativen Prozesse. Besonderer Fokus lag auf der Harmonisierung der IT-Servicebereitstellung und dem operativen Szenario (Bedarfsträger-Orientierung). Die trilaterale Zusammenarbeit (einschließlich der Fähigkeitenentwicklung) wurde durch die Übung weiter gestärkt und die jeweiligen Teilnehmer konnten von einem intensiven Erfahrungs- und Wissensaustausch profitieren. Bis zu einer Umsetzung von neuen Ausbildungsgrundlagen im nationalen Aus- und Weiterbildungsprogramm in der Waffengattung IKT (FüU) gilt diese Übung als eine der wenigen Möglichkeiten Personal in dieser Form der IT-Betriebsführung zu schulen. Die Übungsleitung in Deutschland erhielt im Rahmen des Distinguished Visitors Day (DVD) von unterschiedlichen Seiten sehr positives Feedback, was das hohe Engagement und die ausgeprägte Professionalität der Verantwortlichen unterstrich.

Durch die höchsten Repräsentanten der DACH-Nationen wurde der aktuelle DACH-Beschluss zur Fortführung der Kooperation unterzeichnet und für ÖSTERREICH die weitere Teilnahme nach kurzer Konsolidierung infolge der aktuellen Reorganisation ab dem Jahr 2026 fixiert.

Foto: Bundesheer/SEDLMAIER

Bundesministerium für Landesverteidigung

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

IKT und Cyber Einsatz

Leiter IKTCyE: Bgdr Mag. Arnold STAUDACHER

Die Verbände und Dienststellen der Direktion 6 können mit Stolz auf ein arbeitsintensives Jahr 2024 zurückblicken. Die Cyberkräfte haben sich in den In- und Auslandseinsätzen sowie bei über 30 nationalen und multinationalen Übungen und Vorhaben bewährt. Alle an sie gestellten Aufgaben konnten zur vollsten Zufriedenheit der Führung erfüllt werden.

„Mitten drin – und nicht nur dabei!"

Die Abteilung IKTCyE war bei allen diesen Aktivitäten stets „Mitten drin – und nicht nur dabei". Beispielhaft stellten bei den Auslandseinsätzen Offiziere der Abteilung gleich in 4 Missionen, bei EUFOR ALTHEA, IRINI und ASPIDES sowie bei KFOR wichtige Schlüsselpositionen.

In diesem Jahr war insbesondere das AUTCON UNIFIL aufgrund des Krieges im Nahen Osten stets im Fokus der Bearbeitungen. Die Abteilung war bei schwierigen Rahmenbedingungen ständig damit beschäftigt, die Verbindung des Kontingents nach AUT aufrecht zu erhalten und zu verbessern, was in einer gemeinsamen Kraftanstrengung auch gelang.

Fähigkeitsentwicklung – die Zukunft hat begonnen!

Mit Verfügung eines neuen Organisationsplanes für die Abteilung IKTCyE und deren Einnahme mit Anfang Oktober wurde ein wesentlicher struktureller Meilenstein in der Entwicklung von einem operativen Stabselement der Führungsunterstützung zu einem Führungselement einer eigenständigen Teilstreitkraft erreicht.


Foto: BMLV/HBF

Das Jahr 2024 wird auch als Jahr der Ablöse der IFMIN Technologie durch das neue Tactical Communications Network in die Geschichte der Cyberkräfte eingehen.

Die große Bewährungsprobe erfolgte bei der Übung „Schutzschild 24", wo das Gerät großflächig „im scharfen Schuss" zum Einsatz kam.

Zurecht hat das Einführungsteam TCN in diesem Jahr für ihre Leistungen von der Frau Bundesminister (FBM) einen „Special Award" erhalten.

Im Hinblick auf den Aufbauplan 2032+ hat also die Zukunft in der Direktion 6 mit der Einführung des TCN und mit dem Einsatz von modernem IKT-, und EloKa Gerät (KW Gerät Falcon 3, SATCOM Geräte, TCN, ERFOS Gerät) sowie auch von neuen Cyber Werkzeugen bereits begonnen.

„Im Hinblick auf den Aufbauplan 2032+ hat die Zukunft in der Direktion 6 mit der Einführung des TCN und mit dem Einsatz von modernem IKT-, und EloKa Gerät (KW Gerät Falcon 3, SATCOM Geräte, TCN, ERFOS Gerät) sowie auch von neuen Cyber Werkzeugen bereits begonnen."

Großveranstaltung AIRPOWER24

Im Zeitraum vom 06 09 2024 bis 07 09 2024 fand die Großveranstaltung AIRPOWER24, mit der wehrpolitischen Kernbotschaft „Unsere Luftstreitkräfte – WIR SCHÜTZEN ÖSTERREICH" in Abstimmung auf das Motto „AIRPOWER24 – FLIEGEN.FREIHEIT.BEGEISTERUNG" am Fliegerhorst HINTERSTOISSER in ZELTWEG statt.

Zur Sicherstellung der Führungsunterstützung war in der Projektorganisation AIRPOWER das OrgEt Teilprojektgruppe 6 (TPG6) unter der Leitung IKTCyE abgebildet.

Der Auftrag der TPG6 war es, die uneingeschränkte Führungsfähigkeit der Projektorganisation im Zuge der Vorbereitung, Durchführung und Nachbereitung in den Bereichen

- Informationsmanagement
- Informationsübertragung
- Informationsverarbeitung
- IKT-Sicherheit
- EloKa (Überwachung des elektromagnetischen Spektrums) und
- Militärgeographie

sicherzustellen.

Die TPG6 wurde aus FüU Teilen der Dion1, Dion2, Dion4, Dion6, AbwA, BMK und BMI gebildet und durch zivile Firmen wie TETRON (Funküberwachung) und A1 Event Solution unterstützt.

Foto: BMLV/HBF, Teile TPG6

Grafik: Bundesheer/Dion6, Bedarfsträger Gefechtsstand

In der Durchführungsphase (Aufbauphase vor Ort) wurde die TPG6 in eine A6 Zelle in der TaskForce (TF), eine FüUKp und EloKaKp/FüUB2 (als Teil des Interministeriellen Ortungsverbundes [IMOV]) gruppiert. Die Gesamtstärke der eingesetzten FüU-Kräfte betrug 150 Personen.

Der Auftrag der FüUKp war es, alle FüU-Maßnahmen für die TF sowie die Koordinierung mit den zivilen Mobilfunkbetreibern sowie den anderen Behörden und Einsatzorganisationen sicherzustellen und damit die TF/AP24 bei der Durchführung der Veranstaltung zu unterstützen.

Der IMOV überwachte das elektromagnetische Umfeld (EMU), setzte bei unrechtmäßiger oder sicherheitsgefährdender Nutzung des EMU die geeigneten Maßnahmen unter Abwendung der jeweiligen Befugnisse der beteiligten Dienststellen und trug so zum reibungslosen und sicheren Ablauf der Großveranstaltung bei.

Eine große Herausforderung stellte die Errichtung der IKT-Infrastruktur (ortsfest und verlegbar) am Fliegerhorst HINTERSTOISSER aufgrund der örtlichen Gegebenheiten sowie der unterschiedlichen Sicherheits- und Zutrittsbereiche dar.

Diese konnte nur aufgrund der professionellen Unterstützung aus den Bereichen IKT-Service GRAZ/KLAGENFURT und WIEN sichergestellt werden.

AIRPOWER24 STEIERMARK

Foto: Bundesheer/RedBull, AIRPOWER24

FüU/IKT Auslandskontingente

2024 war im Fachbereich stark durch Herausforderung der Aufbringung des benötigten Fachpersonals für die Kontingente AUTCON/KFOR (Austrian Contingent/Kosovo Force) und AUTCON EUFOR/ALTHEA (Austrian Contingent EU-Force/ALTHEA [Bosnien und Herzegowina]) geprägt. Um die Einsatzaufgaben des FGG6 zumindest eingeschränkt erfüllen zu können, mussten Schlüsselpositionen wie S6 und S6UO&LB phasenweise durch temporäre Entsendungen (max. 28 Tage) abgedeckt werden.

Bei AUTCON/UNIFIL (Austrian Contingent/United Nations Interim Force in Lebanon) im LIBANON wurden die Handlungsoptionen im Fachbereich stark von der äußerst angespannten Sicherheitslage beeinflusst bzw. eingeschränkt.

Trotz dieser herausfordernden Umfeldbedingungen wurden die erforderlichen Führungsverbindungen für die nationale Führung durch Direktion1/Abteilung operative Einsatzführung (Dion1/opEFü) sowie die Anbindung an das ortsfeste Fernmeldesystem des ÖBHs (ofFMSysÖBH) für die Abwicklung der Führungsaufgaben als auch die erforderlichen multinationalen Anbindungen an die jeweiligen Mission LAN durchgehend sichergestellt.

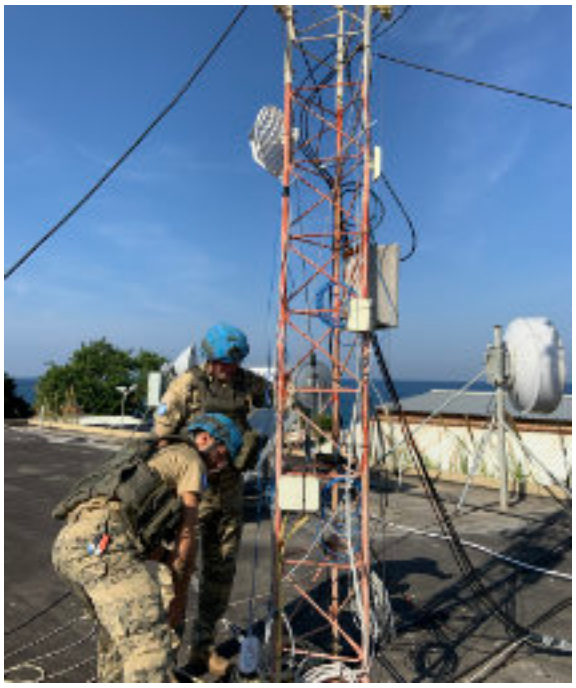


Foto: Bundesheer/Dion6, AUTCON/UNIFIL LIBANON

Trotz aller Einschränkungen konnten unter ff IKTCyE im Zusammenwirken mit IKTCyPl, IKTS, Experten IKT&CySihZ, der FüUS, den Abteilungen LogBstg, LogFü&Trsp der Dion 4, den FüUB 1 und 2, AuslEBa und den HLogZ G und K sowie den Abteilungen OpEPl, OpEFü und Budg&FinMngt/Dion1 die erforderlichen Routinen (Durchführung der jährlichen Wartungen und Adaptierungen der nationalen Verkabelungen in den von AUTCON/UNIFIL, AUTCON/EUFOR ALTHEA und AUTCON/KFOR Camps und den LOT und LMT-Häusern bei AUTCON/EUFOR ALTHEA und AUTCON/KFOR sowie die Durchführung der IKT Sicherheitsüberprüfungen bei AUTCON/EUFOR ALTHEA und AUTCON/KFOR) und die Masse der Vorhaben und Projekte abgearbeitet werden. Folgende IKT-Maßnahmen wurden bei allen 3 Großkontingenten im Jahr 2024 umgesetzt:

- Sicheres Militär Netz (SMN) Servertausch
- Erneuerung und Austausch sämtlicher A3 Drucker von RICOH 2504 auf RICOH 3010
- Anpassung und Modernisierung der Mobiltelefonausstattung
- Erkundung, Erhebung und Beantragung aller IKT-Komponenten sowie die Planung der für 2025 beabsichtigten TCN-Umstellung der AUT Auslandskontingente bei KFOR, EUFOR/ALTHEA und UNIFIL
- Zuweisung und Implementierung von NAS (Network Attached Storage) zu den LOT und LMT, FHT und AufklKp zur Datenarchivierung bei KFOR und EUFOR/ALTHEA.

Zusätzlich wurden auch missionsspezifische Herausforderungen, die sich auf Grund von Strukturanpassungen der Einsatzkontingente, Anpassung der Raumordnung in den Camps oder Anforderungen aus anderen Führungsgrundgebieten ergaben, im Sinne der Bedarfsträger erfolgreich umgesetzt.

Foto: Bundesheer/Dion6, AUTCON/UNIFIL LIBANON

Cyber Dokumentations- und Informationszentrum (CDIZ) in GRAZ

Das CDIZ GRAZ ist ein Element, das sich auf die Dokumentation und Strukturierung aktueller Cyberbedrohungen spezialisiert hat. Mittels OSINT (Open Source Intelligence) werden, nach Einweisung durch das Abwehramt (AbwA), Informationen im Internet gesammelt, strukturiert und zur Bewertung weitergegeben.

In Zusammenarbeit mit dem Cyber Dokumentations- und Forschungszentrum (CDFZ) Wien werden hier Lagebeiträge erstellt und umfassende Recherchen im Bereich der IKT-Sicherheit durchgeführt. Ein Schwerpunkt liegt dabei auf der Analyse aktueller Cyberbedrohungen.

Das CDIZ wurde mit 02/24 im Referat IKT-Sicherheit und Bedrohungslage Cyber (IKTSih&BedrLCy) als temporäres Projekt implementiert.

Das Team des CDIZ GRAZ setzt sich aus Grundwehrdienern und Chargen zusammen. Die Führung und Steuerung erfolgt durch das Referat IKTSih&BedrLCy.

Grafik: Bundesheer/Dion6

IKT-Sicherheit & Bedrohungslage Cyber (IKTSih&BedrLCy)

IKT-Sicherheitsüberprüfungen

Durch das Referat IKT-Sicherheit & Bedrohungslage Cyber (IKTSih&BedrLCy) werden regelmäßig IKT-Sicherheitsüberprüfungen der einsatzrelevanten IKT-Systeme und Services durchgeführt. Diese Überprüfungen dienen dazu, die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen, die für den Einsatz erforderlich sind, zu gewährleisten. Sie haben das Ziel, Schwachstellen, die eine Funktionsfähigkeit und die Sicherheit militärischer Einsätze gefährden könnten, in den IKT-Systemen und Services zu erkennen.

Die bei den Auslandsmissionen des Bundesheeres eingesetzten IKT-Systeme sind einer erhöhten Gefährdung ausgesetzt und müssen entsprechend engmaschig überprüft werden. Grundsätzlich findet dabei eine Überprüfung pro Einsatzkontingent statt, was am Balkan bei KFOR und EUFOR ALTHEA eine halbjährliche und im Nahen Osten bei UNIFIL eine jährliche Sicherheitsüberprüfung bedeuten.

Durch die IKT-Sicherheitsüberprüfungen im Ausland wird das Niveau der IKT-Sicherheit trotz häufiger Personalwechsel und technischer und organisatorischer Umstrukturierungen auf einem hohen Stand gehalten.

Foto: Bundesheer/Dion6

Notkommunikationsübung des ÖBH 2024: - Wir bereiten uns vor!

2024 fanden unter der Federführung des Referates Informationsübertragung (InfoÜ) der Abteilung IKTCyE/Dion6 zwei Notkommunikationsübungen statt.

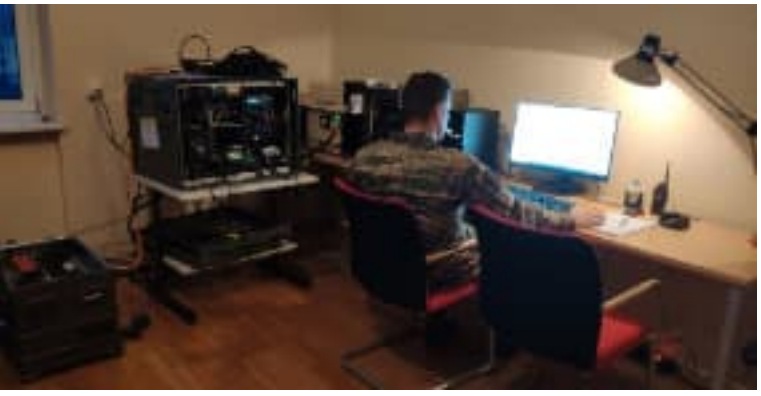


Foto: Bundesheer/Dion6

Als Übungsannahme wurde ein großflächiger Stromausfall in Europa (Blackout) angenommen. Es gibt viele Faktoren, die die Wahrscheinlichkeit für einen sogenannten Blackout erhöhen. Hierzu zählen die steigende Komplexität des Europäischen Verbundnetzes durch die voranschreitende Digitalisierung, klimawandelbedingte extreme Wetterlagen oder auch Cyberangriffe und Terrorismus.

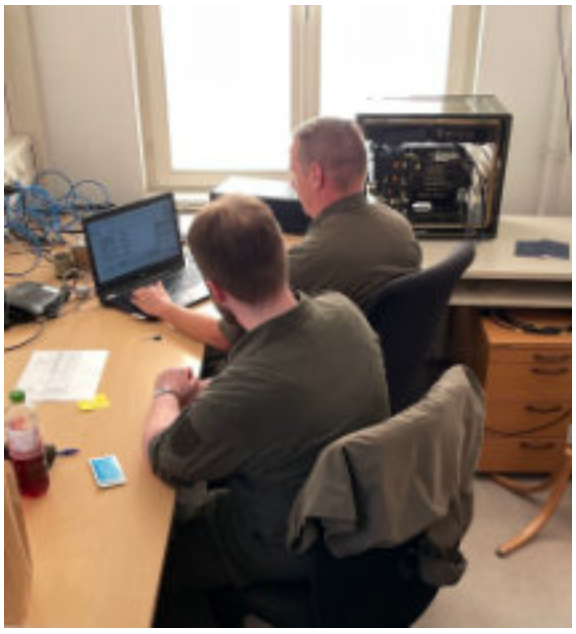


Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Um so wichtiger ist es, die Sicherstellung einer „Notkommunikation" vorzubereiten und auch praktisch immer wieder zu üben. Mehr als hundert IKT Soldaten und Bedienstete aller wesentlichen Verbände und Dienststellen des ÖBH beteiligten sich 2024 bei den österreichweiten Notkommunikationsübungen, errichteten autarke und datenfunkfähige Führungsnetze mittels Kurzwelle und Ultrakurzwelle und übten den Ernstfall unter realitätsnahen Bedingungen.

Zusätzlich wurden Satellitensysteme als Redundanz bei führenden Kommanden mit Erfolg eingesetzt.

Die vorhandenen Abläufe und festgelegten Prozesse zur Sicherstellung einer permanenten Notkommunikation im Anlassfall über mehrere Tage wurden überprüft, evaluiert und ständig verbessert. Einer autarken Stromversorgung aller führenden Kommanden sowie der Funktrupps kommt besondere Bedeutung zu. Die beiden Übungen brachten erneut wertvolle Erkenntnisse für die Sicherstellung einer stabilen Notkommunikation für das ÖBH und werden 2025 fortgesetzt.

Teilstreitkraft Cyber bei den Übungen SCHUTZSCHILD24/EURAD24

Die Durchführung der auf dem Szenario Schutzoperation basierenden bundesländerübergreifenden Großübung SCHUTZSCHILD 24 (NÖ, OÖ, ST und K) im Zeitraum von 10 06 24 bis 21 06 24 stellte nach fast eineinhalbjähriger Planungs- und Vorbereitungsphase den Höhepunkt der Übungstätigkeiten des ÖBH im Jahr 2024 dar. Parallel dazu fand die nationale Zertifizierungsübung des AUT-Anteiles an der European Battlegroup 2025 (EUBG2025), (CSS Baon mit einer FüUKp/KPE) im Großraum GÖTZENDORF - BRUCKNEUDORF statt.

Die handlungsleitende Trias der Dion6 - Connect. Protect. Inform. - fand im Grundauftrag an das abzustellende Stabselement (CyIDCE) beim (-)FHQ/LaSK ihren Niederschlag. Dieser beinhaltete neben der Gewährleistung der militärischen Handlungsfähigkeit in den Einsatzdomänen Cyber und Space sowie dem Informationsraum im Rahmen der Schutzoperation auch die Sicherstellung der ebenenbezogenen (IKT) Führungsfähigkeit sowohl für die Übungsleitung als auch teilweise für die übende Truppe.

Die Abt IKTCyE zeichnete sowohl für die Planung und Befehlsgebung des Einsatzes sämtlicher FüU Kräfte als auch für die Erarbeitung und Steuerung der Übungseinlagen im Cyber und Informationsraum sowie im elektromagnetischen Umfeld verantwortlich.

Grafik: Bundesheer/Dion6 (KI-Generiert), Captain Schutzschild

Zur Wahrnehmung der Aufgaben auf der operativen Ebene sowie im Rahmen der Übungsleitung wurde am Standort der TherMilAK in Wr.NEUSTADT ein Gefechtsstand der Übungsleitung gebildet und ein operativ führendes Kommando unter Leitung Dion1 und mit Beteiligung vieler Direktionen der GDLV und des ÖBH formiert. Die Führung der Cyber- und Informationskräfte, der EloKa Kräfte und der FüU Kräfte erfolgte dabei durch das unter ff IKTCyE gebildete Stabselement CyIDCE (Cyber&Information Domain Coordination Element) welches wiederum in die Bereiche J6/ HICON sowie EXCON/Cyber, EXCON EloKa und EXON InfoOps gegliedert war.

Die wesentlichen Leistungen der Dion6 können wie folgt zusammengefasst werden:

- Errichten und Betreiben des Führungs- und Informationsverbundes durch die Führungsunterstützungstruppe. Hierbei kam das brandneue Tactical Communication Network (TCN) erstmals in einem komplexen Umfeld zum Einsatz. Robuste, digitale Datenhighways haben die Sensoren, Gefechtsstände und Einsatzzentralen von der Kompanie bis zur Übungsleitung auf der operativen Ebene zu einem großen Aufklärungs- und Führungsnetzwerk verbunden.
- Bildung erforderlicher Redundanzen durch Bereitstellung von Alternativ- und Notkommunikationssystemen wie Satellitenkommunikation und datenfähigen Kurzwellenfunk (KuWel LaSK/ HARRIS).
- Überwachung des elektromagnetischen Spektrums, Erfassen, Aufzeichnen und Orten gegnerischer Funksignale durch den Einsatz der neuen Erfassungs- und Ortungssysteme (ERFOS) sowie Schutz der Einsatzkräfte vor funkferngezündeten Sprengfallen durch sogenannte Countering Radio Controlled Improvised Explosive Devices Electronic Warfare System (CREW Systeme).
- Einspielen von Übungseinlagen mit Bezug auf die IKT Sicherheit und auf Cyberangriffe zur Erhöhung der Cyber Awareness bei der übenden Truppe sowie erstmaliger übungsmäßiger Einsatz eines Cyber Rapid Response Teams inkl. Verlegung im Luftmarsch.

- Einspielen von Übungseinlagen zur Sensibilisierung der übenden Truppe hinsichtlich der Herausforderungen im Informationsraum (Fake News, Fake Videos) sowie hinsichtlich des Kampfes um das bessere Narrativ im Rahmen der hybriden Einsatzführung.

In Summe beteiligten sich fast 1000 Personen (ziv/mil) aus allen Verbänden und Dienststellen der Direktion6 an den beiden Übungen Schutzschild 24 und EURAD 24. Somit war jede(r) achte eingesetzte ÜbungsteilnehmerIn aus dem Wirkungsbereich der Cyber-Kräfte.

SCHUTZSCHILD24 bot die perfekten Rahmenbedingungen zur Erprobung neuer Prozesse bei der Erstellung eines domänenübergreifenden Lagebildes in einem FHQ, beim IKT Einsatz und der Bereitstellung von Einsatzservices einschließlich der erforderlichen Abstimmungen der IT Servicemanagement & Control Aufgaben mit den FüUBs und dem IKTBetr sowie bei der Integration der Fähigkeiten der Cyber-, EloKa- und Informationskräfte in die Gesamtplanung und Einsatzführung auf der operativen Ebene.

TCN-Betriebsübung im Rahmen von COMMON ROOF 24

Im Zeitraum von 14.10.2024 bis 18.10.2024 wurde eine Tactical Communications Network (TCN)-Betriebsübung im Rahmen der Übung COMMON ROOF 24 durchgeführt. Bei der durch IKTCyE geleiteten Übung mit Teilnahme durch 3.JgBrig, 4.PzGrenBrig, 7.JgBrig, FüUB1, FüUB2 und der FüUS wurde ein TCN mit 4 Teilnetzen und bis zu 25 TCN Vermittlungseinheiten errichtet.

Foto: BMLV/HBF

Foto: Bundesheer/Dion6

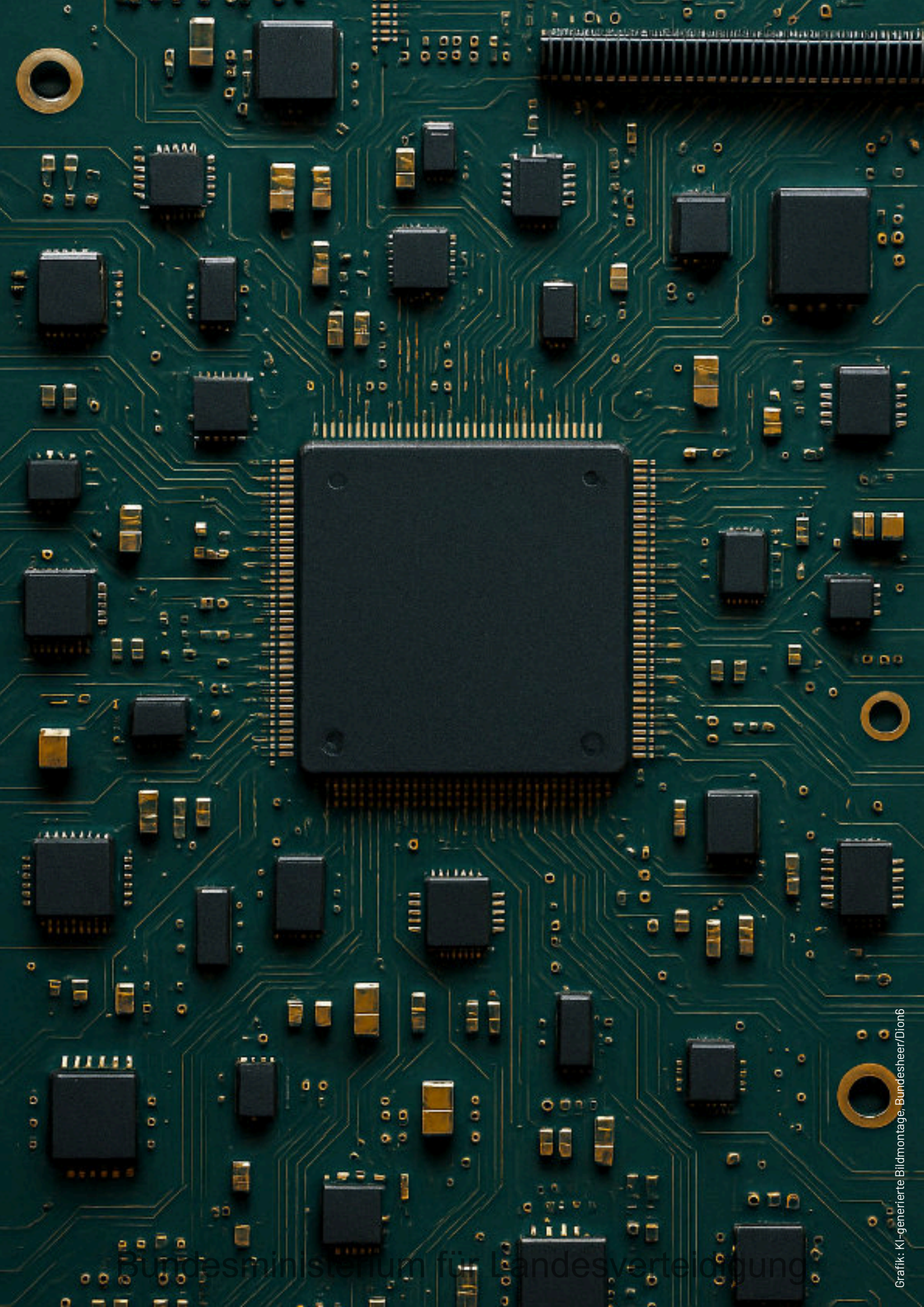
Dieses Netzwerk wurde durch ein Central Network Operation Center (CNOC) unter ff FüUB1, parallel zum AUT SSE (Subordinated Service Management&Control Operations Center) bei der Übung COMMON ROOF 24, gesteuert.

Folgende Ziele wurden mit der TCN-Betriebsübung verfolgt:

- Testung des im September 2024 durchgeführten Softwareupdates im TCN vor allem im Hinblick auf die bei der Übung SCHUTZSCHILD 24 gewonnenen Erkenntnisse in einem großen Netzwerk.
- Festigung des Betriebes im TCN für die Operatoren.
- Vorbereitung des TCN-Betriebspersonals der EUGB2025 auf die multinationale Übung EUROPEAN CHALLENGE 24 im November/Dezember 2024.
- Schulung und Einweisung der jeweiligen Stäbe in TCN.
- Die gleichzeitige Steuerung und Überwachung eines nationalen Netzwerks und eines multinationalen Netzwerks.

Das äußerst engagierte TCN-Betriebspersonal stellte in der Praxis fest, dass durch das Softwareupdate viele „Kinderkrankheiten" beseitigt wurden und TCN wesentlich stabiler funktioniert als vor dem Update. Weiters wurde festgestellt, dass sich die nationalen und internationalen Prozesse in der Steuerung eines Netzwerkes nicht wesentlich unterscheiden. Und die TCN-Operatoren konnten wertvolle Erfahrungen beim Betrieb des neuen TCN gewinnen.

Diese Betriebsübung wird zukünftig zumindest einmal jährlich durchgeführt, um einen entsprechend Einsatz nahen Belastungstest im Gesamtsystem TCN zu gewährleisten.



Bundesministerium für Landesverteidigung

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Budget und Personal

Leiterin Budg&Pers: ADir RgR Doris ZELEZNY

Nach Bekanntwerden der Rahmenbedingungen für die Aufstellung einer weiteren Abteilung in der Direktion 6 wurde der Schwung am Ende des ersten Quartals genützt, um die weiteren Bearbeitungen anzutreiben. Die Sicherstellung der Umsetzung der Reorganisation für die Direktion 6 in der Jahresmitte führte endlich zu einer ausreichenden Planungssicherheit im personellen Bereich.

Damit kann das Personal auch weitgehend dort eingesetzt werden, wo tatsächlich auch die Arbeitsaufgaben liegen. Mit dem Inkrafttreten und dem Abschluss der Reorganisation wurde auch dem Referat Budget & Personal in der Leitungsebene in einem sehr kurzen Takt Leben eingehaucht. Bereits während der Anlaufzeit mit einer erst teilweisen Besetzung des Referats war klar, dass noch eine große Vielzahl an Aufgaben bevorsteht.

Um die Personalführung zu fördern, wird es notwendig sein, weiterhin durch Schulungen und Workshops in die Mitarbeiterentwicklung großzügig zu investieren, weil damit auch die Motivation die Anpassungsfähigkeit an Veränderungen steigen. Anreize zur Anerkennung der Leistungen mit Belohnungen und Auszeichnungen sind nur ein Ausschnitt an weiteren Maßnahmen, die auch zukünftig entscheiden forciert werden müssen. Zu einem guten Personalmanagement gehören auch klare Zielorientierung und Maßnahmen zur Förderung des Teamgeistes.

Foto: BMLV/HBF

Wo sicher noch Luft nach oben herrscht, wäre ein optimiertes Bewerbermanagement-System, das dabei hilft, Bewerbungen professionell zu verwalten, den Auswahlprozess besser zu organisieren und die Kommunikation mit den Bewerbern zu optimieren.

Trotz nicht einfacher Entwicklung und der hohen Belastung der Leitungsebene wird auf einem sehr soliden Fundament im Personalstand aufgebaut, immerhin ist die Direktion 6 eine der wenigen im Ressort, die im laufenden Jahr personell markant dazugewonnen hat und diesen Weg auch konsequent weiterverfolgen muss. Für die Veränderungen und Ziele der Zukunft bedarf es auch enormer Anstrengungen, um weiterhin erfolgreich zu bleiben.

Grafik: Bundesheer/Dion6

Personal

Personelle Entwicklung der Direktionsleitung

Anfang 2024 musste sich die Direktion 6 weiterhin gedulden, was die Umsetzung der Reorganisation betraf. Die Einigung und zügige Umsetzung des Organisationsplans konnte in kurzen Etappen Anfang des 2. Quartals abgeschlossen werden. Damit konnte Mitte des Jahres endlich der langersehnte Prozess zur Überleitung gestartet werden. Mit leichter Verzögerung der Teile der Zentralstelle konnten aber die Einteilungen bis Ende Oktober fixiert werden. Mit Jahresende steht die Direktionsleitung insgesamt bei einem Besetzungsgrad von etwa 74%.

Personelle Entwicklung des IKT&Cybersicherheitszentrums

Die in der Struktur erhöhten SOLL-Arbeitsplätze in den technischen Bereichen wird mittlerweile in zwei Bereichen mit Leiharbeitern gerechnet übertroffen. Dafür sind die nach wie vor säumige Umsetzung der Erhöhung der Arbeitsplätze im Militärischen Cyberzentrum und die hohe Anzahl der Aufträge an die Applikationsentwicklung verantwortlich. Während der IKT-Betrieb gerade noch stabil bleibt, aber mit Nachwuchs zu kämpfen hat, erreicht die IKT - Technik mit dem tatsächlich verfügbaren Personal (inkl. Leiharbeiter) gerade knapp 85% und benötigt aber bei ständig steigender Tendenz an Bereitstellung von IT-Infrastruktur weiterhin konstante Personalgewinnung.

Mit zunehmender Tendenz zur Stärkung der Einsatzvorbereitung und Digitalisierung der Streitkräfte wird relativ schnell eine massive weitere Stärkung der Struktur notwendig sein, um die mittelfristigen Folgeziele mit personeller Kapazität erfolgreich abdecken zu können.

Zusammenfassend war 2024, was die Erfüllung der Personalziele beim Provider betrifft, durchwegs erfolgreich. So steht der Netto - Besetzungsgrad bei knapp über 80%, mit zusätzlichen Arbeitskräften (Leiharbeiter, Praktikanten, Chargen und Lehrlinge) gerechnet sogar bei 93,8%. Dieser Umstand wurde auch durch eine weitreichende Unterstützung der IKTS aus dem Budget der Leiharbeiter erreicht, sollte aber nicht darüber hinwegtäuschen, dass der zukünftige Bedarf für das Zielbild 2032 etwa 100% über dem aktuellen SOLL liegt!

Entwicklung der Schule und der Verbände

Die Führungsunterstützungsbataillone und Führungsunterstützungsschule konnten leicht zulegen, vor allem wenn auch die Kaderanwärter mitbetrachtet werden.

Budgetentwicklung in der Basisleistung

Trotz zusätzlich notwendiger Budgetierungen konnten 2024 insgesamt alle Ausgaben für Betrieb, Ausbildung und Repräsentation der Finanzstellen sowie für die Finanzierung des Handverlags für die Auslandsentsendungen mehr als ausreichend und zufriedenstellend bedeckt werden.

Der Bedarf für eine Budgetreserve wurde bereits zu Jahresbeginn erkannt und mit einer Budgetumschichtung im III. Quartal in die Wege geleitet.

Im Vergleich zu den letzten beiden Jahren konnte damit 2024 eine signifikante Erhöhung der Basisleistung um umgerechnet 0,3 Mio. erreicht werden. Damit wurde der wirklich hohe jährliche Bedarf zur Gänze erfüllt.

Im Bezug auf die Leistungen im Personal und Personal im Sachaufwand sind vor allem drei Komponenten erwähnenswert:

- Mehrverbrauch der gesamten Mehrdienstleistungen um 0,18 Mio. konnte gedeckt werden
- Bezüge und gesetzlicher Sozialaufwand allein überstiegen den BVA im Personal um 0,58%
- Ausgaben für Militärpersonen auf Zeit mit Fixbezug betrugen im Ausmaß knapp 224% des BVA

Im Finanzierungshaushalt für den betrieblichen Sachaufwand überstiegen die Ausgaben den Voranschlag um 18,43%.

Die tatsächlichen Ausgaben konnten durch zugewiesene Budgetreserven und mittels Umschichtung aus dem Personal im Sachaufwand aber sauber abgedeckt werden. Das war auch der sehr gediegenen Zusammenarbeit mit dem fachlichen Vertreter des Haushaltsleitenden Organs zu verdanken.

Die Rolle, Aufgaben und Perspektiven der (neuen) Frauenbeauftragten der Dion6

Seit Anfang September stehen der Dion6 IKT&Cyber (Dion6) mit OR Mag. Helene KAUTZ (Institut für Militärisches Geowesen, kurz IMG, rechtes Bild) und VB Marion JANSKY (IKT-Betrieb/Benutzerbetreuung, kurz BenBe, linkes Bild) zwei langjährige und erfahrene Mitarbeiterinnen des Ressorts, für das Ehrenamt als Frauenbeauftragte und Kontaktfrauen, offiziell zur Verfügung. Unsere Aufgabe ist es, allen Mitarbeiterinnen und Mitarbeitern der Dion6 als Ansprechpartnerinnen bzw. Vertrauensperson zur Verfügung zu stehen, wenn es sich am Arbeitsplatz um Diskriminierung auf Grund des Geschlechts oder sexuelles Fehlverhalten handelt.

Mit Stand 29.01.2025 betrug der Anteil an weiblichen Mitarbeitern in der Dion6 11,83%. Betrachtet man die letzten Jahre ergibt dies, unter anderem aufgrund des erfolgreichen Recruitings, eine leicht positive Tendenz.

Wirft man einen Blick auf die einzelnen Bereiche zeigt es, dass es vor allem bei der Truppe und in Bereichen, die sehr fachspezifisch geprägt sind, schwierig ist, weibliches Personal zu finden wohingegen Bereiche, die service- und supportorientiert sind leichter ist Mitarbeiterinnen für diese Arbeitsplätze zu begeistern.

Warum ist es nun so wichtig, dass für knapp 12% der Dienstnehmer in der Dion6 eigene Ansprechpartnerinnen eingesetzt werden und worauf begründet sich dieses Engagement seitens der Direktion?

Das BMLV und somit auch die Dion6 bekennt sich zu einer aktiven Gleichbehandlungs-politik im Sinne der Zielsetzungen des Bundes-Gleichbehandlungsgesetzes.

Das beinhaltet:

- die Gleichstellung von Männern und Frauen,
- sowie Frauenförderung und
- den Schutz vor Diskriminierungen in der Arbeitswelt aufgrund des Geschlechts, der ethnischen Zugehörigkeit, der Religion, der Weltanschauung, des Alters oder der sexuellen Orientierung

Als wesentliches Ziel der Frauenförderung im BMLV gilt es, den schrittweisen Abbau von bestehenden institutionell oder organisatorisch begründeten Ungleich-behandlungen von weiblichen Bediensteten zu forcieren sowie der Unterrepräsentanz von Frauen im Bundesdienst und Soldatinnen im Ressortbereich, entgegen zu wirken.

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Grafik: pixabay.com

IKT&Cybersicherheitszentrum

Leiter IKT&CySihZ: Bgdr Mag. Dr. Friedrich TEICHMANN, MAS MSc

Das IKT - und Cybersicherheitszentrum (IKT&CySihZ) hat 2024, wie auch die Jahre davor, seinen Auftrag unter dem Motto „Connect – Protect – Inform" voll erfüllt. Dieser Leitspruch reflektiert die schon bei den Vorgängerorganisationen (u.a. das FüUZ) dominanten drei Wirkungsbereichen, die das IKT&CySihZ für das Bundesheer, im Speziellen das Ressort, erfüllt bzw. besetzt.

Führung, ob analog mit Sprache, oder digital über ein COP (Common Operational Picture) kombiniert mit diversen Informationssystemen (z.B. FüIS) verlangt eine sichere und verlässliche Kommunikation bzw. Verbindung. Diese Kernleistung „Connect" des IKT&CySihZ wurde 2024 in verschiedensten Übungen, Einsatzvorbereitungen und bei Einsätzen (auch im Ausland) fortwährend abgerufen: Sprachkommunikation über verschiedenste Netze (u.a. GSM, VHF, KW, RF, Sat), digitale Kommunikation aller Mitarbeiterinnen und Mitarbeiter über ein flächendeckendes Mail-Termin-Management im Ressort, Vernetzung bzw. Datenaustausch der verschiedensten Informationssysteme (z.B. PERSIS, LOGIS, ORGIS, ELAK) und als Basis der Betrieb der Router, Server und Datenbanken, um diese Vernetzung permanent zu ermöglichen (siehe u.a. Leistungsbereich IKT-Betrieb sowie IKT-Te und Appl). Diese Fähigkeit, Daten und Vernetzung, des IKT&CySihZ ist aber nicht auf den militärischen Einsatz beschränkt, sondern wird auch zu einem hohen Grad als Basisleistung für den Betrieb bzw. den Regeldienst im BMLV/ÖBH benötigt und damit trägt das IKT&CySihZ einen wesentlichen Beitrag für einen funktionierenden Dienstbetrieb bei.

„Protect" hatte 2024 für das IKT&CySihZ zwei besonders wichtige Säulen: Einerseits den Schutz der ressorteigenen IKT-Infrastruktur (insbesondere Server und Netze) gegen gezielte Angriffe, d.h. IKT-Sicherheit bzw. Cyber-Operation, aber auch gegen allgemeine Bedrohungen, die die kontinuierliche Vernetzung/Kommunikation unterbinden könnten, d.h. u.a. organisatorische Maßnahmen. Auf Grund der besonderen Sicherheitsanforderungen des Ressorts, speziell durch klassifizierte Daten oder eingeschränkte Services, auch im internationalen Verbund, ist der Schutz der Daten im Ressort eine zentrale Aufgabe des IKT&CySihZ.


Foto: BMLV/HBF

Die CIA-Triade „Confidentiality, Integrity, and Availability" verlangte dem IKT&CySihZ 2024 alle verfügbaren Kräfte ab (siehe insbesondere der Leistungsbereich CyberZentrum), konnte aber für das Ressort bravourös bewältigt werden: durchgehende Vernetzung, kein Datenverlust, keine nicht-autorisierte Datenveränderung, kein „data-breach".

Die letzten Jahre haben das Potential von „Information" bzw. die Gefahr durch Desinformation („fake news") in der Gesellschaft klar aufgezeigt. Das IKT&CySihZ hat mehrere Elemente, die dem Motto „Inform" zugeordnet werden, wie z.B. Eloka (wer ist wie im Elektro-Magnetischen Spektrum aktiv), MilGeo (Landesbeschreibungen, „cultural awareness", Satelliten-Bilder) oder der Cyber-Bereich (Aktivitäten bzw. zentrale Akteure in der Cyber-Domäne). Ohne ein korrektes Lagebild keine Führung, und dazu sind sichere/richtige Informationen die Grundlage. Die Experten des IKT&CySihZ (insbesondere IMG und CyberZentrum) liefern diese verifizierten Informationen und leisten damit einen signifikanten Beitrag für die kritischen Entscheidungsfindungen im Ressort.

Trotz aller Herausforderungen, wie der kontinuierliche Technologiewandel, neue Services oder Erweiterungen im IKT bzw. Service-Bereich auf Grund neuer Plattformen oder Systeme, Ressourcenengpässe (insbesondere Personal und Infrastruktur), aber auch Anpassungen durch die ReOrganisation des zu bedienenden BMLV/ÖBH kann das IKT&CySihZ als der interne Service-Provider auf ein erfolgreiches Jahr 2024 zurückblicken.


Foto: BMLV/HBF

Führungsabteilung

seit 01.10.2024 mit der Führung betraut:
HR Rene GÜNTHER, BA MA

Im Jahr 2024 wurde die Direktion 6 durch eine bedeutende Umgliederung und Neuausrichtung geprägt. Am 1. Oktober 2024 wurde die Führungsabteilung des IKT- und Cybersicherheitszentrums aus der Direktion 6 – IKT und Cyber herausgelöst und wieder dem IKT- und Cybersicherheitszentrum eingegliedert. Diese Veränderung hatte weitreichende organisatorische Auswirkungen, da die Führungsabteilung nun eine zentrale Koordinierungsstelle innerhalb der Direktion 6 übernehmen musste.

Da die Direktion 6 über keine eigene Stabsstruktur verfügt, ist die Führungsabteilung nun für die Bearbeitung von Geschäftsfällen sowie die Koordination der verschiedenen Aufgaben der Führungsgrundgebiete 1 bis 6 und Budgetangelegenheiten der haushaltsführenden Stelle zuständig.

Ein weiteres Ziel ist die Neuausrichtung der Führungsabteilung durch die Schaffung neuer Arbeitsplätze und deren Besetzung, um die Direktion 6 - IKT und Cyber sowie das IKT&CySihZ effektiv zu unterstützen. Dies stellt eine bedeutende Herausforderung dar, da die Struktur an die wachsenden Anforderungen angepasst werden muss, um den dynamischen Veränderungen gerecht zu werden.

Personalverwaltung

Im vergangenen Jahr lag der Fokus der Personalverwaltung zweifellos auf der Reorganisation der Dion6. Im Rahmen dieser Umstrukturierung wurde die Dion6 in zwei separate Einheiten aufgespalten: Dion6 und IKT&CySihZ.

Eine der zentralen Herausforderungen dieser Umstellung war die erhebliche Erhöhung der zu verwaltenden Personalressourcen.

Diese Veränderung konnte jedoch erfolgreich bewältigt werden, indem gezielt Unterstützung durch neue Teammitglieder gewonnen wurde. So wurden zwei Praktikantinnen aufgenommen, die maßgeblich dazu beitrugen, die administrativen Aufgaben zu stemmen. Zudem konnte Ende des Jahres eine Referentin für den Bereich IKT&CySihZ gewonnen werden, was die Personalabteilung weiter stärkte und die Effizienz in der Verwaltung erheblich steigerte.

Besonders hervorzuheben ist, dass im Jahr 2024 eine große Anzahl an AÜG-Mitarbeiterinnen und AÜG-Mitarbeiter (Mitarbeiterinnen und Mitarbeiter nach dem Arbeitsüberlassungsgesetz) aufgenommen werden konnten. In Summe wurden mehr als 40 AÜG- Mitarbeiter für dieses Jahr erfasst.

Des Weiteren schaffte man es, nach erfolgreicher Einarbeitung und Leistung, insgesamt 32 AÜG-Mitarbeiter in den internen Dienststand zu übernehmen. Dank dieser gezielten Maßnahmen konnte die Personalverwaltung trotz der zusätzlichen Herausforderungen durch die Reorganisation einen erfolgreichen Verlauf im Jahr 2024 verzeichnen.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Militärische Sicherheit

Im Jahr 2024 führten nahezu 100% der Bediensteten die IKT-Sicherheitsbelehrung im internen Lernprogramm SITOS durch. Die jährliche Belehrung zur militärischen Sicherheit wurde, wie in der Vergangenheit, in Form eines Handouts zur nachweislichen Kenntnisnahme bereitgestellt.

Ein wesentlicher Schwerpunkt der Tätigkeit im Referat militärische Sicherheit lag bei der Bearbeitung/ Einleitung von Verlässlichkeitsprüfungen. Es wurden 200 Prüfungen eingeleitet und an die zuständigen Militärkommanden bzw. an das Abwehramt zur Durchführung übermittelt. Jährlich werden ca. 200 Geheimschutzverpflichtungen mit den Mitarbeiterinnen und Mitarbeitern bzw. externen Personal durchgeführt.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Durch den stetigen Aufwuchs kam es zur Bearbeitung und Verwaltung von etwa 40 Dauerpassierkartenanträgen im Jahr 2024 welche anschließend den neuen Mitarbeiterinnen und Mitarbeitern ausgehändigt wurden. Durch das Vorzeigen der Karte beim Sicherheitsdienst ist ein Zutritt in die militärischen Liegenschaften für den Inhaber möglich.

Das Referat militärische Sicherheit unterstützt die Schlüsselverantwortlichen und Schlüsselbearbeiter bei der Einhaltung der Schlüsselordnung um einen Zutritt von unbefugten Personen zu verhindern. Bei den präventiv durchgeführten Suchtmittelüberprüfungen, die mit Unterstützung durch das MilKdoW bzw. dem BMI stattgefunden haben, gab es erfreulicherweise keine Beanstandungen.

Grafik: Bundesheer/Dion6, Aufgabenfelder Militärische Sicherheit

Darüber hinaus wurden etwa 50 Security Clearances bei der zuständigen Fachabteilung beantragt. Bei 20 Firmen wurde eine Firmenüberprüfung eingeleitet um die Voraussetzungen einer Zusammenarbeit sicherzustellen.

Im Zuge der Sicherheits-/Schließkontrolle wurden Mängel mit den jeweilig Verantwortlichen besprochen um die Awareness im Bereich der militärischen Sicherheit zu erhöhen.

Das 4. Quartal 2024 war, durch die Bearbeitung und Genehmigung von Zutrittsanträgen für das Folgejahr, geprägt. Dies umfasst in etwa 8000 Buchungszeilen die im System administriert werden müssen.

Im Laufe des Jahres wurden ca. 50 interne Vorfälle im Referat aufgearbeitet. Ein Schwergewicht ist es, die Awareness bzgl. militärischer Sicherheit der Bediensteten zu erhöhen. Daraus resultierend wurden Kaderfortbildungen für die eingeteilten Sicherheitsbeauftragten und für die Bediensteten der Direktion 6 durchgeführt.

Die militärische Sicherheit ist kein Selbstzweck!

10 Grundregeln für die militärische Sicherheit

- Seien Sie verschwiegen!
- Seien Sie misstrauisch!
- Achten Sie auf Anvertrautes!
- Seien Sie aufmerksam, wachsam und kritisch!
- Halten Sie Maß!
- Seien Sie ein positives Vorbild!
- Geben Sie eigene Fehler zu!
- Melden Sie nachrichtendienstliche Verdachtsmomente und Druck!
- Benutzen Sie Ihren Hausverstand!
- Halten Sie sich an die Regeln der militärischen Sicherheit!

Grafik: pexels.com

Logistik & Infrastruktur & Hausherr

Im Zuge des Jahres 2024 wurden in der Logistik, abgebildet als Referat Versorgung seit 01 01 24 in der FüAbt IKT&CySihZ, in der Optimierung der Logistikprozesse und der Zusammenarbeit mit den Bereichen IKT&-CySihZ deutliche Verbesserungen generiert. Das Ziel, für jeden Bereich logistisches Fachpersonal bereitzustellen, konnte durch konsequente Rekrutierung von Kader aus anderen Verbänden und Gewinnung von interessierten Soldaten aus dem Rekrutenpool erfüllt werden.

Mittlerweile ermöglicht die Kaderstärke auch ein Generieren von Kader für andere Fachgebiete wie Wirtschaft, Kraftfahrwesen und IT. Seit 2020 wurden 19 neue Mitarbeiterinnen und Mitarbeiter und Kader für die Dion6 und das IKT&CySihZ gewonnen.

Neben dem logistischen Tagesgeschäft wurden Anstrengung zur Implementierung des Kraftfahrwesens (KFW) im IKT&CySihZ unternommen, um auch in diesem Bereich mit 170 Heeresführerschein (HFS)-Besitzern, 23 Kfz, der neuen Aufgabe Escape Room mit LKW und Hängergespann und Ausbilden von HKf aus jedem ET, selbständig agieren zu können.

Im Bereich Infrastruktur konnten bescheidene Erfolge erzielt werden, wonach die FüAbt in das Obj 4 Suppeurtrakt zusammengeführt wurde und somit den Bereichen mehr Raum zugestanden werden konnte. Das Raum und Funktionsprogramm für den Umbau STÖCKELTRAKT mit Ausblick auf ÖBH2032+ wurde mit den Bereichen erfolgreich erstellt und der Dion7 übermittelt.

Aufgrund RIVIT und der schwächelnden Wirtschaft erfolgte ein Aufnahmeboom von IKT Spezialisten, das eine Raum/Büro Knappheit zur Folge hatte und eine Ersatzinfrastruktur in Form von Containerbauten mit Anbindung an das Obj6 bedarf. Eine Waffenkammer und Munitionsbunkeranlage wurden eingepreist und, aufgrund des Bedarfes der Verfügbarkeit der Waffen und Munition bei diversen Bedrohungsstufen genehmigt.

Im Bereich der Infrastruktur von Nachgeordneten wird mit Nachdruck versucht Kasernenverkäufe zu verhindern, die Infrastruktur zu verbessern und Cyber Ranges zu implentieren. Für die Elektronikwerkstätten beim FüUB2 wurden zusätzliche Gelder bereitgestellt, das FüUB1 erhielt eine Leichtbauhalle für die EloWkst.

Die Aktivierung der Dienste als Hausherr zeichnete 2024 als erfolgreiches Projekt in Zusammenarbeit mit IKTBetr und milSih und umfasst die Überprüfung aller Fernmeldesystemräume in den Liegenschaften ÖBH. Die Überprüfung besteht aus Kontrolle des Zutritts über den OvT, die Funktionsfähigkeit, bauliche Sicherheit und Umsetzung der Präventivmaßnahmen in den Netzwerkräumen. 2024 erfolgte mit Schwergewicht das Bundesland NIEDERÖSTERREICH und WIEN.

Im Großen und Ganzen kann das Jahr 2024 erfolgreich für das Ref Vers angesehen werden.

Wirtschaftsverwaltung

Aufgrund der Aufnahmen neuer Mitarbeiterinnen und Mitarbeiter sowie eines notwendigen Austauschs abgelebter und unbrauchbar gewordener Büromöbel war es erforderlich, zusätzliches Budget für die Beschaffung neuer Büromöbel bereitzustellen. Die Bereitstellung und Nutzung der finanziellen Mittel erfolgte effizient und zielgerichtet, um den Betrieb aufrechtzuerhalten und notwendige Ressourcen für die Arbeitsfähigkeit sicherzustellen.

Grafik: KI-generierte Bildmontage, Bundesheer/Dio


Foto: BMLV/HBF

Applikationen

Leiter Appl:
HR Dipl.-Ing. Gerald HOFMEISTER

Der Bereich Applikationen im IKT&CySihZ zeichnet sich verantwortlich für die Bereitstellung, den Betrieb und die Weiterentwicklung von ca. 150 IT-Services für über 20.000 User in unterschiedlichen Kundennetzen und „Sicherheitszonen" im In- und Ausland aus.

Neben diesen Tätigkeiten lag das Schwergewicht bei der Erstellung wesentlicher Planungsdokumente für das IKTSystem ÖBH2032+ gemäß dem Aufbauplan 2032+ und dem Zielbild 2032 samt einer ersten Ressourcenabschätzung.

Weitere wesentliche Schwerpunkte wurden im Voranbringen der Digitalisierung im Verteidigungsressorts gesetzt.

Hervorzuheben sind die Vorarbeiten für die Beschaffung eines Battlefield Management Systems für die Landstreitkräfte, die Implementierung eines Fähigkeiteninformations-, planungs- und -steuerungssystems zur Unterstützung der Planungsaktivitäten in den zentralen Prozessen der Landesverteidigung sowie der Ausbau des eGovernment-Service „bundesheeronline" als zentrale Schnittstelle für Einbringen von Wehrpflichtigen im Rahmen des Stellungsprozesses.

Bauwesen-Applikationen

Schwerpunkt Interoperables Zutrittsmanagement (iZMS)

Innerhalb der Abteilung war im neuen Referat Objektsicherheits-Informationssyteme die Umsetzung des Pilotprojektes iZMS eines der Kernaufgaben. In dem Projekt geht es vor allem um folgende Punkte:

- Nutzung von Standards im Zutrittsbereich wie OSS-SO
- Implementierung von Schlössern unterschiedlichster Hersteller
- Ausbau der Nutzungsmöglichkeiten vor aktuellen RFID-Standards

Im Zuge des Pilotprojektes wurde durch den Anbieter erkannt und entschieden einen neuen Client zu entwickeln, damit einerseits die Anforderungen umgesetzt und andererseits für den Endnutzer ein geeignetes Werkzeug zur Verfügung gestellt werden kann.

Um die geforderten Funktionalitäten laufend zu testen, galt es ein entsprechendes Qualitätsmanagement zu entwickeln und zu implementieren. Dafür wurden die geforderten Funktionalitäten in Leistungsziele zusammengefasst und entsprechende „use cases" entwickelt.

Grafik: Bundesheer/Dion6

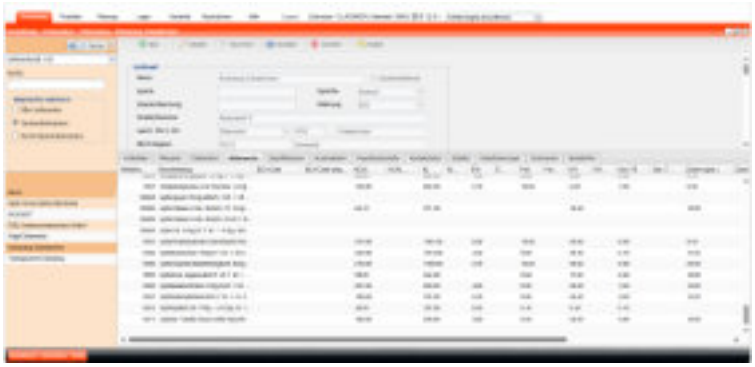
Küchenmanagementssystem (KMS)

Im Bereich des Küchenmanagements wurden durch die Abteilungen die Vorbereitungen für die Abnahme der neu beschafften Software necta und das Rollout auf weitere Standorte erfolgreich umgesetzt. Dabei galt es ua. die über 30 Jahre alte Software durch eine neue, den aktuellen Standards entsprechende SW-Lösungen zu ersetzen.

Nachdem in dem Projekt die Digitalisierung eine sehr große Rolle spielt, mussten ua. mit den Lieferanten die in der Branche üblichen Schnittstellen vorbereitet und implementiert werden.

Im Zuge des Rollouts konnte im Jahr 2024 die gesamte Regionalküche KLAGENFURT mit allen angeschlossen Finalisierungsküchen erfolgreich auf das neue zentrale KMSnecta umgestellt werden. Dabei mussten auch bestehende Küchengeräte und Verpackungsmaschinen in das System integriert werden.

Mit Ende 2024 wurde das weitere Rollout mit der Erhebung und den Vorbereitungen im Bereich Niederösterreich gestartet und soll 2025 umgesetzt werden.



Grafik: Bundesheer/Dion6

Ausbau Sicherheitszone militärisches Gesundheitswesen

Die im Bereich der Sicherheitszone militärisches Gesundheitswesen implementierten Services und Gerätschaften wurden im Jahr 2024 drastisch ausgebaut und integriert. Ein der Hauptaufgaben dabei war die Erhebung und Implementierung des Laborinformationssystems sowie der Röntgeninformationssysteme (RIS) und des Picture Archiving and Communication Systems (PACS) samt den dazugehörigen Geräten in den Stellungsstraßen des ÖBH.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Eines der Kernthemen, welches uns in den folgenden Jahren beschäftigen wird, ist die Beschaffung eines Medizinischen Informationssystems kurz „MEDIS“. Dabei handelt es sich um eine marktkonforme und dem Stand der Technik entsprechende Softwareplattform, welche sämtliche Anforderungen im Bereich der Medizin im ÖBH abdecken soll.

Vorbereitungen Entwicklung DGMN 2.0

Im Jahr 2024 starteten die Vorbereitungen zur (Weiter-)Entwicklung des dynamischen gesicherten Militärnetzes. Im Zuge der Umsetzung dieses Projektes soll neben der Nutzung von Synergien, Schnittstellen und dem vorhandenen „know how“ die bestehende und über Jahrzehnte weiterentwickelte Basis-Infrastruktur überarbeitet und auf neue Beine gestellt werden.

Grafik: Bundesheer/Dion6, Logo DGMN 2.0

Eines der Kernziele in dem Projekt ist ua. die Sicherheit weiter zu erhöhen und eine Multifaktor-Authentifizierung zu implementieren.

Einsatzapplikationen

Battlefield Management System & Führungsinformationssystem neu

Für die Abteilung Einsatzapplikationen stand das Jahr 2024 im Zeichen der ersten großen Schritte in Richtung der "Digitalisierung des Gefechtsfeldes" entsprechend den Zielen des Aufbauplans ÖBH 2032+.

Mit der nun vertraglich fixierten Beschaffung eines Battlefield Managment Systems (BMS) für die gesamten Landstreitkräfte erfolgt die Ablöse des veralteten Führungsinformationssystems (FüIS) PHÖNIX durch eine gemeinsame Software-Suite.

Diese besteht aus dem BMS "SitaWare Frontline" und dem FüIS "SitaWare Headquarters".

Damit werden die zentralen IT-Services eines ebenen- und waffengattungsübergreifenden Führungsverbundes realisiert.

PANDUR EVO

In engem Zusammenhang damit steht die ebenfalls 2024 finalisierte Beschaffung des "Radpanzers" Pandur Evo Batch 4. Beide großen Vorhaben sind auf das Engste miteinander verwoben, weil alle zwölf Varianten des Pandur Evo ebenso wie hinkünftig jedes andere geschützte Fahrzeug der Landstreitkräfte mit dem BMS ausgestattet werden. In vielen dieser Fahrzeuge sind Sensor- und Waffeneinsatzsysteme zu implementieren und mit dem BMS/FüIS in einem Verbund "Aufklärung-Führung-Wirkung" zusammenzuschließen. Ziel dieser technisch und organisatorisch herausfordernden Integration hochmobiler IKT-Services ist die militärisch unbedingt notwendige, deutliche Verkürzung der Dauer "Sensor to Shooter" und generell die Verbesserung der Lagebilder auf allen Führungsebenen.

Beobachtungs- und Aufklärungsausstattung

Neben den beiden neuen Großprojekten und der Betriebsunterstützung (Systemerhaltung und 2nd Level Support) für alle derzeit betriebenen Einsatzapplikationen - u. a. Datenfunksoftware, ABC-Informationssystem, Führungssimulator, Funknetzmanagementsystem, Friendly Force Tracking - wurde 2024 in Zusammenarbeit mit dem Amt für Rüstung und Wehrtechnik eine Güteprüfung des Aufklärungssystems BAA EO (Beobachtungs- und Aufklärungsausstattung elektro-optisch) am geschützten Mehrzweckfahrzeug Husar durchgeführt.

Foto: Bundesheer/Dion6

Combined Federated Battle Laboratories Network (CFBLNet)

Grafik: Bundesheer/Dion6, Logo CFBLNet

Die Interoperabilität von IKT-Services ist ebenfalls eine "conditio sine qua non" im Hinblick auf die Einsatzfähigkeit des Bundesheeres im internationalen Verbund. Das österreichische "Battle Lab" am Combined Federated Battle Laboratories Network (CFBLNet) war im abgelaufenen Jahr nahezu im Dauerbetrieb, um im Rahmen der Federated Mission Networking (FMN) Testarbeitsgruppe CIAV und der NATO-Großübung CWIX einsatzwichtige IKT-Services mit Partnernationen zu testen und zu zertifizieren. Da FMN ca. alle zwei Jahre eine neue, umfangreichere Version von IKT-Spezifikationen und prozessualen Vorgaben verabschiedet, sind Interoperabilitätstests und Zertifizierungen permanente Aufgabenstellungen, die durch das Referat Inteoperabiliäts- und Testzentrum bestmöglich für den gesamten Verantwortungsbereich der Direktion 6 unterstützt werden.

Grafik: CWIX, Logo

Informationsmanagement&Büroautomation

Schwerpunkt Einsatzorientierung

Ein wichtiger Schwerpunkt der Abteilung Informationsmanagement&Büroautomation war im Jahr 2024 die Einsatzorientierung betreffend die durch die Abteilung bereitgestellten Core-Services:

- Informal Messaging (Mail): eingesetztes Produkt HCL Domino/Notes
- Text Based Collaboration (Chat): Produkt in Evaluierung
- Web Hosting (CMS): Produkt Liferay CE
- Calendaring&Scheduling: eingesetzte Produkte HCL Domino/Notes, Liferay CE

Hierbei galt es die Kernanforderungen an die Einsatzorientierung umzusetzen:

- Autarkie im Einsatzraum: Die betroffenen IT-Services müssen ohne Rückwärtsverbindung zu den zentralen Rechenzentren lauffähig sein
- Interoperabilität: Die betroffenen IT-Services müssen mit IT-Services von Partner-Nationen kommunizieren können und die Anforderungen gemäß Federated Mission Networking (FMN) müssen erfüllt sein
- Einsatztauglichkeit/Truppentauglichkeit: Nutzung und Betrieb der IT-Services durch die Truppe im Einsatzraum müssen möglich sein

Die Erfüllung der Anforderungen insbesondere betreffend FMN wurden bei der internationalen Interoperabilitätsübung CWIX2024 (Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise) getestet.

Betreffend Chat wurde das Produkt Element-Messenger umfassend evaluiert, dieses ist technisch geeignet und erfüllt die Anforderungen der Bedarfsträger und Anwender. Aufgrund der hohen Kosten wird die Evaluierung jedoch im Hinblick auf Open-Source Produkte fortgesetzt.

Eine große Herausforderung stellt betreffend sämtlicher Services die Umsetzung des Information Labeling (Kennzeichnung von Informationen und deren Überprüfung gemäß vorgegebener Standards, zwingende Interoperabilitätsanforderung) dar. Dieses wird ein Kernthema des Jahres 2025 sein.

Fähigkeiteninformations-, planungs- und -steuerungssystem (FIPS)

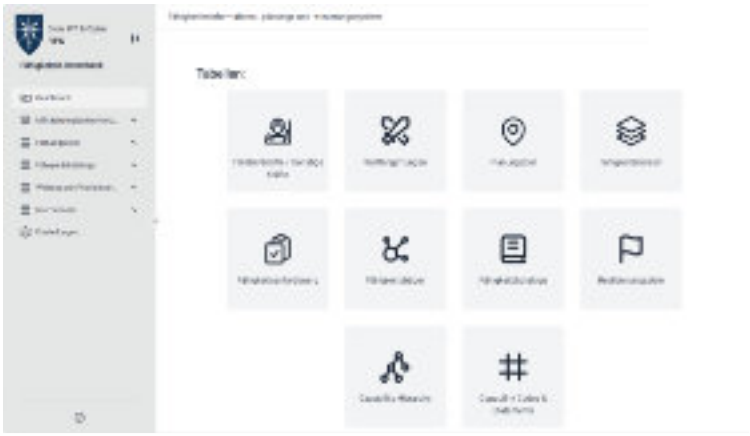
Das Fähigkeitsinformations-, planungs- und -steuerungssystem (FIPS) dient der Digitalisierung der zentralen Prozesse der Landesverteidigung. Ziel ist es ein flexibles IT-Service bereitzustellen, das sämtliche Planungsaktivitäten im BMLV/ÖBH beginnend von der militärstrategischen Planung über die Fähigkeits&Grundsatzplanung, die Strukturplanung, Beschaffung und Umsetzung in allen Entwicklungslinien bis hin zu Bereitstellung, Betrieb und Aussonderung unterstützt.

FIPS besteht aus den folgenden Modulen:

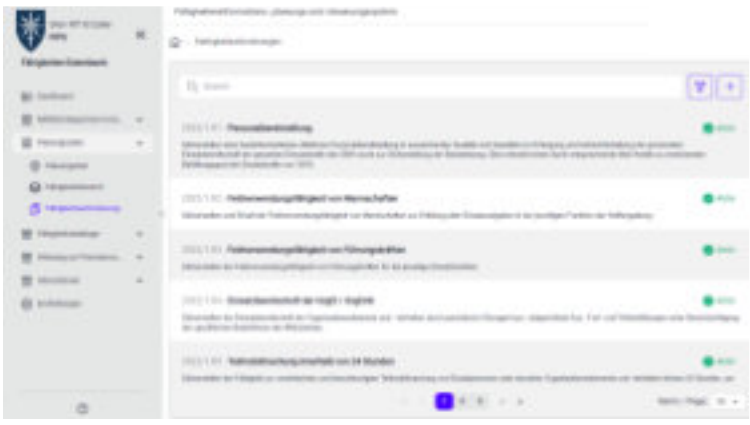
Grafik: Bundesheer/Dion6, MilgesW

Im Jahr 2024 wurde intensiv an den Modulen Fähigkeiten-Datenbank und Portfolio-Management gearbeitet, für beide Module konnte die Initial Operating Capability erreicht werden. FIPS wurde bereits für die Verarbeitung von Daten der Klassifizierungsstufen EINGESCHRÄNKT, Restreint UE und NATO Restricted zugelassen.

Auszug Fähigkeiten-Datenbank:

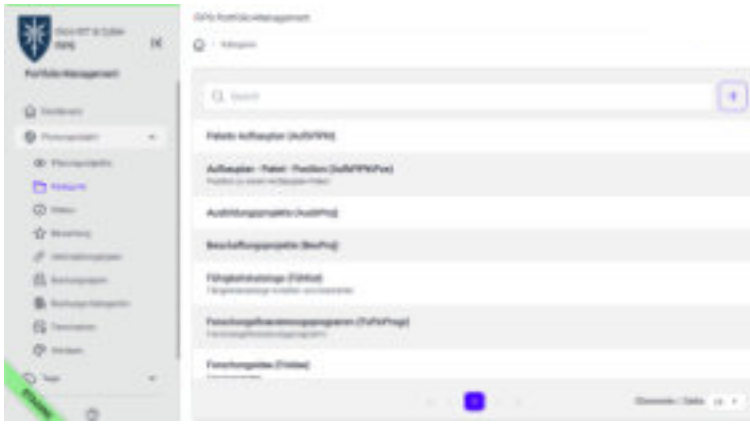


Grafik: Bundesheer/Dion6, FIPS Cockpit

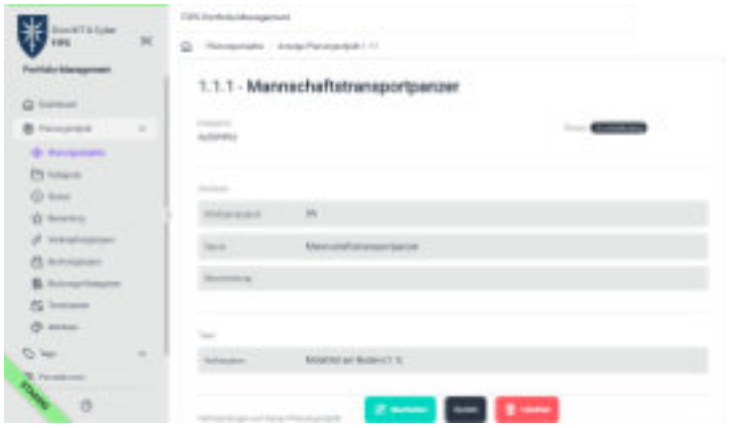


Grafik: Bundesheer/Dion6, Fähigkeitsanforderung

Auszug Portfolio-Management:



Grafik: Bundesheer/Dion6, PortfolioMngt Planungsobjekt-Kategorien



Grafik: Bundesheer/Dion6, PortfolioMngt Planungsobjekt

Als neues Modul ist 2024 das Modul Research Information System Evolution (RelS Evo) dazu gekommen. Damit werden die Forschungsprozesse des BMLV/ÖBH unterstützt.

Es ist geplant die Final Operational Capability (FOC) für alle Module bis 2028 zu erreichen.

Organisations- und Logistikapplikationen (Org&LogAppl)

Versand und Zustellung

Das LOGIS-Teilsystem Versand und Zustellung unterstützt die Zuführung von Material aus den Lagern (HLogZ, HBA, ...) an die Bedarfsträger. Diese Funktionalität löst die bisher erfolgreich eingesetzte Access-Anwendung „Schmidt-DB" ab.

Aus dem Lager ausgegebenes Material wird in Packstücken je Bedarfsträger verpackt. Diese werden im eigenen Zustellbereich des Lagers mittels Zustellfahrten an die Bedarfsträger zugestellt.

Packstücke für Bedarfsträger im Zustellbereich anderer Lager werden zu Versandstücken zusammengefasst und per Versandfahrten an das jeweilige zustellende Lager weitergeleitet. Im zustellenden Lager werden die Versandstücke aufgelöst und die Packstücke an die Zustellung weitergeleitet.

Die Packstücke und Versandstücke sind eindeutig identifiziert und mit Barcode-Etiketten gekennzeichnet. In der gesamten Prozesskette ist eine effiziente Dokumentation der Vorgänge mittels Barcode-Leser ermöglicht. Damit ist die Sendungsverfolgung (Asset- und Consignment-Tracking) sichergestellt und für den Bedarfsträger ist die Information über den Verbleib des erwarteten Materials jederzeit auf Knopfdruck abrufbar.

Auswertungen aus der Prozessdokumentation ermöglichen die Verbesserung und Optimierung dieses Abschnittes der Lieferkette.

Für die Akteure in den Lagern steht eine moderne Web-Applikation mit tätigkeitsorientierter Unterstützung und einfacher Bedienbarkeit (Barcode-Leser, Drag&Drop, automatischer Druck von Etiketten und Belegen, ...) auf Basis der LOGIS-Web-Technologie zur Verfügung.

Arbeit an der Packstation

Grafik: Bundesheer/Dion6, Versand&Zustellwesen Packstation

- Bildung von Packstücken je Bedarfsträger aus Ausgabeanweisungen
- Bildung von Versandstücken je zustellendem Lager aus Packstücken

Arbeit an der Verladestation

- Beladen und Abrechnen von Zustellfahrten

Grafik: Bundesheer/Dion6, Versand&Zustellwesen Verladestation

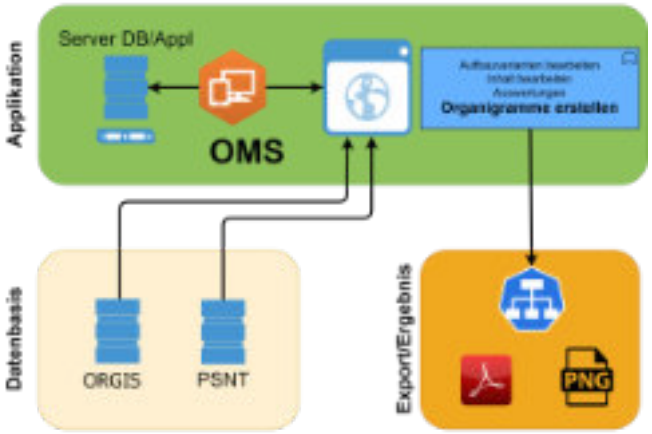
- Beladen und Entladen von Versandfahrten
- Auflösen von Versandstücken

Organisations-Management Service (OMS)

Das Organisations-Management Service (OMS) dient

- zur Organisations- und Personalplanung im Rahmen von Reorganisationen der Zentralstelle BMLV und der oberen Führung
- als Unterstützung zur Bildung und Anpassung einer klar strukturierten Aufbauorganisation und zur Effizienzsteigerung
- zur komfortablen, schnellen Erstellung und einfachen Anpassung von Organigrammen einzelner bzw. größerer Strukturelemente auf Basis aktueller ORGIS Daten inkl. Besetzungen aus PSNT mit vollständiger Bearbeitungsmöglichkeit

Die Analysen wurden bereits Mitte 2022 begonnen.



Grafik: Bundesheer/Dion6, Systemarchitektur OMS

Durch die Dringlichkeit der Ablöse der IDV Anwendung für Arbeitsplatzbeschreibungen durch das Arbeitsplatzinformationssystem (APLIS), wurde mit der Umsetzung nach Bereitstellung eines voll funktionsfähigen Prototyps, erst im November 2023 begonnen. Nach kurzer Entwicklungszeit wurde die erste Version V24.1 der Fachabteilung Org bereits Anfang Mai 2024 präsentiert. Es folgte Ende Juni 2024 eine weitere Release V24.2 mit den durch die Fachabteilung ergänzten Anforderungen und Änderungswünschen.

Die neue Release V25.1, die im 1.Quartal 2025 bereitgestellt wird, beinhaltet neue Kopierfunktionen und Attribute zum Arbeitsplatz. Im Laufe des Jahres wird der geplante OMS Komplettausbau realisiert und die Analyse zur Nutzung des OMS für die Abbildung der Geschäftseinteilung und Dienstanweisung des BMLV gestartet.

Grafik: Bundesheer/Dion6, Beispiel Organigram OMS Abteilung mit 3 Referaten

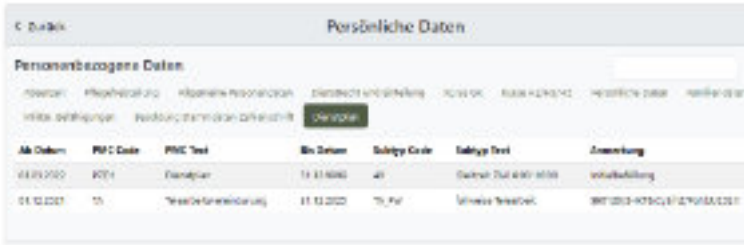
Personalapplikationen (PersAppl)

Die Abteilung Personalapplikationen steht für Digitalisierung und eGovernment im BMLV. Die hohe Steigerung der Nutzungszahlen dokumentieren den Bedarf sowie die Akzeptanz der User an Digitalisierung im österreichischen Bundesheer.

PAAN-Zeitmanagement

Grafik: Bundesheer/Dion6, KRONOS PAAN-Zeitmanagement

PAAN-Zeitmanagement wird mittlerweile BMLV-weit tagtäglich intensiv genutzt. Es wurden über 500.000 Anträge über das PAAN-Antragswesen im Jahr 2024 gestellt und ca. 16.000 Anwender nutzen KRONOS-Zeiterfassung täglich.



Grafik: Bundesheer/Dion6, bundesheeronline Selbstauskunft

Die wesentlichen Erweiterungen des Jahres 2024 sind der elektronische Genehmigungsprozess, die Integration der WEB-Standesliste mit Kronos-Zeiterfassung und die Selbstauskunft. Eine der Herausforderungen für 2025 ist die Bereitstellung von PAAN-Zeitmanagement über das BMLV-Stammportal, um auch jenen Bediensteten, die über keine personifizierte SMN-Chipkarte verfügen, eine Teilnahme über private Devices bzw. über das DGMN zu ermöglichen.

Über die aus KRONOS aufrufbare Selbstauskunft kann der Anwender sich über Daten, die in PERSIS über ihn gespeichert sind, informieren. Künftig soll der Anwender die Möglichkeit haben, selbstständig Daten in die Personalverwaltung einzubringen. Als erste Personalmeldung wird 2025 der Kurantrag in der Selbstauskunft umgesetzt. Dies wird künftig die Personalverwaltung im BMLV nachhaltig verändern.

Grafik: Bundesheer/Dion6, bundesheeronline Statistik

bundesheeronline

Die Erfolgsgeschichte von „bundesheeronline" konnte im Jahr 2024 fortgesetzt werden.

Grafik: Bundesheer/Dion6, bundesheeronline

„bundesheeronline" als das eGovernment-Service des BMLV wurde unter anderem um die Verfahren „Familien-/Partnerunterhalt für Zivildiener", „Milizausbildungsvergütung" und „Dienstzeitbestätigung" erweitert.

An allgemeinen Funktionalitäten wurden die digitale Zustellung von amtlichen Schriftstücke und das Beschwerdewesen hinzugefügt. Mittlerweile sind mehr als 44.000 Personen registriert. An die 90 % an Bankverbindungen im Wehrrecht werden digital über „bundesheeronline" eingebracht. Die großen Herausforderungen für das Jahr 2025 sind die Bereitstellung der Verlässlichkeitserklärung im „bundesheeronline" als auch das Einbringen von „Freiwilligenmeldungen" bis hin zu zivilen Bewerbungen. Auf Basis des erfolgreichen Projektes „bundesheeronline" wurde das neue Projekt „Digitalisierung Wehrdienst" zum Jahresende durch GDPräs beauftragt.

Ziel des neuen Projektes ist unter anderem die zielgruppengerechte Kommunikation zwischen Wehrpflichtigen und Ergänzungsbehörden, die größtmögliche Planungssicherheit der Wehrpflichtigen sowie die Digitalisierung des Stellungsprozesses.

Ausbildungskatalog - ZAK

Mit der Inbetriebnahme des zentralen Ausbildungskataloges (ZAK) Anfang 2024 wurde die langjährige IDV-Anwendung KURSIS abgelöst und damit die Phase I von ZAMS (zentrales Ausbildungsmanagementsystem) abgeschlossen.

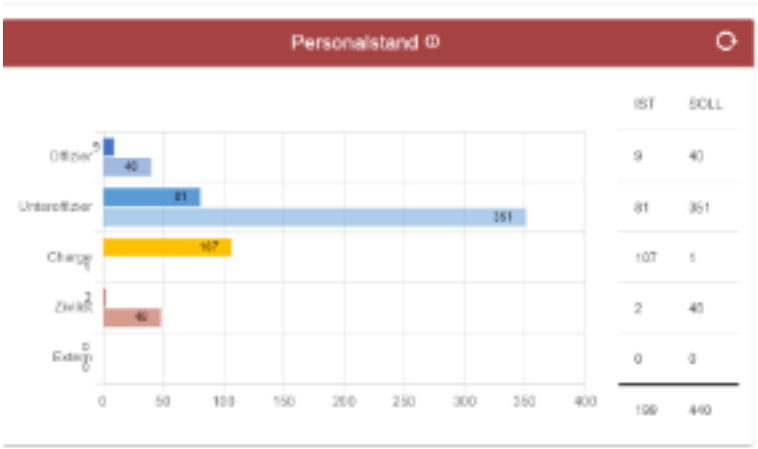
In der Folgephase 2025 wird eine verbesserte Unterstützung der Planungsaktivitäten als auch ein Kurs- und Lehrgangsmanagementsystem (KULM) umgesetzt.

Personalmeldesystem PMSE

Das neue Personalmeldesystem Einsatz (PMSE) wurde bereits bei Common Roof 2024 und bei Daedalus erprobt und wird Mitte 2025 in Betrieb genommen werden und damit die IDV-Anwendung COPID vollständig ablösen.

Die Personalapplikationen werden am Stand der Technik gehalten und an gesetzliche Erfordernisse angepasst.

Die durchgeführten Anpassungen werden in den Release Notes dokumentiert und sind durch Anklicken des PS-NT Logos für alle Anwender erreichbar.



Grafik: Bundesheer/Dion6, PMSE


Foto: BMLV/HBF

IKT-Technik

Leiter IKTTe:
Mag. Wolfgang HACKER

Im Jahr 2024 war der Bereich IKT-Technik von bedeutenden Entwicklungen geprägt. Der Personalaufwuchs stellte dabei einen wichtigen Schritt dar, um den steigenden Anforderungen gerecht zu werden. Durch die Erweiterung des Teams konnten neue Kompetenzen gewonnen werden.

An der Neuausrichtung des IKT-Systems ÖBH wurde intensiv mitgearbeitet, ferner wurden zahlreiche Planungsgrundlagen erarbeitet.

Es wurden IKT-Projekte erfolgreich umgesetzt, sowie in die Erhaltung und Weiterentwicklung der bestehenden Infrastruktur investiert. Die Einführung von Plattformen, neuen Technologien und die Integration von weiteren Softwarelösungen tragen wesentlich zur Digitalisierung der militärischen sowie der Prozesse des täglichen Dienstbetriebes bei.

Besonders hervorzuheben ist die Weiterentwicklung der technischen IKT-Architektur, die Grundlagen für die steigenden Anforderungen an das IKT-System ÖBH bieten soll.

Dank der hervorragenden Zusammenarbeit mit unseren vorgesetzten Dienststellen, Kunden, den Organisationselementen der Direktion 6 - IKT und Cyber sowie externen Partner konnten wir erfolgreich die für 2024 gesetzten Ziel erreichen.

GPU Cluster

Moderne Machine Learning (ML) und Artificial Intelligence (AI) Workloads zeichnen sich durch spezielle Hardwareanforderungen aus, welche vorrangig durch GPUs (Graphics Processing Units) abgedeckt werden können. Hierzu wurden im Bereich IKTTe entsprechende Server mit State-of-the-Art NVIDIA H100 Grafikkarten beschafft und im Rechenzentrum integriert. Um die Hardware optimal nutzen zu können und gleichzeitig eine Plattform für moderne Workloads zu schaffen, wurde ein Kubernetes Cluster für ML/AI Workloads auf Basis dieser Hardware geschaffen. Mit RKE2 (Rancher Kubernetes Engine, auch bekannt als "Rancher for Government") existiert nun ein moderner Kubernetes Cluster, welcher sich durch folgende Eigenschaften auszeichnet:

- Fokus auf Security und Compliance (FIPS 140-21 [Federal Information Processing Standard Publication 140-2 is a U.S. government computer security standard used to approve cryptographic modules.], CVE Checks2 [Common Vulnerabilities and Exposures ist ein vom US-amerikanischen National Cybersecurity FFRDC betriebenes und von der Mitre Corporation gepflegtes System zur standardisierten Identifikation und Benennung von öffentlich bekannten Sicherheitslücken und anderen Schwachstellen in Computersystemen], CIS3 [Center for Internet Security] Benchmark)
- schlank, sehr nahe am Kubernetes Standard
- Support für airgapped (=vom Internet getrennte) Systeme/Installationen

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Grafik: Bundesheer/Dion6, GPU-Cluster

Architektur

Der GPU Cluster besteht aktuell aus drei Steuerungsknoten (Control Plane Nodes) und drei GPU Server mit jeweils vier Datacenter GPUs. Eingesetzte Container können diese GPU's nutzen. Der GPU Cluster wird derzeit für regelmäßig stattfindenden Datentransformationsprozesse, für verschiedene Chat Services sowie für die Bereitstellung von Entwicklertools, wie zum Beispiel „VSCode" (Unterstützung beim Erstellen von Programmcode), verwendet.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Während der kontinuierlichen Bereitstellung dieser Services konnten ohne Downtime bzw. Service Einschränkungen weitere Nodes dem Cluster hinzugefügt bzw. die Kubernetes Version von 1.30 auf 1.31 aktualisiert werden.

Warum Kubernetes?

Die traditionelle Vorgehensweise bei der Bereitstellung von Anwendungen in Produktionsumgebungen birgt eine Reihe von Herausforderungen. Die manuelle Verwaltung von Servern (beantragen, „feste" Parameter wie CPU/RAM/Disk), der hohe Aufwand bei Skalierung und Rollbacks (individuell je Service!) sowie die Abhängigkeit von festen Umgebungen sind nur einige Beispiele dafür.

Durch Automatisierung, standardisierte Deployments (Einsatz neuer Anwendungen oder Aktualisierung von Bestehenden), Service Discovery (Automatisierte Verteilung der Anwendungen innerhalb des Kubernetes Clusters), Permissions Management (Administration der Zugriffsrechte) u. High Availibility (Hochverfügbarkeit bzw. Ausfallsicherheit von Systemen) Features wie Selbstheilung bietet Kubernetes eine Vielzahl von Vorteilen bei der Bereitstellung von Anwendungen.

- Automatisierung: Durch die Automatisierung von Deployment-Prozessen können Fehler reduziert und die Effizienz gesteigert werden.
- Rolling Updates: Eine neue Version wird schrittweise ausgerollt, ohne dass die Anwendung unterbrochen wird.
- Rollback: Die automatische Rückkehr zur letzten funktionierenden Version.
- Blue-Green Deployment: Der Parallelbetrieb von zwei Versionen (z. B. v1 und v2), mit dem Vorteil eines sicheren Wechsels der Anwendungen durch Umleitung der bestehenden Prozesse.

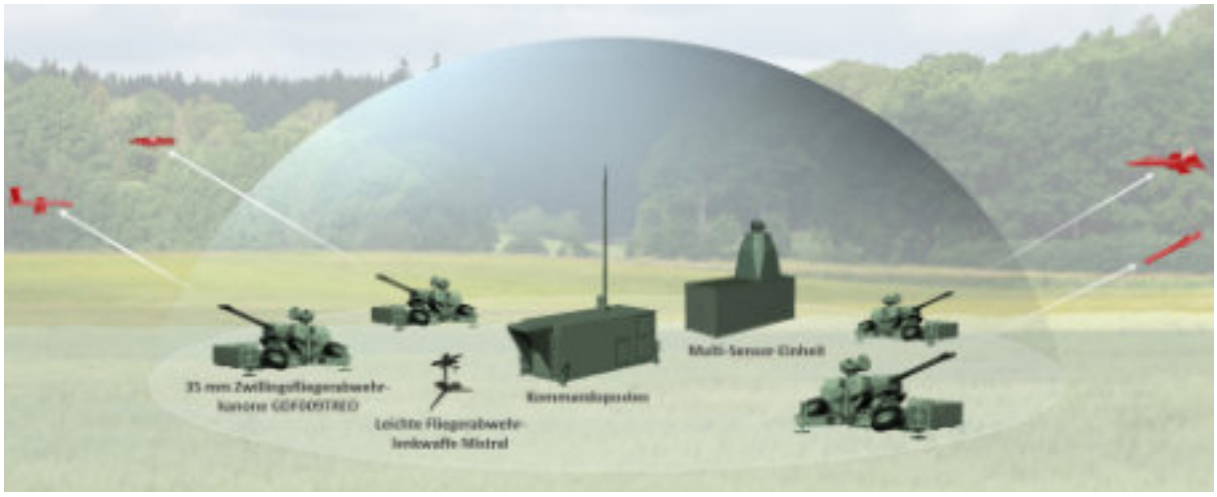
Weitere positive Effekte ergeben sich durch die Standardisierung: moderne Software Komponenten bieten für Kubernetes einen einheitlichen Update/Rollback Prozess. Zudem vereinfacht es den Knowhow Transfer für bestehende bzw. das Onboarding neuer Mitarbeiterinnen und Mitarbeiter. Mit dem RKE2 GPU Cluster existiert daher nun eine zukunftssichere Plattform für bestehende und kommende AI/ML Workloads im Unternehmen.

Nutzungsdauerverlängerung 35mm Feuereinheit (NDV 35mm)

Aufgrund von Obsoleszenzen und des Alters des Feuerleitgerät 98 und der 35mm Zwillingsfliegerabwehrkanone, wurde das Vorhaben NDV 35mm gestartet. Eine taktische Einheit besteht aus einer Multi Sensor Unit (MSU), einem Kommandoposten (TLCN) und 4 35mm Zwillingsfliegerabwehrkanonen. Weiters können auch leichte Fliegerabwehrlenkwaffen vom Typ Mistral angesteuert werden.

Die MSU besteht im wesentlichen aus einem modernen Radarsystem, welches auch die Möglichkeit der Freund/Feind Kennung bietet und aus elektrooptischen Systemen, welche eine passive Zielverfolgung ermöglichen.

In der TLCN werden Radardaten von der MSU und auch von übergeordneten Systemen verarbeitet.



Grafik: Bundesheer/Dion6, NDV 35mm

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Die Daten (Radar und elektrooptisch) werden zur Bedrohungsbewertung herangezogen und an den Richtschützen zur Bekämpfung von zugewiesenen Zielen weitergegeben.

Die modifizierte 35mm Zwillingsfliegerabwehrkanone besitzt ein eigenes Radarsystem und ein elektrooptisches System zur Zielverfolgung. Der Richtschützen bedienen die 35mm Zwillingsfliegerabwehrkanonen von der TLCN aus. Es besteht jedoch die Möglichkeit die Kanone über eine lokale Konsole zu bedienen. Es können verschiedene Munitionsarten verschossen werden.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Das NDV 35mm ist ein modernes Waffensystem mit dem die Fliegerabwehrtruppe der LRÜ für die Zukunft gut gerüstet ist. Ende 2025 soll das Schulungssystem geliefert werden und ab 2026 laufen die ersten Feuereinheiten zu.

Das Vorhaben wird von WSM geleitet. Laufend finden Abstimmungen mit dem Auftragnehmer und dem Nutzer (LRÜ) statt.

IKTTe ist im Vorhaben Nutzungsdauerverlängerung 35mm für die Güteprüfung und Systembetreuung der Radarsysteme verantwortlich, weiters fallen Teile der IKT Komponenten sowie die Einbindung in das IKTSystem Einsatz in unseren Verantwortungsbereich.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Teststellung föderierte Video-Lösung „Open Talk“

Das im BMLV/ÖBH eingesetzte Videokonferenzsystem (VKS) 13 ist für die Bearbeitung von Informationen zugelassen, deren Klassifizierung höher als "OFFEN" sind. Daran sind jedoch Bedingungen geknüpft, deren Einhaltung durch die Technische Systembetreuung überwacht wird. Dazu gehört auch, dass nur solche Geräte eingesetzt werden, die vom Hersteller noch mit Sicherheits-Updates unterstützt werden. In nächster Zeit fällt eine ganze Geräteklasse aus dieser Unterstützung und muss daher ersetzt werden.

Der derzeitige Systemaufbau des VKS13 im TCN (Tactical Communication Net) sieht eine Verbindung zu zentralen Komponenten vor. Das ist im "Inselbetrieb", oder bei eingeschränkter Konnektivität in das ortsfeste Netz ein Problem und führt zu eingeschränkter Funktionalität.

Die Technische Systembetreuung hat sich daher nach Alternativen umgesehen, mit der sowohl die auslaufende Zulassung eines Teils der Hardware als auch die Problematik mit der Notwendigkeit von zentralen Komponenten gelöst werden können.

Das Zauberwort der gefundenen Lösungen heißt dabei "Federation". Der Vorteil des föderierten Ansatzes für das Identitätsmanagement in vernetzten Systemen besteht darin, dass die einzelnen Knoten jeweils für ihre "Bürger"

Grafik: Bundesheer/Dion6, KI Verwendung

verantwortlich sind und diese sich in sogenannten "Circles of Trust" bewegen können, ohne sich jedes Mal neu anmelden zu müssen.

IKTTe hat zwei Systeme identifiziert, die eine Video-Lösung mit einem föderierten Ansatz bieten:

- Element Call auf Basis des Matrix-Protokolls, und
- OpenTalk (OT)

Element Call wird durch die Abteilung HW&SysSW (Hardware&SystemSoftware) getestet und auf die Fähigkeiten hin beurteilt, während OpenTalk durch die Technische Systembetreuung VKS in einer Teststellung seit April 2024 die Tauglichkeit für das TCN testet.

Zusätzlich zu den beiden oben genannten Herausforderungen besteht auf Seiten des BMLV/ÖBH der Wunsch, ein System zu beschaffen, das auf Standardkomponenten des BMLV läuft, nach Möglichkeit Open Source ist, und in jedem Fall offene Standards unterstützt.

Nachdem in einem ersten Schritt die OpenTalk Teststellung in einer Virtuellen Maschine lauffähig gemacht wurde (mit besonderer Unterstützung des Referats Managementsysteme), konnte im Herbst die Funktionalität so weit erweitert werden, dass nun auch die Chipkarten als Token für die Anmeldung am System verwendet werden können.

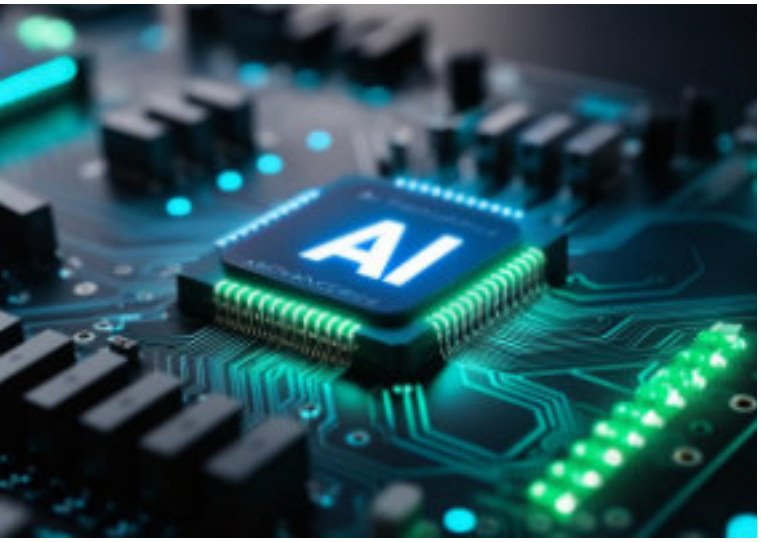
Das System OpenTalk steht im Q1/2025 vor einer weiteren Funktionserweiterung. Erstmalig werden dann OT-Nodes auf TCN-Servern von Vermittlungssystemen eines Übungstruppenkörpers aufgebracht, und das System der Föderation getestet.

Wenn diese Testungen erfolgreich absolviert werden können, so ist dann für Juni 2025 ein "Stresstest" vorgesehen, bei dem etwa auf ein Drittel der TCN-Server, verteilt über das ganze Bundesgebiet, OT-Instanzen installiert werden sollen, und ein dichtes Programm an Verbindungsrelationen hergestellt und auf Qualität und Stabilität getestet werden sollen. Mit einem gleichzeitigen Sicherheitsaudit sollen die Grundlagen für die Zulassung des Systems geschaffen werden.

Ziel der seit Beginn 2024 laufenden Arbeiten ist es, Grundlagen zu erstellen, damit im Laufe des Jahres 2025 eine Einleitung zur Beschaffung für den Abersatz der nicht mehr verwendbaren Hardware im VKS13 erfolgen kann. Damit stehen dann neben einem Verbleib beim derzeitigen Systemlieferanten auch Alternativen zur Verfügung.

Die Teststellung OpenTalk hat über die Grenzen des Ressorts hinaus Beachtung gefunden. Bei einem Vortrag im Rahmen des EU-Projekts "Open Source in der Verwaltung" wurden andere

Ministerien, die Parlamentsdirektion und andere "gewichtige" Vertreter des öffentlichen Dienstes auf die Teststellung des BMLV aufmerksam und durch den Referatsleiter Sprachdienste in die geplanten Abläufe eingewiesen. Zahlreiche Dienststellen haben sich darauf als Beobachter der weiteren Testungen avisiert.



Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

KI@ÖBH-2024 - ein Rückblick

Die sehr dynamischen Entwicklungen im Bereich der künstlichen Intelligenz machen Veränderungen nötig, die sich auch deutlich in den bewaffneten Konflikten der letzten Zeit gezeigt haben. Im Zentrum des Jahres 2024 stand also der Aufbau eines Kernteams, das sich dem Knowhow und im ersten Schritt der Etablierung grundlegender Fähigkeiten für die Handhabung und den Betrieb von KI Anwendungen auf breiterer Basis im ÖBH und BMLV widmen kann.

Am Anfang einer sinnvollen Entwicklung stand die Erhebung des Bedarfs und die Identifikation grundsätzlicher use-cases. In Folge wurden die formulierten Anforderungen geschärft und als "proofs-of-concept" (PoCs), also als Erstellung einfacher technischer Machbarkeitsstudien, dargestellt.

Hardware

Für KI Lösungen ist besondere Rechenleistung erforderlich. Informationen über Technologien und Hardware Plattformen für den autarken Betrieb und das Training von KI Modellen wurden daher recherchiert und entsprechende Angebote eingeholt. Dementsprechend konnten Anschaffungen erfolgreich durchgeführt werden, die zum Einen aus KI Workstations bestehen, die als experimentelle Arbeitsplätze und erste kleine Serverplattformen verwendet werden konnten.

Die größere Ausrollung von KI Anwendungen macht zum Anderen auch entsprechende GPU Server nötig, die ins Rechenzentrum integriert wurden (mit ausdrücklichem Dank an die verantwortlichen Unterstützer).

Kooperation

Information und Kommunikation über Interessen und die Entwicklungen sind ein wesentlicher Teil notwendiger Zusammenarbeit, daher wurden wiederholte Treffen unter dem Namen "DAMLAI" abgehalten (Data Analysis, Machine Learning, Artificial Intelligence), um die Einladung zur Kooperation und das Auffinden von Synergien zu ermöglichen, welche die großen Anforderungen tragbarer machen. Diese Treffen waren gut besucht und haben positive Rückmeldungen der Teilnehmer eingebracht, die wertvolle Einsichten in die Anforderungen der Bedarfsträger erlaubten. Im Zuge dieser Bemühungen wurde vom KI Team auch auf der Leistungsschau zum Nationalfeiertag 2024 ein Informationsstand ausgerichtet, wo exemplarische Anwendungen von KI den interessierten Besuchern gezeigt werden konnten.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Entwicklungswerkzeuge

Für Arbeiten mit und an KI Modellen konnte eine Art Werkbank für die Entwicklung ("MLops" - Machine learning operations - Plattform) namens "MLflow" aufgebaut werden.

Regelmäßige Datentransformationsprozesse für die Vorbereitung und Aufgaben maschinellen Lernens wurden in sogenannten "data pipelines" ermöglicht.

Anwendungen

Als technische Machbarkeitsstudien wurden vom KI Team folgende Use-cases identifiziert und erste Umsetzungen ausgearbeitet:

- AI Chat:

Mittels OpenWeb UI wurde eine autarke Plattform ähnlich ChatGPT aufgesetzt.

- Übersetzung:

Durch die Verwendung von frei verfügbaren KI Modellen (LLMs) konnte ein autarkes maschinelles Übersetzungsservice eingerichtet werden.

- Softwareentwicklungsunterstützung:

Für das häufig verwendete Entwicklerwerkzeug "VScode" wurde autarke KI Integration ermöglicht.

- Textkorpus Erschliessung:

Zum besseren Erarbeiten von umfangreichen Textcorpora wurde ein KI System ("RAG") eingerichtet, das anhand der Dokumentation des BMS "Sitaware" beispielhaft die Inhaltserschliessung mittels natürlichsprachlicher Fragen ermöglicht.

- Anwendungsunterstützung:

Um weiteren Bedarfsträgern die Arbeit mit KI-Unterstützung zu ermöglichen, wurde in Kooperation mit dem Mil-Cyber-LZ der Zugang zu KI Sprachmodellen erfolgreich etabliert.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Forschung

Zur sicheren und verantwortungsvollen Weiterentwicklung des Bereichs der Anwendungen künstlicher Intelligenz im Ressort, wurden in Kooperation mit dem Referat für Cybergrundlagen und Innovation Forschungsprojekte eingeleitet, die den gewünschten Pfad begleiten.

Umstellung Liegenschaftsserver

Nachdem 2023 die Beschaffung und Lieferung der neuen Serverhardware für die Liegenschaftsserver erfolgt ist, konnte 2024 die Zuweisung der Hardware, die Vorkonfektionierung der Serverracks, die Aufstellung/Installation und Inbetriebnahme, der Parallelbetrieb und die Umstellung der Liegenschaftsserver begonnen werden.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Ziel war es seitens SysEntwg2VE die Phasen Aufstellung/Installation, Inbetriebnahme, Parallelbetrieb und Umstellung so vorzubereiten, dass dies dezentral durch Benutzerbetreuung (BenBelT) gesteuert durchgeführt werden kann, dass die oa. einzelnen Phasen vollständig automatisiert sind und durch BenBelT auch selbstständig angestoßen werden können.

So ein Vorhaben, welches alle Liegenschaftsserver betrifft, konnte nur durch die Unterstützung und ausgezeichnete Zusammenarbeit folgender Organisationseinheiten gelingen:

- Dion1: S4 und S6 der MilKden, Brigaden und Bataillone
- Dion4: Disp&BetrFü; RefIKT(of)/Disp&BetrFü, HLogZ WIEN/IKTAbt/ITEloRadWkst&SysWkst und IKTAbt der HlogZ
- Dion6: Appl/EinsAppl & PersAppl, IKTBetr/BenBeIT, IKTTe/HW&SysSW & Komm & TeQA und IKTCyE

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Durch die Priorisierung der Umstellung der Liegenschaftsserver im Dion6 Vorhabensportfolio konnten die Ressourcen intern gebündelt und ein Schwergewicht gebildet werden. Dies ermöglichte folgende zeitliche Umsetzung:

- April/Mai 2024: vollautomatisierte Umstellung von Testlokationen
- 14.06.2024: Abschluss Aufstellung/Installation, Inbetriebnahme, Parallelbetrieb und Sicherstellung, dass alle Daten auf die neue Liegenschaftsserver-VMs synchronisiert sind und die Erstreplikation des neuen Backup/Recovery-Verfahrens abgeschlossen ist
- 19.06.2024: Freigabe der österreichweiten Umstellung aller Liegenschaftsserver
- 20.06.2024 – 30.08.2024: Umstellung aller Liegenschaftsserver im Sicheren Militär Netz (SMN), wobei bis zu 15 Liegenschaftsserver an einem Tag umgestellt worden sind

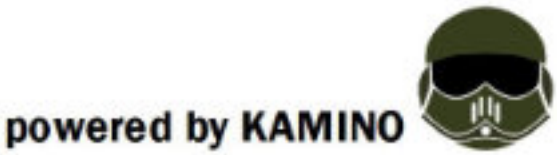
Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Die Umstellung der TCN-Server und abgesetzter Sondernetze ist mit 2025 abgeschlossen und das Vorhaben Umstellung Liegenschaftsserver beendet.

Die dezentrale Serverinfrastruktur der Liegenschaftsserver im SMN, im TCN und bei abgesetzten Sondernetzen ist damit für die Herausforderungen von ÖBH2032+ und dem IKTSysE gut aufgestellt. Nicht nur neue leistungsstarke Hardware, sondern auch neue Funktionalitäten stellen die Voraussetzungen und Reserven sicher, um flexibel auf Anforderungen reagieren zu können.

Die beiden wichtigsten neuen Funktionalitäten sind erstens ein neues Backup/Recovery-Verfahren, dass keine Bandlaufwerke benötigt und zweitens die Virtualisierung der Liegenschaftsserver und erforderlicher zusätzlicher Services. Durch diese Virtualisierung können somit auf einem physischen Server mehrere Liegenschaftsserver und zusätzliche Services gleichzeitig betrieben werden.

Die Umsetzung dieses Vorhabens hat sich an den Führungsgrundsätzen Schwergewichtsbildung, Kooperation und Einfachheit orientiert. Vor allem das letztere war der Treiber für die durchgehende Automatisierung, welche in enger Abstimmung mit BenBeIT implementiert worden ist und welche die Dezentralisierung der Umstellung überhaupt ermöglichte. Dank allen Beteiligten und vor allem den KAMINO-Twins.



Grafik: Bundesheer/Dion6, KAMINO


Foto: BMLV/HBF

Militärisches Cyberzentrum

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

2024 war für das MilCyZ ein Jahr voller Herausforderungen und bedeutender Fortschritte. In einem zunehmend komplexeren globalen Sicherheitsumfeld haben wir unsere Fähigkeit zur Abwehr und Reaktion auf Cyberangriffe weiter gestärkt.

Herausragende Highlights waren unter anderem die erfolgreiche Teilnahme an der Locked Shields Übung 2024 sowie an weiteren EU- und NATO weiten, groß angelegten Cyber-Übungen, bei der alle Beteiligten ihre Fähigkeiten unter realistischen Bedingungen testen und festigen konnten.

Zudem haben wir weiterhin in enger Zusammenarbeit mit europäischen und internationalen Partnern zusammengearbeitet und sind seit Mai 2024 vollwertiges Mitglied des PESCO CRRT Projektes (Cyber-Rapid-Response-Team).

Dies brachte ein weiteres Highlight hervor: Den ersten EU-Einsatz der ÖBH-Kräfte im europäischen Cyber Rapid Response Team in Moldau.

Unsere Zusammenarbeit mit der Industrie und Forschungseinrichtungen wurde weiterhin intensiviert, um die neuesten Entwicklungen im Bereich der Cybertechnologien schnell in unsere Strukturen zu integrieren. Um insbesondere die Innovation im Bereich Cyberverteidigung zu stärken.

2024 wurde zudem durch weiteren Aufbau einer mil. Cyber Range eine Trainingsumgebung geschaffen, in der unsere Cyber-Experten realistische Cyber-Einsätze üben können.

Die kontinuierliche Verbesserung dieser Infrastruktur trägt maßgeblich dazu bei, die Cyberabwehrkompetenz des Österreichischen Bundesheeres auf höchstem Niveau zu halten.

Eine der größten Herausforderungen war 2024 und wird auch noch in den Folgejahren die sichere Integration neuer Waffensysteme und moderner Führungs- und Kommunikationsmittel in die IKT-Landschaft des ÖBH sein. Ziel ist hier auf allen Ebenen und in allen mil. Domainen die Resilienz gegen Bedrohungen aus dem Cyber-Raum zu stärken und gegen hybride Bedrohungen gewappnet zu sein.

Wir sind stolz darauf, die digitale Souveränität Österreichs weiter zu sichern und einen Beitrag zur Stärkung der europäischen Sicherheitsarchitektur zu leisten.

Locked Shields 24

Seit 2012 nimmt das MilCyZ und seine Vorgängerorganisationen (mit einigen Ausnahmen) jährlich an der Cyberübung „Locked Shields" teil. Organisiert wird diese vom NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) und gehört zu den weltweit anspruchsvollsten Übungen im Bereich der Cybersicherheit. In dieser Übungsreiche übernehmen Spezialisten des MilCERT neben dem eigenständigem Blue Team auch immer Rollen der Angreifer im Red Team wahr.

Grafik: Logo Blue Team LS24

2024 nahm das Blue Team Österreich-Schweiz mit Unterstützung von Partnern aus der US National Guard an dieser hochkomplexen Übung teil. Dazu verlegten rund 30 Cyber- und InfoOps-Experten für 2 Wochen an einen Standort in der Schweiz. „Locked Shields" zielt darauf ab, die Reaktionsfähigkeit, Verteidigungsstrategien und taktisches Handeln gegen reale Cyberbedrohungen zu üben. Dabei werden groß angelegte Cyberangriffe auf kritische Infrastrukturen simuliert, bei dem über 2000 Cyberexperten aus 40 Nationen in 20 Teams gegeneinander antreten. Die Teilnehmer müssen ihre Services verfügbar halten und ihre Systeme wiederherstellen, während sie gleichzeitig versuchen, die Angreifer zu identifizieren und deren Aktivitäten zu stoppen und ev. auch Systeme zurück zu erobern. Das österreichische Blue Team hatte die Aufgabe, als Verteidiger zu agieren und die simulierte IT-Infrastruktur zu schützen.

Die Herausforderung bestand darin, Angriffe, wie DDoS-Attacken, Malware-Infiltrationen und Advanced Persistent Threats (APTs), aber auch Defacements, in Echtzeit abzuwehren. Dabei mussten nicht nur technische Fähigkeiten zur Netzwerk- und Systemsicherheit eingesetzt werden, sondern auch rasche Entscheidungen in der Koordination und Kommunikation getroffen werden, um eine schnelle und effektive Abwehr zu gewährleisten.

Zudem muss regelmäßig ein Lagebild für das übergeordnete Kommando erstellt sowie rechtliche Fragestellungen im internationalen Rechtsraum ausgearbeitet und berücksichtigt werden. Schließlich muss das Handeln des Blue Teams im Rahmen der Rechtsnormen bleiben.

Besonders herausfordernd war die Vielfalt der Bedrohungen. Das Red Team, das die Angriffe simulierte und auch praktisch durchführte, nutzte eine breite Palette von Taktiken, von klassischen Angriffen bis hin zu komplexeren, schwer erkennbaren Bedrohungen wie Zero-Day-Exploits. Das österreichische Team musste sowohl technische Lösungen finden als auch in einer stressigen, dynamischen Umgebung die richtigen Prioritäten setzen.

Darüberhinaus gilt es auch die Kommunikation (Öffentlichkeitsarbeit, sowie minimal Psy-/InfoOps) im Griff zu halten und auf etwaige Medienanfragen zu reagieren, bzw. auch proaktiv im Informationsraum zu agieren.

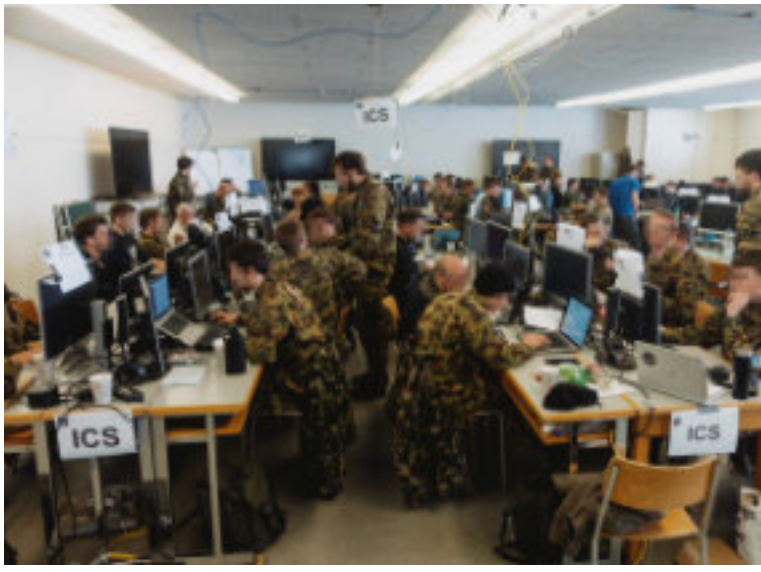


Foto: Bundesheer/Dion6, Logo Blue Team LS24

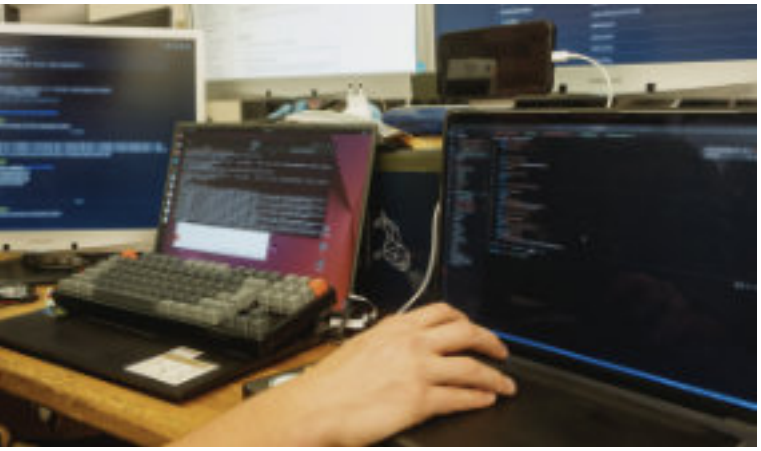


Foto: Bundesheer/Dion6, Arbeitplatz bei der LS24

Die Teilnahme an „Locked Shields" ermöglichte den Österreichischen und Schweizer Kameraden wertvolle Erfahrungen in der Verteidigung gegen komplexe Cyberangriffe zu sammeln und zeigte die Bedeutung von internationaler Zusammenarbeit und schnellem Handeln.

Es war eine Gelegenheit, die Fähigkeiten auf die Probe zu stellen, voneinander zu lernen und auf zukünftige Herausforderungen in der Cyber-Domaine noch besser vorbereitet zu sein.

InnoVision

Grafik: Bundesheer/Dion6, Logo InnoVision

Die neue Eventreihe des Militärischen Cyber-Zentrums (MilCyZ) der Direktion 6 - IKT und Cyber entstand aus der Notwendigkeit, zukunftsorientiert zu denken, um künftigen Herausforderungen und Bedrohungen wirksam und innovativ begegnen zu können. Die erste InnoVision-Veranstaltung des Österreichischen Bundesheeres am 15. November 2024 in der Sala Terrena, war ein voller Erfolg.

Mehr als 120 nationale und internationale Teilnehmer:innen aus den Bereichen Wirtschaft, Wissenschaft, Forschung und öffentlicher Verwaltung haben sich in der STIFT-Kaserne eingefunden um gemeinsam den Herausforderungen der so wichtigen Schnittstelle zwischen Innovation und Cybersicherheit zu begegnen.

Mit einer beeindruckenden Agenda und hochkarätigen Speakern bot die Veranstaltung eine einzigartige Plattform für den Austausch innovativer Ansätze, um den Herausforderungen der Cybersicherheit und Cyberverteidigung zu begegnen.

Die interaktiven Methoden, die im Rahmen des Events punktuell gesetzt wurden, um das Publikum zum kreativen Mitwirken anzuregen, wie Expert Prediction Bingo, Horizon Scanning, Idea Brain Storming, Innovation Speed Dating und der Einsatz von Mentimeter erwiesen sich als sehr willkommene Abwechslung und gelegene Möglichkeit des interaktiven Mitwirkens während der Veranstaltung.

Die Veranstaltung hat einen neuen Maßstab gesetzt und gezeigt, wie entscheidend der interdisziplinäre Austausch und innovative Ansätze für die Kooperation und Kommunikation zwischen Behörden, Industrie, Start-ups und Universitäten im Bereich Cybersicherheit und –Verteidigung ist.

Die InnoVision-Reihe soll auch in Zukunft eine Plattform für Innovation sein. Ab dem nächsten Jahr sind jährlich zwei Fokus-InnoVision-Meetings geplant, die jeweils spezifische Themen der Cybersicherheit und Cyberverteidigung behandeln. Darüber hinaus soll alle zwei Jahre eine umfassende InnoVision-Konferenz stattfinden. 2026 sollen die ersten Ergebnisse aus den Fokusmeetings präsentiert und Pitches der gesammelten Innovationsideen zu sehen sein. Außerdem feiert das neue InnoVision Wettbewerb-Format seine Prämiere.

Foto: Bundesheer/Dion6, Team InnoVision

NATO TIDE Sprint

Das BMLV war beim NATO TIDE Sprint, einer international ausgerichteten Veranstaltung zur Förderung der Interoperabilität und digitalen Transformation innerhalb der NATO vertreten. Der Fokus der Teilnahme lag auf dem Bereich Data Centric Security, der sich mit der Entwicklung innovativer Konzepte und Strategien zur datenzentrierten Sicherheit befasst. Durch die Zusammenarbeit mit internationalen Experten aus Militär, Industrie und Wissenschaft konnten wertvolle Impulse für die Weiterentwicklung der Sicherheits- und Interoperabilitätsfähigkeiten gewonnen werden, die für zukünftige Anforderungen von entscheidender Bedeutung sind.

Foto: Bundesheer/Dion6, NATO-TIDE Sprint Auszug der Teilnehmer

Foto: Bundesheer/Dion6, NATO-TIDE Sprint

Crossed Swords 2024

Auch 2024 nahm das Militärische Cyberzentrum wieder an der Übung „Crossed Swords 2024" teil, die rund 200 Teilnehmer aus 40 Ländern – darunter sowohl NATO- als auch Nicht-NATO-Mitglieder – zusammenbrachte, um Cyberoperationen in einer realistischen, simulierten Krisenumgebung zu trainieren. Veranstalter der Übungsserie ist das NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in TALLINN.

Ziel der Übung war es, militärische Führungselemente in der Steuerung und Kontrolle auch offensiver Cyberfähigkeiten auszubilden und gleichzeitig taktische und operative Fähigkeiten im Bereich Cyberspace weiterzuentwickeln. Das Szenario spielte in einem fiktiven Kontext, in dem der befreundete Staat „Berylia" sich in einem bewaffneten Konflikt mit dem feindlichen Staat „Crimsonia" befand. In diesem Rahmen meisterten die Teilnehmer hochdynamische Angriffe und arbeiteten unter hohem Druck an strategischen Zielen, die die Regierung Berylias vorgab.

Besonderes Augenmerk lag auf der Integration modernster Technologien und der Unterstützung durch Partner aus der Industrie und Wissenschaft. Diese Zusammenarbeit ermöglichte es, die Übung äußerst realitätsnah zu gestalten und den Einsatz innovativer Technologien zu integrieren. Diese Tools verbesserten nicht nur die situative Bedrohungserkennung, sondern unterstrichen auch die Bedeutung öffentlich-privater Partnerschaften in der Cybersicherheit und Defence.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Ein weiterer Schwerpunkt lag auf der digitalen Forensik, bei der Cyber-Spezialisten reale Herausforderungen, wie die Datenwiederherstellung von verschlüsselten Geräten oder die Analyse von containerisierten Systemen bewältigten. Auch die Analyse von Standortdaten spielte eine wichtige Rolle, da sie essenziell für die Erkennung und Abwehr von Sicherheitsbedrohungen war.

Die Übung hat deutlich gemacht, wie wichtig internationale Zusammenarbeit und der Austausch globaler Erfahrungen für die Stärkung der Cyberresilienz sind. Realitätsnahe Szenarien und hochmoderne Technologien ermöglichten es den Teilnehmern, wertvolle Erkenntnisse zu gewinnen und Fähigkeiten weiterzuentwickeln, um künftigen Herausforderungen im Cyberspace besser begegnen zu können.

Durch die äußerst erfolgreiche Teilnahme konnte das Militärische Cyber-Zentrum seine Kompetenzen im internationalen Umfeld präsentieren und einen wichtigen Beitrag zur Weiterentwicklung der Cyber-Fähigkeiten des ÖBH erbringen.

Cyber Rapid Response Team (CRRT) und deren Bedeutung für das Österreichische Bundesheer

Mit der Vollmitgliedschaft des Österreichischen Bundesheeres im EU PESCO Cyber Rapid Response Team (CRRT) seit Mai 2024 hat das MilCyZ innerhalb der Dion6 einen bedeutenden Schritt in der Stärkung seiner nationalen Cyberabwehrkapazitäten und der europäischen gemacht. Die organisatorische Umsetzung konnte jedoch noch nicht abgeschlossen werden.

Schnelle Reaktionsfähigkeit als Schlüssel

CRRTs sind spezialisierte Einheiten, die im Falle schwerwiegender, komplexer und hochdynamischer Cyberangriffs schnell und effektiv reagieren, um kritische Infrastruktur zu schützen und die Folgen von Cyberbedrohungen zu minimieren. Diese Fähigkeit ist von entscheidender Bedeutung.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Das PESCO CRRT-Netzwerk hat in den vergangenen Jahren bei mehreren nationalen und internationalen EU-Einsätzen, sowie EU-Übungen unter Beweis gestellt, schlagkräftig es ist. Seit heuer leistet auch Österreich wertvolle Beiträge dazu und war bereits international im Einsatz.

Foto: Bundesheer/Dion6, CRRT bei der Schutzschild 24

Qualifiziertes Personal und spezialisierte Ausrüstung

Die Wirksamkeit eines CRRT hängt nicht nur von einer schnellen Reaktionszeit ab, sondern auch von der Qualität des eingesetzten Personals und der verfügbaren Ausrüstung. Die erforderliche Spezialausrüstung ist nun seit bald 1,5 Jahren im Beschaffungsprozess und steht kurz vor der Auslieferung. Rekrutierung und Ausbildung von hochqualifizierten Cybersicherheitsexperten ist derzeit etwas erschwert, da mit der Umsetzung der Vorhabensabsicht erforderliche Planstellen noch auf sich warten lassen.

Übungen und kontinuierliche Verbesserung

Nichtsdestotrotz haben die Experten des MilCyZ große Leistungen vollbracht und waren etwa auch im Rahmen der Großübung „SCHUTZSCHILD 2024" zweimal im Einsatz um das Bewusstsein für die Domäne Cyber bei der Truppe zu stärken. Auch Teilnahmen an internationalen Übungen im Rahmen PESCO CRRT wurden erfolgreich absolviert. Diese Übungen simulieren reale Bedrohungsszenarien und bieten eine wertvolle Gelegenheit, die Reaktionsfähigkeit und technischen Kompetenzen des CRRT-Teams zu verbessern.

Durch die Teilnahme an solchen Übungen stellt das Österreichische Bundesheer sicher, dass es jederzeit auf den neuesten Stand der Technik und Taktik vorbereitet ist und mit seinen internationalen Partnern effektiv zusammenarbeiten kann.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Zusammengefasst stärkt die Mitgliedschaft im EU PESCO CRRT nicht nur die Fähigkeit des Österreichischen Bundesheeres, auf Cyberangriffe schnell und gezielt zu reagieren, sondern fördert auch die europäische Zusammenarbeit in der Cybersicherheit. Qualifiziertes Personal und moderne Ausrüstung bleiben dabei die entscheidenden Faktoren für den Erfolg dieser wichtigen Aufgaben.

MIC24

Die Cyberübung „MIC 2024" (milCERT Interoperability Conference) ist ein bedeutendes internationales Event, das auf die Förderung der Zusammenarbeit und Interoperabilität der militärischen CERTs (Computer Emergency Response Teams) innerhalb der EU ausgerichtet ist. Diese Übung, organisiert von der Europäischen Verteidigungsagentur (EDA), bringt Experten aus dem Militär, um gemeinsam auf Cyberbedrohungen zu reagieren und ihre Reaktionsstrategien zu testen. Im Jahr 2024 nahm Österreich erneut an der MIC teil, um seine Cybersicherheitsfähigkeiten in einem internationalen Kontext weiter zu stärken.

Dabei besteht die Übung aus einem technischen Anteil, bei dem in realitätsnahen Szenarien verschiedene Cyberangriffe erkannt und gemeldet werden müssen. Ein zentrales Element war die Kommunikation und der Informationsaustausch zwischen den verschiedenen CERTs, um eine koordinierte und effiziente Antwort auf die Bedrohungen zu gewährleisten.

Grafik: Bundesheer/Dion6, Cyber Range

Neben dem technischen Anteil gibt es kurz darauf folgend einen operativen Anteil, bei dem sich die Leiter der milCERTs austauschen und gemeinsam die Herausforderungen auf Leiterebene besprechen. Auch nationale Strukturen werden verglichen um Best Practices für die Behandlung von Cybervorfällen zu identifizieren. Durch die Übungsserie sollen Anforderungen für das sogenannte MICNET zur permanenten Zusammenarbeit evaluiert werden.

Damit soll eine Austauschplattform etabliert werden, um im täglichen Leben der milCERTs der EU eine Erleichterung zur Zusammenarbeit und den relevanten Datenaustausch zu gewährleisten.

Durch die Teilnahme an „MIC 2024" konnte Österreich nicht nur seine eigene Cyberabwehr stärken, sondern auch zur Weiterentwicklung der europäischen Cybersicherheitsarchitektur beitragen. Die Übung verdeutlichte die Bedeutung von Kooperation und interdisziplinärem Austausch in der heutigen vernetzten Welt, um Cyberbedrohungen effektiv zu begegnen.

Foto: Bundesheer/Dion6

Cyber Range

Im vergangenen Jahr konnten wichtige erste Schritte bei der Einführung einer Cyber Range Umgebung des ÖBH getätigt werden. Mit zunehmenden technologischen Fortschritten, stehen militärische Organisationen mehr und mehr vor der Herausforderung, sich auf die stetig wachsende Bedrohungen vorzubereiten. Zur Bewältigung dieser, ist die Einführung von militärischen Cyber Ranges – hochspezialisierte Trainings- und Simulationsumgebungen, welche es ermöglichen, Fähigkeiten im Umgang mit Cyberbedrohungen zu verbessern und sich auf mögliche Szenarien vorzubereiten.

Mit der Teilnahme an diversen Forschungs- und Arbeitsgruppen konnten die Bedarfe Österreichs in diesem Feld für die Kooperation mit internationalen Partnern eingebracht werden.

Hierbei konnten wichtige Erkenntnisse für die Implementierung der eigenen Cyber Range gewonnen werden und zusätzlich konnte sich das Österreichische Bundesheer als verlässlicher Partner in diesem Bereich etablieren.

Für die Cyber Range ÖBH gibt es mittlerweile neben einem Umsetzungs- und Implementierungskonzept zusätzlich laufende Beschaffungen, um einen IOC zeitnahe sicherstellen zu können. Zudem ist neben der Unterstützung für IT Systeme die Einbindung von KT, ELOKA und OT in Vorbereitung. Die notwen-

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

digen Fähigkeiten in diesen Bereichen konnten neben einem intensiven Knowledge Transfer durch unsere langjährige Partnernation ESTLAND auch durch die laufende Unterstützung verschiedener Übungsvorhaben durch das MilCyZ erworben und gefestigt werden. Zudem konnte die Kooperation mit unserem State Partner USA/VERMONT bei einem Besuch der National Guard Cyber Range vertieft und gefestigt werden. Im vergangenen Jahr wurden zudem einige Übungsvorhaben in der Organisation und Planung unterstützt. Besonders sind hierbei die Teilnahme an der Übungsorganisation bei der „LOCKED SHIELDS" und der „SCHUTZSCHILD" hervorzuheben. Durch den Einsatz der Kräfte des MilCyZ konnten hierbei zentrale Übungsszenarien vorbereitet und durchgeführt werden. Insbesondere konnte während der Schutzschild 24 die Cyberdomäne erstmalig bei einer Großübung in ÖSTERREICH einbezogen werden.

Die Umsetzung der Cyber Range des ÖBH ist daher ein wichtiger Teil moderner Streitkräfte und zentraler Bestandteil für die holistische Cyberverteidigung Österreichs. Im vergangenen Jahr konnten diverse Herausforderungen bewältigt und die Position Österreichs im internationalen Umfeld nachhaltig gefestigt werden. Das MilCyZ ist daher weiterhin mit Nachdruck an der Implementierung einer zentralen Cyber Range Umgebung für das ÖBH befasst und unterstützt laufend die Organisation und Planung von div. Übungsvorhaben im Bereich der Cyberdomäne.

Sicherheitskonzepte und Informationssicherheit

Im vergangenen Jahr wurden die Fähigkeiten zur Ausarbeitung systemspezifischer Sicherheitsanforderungen neu auf die Herausforderungen der militärischen Einsatzumgebung ausgerichtet. Durch Erkenntnisse aus aktuellen internationalen Konflikten, ist auch für das Österreichische Bundesheer der Bedarf gegeben, sich diesen neuen Herausforderungen und Bedrohungen zu stellen und IKT-, OT-Systeme und IT-gestützte Waffensysteme dahingehend anzupassen. Eine Stärkung der IKT-Architektur im Einsatzraum bei Systemen wie Beispielsweise TCN oder der Einführung PANDUR ist die Grundlage für zuverlässige und gegen Cyberangriffe resiliente Systeme und damit eine Voraussetzung für die erfolgreiche Einsatzbereitschaft im

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Zuge der Führungsunterstützung. Die aufwändigen Beitragsleistungen in der Konzeption der durch die Dion6 zu entwickelnden Systeme, führen zu einem einheitlichen Gesamtbild der IKT-Sicherheitsarchitektur und ermöglichen somit die effiziente Entwicklung neuer Systeme und Services, in denen Sicherheit von Anfang an bereits geplant und integriert ist.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Die durch Sicherheitsexperten mittels Penetration Testing und Complience Checks durchgeführten Überprüfungen, Akkreditierungen und sicherheitstechnischen Abnahmen der IKT-Systeme des ÖBH haben auch im vergangenen Jahr wieder dazu beigetragen zahlreiche Sicherheitslücken und Gefährdungen aufzudecken und deren Behebung zu veranlassen, um damit die Verteidigungsfähigkeit der Systeme zu stärken. Dabei konnten unsere Experten neue kritische Sicherheitslücken selbst in weltweit von anderen Armeen bereits eingesetzten Produkten auffinden. In enger Zusammenarbeit mit den Herstellern wurden Lösungen ausgearbeitet um im militärischen Eigeninteresse diese Sicherheitslücken zu beheben und so die resilient militärischer Systeme zu erhöhen.

Multinationale Kooperation in der Elektronischen Kampfführung

Im österreichischen Bundesheer werden militärische Maßnahmen unter Ausnutzung der elektromagnetischen Strahlung unter der Verwendung der Bezeichnung und der gleichnamigen Waffengattung „Elektronische Kampfführung“ (EloKa) zusammengefasst. Die englisch Bezeichnung lautet „Electronic Warfare“ (EW).

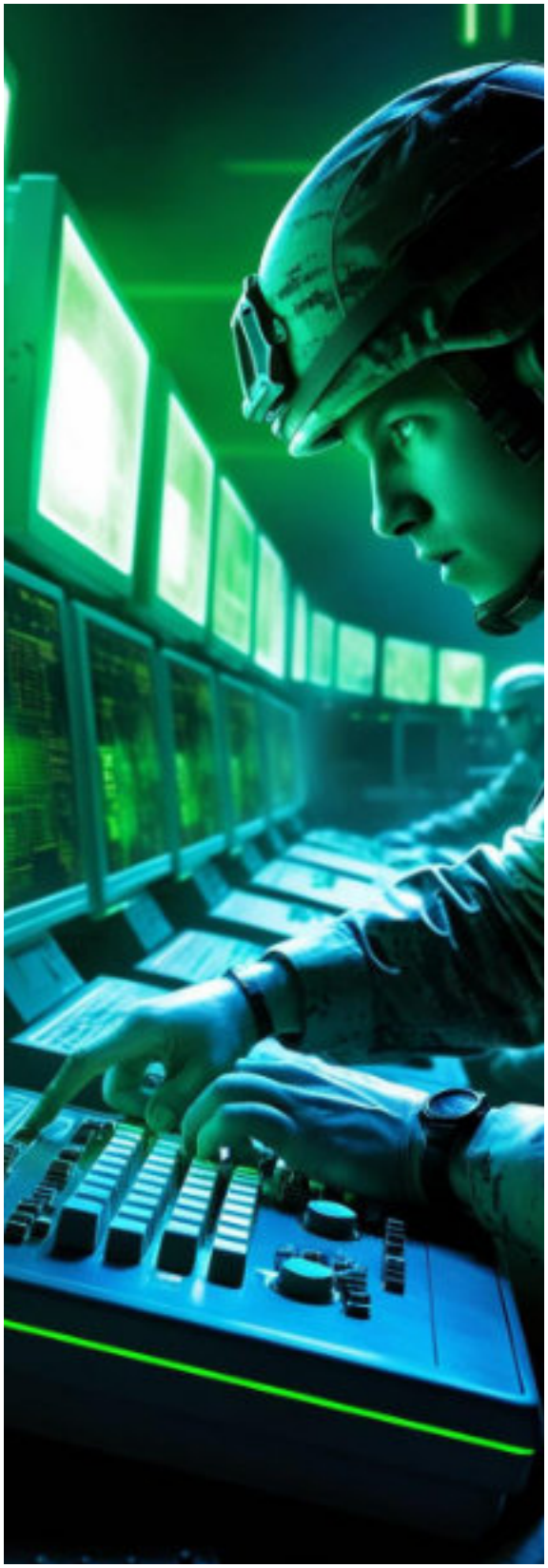
Neben nationalen Anstrengungen beteiligt sich ÖSTERREICH auch an internationalen Aktivitäten, um unter anderem eine bestmögliche Wirksamkeit gegen weltweit in Einsatzräumen verwendete Bedrohungen zu erreichen.

Konkret geschieht dies mit einer multinationalen Kooperation als Partnernation in zwei Arbeitsgruppen der "Aerospace Capability Group 3 on Survivability" in der "NATO Air Force Armaments Group".

Die Sub-Group 1 "NATO Electromagnetic Countermeasures for Force Protection Countering Small Unmanned Radio Frequency Threats Covering Land, Sea, Air Domain" beschäftigt sich mit der Verbesserung der Fähigkeiten und der Kompatibilität im Bereich der Hochfrequenztechnik für Gegenmaßnahmen gegen kleine, funkferngesteuerte unbemannte Systeme und funkferngesteuerte improvisierte Sprengkörper.

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, dem vertieften Kennenlernen von Baugruppen, Übertragungsverfahren und deren Beeinflussungsmöglichkeiten und in diesem Jahr durch Österreich erstmals der Signalanalyse zur weiteren Bedrohungsanalyse.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6



Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Heuer nahm zum dritten Mal eine österreichische Delegation von technischem EloKa-Fachpersonal des Unterstützungszentrums EloKa (UZEloKa) des Militärischen Cyber-Zentrums an der WDO 2024 in SCHWEDEN teil. Im September 2024 waren insgesamt zehn Nationen (AUSTRALIEN, BELGIEN, DÄNEMARK DEUTSCHLAND, LUXEMBURG, NIEDERLANDE, NORWEGEN, SCHWEDEN, SPANIEN UND ÖSTERREICH) zu Gast in LINKÖPING. Neben der Teilnahme an der nächsten geplanten WDO mit österreichischem EloKa-Fachpersonal ist wieder die Durchführung einer eigenen Mess- bzw. Teststation zur Signalanalyse durch österreichische Spezialisten der Abteilung UZEloKa geplant.

Die "Sub-Group 2 on Self-Protection Measures for Joint Services Airborne Assets" beschäftigt sich mit dem Selbstschutz von Luftfahrzeugen. Das UZEloKa konnte bei der multinationalen Übung XAVER 2024 in DEUTSCHLAND gemeinsam mit den übenden Vertretern der Luftstreitkräfte einsatzrelevante Erkenntnisse gewinnen.

Die aktuellen Konflikte zeigen die laufenden und raschen Veränderungen der eingesetzten Technik am Gefechtsfeld. Es braucht die internationale Kooperation in dieser technischen Waffengattung, um auf diese Entwicklungen adäquat reagieren zu können.

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6


Foto: BMLV/HBF

IKT-Betrieb

Leiter IKTBetr:
HR Mag. Peter BINDER, MSc MSc

Mit 01. September 2024 wurde ich, HR Mag. BINDER, MMSc, fix mit der Führung des Fachbereichs IKTBetr im IKT&CySihZ betraut.

Es ist mir als langgedientem Betriebsmitarbeiter eine Ehre und ein Vergnügen die Damen und Herren des Fachbereichs in dieser Zeit des Umbruchs, der Transformation in eine neue betriebliche Zukunft zu führen.

Einerseits ist nun mit der finalen Gliederung des IKT&CySihZ ein organisatorischer Meilenstein gelegt, wie sich auch schon das kommende ÖBH, Schlagwort ÖBH 2032+, am Transformationshorizont zeigt.

Der Fachbereich IKT-Betrieb steht an der Schwelle einer großen Veränderung, es ist die Zeit des Wandels, eine Zeit voller spannender und fordernder Herausforderungen.

Eine Zeit voller Möglichkeiten, die Möglichkeit zu neuen digitalen Ufern aufzubrechen. Die digitale Transformation, unter Einbeziehung neuester Techniken, betrifft nicht nur unsere Systeme und Prozesse, sondern auch die Art, wie wir zusammenarbeiten und Mehrwert für unsere Dienststelle und das Ressort schaffen.

Diese Herausforderung sehe ich als einzigartige Chance, unsere IT-Landschaft zu optimieren, zukunftssicher zu gestalten.

Gemeinsam mit den Damen und Herren des Fachbereichs, mit den Kolleginnen und Kollegen der anderen Fachbereiche werden wir bestehende Strukturen hinterfragen, innovative Technologien einführen und die Effizienz unserer Abläufe steigern. Im Fachbereich IKT-Betrieb stehen für mich damit zwei Prinzipien unverrückbar im Fokus: Teamarbeit und Anpassungsfähigkeit.

Natürlich bringt jede Veränderung Unsicherheiten mit sich, aber ich bin überzeugt, dass wir mit einer klaren Vision und dem Engagement unserer Mitarbeiterinnen und Mitarbeiter Großes erreichen werden.

Der beste Weg in die Zukunft ist nicht sie passieren zu lassen, der beste Weg in die Zukunft ist sie zu gestalten. Ich freue mich, mit meinen Mitarbeiterinnen und Mitarbeitern diesen Weg entschlossen und mit Zuversicht zu beschreiten.

IT-Provider: Erfolgreicher Betrieb des Tactical Communications Network (TCN)

Das Jahr 2024 war geprägt von signifikanten Fortschritten und Erfolgen im Bereich der Informations- und Kommunikationstechnologie (IKT) durch den Einsatz des neuen Tactical Communications Network (TCN). Besonders die größte Übung des Jahres, SCHUTZSCHILD 24, stellte die Leistungsfähigkeit und Innovationskraft des IT-Providers eindrucksvoll unter Beweis. Nachfolgend werden die zentralen Meilensteine und Herausforderungen hervorgehoben, die im Zuge des TCN-Einsatzes gemeistert wurden.

SCHUTZSCHILD24 – Die erste großflächige Integration des TCN

Im Rahmen der SS24 wurde das TCN erstmals in einem übergreifenden Verbund eingesetzt. Das FüUB2 übernahm dabei eine Schlüsselrolle und wurde beauftragt, ein Central Network Operations Centre (CNOC) zur Steuerung und Überwachung der Teilnetze der Kampfverbände aufzubauen und zu betreiben. Das CNOC war für die Planung, Steuerung, den Betrieb sowie die Überwachung der Verbindungen zwischen Übungsleitung und nachgeordneten Dienststellen verantwortlich. Ebenso fiel der IKT-Betrieb des Übungsleitungsgefechtsstandes in den Aufgabenbereich des CNOC.

Die Benutzerbetreuung wurde durch die CNOC speziell bei Problemen unterstützt, die nicht durch den 1st Level Truppen-Betriebssupport gelöst werden konnten. Besonders herausfordernd erwiesen sich „Kinderkrankheiten" bei der Datenfunk-Übertragung und dem Tactical-Voice-Service.

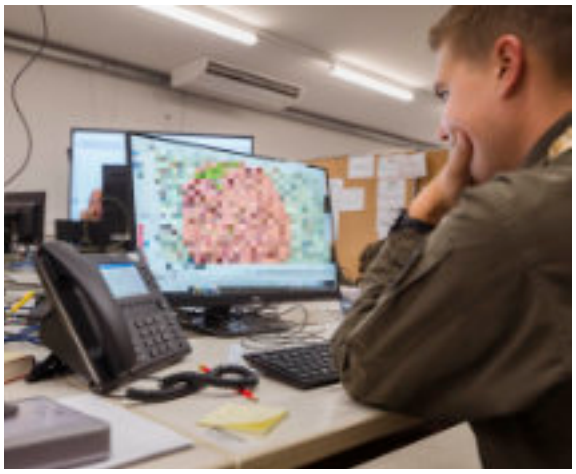


Foto: BMLV/Paul Kulec

Dank der engen Zusammenarbeit mit Technikexperten im Bereich IKT-Technik und Sprachdienste konnten diese Probleme jedoch entweder durch Workarounds oder gänzlich behoben werden. Ein weiterer Meilenstein war der Einsatz des Netzwerkmanagementsystems „Spectrum", mit dem die Netzüberwachung und der Betrieb erprobt und optimiert wurden. Diese Tests trugen wesentlich dazu bei, den Betrieb des TCN zu stabilisieren und zu verbessern.

Wertvolle Erkenntnisse durch Einsätze

Der Einsatz des TCN im Rahmen der Übung SS24 brachte eine Fülle an praktischen Erfahrungen, die die Netzbetriebsplanung, die Betriebsführung und den technischen Support nachhaltig verbesserten. Insbesondere im Bereich Server, Netzwerke und Sprachdienste wurden entscheidende Erkenntnisse gewonnen, die für zukünftige Einsätze genutzt werden können.

Herausforderungen und Lösungsansätze

Die Einführung eines neuen Kommunikationsnetzwerks bringt stets technologische und organisatorische Herausforderungen mit sich. So galt es beispielsweise, die Datenfunk-Übertragung und den Tactical-Voice-Service zu stabilisieren. Diese Aufgaben wurden mit hoher Priorität bearbeitet, um die Funktionsfähigkeit des Netzwerks sicherzustellen.

Der IKT-Support wurde im Rahmen der weiteren Übungen der Truppe zunehmend dezentralisiert. Hierbei war es das Ziel, den TCN-IKT-Support über die Betriebsführung der Truppe selbstständig abzuwickeln:

- 1st Level: Betreuung durch die Bataillone
- 2nd Level: Support auf Brigadeebene
- 1st Level 2nd Line: Unterstützung durch die Benutzerbetreuung IT-West

Personal im Einsatz

Die Übung SS24 erstreckte sich über drei Wochen, in denen ein Mitarbeiter durchgehend und sechs weitere Mitarbeiter der Benutzerbetreuung abwechselnd an der TherMilAk in Wiener Neustadt eingesetzt waren. Diese Einsätze forderten eine hohe Flexibilität und Expertise, um den Betrieb reibungslos zu gewährleisten.

Kontinuierliche Verbesserung durch praktische Erfahrungen

Mit jeder weiteren Übung und jedem Einsatz, wie beispielsweise die DAEDALUS24, kann das Personal zusätzliche Erfahrungen sammeln, die den Betrieb des TCN weiter verbessern. Das stetige Lernen und Anpassen der Prozesse sorgte dafür, dass sowohl die Effizienz als auch die Stabilität des Netzwerks stetig zunahmen.

Ausblick und Weiterentwicklung

Die Übungen und Einsätze im Jahr 2024 haben gezeigt, dass das Tactical Communications Network eine wesentliche Rolle in der modernen Kommunikationstechnologie der Truppe spielt. Durch die gesammelten Erfahrungen und kontinuierlichen Verbesserungen wird das TCN künftig noch effizienter eingesetzt werden können.

Die Zusammenarbeit zwischen den verschiedenen Einheiten, die Integration neuer Technologien und die Bewältigung von Herausforderungen haben nicht nur den Betrieb des TCN auf ein neues Niveau gehoben, sondern auch die Expertise des IT-Providers eindrucksvoll unter Beweis gestellt. Der Leistungsbericht 2024 zeigt klar: Die Weichen für eine zukunftsfähige und stabile IKT-Infrastruktur sind gestellt.

Serverrollout 2024

Ablauf

Das Jahr 2024 ist für die Benutzerbetreuungen in WIEN, SALZBURG und GRAZ ganz im Zeichen der Serverablöse gestanden. Die schon in die Jahre gekommenen Liegenschaft-Server wurden planmäßig durch die neuen, wesentlich leistungsstärkeren Server ersetzt.

Hierbei ist nicht nur die bessere Prozessorleistung hervorzuheben, sondern vor allem die schnellere Netzwerkanbindung. Der Speicherplatz, welcher ebenfalls nicht mehr ganz zeitgemäß dimensioniert und permanent übervoll war, ist nun ausreichend dimensioniert und wird für die nächsten Jahre ausreichen, mit der Option diesen im Bedarfsfall zu erweitern.

Das Rollout wurde regional durch die Serverspezialisten der jeweiligen Benutzerbetreuungen in enger Zusammenarbeit mit den lokalen Liegenschaft-Leitbedienern koordiniert. Die logistische Anlieferung gestaltete sich aufgrund der unterschiedlichen Aufstellungsorte (z.B. Serverrack im 1. od. 2. Stock eines Gebäudes) mitunter ziemlich schwierig. Die Installation und der Einbau der Hardware wurde mit Unterstützung von IKT-Service/HLogZ vor Ort durchgeführt, der Klon der Server erfolgte dann durch die Benutzerbetreuungen. Hierbei ist dem Referat „Systementwicklung 2. VE“ großer Dank für die Entwicklung des Klons und der Automatismen auszusprechen, wodurch die Klonzeit und auch die mögliche Fehlerquote durch viele manuelle Interaktionen minimiert bzw. sogar eliminiert wurde. Nach einem anschließenden erfolgreichen Datensync wurden die alten Server heruntergefahren und der neue Server produktiv gestellt.

So wurden in der Zeit von April bis September sämtliche Liegenschaft-Server im In- und Ausland abgelöst. In Zahlen ausgedrückt sprechen wir hier von insgesamt 180 physischen Servern, auf welchen 245 Liegenschaft-Server virtualisiert im Einsatz sind.

Bei den neuen Servern wird auf Virtualisierung gesetzt, was eine einfachere Administration in Bezug auf Startzeiten mit sich bringt. Ebenso wird die Speicherplatzverwaltung und Erweiterbarkeit derselben vereinfacht. Der wirklich große Vorteil ist aber, dass es nun möglich ist, mehrere Liegenschaft-Server, sogenannte Instanzen, auf ein und der selben Serverhardware parallel laufen zu lassen, womit es auch zu einer Reduktion der benötigten physischen Hardware kommt.

Gleichzeitig mit der Installation der neuen Liegenschaftsserver wurden die netzwerktechnisch vorangestellten Switches auf die neueste Generation ausgetauscht, wodurch die Anbindung der Server über die beiden 10gbit-Interfaces (SFP+) möglich ist und der praktische Datendurchsatz dadurch erheblich ansteigt.

Zusammengefasst kann man sagen, dass für die User die Downtime, also der Arbeitsausfall bedingt durch die Umstellung gegen Null tendierte.

Die neue, schnellere, größer und zukunftsweisend orientierte Speicherplatzdimensionierung wirkt sich positiv auf das Benutzererlebnis bzw. die Arbeitsmotivation aus. Aus Sicht der Benutzerbetreuung ist nicht nur das Arbeiten mit aktueller Hard- und Software interessant(er), sondern auch die Zuverlässigkeit und die damit verbundene Firmengarantie eine positive Entwicklung und ein Muss für eine zeitgemäße Benutzerbetreuung im Sinne des schnellen und dabei immer freundlichen Supports.

Leitsysteme im BMLV

Mitte der 90er Jahre, wurde das verlegbare und ortsfeste Kommunikationssystem IFMIN, mit entsprechend ausgebauter Infrastruktur angekauft, aufgebaut und eingeführt. Für die Sicherstellung der Verfügbarkeit wurde parallel dazu ein Leitsystem zur Überwachung und Steuerung der Kommunikationssysteme, Fernmeldenetze und der ortsfesten Infrastruktur implementiert.

Gefahren Melde und Fern Wirk System (GMFWS)

Das Leitsystem GMFWS wurde nach dem Aufbau von IFMIN auch in allen anderen Liegenschaften im BMLV Bereich ausgebaut.

Die grundsätzliche Aufgabe des Systems ist:

- Informationserfassung in zu überwachenden Objekten
- Weiterleitung der Informationen an dezentrale Leitstellen unter Zuhilfenahme verschiedenster Übertragungstechnologien
- Visualisierung der Informationen in den Leitstellen
- Erfassung und Verteilung der Operatoreingaben an die zu steuernden Objekte
- Ausgabe der analogen und digitalen Steuerbefehle an die Primärtechnik in den Objekten
- Lokale, autonome Verarbeitung und Steuerung in den Objekten

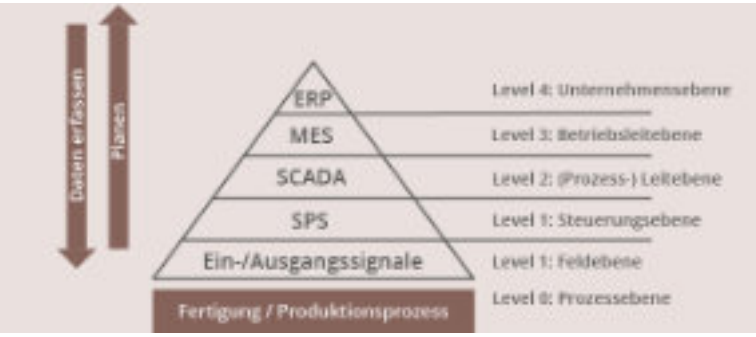
In den Leitständen, welche österreichweit verteilt sind, werden die Informationen der Primärsysteme dem Operator visualisiert, worauf er bei Abweichungen vom Normalzustand geeignete Maßnahmen über die Ferne treffen kann, um einen störungsfreien Betrieb und damit eine hohe Verfügbarkeit der Primärsysteme zu gewährleisten.

Die Überwachung und Steuerung der Systeme erfolgt durchgehend (24/7) über zwei Zentralen (Leitstände) und beinhaltet folgende Primärsysteme:

- Netzersatzanlagen (Notstromanlagen)
- Klimaanlagen
- Kommunikationssysteme (IFMIN,TKV, RV,...)
- Datennetze
- Brandmeldeanlagen
- Zutrittskontroll- und Alarmanlagen
- Niederspannungsanlagen
- USV
- Videoanlagen
- Nebenstellenanlagen

Der Aufbau der Anlagen entspricht der in der Tunnelsteuerung, Energieprovider und Industrie angewendeter Technik mit sehr hohen Sicherheitsaspekt. Um höchstmögliche Sicherheit zu gewährleisten, wurde das GMFWS netzwerkmäßig in ein autarkes Netz eingefügt, was den Zugriff von unberechtigter Stelle abwendet. Zusätzlich sind alle Verbindungen untereinander verschlüsselt, um Missbrauch vorzubeugen.

Der Aufbau eines Leitsystems erfolgt gemäß Automatisierungspyramide:



Grafik: Bundesheer/Dion6, Automatisierungspyramide Leitsystem

Bundesministerium für Landesverteidigung

Und ergibt dann folgenden Systemaufbau:

Die GMFWS Gruppe IKT-Betrieb plant, programmiert die Komponenten inkl. Visualisierung und unterstützt den IKT-Service beim Auf- und Umbau der Anlagenteile. Die Einbindung der unterschiedlichen Systeme in das Leitsystem ist zwischendurch eine Herausforderung für unsere Techniker, da keine Eingriffe bzw. Änderung in die einzubindenden Komponenten erfolgen sollen.

Davon hängt auch die Zuverlässigkeit der übertragenen Meldungen ab, die ein Höchstmaß an Verfügbarkeit gewährleisten sollen.

Im Visualisierungsserver erfolgt die Visualisierung mittels Prozessbilder. Alarme werden je nach Kategorie und Priorität in Alarmlisten ausgegeben, die vom Bedienungspersonal überwacht und abgearbeitet werden. Je nach Fehlerart müssen unterschiedliche Services zur Instandsetzung entsandt werden.

Jegliche ein- oder ausgehende Information wird in Datenbanken festgehalten, um jederzeit eine Statistik bzw. Fehlerhistorie zu erzeugen.

FMSysÖBH – BOS (Behörden und Organisationen mit Sicherheitsaufgaben)

Das BOS-AUSTRIA Netz ist innerhalb des österreichischen Bundesheeres ein fester Bestandteil in der täglichen Kommunikationslandschaft. Der tägliche Einsatz der BOS-Endgeräte ist in vielen Organisationselementen zum Standard geworden.

Die BOS-Endgeräte können gem. dem definierten TETRA-Standard auf Basis der bestehenden Infrastruktur österreichweit untereinander mit eindeutiger Rufzuordnung kommunizieren.

Durch IKT-Betrieb werden folgende Tätigkeiten innerhalb BOS-AUSTRIA wahrgenommen:

- Sicherstellung eines Sevicedesks für alle BOS-User.
- Konfiguration der BOS Endgeräte, aller eingeführten Hersteller und Einbauvarianten.
- Erstellung von Sonderkonfigruationen für diverse Organisationen.
- Erprobung von Spezialzubehör für unterschiedliche Hersteller.
- Enge Zusammenarbeit mit dem Betreiber BOS-AUSTRIA.

Eine besondere Herausforderung war die Planung und die Durchführung des Betriebes für die AIRPOWER 2024 in ZELTWEG. Auf Grund der hohen Anzahl an Organisationen und Endgeräten vor Ort, wurden die Sendeeinrichtungen im Umfeld der AIRPOWER 2024 verstärkt und umgebaut. Eine besondere Herausforderung war das Monitoring und die Optimierung in enger Zusammenarbeit mit dem Betreiber BOS-AUSTRIA.

Das Jahr 2024 war ebenfalls geprägt von Änderungen in den jeweiligen Organisationen und die Anpassung der Kommunikationsstrukturen im BOS-AUSTRIA Netz für die neuen Strukturen. Diese laufenden Änderungen, müssen an alle BOS-Endgeräte übertragen werden, um die reibungslose Kommunikation innerhalb des Bundesheeres zu gewährleisten. Zusätzlich werden die Versorgungskarten der Netzabdeckung in Zusammenarbeit mit dem

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Betreiber BOS-AUSTRIA durch IKT-Betrieb aufbereitet und über die festgelegten Kommunikationswege verteilt, um die Einsatzbereitschaft und die Planungsgrundlagen für die Kommunikation bereitzustellen.

Bei unzureichender Netzversorgung innerhalb einer militärischen Liegenschaft, wurde durch IKT-Betrieb gemeinsam mit dem Betreiber (BOS AUSTRIA), Netzmessungen und Dokumentationen angefertigt und anschließend einer Netzoptimierung zugeführt. Somit konnte die Versorgungssicherheit und Erreichbarkeit im BOS-AUSTRIA Netz stabilisiert und erhöht werden.

IKT-Betrieb führte, gemeinsam mit zivilen Firmen, Testungen von verschiedenen Audio-Komponenten durch, um die Erfordernisse der Einsatzorganisation oder spezielle Einsatzkräfte bei der Auswahl und Konfiguration der richtigen Audio-Devices zu unterstützen.

Im Jahr 2024 wurden durch das BMLV etliche, neue BOS-Endgeräte beschafft. IKT-Betrieb bearbeitet alle technischen Maßnahmen im Rahmen des Implementierungsprozesses um die Geräte dem Regelbetrieb und dadurch dem Bedarfsträger übergeben zu können.

Der Implementierungsprozess beginnt bei logistischen Maßnahmen, der Konfiguration und der Dokumentation der BOS-Endgeräte.

IKT-Betrieb stellte im Jahr 2024, trotz mangelnder Bearbeitungskapazität und Ressourcen, den Betrieb des BOS-AUSTRIA Netzes in hervorragender Qualität sicher und ist somit ein fester Bestandteil der militärischen Kommunikationslandschaft im österreichischen Bundesheer.

IKTBetr/BetrFü/BetrFüKT

IKT-Unterstützung

Im Bereich IKT-Betrieb ist die Abteilung Betriebsführung verantwortlich für die Systemorganisation und den ordnungsgemäßen Betrieb der zentralen IKT-Infrastruktur, sowie des ortsfesten Fernmeldesystems des Österreichischen Bundesheers (ofFMSysÖBH).

Die Abteilung Betriebsführung koordiniert, steuert und überwacht bei Übungen und Einsätzen des ÖBH die Einbindung der verlegbaren IKT-Truppensysteme in betrieblichen Belangen und stellt nach der Einbindung die Nutzung der IKT-Services für selbige sicher.

Zur Steuerung und Überwachung des ofFMSysÖBH und insbesondere der Schnittstellen zum vlgbFMSys, wird in der Abteilung Betriebsführung das funktionale Element der „Systemsteuerung" gebildet.

Die Systemsteuerung setzt sich aus den für die jeweiligen Teilsysteme des FMSysÖBH zuständigen Systemingenieure (SysIng), sowie die für den operationellen Betrieb verantwortlichen Funktionen in der Betriebsführungs- und –überwachungszentrale (BÜZ) zusammen. Die BÜZ ist georedundant an 2 Standorten ausgeführt.

Bei bedeutenden Vorhaben, wird von der Systemsteuerung zusätzlich benötigter Support, von den Bereichen des IKT&CySihZ und von heereseigenen Instandsetzungskräften, von HLogZ/IKTService sowie von LRÜ/TLZ angefordert.

Die Systemsteuerung stellt im Rahmen der Einbindung verlegbarer

Foto: Bundesheer/Dion6, BOS-Endgerät

Komponenten in das ofFMSysÖBH bei Übungen und Einsätzen die IKT-Unterstützung für die Truppe sicher. Der IT-Support für die verlegbaren Vermittlungseinheiten wird durch das Referat BenBeITW der AbtBenBetr wahrgenommen, welches auch bei Bedarf vorort Unterstützung bei der Truppe leistet. Durch das Personal der BenBeITW wird auch die Funktion des SysIng IT als Teil der Systemsteuerung bekleidet.

Die Luftraumsicherungsoperation DAEDALUS24 wurde unter Abstützung auf das ofFMSys erstmals mit TCN-Komponenten im vlgb Bereich abgedeckt. Das Tactical Communication Network (TCN) ist ein militärisches IP basierendes IKT-System (inkl. Sprachservice) und stellt die Ablöse der seit über 30 Jahren im Betrieb befindlichen Integrierten Fernmeldeinfrastruktur (IFMIN) sicher. Die Ausphasung des Systems IFMIN wurde bereits Ende 2024 begonnen und soll noch im Jahr 2025 in mehreren Phasen abgeschlossen werden. In diesem Zuge werden alle Schnittstellen von IFMIN zu anderen Systemen im ortsfesten Bereich (ortsfestes Richtverbindungsnetz, Dienstenetz, Nebenstellenverbund, zivile Provider,...) außer Betrieb genommen und auch die Hardware ordnungsgemäß abgebaut und außer Stand genommen.

Im Rahmen der DAEDALUS24 hat sich auch der Einsatz von Personal der BÜZ beim S6 bzw. bei der NOC (Network Operation Center) als Verbindungsglied zur Systemsteuerung bewährt. Gerade in der Einführungsphase des neuen Systems hilft dies wesentlich bei der Evaluierung der Betriebsabläufe speziell im Zusammenwirken zwischen S6/NOC mit der Systemsteuerung. Dies dient insbesondere beim Auftreten von Störungen zu einer Optimierung von Abläufen bei der gemeinsamen Fehlerbehebung.

Bei der Großübung SCHUTZSCHILD24 konnten weitere Erkenntnisse bei der Zusammenarbeit der Systemsteuerung mit den jeweiligen Funktionselementen der Truppe gesammelt werden.
Eine wesentliche Herausforderung stellt der Aufwuchs und die Ausbildung von neuem Personal in allen Bereichen des Betriebes der IKT-Services dar, insbesondere in den nächsten Jahren auf Grund vermehrter altersbedingter Abgänge.

Release-Unterstützung 2024

Durch gezielte Schulungen und eine enge Zusammenarbeit mit den Anwendern gewährleisten wir einen reibungslosen Betrieb. Bei komplexeren Problemen arbeiten wir eng mit den Abteilungen Materialwirtschaft und Logistik-Applikationen zusammen.

Im Jahr 2024 unterstützten wir bei den beiden großen Releases Mitte und Ende des Jahres und trugen maßgeblich zur erfolgreichen Implementierung von Verbesserungen bei.

Ausblick 2025

Für das Jahr 2025 erwarten wir auf Grund der flächendeckenden Umsetzung der Ist-Gerätestrukturen von:

- IKT-Gerät (TCN, TKV)
- Waffen (MP90, STG77A1 NF, MG74) und
- Gefechtsfahrzeugen (Dingo, EVO PANDUR, HÄGGLUNDS)

mit einem gesteigerten Supportbedarf.

Die Umstellung auf die „Neue Technologie“ wird weiter vorangetrieben, hier stehen die Bereiche Materialstammdaten sowie die Verwaltung von Dokumenten und Organisationseinheiten auf dem Programm. Mobilität und Kommunikation sind elementare militärische Bedürfnisse, aus denen sich ein zunehmender Bedarf an „mobiler Kommunikation“ im militärischen Alltag ableitet.

Diesem Bedarf wird im IKT-Bereich derzeit unter anderem durch Services wie SMN-Mobile, mobile Endgeräte (Notebooks), Satelliten-Internet, WLAN, Webmail sowie mobile Sprach- und Datendienste (mit und ohne Sprachverschlüsselung) entsprochen.

Aktuell sind mehr als 2.000 Angehörige des BMLV/ÖBH mit Smartphones der neuesten Generation ausgestattet. Die Anzahl der eingesetzten Geräte wird sich 2025 auf etwa 4.000 Geräte verdoppeln. Diese Smartphones sind so im SMN (sicheres militärisches Netzwerk – vormals 3. VE) integriert, dass jeder Smartphone-Anwender Zugriff auf seine Informationen aus dem Mail-und Terminmanagement hat.

Darüber hinaus sind dienstlich relevante Apps vorinstalliert und kann die Freigabe weiterer Apps bei nachweislich dienstlichem Bedarf beantragt werden. Die eingesetzten Smartphones werden mittels MDM (Mobile-Device-Management) zentral verwaltet und von den Service-Schwerpunkten INTERNET und MTM (zukünftig zusammengefasst im Service-Schwerpunkt „Mobile Kommunikation") administriert, überwacht und die Anwender technisch und betrieblich unterstützt.

Etwa ein Viertel der Smartphones ist mit verschlüsselter Sprachtelefonie auf Basis einer App ausgestattet und ermöglicht den Anwendern, eine abhörsichere Kommunikation untereinander. Administration und (technische) Unterstützung der aktuell ca. 1.250 Anwender sind ebenfalls bei IKT-Betrieb angesiedelt.

Was die derzeit in Betrieb befindlichen mobilen Internet-Endgeräte (Internet-Notebooks mit mobilem Datenzugang über WLAN, Datenstick oder mobile Router) betrifft, steht ebenfalls ein Technologiewechsel bevor. Internetfähige Endgeräte welche aktuell mit dem BMLV-Universalclone ausgestattet sind, werden 2025 durch DGMN-Geräte (Dynamisch gesichertes militärisches Netzwerk) abgelöst, der Support für alle internetfähigen Endgeräte verschiebt sich vom Bereich Applikationen in den Bereich IKT-Betrieb und wird auch zukünftig von gewohnter Stelle (Standort Innsbruck) wahrgenommen.

Zur Sicherstellung von E-Mail-Kommunikation „aus der Bewegung" steht das BMLV-Webmail-Portal zur Verfügung. Es bietet die Möglichkeit, jederzeit, von überall und über verschiedenste Plattformen (PC, Notebook, Tablet, Smartphone, ...) auf seine Nachrichten zuzugreifen. Zur Verhinderung unautorisierter Zugriffe wurde das BMLV-Webmail um die Funktion MFA (Multi-Faktor-Authentifizierung) erweitert. Auftragsgemäß steht BMLV-Webmail mittlerweile auch definierten Funktionen aus der Miliz zur Verfügung.

Zum Selbst- und Fremdschutz werden alle einlangenden und ausgehenden E-Mails durch zahlreiche Systeme im Hintergrund und ohne Zutun der Anwender auf Malware überprüft. Eine der Instanzen, mit der Anwender am ehesten in Berührung kommen ist MAVE, ein System welches verdächtige Inhalte aus Nachrichten ausfiltert und betroffene Anwender automatisch informiert. Bei Bedarf besteht dann die Möglichkeit einer manuellen Zweitprüfung (und ggf. Freigabe) durch den zuständigen Support.

WLAN hat sich mittlerweile zu einem häufig genützten und unverzichtbaren Service entwickelt. Der Einsatz von WLAN im BMLV/ÖBH umfasst unter anderem die Bereitstellung von Internet für Rekruten (Sozial-Internet), Internetanbindung von Endgeräten über mobile Router, Sonderfälle in denen Festnetz-Internet aus technischen, sicherheitstechnischen oder wirtschaftlichen Gründen nicht eingesetzt werden kann, soziale Kommunikation via Internet im Rahmen von Auslandseinsätzen (z.B. UNIFIL/LIBANON) oder die Unterstützung nationaler und internationaler Übungen, Veranstaltungen und Konferenzen durch Beistellung und Support von WLAN Services.

Im Rahmen von Auslandseinsätzen und (internationalen) Übungen kommt zunehmend Internet via Satellit zum Einsatz. Benutzerunterstützung und Support für SAT-Internet und weitere Services wie SMN-Mobile runden das Portfolio des IKT-Betrieb in Hinblick auf mobile Kommunikation ab.

SSP IT EF (Service Schwerpunkt Eurofighter)

Rückblick 2024

Das Jahr 2024 war für den Service Schwerpunkt Eurofighter wieder ein überaus erfolgreiches Jahr. Ist doch das Team um Oberst FISCHER im Fachbereich IKT-Betrieb ein unverzichtbarer Teil der Eurofighter-Erfolgsgeschichte. Hier wird seit der Eurofighter-Einführung der Ground-Support wahrgenommen und effizient, egal wo die Eurofighter zum Einsatz kommen, umgesetzt. Der herausforderndste Einsatz 2024 war sicherlich das EFT Luftzielschießen in Italien. Der Service Schwerpunkt Eurofighter unterstützte den Einsatz durch die Bereitstellung einer Rückwärts-Anbindung zwischen der italienischen Air Base und Zeltweg. Damit wurde sichergestellt, dass auch bei einer erforderlichen alternativen Landung der Betrieb des Eurofighter-Systems reibungslos fortgeführt werden konnte.

Foto: Bundesheer/Dion6

Ausblick 2025:

2025 wird das Jahr sein, in dem der österreiche Eurofighter seine 20 000 Flugstunde absolviert. Ein Meilenstein, der auch die Leistungen des SSP EF zum Ausdruck bringt. Ebenso gibt es wieder eine neue Auslandsherausforderung. In der zweiten Jahreshälfte 2025 findet in Portugal eine NATO-Übung statt, bei welcher der SSP wieder eine Rückwärts-Anbindung nach Österreich konfigurieren wird. Zudem wird auch eine vollständige Netzwerkinfrastruktur vor Ort konfiguriert und betrieben, um den Einsatz des Systems optimal zu unterstützen. Mit bewährter Expertise blickt das Team dieser und allen weiteren Aufgaben optimistisch entgegen.

First-Level Support ELAK

Die First-Level-Supportabteilung von ELAK ist das Rückgrat der täglichen IT-Unterstützung für rund 15.000 Benutzer in ganz ÖSTERREICH. Mit einer beeindruckenden Erstlösungsrate von 95 % leistet das Team einen wesentlichen Beitrag zur Sicherstellung eines reibungslosen Betriebs der Applikation.

Herausforderungen 2024

Besonders herausfordernd sind die jährlichen großen Updates, die den Supportaufwand für zwei bis vier Tage nahezu verdoppeln. Trotz dieser Belastung und einer personellen Unterbesetzung hat das Team im Jahr 2024 alle Herausforderungen souverän gemeistert.

Beeindruckende Umfrageergebnisse

Die Ergebnisse der österreichweiten Qualitätsumfrage des 2nd Level Supports unterstreichen die hervorragende Arbeit des First-Level-Teams: Die Benutzer loben insbesondere die hohe Kompetenz und Freundlichkeit der Supportmitarbeiterinnen und Mitarbeiter.

Ausblick 2025

Mit diesem Rückhalt und bewährtem Engagement blickt die Abteilung optimistisch auf die Herausforderungen des Jahres 2025, um weiterhin einen erstklassigen Service zu bieten.

Foto: Bundesheer/Dion6

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Bundesministerium für Landesverteidigung


Foto: BMLV/HBF

Institut für Militärisches Geowesen

Leiter IMG: ObstdhmtD Mag. Dr. Tamino EDER, MBA

Das Jahr 2024 hat den Fachdienst MilGeo bzw. das Institut für Militärisches Geowesen (IMG) sowohl inhaltlich als auch formal in bedeutender Weise vorangebracht und damit die Unterstützungsfähigkeiten des hochspeziellen Fachdienstes für das Ressort massiv verbessert.

Formal wurde im Zuge der Reorganisation der Direktion 6 - IKT und Cyber die Führung des Fachdienstes MilGeo unter der Leitung des IMG hergestellt. Damit wurde eine den Führungsgrundsätzen entsprechenden „Einheit der Führung" im Fachdienst implementiert.

Organisatorisch wurden dem IMG zwei zusätzliche Arbeitsplätze zugeordnet. Einerseits wurde aus der ehemaligen FüU eine Planstelle für strategische bzw. internationale Agenden übergeleitet und andererseits konnte ein Arbeitsplatz Militärgeologie für eine bisher bestandene Fähigkeitslücke am IMG geschaffen werden. Als Service Provider kann das IMG ab jetzt auch den steigenden Bedarf an bodenkundlichen, petrologischen sowie hydrologischen Analysen/Auswertungen im ÖBH wie auch in der Heeresverwaltung decken.

Der organisatorische Aufbau am IMG ist aber damit noch nicht abgeschlossen, denn im Jahr 2024 wurde durch die Erstellung eines neuen Konzeptentwurfes „MilGeowesen 2.0" der Aufbau eines neuen Referates „Space-Based Earth Observation" (SBEO) entworfen. Im Zuge des Aufbauplanes 2032+ sollte auch diese Fähigkeitslücke geschlossen werden.

Die Wichtigkeit der militärischen Nutzung von Satellitenbildern und deren Auswertung ist unumstritten und wird durch deren leichte Verfügbarkeit, vermehrt auch von hochqualitativen Aufnahmen, derer noch mehr an Bedeutung gewinnen.

Aufgrund der geänderten sicherheitspolitischen Rahmenbedingungen bzw. der Ausrichtung des ÖBH an das moderne Gefechtsfeld hat sich auch der MilGeo-Dienst weiterentwickelt. Nachdem der Fachbereich MilGeo im internationalen Umfeld für gewöhnlich dem Führungsgrundgebiet 2 zugeordnet ist, orientieren sich die Prozessabläufe bei der Auftragsbearbeitung am sogenannten „Intel-Cycle", welcher die Schritte Tasking, Collection, Processing und Dissemination umfasst.

Das IMG ist durch seine fachliche Expertise, moderne Technologien und optimierte Prozesse bestens aufgestellt, um als zentraler Service Provider für Geoinformationen im ÖBH die kommenden Herausforderungen (ÖBH2032+) bewältigen zu können. Als „High Value Asset" wird das IMG daher einen essenziellen Beitrag zur Informationsüberlegenheit im Aufklärung-Führungs-Wirkungsverbund leisten.

Multinational Capability Development Campaign (MCDC)

Das IMG nahm im "Arktikum" in ROVANIEMI (FINNLAND) von 26. Februar bis 1. März 2024 am Multinational Capability Development Campaign (MCDC), Projekt "Climate Change in the Arctic: Security Implications and Military Consequences (CLIMARCSEC)" Workshop #3 teil.

Ziel war es, gemeinsam mit dem internationalen Team aus über zehn Nationen, ein Konzept zur Bewältigung der militärischen Herausforderungen in der Arktis zu konkretisieren und verbessern. Die Auswirkungen des Klimawandels führen, bis zu viermal schneller als im globalen Durchschnitt, zu starken Veränderungen in der Arktis - Fokus des Projektes ist die europäische Arktis. Das daraus folgende Aufschmelzen des Permafrostes, der dramatische Rückgang des Eisschildes und höhere Temperaturen erhöhen jetzt schon die lokale Erreichbarkeit sowohl für zivile als auch militärische Vorhaben.

CLIMARCSEC untersucht das Konfliktpotential dieser Entwicklung und erarbeitet ein Konzept für die Identifikation und Verringerung von militärischen Fähigkeitslücken. Dabei werden explizit nicht nur arktische Nationen adressiert, sondern ebenfalls indirekt betroffene Länder um zusätzlich eine Bewusstseinssteigerung des Themas „Sicherheit in der Arktis“ zu erzeugen.

Mit der Teilnahme eines Experten des IMG aus dem Bereich Militärgeologie, leistet das ÖBH einen wertvollen Projektbeitrag zur "Situational Awareness" und gewinnt dabei Know-How in der Risikoanalyse und Fähigkeitenentwicklung.

Grafik:Bundesheer/Dion6

Foto: Bundesheer/Dion6

Besuch BH GÄNSERNDORF am IMG

Am Mittwoch, dem 28. Februar 2024, besuchte eine hochrangige Delegation der Bezirkshauptmannschaft GÄNSERNDORF das IMG.

Unter der Leitung des Bezirkshauptmannes Dr. Martin STEINHAUSER nahmen weitere zehn Führungskräfte Einblick in die vielfältigen Produkte, Prozesse sowie in die eingesetzten Technologien des IMG. In Form eines Stationsbetriebes wurden den Gästen die Referate und Mitarbeiterinnen und Mitarbeiter mit deren Aufgaben im Detail vorgestellt.

Der spannende Wissensaustausch fand mit dem Vorsatz, sich bald wieder treffen zu wollen, seinen Ausklang.

QGIS Schulung bei AAB3

Von 5. bis 7. März 2024 fand im Zuge der Einsatzvorbereitung für die 50. KFOR-Rotation seitens IMG eine Softwareschulung für Kameraden der 1. AufklKp/AAB3 statt.

Bereits im März 2023 wurde seitens der Waffengattung Aufklärer Interesse an dieser Software bekundet initiiert, der zur Folge hatte, dass QGIS als sehr brauchbare Software für die tägliche Arbeit erkannt wurde und als Mehrwert für die Truppe gesehen wird.

Die Software dient zum Erfassen, Darstellen, Analysieren und Publizieren georeferenzierter Daten.

Seit der KFOR-Rotation 49 (AAB7) verwenden nun die Aufklärer im Einsatzraum diese Software um ihrer Arbeit im Zeitalter der Digitalisierung "State of the Art" nachgehen zu können.

Das Spektrum reicht von

- der Planung von Hubschrauberflügen zur Aufklärung,
- über die Planung von Einsätzen der Spähaufklärung,
- dem Erstellen von Geodaten für die im Einsatz verwendeten GPS-Geräte,
- das rasche Erstellen von hochwertigen Kartenmaterial für den Eigenbedarf, Geländemodellen und Oberflächenmodellen
- dem Georeferenzieren von Luftbildern,
- dem räumlichen Darstellen von Aufklärungsergebnissen (Erstellen von Geo-Datenbanken)
- bis hin zum Erstellen von hochauflösenden 3D Modellen für Befehlsausgaben und Einsatznachbesprechungen.

All diese Geodaten und Produkte können einfach und effizient mit all den Bedarfsträgern innerhalb der Kompanie analog und digital geteilt bzw. weiterbearbeitet werden.

So können diverse RECCE Aufträge mittels QGIS geplant werden sowie die Zwischenergebnisse räumlich aufgearbeitet und das Endergebnis in die im Einsatzraum verfügbaren Systeme eingearbeitet werden.

Foto: Bundesheer/Dion6

3D-Modellierung des Grazer Schloßbergs

Im Kontext der Übung SCHUTZSCHILD 24 wurde in Zusammenarbeit mit der Vermessungsabteilung der Direktion 7 - Militärisches Immobilienmanagementzentrum das Stollensystem des Grazer Schloßbergs aufgenommen und für die 3D-Darstellung in Virtual Reality und BORIS aufbereitet.

Das 3D-Modell soll in der Beurteilung der Umfeldbedingungen den Stab speziell hinsichtlich der Strukturen unter der Oberfläche eines urbanen Raumes sensibilisieren und den Blick auf den Einsatzraum komplettieren.

Die Vermessung erfolgte primär mittels Laserscanner auf Stativ und einem hochmobilen Hand-Laserscanner. Zur Stabilisierung der einzelnen Scans und für den Anschluss an das Weltkoordinatensystem wurde eine Totalstation und satellitengestützte Vermessungsverfahren eingesetzt.

MN GSG „iSNEx24“in VALCARTIER / KANADA

Etwa 100 Soldateninnen und Soldaten aus 11 Ländern, darunter fünf Mitarbeiter des IMG, nahmen von 21. April bis 10. Mai 2024 an einer

Foto: Bundesheer/Dion6

Vermessungsübung auf dem Stützpunkt VALCARTIER teil, um den Wissensaustausch zwischen Kanadas Verbündeten in einer durch den Konflikt in der UKRAINE veränderten Welt zu erleichtern.

Die Übung "iSNEx24" wurde von der Multinational Geospatial Support Group (MN GSG) durchgeführt, die die NATO-Mitgliedsstaaten unterstützt. Obwohl die Übung in KANADA stattfand, hatte DEUTSCHLAND das Kommando.

"Wir erleben mit der russischen Bedrohung einen Wandel in Bezug auf die Sicherheit in der Welt und insbesondere in EUROPA", erklärt Kapitän z.S. Uwe FREY von der Deutschen Marine und Kommandant der MN GSG. "Es bedeutet, dass wir unsere Art und Weise, Dinge zu tun, überprüfen müssen." Daher müssen Militärvermesser in der Lage sein, ihre Arbeit unter schwierigen Bedingungen auszuführen, wie es beispielsweise in der UKRAINE der Fall ist.

"Wir können bestimmte Informationen mit Karten oder Satelliten haben, aber manchmal müssen wir selbst ins Feld gehen, um zu beobachten und unsere Messungen durchzuführen", sagt Kapitän z.S. FREY. Daher ist es wichtig, sicherzustellen, dass verbündete Länder, die manchmal unterschiedliche Technologien verwenden, weiterhin miteinander zusammenarbeiten können.

"Wir haben eine kleine militärische Vermessungskapazität in KANADA, so dass jede größere Vermessungsaufgabe in einem Koalitionskontext durchgeführt wird", erklärt Major Martin ST-AMAND, Kommandeur der Pionierstaffel im Canadian Armed Forces Mapping Service.

Auf dem Trainingsgelände auf dem Stützpunkt Valcartier werden zum Beispiel deutsche und litauische Teams Drohnenmodelle fliegen, die sie normalerweise nicht verwenden. "Wir haben das Feld zwischen unseren beiden Teams aufgeteilt und können unsere Ergebnisse vergleichen", erklärt Major René ANGER von der Bundeswehr, der während der Übung getroffen wurde.

"Die Litauer haben eine andere Art von Drohne, die mit verschiedenen Kameras in kurzer Zeit mehr Boden abdecken kann."

Foto: le journal de québec

Die Bedingungen eines bewaffneten Konflikts werden zum Teil durch fiktive Szenarien reproduziert. In diesem Fall ist die Südküste von QUEBEC CITY in die Hände von Feinden Kanadas gefallen, die eine Frontlinie durch die Capitale-Nationale aufrechterhalten müssen.

Diese Simulation könnte möglicherweise noch weiter vorangetrieben werden, so der Beobachter der französischen Armee, Kommandant Franck SAUGER-MELIANO. FRANKREICH möchte möglicherweise die gleiche Übung in zwei Jahren organisieren.

"Bei dieser Art von Übung sollten wir uns vielleicht darauf vorbereiten, uns militärischer zu engagieren", sagte er. "Es wäre verdient, dass die Männer mit Waffen bewaffnet wären. [...] Es wäre realistischer. Wenn man sieht, was im Osten passiert: Ukrainische Vermessungsingenieure, sie sind an vorderster Front und sie sind exponiert."

Ansonsten ermögliche das Zusammenleben mit anderen Ländern auch den kulturellen Austausch, fügt Major Martin ST-AMAND hinzu.

"Wir konnten alle internationalen Teilnehmer dazu bringen, die Sehenswürdigkeiten von QUEBEC CITY zu besuchen. Es wurde sehr gut angenommen!"

Foto: le journal de québec

DROHNEN, TRADITIONELLE VERMESSUNGEN UND LIDAR-SYSTEME

15 Tage lang wurden hundert Soldatinnen und Soldaten für die Übung "iSNEx24" mobilisiert.

Einige Militärvermesser führen traditionellere geografische Vermessungen mit Stativinstrumenten durch. Andere verwenden verschiedene Arten von Drohnen, die von den Streitkräften verbündeter Länder eingesetzt werden.

Ein mit einem LIDAR-Lasersystem ausgestatteter Lastwagen wurde auch im Rahmen der Übung eingesetzt, die im Wald auf den Übungsplätzen des Militärstützpunkts VALCARTIER stattfand.

Bericht: le journal de québec

F-087 Basislehrgang Geographische Informationssysteme 2024

Von 13.05. bis 17.05.2024 fand in der SCHWARZENBERG Kaserne der 12. Basislehrgang GIS statt.

Das IMG als Anwenderfachabteilung von GIS Software im Österreichischen Bundesheer veranstaltet zweimal im Jahr einen Basislehrgang GIS um Mitarbeiterinnen und Mitarbeitern, die geographische Daten erfassen, digitalisieren, analysieren, darstellen und archivieren, im Umgang mit der doch sehr umfangreichen Software zu schulen.

Aufgrund der unterschiedlichsten Tätigkeitsfelder der Teilnehmer wurde die, in ALLEN Netzen und auch auf Stand Alone Geräten verfügbare, Software QGIS unterrichtet.

Neben Theorie Einheiten - Was ist ein GIS, was sind Vektordaten, was sind Rasterdaten – was ist eine Georeferenz, warum ist es wichtig zu wissen, dass die Erde keine Kugel sondern ein Geoid ist? - stand vor allem das praktische Arbeiten im Vordergrund. Die Teilnehmer aus den Dienststellen der Luftaufklärung, der Luftraumüberwachung, des Ausbildungs- und Simulationszentrums Zeltweg sowie Mitarbeiterinnen und Mitarbeiter aus dem Bereich Umweltschutz und MilGeo der Militärkommanden K und S konnten so ihre Fertigkeiten vertiefen.

Einer erfolgreichen Verwendung der Software am eigenen Arbeitsplatz steht somit nichts mehr im Wege!

Navigation Warfare Test- und Versuchsreihe am TÜPl Seetaler Alpe 2024

Das IMG der Dion6 lud vom 3. Juni bis 7. Juni 2024 zu einer Navigation Warfare Test- und Versuchsreihe am TÜPl Seetaler Alpe ein. Die Übung fand in Kooperation mit dem ARWT, der Dion2, rund 20 nationalen und internationalen Forschungspartnern sowie der Frequenzbehörde und AustroControl statt, die zum großen Erfolg der Veranstaltung beitrugen.

Foto: Bundesheer/Dion6

Im Zuge der Übungswoche wurden die Fähigkeiten im Bereich Navigation Warfare (NavWar) praktisch erprobt und dabei konnten wertvolle Erfahrungen für die Weiterentwicklung gesammelt werden. Der Schwerpunkt lag dabei auf der Aussendung von GNSS-Störsignalen (Global Navigation Satellite System, z.B. GPS) wie dem Jamming (kein GPS-Empfang möglich) oder dem Spoofing (falsche Position wird empfangen). Untersucht wurde

Foto: Bundesheer/Dion6

unter anderem die Resilienz von Heeresgeräten gegenüber Störattacken wie dem BOS Digitalfunkgerät oder dem Hubschrauber AB 212. Darüber hinaus konnte erstmals das Mobile Survey Tool zur Protokollierung und Kartierung der Testergebnisse im praktischen Einsatz getestet werden.

Die teilnehmenden zivilen Fachexperten kamen von den Universitäten LAIBACH, der TU TRIEST, der TU GRAZ sowie verschiedenen Forschungspartnern aus ÖSTERREICH, den NIEDERLANDEN, ITALIEN, SLOWENIEN und SPANIEN.

Schutzschild 24 – Aufgaben im Bereich MilGeo

Der militärische Geodienst (MilGeo) stellt verschiedene Geoinformationsprodukte, wie topographische und thematische Karten, interaktive 3D-Visualisierungen oder geographische Analysen, für den militärischen Bedarfsträger auf verschiedenen Ebenen zur Verfügung.

Foto: Bundesheer/Dion6

Im Rahmen der SCHUTZSCHILD 2024 wurde bereits im Übungsvorfeld durch das Institut für Militärisches Gewesen (IMG) der Direktion 6, und weiterem MilGeo-Fachpersonal auf Militärkommando- und Brigadeebene für Bedarfsträger diverse Kartenwerke, 3D-Visualisierungen und Analysen erstellt.

Während der Übung stand MilGeo-Fachpersonal auf Ebene HICON, Militärkommando und Brigade den jeweiligen Bedarfsträgern zur Verfügung, um kurzfristige Produktanfragen zu bearbeiten und mit Expertise zu unterstützen.

Dabei wird nicht nur aktives Personal, sondern auch Wissen und Fähigkeiten aus der Miliz vor Ort eingesetzt. Ergänzendes Fachwissen und zur Kompensation von Arbeitsspitzen betrieb das IMG ein Reachback-Element am Standort WIEN.

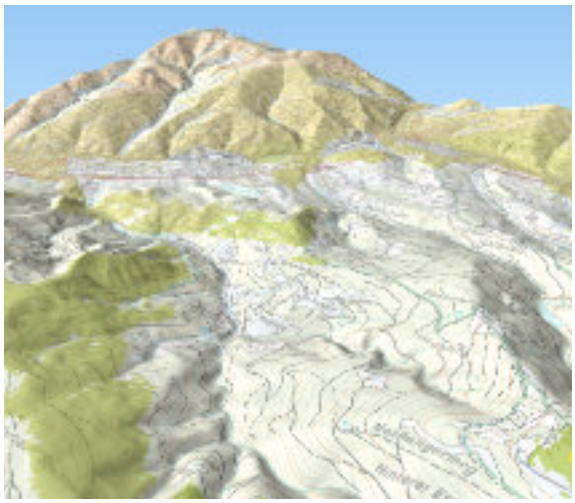


Foto: Bundesheer/Dion6

Während der Übung wurden beispielsweise durch das mobile MilGeoEt am J6/HICON topographische Karten ausgewählter Räume, Lagekarten zur geographischen Darstellung der verschiedener Fernmeldesysteme, Analyse der Bodenbeschaffenheit und der Naturgefahren im Zusammenhang mit den Zufahrtswegen und Standorten der eingesetzten Fernmeldesystemen oder flächige Sichtfeldanalysen mit 3D-Darstellung erstellt.

Mit seinen fachlichen Beiträgen und Produkten trägt der militärische Geodienst auf unterschiedlichsten Ebenen zum umfassenden Verständnis des Einsatzraumes bei.

„CIWIX 2024“ in Polen – Teilnahme IMG

Vom 3. bis 21. Juni 2024 fand die diesjährige "Coalition Warrior Interoperability Exercise" (CWIX) der NATO im "Joint Forces Training Center" (JFTC) in der Stadt BYDGOSZCZ (deutsch BROMBERG) in POLEN statt.

Die Übung unterstützt das Ziel der "Zero day compatibilty" der NATO. Das heißt, in einem multinationalen Einsatz sollen die IT Systeme der teilnehmenden Nationen und der NATO Kommando Struktur von Beginn an interoperabel sein. Das ist die Grundlage für jeden elektronischen Informationsaustausch. In diesem Zusammenhang ist die CWIX auch die Keimzelle der "Federated Mission Networking Initiative" (FMN). Mit über 2500 Teilnehmern aus 40 Nationen war die CWIX 2024 die weltweit größte derartige Übung.

Das IMG nimmt seit 2012 mit einem Geosupport Element an der Übung teil und ist in die GeoMetOc Focus Area eingebettet. Hier wird vor allem der service-basierte Austausch von Geoinformationen getestet. Somit wird gewährleistet, dass die Services der einzelnen Nationen standardkonform und kompatibel sind. Weitere Themen sind moderne Geodatenformate sowie die Frage, wie eine "Multi Domain Operation" (MDO) optimal mit Geoinformationen unterstützt werden kann. Über das reine Testen hinaus bot die CWIX auch die einmalige Gelegenheit zum fachlichen Austausch mit Geo-Experten aus 13 verschiedenen Nationen. So war die CWIX ursprünglich der Impulsgeber für die Entwicklung des mittlerweile weithin bekannten GeoWebService. Die weitere kontinuierliche Teilnahme an der CWIX stellt sicher, dass die eigenen Systeme kompatibel und interoperabel bleiben und dass technologische Möglichkeiten und Herausforderungen frühzeitig erkannt werden.

Foto: Bundesheer/Dion6

Grafik: Bundesheer/Dion6

Am Ende der Übung wurde bekanntgegeben, dass ab 2025 mit ADir Hauptmann Nikolaus PRUZSINSZKY wieder Österreich für 3 Jahre die Führung der GeoMetOc Focus Area übernimmt - ein Beweis für das Vertrauen in die Kompetenz des IMG!

AIRPOWER24 – Aufgaben IMG

„Fliegen. Freiheit. Begeisterung.“ - unter diesem Motto stand die AIRPOWER24, die von 06. bis 07. September 2024 bereits zum elften Mal am Fliegerhorst HINTERSTOISSER in ZELTWEG stattfand.

Um die AIRPOWER24 mit designiertem Kartenmaterial zu versorgen, wurden zwei Bedienstete des IMG während der Aufbau- und Durchführungsphase vor Ort in die FüUKp/TPG6 eingegliedert, um den Bedarf an Kartenmaterial abzudecken.

Durch das AIRPOWER-Projektbüro wurden bereits im Vorfeld sämtliche AIRPOWER-relevanten Geodaten zusammengefasst und daraus folgend verschiedenartige AIRPOWER-Kartenwerke in unterschiedlichen Maßstäben durch IMG aufbereitet.

In Koordination mit dem ReproZ/Wien wurden rund 1500 Papierkarten gedruckt und in weiterer Folge im Rahmen der AIRPOWER24 an verschiedenartige Bedarfsträger ausgegeben. Neben der Verteilung der standardmäßigen AIRPOWER-Kartenwerke wurden auf Anfrage auch diverse Sonderkarten in kleiner Auflagezahl vor Ort aufbereitet und gedruckt.

Zusätzlich zur klassischen analogen Kartenvariante wurden ebenso die AIRPOWER-Kartenwerke in digitaler Version an unterschiedliche Bedarfsträger bereitgestellt, um die Kartendarstellung auch in diverse, bei der AIRPOWER24 eingesetzte, technische Systeme sicherstellen zu können.

Die erstmalige Bereitstellung von AIRPOWER-Kartenwerke über das IMG-GeoWebService in SMN wurde im Rahmen der Veranstaltung von unterschiedlichen Stellen als durchaus positiv angenommen und diese zusätzliche Möglichkeit der Kartenbereitstellung konnte dadurch einen noch breiteren Nutzerkreis erreichen.

MilGeo-Besprechung mit CZE in SALZBURG

Von 29. November bis 1. Dezember 2023 fand in PRAG / CZE die MilGeo-Besprechung statt. Anlässlich dieses Besuches wurde eine Gegeneinladung für die CZE Seite ausgesprochen.

Dieser Besuch in ÖSTERREICH fand dann von 2. bis 4.Oktober 2024 in der SCHWARZENBERG-Kaserne in SALZBURG statt.

Gegenstand dieser Besprechung waren neben dem allgemeinen Informationsaustausch im Fachbereich MilGeo noch folgende Themenschwerpunkte:

- Zukünftige strategische Ausrichtungen der MilGeo-Dienste
- Navigation Warfare (Spoofing und Jamming)
- Satellitenmission Earth Observation
- D-Visualisierungsmöglichkeiten

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Nationalfeiertag 2024

Auch im Jahre 2024 war das IMG anlässlich der Feierlichkeiten zum Nationalfeiertag im Rahmen der Themeninsel "Cyber, Forschung und Technik" Am Hof in der Wiener Innenstadt eingebunden.

Unter Federführung der Direktion 6 und in bester Zusammenarbeit mit der Abteilung WFE war das IMG am 25., 26. und am 27.10.2024 mit einem eigenen Stand und an einem weiteren unterstützend präsent:

- "MilGeo", ff. IMG,
- "Space", ff. Joanneum Research

BWÜ 2024 – Operation „Earthquaker“

Zweck

Die Miliz ist ein wesentlicher Bestandteil des militärischen Geodienstes, bringt dabei Spezialwissen ein und stärkt die Durchhaltefähigkeit im In- und Ausland.

Für den Erhalt bestehender und die Entwicklung neuer Fähigkeiten in der Miliz, wie auch für das Zusammenarbeiten zwischen Aktivkader und Miliz unter einsatznahen Bedingungen, wurde Mitte November 2024 am ABC- & KatHÜPl TRITOLWERK bei Wr. NEUSTADT geübt.

Ziel

Ziel des Szenarios war es, nach einem Erdbeben in "TRITOL-Stadt" rasch Führungsmittel für AFDRU bereitzustellen. Dafür wurden Schadstellen mittels geographischer Methoden aus der Luft, vom Boden und im Untergrund dokumentiert und in unterschiedlichen Geo-Produkten dargestellt.

Das Szenario erlaubte das Üben aller Prozessschritte im Zuge dieser Produkterstellung.

Foto: Bundesheer/Dion6

Besuch aMA Korps am IMG

Am 12. Dezember 2024 besuchten die in Österreich akkreditierten ausländischen Militärattachés aus elf Nationen das IMG.

Im Laufe eines Vormittags wurden sie in die Aufgaben, Angelegenheiten und ausgewählte Projekte des Österreichischen MilGeowesens eingewiesen.

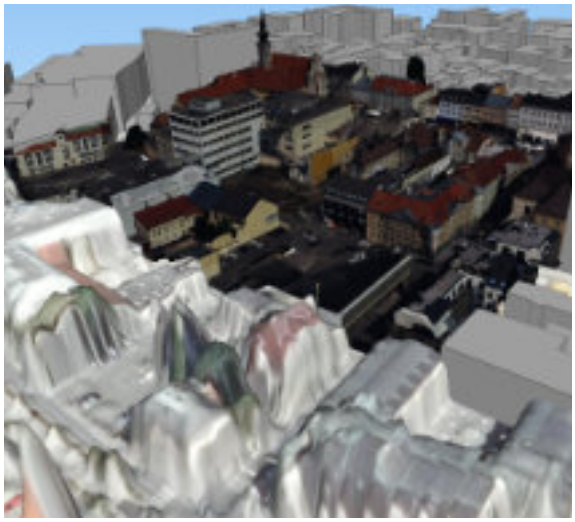
Foto: Bundesheer/Dion6

BORIS

BORIS ist ein Produkt des IMG, das der interaktiven 3D-Geländedarstellung dient. Dabei wird das Relief mit unterschiedlichen Texturen versehen und um 3D-Objekten, wie Gebäude, ergänzt. Ebenfalls erlaubt BORIS kleine Analysen auf das Gelände anzuwenden, wodurch ein tieferes Verständnis über einen Raum erlangt wird. Dabei können Fragen u.a. über die Entfernung zum Horizont, den einsehbare Raum von einem Ort aus, oder über das Geländeprofil beantwortet werden.

Über das Jahr 2024 betrachtet hat sich einiges bei BORIS getan:

In der Interaktion mit den Bedarfsträgern ermöglichen Musterakte und die Intranetseite des IMG einen effizienten Informationsaustausch. Darunter fallen Produktantrag mit relevanten Parametern oder das passende Medium zur digitalen Produktbereitstellung.



Grafik: Bundesheer/Dion6, Ausschnitt St. Pölten aus BORIS

Die Erstellung von BORIS geschieht mit standardisierten Inhalten und basiert dabei auf Vorlagen-Projekte, wodurch der Abschluss eines Auftrages meist innerhalb eines Tages möglich ist. Und auf Grundlage der qualifizierten Rückmeldung von Nutzern – speziell JgB25 und Generalstabsausbildung – wurde eine funktionelle Produktanpassung durchgeführt, die bereits in der aktuellen Version 2025.1 den Bedarfsträgern zu Verfügung steht.

Bedarfsträger dieses Produktes des IMG finden sich großteils im Verantwortungsbereichs der Direktion 1 (kleine Verbände der 7.JgBrig) aber auch bei Direktion 2 (LuU) und Direktion 5 (LVAk und TherMilAk) . Im Vorfeld von Übungen ist eine vermehrte Nachfrage zu erkennen (SCHUTZSCHILD 2024), wobei nicht nur BORIS für Räume im Inland, sondern auch bspw. vier Räume in BULGARIEN für HTS/GebKpfZ erstellt wurden.

Insgesamt sind im Jahr 2024 mit dem Produkt BORIS knapp 50 Räume im In- und Ausland dem Bedarfsträger zur Verfügung gestellt worden – eine Zahl die die Notwendigkeit und die Qualität dieses IMG-Produktes widerspiegelt.

Kartenprodukte

Das Bundesamt für Eich- und Vermessungswesen (BEV) hat einen neuen Zeichenschlüssel für die „Topographische Karte 1 : 50 000" (ÖK50) mit mehr farbigen Akzenten und zeitgemäßen Schriftarten für ein klareres und leichter lesbares Kartenbild eingeführt. Das IMG passt entsprechend das Erscheinungsbild der Truppenübungsplatzkarten an. Als erstes Produkt ist die Neuauflage der ÖMK25 LIZUM/WALCHEN im Herbst 2024 in diesem neuen und übersichtlicheren Design erschienen.

Die sicherheitspolitischen Assistenzeinsätze Migration im BURGENLAND und der SÜDSTEIERMARK wurden mit Sonderausgaben der ÖK50 unterstützt. Für die MGI SÜDSUDAN und die MLBs KOSOVO und TÜRKEI wurden satellitenbildgestützte Übersichtskarten und Stadtpläne der Hauptstadt angefertigt, sowie die Publikationen jeweils mit zahlreichen thematischen Karten ausgestattet.

Der VAtt in ISRAEL hat eigens erstelltes, großmaßstäbiges Kartenmaterial für seinen Zuständigkeitsbereich erhalten. Weiters wurden politische Übersichtskarten für den VAtt in ROM (ITALIEN, SPANIEN, PORTUGAL und MALTA) angefertigt. Für den TÜPl SEETALER ALPE wurde die Spezialkarte des Lagerbereiches auf Basis eines Orthophotos, sowie die Laufwegekarte aktualisiert. Spezielle Übungskarten wurden unter anderem für die Bedarfstäger GStb, 3.JgBrig, ABCAbwZ, GebKpfZ, HTS und MP produziert. Sonderausgaben von Standardkarten mit

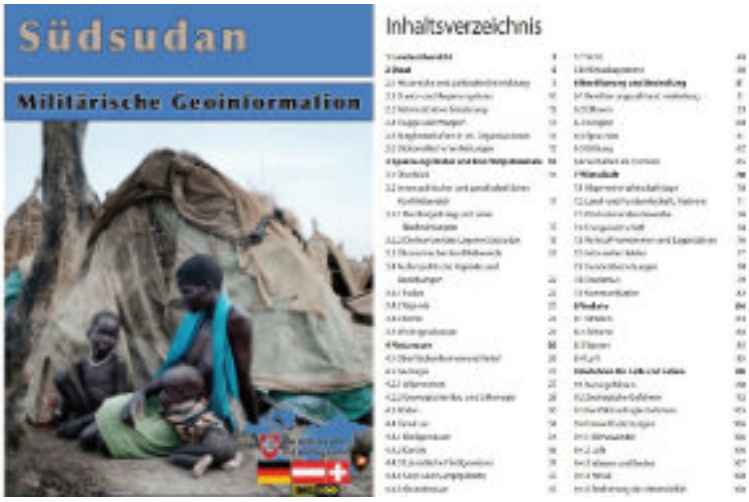
Grafik: Bundesheer/Dion6, ÖMK25 TÜPl LW-Detail

maßgeschneiderten Ausschnitten wurden beispielsweise für AAB7, ARWT, HTS, JgB19 und MilKdo W bereitgestellt.

Die Veranstalter der Märsche „Graf Starhemberg", Marc Aurel" und „Ostarrichi" wurden antragsgemäß mit eigenen Marschkarten versorgt. Für zahlreiche Orientierungsläufe diverser Bedarfsträger wurden OL-Karten im Maßstab 1 : 25 000 in speziellem Layout geliefert. Anträge zur Herstellung von thematischen Karten in allen Maßsstabsbereichen konnten für IFK, IHMF, ISS und TherMilAk umgesetzt werden. Anhand dieser (unvollständigen) Aufzählung lässt sich sehr gut sowohl das breit gefächerte Leistungsspektrum an kartographischen Produkten aller Maßstabsbereiche, als auch die „Kundenvielfalt" erkennen.

Militärische Landesbeschreibungen (MLB) und Militärische Geoinformationen (MGI)

Für ausgewählte Krisengebiete der Erde und (potenzielle) Einsatzräume des ÖBH erstellt



Grafik: Bundesheer/Dion6, Coverbild der MGI Südsudan & Inhalte MLB/MGI 2024

Dion6/IMG Militärgeographische Landesbeschreibungen (MLB) und Militärische Geoinformationen (MGI). Diese landeskundlichen Informationen stellen einen allgemeinen Überblick über das jeweilige Land zu verschiedenen Themengebieten dar (Inhalte siehe untenstehende Abbildung). Sie dienen militärischen Planern als Bearbeitungs- und Beurteilungsunterlage sowie Soldatinnen und Soldaten als Einstiegsinformation bei einem Einsatz.

Aufbau und Gliederung von MLB und MGI sind deckungsgleich, ein Unterschied besteht lediglich im beteiligten Kreis von Autoren bzw. Dienststellen. Während die MLB ein rein österreichisches Produkt unter Beteiligung verschiedener Dienststellen des Bundesheeres (IMG, IFK, MilMed etc.) ist, entsteht eine MGI im Rahmen einer seit dem Jahr 2010 permanent laufenden Kooperation der militärischen Geodienste aus DEUTSCHLAND, ÖSTERREICH und der SCHWEIZ („DACH"). Dion6/IMG, ZGeoBW (Zentrum für Geoinformationen der Bundeswehr) und die Schweizer Armee wirken an der Erstellung der Schriftenreihe „Militärische Geoinformation" (MGI) arbeitsteilig zusammen. Koordinierung, Kartographie, Lektorat und Layoutierung werden dabei federführend von Dion6/IMG wahrgenommen.

2024 wurden folgende MLB/MGI erstellt:

MLB: KOSOVO & TÜRKEI, MGI: SÜDSUDAN & LIBYEN

Secure PNT & Navigation Warfare

Auch im Jahr 2024 führte das Referat Navigation erneut zwei einwöchige Secure PNT- und Navigation Warfare (NavWar)-Übungen am Truppenübungsplatz TÜPl SA durch.

Foto: Bundesheer/Dion6, Bgdr TEICHMANN mit MIl-IKTFü Fhren, Forschungspartnern und dem Ref Navigation

Die erste Übung fand vom 03. bis 07. Juni 2024 statt und konzentrierte sich auf die Vermessung eigener Systeme sowie die Erprobung von Prototypen aus nationalen Forschungsprojekten. Ziel war es, diese Technologien weiterzuentwickeln und ihre Leistungsfähigkeit unter realistischen Bedingungen zu testen, um diese in weiterer Folge optimieren zu können.

Die zweite Übung, die vom 7. bis 11. Oktober 2024 durchgeführt wurde, legte den Fokus auf internationale Kooperation und Wissensaustausch. Zudem diente sie als Vorbereitungsevent für das EDA CatB RIPTIDE-Projekt. Im Rahmen dieser Übung wurden umfangreiche Mess- und Versuchsreihen unter Einsatz unterschiedlicher Luftfahrzeuge durchgeführt. Geplant war der Einsatz eines AW169-Hubschraubers, der witterungsbedingt nicht zum Einsatz kam, sowie die erfolgreiche Testung der Payload einer ÖBH-Drohne. Die Durchführung wurde durch dienststellenübergreifende Zusammenarbeit und die Unterstützung verschiedener Partnerorganisationen erheblich gestärkt. Recht herzlichen Dank dafür!

Zusätzlich wurde die Übung genutzt, um den Studierenden des 5. Semesters des MilAk-Studiengangs Mil-IKTFü im Rahmen der Lehrveranstaltung „Einführung in die Navigation" einen praxisnahen Einblick in die Thematik Jamming und Spoofing zu geben.

Dabei erhielten sie die Gelegenheit, nationale Forschungspartner kennenzulernen und ein vertieftes Verständnis für die Bedeutung der Thematik sowie die Sensibilisierung im Bereich der PNT-Sicherheit zu erlangen.

Diese NavWar-Übungen leisten einen wesentlichen Beitrag zur Weiterentwicklung der Fähigkeiten im Umgang mit PNT-Technologien. Sie stärken die Resilienz gegenüber Störungen und Manipulationen, fördern den Aufbau operativer Kompetenzen und tragen maßgeblich zur Sicherheit und Effizienz kritischer Infrastrukturen bei.

Space

LEO 2 VLEO

Im Einklang mit dem vierten Ziel der „Österreichischen Militärischen Weltraumstrategie 2035+"

Grafik: Bundesheer/Dion6, AUT-NED LEO-2-VLEO-Satellitenkonstellation

verfolgt das BMLV den Wandel vom reinen Nutzer hin zum aktiven Akteur und Dienstleister im Bereich der Weltraumtechnologie.

In diesem Kontext wurde gemeinsam mit dem niederländischen Verteidigungsministerium (DSSC) im Rahmen eines EDA CatB-Forschungsprojekts das Vorhaben „LEO-2-VLEO – Military Crisis-Response Satellite Constellation" initiiert. Die Projektverantwortlichkeiten sind klar definiert: Während die NIEDERLANDE den Satellitenbus und das Antriebssystem bereitstellen, liegt die Entwicklung der gesamten Nutzlast in österreichischer Verantwortung.

Das zentrale Ziel dieses Projekts ist die In-Orbit-Demonstration einer Satellitenkonstellation zur Krisenreaktion im Low Earth Orbit (LEO). Die Besonderheit dieser Konstellation besteht in der Fähigkeit, Satelliten gezielt in den Very Low Earth Orbit (VLEO) abzusenken und anschließend wieder in den LEO anzuheben.

Darüber hinaus verfolgt das Projekt die Entwicklung einer kosteneffizienten Lösung durch den Einsatz von Standardkomponenten, die eine rasche Implementierung ermöglichen. Im Rahmen der Demonstration soll das Missionspotenzial der LEO-2-VLEO-Konstellation umfassend analysiert werden, insbesondere in den Bereichen Formationsflug, innovative Nutzlasten sowie die Bereitstellung operationeller Produkte und Services.

Zusätzlich werden Erkenntnisse über sämtliche Phasen des Satellitenlebenszyklus gewonnen, um künftige Entwicklungen im militärischen Weltraumsektor gezielt voranzutreiben.

Basiskurs Space

Die erfolgreiche Etablierung der Domäne Weltraum mit all ihren Herausforderungen innerhalb des BMLV/ÖBH erfordert frühzeitige Investitionen in gezielte Maßnahmen zur fachspezifischen Basisausbildung im Bereich Personal und Ausbildung.

Vor diesem Hintergrund wurde der „Basiskurs Space & Security" durch das Referat Navigation/IMG in Kooperation mit dem Österreichisches Weltraum Forum (ÖWF) initiiert.

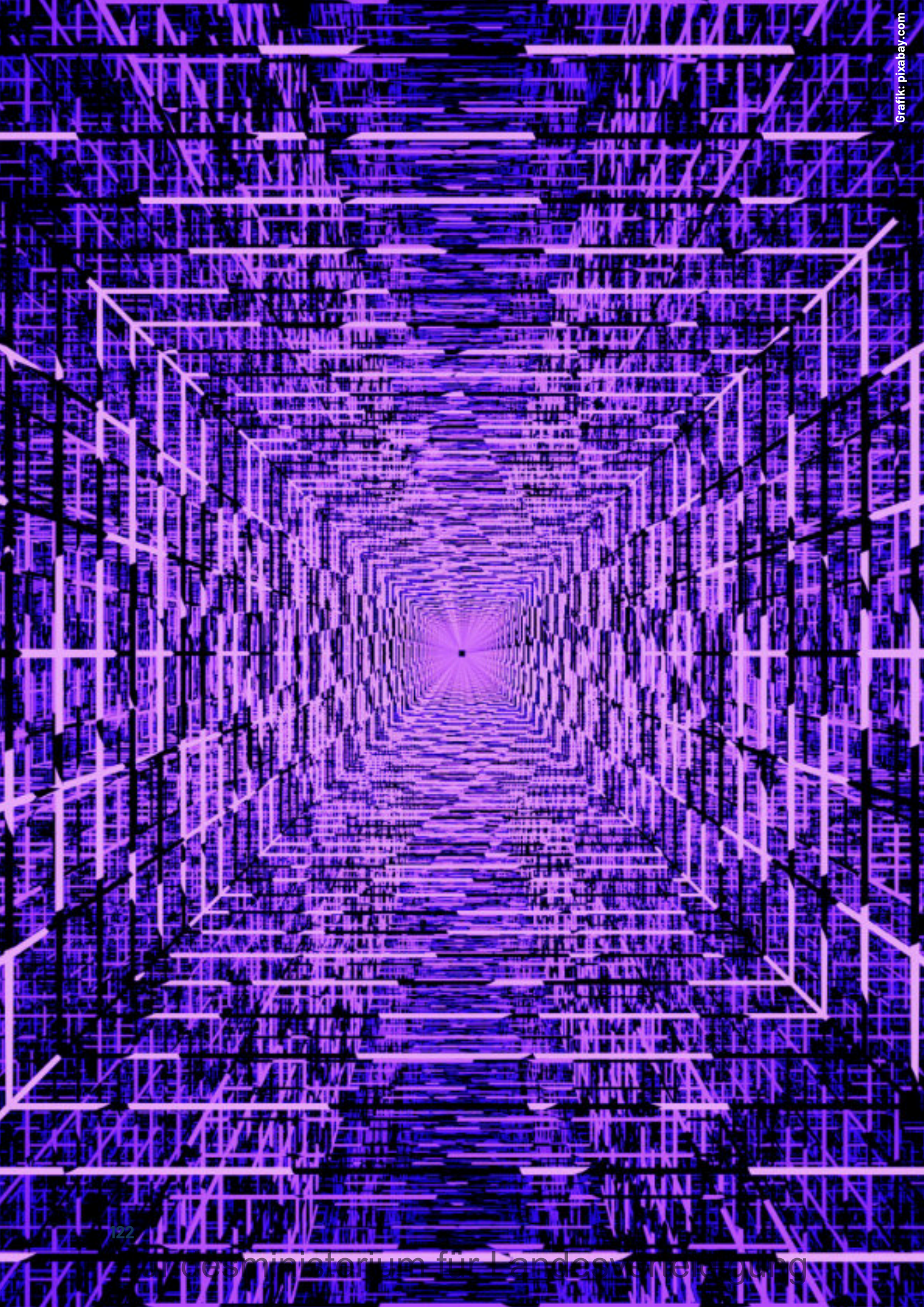
Die erste Durchführung des Lehrgangs fand vom 02. bis 06. Dezember 2024 an der Führungsunterstützungsschule (FüUS) in der Starhemberg-Kaserne statt.

Der Kurs vermittelt grundlegendes Wissen zu militärischer Raumfahrttechnologie, beleuchtet strategische Aspekte der Konfliktführung im Weltraum und analysiert internationale Fähigkeiten sowie wirtschaftliche, organisatorische und legislative Rahmenbedingungen.

Neben der theoretischen Wissensvermittlung bietet der Lehrgang auch die Möglichkeit, durch die Erarbeitung und Analyse realer Szenarien praxisnahe Fähigkeiten zu entwickeln. Damit schafft der Kurs eine essenzielle Grundlage für die Weiterentwicklung der nationalen Kompetenz im Bereich Space Security und unterstützt langfristig den Fähigkeitsaufbau in diesem zukunftsweisenden Bereich.

Der „Basiskurs Space & Security" wird künftig als jährliche Kaderfortbildung angeboten, mit dem langfristigen Ziel, in den Wahlfachkatalog der MilAk aufgenommen und dort etabliert zu werden.

Foto: Bundesheer/Dion6, Lehrpersonal und Kursteilnehmer des ersten Basiskurses Space & Security an der FüUS



Grafik: pixabay.com

Kompetenzzentrum für Landesverteidigung

Führungsunterstützungsbataillon 1

Kommandant FüUB1: Obst Ernst BERTHOLD, MSD

Als Orientierung nach innen, handlungsleitend und motivierend für das Bataillon als Ganzes sowie nach außen deutlich machend, wofür wir als Verband stehen, verfügt das FüUB1 über ein Leitbild welches wie folgt lautet:

Wir sind ein, der Direktion 6 direkt unterstellter, kaderstarker, dynamischer Verband und vereinigen hohen technischen Standard mit zeitgemäßer Flexibilität und fundierter Erfahrung. So garantieren wir unverzügliche und sichere Verbindungsherstellung, rasches Reagieren auf Lageänderungen und damit fachlich hochwertige Problemlösungen.

Unsere Fähigkeiten sind unter anderem:

- Sicherstellung der ununterbrochenen Führungsfähigkeit unserer Bedarfsträger nach den Prinzipien eines Force Providers
- Sicherstellung des Betriebes eines interoperablen, taktischen Informations- und Kommunikationsnetzwerkes und dessen dezentrale Administration und Steuerung

Grundsätzlich gilt dieses Leitbild, insbesondere die Vision und die Mission auch angesichts der Veränderungen des Bundesheeres in Bezug auf das Zielbild 2032 weiterhin, allerdings müssen insbesondere Leitsätze entsprechend angepasst werden.

Durch die Einführung des neuen Systems TCN flächendeckend auf alle Verbände des Bundesheeres bis zur Ebene Einheit sind insbesondere die Brigaden befähigt einen Großteil ihres IKT Bedarfes selbst zu stellen.

Die Aufgabe des FüUB1 als Force Provider verringert sich daher auf ein Minimum und der Focus wird wieder auf die Sicherstellung der Führungsfähigkeit auf operativer und strategischer Ebene als High Value Asset im Bereich höherer Kommanden, sowie besonderen Fähigkeiten im Bereich elektronische Kampfführung oder multinationaler Kompatibilität liegen.

Erste Erkenntnisse durch den Einsatz der neuen Systeme konnten 2024 durch unseren Verband im Zuge der Luftraumschutzoperation DÄDALUS24 und der Großübung SCHUTZSCHILD24 gewonnen werden.


Foto: BMLV/HBF

Unter anderem zeigte sich, dass auch im Bereich Überwachung und Steuerung der Netzwerke bezüglich Servicemanagement, Prozessen und Abläufen Anpassungen an die bisherigen Verfahren zukünftig gemacht werden müssen.

Die Erfahrungen aus der multinationalen Übungsserie COMMON ROOF haben sich in dieser Hinsicht als wertvolle Unterstützung zur Bewältigung dieser Aufgabe erwiesen.

Unser Bataillon durfte auch 2024 als federführender Verband an dieser trinationalen IKT Übung im DACH Rahmen (DEUTSCHLAND, ÖSTERREICH, SCHWEIZ) teilnehmen und die gewonnenen Erkenntnisse und Erfahrungen weitergeben um diese in die zukünftige Organisation, Ausbildung und Vorschriften einfließen zu lassen.

Durch die mittelfristige Eingliederung einer Kompanie für elektronische Kampfführung werden sich auch diese für uns neuen Fähigkeiten in den Leitsätzen wiederfinden.

Das Jahr 2024 war für das FüUB1 in vielerlei Hinsicht ein sehr forderndes. Zusammengefasst kann jedoch resümiert werden, dass die gestellten Aufträge abgearbeitet und die für 2024 gesteckten Ziele erreicht wurden.

Die Soldaten und Soldatinnen unseres Verbandes sind auch für die kommenden Aufgaben gut gerüstet und bereit die geforderten Aufgaben getreu unserem Motto „schnell-flexibel-sicher" durchzuführen.

AssE KÄRNTEN

Von ende März bis ende Juni unterstützte das Führungsunterstützungsbataillon 1 im speziellen die 3.Führungsunterstützungskompanie bei der Grenzraumsicherung im Zuge eines Sicherheitspolizeilichen Assistenzeinsatzes.

Foto: Bundesheer/Dion6

Die FüU-Kompanie unterstütze tatkräftig bei den Grenzübergängen und Kontrollierte die Einreisenden in das Bundesgebiet. Hier konnten die Cybersoldaten von ihrer im Vorfeld durchgeführten Ausbildung profitieren und konnten alle an sie gestellten Aufgaben erfüllen. Das Kader der Kompanie war in verschiedenen Kommandantenfunktionen eingeteilt und die Truppe wurde durch die Miliz gestellt. Jene bekamen durch die Berufssoldaten der 3.Kp eine fundierte Aufschulung und Ausbildung um auf alle Eventualitäten welche der Einsatz mit sich bringt vorbereitet zu sein.

Nach Ablauf des AssE übergab die Kompanie ihren Aufgabenbereich an die ablösenden Teile. Zum Abschluss des Einsatz würde die Einsatzmedaille durch den Stellvertretenden Militärkommandanten von Kärnten Oberst Stefan LEKAS überreicht.

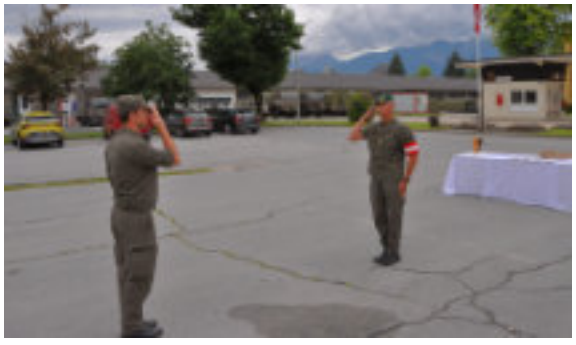


Foto: Bundesheer/Dion6

Bilateraler Truppenbesuch des Partnerverbandes aus VRHNIKA

Am 10 10 24 besuchte eine Delegation des Partnerverbandes EKIS SAF VRHNIKA aus SLOWENIEN während der Übung Common Roof 24 unser Bataillon. Gastgeber Oberst Ernst BERTHOLD begrüßte persönlich die Besucher bestehend aus LTC Sergej RODMAN, CPT Matej POLAK, SMG Gregor BIZJAK.

Der Bataillonskommandant begleitete die slowenischen Soldaten zuerst durch die verschiedenen Übungsstäbe und ermöglichte somit einen Überblick über den bisherigen Übungsverlauf. Zum Abschluss des ersten Tages besichtigten unsere Gäste auch den Traditionsraum des Führungsunterstützungbataillons 1.

Foto: Bundesheer/Dion6

Am zweiten Tag folgte eine Geräteschau und Basisinformationen über das neue im Zulauf befindliche TCN Gerät. Im Anschluss daran fand in der Kaserne der Traditionstag der Fernmelder statt, an welchem die Delegation ebenfalls teilnahm und der den Besuch abrundete.

Foto: Bundesheer/Dion6

Common Roof 24

Auch in diesem Jahr fand die multinationale Übung Common Roof statt. Bei dieser Informations- und Kommunikationstechnologie Übung nehmen die Nationen SCHWEIZ (CH), DEUTSCHLAND (D) und ÖSTERREICH (A) teil. Aus den Kürzeln der Nationen wird die Bezeichnung DACH gebildet und diese Bezeichnung trifft den Grund der Übung ganz gut. Es sollte ein Dach über die Nationen gezogen werden um in einem grenzübergreifenden Katastrophenfall die Kommunikation zu gewährleisten. Es geht darum, dass sich die Einsatzorganisationen und auch das Militär, ein gemeinsames Netz aufstellen um sich koordinieren zu können.

Hier werden jedes Jahr die Systeme und das Führungsnetz in die Probe geschickt um im Ernstfall auf Ausfälle des Netzes rasch und zielorientiert reagieren zu können.

Im Jahr 2023 war ÖSTERREICH die Lead-Nation und hatte viele Aufgabe im Bereich der Organisation und der Durchführung. Dieses Jahr war Deutschland in Lead und hatte somit die Übungsleitung über. Im Vorfeld fanden einige Besprechungen in den verschiedenen Nationen statt. Hier konnte sich die fast schon familiäre Community der Common Roof erneut treffen und im Sinne der Aufgabe sich abzusprechen.

Die Hauptübung fand im Zeitraum von 07 10 bis 18 10 2024 statt. In der Vorwoche wurden in der LUTSCHOUNIG Kaserne schon Lichtwellenleiter Kabel verlegt, Server errichtet und die Lehrsäle auf Stand gebracht. Hierzu mussten sogenannte Floorpläne erstellt werden, um die Kabelführungen kontrolliert und strukturiert durchführen zu können.

Foto: Bundesheer/Dion6

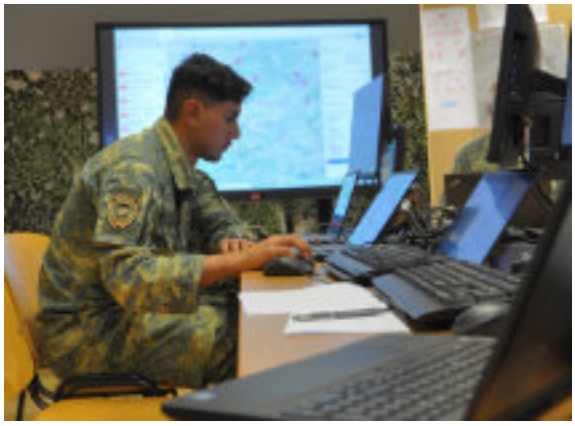


Foto: Bundesheer/Dion6

Das Szenario der diesjährigen Übung begann mit einer Friedensmission - auch Stabilisierungsoperation genannt, - wie sie zum Beispiel real im KOSOVO durchgeführt wird. Aufgrund von Lageänderungen ging man in einen Verzögerungskampf über um den eigenen Kräften die Möglichkeit zu geben neue Stellungsräume zu beziehen und aus diesen heraus zu verteidigen.

Hier verlegte nicht nur die Truppe - auch die eingesetzten Gefechtsstände mussten einen Stellungswechsel durchführen. Dazu mussten die Systeme heruntergefahren und am neuen Gefechtsstand neu hochgefahren werden.

Die größte Herausforderung war es die verschiedenen Systeme kontrolliert abzuschalten um keine Unterbrechung in der Führungsfähigkeit der IT-Netze zu riskieren. Während dieser geübten Szenarien konnten einige Lernfelder erkannt werden und dies ist der Sinn und Zweck einer Übung: sich auf den scharfen Schuss vorzubereiten!

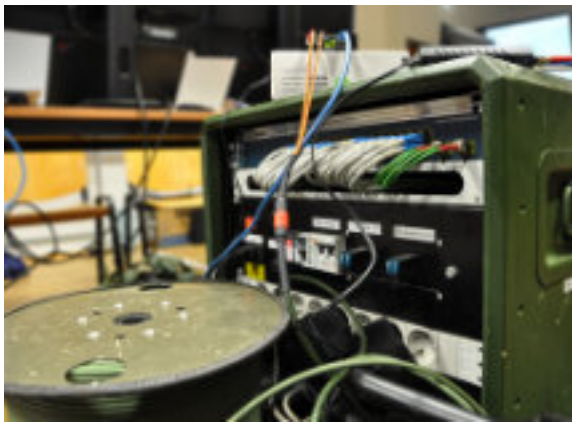


Foto: Bundesheer/Dion6

Luftraumsicherungsoperation DÄDALUS 2024

Von 13 bis 20 01 2024 sichern die Luftstreitkräfte anlässlich des Weltwirtschaftsforums in DAVOS (SCHWEIZ) verstärkt den österreichischen Luftraum.

Dazu wurde ein Flugbeschränkungsgebiet über Teilen Vorarlbergs und Tirols errichtet. Mehr als 1.000 Soldatinnen und Soldaten sowie 24 Luftfahrzeuge – zwölf Flächenflugzeuge und zwölf Hubschrauber – sorgen für die Sicherheit der Veranstaltung und schützen die örtliche Bevölkerung vor Gefahren aus der Luft. Es werden unter anderem Patrouillenflüge zur Überwachung, Flüge zu Identifizierung von Luftraumverletzungen, Transporte sowie „Cross-Border Operations" mit der Schweiz durchgeführt.

Flüge über die Staatsgrenze hinaus werden laufend zwischen ÖSTERREICH und der SCHWEIZ im Rahmen der Weiterentwicklung der Zusammenarbeit intensiviert.

Mehr als 400 Soldatinnen und Soldaten sorgten für sie Sicherheit der Veranstaltung und schützen die Bevölkerung vor Gefahren aus der Luft. Seit 01 02 2019 ist das Abkommen zwischen der Republik ÖSTERREICH und der Schweizerischen Eidgenossenschaft bezüglich der Zusammenarbeit im Bereich der grenzüberschreitenden Sicherung des Luftraumes gegen nichtmilitärische Bedrohungen aus der Luft vollinhaltlich in Kraft. Ein Radarbataillon überwachte den Luftraum über VORARLBERG mit speziellen Aufklärungs- und Tiefflugerfassungsradargeräten und hielt Verbindung zu den Überwachungsstationen in der SCHWEIZ und DEUTSCHLAND.

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Damit alle Luftfahrzeuge alle für den Luftverkehr notwendigen Informationen und Messdaten bekamen, errichteten die Führungsunterstützungssoldaten ein breitbandiges Datennetz. Die Sicherstellung der Funktionalität und der hohen Qualität von allen benötigten Datenleitungen erfüllten die Cyberkräfte problemlos.

Hier unterstütze die 3.FüUKp zur Bewältigung der gestellten Aufgaben mit Richtfunktrupps. Während der gesamten Übung konnten die Villacher Fernmelder alle Aufträge friktionsfrei erfüllen und damit eine wesentlichen Beitrag zum Übungsverlauf leisten

Sicherheitstag bei der Hauptfeuerwache Villach

Am Samstag dem 28 09 24 lud der Kärntner Zivilschutzverband zum jährlichen Sicherheitstag in die Hauptfeuerwache VILLACH ein.

Bei diesem Tag stellen sich die verschiedenen Zivilschutzorganisationen vor und informieren die Bevölkerung über ihre Tätigkeiten, Aufgabenbereiche und speziellen Ausrüstungen. Von der Leistungsfähigkeit der einzelnen Organisationen konnten sich die Besucher bei verschiedenen Vorführungen überzeugen. Weiters gab es auch Informationsveranstaltungen, wie man sich in Notsituationen richtig verhält, - sei es bei einem Fettbrand in der eigenen Küche oder im Umgang mit Bewusstlosen.

Foto: Bundesheer/Dion6

Der Wettergott war der Veranstaltung nicht gnädig, trotzdem konnte man sich über eine große Anzahl von Besuchern freuen. Bei verschiedenen Ständen konnten sich die Interessierten gezielte Information über jede Organisation holen.

Das Bundesheer präsentiert sich bei diesem Sicherheitstag mit Militärpolizei, Sanitätszentrum Süd und den Pionieren. Ergänzend gab das Heerespersonalamt Auskunft über verschiedene Karrieremöglichkeiten beim Bundesheer. Auch wir Cybersoldaten betrieben ein Informationsmodul. Hier konnten Besucher Neues über TCN (neues Kommunikationssystem des Bundesheeres) und Notfallkommunikationssysteme erfahren. Mit einigen Amateurfunkern und Funk-Spezialisten der Zivilschutzorganisationen wurden auch vertiefende Fachgespräche geführt.

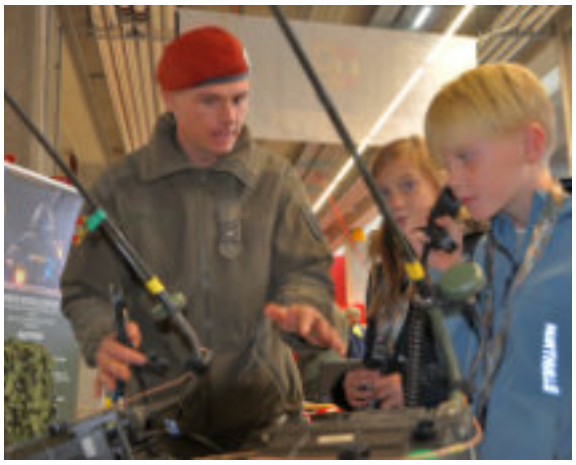


Foto: Bundesheer/Dion6

Tag der Schulen

Auch heuer veranstalte das Militärkommando KÄRNTEN zwei „Tage der Schulen". Die Schülerinnen und Schüler, sowie das Lehrpersonal bekamen dabei einen Einblick in den Soldatenalltag.

Am Dienstag, dem 02 07 2024, waren von 0800 bis 1230 Uhr die Türen der KHEVENHÜLLER-Kaserne in KLAGENFURT geöffnet. Viele Besucher konnten gezählt werden. Der Tag der Schulen dient dazu, der Kärntner Schuljugend einen Überblick über die Aufgaben, Ausbildung, Ausrüstung und Ausstattung des Bundesheers zu geben. Dieser Tag versteht sich deshalb auch als 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 Berufsfeldes machen will.

Neben diversen Informationsständen zum Thema gab es für unsere jungen Gäste in der Kasernen auch diverse Kostproben aus der Truppenküche.

Cybersoldaten, Infanterie, schwere Lastsysteme, Pioniergerät und Information zu umfassenden Lehrlingsausbildung bei Heereslogistikzentrum ermöglichten eine umfassenden Einblick in die vielen Tätigkeiten beim Bundesheer.

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Die Soldatinnen und Soldaten des FüUB1 betrieben den Informationsstand Cyber inklusive einem Datenfunksystem bei dem die Schüler und Lehrpersonal die Gelegenheit hatten, Einblicke in die Waffengattung Führungsunterstützung zu bekommen, und mittels Ultrakurswellen zu kommunizieren. Somit hatten die Teilnehmer über den gesamten Tag verteilt die Möglichkeit verschiedenste Gerätschaften auszuprobieren und sich über die Leistungsfähigkeit des Bundesheeres 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 und somit in die Welt des Mediums Radio einzutauchen.

Foto: Bundesheer/Dion6

Traditionstag 2024

Am Freitag, den 11. Oktober 2024, feierten die Villacher Fernmeldesoldaten in der LUTSCHOUNIG-Kaserne ihren alljährlichen Traditionstag. Der Bezug zur Tradition der Fernmeldesoldaten findet sich im Armeebefehl von Generaloberst von Boroevic vom 8.Oktober 1916, worin er die Leistungen der Telegraphentruppe während der Isonzoschlachten im 1. Weltkrieg besonders würdigt.

Foto: Bundesheer/Dion6

Bei nahezu wolkenlosem Himmel konnten wir zur Feier eine Vielzahl an Offizieren und Vertretern des öffentlichen Lebens bei uns begrüßen. Auch Abordnungen von zivilen Traditionsverbänden wie der Traditionsgendarmerie, Österreichischer Kameradschaftsbund, Marinekameradschaft und Villacher Bürgergarde umrahmten die Veranstaltung sehr farbenfroh.

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Die Militärmusik des Militärkommandos KÄRNTEN begleitete akustisch den traditionellen Festakt und sorgte für eine tadellose musikalische Begleitung.

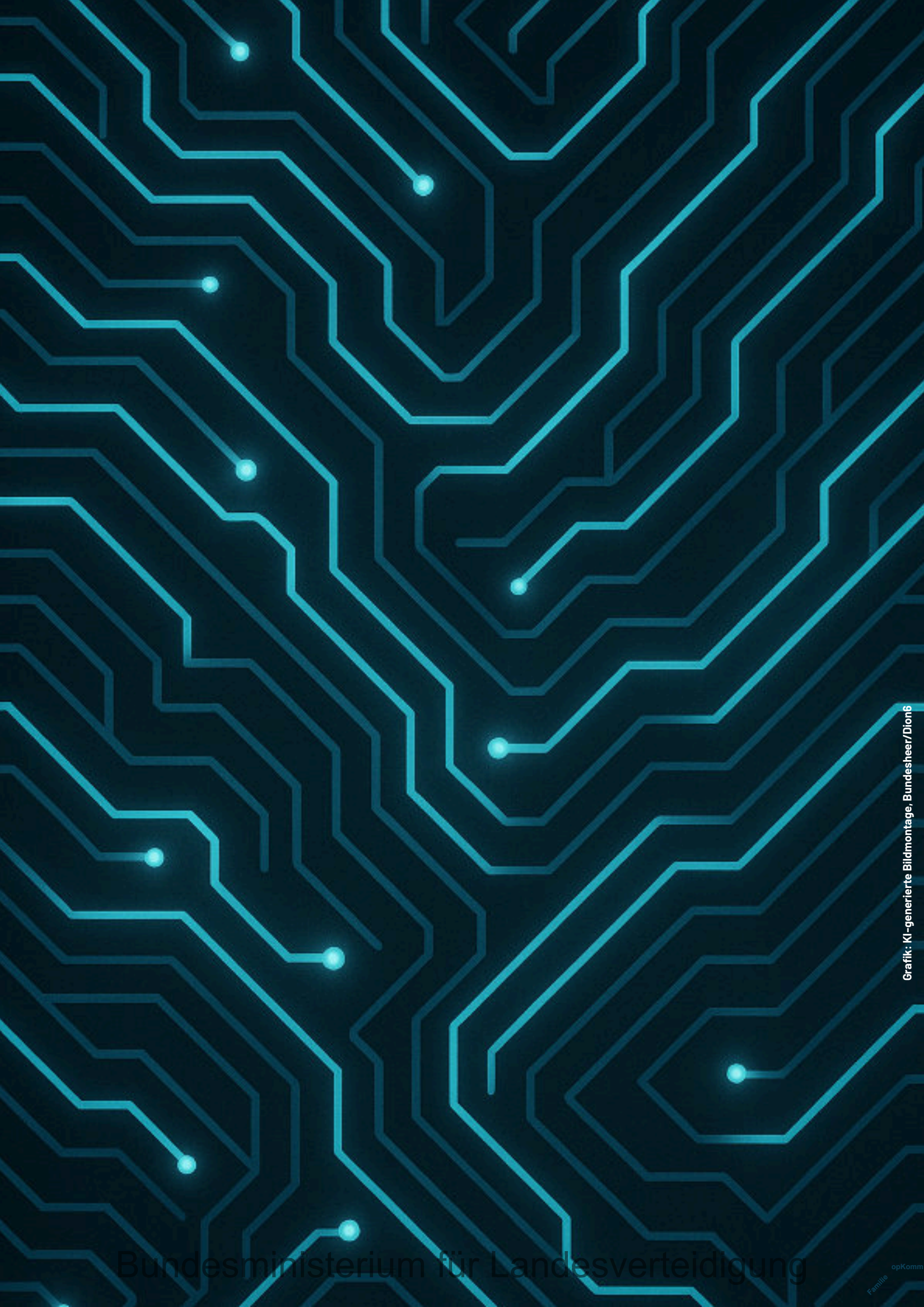
Der heurige Festakt stand unter anderem im Zeichen der Weiterentwicklung der Cyberkräfte zur Bewältigung der Herausforderungen zukünftiger Einsätze und Aufgabenbereiche sowie der daraus ableitbaren Veränderungsnotwendigkeiten und Adaptierungserfordernisse für die Fachabteilung der Cyberkräfte, der Direktion 6. Bataillonskommandant Oberst BERTHOLD sprach in seiner Rede die fortschreitende Entwicklung im technischen Bereich im Speziellen im Cyberraum an und betonte die Auswirkungen des steigenden Informations- und Kommunikationsbedarfs und die damit einher gehenden Gefahren, welche im Cyberspace in postindustriellen, zunehmend digitalisierten Gesellschaften lauern. Auch die damit einhergehende laufende technische Adaptierung von Kommunikationsgerätschaften zur Sicherstellung der Interoperabilität für zukünftige Einsätze im In- und Ausland sowie zwischen Nationen strich der Bataillonskommandant gezielt in seiner Rede hervor.

Als besondere Ehre konnten wir als militärischen Höchstanwesenden den Kommandanten aller Cyberkräfte im Bundeheer und Leiter der Direktion 6, Generalmajor Mag. Ing. Hermann Kaponig, bei uns willkommen heißen. Der Kommandant der Cyberkräfte verwies in seiner Ansprache auf das weite Betätigungsfeld der Waffengattung Cyber auch bei nunmehr beinahe täglichen Angriffen aus dem Cyberspace und den enormen Relevanzgewinn durch fortschreitende Digitalisierung am Gefechtsfeld und des in diesem Zusammenhang notwendigen Ausbaus und der Adaptierung von Führungsunterstützung, das klar weit über Funken und Kabelverlegen hinausgeht. Auch die nunmehr beschlossene Neuaufstellung einer Kompanie für elektronische Kampfführung beim FüUB1 war Teil seiner Ausführungen.

Ziviler Höchstanwesender war der Präsident des Kärntner Landtags, Ing. Reinhard Rohr. Rohr spannte in seiner Ansprache den Bogen vom Beginn des Begriffs Tradition über die Bedeutung der Partnerschaft des FüUB1 mit der Stadt Villach hin zur Relevanz der Sicherstellung eines subjektiven Sicherheitsgefühls bei der Bevölkerung in Zeiten multipler Krisen, die die Notwendigkeit zu Verbesserungen der Ausrüstung des Heeres bei den Österreichern ins Bewusstsein gebrannt hat.

Anschließend an den Festakt lud der Bataillonskommandant auf Kostproben aus der Finalisierungsküche vor den Speisesaal der LUTSCHOUNIG-Kaserne unter die Flugdachkonstruktion ein.

Foto: Bundesheer/Dion6



Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Bundesministerium für Landesverteidigung

Führungsunterstützungsbataillon 2

Kommandant FüUB2: Obst Johannes NUSSBAUMER, MSD

Das Jahr 2024 war in erster Linie von einer sehr hohen Auftragslage gekennzeichnet, mit der Herausforderung der Aufbringung von ausreichend qualifiziertem Personal für Einsätze, Kurse und Lehrgänge.

Bei zahlreichen Übungen und Einsätzen, sowohl im Inland wie auch im Ausland, konnten die Spezialisten des FüUB2 als Force Provider Cyberkräfte im IKT- aber auch im EloKa-Bereich ihre Expertise zur erfolgreichen Auftragserfüllung der Bedarfsträger einbringen.

Erwähnen möchte ich dabei die Übung SCHUTZSCHILD24, wo das Tactical Communications Network erstmalig in einem komplexen Szenario und bundesländerübergreifend eingesetzt wurde. Im gesamten Übungsraum verbanden digitale Datenhighways die übende Truppe des ÖBH von der Übungsleitung bis zur Kompanie sowie die Sensoren, Gefechtsstände und Einsatzzentralen zu einem großen Führungs- Aufklärungs- und Wirkungsverbund.

Die EloKa-Kompanie des FüUB2 setzte bei der Übung SCHUTZSCHILD24 ihre Erfassungs- und Ortungssysteme ein, welche das elektromagnetische Spektrum laufend auf Anomalien überwachte und die gegnerischen Funksignale aufspürte. 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 erstmalige Einsatz eines Central Network Operations Centre am Gefechtsstand des FüUB2 zur Steuerung und Überwachung der Teilnetze der Kampfverbände und die Zusammenarbeit mit der Benutzerbetreuung vor Ort, brachten zukunftsweisende Erkenntnisse für die Weiterentwicklung zeitgemäßer Netzwerkstrukturen.

Mein besonderer Dank gilt vor allem den Kadersoldaten und Soldatinnen des FüUB2, die mit überdurchschnittlichem persönlichen Einsatz Aufträge erfüllt haben, auch dann, wenn sie nicht mit entsprechender Priorität hinterlegt waren. Das für die Führung und Ausbildung verantwortliche Kaderpersonal hat im Jahr 2024 hervorragende Leistungen erbracht.


Foto: BMLV/HBF

Dazu ist anzumerken, dass nur ein gut ausgebildeter und leistungsfähiger Kadersoldat in der Lage ist, die Herausforderungen des Einsatzes und des täglichen Dienstbetriebes zu bewältigen, und er wirkt darüber hinaus auch durch sein Beispiel positiv und motivierend gegenüber seinen anvertrauten Soldatinnen und Soldaten. Eine gediegene Ausbildungsvorbereitung, ausreichende Vorschriften-kenntnisse sowie ein empathisches Verhalten gegenüber jeglichen Mitarbeiterinnen und Mitarbeiter bleiben Kernelemente einer erfolgreichen Ausbildung. Durch ihr gezeigtes Verhalten in der Öffentlichkeit, sowie bei Übungen und Einsätzen aller Art tragen Sie alle zu einem positiven Image des Bundesheeres bei.

Die in den vergangenen Jahren eingeleiteten Reformen und Investitionen sollen das ÖBH fit für die Zukunft machen. Dank der erhöhten finanziellen Mittel wird auch die Waffengattung der Cyberkräfte modernisiert und die Einsatzbereitschaft gestärkt. Die aktuellen Krisen fordern uns mehr den je, unsere Kapazitäten und unsere Fähigkeiten weiter zu stärken. Gleichzeitig bleibt die Personalfrage entscheidend. Wir brauchen im FüUB2 motivierte und gut ausgebildete Soldatinnen und Soldaten, die bereit sind, unsere modernen IKT- und EloKa-Systeme zu bedienen und in den Dienst der Sicherheit unseres Landes zu stellen. Die „Mission Vorwärts" fordert daher auch von allen Bediensteten des FüUB2, aktiv zur Personalgewinnung beizutragen. In diesem Sinne ermutige ich mein Kader weiterhin, auch in Zukunft jenes Engagement und jene Initiative einzubringen, die unser Bataillon als verlässliche Organisation im Frieden aber auch in Krisenfällen auszeichnen soll.

Das FüUB2 am Girls Day 2024

Das Führungsunterstützungsbataillon 2 präsentierte sich am Girls Day 2024 in der SCHWARZENBERG-Kaserne in SALZBURG von seiner besten Seite. Zwischen schweren Pioniermaschinen, dem neuen Hubschrauber Leonardo AW169 und der Militärpolizei konnte auch die Truppe der Führungsunterstützung aus ST. JOHANN IM PONGAU mit einer statischen Vorführung des Geräts und Gesprächen mit der Truppe bei den Teilnehmerinnen und Teilnehmern punkten. Das Gerät der Kaderpräsenzeinheit mit Splitterschutzweste, der neuen Nachtsichtbrille und dem modifizierten Sturmgewehr zog die Aufmerksamkeit der Besucherinnen auf sich. Des Weiteren konnte ein Richtfunkmast mit einer Antenne des Tactical Communication Network (kurz TCN) sowie eine Satellitenanlage besichtigt werden. Erfahrungen, die Absolvierung der Basisausbildung betreffend, konnten durch die Grundwehrdiener des Funkzuges der 3. Führungsunterstützungskompanie an die Besucherinnen weitergeben werden.

Foto: Bundesheer/Dion6

Nationalfeiertag in der Schwarzenbergkaserne

Themeninsel IKT & Cyber

Am 26. Oktober öffnete die Schwarzenbergkaserne die Tore für die Zivilbevölkerung, um den unterschiedlichen Verbänden die Möglichkeit zu geben, ihre Ausrüstung und die damit verbundenen Aufgaben und Fähigkeiten präsentieren zu können.

Foto: Bundesheer/Dion6

Neben den mechanisierten Kräften, dem Jagdkommando, der Militärpolizei sowie den Luftstreitkräften, bot auch das Führungsunterstützungsbataillon 2 (FüUB2) mit der „Cyber-Insel" sein Gerät zur Besichtigung an. Ziel war hier nicht nur neues Personal für den Verband anzuwerben, sondern der Bevölkerung auch die Aufgaben des Verbandes näherzubringen. Bereits am Donnerstag verlegte die 1. Führungsunterstützungskompanie (1.FüUKp) sowie Teile der Führungsunterstützungskompanie (eloKa) nach SALZBURG, um die Geräteschau für den Nationalfeiertag vorzubereiten. Anhand der Cyber-Insel-Module konnten die einzelnen Züge der 1.FüUKp sowie der FüUKp(eloKa) ihre Aufgaben und Fähigkeiten im Einsatz darstellen. Der I.IKTZg präsentierte dabei das Tactical Communication Network (TCN), sowie das Vermittlungssystem Großer Verband. Gezeigt wurde dabei vereinfacht der Aufbau einer Verbindung vom Vermittlungssystem zu einem Gefechtsstand mit unterschiedlichen Anschlüssen. Viele Besucher bestaunten auch die Band IV Antennen des II.IKTZg.

Foto: Bundesheer/Dion6

Mit diesen erfolgt die Einbindung von IKT-Systemen mit hoher Datenrate. Für viele Besucher war nicht nur die Höhe der Antenne beeindruckend, sondern auch der auffallende Antennenkopf. Am meisten wurde die bewegliche Befehlsstelle des Funkzuges bewundert. Vor allem die Tarnung sowie die zwei „versteckten" Fahrzeuge lockten nicht nur Eltern, sondern auch viele Kinder an. Die FüUK-p(eloKa) zeigte ihre Ausrüstung und die Einsatzmöglichkeiten im In- und Ausland. Dargestellt wurde, wie Frequenzen erfasst, und über hohe Reichweiten Informationen gewonnen werden können.

Die hohe Besucheranzahl zeigte das rege Interesse der Bevölkerung an den Fähigkeiten des Bundesheeres. Durch die vielen Gespräche konnten wir vielleicht bei dem einen oder anderen das Interesse an einer beruflichen Laufbahn beim Bundesheer wecken.

Neujahrsempfang beim Führungsunterstützungsbataillon 2

Foto: Bundesheer/Mario Majer

Das neue Jahr begann mit einem besonderen Ereignis im Veranstaltungskalender des Führungsunterstützungsbataillons 2 (FüUB2), dem Neujahrsempfang des Bataillonskommandanten am 12. Jänner 2024. Die Veranstaltung bot insbesondere den Behördenleitern, Lokalpolitiker, Partner und Persönlichkeiten des öffentlichen Lebens die Möglichkeit, sich über die Aufgaben und Leistungen des FüUB2 und die aktuellen Entwicklungen im Österreichischen Bundesheer zu informieren. Ein besonderes Zeichen der gegenseitigen Wertschätzung war aber auch die Anwesenheit zahlreicher Bürgermeister, Schulleiter, Vertreter von Einsatzorganisationen und Vereinsobmänner.

Foto: Bundesheer/Mario Majer

Nach einer Fanfare, gespielt vom Ensemble der Militärmusik Salzburg, begrüßte der Bataillonskommandant, Oberst Johannes NUSSBAUMER die zahlreich anwesenden Gäste. Der anschließende Jahresrückblick wurde in Form einer Videopräsentation gestaltet. Kernpunkt dieses Vortrages war die erfolgreiche Teilnahme der IKT-Spezialisten des FüUB2 an zahlreichen Übungen und Einsätzen im In- und Ausland.

Als besondere Herausforderung bezeichnete Oberst Nussbaumer die Gewinnung und das Halten neuer Mitarbeiterinnen und Mitarbeiter. „Dabei müsse vor allem die deutliche Anhebung des Anteils an Soldatinnen im Österreichischen Bundesheer gelingen", so der Bataillonskommandant. Als ein wichtiges Instrument der Personalgewinnung sieht der Kommandant die Verleihung des Zertifikats „Familienfreundlicher Arbeitgeber". Um die Attraktivität des FüUB2 als Arbeitgeber zu erhöhen verpflichtete sich der Verband zur Verwirklichung einer familienbewussten Personalpolitik. Besondere „Highlights" des vergangenen Jahres waren zudem die Auszeichnung des ehemaligen Gefreiten Michael Bogensberger als „Salzburger Grundwehrdiener des Jahres 2023" sowie der Weltmeistertitel im 50m-Pistolen Bewerb der Frau Stabswachtmeister Sylvia Steiner bei der WM in Baku. Mit der Vorstellung der im letzten Jahr zum FüUB2 ausgemusterten Offiziere und Unteroffiziere und dem Ausblick auf das Jahr 2024 endete das offizielle Programm des diesjährigen Neujahrsempfanges.

Foto: Bundesheer/Mario Majer

Notkommunikationsübung KW/UKW

Im Jahr 2024 wurden im Auftrag der Dion6/IKTCyE zwei Notkommunikationsübungen durchgeführt. Das Ziel dieser Übungen war die Errichtung und der Betrieb eines autarken Netzes mittels Datenfunk- und Satellitenverbindungen, um die Führungsfähigkeit der Generaldirektion für Landesverteidigung (GDLV) im Rahmen von Extremereignissen sicherstellen zu können.

Insgesamt wurden im Rahmen dieser Übungen durch das FüUB2 jeweils drei Netze aus der SCHWARZENBERG-Kaserne betrieben. Dies waren die Leitfunkstellen (LtFuSt) der beiden Netze der Dion1 mit den Militärkommanden, dem VR1 und der AuslEBa als Unterfunkstellen (UFuSt), sowie die LtFuSt im Netz GDLV mit den vier Landbrigaden, der FüUS, dem FüUB1 und dem JaKdo als UfuSt. Zudem befand sich am Standort SALZBURG noch ein Funktrupp BFF-32 von der Dion2 der Luftstreitkräfte. Zusätzlich wurde durch das FüUB2 mit Unterstützung durch das FüUB1 und LuU, eine schichtfähige Netzsteuerung zur Überwachung und Koordinierung der vier Kurzwellennetze gestellt. Bei der Übung am 05. November kam zusätzlich noch das System „Internet via Satellit" zur Überlagerung der Verbindung bei der Notkommunikationsübung zum Einsatz. Ebenso waren in ganz ÖSTERREICH noch Funknetze mit dem UKW-Funkgerät CONRAD zur Sicherstellung der Verbindung zu Dienststellen der Dion4 eingesetzt.

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Insgesamt waren bei den 42 Funkstellen der Direktionen 1, 2, 4, 6 und 8, bei den Militärkommanden, den Brigaden, dem Jagdkommando und den beiden FüUB, gesamt ca. 150 Personen österreichweit bei der Übung eingesetzt. Der Personaleinsatz wurde bei der Übungsleitung und der Einlagensteuerung durch mehrere Bedienstete, vorwiegend gestellt durch die Dion6 ergänzt. Gesamt waren bei der Übung 26 KW und 16 UKW-Stationen im Einsatz, davon wurden sieben Standorte mit Mehrkanal-Satellitenanlagen (MkSAT) ergänzt. Unter Leitung der Dion6/IKTCyE wurden dabei in den Funknetzen 200 Sprüche und über Internet via Satellit 50 Meldungen abgesetzt. Die Übertragung der Sprüche erfolgte fast ausschließlich über die Datenfunksoftware (DaFuSo2).

Die Zielsetzung, Errichtung von autarken Funknetzen im Falle eines Blackout sowie die Sicherstellung der Führungsfähigkeit der GDLV auf operativer Ebene, wurde erreicht.

Tag der Schulen 2024 in der SCHWARZENBERG-Kaserne

Auch dieses Jahr war das Führungsunterstützungsbataillon 2 mit Mannschaft und Gerät beim Tag der Schulen in der Schwarzenbergkaserne vertreten. Schüler wie auch Lehrer konnten sich über die Aufgaben und Fähigkeiten des Verbandes informieren. Das EloKa-Fahrzeug IVECO mit seinem Zubehör war besonders stark besucht. Des Weiteren konnten die Schüler mittels Funkgeräte Gespräche führen, woran sie besonderen Spaß hatten.

Foto: Bundesheer/Wolfgang Riedlsperber

Unter anderem wurde auch das neue Tactical Communication Network (TCN) präsentiert. Die Besucher konnten sich auch das Vermittlungssystem Großer Verband im Detail ansehen. Gespräche zwischen Truppe, Schülern sowie Lehrpersonal durften natürlich auch nicht fehlen. Im Großen und Ganzen war es für das Führungsunterstützungsbataillon 2 ein gelungener Tag. Vielleicht gelang es uns bei dem einen oder anderen das Interesse an einer beruflichen Laufbahn im Bundesheer zu wecken.

Foto: Bundesheer/Wolfgang Riedlsperber

TCN-Betriebsübung Teilnetz FüUB2

Im Rahmen der Übung „COMMON ROOF 24“ wurde im Zeitraum vom 14. bis 17. Oktober 2024 erstmalig eine TCN-Betriebsübung durchgeführt. Diese TCN-Betriebsübung diente im Wesentlichen der Festigung der IKTUO im Umgang mit den TCN-Vermittlungseinheiten im Rahmen eines gemeinsamen Netzwerkes. Weiters diente die Übung der Festigung der Kenntnisse beim Betrieb eines TCN-Netzwerkes mit einem Central Network Operation Center (CNOC), mehreren Network Operation Center (NOC), bei gleichzeitigem Betrieb eines zusätzlichen multinationalen Netzwerkes aus einem sogenannten Subordinated Service Management and Control Operations Element (SSE). Diese SSE, für den internationalen Anteil der Übung, sowie die CNOC für die TCN-Betriebsübung wurden durch das Führungsunterstützungsbataillon 1 gestellt und befanden sich für die Übungsdurchführung in VILLACH.

Foto: Bundesheer/Dion6

Im Teilnetz des Führungsunterstützungsbataillons 2 waren somit eine NOC, die präsente 1. Führungsunterstützungskompanie (1.FüUKp) mit dem Einrückungstermin Juni 2024 sowie der verlegbare Anteil der KPE-Kompanie eingesetzt. Ziel war es, zusätzlich zu den oben angeführten Punkten, einen Organisationsrahmen für eine erste Zielüberprüfung der 1.FüUKp zu stellen und zusätzlich die Kommunikation zwischen den einzelnen Fernmeldestellen (FMSt) und der NOC zu verbessern.

Foto: Bundesheer/Dion6

Auch für das Kaderpersonal der 1.FüUKp war es, seit der Einführung von TCN, die erste Übung in der Aufträge im Kompanierahmen abgearbeitet und mit einer NOC zusammengearbeitet wurde. Bereits die Inbetriebnahme des verlegbaren Anteils gestaltete sich aufgrund des im September eingespielten Updates des TCN-Systems als schwierig, da einige Grundkonfigurationen und Berechtigungen geändert bzw. gelöscht wurden. Durch das Fehlen von Netztrupp-Kommandanten leidet vor allem die seriöse Übungsvorbereitung.

Nach Übungsbeginn konnte das Übungsnetz am Folgeabend gegen 1800 Uhr fertiggestellt werden. Dieses wurde bis zum nächsten Morgen betrieben und anschließend entsprechend den Vorgaben der NOC umgebaut. Die Umbauphase wurde durch die Netzsteuerung und die Führungsunterstützungskompanie für Optimierungen genutzt, sodass diesmal die Errichtung des Netzes bereits am Nachmittag beim ersten Versuch abgeschlossen werden konnte. Für den I.IKTZg der 1.FüUKp galt es Teile eines Brigadegefechtsstandes an mehreren Standorten zu errichten und nach einem teilweisen Gefechtsstandwechsel wieder in Betrieb zu nehmen. Am Donnerstag erfolgte für Teile des I.IKTZg eine Einweisung in die so genannten „ad-hoc-TAP". Diese sollten in den nächsten Wochen zulaufen, die Durchführung von Updates erleichtern, sowie bei Bedarf auch bei Übungen eingesetzt werden.

Durch die KPEKp wurde das Übungsvorhaben vor allem für Erprobungen als Vorbereitung zur „EUROPEAN CHALLENGE 24" in Bergen (DEUTSCHLAND) genutzt. Dabei wurde das Schwergewicht auf die Testung möglicher Einbindungen des Österreichischen Kontingents, abseits der üblichen Einbindungsmöglichkeiten in militärischen Liegenschaften oder Truppenanschaltepunkten (TAP), gelegt. So wurde neben der Einbindung mittels Mehrkanal-Satellitenkommunikationsanlage, auch die Möglichkeiten mittels „Internet-via-Satellit" sowie „ad-hoc-TAP" erprobt. Bereits im Rahmen der Übungsdurchführung konnte man den Mehrwert für die übende Truppe anhand von deutlich verbesserten Betriebsabläufen von Phase 1 auf Phase 2 erkennen. Diese, im Rahmen der Betriebsübung gewonnenen Erkenntnisse, können somit hinkünftig bei Übungen und Einsätzen angewendet werden.

Traditionstag beim FüUB2

Am 04. Oktober veranstaltete das FüUB2 den Traditionstag der Fernmeldetruppe zum Gedenken den unter schwierigsten Bedingungen erbrachten Leistungen der damaligen Telegraphentruppe des k.u.k. Telegraphenregimentes in der 7. Isonzoschlacht 1916. Die besonderen Verdienste dieser Spezialeinheit findet im alljährlichen Traditionstag eine besondere Würdigung. Der Bataillonskommandant, Oberst Johannes Nussbaumer verwies in seiner Ansprache auf die Teilnahme des FüUB2 an der seit Jahren größten Übung des Bundesheeres, der SCHUTZSCHILD24. Die besondere Herausforderung dabei war der erstmalige Einsatz des Tactical Communications Network (TCN) in einem komplexen, bundesländerübergreifenden Einsatz.

Foto: Bundesheer/Wolfgang Riedlsperber

Foto: Bundesheer/Wolfgang Riedlsperber

Die Militärmusik Salzburg leitete mit dem Cybermarsch zum Höhepunkt des diesjährigen Traditionstages, der erstmaligen Verleihung der Cyberleistungsabzeichen in Silber, an verdiente Soldaten des Aktivstandes des FüUB2, durch den Kommandanten der Cyberkräfte, Herrn Generalmajor Hermann Kaponig, über.

Foto: Bundesheer/Wolfgang Riedlsperber

Um das Cyberleistungsabzeichen in Silber zu erhalten, sind besondere Leistungen in der Waffengattung und eine mindestens 15-jährige Fachverwendung innerhalb der Cyberkräfte Voraussetzung. Der Traditionstag mit zahlreichen Ehren- und Festgästen bildete dazu einen würdigen Rahmen. Nach dem liturgischen Teil erfolgte die Kranzniederlegung beim Gedenkstein der Fernmeldetruppe. Das Erbitten weiterer Befehle und der gemeinsame Ausmarsch der angetreten Truppe und Vereine beendete den Festakt.

FüUB2 bester Truppenkörper im Wettkampfjahr 2024

Die Bediensteten des FüUB2 überzeugen nicht nur durch ihre Fachkompetenz im Bereich IKT und EloKa, sondern immer wieder auch in sportlichen Belangen. Im Rahmen der Heeresmeisterschaften im Schibergsteigen 2025 am Truppenübungsplatz Hochfilzen erfolgte die Ehrung der besten Truppenkörper im Wettkampfjahr 2024. Dabei konnte das FüUB2 die Gesamtwertung für sich entscheiden. Die Truppenkörperwertung wird durch die Vergabe von Punkten bei sämtlichen Heeresmeisterschaften ermittelt. Bewertungspunkte werden dabei für die ersten fünfzehn Plätze bei Einzelwettkämpfen in der Allgemeinen- und Seniorenklasse der Männer und Frauen, sowie bei Mannschaftswettkämpfen vergeben.

Foto: Bundesheer/Dion6

Bundesministerium für Landesverteidigung

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Führungsunterstützungsschule

Kommandant FüUS: ObstdG Mag. Franz SITZWOHL, MSc

Nach meiner Rückkehr aus den USA im Juli 2024 übernahm ich wieder das Kommando über die FüUS. Bereits während meines Studiums an der US National Defense University College of Information and Cyberspace in Washington DC begann ich mit den Vorbereitungen zur Ausbildung für die Informationskräfte des ÖBH (PsyOps-Truppe (Psychologischer Kampf) sowie die Kommunikations-Truppe) an der FüUS.

Neben den Cyberkräften, der IKT-, EloKa- (Elektronischer Kampf) und Cyber-Truppe, werden nun neue Fähigkeiten für den Informationsraum etabliert. Dazu sind (Stabs-)Funktionen für Informationsoperationen sowie Informationskräfte auszubilden und für das ÖBH bereitzustellen.

Zunehmend muss dafür auf Expertisen unserer Milizexperten aber auch auf außerhalb des Ressorts zurückgriffen werden. Mit 2025 werden weitere Schritte gesetzt und mit dem Einrichten der Projektarbeitsgruppe „Cyber und Informationstruppenschule (CyITS)“ begonnen. Es werden heuer auch die ersten Lehrgänge an der FüUS abgehalten.

Daneben brachte 2024 eine Vielfalt von Vorhaben sowie Aktivitäten mit sich, welche eindrucksvoll die Bandbreite und die Professionalität des Personals der FüUS widerspiegelten. In einer global unsicheren Zeit ist es umso wichtiger, um im Cyber und Informationsraum gut aufgestellt zu sein. Das Ausrollen des „Tactical Communication Network (TCN)“ wurde durch einen Festakt unserer Frau Bundesministerin Klaudia Tanner gewürdigt.


Foto: BMLV/HBF

Unser Neujahrsempfang, die FüU-Seminare und andere Events informierten über Neuerungen und Planungen im Fachbereich. Aber auch die Beteiligung an Forschungsprojekten und Aktivitäten unterstreichen die vielfältigen Fähigkeiten der FüUS.

Militärische Übungen waren sowohl für Kursteilnehmer als auch für das Kader der FüUS inklusive unseren Milizkameraden und -experten herausfordernd und lehrreich.

Das Highlight unseres Traditionstages waren die Begründung der Partnerschaft mit der Stadtgemeinde LAA AN DER THAYA sowie die erstmalige Verleihung der Cyberleistungsabzeichen in Silber für verdiente Bedienstete.

„Daneben brachte 2024 eine Vielfalt von Vorhaben sowie Aktivitäten mit sich, welche eindrucksvoll die Bandbreite und die Professionalität des Personals der FüUS widerspiegelten. In einer global unsicheren Zeit ist es umso wichtiger, um im Cyber und Informationsraum gut aufgestellt zu sein.“

Neujahrsempfang der FüUS

Am 30. Jänner 2024 fand der Neujahrsempfang der FüUS in der STARHEMBERG-Kaserne statt. Obst HOFFMANN konnte zahlreiche Gäste begrüßen. Nach einem kurzen Rückblick inklusive einiger Zahlen und Fakten des vergangenen Jahres folgten interessante Beiträge zu den wichtigsten Aufgaben der FüUS. Ein Exkurs zur Ausbildung am TCN war ebenso kurzweilig wie ein Einblick in EloKa. Danach folgte eine ausführliche Information inkl. zukünftiger Ausblicke betreffend der Ausbildung der Cyber GWD durch das Lehrelement.

Im Zuge der Vorstellung des Vereins „Freunde der Führungsunterstützungsschule" durch den ehemaligen Schulkommandanten Obst i.R. Christian WALLY betonte auch er die Wichtigkeit der FüUS, besonders in der Zukunft. Am Ende der Feierlichkeiten wurde außerdem das "ausgediente" Fernmeldebewährungsabzeichen der Fernmeldesammlung des HGM zur historischen Aufbewahrung übergeben.

Foto: Bundesheer/Dion6

Ausbildung TCN

Die FüUS blickt auf eine erfolgreiche Durchführung der TCN-Ausbildung im Jahr 2024 zurück. Im 1. Quartal wurden ca. 100 Personen erfolgreich ausgebildet, womit ein weiterer solider Grundstein für die Einsatzbereitschaft des TCN Systems gelegt wurde.

Foto: Bundesheer/Dion6

Von März bis Juli 2024 erfolgte dann die planmäßige Rückgabe des zu Ausbildungszwecken an die FüUS ausgegebenen Geräts.

Ende Juli führte das Kernteam TCN/FüUS beim FüUB1 einen Workshop durch um solide Grundlagen und Curricula für die weitere zukunftsfähige Durchführung der TCN-Lehrgänge zu gewährleisten.

Zudem fand unter der Verantwortung der FüUS im Jahr 2024 jeweils ein ausgelagerter Lehrgang beim FüUB2 und beim StbB6 statt. Diese ermöglichten es, Expertise ortsnah und effizient zu vermitteln.

Die Zusammenarbeit mit dem TCN Kernteam wird seitens der FüUS weiterhin gepflegt, um Änderungen sowie Neuerungen so effizient wie möglich an die Truppe kommunizieren zu können. Die FüUS setzt auch im kommenden Jahr auf hohe Ausbildungsqualität und praxisorientierte Weiterbildung.

Übergabe TCN und MUV NORIKER

Am Montag, den 18. März 2024, fand die Übergabe des Kommunikationssystems TCN statt. FBM Klaudia TANNER übergab im Beisein von GenMjr Harald VODOSEK und GenMjr Hermann KAPONIG das neue System an die Truppe. Durch das Kommunikationssystem werden wesentliche Voraussetzungen für die Digitalisierung geschaffen. Zudem wurde erstmals der Nachfolger des Fernmelde-Pinzgauers, der IVECO Multirole Utility Vehicle (MUV) „NORIKER" vorgestellt.

Foto: Bundesheer/Dion6

Mit dieser Beschaffung erlangt das ÖBH die Fähigkeit, die breitbandige Vernetzung im Fernmeldesystem des Österreichischen Bundesheeres bis auf Einheitsebene und zu wichtigen Sensoren sicherzustellen. Die beschafften TCN - Gerätesätze werden bei den Führungsunterstützungskompanien der Brigaden, den IKT–Zügen der Bataillone und den Führungsunterstützungsbataillonen eingesetzt und finden sich in Wechselaufbauten, Sheltern und Containern genauso wie in Fahrzeugen wie IVECO „NORIKER", PANDUR oder ULAN.

Die Schulungen am neuen System übernimmt die FüUS als zentrale Ausbildungsstätte des Führungsunterstützungspersonals.

ALPENTRIODE 2024

Diese trinationale Übung mit angehenden IKT-Offizieren aus DEUTSCHLAND, ÖSTERREICH und der SCHWEIZ ist fester Bestandteil der internationalen Kooperation. Der Austausch mit anderen Nationen bringt hohe Erweiterung der internationalen Kompetenzen. Das Zusammenspiel zwischen operativem und taktischen Planungsprozess kann, speziell hinsichtlich der Offiziersausbildung, sehr gut dem österreichischen Modell angepasst werden.

Foto: Bundesheer/Dion6

Ziel der Übung war die Planung der Gefechtsstände der eingesetzten Manöverelemente sowie deren Verbindungsrelationen sowie IKT-Planung für die im Rahmen der Division eingesetzten Brigaden.

Die Bedeutsamkeit der Anpassung des Bundesheeres an internationales Niveau im Bereich Ausstattung und Infrastruktur, ist durch den Aufenthalt deutlich geworden. Die Interoperabilität mit DEUTSCHLAND und SCHWEIZ ist möglich, bedarf jedoch einer Anpassung der zur Verfügung gestellten finanziellen Mittel. Die ALPENTRIODE zeigt deutlich die Gemeinsamkeiten sowie feinen Unterschiede in den Planungsverfahren aller drei Armeen. Die Deutsche Bundeswehr verwendet primär Satelliten- Kommunikation, welche in Österreich noch wenig bis kaum Anwendung findet. Eine Weiterentwicklung der Ausbildung an der FüUS im Bereich SPACE ist daher notwendig und sachdienlich.

Kommandant Fernmeldestelle: Eine fordernde militärische Ausbildung

Die Ausbildung zum Kommandanten Fernmeldestelle ist ein intensiver Lehrgang, der technisches Fachwissen, Gefechtstechniken und Führungsqualitäten unter anspruchsvollen Bedingungen vermittelt.

Foto: Bundesheer/Dion6

Der Lehrgang deckt die Themenfelder Grundlagen der Cyberkräfte, Gefechtstechnik, Waffen- und Geräteausbildung sowie standardisierte Befehlsformate ab. Beginnend mit der zweiten Woche erfolgt die praxisorientierte Ausbildung im Gelände, unterstützt durch den Einsatz von Simulationssystemen und realitätsnahen Szenarien wie das Scharfschießen.

Die abschließende Bewertung setzt sich aus schriftlichen und praktischen Prüfungen zusammen, wobei die fehlerfreie Anwendung der Befehlsformate sowie der Ablauf an der FMSt im Fokus steht. Zu den zentralen Herausforderungen zählen die Bereitstellung qualifizierter Ausbilder und technischer Ressourcen sowie die Anpassung an komplexe Einsatzbedingungen. Eine mögliche Verlängerung des Lehrgangs wird erwogen, um die praktische Ausbildung weiter vertiefen zu können.

Tag der Schulen

Am Donnerstag, den 12.09.2024, fand in der STARHEMBERG-Kaserne der "Tag der Schulen" statt. Mit Unterstützung der Miliz-Kameraden wurden den Jugendlichen die Tätigkeiten der FüUS nähergebracht. Diese konnte sowohl in Lehrsälen als auch am Kasernengelände erfahren und ausprobiert werden.

Die Angehörigen der FüUS zeigten ihre Leistungen und Fähigkeiten am Gerät.

TCN war eines der Herzstücke dieser Leistungsschau. Auch konnten die Schüler neben dem Funküberwachungs- und Ortungssystem RAMON beim Gefechtssimulationssystem CATT (Combined Arms Tactical Trainer) selbst interagieren. Abgerundet wurde mit Stationen zu den Themen Kurz- und Ultrakurzwelle.

Zusätzlich zur FüUS präsentierte sich auch die Theresianische Militärakademie und zeigte die Möglichkeiten einer Karriere als IKT-Offizier auf.

Auch vor Ort waren Vertreter der Dion6, um aus den Bereichen Militärisches Geowesen und Militärische Cyberabwehr zur informieren. Ein besonderes Highlight war der "Escape Room" der Dion6, in welchem jeweils zwei Teams gegeneinander spielen konnten.

Foto: Bundesheer/Dion6

Bei der Sportstation sorgte das Lehrelement mit einem ausgewählten Trainingsprogramm für schweißtreibende Momente.

Foto: Bundesheer/Dion6

Führungsunterstützungsseminare

Die jährlichen Führungsunterstützungsseminare sind eine zentrale Veranstaltung für die Weiterbildung und Vertiefung von Kompetenzen im Bereich der militärischen Kommunikation und Führungsunterstützung.

Die Keynotes wurden durch GenMjr KAPONIG bei den Offizieren und Vzlt Leopold RADLMAIR bei den Unteroffizieren übernommen. Ein Schwergewicht stellte bei beiden Seminaren das Zielbild ÖBH 2032 dar, welches aus Sicht der Planung und der Bereitstellung ausführlich dargelegt wurde.

Foto: Bundesheer/Dion6

Ebenso wurden die neuesten Entwicklungen im Bereich TDR und TCN präsentiert. Ein Lagebericht über den Einsatz während der Schutzschild verdeutlichte dabei die Herausforderungen für die kommenden Jahre. Auch dieses Jahr fanden unsere Kameraden aus dem DACH Verbund den Weg zu uns, heuer mit Vorträgen über die Führungsinformationssysteme der Deutschen Bundeswehr und der Schweizer Armee. Der Besuch durch General Rudolf STRIEDINGER unterstrich die Wichtigkeit dieses Vorhabens.

Foto: Bundesheer/Dion6

Forschungsprojekt Bumblebee

Die FüUS führt gemeinsam mit dem Austrian Institute for Technology (AIT), der Militärakademie und der Zentralen Dokumentation (ZentDok) der Landesverteidigungsakademie das Forschungsprojekt Bumblebee durch. Ziel ist es, eine Ausbildung für ein zukünftiges Cyberlabor zu erstellen. Die Zusammenarbeit mit einer zivilen Forschungseinrichtung ermöglicht es, die Abläufe außerhalb des ÖBH besser zu verstehen und die für uns geeigneten Ausbildungsinhalte zu implementieren. 2024 fand bereits eine erste Testphase statt, in der die Fähnriche des Studienganges „Militärische IKT-Führung" (millKTFü) gemeinsam mit den Cyber GWD der ZentDok sowohl ihre Fähigkeiten verbessern konnten, als auch das neu Gelernte in praktischen Aufgaben unter Beweis stellen mussten. Die daraus gewonnenen Erfahrungen werden genutzt um das Ausbildungskonzept zu verbessern und in einer neuerlichen Übung 2025 zu erproben. Nach Abschluss des Projekts kann die FüUS dieses direkt in die Ausbildung integrieren.

Miliz an der FüUS

Auch heuer bewiesen die Kameraden der Miliz erneut, dass sie ein unverzichtbarer Bestandteil der FüUS sind. Unabhängig vom Dienstgrad oder Funktion zeichnete sich dies durch eine hohe Bereitschaft zur Unterstützung im täglichen Dienst- und Ausbildungsbetrieb und durch die Teilnahme an Einsätzen im In- und Ausland aus. Erstmals wurde ein Miliz Jour Fixe in Kooperation mit dem Sanitätszentrum Ost (SanZ Ost) durchgeführt, ein weiteren Schritt zur Stärkung der Zusammenarbeit.

Ein Highlight war die Teilnahme der Experten im Militär an der beorderten Waffenübung der Dion6. Dabei wurden zentrale militärische Fähigkeiten, wie die sichere Handhabung von Waffen, im Rahmen eines durch die FüUS organisierten Scharfschießens aufgefrischt. Ein wesentlicher Schwerpunkt lag dabei auf der Ausübung der jeweiligen Einsatzfunktion.

Einige Milizkameraden leisteten hier einen bedeutenden Beitrag zur Weiterentwicklung der Ausbildung der Cyber GWD und trugen so aktiv zur Zukunftsfähigkeit der FüUS bei.

Cyber Grundwehrdienst an der FüUS

Ob als Programmierassistent oder Netzwerktechniker in der Dion6, als Informations- und Dokumentationsgehilfe an der LVAk oder als IT-Gehilfe bei den Schulen, den Brigaden und Militärkommanden, Cyber GWD leisten einen unverzichtbaren Beitrag im ÖBH, überall dort wo IT-Kenntnisse verlangt werden. Ihr Grundwehrdienst gliedert sich in 2 Monate Ausbildung und 4 Monate Dienst in der Funktion.

Mit April 2024 wurde Olt WESELKA als neuer Kommandant des zentralen Cyberschulungszentrums (zCSZ) ernannt. Seither wurde die Ausbildung Schritt für Schritt modernisiert. Das zCSZ an der FüUS ist die ausbildungsverantwortliche Stelle, welche die unterschiedlichen Funktionen in einem gemeinsamen Kurs auf die späteren Verwendungen vorbereitet. Insgesamt wurden 3 Cyber Basiskurse im Februar, Juni sowie Oktober 2024 für je ca. 60 GWD durchgeführt. Mit jedem Kurs steigen die Ansprüche und die Qualität der Ausbildung. Neue Kursinhalte zum Thema Künstliche Intelligenz (KI) und Technologien der Zukunft sind nur ein Teil.

Der Weg ist klar. Das Potenzial der jungen IT-Absolventen, welche zu uns kommen, ist noch lange nicht ausgeschöpft. Um die nötige Tiefe und Qualität für eine Cyber Ausbildung der Zukunft zu erreichen, wird 2025 eine Verdreifachung der Kursdauer unumgänglich!

Foto: Bundesheer/Dion6

Traditionstag der Führungsunterstützungstruppe am 08.10.2024

Im Rahmen des militärischen Festaktes werden jedes Jahr die Verdienste der Telegraphentruppe gewürdigt.

Heuer wurde dieser Festakt noch durch weitere Höhepunkte gekrönt: Die Verleihung der Cyberleistungsabzeichen in Silber, die Unterzeichnung der Partnerschaftsurkunden mit der Stadtgemeinde LAA AN DER THAYA sowie der Besuch unserer FBM TANNER.

Foto: Bundesheer/Dion6

Am Festakt nahmen Vertreter aus Politik und Wirtschaft, Partner der FüUS sowie ehemalige Angehörige teil. Während dieses feierlichen Rahmens wurde die Verleihung der Cyberleistungsabzeichen in Silber durch GenMjr Kaponig an verdiente Mitarbeiter vorgenommen.

Ein Highlight der Veranstaltung war die Unterzeichnung der Partnerschaftsurkunden zwischen der Stadtgemeinde LAA AN DER THAYA, vertreten durch Frau Bürgermeisterin Brigitte RIBISCH sowie der FüUS, vertreten durch ObstdG Franz SITZWOHL. Anschließend wurden zum Gedenken an verstorbene und gefallene Kameraden Kränze am Denkmal der STARHEMBERG-Kaserne niedergelegt.

Abschließend würdigte FBM den neuen Partner mit der offiziellen Auszeichnung "Partner des Bundesheeres" und gratulierte den Trägern der Cyberleistungsabzeichen recht herzlich.

Foto: Bundesheer/Dion6

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Bundesministerium für Landesverteidigung

Bundesministerium für Landesverteidigung

Grafik: KI-generierte Bildmontage, Bundesheer/Dion6

Unsere Partner

Direktion 6 – IKT und Cyber

SPENGERGASSE
ausbildung mit zukunft

Führungsunterstützungsbataillon 1

villach

Führungsunterstützungsbataillon 2

St. Johann Salzburg

SIEMENS

Führungsunterstützungsschule

Stadtgemeinde Laa an der Thaya

WIENER NETZE

Abbildungsverzeichnis

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 Softwareentwicklungsumgebung)
Appl	Abteilung Applikation
Application Level Firewalling	Netzwerksicherheitskomponente auf Anwendungsebene
Arbeitsplatzfixes	Fehlerbehebungspunkte von Softwareproblemen
ArcGIS	Geoinformationssystem-Software
ARWT	Amt für Rüstung und Wehrtechnik
ASECOS	

AssE	System zur verschlüsselten Übertragung von Daten
Audit	Assistenzeinsatz
AÜG	Überprüfung
AUT	Arbeitskräfteüberlassungsgesetz
AUTCON	Austria
AUVA	Austrian Contingent (Kontingent im Auslandseinsatz)
	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	
BMLRT	

Stichwortverzeichnis

BMLV

BMS

BOS

Bruteforce

BRZ

BV Meldung

BVT

BVT/CSC

BWÜ

C

C4

CAD

Carrier-Ethernet

CCI

CFBLNet

ChangeManagement

Chat

ChdStb

Chipkarte

CIO/CDO

CIRP

CISDefence

CKM

CKMS

- Bundesministerium für Inneres
- Bundesministerium für Landwirtschaft, Regionen und Tourismus
- Bundesministerium für Landesverteidigung
- Battlefield Management System
- Behörden und Organisationen mit Sicherheitsaufgaben
- Methode, unerlaubten Zugriff auf IT-Systeme zu erlangen
- Bundesrechenzentrum
- Meldung Besonderer Vorfälle
- Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
- BVT/Cyber-Security-Center
- Beorderten-Waffenübung
- Cyber Crime and Competence Center (nationale Koordinierungs- und Meldestelle zur Bekämpfung von Cyberkriminalität)
- Computer-Aided-Design (Rechnerunterstütztes Konstruieren)
- Erweiterung von Ethernet für Telekommunikation
- Controlled cryptographic Item
- Combined Federated Battle Laboratories Network (Netzwerk zum simulieren von Trainingsumgebungen)
- Laufendes umfassendes Veränderungsmanagement
- digitale Umgebung zum Nachrichtenaustausch
- Chef des Stabes
- Mittel zur Authentifizierung
- Chief Informational Officer/Chief Digital Officer

CMS	(strategische Position in der Führungsebene im Bereich IT)
CNA	College International pour la Recherche en Productique (Internationale Akademie für Produktionstechnik)
CND	Computer and Information Systems Defence
CNE	Cyberkrisenmanagement
CO-IServices	Chipkarten-Management-System
COMEX	Content Management System
COMMON ROOF	Computer Network Attack
COMSEC	Computer Network Defence
Content Disarm and Reconstruction	Computer Network Exploitation
Core-Services	Community of Interest Services (Interessensgemeinschaft)
Covid-19	Communication Exercise 20
CR	Internationale Übung für Interoperabilität im DACH Raum
CST	Communication security
Custom App	Technologie um Schadsoftware aus Daten zu entfernen
CWIX	Kerngruppe wichtiger Anwendungen (z.B. E-Mail, VPN, etc.)
Cybär	SARS CoV-2 Virus („Corona-Pandemie“)
CyberTruppe	Common Roof (Übung)
Cyberabwehr	Custodial Support Team
Cyberangriff	Angepasste Applikation
Cyberbedrohung	Coalition Warrior Interoperability Exercise
Cyberdomäne	Maskottchen IKT&CySihZ
Cyberkoordinator	Militärisches Element zur Beherrschung des vollen Spektrums des Kampfes in Computernetzwerken
Cyberkräfte	Abwendung von Attacken auf Netzwerke und Computersysteme
Cyberkriminalität	
Cyberkrise	

Stichwortverzeichnis

Cyberlage	▶ Gezielte Attacke auf größere Rechnernetzwerke, spezifisch wichtiger Infrastruktur
CyberOps	▶ Bedrohungen im Cyberraum (Cyber Kriminalität, Identitätsmissbrauch, Cyberangriffe oder der Missbrauch des Internets)
Cyberraum	▶ Dimension der militärischen Einsatzführung, wie Land, Luft, See oder Weltraum
Cybersicherheit	▶ Steuerungsorgan der Cyberdömane des BMLV auf strategischer Ebene
Cyberverteidigung	▶ Teilstreitkraft des ÖBH zur Beherrschung sämtlicher taktischen Maßnahmen zum Schutz der militärischen Netze
Cybervorfälle	▶ Straf- oder verwaltungsstrafrechtlich relevante, normierte Angriffe aus dem Cyberraum
	▶ Eskalationsstufe von Cybervorfällen, ausgerufen durch den BMI (NISG §3 Abs.22, §24)
D	▶ Darstellung der Eigenlage des ÖBH im Cyberraum und als Teil des militärischen Gesamtlagebildes
DACAN	▶ Cyber-Operations (Handlung im Cyberraum)
DACH	▶ Der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab
DADR	▶ Gesamtheit aller Technologien, Prozesse und Vorgehensweisen , die Netzwerke, Computer, Programme und Daten vor Angriffen, Schäden oder unerlaubten Zugriffen schützen sollen
DAEDALUS	▶ Gesamtheit aller Maßnahmen zum Schutz vor Cyberangriffen und zur Erhöhung der Cybersicherheit
Datenfunksoftware	▶ Böswilliges oder versehentlich herbeigeführtes Ereignis, das die Cybersicherheit eines Informationssystems oder die Sicherheit der verarbeiteten Informationen gefährdet oder Sicherheitsrichtlinien, Sicherheitsprozesse oder Nutzungsbedingungen verletzt
Dashboard	
Data Loss Prevention	
DBMS	
DDoS	▶ distribution and accounting agency NATO
DGIWG	▶ Deutschland-Österreich-Schweiz
DGMN	▶ Deployable air defence radar
DhFMO	▶ Luftraumsicherungsoperation
DhSys	▶ Software zur Übertragung von Daten über Funk
Dienstenetz	▶ Visualisierung von Daten
	▶ Maßnahme zum Schutz der Vertraulichkeit von Daten
	▶ Datenbank Management System

Digitaler Zwilling	
Digitalisierung	
dpi	
DSB	
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	
Emotet	
EOW	
ePAT	
EPR	
ERGIS	
ESS	
ETB	
Ethernet	
EU Battle Groups	
EUBG	

Stichwortverzeichnis

FüSim	
FüU	
FüUB	
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	
Global Mapper	
GNSS	
GOB	Erste Verteidigungslinie
Goldhaube	Fernmelde-Planung
GovCERT	Federated Mission Networking
GovNetBox	Fernmeldesystem ÖBH
GPS	Funknetzmanagementsystem (Software)
Grafana	IKT-Fähigkeiten des ÖBH, die Bedarfsträgern nicht zur Verfügung stehen, sind zentral beim IKT&CySihZ bereitzuhalten
Grundwehrdienst	Österreichisches Verteidigungsforschungsprogramm
GStb	Forschungsprojekt Cyber Attack Decision and Support Platform
GUI	Free & Open Source Software for GeoInformationSystems
GWD	Frequenz- und Schlüsselwesen
GWS	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
	Führungssimulator
	Führungsunterstützung
	Führungsunterstützungsbataillon

Stichwortverzeichnis

H

- Hardware
- Headset
- HF
- HGG
- HGLLG
- HLogZ
- HNaA
- Homeoffice
- Hotline
- HPA
- HTBLVA
- HTS
- HTTP
- HTTPS
- Hybride Bedrohungen

I

- i3VE-Smartphone
- Identity Awareness
- IDU
- IFC
- IFF
- IKDOK
- IKT

- Geografisches Informations System
- GIS Software-Komplettlösung
- Global Navigation Satellite System
- Geschäftsfallorientierte Bearbeitung
- Passives Element der österreichischen militärischen Luftraumüberwachung (primär und sekundär)
- Governmental Computer Emergency Readyness Team
- Hochsichere VPN-Lösung für bestimmte Geheimhaltungsstufen
- Global Positioning System
- Programm zur graphischen Darstellung von Daten
- Pflicht eines jeden österreichischen Staatsbürgers, der als tauglich eingestuft ist
- Generalstab
- Graphical User Interface (grafische Benutzeroberfläche)
- Grundwehrdiener/-dienst
- GeoWebService

- Physische Komponenten in der IT
- Kopfhörer mit Mikrofon
- High Frequency (Hohe Frequenz)
- Heeresgebührengesetz
- Hochgebirgslandelehrgang
- Heereslogistikzentrum
- Heeresnachrichtenamt
- Büroarbeit am Wohnort
- Heißer Draht (Telefonischer Auskunfts- und Beratungsdienst)
- Heerespersonalamt

IKT-Truppe	
IKTBetr	
IKTCyPl	
IKTPl	
IMM	
Inbound	
Incident	
Incident Handling Process Post Incident	
Incident Response	
InfluxDB	
Information Protection Node	
INMARSAT	
InstFl/FlFlATS	
Intrusion Detection and Prevention	
IP-Netzwerke	
IRIDIUM	
ISK	
ISMS	
IT	
ITSM	
iZMS	
	Höhere technische Bundes Lehr- und Versuchsanstalt
	Heerestruppenschule
	Hypertext Transfer Protocol
	Hypertext Transfer Protocol Secure
	Einsatz von konventionellen und unkonventionellen Methoden durch staatliche und nichtstaatliche Akteure in koordinierter Weise, ohne die Schwelle eines offiziell erklärten Krieges zu erreichen.
	iPhones speziell gesichert für das sichere militärische Netz
	Identitätsbewusstsein
	Integrated Display Unit (Displayeinheit für Luftfahrzeuge)
	Industry Foundation Classes (ISO-Standard zur digitalen Beschreibung von Gebäudemodellen)
	Identification Friend/Foe (Freund-Feind-Erkennung)
	Innerer Kreis der operativen Koordinierungsstruktur
	Informations- und Kommunikationstechnologie (Überbegriff aller computer- und netzwerkbasierten Technologien, als auch der verbundenen Wirtschaftsbereiche)
	Truppenteil der Cyberkräfte
	IKT-Betrieb (Bereich des IKT&CySihZ)
	Planungsabteilung IKT&Cyber für die GDLV
	Abteilung IKT-Plan im BMLV
	Informationsmodul Miliz
	Eingehend (Datenübertragung)
	Vorfall
	Bewältigung von Vorfällen
	Reaktion auf Vorfälle

J

J5	
J6	

Stichwortverzeichnis

Liferay DXP	Kommando Führungsunterstützung und Cyber Defence
Loadbalance	Kommando Streitkräfte
Lockdown	Kommando Streitkräftebasis
LOD	Kosovo Forces (Höchster Geograph der KFOR)
Log	Künstliche Intelligenz
LOGIS	Identische Kopie (des Betriebssystems)
Look-and-Feel	Aufreihung vieler Geräte auf denen das geklonte Betriebssystem installiert wird
LOR	Kryptographie (Wissenschaft der Verschlüsselung von Informationen; Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind)
LRR	Kursinformationssystem
LRSiOp	Kurzwelle Land
LSF	
LTE	
Lu/Lu Schießen	
LuAufklESt	Markieren/Beschriften von Daten/Objekten
LVId	Local Area Network (Lokales Netzwerk)
LWL	Chipkartentechnologie
LZ	Leichter Mehrzweck-Hubschrauber des ÖBH
	Luftfahrtgesetz

M

	Lessons Identified/Lessons Learned
Malware	PuMa-Ablöse (neues CMS)
Matchbox	Lastverteilung in Netzwerken
MAVE	Eine Ausgangssperre oder Absperrung bzw. Versiegelung von Gebäuden und Bereichen
mblGeoEt	Low Altitude Danger (Unterer Luftraum, Flugbeschränkungsgebiet)
MD	Dokumentationsdaten von Änderungen/Ereignissen
Metadaten	Logistikinformationssystem
Metrics Collection	Aussehen und Bediengefühl

Stichwortverzeichnis

MPH FTCN	Military Computer Emergency Readyness Team
MPR	military Cyber-Protection System (Militärisches Cybersicherheitssystem)
MSK17	Militärisches Geowesen
MSS	Militärisches Geowesen Virtual Analysis
MTM	Militärisches Informationssystem
Multiplexing	Streitkräfte, die zum größten Teil/vollständig aus Wehrpflichtigen im Bedarfsfall aufgestellt werden
MUX	Experten aus verschiedenen Wissensgruppen aus dem Milizstand
	Militärisches Immobilien Management Zentrum

N

NAFRA	Malware Information Sharing Platform (Plattform für Bedrohungsinformationsaustausch)
NATO	Einsatznetzwerk
NavWar	System zur Planung von Einsätzen
NCAS	Militärische Landesbeschreibung
NDA/MoD	Midlife Upgrade
Network Deception Lösung	Modus selektiv/Modus verschlüsselt (Sekundärradar)
NGIF	Bewegungskrankheit
NISG	Europäische Ausbildungsinitiative zur Verbesserung der Gebirgseinsatzfähigkeit
NSA	Mobilität in der Verwaltung (Zentrale Steuerung aller Dienstkraftfahrzeuge der Ministerien)
NVÖ	Navigationssystem (Aktuelle Position wird immer in der Mitte der Karte anstatt als Koordinaten angezeigt
	Mid Planning Conference
	Future Tactical Communication Network
	Microwave Packet Radio

O

ÖBH	Militärstrategisches Konzept 2017
	Microwave Service Switch
	Mail- und Termin Management
ObstdG	Prozess des MUX
ODU	Multiplexer analoge/digitale Selektionsschaltung, bei der aus mehreren Eingängen ein Ausgang geschaltet werden kann
OE	

Stichwortverzeichnis

PKI

Plug and Play

PM-Bund

PostgreSQL

PrK

ProofofConcept

PS-NT

PTC

PTMP

PTT

PuMa

Q

QGIS

QR-Code

R

Radar

RadStlg

Ransomware

Rasterbildform

RCID

RCIED

Rechenzentrum

redundant

Release

Reputationsdatenbanken

zugänglich, Quellcode öffentlich verfügbar)

- Operationskoordination
- Amerikanisches Soft- und Hardwareunternehmen
- Österreichischer Rundunk
- Organisation (Abteilung im BMLV)
- Organisationsplan Informationssystem
- Organisationsplan
- Ortsfeste Radarstation
- Verzerrungsfreie und maßstabsgetreue Abbildung der Erdoberfläche aus Luft- oder Satellitenbildern abgeleitet
- Ausgehend

- PERSIS Automationsunterstützte Abrechnung von Nebengebühren
- Neue, zeitlich begrenzte, weltweite, starke Ausbreitung einer Infektionskrankheit mit hohen Erkrankungszahlen
- Personalabteilung A im BMLV
- Personal Applikationen
- Personalinformationssystem
- Post Gre Backup Restore
- Beschaffung persönlicher Daten anderer unwissender Personen
- InteroPerability and DIgitization Of INtelligencE GathEring PRocesses ;)
- Public Key Infrastructure (System, das digitale Zertifikate ausstellen, verteilen und prüfen kann)
- Anschließen und loslegen
- Personalmanagement des Bundes mit SAP
- Freies objektrelationales DBMS
- Präsidentschaftskanzlei
- Funktionsbeweis eines ersten Prototypen
- Personalsysteme Neue Technologie

Stichwortverzeichnis

S

SD4MSD	verbreiteten Architektur von Kommunikationsprotokollen
SDH	Resilient Position Navigation and Timing Testing for Defence
SecOps	
Security Patches	Veröffentlichung neuer Softwareproduklte und die Verteilung an Kunden sowie die Integration in bestehende Systeme
selWLANRekr	Netzwerkgerät, das Daten zwischen mehreren Netzwerken weiterleitet (trennt Netzwerke)
SIEM	Wegfindung im Netzwerk zur nächsten Station eines Datenpaketes
sihpolAssE	Restricted Operation Zones
Silentel	Rapid Response Team (Schnell einsatzbereites Team)
SIM-Karte	Resolute Support Mission
SK	Gehärtete Notebooks
SKB	Abteilung für Rüstungspolitik im BMLV
SMIR	Retrieval Ware (Metadatensuchmaschine)
SMN	Rechenzentrum
SMN.mobile	Ressourcen-, Ziel- und Leistungsplan
SMS	
Software	
Spam	
Spoofing	Security Accreditation Authority (Akkreditierung von Informations- und Kommunikationstechniksystemen)
Sport	Storage Area Network
SSD	Software-Testumgebung; Isolierter Bereich ohne Auswirkung auf die Umgebung
SSP	Für den Betrieb essentielle Arbeitskräfte
SSP ZABL	Schlüsselwesen
SSP ZS	Single Channel per Carrier Mode (Ein Kanal pro Gerät)
SSRS	Single Device for Multiple Security Domains (Ein Endgerät für verschiedene Sicherheitsstufen)
Stammportal	Synchrone Digitale Hierarchie
	Security Operations

Stichwortverzeichnis

TKV	Bundes
TLZ	Standardisation Agreement - NATO
TN	Alleinstehendes (IT-)Produkt
topographisch	Sicherheitsunbedenklichkeitsbescheinigung
Tracker	Software
Tunneling	Multinationale Hubschrauber-Übung
TÜPl	Umschalter, Weiche (Kopplungselement in Rechnernetzwerken)
TvZ	

U

	Technical Agreement
UHF	Tragbarer flacher, leichter Computer mit Bildschirm der durch Eingaben mit den Fingern reagiert
UNFICYP Force Cartographer	Gerät zur Horizontalrichtung- Vertikalwinkel- und Schrägstreckenbestimmung
UNIS	Truppenanschaltpunkte
Updates	Tactical Communication Network
URL	Time Division Multiplexing (Methode zur Übertragung von Datenströmen)
UseCase	Technische/Taktische Fähigkeiten
USV	Technologiegespräche Forum Alpbach
UZEloKa	Datenökosystem (Liste aller Technologiedienste zum Erstellen/Ausführen einzelner Anwendungen)

V

	Teilmobilisierung der Streitkräfte (Einberufung von Teilen der Miliz)
VbÜb	Ableistung des Grundwehrdienstes mit leichten körperlichen Einschränkungen, „Grundwehrdienst nach Maß“
VersNr	Regelmäßiges Arbeiten an einem anderen Arbeitsplatz als das Gebäude des Arbeitgebers
VFR/IFR	Truppenfunksystem
VHF	Informationsbeschaffung über Bedrohungen und Bedrohungsakteure im Cyberraum
Visual Computing	Erkennung, Untersuchung und Reaktion auf Schadsoftware im Netzwerk
Visualisierung	NATO Luftraumüberwachungsübung, an der nur Einheiten mit Tiger im Namen oder Wappen

Stichwortverzeichnis

WPTT	Grafische Datenverarbeitung
WSM	Umwandlung abstrakter Daten in eine grafische, visuell erfassbare Form
X	
	Videokonferenzsystem 13
	Verlegbares Fernmeldesystem
XIRIS	
	Verlegbares Rechenzentrum
Z	
	Virtuelle Maschine (virtuelle Umgebung zur Simulation von IT-Geräten, PC am PC)
ZBS	Vollzugsordnung für den Funkverkehr
ZEDVA	Virtual Private Network (gesicherte Netzwerkverbindung mithilfe von Tunneling)
ZentDok	Virtual Reality (Virtuelle Realität - meist mit Vollvisierbrille)
Zerologon	
	Überkeit hervorgerufen durch die Verwendung einer VR-Brille (vergleichbar mit Seekrankheit)
ZGeoBW	
	Very Small Aperture Terminal (Satellitenempfänger und Sender mit Antennen für satellitengestützte Kommunikation)
zIaaS	
ZMS	Verpflegsteilnehmer-Erfassung und bargeldlose Abrechnung
ZTA	Video-Tele Conference (Videokonferenzsystem)

Bundesministerium für Landesverteidigung

IMPRESSUM:
Republik Österreich
Bundesministerium für Landesverteidigung

Medieninhaber:
Republik Österreich / Bundesministerium für Landesverteidigung (BMLV)
Roßauer Lände 1, 1090 Wien
Herausgeber: Direktion 6 - IKT und 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 und Cyber,

Produziert nach den Richtlinien des Österreichischen Umweltzeichens

Platzhalter für Zertifizierungslogo

Bundesministerium für Landesverteidigung