LEISTUNGSBERICHT

DIREKTION 6 – IKT und CYBER

2025

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

Liebe Leserinnen und Leser!


Foto: BMLV/HBF

BM Mag. Klaudia Tanner

Die geopolitische Sicherheit ist im Wandel und stellt uns speziell in Europa vor neue Herausforderungen. Die Entwicklung neuer Technologien schreitet mit immenser Geschwindigkeit voran und erfordert ständige Anpassungen und Erneuerungen. In diesem Kontext steht das Österreichische Bundesheer vor neuen Aufgaben, die auch die Direktion 6 – IKT und Cyber betreffen.

Unsere Mission Vorwärts ist ein Bekenntnis zu Fortschritt und Innovation. Wir investieren in zukunftsweisende Technologien, um unsere Fähigkeiten zu stärken und die Sicherheit unserer Bürgerinnen und Bürger zu gewährleisten. Mit dem Aufbauplan ÖBH2032+ setzen wir die Modernisierung des Bundesheeres konsequent fort und schaffen die Fähigkeiten zur modernen Landesverteidigung. Das beste und modernste Gerät nützt nichts, wenn wir nicht ausreichend Soldatinnen und Soldaten haben, die es bedienen.

Auch hier sind wir auf einem guten Weg und konnten die Personalstärke sowohl bei Soldatinnen und Soldaten als auch Zivilbediensteten trotz Pensionierungswelle anheben. Ein weiterer Meilenstein zu diesem Ziel ist die Reform des Wehrdienstes. Die Ergebnisse der Wehrdienstkommission liegen ebenfalls auf dem Tisch und werden einen wichtigen Teil hin zu einsatzfähigen Soldatinnen und Soldaten zum Schutz unserer Republik und seiner Bürgerinnen und Bürger beitragen.

Ein besonderes Augenmerk liegt hierbei auf dem Cyber- und Informationsraum. Moderne Sicherheit ist ohne digitale Technologien nicht mehr vorstellbar und einsetzbar. Das Motto der Direktion 6 – IKT und Cyber „Verteidigung beginnt Digital" unterstreicht die Bedeutung digitaler Vernetzung in hybriden Konflikten. Wir bauen auf innovative Lösungen, um unsere Streitkräfte zukunftssicher zu machen.

Digitale Souveränität ist dabei ein zentraler Pfeiler – wir müssen unabhängig bleiben und unsere digitalen Systeme schützen, um in einer vernetzten Welt verteidigungsfähig zu bleiben. Das Österreichische Bundesheer muss auch dann noch handlungsfähig sein, wenn sonst nichts mehr funktioniert.

Ein besonderer Fokus liegt auf unserem Engagement im Weltraum, insbesondere bei dem Projekt LEO-2-VLEO. Diese Initiativen ermöglichen es uns, kommunikative und technische Fähigkeiten für ein Lagebild auf ein neues Level zu heben - was für eine moderne Verteidigung unerlässlich ist.

Gleichzeitig sehen wir uns zunehmend mit den Herausforderungen von Desinformation und Fake News konfrontiert. Ein klares Lagebild und das Schaffen von Resilienz durch transparente Aufklärung und Information sind die Voraussetzungen, um diesen Bedrohungen entgegenzuwirken.

Ich danke allen Soldatinnen und Soldaten, Zivilbediensteten und besonders den Mitarbeiterinnen und Mitarbeitern der Direktion 6 – IKT und Cyber für ihren unermüdlichen Einsatz. Gemeinsam schaffen wir ein modernes Bundesheer, das den Herausforderungen des 21. Jahrhunderts wirkungsvoll begegnen kann.

Mag. Klaudia TANNER
Bundesministerin für Landesverteidigung

Bundesministerium für Landesverteidigung

Sehr geehrte Damen und Herren!

General Mag. Rudolf Striedinger

Angesichts aktueller globaler Herausforderungen muss sich auch das Österreichische Bundesheer kontinuierlich anpassen und weiterentwickeln.

Das Zielbild ÖBH2032+ dient dabei als Vorgabe, die durch die Synchronisation von Personal, Gerät und Infrastruktur einen Weg für ein sicheres Österreich weist und die Handlungsfähigkeit unserer Streitkräfte gewährleistet.

Die Direktion 6 - IKT und Cyber steht im Fokus der Fähigkeitsentwicklung unseres Bundesheeres. Ohne Digitalisierung und innovative Lösungen ist eine moderne Landesverteidigung nicht mehr denkbar. Moderne Waffensysteme sind eng miteinander vernetzt und können nur noch computergestützt effizient und in der erforderlichen Geschwindigkeit zur Wirkung gebracht werden; und dies sowohl in der Luft, zu Land oder im digitalen Raum.

Die Verwendung von KI-unterstützten Systemen in unterschiedlichen Anwendungen wird die Cyberkräfte in den nächsten Jahren ebenso fordern wie die Herausforderungen im Informationsraum. Doch ich bin zuversichtlich, dass die Direktion 6 - IKT und Cyber mit technisch entsprechender Ausrüstung und gut ausgebildetem und engagiertem Personal auch diese Aufgaben meistert.

Eine weit über das Bundesheer hinausreichende Herausforderung stellt die digitale Souveränität dar. Hier gilt das Österreichische Bundesheer als Vorreiter bei der Einführung von Open Source Produkten wie zum Beispiel Libre Office. Zu diesem Thema sind die Experten der Direktion 6 – IKT und Cyber auf nationaler und internationaler Bühne sowohl im öffentlichen als auch im privaten Sektor als Berater sehr gefragt und unterstützen auf breiter Basis.

Mit dem Projekt LEO2VLEO weitet das Österreichische Bundesheer seine Kompetenz bis in den Weltraum aus. Mit insgesamt 5 eigenen Satelliten wird in Kooperation mit den Niederlanden ein wichtiger Beitrag zu Europas Bedarf an souveränen, schnell reagierenden Weltraumressourcen geleistet.

Insgesamt steht das Österreichische Bundesheer mit seinen Cyber- und Informationskräften vor vielschichtigen Herausforderungen, denen wir uns gemeinsam mit Weitsicht, Mut und Zusammenhalt stellen müssen und werden.

General Mag. Rudolf STRIEDINGER
Chef des Generalstabs

Inhaltsverzeichnis

Direktion 6 – IKT und Cyber

Leiter der Dion6, Kommandant der Cyberkräfte, CDO&CIO des BMLV: GenMjr Ing. Mag. Hermann KAPONIG

Sehr geehrte Damen und Herren,
werte Leser unseres Leistungsberichts 2025.

Wir verfassen seit 2020 jährlich einen Jahresbericht zu unserem Leistungsbereich. Vor ihnen liegt nun unser sechster Leistungsbericht für den Betrachtungszeitraum 2025. 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 im Jahr 2025 bereits umgesetzt werden konnte oder in Angriff genommen wurde.

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.

Der vorliegende Leistungsbericht ist der letzte Leistungsbericht, den ich als CDO&CIO und als Cyber Koordinator des BMLV, als Leiter der Direktion 6 – IKT&Cyber und als Kommandant der Cyber- und Informationskräfte des ÖBH, mit einem Vorwort versehen darf. Ich beende meine aktive Dienstzeit mit 31. März 2026 und verabschiede mich in den Ruhestand.

Bei dieser Gelegenheit darf ich mich herzlich für die Führung durch die vorgesetzten Stellen und die mir zugestandenen Handlungsfreiheit in der Wahrnehmung unserer Aufträge bedanken.


Foto: BMLV/HBF

Auch möchte ich mich für die oftmals gewährte Unterstützung und die hervorragende Zusammenarbeit mit anderen Dienststellen des Verteidigungsressorts, anderen Stellen des Bundes und nationalen und internationalen Partner herzlich bedanken.

Mein besonderer Dank gilt natürlich unseren Kommandanten und Leitern, sowie den Mitarbeiterinnen und Mitarbeitern der Direktion 6 - IKT&Cyber, die mit ihrer Loyalität, mit ihrem Engagement, mit ihrem Wissen und ihren Fähigkeiten, sowie ihren Erfahrungen, die Erreichung der Zielsetzungen unterstützt und zum Erfolg unserer gemeinsamen Arbeit entscheidend beigetragen haben.

Es war mir eine Ehre, über insgesamt mehr als 11 Jahre an der Spitze dieser Organisation zu stehen und dem Österreichischen Bundesheer dienen zu dürfen.

„Unser Ziel ist es, dass wir in den nächsten Jahren die aktuell noch sehr zentralisierte gesamte IKT-Struktur, auf ein dezentrales Cloud-basierendes Netz, das sogenannte IKTSystemÖBH2032+, umbauen.“

Auch das Jahr 2025 war wesentlich vom Thema der digitalen Transformation geprägt. Hier haben wir wieder maßgebliche Beiträge zur Digitalisierung der Streitkräfte und der Verwaltung geleistet. Im Schwergewicht waren hier natürlich die einsatzorientierten Planungen und Umsetzungen zum Aufbauplan ÖBH2032+ und hier im Besonderen zum Zielbild ÖBH2032. Alles Maßnahmen, die darauf abzielen, unseren Soldaten jene Fähigkeiten zur Verfügung stellen zu können, die in Richtung eines digitalisierten domänenübergreifenden Lagebildes, eines beschleunigten Führungsprozesses und einer erhöhten Wirkung im Einsatz abzielen (Aufklärungs- Wirkungs- und Führungsverbund). Ziel ist es weiterhin alle Maßnahmen dahingehend zu setzen, um die Verteidigungsfähigkeit unseres Bundesheeres weiterzuentwickeln und eine Führungsüberlegenheit im Einsatz herzustellen.

Unser Ziel ist es, dass wir in den nächsten Jahren die aktuell noch sehr zentralisierte gesamte IKT-Struktur, auf ein dezentrales Cloud-basierendes Netz, das sogenannte IKTSystemÖBH2032+, umbauen. Core-Cloud, Business-Cloud, Mission-Cloud und Plans-Cloud sind Begriffe, die derzeit in aller Munde sind. Ähnliche Systeme werden aktuell in vielen europäischen Staaten geplant oder befinden sich bereits in Umsetzung.

Die Planungsarbeiten und Testungen dazu binden überwiegend die Kräfte in der Direktion 6. Die Ziele sind ambitioniert, aber erreichbar. Wir müssen es schaffen in diese Liga aufzusteigen, um insbesondere in hybriden Bedrohungsszenarien wirklich in allen Domänen verteidigungsfähig zu werden.

2025 hat es in der Direktion 6 auch einige bemerkenswerte Personalveränderungen auf oberer Ebene gegeben.

Oberst des Generalstabsdienstes Mag. Klaus JENSCHIK wurde Anfang 2025 mit der Führung unserer Planungsabteilung IKT-Cyber-Plan (IKTCyPl) betraut.

Im Rahmen eines Festakts durfte ich Mitte des Jahres die Leitung des IKT-und Cybersicherheitszentrums (IKT&CySihZ) an Brigadier Hofrat Dr. Fritz TEICHMANN übergeben.

Im 3. Quartal 2025 wurde Oberst des Generalstabsdienstes Mag. Guido KRAUS zum neuen Leiter der Führungsabteilung und gleichzeitig stellvertretenden Leiter des IKT&CySihZ, bestellt.

Erfreulich war 2025 auch unsere weiterhin hervorragende Personalgewinnung in allen Ebenen und Fähigkeitsbereichen.

In diesem Zusammenhang darf ich unserem Personalbereich für deren unermüdliche Arbeit danken, aber auch unserem Dienststellenausschuss meinen besonderen Dank für die hervorragende Arbeit und dem konstruktiven Miteinander aussprechen.

Bei dieser Gelegenheit darf ich mich bei allen Kommandanten, Leitern und Mitarbeiterinnen und Mitarbeitern herzlich für die gezeigten Leistungen im Jahr 2025 bedanken und sie gleichermaßen auch dazu auffordern, im folgenden Jahr mit ihrem Engagement, Wissen und Erfahrung ihren wesentlichen Beitrag für die Erhaltung und Weiterentwicklung der Führungsfähigkeit unseres Bundesheeres beizutragen.

Auch die Anerkennung unserer Arbeit ist wichtig.

So war es äußerst erfreulich, dass unsere Anstrengungen in Richtung einer „Digitale Souveränität" entsprechend anerkannt und gewürdigt werden. Damit hat das Bundesheer sowohl national als auch international breite Anerkennung und Wertschätzung erfahren. Wir konnten dazu erste wesentliche Akzente setzen.

So habe wir im Sinne der „Open Source Strategy (OSS)" z.B. mit der konsequenten Einführung eines neuen Office-Pakets (Libre Office), einem neuen gesicherten Videokonferenzservice (Open Talk), offenen Datenbank-Systemen (PostgreSQL) und LINUX-Servern, erfolgreiche Schritte in die richtige Richtung setzen können.

Ganz besonders stolz sind wir auch darauf, dass unser „Chief Technical Officer (CTO) und Bereichsleiter IKT-Technik im IKT und Cybersicherheitszentrum, Herr Mag. Wolfgang HACKER, als „Zivilbediensteter des Jahres 2025" im Verteidigungsressort gekürt wurde.

Auch besonders hervorzuheben ist, dass das BMLV mit dem Projekt „Bundesheer Online" den „Verwaltungspreis der Republik Österreich 2025" gewonnen hat. Daher wurde das Siegerteam des BMLV aus dem Bereich des Heerespersonalamtes und der Abteilung Personalapplikationen des IKT&CySihZ entsprechend geehrt. Ein wesentlicher Erfolg im Rahmen der Arbeiten zum „Projekt Digitalisierung Behördenverfahren".

2025 haben wir auch wieder bei der weltweit größten Cyberübung der NATO, der „LOCKED SHIELDS 2025" mit geübt. Wir haben diesmal in einem trinationalen Team AUT-NLD-USA/US National Guard VERMONT mit externer Verstärkung aus dem gesamtstaatlichen Bereich teilgenommen. Erstmalige haben wir heuer dabei auch die strategische Ebene mit abgedeckt und konnten daraus wesentliche Erfahrungen für Weiterentwicklungen gewinnen.

Natürlich waren wir auch bei vielen anderen Übungen, wie z.B. bei der EloKa-Übung „Alpine Jam" im Elektromagnetischen Spektrum, der Luftraumsicherungsoperation „DÄDALUS25", der „WALDVIERTEL25" oder der DACH-Übung „COMMON ROOF 25" mit dabei.

Unsere Führungsunterstützungsbataillone, der IKT-Betrieb des IKT&CySihZ und die Führungsunterstützungsschule waren zudem bei vielen anderen Übungen der Land- und Luftstreitkräfte eingebunden. Nicht zu vergessen ist unsere erfolgreich fortgesetzte Übungsserie zur Notkommunikation (KW, UKW, SAT), die uns z.B. auf Blackout-Szenarien vorbereiten.

Auch war das Jahr von einer Vielzahl an Planspielen des Generalstabs zur Fähigkeitsentwicklung zum ÖBH2032 geprägt. Ganz wesentlich für uns war hier das „Planspiel Führungsüberlegenheit".

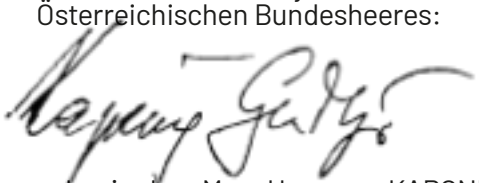
Nicht zu vergessen sind auch die vielen Vorbereitungen für die einsatzorientierten Aufgabenstellungen für den strategischen Leitungsstab/BMLV, das operative „Force Headquarter" (FHQ), oder unser taktisches „Cyber Information Domain Component Command" (CIDCC)

Neben den Bearbeitungen für den Cyberraum (Cyber-Truppe, EloKa-Truppe, FüU-Truppe), haben wir auch im Bereich des Informationsraums und des Weltraums wesentliche Entwicklungsschritte gemacht. Hervorzuheben sind hier z.B. unsere Aktivitäten LEO2VLEO und BEACONSAT, womit wir in weiterer Folge eigene „payload auf Satelliten" zur Erdbeobachtung und „Navigation Warfare" im All haben werden. Ein weiterer wesentlicher Schritt zur Unabhängigkeit von anderen militärischen oder kommerziellen Services.

Eine Vielzahl an Aktivitäten gab es auch im Bereich der Veranstaltungen im Rahmen der Öffentlichkeitsarbeit wo Fähigkeiten und Projekte für den Cyber-, Informations- und Weltraum präsentiert wurden. Neben der Informationsvermittlung und Bewusstseinsbildung, eine ganz wichtige Komponente für Personalgewinnung und Awareness-Schulung im Fachbereich. Unverzichtbar waren hier im Besonderen die Einsätze unserer Informationsoffiziere und die Präsentationen unseres „Cyber Escape Rooms", den wir heuer mit einem weiteren neuen Szenario bestückt haben.

Alles zusammen eine tolle Teamleistung, auf die wir besonders stolz sein können.

Der Kommandant der Cyberkräfte des Österreichischen Bundesheeres:



Generalmajor Ing. Mag. Hermann KAPONIG

Dion6

Kommandounteroffizier

Vizeleutnant Leopold RADLMAIR


Foto: BMLV/HBF

Wie lange sind Sie in der Direktion 6 und ihren Vorgängerorganisationen und wie hat Ihr Werdegang bis dahin ausgesehen?

Mein Werdegang im Österreichischen Bundesheer (ÖBH) beginnt am 1. April 1982, wo ich zum Panzergrenadierbattailon 13 (PzGrenB13) Ried eingerückt bin und als Panzerfahrer verwendet wurde. Im September 1983 wechselte ich zum Jagdpanzerbattaillon 7 (JaPzB7) - siehe Bild - nach Salzburg. Am 1. August 1985 habe ich meinen Dienst bei der Transportkompanie/ Radarstationskommando (TrspKp/RadStatKdo) Luftraumüberwachung (LRÜ) als stellvertretender Kommandant Transportzug (stvKdt TrspZg) angetreten und wurde nach meiner Ausbildung am 1. Mai 1990 Zugskommandant (ZgKdt). In dieser Kompanie habe ich auch den Fähnrich Christof Tatschl kennen gelernt.

Nach seiner Ausmusterung als Leutnant hat er mich dazu bewogen, dass ich mir EDV – Kenntnisse aneigne. Mit diesen erworbenen Kenntnissen war auch der Grundstein, für meine Verwendung ab 1. September 1996 im Militärkommando Salzburg (MilKdo S) als Hilfsreferent Führung&Organisation (HiRef Fü&Org), gelegt. In dieser Funktion war eine meiner wesentlichen Aufgaben die Einführung der EDV und die damit verbundene Ausbildung des Kaderpersonals im Befehlsbereich 8 (Salzburg).

Schon mit 1. Februar 1998 wurde ich als HiRef IT-Offizier (ITO) beim Korpskommando 2 (KpsKdo II) in der Schwarzenbergkaserne bestellt und mein Aufgabenbereich erstreckt sich nun auch um die Bereiche Militärkommando Tirol (MilKdo T), Militärkommando Vorarlberg (MilKdo V) und die 6. Jägerbrigade (6.JgBrig).

Noch im Herbst desselben Jahres wurde ich der erste Beurteiler für den ECDL im ÖBH und es konnte somit das erste Testcenter im ÖBH zum Erwerb des Europäischen Computer Führerschein in der Schwarzenbergkaserne errichtet werden. Durch die Strukturreformen kam ich zum Kommando 2 Korps (Kdo II Kps) zum Kommando Land (Kdo Land) zum Streitkräfteführungskommando (SKFüKdo) wo ich auf Grund meiner ständigen Fort- und Weiterbildung im Fachbereich mit 1. März 2017 zum Sachbearbeiter der J6 Abteilung aufstieg.

Es war auch das Jahr wo die J6 Abteilung umgewandelt wurde zur G3/G5 Abteilung im Kommando Führungsunterstützung und Cyberdefence (KdoFüU&CD). Der Höhepunkt meiner militärischen Laufbahn war jedoch mit 10. Jänner 2022 wo ich von GenMjr Ing. Mag. Hermann Kaponig zum Kommando-Unteroffizier (KdoUO) der neu aufzustellenden Direktion 6 - IKT und Cyber eingeteilt wurde.

Wie hat sich die IT im Bundesheer während Ihrer Dienstzeit verändert?

Zusammengefasst und kurz gesagt „Sehr stark". Als ich meinen Dienst 1982 angetreten habe standen an Stelle von Notebooks und PC noch Schreibmaschinen in den Büros. Meine erste dienstliche Berührung mit einem PC hatte ich im September 1996.

Das Betriebssystem war Windows 3.1 und wurde später durch Windows NT 4.0 abgelöst. Bei der Telefonie gab es natürlich auch wesentliche Entwicklungssprünge. Als junger Unteroffizier war für das Gespräch in eine andere Liegenschaft noch die Vermittlung erforderlich.

Als Verbindungsmittel hatten wir im Bereich Funk das TFF 21 und das AN/PRC 77 diese sind heute nur noch in einem Fernmelde-Museum zu besichtigen.
Die Vielzahl an Anwendungen und Lernprogrammen welche heute dienstlich zur Verfügung gestellt werden, würde bei einer zeitgemäßen Ausstattung jedoch mindestens ein Tablet und ein Smartphone für jeden Mitarbeiter rechtfertigen.

Was war Ihr persönliches Highlight innerhalb der Direktion 6 - IKT und Cyber?

Ich verbrachte viele schöne Zeiten im Bundesheer. Als Ausbilder in den verschiedensten Funktionen beim PzGrenB13 beim JgPzB7 und bei der LRÜ. Als Soldat in der Verwaltung beim MilKdo S beginnend über das KpsKdo II bis hin zum SKFüKdo ist der Weitblick über die Aufgaben des Bundesheeres und das Zusammenwirken der verschiedenen Waffengattungen stetig gewachsen.

Im Jahr 2017 wurde im militärstrategischen Konzept die Teilstreitkraft „Cyber- und Informationskräfte" festgelegt. Im Juni 2021 erfolgte die dafür erforderliche Anordnung zum Aufbau der Direktion 6 - IKT und Cyber. Mit Jänner 2022 wurde mir die Ehre zu Teil, Kommandounteroffizier dieser Teilstreitkraft zu sein. Zu sehen wie aus einer Unterstützungstruppe eine Teilstreitkraft wird, und dabei auch noch mitwirken zu können, ist sicher etwas Einzigartiges und somit mein ganz persönliches Highlight.

Foto: Vzlt Radlmair im Panzer, Bundesheer

Foto: Andorf SCHIMON

Welchen Rat möchten Sie Ihrem Nachfolger mit auf den Weg geben?

Mit Ratschlägen ist das immer so eine eigene Sache. Der beste Ratschlag ist „Keinen Ratschlag zu geben". Mein Nachfolger soll seine eigenen Eindrücke gewinnen und seine Erfahrungen im Bereich der Cyber- und Informationskräfte machen. Ein Blick von außen bringt oft neue Ansätze zu Tage. Dies bedeutet Fortschritt und nicht Stillstand. Dabei werden ihm sicher auch die Anliegen der Chargen und Unteroffiziere zur Kenntnis gelangen. Im Bewusstsein, dass ein Kommandounteroffizier als höchster Unteroffizier in der Teilstreitkraft kein Parteifunktionär oder Personalvertreter ist, kann er seine somit gewonnenen Erkenntnisse dem Kommandanten unvoreingenommen vortragen.

Was würden Sie Leuten raten, die überlegen, zu den Cyberkräften im Österreichischen Bundesheer zu gehen?

Bei den Cyber- und Informationskräften gibt es sehr breit gefächerte Aufgaben und hier sind nicht nur Computer- und Programmierspezialisten am Arbeiten. In dieser zukunftsorientierten Teilstreitkraft kann daher jeder seine Fähigkeiten einbringen. Meine Antwort auf die Frage:

„Nicht lange überlegen, TUN!"

HIGHLIGHTS

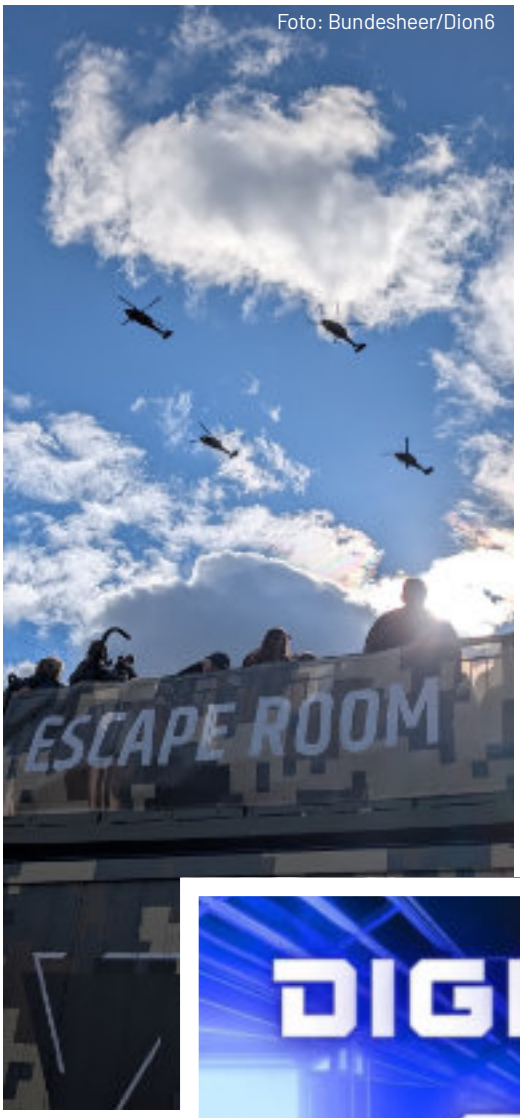


Foto: Bundesheer/Dion6

Nationalfeiertag 2025

Zum 70 Jährigen Jubiläum präsentierte das Bundesheer am 26. Oktober den zahlreichen Besucherinnen und Besuchern eine großartige Leistungsschau in der Wiener Innenstadt.

Die Themeninsel Cyber, Forschung und Technik war mit elf Stationen vor Ort und konnte die Besucherinnen und Besucher mit ausgefallen Ausstellungsstücken begeistern. Unter anderem war zu sehen: Tracker und Drohnen (Tracker-Sim, MagneX und Klein-Drohnen), künftige Weltraumtechnik, der Warthog (eine Forchungsplattform für autonomes Fahren im Gelände), ein BACKBONE/ Battlepad, KI, TCN Signal-Analyse "Narda" und vieles mehr. Zusätzlich zur Themeninsel luden unser Escape Room, ein Drohnenkäfig für Drohnenflüge mit einer Live-Übertragung der Kamerabilder auf große Screens und die neuen Nachtsichtgeräte zum Mitmachen und Ausprobieren ein.

(S. 39)

Grafik: Bundesheer/Dion6

Digital ganz Real

Seit April 2025 veröffentlicht die Direktion 6 - IKT und Cyber auf Social-Media-Plattformen eine neue Videoreihe. Mit ObstltdG Markus Schmid als Gesicht der Kampagne werden komplexe Themen rund um IKT und Cyber verständlich dargestellt. Die Staffeln behandeln unter anderem Cyber-Grundlagen, die Rolle der Direktion 6 - IKT und Cyber, Cyber-Abwehr sowie Fake News und Deep Fakes. Ziel ist es, ein besseres Verständnis für die Vielschichtigkeit des Cyber- und Informationsraums zu vermitteln.

(S. 39)

Foto: Bundesheer/Dion6

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Wargame Führungsüberlegenheit

Beim Wargame Führungsüberlegenheit sollten vor allem die bisher erarbeiteten Grundlagen zur Umsetzung des Zielbildes des ÖBH2032+ in den Bereichen Führungsunterstützung, elektromagnetische Kampfführung, Kampfführung im Cyberraum und die Services im Weltraum überprüft und vertieft werden. Der Fokus der Betrachtung lag auf dem Führungs-, ISTAR-, Wirkungs- und Unterstützungsverbund des mobilgemachten ÖBH2032+ auf der strategischen Ebene bis zur Brigade/Bataillon. Das Institur für militärisches Geowesen (IMG) konnte dabei seine bestehenden interaktiven und immersiven Produkte zur 3D-Geländedarstellungen inklusiv des Nutzungsprozesses von BORIS, VRANZ und ALOIS präsentieren.

(S. 50, 107)

Informationsmanagement-System

Das Informationsmanagement umfasst das Erfassen, Speichern, Analysieren, Verteilen, Schützen und Löschen von Daten. Im militärischen Kontext ist es eine entscheidende Ressource für digitale Souveränität und ermöglicht Kommandanten, durch ein klares Lagebild schnelle Entscheidungen zu treffen. Innerhalb der Generaldirektion Landesverteidigung (GDLV) laufen parallele Planungs- und Realisierungsschritte, um zukünftige IKT-Anforderungen der hybriden Kriegsführung zu meistern.

(S. 43-47)

HIGHLIGHTS

TCN-Umstellung im Ausland

Im Jahr 2025 stellte das ÖBH seine Auslandsmissionen von der veralteten Integrierte Fernmelde-infrastruktur (IFMIN) auf das moderne Tactical Communication Network (TCN) um. Trotz Herausforderungen durch alte Verkabelungen und Systeme wurde die Umstellung erfolgreich abgeschlossen. Die Modernisierung brachte eine höhere Bandbreite, moderne Telefonie und eine zukunftsfähige Grundlage für zukünftige Anwendungen. Die ständige Einsatzbereitschaft der Truppen wurde gewährleistet, und die sorgfältige Planung sowie Schulung trugen zum Erfolg bei, der einen wichtigen Meilenstein in der Digitalisierung des ÖBH darstellt.

(S. 53-54, 101, 115)

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Weltweit größte Cyber-Übung Locked Shields 2025

Im Mai 2025 nahm die Direktion 6 - IKT und Cyber an der weltweit größten Cyber-Verteidigungsübung "Locked Shields" teil, die vom CCDCoE organisiert wurde. Österreich stellte ein Team von über 100 Experten, unterstützt durch Partner aus den Niederlanden und den USA, um in einer realistischen Übung kritische Infrastrukturen vor simulierten Cyberangriffen zu schützen. Die Übung forderte die Blue Teams heraus, technische und strategische Fähigkeiten unter hohem Zeitdruck einzusetzen, um Angriffe abzuwehren und die Kommunikation zu gewährleisten.

(S. 38, 48, 58, 87-88, 92-93)

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Foto: Österreichischer Verwaltungspreis 2025, BMLV/HBF

Informationsfreiheitsgesetz-Service

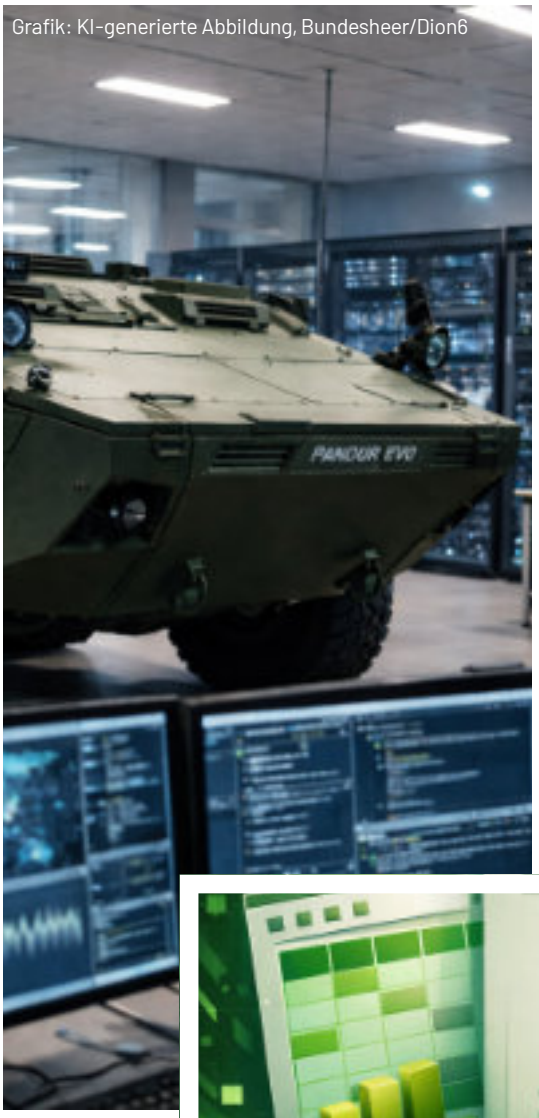
Zum 1. September 2025 trat das Informationsfreiheitsgesetz (IFG) in Kraft, das Bürger Zugang zu Informationen der Verwaltung ermöglicht und die proaktive Veröffentlichung von Verwaltungsvorgängen vorsieht. Im BMLV wurde das "IFG-Service" entwickelt, um Dokumente im öffentlichen Interesse zu veröffentlichen. Über das Portal "data.gv.at" werden freigegebene Informationen bereitgestellt. Zudem wurde ein Information Exchange Gateway (IEG) implementiert, das den Informationsfluss durch Sicherheitsmechanismen wie Segmentierung und Transportverschlüsselung schützt und automatisiert nach Schutzbedarf prüft. Dieses System unterstützt die Anforderungen des IFG und gewährleistet den Schutz sensibler Daten.

(S. 51, 74, 91)

Österreichischer Verwaltungspreis

Die Abteilung Personalapplikationen ist der zentrale Anbieter von Personaldaten im österreichischen Bundesheer und treibt die Digitalisierung und eGovernment im BMLV voran. Im Jahr 2025 wurde die Plattform "bundesheeronline" mit dem österreichischen Verwaltungspreis in der Kategorie "Innovatives Servicedesign und digitale Services" ausgezeichnet. Die Auszeichnung wurde unter anderem für den direkten Kommunikationskanal zwischen Antragstellern und Referenten via Chat sowie die transparente Darstellung des Bearbeitungsstatus verliehen. Die Plattform verzeichnet eine hohe Akzeptanz mit rund 70.000 registrierten Anwendern und wird kontinuierlich um weitere Verfahren, wie die Verlässlichkeitserklärung und diverse Meldungen, erweitert.

(S. 76)



Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Pandur EVO IKT-Labor

Im Juni 2025 wurde das PANDUR IKT-Labor eröffnet. Mit der Beschaffung von neuen PANDUR Evo ist die Ausarbeitung von Konzepten für den IKT-Einsatz und praktische Tests notwendig. Das Labor ermöglicht die schrittweise Konfiguration und Integration von IKT-Systemen, einschließlich des digitalen Interkomm-Systems, unter Einbindung der Truppe. Durch die flexible Konfiguration der Fahrzeuge und die Verzahnung verschiedener Systeme im Labor soll das Zusammenspiel der Komponenten getestet werden. Langfristig ist das Labor Teil des geplanten Zentrums für Integration, Prozessvalidierung und Testung.

(S. 81)


Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Einführung der OpenSource Software LibreOffice

Im Jahr 2025 setzte das BMLV/ÖBH den Schritt zur digitalen Souveränität fort, indem Microsoft Office durch das Open-Source-Produkt LibreOffice ersetzt wurde. Diese Maßnahme zielt darauf ab, die Unabhängigkeit von einzelnen Anbietern zu stärken und die Fähigkeit zu gewährleisten, auch in Krisensituationen weiterarbeiten zu können. LibreOffice wurde verpflichtend für die Dokumentenerstellung in ELAK implementiert, wobei der 1st-Level-Support durch die Benutzerbetreuung gewährleistet wird. Die Investition in die Weiterentwicklung von LibreOffice, einschließlich des Beitrags von Code zur Open-Source-Community, unterstreicht das Engagement für eine nachhaltige und unabhängige Lösung.

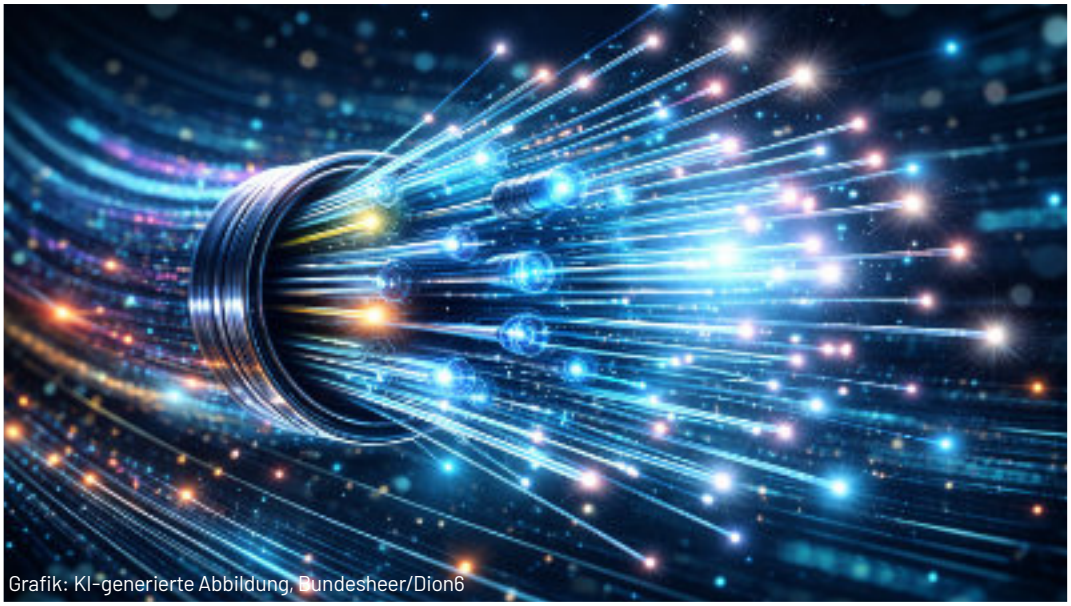
(S. 83, 102)

InnoVision

Im Jahr 2025 führte das Militärische Cyberzentrum zwei Fokusgruppenmeetings im Rahmen der InnoVision-Reihe durch, die sich auf die zukünftige Entwicklung des Cyberlagebilds und auf Security Operations Centers (SOC) konzentrierten. Im Mai diskutierten Experten aus Wirtschaft, Industrie und Behörden innovative Lösungsansätze für Cyberbedrohungen, während im November der Fokus auf einem mobilen, hierarchischen SOC lag. Die Workshops förderten den Austausch und die Entwicklung neuer Ideen, die bis Mai 2026 zu detaillierten Forschungsprojekten ausgearbeitet werden sollen. Im Juni 2026 wird eine weitere InnoVision mit Präsentationen und Juryentscheidung stattfinden, um die nächsten Schritte im Cyberverteidigungsbereich zu bestimmen.

(S. 89-90)

Foto: Bundesheer/Dion6



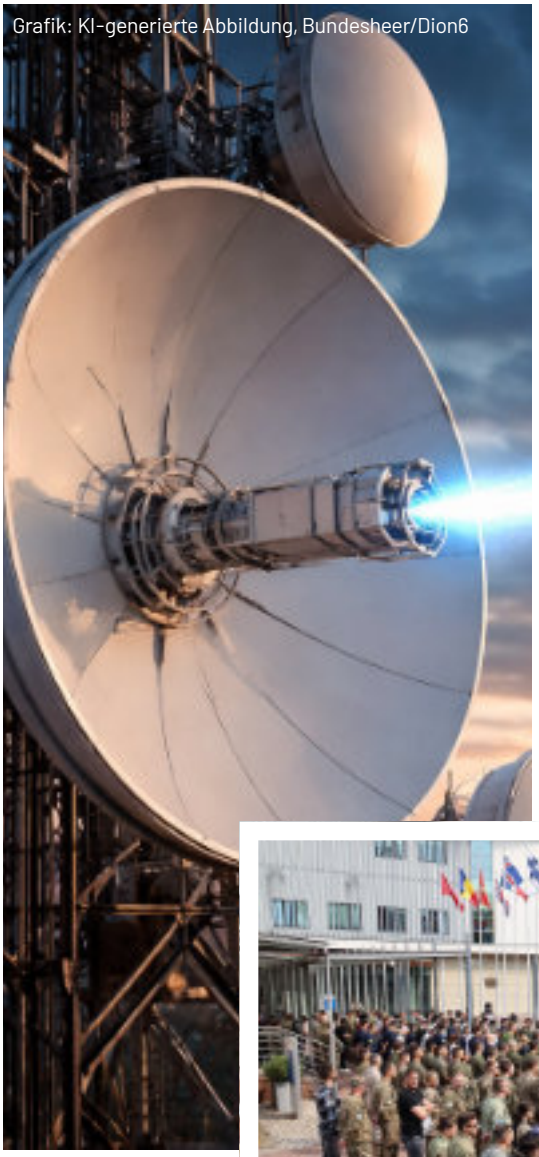
Grafik: KI-generierte Abbildung, Bundesheer/Dion6

HIGHLIGHTS

LWL-Ausbau BMLV

Im Rahmen des LWL-Ausbaues BMLV wurde im Jahr 2025 erfolgreich mehr als 30 Liegenschaft auf LWL-Knoten umgestellt. Mit dieser Infrastruktur wurden die Rahmenbedingungen für die Nutzung von hohen Bandbreiten unterschiedlicher Services in den Liegenschaften hergestellt.

HIGH LIGHTS



Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Fertigstellung Midlife-Upgrade im ortsfesten Richtfunk

Mit Ende 2025 wurden Arbeiten für das Upgrade am ortsfesten Richtfunk gemeinsam mit IKTTe und den ausführenden Firmen fertigstellt.Die umfangreichen Änderungsmaßnahmen im ortsfesten Richtfunk waren erforderlich, um das bestehende österreichweite Netz für die künftigen Anforderungen bereitzustellen.

Foto: CWIX25, NATO Strategic Warfare Development Command

Übung Coalition Warrior Interoperability eXploration, eXperimentations, eXamination eXercise (CWIX) 2025

CWIX 2025 war die größte IKT-Veranstaltung der NATO mit 3250 Teilnehmern aus 40 Nationen. Über 400 militärische IKT-Systeme wurden im multinationalen Verbund getestet. Österreich war an zwei Standorten in Polen präsent, ein Teil der Tests erfolgte auch vom AUT Battle Lab in Wien. Der Schwerpunkt lag auf der Zertifizierung von IKT-Services im Rahmen des FMN-Programms für die Zusammenarbeitsfähigkeit in Joint- und Multi-Domain-Operations. Die Tests waren in 18 Focus Areas organisiert, darunter GeoMetOc-Service und JISR, wobei österreichische Experten bedeutende Beiträge leisteten. Die Veranstaltung brachte wertvolle Erkenntnisse für die nationale Fähigkeitsentwicklung.

(S. 77-78)

Foto: Bundesheer/Dion6

Übung MERCATOR 2025

Um neue sowie bestehende Fähigkeiten zu erproben und unter Einsatzbediungungen zu festigen, führte das IMG 2025 die fortan regelmäßige Erhebungs-Übung MERCATOR durch. Zwischen 24.11.2025 und 27.11 nahmen insgesamt 15 Personen des IMG, der Miliz und Expertenpools erfolgreich teil. Während der Übung kamen eigene Erhebungsgeräte sowie eine Vermessungsstation zum Einsatz. Ergebnisse sind drei Roadbooks am TÜPL Allentsteig, logistische Detailpläne des Bahnhofs WURMBACH und der UTA STEINBACH, sowie eine militärgeographische Beschreibung des WALDVIERTELS mit Übersichtskarte.

(S. 108)

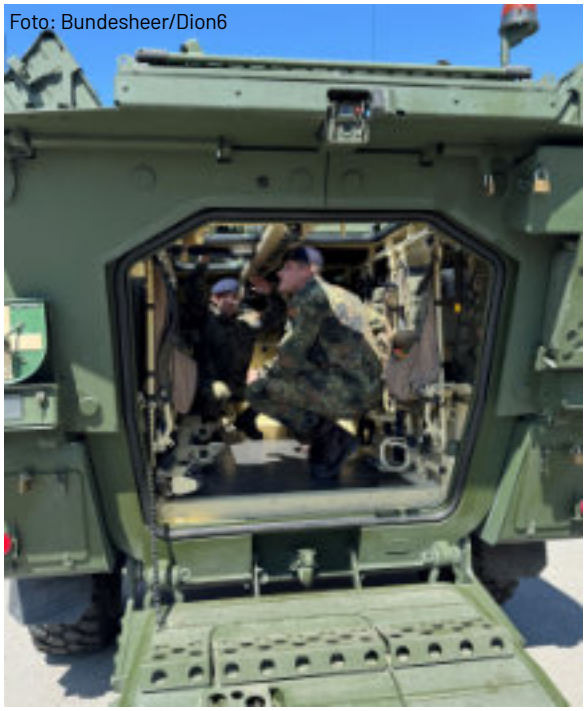


Foto: Bundesheer/Dion6

Alpentriode

Zwischen dem 11. und 16. Mai 2025 fand in Österreich die multinationale Übung Alpentriode statt, bei der IKT-Truppen aus Österreich, Deutschland und der Schweiz zusammenarbeiteten. Ziel war es, Führungs- und Kommunikationsverfahren zu vertiefen, moderne Systeme zu erproben und die Kameradschaft zu stärken. Die Woche begann mit technischer Ausbildung und praktischen Übungen, bei denen die Teilnehmer sich mit österreichischen Fernmeldesystemen und dem Führungsinformationssystem SitaWare vertraut machten.

(S. 124)

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Desinformation

Am 29. April 2025 fand eine Kaderfortbildung der Führungsunterstützungsschule (FüUS) zum Thema Desinformation statt. Experten diskutierten die Herausforderungen durch Deepfakes, Fake News und hybride Bedrohungen. Sie betonten, dass Desinformation gezielt eingesetzt wird, um Verwirrung zu stiften und strategische Fehlentscheidungen herbeizuführen. Die schnelle Verbreitung in sozialen Medien erschwert die Bekämpfung. Wichtig ist die Unterscheidung zwischen Fehlinformation, Desinformation und Falschinformation, wobei die Täuschungsabsicht des Absenders im Vordergrund steht. Kritische Prüfung von Quellen und Inhalten ist entscheidend, um nicht zu Desinformationskampagnen beizutragen.

(S. 36, 124-126)


Foto: Bundesheer/Dion6

30 Jahre Partnerschaft der Stadt Villach und Führungsunterstützungsbataillon 1 (FüUB1)

Am 16. Mai 2025 feierte das FüUB1 sein 30-jähriges Partnerschaftsjubiläum mit der Stadt Villach. Die Partnerschaft, die 1995 von Oberst Günther Janda und Bürgermeister Helmut Manzenreiter begründet wurde, zielt auf die Stärkung der Beziehungen zwischen militärischen und zivilen Organisationen ab. Während der Jubiläumsfeier, die mit einem Platzkonzert der Militärmusik Kärnten begann, betonten der Bataillonskommandant Oberst Ernst Berthold und Bürgermeister Günther Albel die positiven Synergieeffekte der Zusammenarbeit. Der Militärkommandant von Kärnten, Brigadier Mag. Philipp Eder, und der Landtagspräsident Ing. Reinhart Rohr waren ebenfalls anwesend. Höhepunkt der Veranstaltung war der Austausch von Partnerschaftsgeschenken und die Verleihung der Auszeichnung „Ehrenfunker" an den Bürgermeister. Anschließend lud man zu einem gemütlichen Beisammensein mit Gulaschkanone im Rathaus ein.

(S. 111)

HIGHLIGHTS

Foto: Bundesheer/Dion6

Foto: Bundesheer/Dion6

Übung Alpine Jam

Vom 4. bis 14. August 2025 fand auf dem Truppenübungsplatz Hochfilzen die Übung "ALPINE JAM 25" statt, bei der Techniker und EloKa-Fachpersonal aus Österreich, Deutschland und der Schweiz zusammenarbeiteten. Ziel der Übung war die Optimierung von CREW-Systemen gegen funkferngezündete Sprengfallen und Mini-/Microdrohnen. Die Wirksamkeit der Störsysteme wurde auf zwei Teststrecken gegen über 20 Drohnentypen und 30 RCIED-Auslöser getestet. Die Zusammenarbeit basierte auf gegenseitigem Vertrauen und der Überzeugung, dass der Schutz der Soldaten oberste Priorität hat. Die Übung bestätigte die Bedeutung internationaler Zusammenarbeit und Interoperabilität in modernen Bedrohungsszenarien. Die positiven Ergebnisse motivierten die drei Nationen, die Übungsserie 2027 fortzusetzen.

(S. 59)

Übung Waldviertel 2025

Vom 16. bis 27. Juni 2025 führte die Theresianische Militärakademie gemeinsam mit der 4. Panzergrenadierbrigade die Übung "Waldviertel 25" am Truppenübungsplatz Allentsteig durch. Das Führungsunterstützungsbataillon 2, das auch die Führungsunterstützungskompanie des Panzerstabsbataillons 4 integrierte, sicherte die Kommunikationsverbindungen und richtete ein Central Network Operations Center ein.

(S. 118)

IKT Bereitstellung und Nutzungsmanagement

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

Mit Februar 2025 wurde ich als Ltr IKTBstg& NuMngt bestellt und mit Frühjahr 2025 war der Organisationsplan der Abteilung so weit fertiggestellt und genehmigt, dass der personelle Aufbau der Abteilung nachhaltig beginnen konnte. Durch die Einteilung des fehlenden Referatsleiters für das Ref NuMngt&FüU mit Dezember 2025 waren dann auch alle Führungspositionen in der Abteilung besetzt. Zudem ist es gelungen 9 Mitarbeiter zu gewinnen und weitere geeignete Interessenten stehen als Mitarbeiter in Aussicht. Damit konnte die personelle Basis gebaut werden, um den funktionellen Aufbau der Abteilung als zentrales Steuerungselement für die Dion6 umzusetzen. Die Abteilung bewegt sich dabei in dem komplexen Umfeld der Digitalisierung der Streitkräfte und der Verwaltung. Durch die Aufstellung eines CDO/CIO-Elements kann nun der CDO/CIO gezielt und durchgängig in seiner Aufgabe unterstützt werden.

Die Kernaufgabe der Abteilung ist es die Abläufe von der Planung über die Bereitstellung bis zum Einsatz der Kräfte der Direktion 6 – IKT und Cyber 6 zu steuern und durch ein Nutzungsmanagement zu koordinieren. Eine enge Koordination und gute Zusammenarbeit mit der beschaffenden Direktion 5 und der planenden Direktion Fähigkeits- und Grundsatzplanung (Fäh&GSPl) sind Grundvoraussetzung für den Erfolg. Mit diesem Auftrag wird die Abteilung zum Hüter des Fortschritts des Aufbauplans ÖBH2032+ zur Erreichung des Zielbildes ÖBH2032 im eigenen Fähigkeitenbündel. Dazu wird ein modernes Projekt- und Programmmanagement nach dem Prinzip PRINCE2 implementiert, um synchronisiert in den Vorhaben arbeiten zu können. Die Prozesse der Abteilung werden dabei durch das Projekt: „Einführung des prozessorientierten Wissensmanagements" unter Nutzung der international normierten Prozessbeschreibungssprache BPMN (Business Process Model and Notation) nach modernsten Gesichtspunkten der Organisationsentwicklung entwickelt.

Durch die Einführung neuer völlig vernetzter Systeme und deren Integration in ein System of Systems auf Basis des IKTSysÖBH2032+ bekommt das Thema der Architekturentwicklung auf allen Ebenen besondere Bedeutung. Dazu wird es notwendig sein eine Unternehmensarchitektur klar zu definieren, die sich an den Digitalisierungszielen der Streitkräfte orientiert


Foto: BMLV/HBF

und in der die übergeordneten Ziele für die gesamte Organisation, einschließlich der Prozesse und Datenobjekte definiert werden. Erst davon abgeleitet, kann die für die Streitkräfte (SK) notwendige System- und Anwendungsarchitektur erstellt werden und die durch die Digitalisierung versprochenen Vorteile erbringen. Der Fähigkeitenbündel Informationsoperation hat im Jahr 2025 besonders durch den Knowhow Erwerb, spezielle durch die Unterstützung unserer Partner der U.S. National Guard Vermont, große Fortschritte erzielt. Es wird nun Zeit die nächsten Schritte im Sinne der Organisationsentwicklung zu gehen und den InfoOps Nukleus in der Abteilung zu erweitern. In 2025 ist es gelungen die Verbindung zu Partnern, allen voran der D-A-CH (Deutschland-Österreich-Schweiz) – Gemeinschaft und der oben genannte U.S. National Guard, zu Forschungseinrichtungen wie zum Beispiel dem Fraunhofer Institut FKIE, zur Akademia und Partnerfirmen zu verstärken und ihren Input gut zu nutzen. Nicht zuletzt ist es durch den unermüdlichen Einsatz des Referats InfoOps&opKomm gelungen die Personalwerbung und die Zusammenarbeit mit unseren Partnern aus dem Ausbildungsbereich auf hohen Niveau zu halten. Die dabei gezeigte Kreativität und die eigenständige Weiterentwicklung des Cyber Escape Rooms seien besonders hervorgehoben.

Die Abteilung IKTBstg&NuMngt erfüllt seit Beginn des Bestehens ihre Aufgabe und wird ihre Wirkung durch die weitere Befüllung des Personalrahmens, der laufenden hochwertigen Weiterbildung der Mitarbeiter und der konzentrierteren Ausrichtung der Prozesse auf die Kernaufgaben der Dion6 noch wesentlich steigern.

IKT-Steuerung

Mit Wirksamkeit 01.10.2025 wurde innerhalb der Direktion 6 - IKT und Cyber das Referat IKT-Steuerung eingerichtet. Damit wurde ein seit Langem notwendiger organisatorischer Baustein geschaffen, um die wachsende Komplexität der IKT-Landschaft des Bundesministeriums für Landesverteidigung und insbesondere des ÖBH zielgerichtet, koordiniert und zukunftsorientiert zu steuern. Das Referat befindet sich noch in der Aufbauphase, hat aber bereits wesentliche Arbeitsprozesse etabliert, erste Ergebnisse erzielt und zentrale Weichenstellungen vorgenommen.

Das Referat IKT-Steuerung (RefIKTStrg) verantwortet das eigenständige Management der ihm übertragenen Aufgaben und nimmt eine Querschnittsrolle ein, die den gesamten Lebenszyklus von IKT-Systemen, Services und Anwendungen umfasst. Damit wird eine zentrale Steuerungsfähigkeit innerhalb der Dion6 geschaffen, die bisher nur fragmentiert vorhanden war.

Die Kernaufgaben reichen von der systematischen Verwaltung und Weiterentwicklung des IT-Umsetzungsportfolios und des IT-Architekturportfolios über die Koordination von Leistungen zwischen dem IKT und Cybersicherheitszentrum (IKT&CySihZ) bis hin zur unmittelbaren Steuerung interner Abläufe in der Direktion 6 - IKT und Cyber. Diese Tätigkeiten stellen sicher, dass Vorhaben und Maßnahmen in der Dion6 nicht nur technisch, sondern auch organisatorisch aufeinander abgestimmt sind.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Ein Schlüsselauftrag des neuen Referats ist die Erstellung von Vorgaben für Portfolio-, Programm- und Projektmanagement. Damit werden erstmals verbindliche und institutionalisierte Standards geschaffen, die als gemeinsame Grundlage für alle in der Direktion 6 - IKT und Cyber geführten oder unterstützten IKT-Programme dienen. Die Entwicklung solcher übergreifenden Vorgaben ist eine Grundvoraussetzung für eine moderne, transparente und steuerbare IKT-Organisation.

Ebenso wichtig ist die Verantwortung des Referats für die Weiterentwicklung der technischen Architektur des IKT-Systems ÖBH (IKTSysÖBH), die in enger Abstimmung mit IKT-Cyber-Plan (IKTCyPl) erfolgt. Die Erstellung von systematischen Vorgaben für das Engineering rundet dieses Aufgabenfeld ab. Besonders hervorzuheben ist die Etablierung des Programms BEAM (BMLV Enterprise Architektur Modell), das eine zentrale Stellung im Arbeitsprogramm des RefIKTStrg einnimmt. Die fachlich-technische Bearbeitung des Projekts liegt beim IKTCyPl, die Gesamtsteuerung und das Programmanagement jedoch beim Referat. Dadurch entsteht eine klare Rollenverteilung: Während die IKTCyPl die inhaltliche und methodische Ausarbeitung verantwortet, stellt das RefIKTStrg sicher, dass der programmatische Rahmen, die Governance, der Fortschritt und die Einbettung in die Gesamtstrategie gewährleistet sind.

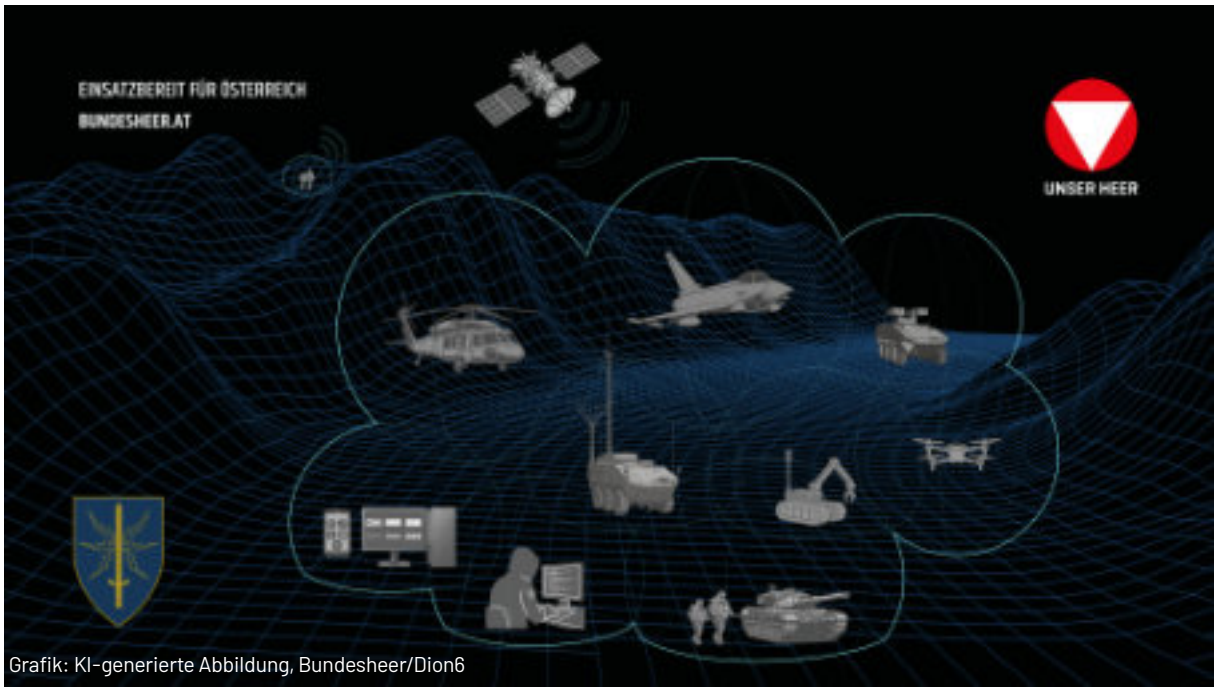
Das Programm BEAM ist unverzichtbar für die geplante Mission-Cloud und deren künftigen Betrieb im ÖBH-Kontext. Ohne eine konsistent modellierte und organisationsweit abgestimmte Enterprise-Architektur lassen sich weder Interoperabilität noch übergreifende Services realisieren. BEAM legt unter anderem die Baseline-Architektur fest, an der sich die künftigen technischen, organisatorischen und betrieblichen Anforderungen orientieren werden müssen. Die enge Verzahnung von Architektur, Governance und Umsetzung ist entscheidend, um einen nachhaltigen und belastbaren digitalen Transformationspfad zu ermöglichen.

Ein weiterer Schwerpunkt des Berichtszeitraums ist die Mission-Cloud. Dieses Vorhaben stellt die künftige zentrale IKT-Betriebsarchitektur des Bundesheeres dar und ist essenziell für die Fähigkeit, moderne, skalierbare und resilient bereitgestellte Services in Einsatz und Grundbetrieb gleichermaßen verfügbar zu machen. Gemeinsam mit dem PANDUR-Projekt wurde im Berichtszeitraum eine Proof-of-Concept-Phase vorbereitet und gestartet. Dabei arbeitet das IKT&CySihZ eng mit dem Referat und den weiteren beteiligten Organisationselementen zusammen.

Die Mission-Cloud wird in dieser Phase erstmals unter realitätsnahen Bedingungen getestet und weiterentwickelt. Die Einbettung in ein einsatznahes, adaptierbares Umfeld ermöglicht es, frühe Rückmeldungen zu technischen, organisatorischen und betrieblichen Aspekten zu erhalten. Diese Phase dient damit nicht nur als Innovationsfeld, sondern auch als Validierungsinstrument, das für die weitere Skalierung auf Verbands- und Systemebene maßgeblich ist.

Das Zusammenspiel mit dem PANDUR-Projekt trägt wesentlich dazu bei, konkrete Anforderungen aus der Truppe frühzeitig zu berücksichtigen und die Mission-Cloud auf echte Nutzbarkeit auszurichten.

Parallel zu diesen architektur- und cloudbezogenen Vorhaben unterstützt das Referat die Einführung und Anwendung der Projektmanagementmethodik PRINCE2, die im Schwesternreferat Nutzungsmanagement & Führungsunterstützung (NuMngt&FüU) geführt wird. Das RefIKTStrg arbeitet eng mit diesem Referat zusammen, um die Standardisierung und Professionalisierung des Projekt- und Programmmanagements weiter voranzutreiben.



Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Dadurch werden die IKT-Programme der Direktion 6 - IKT und Cyber schrittweise nach anerkannten internationalen Standards geführt, was die Transparenz erhöht, Risiken reduziert und die Steuerbarkeit verbessert.

Neben den strukturellen und inhaltlichen Aufgaben wurde auch besonderer Wert auf den personellen Aufbau gelegt. Das Referat konnte im Berichtszeitraum mehrere neue Mitarbeiterinnen und Mitarbeiter gewinnen. Diese Verstärkung bildet die Grundlage, um die steigenden Anforderungen in den Bereichen Portfoliomanagement, Architektur, Programmsteuerung und Service-Governance mittelfristig zuverlässig erfüllen zu können. Die neuen Kräfte bringen sowohl technische als auch organisatorische Kompetenzen mit, wodurch das Referat in seiner Breite und Tiefe an Leistungsfähigkeit gewinnt.

Zusammenfassend lässt sich festhalten, dass das Referat IKT-Steuerung trotz seiner erst kurzen Existenz eine zentrale Rolle für die digitale Ausrichtung der Direktion 6 - IKT und Cyber übernehmen wird und bereits schon übernimmt. Durch die Bündelung von Architektur-, Portfolio- und Programmsteuerungsaufgaben wird eine klare organisatorische Grundlage geschaffen, die für das Gelingen zentraler Vorhaben wie BEAM und Mission-Cloud notwendig ist.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Die enge Zusammenarbeit mit den Partnerorganisationen in Direktion 6 - IKT und Cyber und darüber hinaus, die Einführung verbindlicher Standards sowie der kontinuierliche personelle Aufbau bilden die Voraussetzung dafür, dass das Referat auch künftig seine Funktion als steuernde und koordinierende Einheit innerhalb der IKT-Organisation des Ressorts erfolgreich wahrnehmen kann.

Dadurch werden die IKT-Programme der Direktion 6 - IKT und Cyber schrittweise nach anerkannten internationalen Standards geführt, was die Transparenz erhöht, Risiken reduziert und die Steuerbarkeit verbessert.

Neben den strukturellen und inhaltlichen Aufgaben wurde auch besonderer Wert auf den personellen Aufbau gelegt. Das Referat konnte im Berichtszeitraum mehrere neue Mitarbeiterinnen und Mitarbeiter gewinnen. Diese Verstärkung bildet die Grundlage, um die steigenden Anforderungen in den Bereichen Portfoliomanagement, Architektur, Programmsteuerung und Service-Governance mittelfristig zuverlässig erfüllen zu können.

Die neuen Kräfte bringen sowohl technische als auch organisatorische Kompetenzen mit, wodurch das Referat in seiner Breite und Tiefe an Leistungsfähigkeit gewinnt.

Zusammenfassend lässt sich festhalten, dass das Referat IKT-Steuerung trotz seiner erst kurzen Existenz eine zentrale Rolle für die digitale Ausrichtung der Direktion 6 - IKT und Cyber übernehmen wird und bereits schon übernimmt.

Durch die Bündelung von Architektur-, Portfolio- und Programmsteuerungsaufgaben wird eine klare organisatorische Grundlage geschaffen, die für das Gelingen zentraler Vorhaben wie BEAM und Mission-Cloud notwendig ist.

Einführung von PRINCE2 in der Direktion 6 - IKT und Cyber

In der Direktion 6 - IKT und Cyber wurde der Bedarf nach einem Rahmenwerk identifiziert, um die Projekt- und Programmlandschaft von einem reaktiven zu einem proaktiven und steuerbaren Betrieb zu transformieren. Es gilt Risiken zu vermeiden und Ressourcen sinnvoll einzusetzen.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Die Wahl fiel auf PRINCE2 (PRojects IN Controlled Environments). Im Zuge von Foundation Schulungen für Projekt- sowie Programmmanagement wurden die Teilnehmer in PRINCE2 geschult, zertifiziert und konnten in Arbeitsgruppen bereits erste Ansätze für Templates und Arbeitsweisen zur Überführung bestehender Projekte und Programme in PRINCE2 erarbeiten. Die Einführung von PRINCE2 als Grundlage für zukünftige Projekte und Programme wird bereits als ein Programm nach PRINCE2 behandelt und abgearbeitet.

Die klare Fokussierung auf die fortlaufende geschäftliche Rechtfertigung (Business Case) über den gesamten Projektlebenszyklus hinweg stellt sicher, dass Ressourcen nur in Projekte investiert werden, die tatsächlich zum Unternehmenserfolg beitragen. Projekte ohne klaren Mehrwert können frühzeitig gestoppt werden, was Fehlinvestitionen jeglicher Art massiv reduziert. Die Methodik organisiert Projekte in Management-Phasen mit festen Entscheidungspunkten (Gates). Dies ermöglicht der Führung das Projekt nur an kritischen Übergängen überprüfen zu müssen. Durch das Prinzip Management by Exception (Steuern nach dem Ausnahmeprinzip) wird die Führungsebene entlastet, da nur dann eingegriffen werden muss, wenn definierte Toleranzen (Zeit, Budget, Umfang) überschritten werden. Dies erhöht die Steuerbarkeit und vermeidet die Überlastung mit operativen Details. Im Zuge der Schulungen wurde von den Teilnehmer sehr schnell erkannt, dass es wichtig ist eine einheitliche Sprache zu sprechen und klare Rollen und Verantwortlichkeiten zu definieren. Diese Grundlage liefert PRINCE2 und beseitigt damit auch vorherrschende Zuständigkeitskonflikte. Dadurch wird die Entscheidungsfindung beschleunigt, da jeder Projektbeteiligte seine Befugnisse und Aufgaben genau kennt. Durch die systematischen Management-Themen (Risiko, Qualität, Pläne) werden Probleme nicht erst am Ende erkannt, sondern proaktiv gesteuert. Dies ist entscheidend um Fehlinvestitionen oder sicherheitsrelevante Probleme zu vermeiden. Der Fokus auf Produkte und tatsächlich messbaren Nutzen reduziert Unklarheiten und soll die Akzeptanz der Mitarbeiterinnen und Mitarbeiter erhöhen. Die obligatorische Dokumentation von Lessons Learned verankert zudem einen kontinuierlichen Verbesserungsprozess.

Die Direkton 6 beabsichtigt PRINCE2 als Framework einzuführen, um ihre Projektergebnisse in puncto Verlässlichkeit, Effizienz und strategische Ausrichtung umzustellen und erhofft sich durch die Schaffung gemeinsamer Standards auch die Zusammenarbeit über die Direktion hinaus zu erleichtern. Die anfänglichen Investitionen in Schulung und Anpassung amortisieren sich durch die Vermeidung von kostspieligen Projektabbrüchen und die Steigerung der Termintreue.

Prozessorientiertes Wissensmanagement mittels der webbasierten Software ADONIS

In den nächsten 10 Jahren werden circa 8000 Personen des ÖBH den Ruhestand antreten. Hinzu kommt auch die zunehmende Bereitschaft der Mitarbeitenden, Dienstverhältnisse zu lösen, um anderswo beruflich tätig zu werden.

Das Durchschnittsalter im Ressort betrug 2024 42,5 Jahre (auf Ebene der Direktionen ist es noch höher). Wenn Erfahrungs- und Arbeitswissen nicht oder unzureichend dokumentiert ist, droht dadurch der Verlust (organisations-)kritischen Wissens. Das kann schlimmstenfalls die Handlungsfähigkeit und Flexibilität der betreffenden Organisationseinheiten (OE) einschränken.

Das gegenwärtige Informationszeitalter ist unter anderem durch das digitale Durchdringen aller Lebensbereiche geprägt. Die dadurch entstehende Dynamik ermöglicht schnelleres und präziseres Arbeiten. Dieser Wandel wird durch gesteuerte, zentrale Bereitstellung von Information und Wissen sowie KI-Automatisierung unterstützt.

Als zentrale Zukunftsaufgabe wurde die Digitalisierung des Bundesheeres ausgemacht, bei der die Direktion 6 - IKT und Cyber eine führende Rolle einnimmt.

Die Kenntnis der eigenen Prozesse ist die Basis für die Digitalisierung dieser. Während der Modellierung der Prozesse können schon Optimierungsmöglichkeiten erkannt und Ansätze für die Digitalisierung herausgearbeitet werden. Unter Nutzung von Mitteln der IKT und der KI können die Prozesse dann vereinfacht, gekürzt und leichter zugänglich gemacht werden.


Grafik: KI-generierte Abbildung, Bundesheer/Dion6


Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Die Leitung der Direktion 6 - IKT und Cyber hat die diesbezüglichen Herausforderungen erkannt und ergreift Maßnahmen, um den Wissenserhalt und Wissenstransfer zu begünstigen, sowie die digitale Transformation zu ermöglichen. Eine dieser Maßnahmen ist die Initiierung eines Projekts zur Einführung eines prozessorientierten Wissensmanagements mittels Business Process Model Notation (BPMN)-basierter Software.

Der diesbezügliche Projektauftrag lautet:

Einführung des prozessorientierten Wissensmanagements mittels der webbasierten Software ADONIS innerhalb der Direktion 6 - IKT und Cyber/Leitung (das sind die Abteilungen IKTBstg&NuMngt, IKTCyE, IKTCyPl und das Referat Budg&Pers) in 5 Phasen, unter Bedachtnahme auf die Individuallage der verschiedenen angesteuerten Organisationseinheiten, beginnend mit September 2025.

Mit der Durchführung des Projektmanagements wurde das Referat Informations- und Wissensmanagement (RefIWM) der Abteilung IKTBstg&NuMngt der Direktion 6 - IKT und Cyber beauftragt. Dieses Projekt wird nach dem Projektmanagementframework PRINCE2 (PRojects In Controlled Environments 2) durchgeführt - eine weltweit anerkannte und bewährte (prozessbasierte) Projektmanagement-Methode aus dem britischen Raum, die durch ihre Anpassungsfähigkeit an die notwendigen Bedarfe besticht.

Der Projektplan sieht die Erfüllung des Auftrages bis zum I. Quartal 2027 vor.

Die listenmäßige, systematische Sammlung aller in der Direktion 6 - IKT und Cyber/Leitung durchzuführenden Norm-Prozesse sollte mit Beginn 2026 abgeschlossen sein. Danach folgt die Vermittlung des notwendigen Basiswissens zur Umsetzung des prozessorientierten Wissensmanagements mittels der Softwareanwendung ADONIS in Form von Workshops für ausgewählte Mitarbeitende. Anschließend werden priorisierte Prozesse in der Applikation ADONIS „modelliert" (= die einzelnen Prozessschritte werden visuell zusammenhängend dargestellt und mit den notwendigen, aktuellen Wissensprodukten und Beschreibungen hinterlegt).

Bis Herbst 2026 sollten dann referats- bzw. abteilungsübergreifende Prozesse der Direktion 6 – IKT und Cyber über einen Intranet-Link (auch ohne zugewiesener Software ADONIS) abrufbar sein. Das Projekt endet nach einer Projektevaluierung und der Regelung des Überganges von der Projektorganisation in die Linienorganisation. So die Ergebnisse den Erwartungen entsprechen, ist mit einer Ausweitung auf die gesamte Direktion zu rechnen.

Dieses Projekt ist ein Beitrag zur Durchführung und Entwicklung von Verbesserungsmaßnahmen, die das ÖBH (und speziell die Direktion 6 – IKT und Cyber) stärken sollen. Fortschritt kann nur gelingen, wenn wir uns gemeinsam bewegen und Neues wagen.

Denn: „Wer immer tut, was er schon kann, bleibt immer das, was er schon ist." (Henry Ford)

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Unterstützungselement CDO&CIO

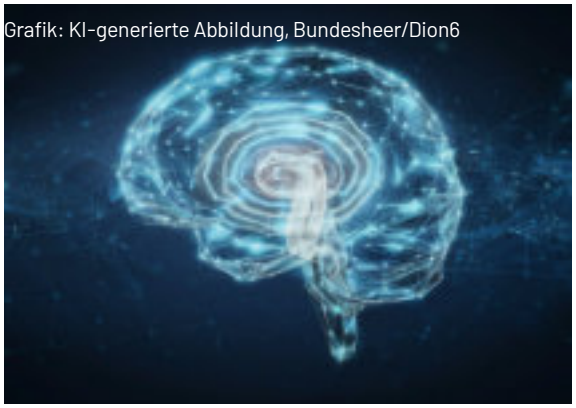
Im Alltag begegnet uns der Begriff Digitalisierung immer häufiger. Doch was bedeutet Digitalisierung eigentlich und warum ist sie so wichtig?

Digitalisierung betrifft nicht mehr nur klassische IT-Bereiche oder spezialisierte Technologien. Heute durchdringt die Digitalisierung nahezu alle Lebens- und Gesellschaftsbereiche. Sie eröffnet Chancen für Innovation, Effizienz und Nachhaltigkeit: Sie kann die Produktivität steigern, Wirtschaftswachstum und Wohlstand fördern, Verwaltungskosten senken und gesellschaftliche Teilhabe erleichtern. Auch für Einzelpersonen ergeben sich Vorteile, etwa durch staatliche E-Services, die über Anwendungen wie ID-Austria unkompliziert zugänglich werden.

Gleichzeitig gewinnt die Digitalisierung vor dem Hintergrund geopolitischer Konflikte, wirtschaftlicher Krisen und hybrider Bedrohungen zunehmend sicherheitspolitische Bedeutung. Die vermehrten Angriffe auf kritische Infrastrukturen (etwa durch Drohnen in anderen EU-Mitgliedstaaten) machen deutlich, dass digitale Fähigkeiten für die Sicherheit Österreichs unverzichtbar geworden sind. Dazu zählen unter anderem die Erstellung und Bereitstellung von Lagebildern in Echtzeit, der Einsatz von Drohnen und Satellitennetzwerken für eine zuverlässige Befehlsübermittlung sowie die umfassende Vernetzung des Gefechtsfelds.

In diesem Zusammenhang darf auch der Bereich der Künstlichen Intelligenz nicht außer Acht gelassen werden. KI-gestützte Analysen und Mustererkennungen leisten einen wichtigen Beitrag zur Führungsunterstützung. Die Technologie zeigt bereits in aktuellen Konflikten ihr Potenzial und wird in naher Zukunft zu einem festen Bestandteil moderner militärischer Fähigkeiten werden.

Damit die Potenziale der Digitalisierung im ÖBH bestmöglich ausgeschöpft werden können, verantwortet der CDO/CIO die Entwicklung digitaler Strategien, die Steuerung der organisatorischen Transformation, den Aufbau einer datengetriebenen Organisationskultur


Grafik: KI-generierte Abbildung, Bundesheer/Dion6

sowie die Weiterentwicklung des Innovationsmanagements. Strategische Leitlinien und bundesweite Innovationsvorhaben werden im Rahmen der CDO-Task-Force gemeinsam mit den weiteren CDOs abgestimmt und festgelegt.

So wurden etwa zentrale Strategien wie der Digital Austria Act, das sich auf die Digitalisierung in Österreich konzentriert, ressortübergreifend erarbeitet. Dieses digitale Arbeitsprogramm der Bundesregierung umfasst 117 Maßnahmen und 36 Digitalisierungsgrundsätze, die die digitale Entwicklung des Landes weiter vorantreiben sollen. Ebenso sind andere wichtige Strategiedokumente, darunter die Strategie für Künstliche Intelligenz, die Datenstrategie für Österreich oder die Digitale Kompetenzoffensive, Ergebnisse der interministeriellen Zusammenarbeit der CDOs.

Das Unterstützungselement CDO&CIO (UEtCDO&CIO) unterstützt den CDO/CIO bei der Planung und Koordination der Umsetzung von Vorhaben im Rahmen der digitalen Transformation. Dazu gehört die Zuarbeit bei der Analyse der ressortinternen Strategien (Digitalisierungsstrategie, IKT-Strategie, Datenstrategie, KI-Strategie) ebenso wie die eigenständige Entwicklung konkreter Projekte zu den darin definierten Handlungs- und Themenfeldern.

Außerdem koordiniert das UEtCDO&CIO die Umsetzung der entwickelten Digitalisierungsprojekte und Digitalisierungsvorhaben nach der entsprechenden Entscheidung durch den CDO/CIO.

KI-Assistenten

Die rasante Verbreitung von KI-Assistenzsystemen eröffnet enorme Potenziale für Effizienzsteigerungen und datenbasierte Entscheidungsfindung, doch gleichzeitig birgt die unkontrollierte Einführung erhebliche Risiken wie Compliance-Verstöße, ethische Fehltritte, Datenmissbrauch und unvorhergesehene Fehlfunktionen.

Daher ist ein strukturierter Prozess zur Implementierung von KI-Assistenten unverzichtbar, weil er systematisch Anforderungen definiert, geeignete Technologie- und Datenquellen auswählt, klare Verantwortlichkeiten und Governance-Mechanismen etabliert, Pilot- und Validierungsphasen integriert sowie kontinuierliches Monitoring und Anpassungen sicherstellt – ein Ansatz, der sowohl die strategische Nutzenmaximierung als auch die Risikominimierung gewährleistet.

In der nachfolgenden Abbildung ist ein Prozess für die Einführung von KI-Systemen vereinfacht dargestellt.

Abbildung 1: Übersicht der neun Kriterien für einen nachhaltigen KI-Einsatz
© Idea_Lab, Universität Graz

Grafik: Idea_Lab, Universität Graz

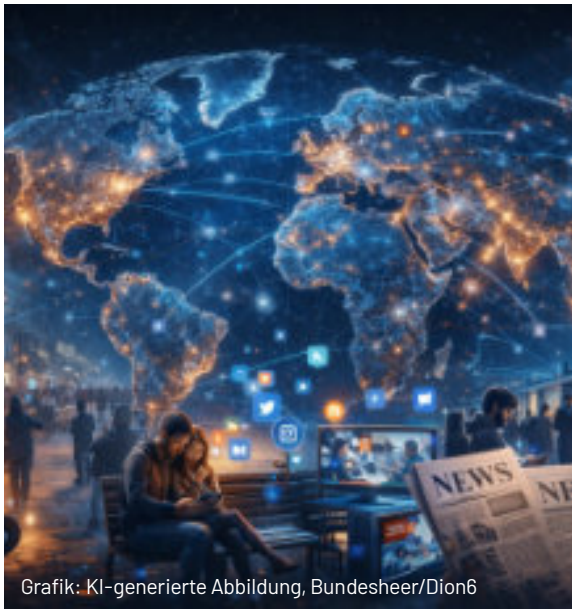
InfoOps&opKomm

Die Informationskräfte spielen eine entscheidende Rolle bei der Abwehr von Bedrohungen im Informationsraum und der Aufrechterhaltung der kognitiven Sicherheit im digitalen Zeitalter. Durch das Verständnis und die operative Tätigkeit im Informationsraum stärken sie die nationale Resilienz und schützen vor der manipulativen Nutzung von Informationen.

InfoOps

Im Zielbild 2032+ erging der Auftrag zum Aufbau der Informationskräfte bestehend aus den Kommunikationstruppen und den PsyOps-Truppen, geführt durch das aufzubauende Kommando Informationsoperationen.
Diese sind befähigt den Kampf im Informationsraum zu führen. Sie verteidigen Österreich als integraler Bestandteil der militärischen Strategie in der virtuellen Domäne Informationsraum, erhöhen die Effektivität der Streitkräfte und schützen uns vor kognitiver Kriegsführung und gegnerischer Beeinflussung.

Die Informationskräfte operieren als wichtiger Bestandteil der hybriden Kriegführung in den Einsatzarten „Beeinflussen", „Informieren" und „Analyse und Auswertung".



Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Sie dienen der Stärkung der Moral der eigenen Truppe und Bevölkerung und sonstiger befreundeter Gruppierungen und deren Schutz vor feindlicher Desinformation und Propaganda sowie der Beeinflussung gegnerischer Kräfte oder definierter Zielgruppen zur Schwächung des Willens und der Kampfmoral.

Der Informationsraum umfasst alle Formen von Informationen und deren Verbreitung, einschließlich der psychologischen Dimension, in der Menschen Informationen deuten und darauf reagieren.

Durch die zunehmende Bedeutung der Technologie der Vernetzung und der digitalen Kommunikation in globalen Austauschprozessen ist der Informationsraum zu einem zentralen Element moderner Kriegsführung geworden.

Im militärischen Bereich nutzen Operationen digitale Technologien, um strategische Informationen zu sammeln, zu analysieren und zu verbreiten.

Die Verbreitung von Botschaften im Informationsraum erfolgt dabei über verschiedene Kanäle, darunter klassische Medien wie Radio, Fernsehen und Print, aber auch über soziale Netzwerke und digitale Plattformen.

Um das Zielbild 2032+ zu verwirklichen wurden 2025 folgende Schritte gesetzt:

- Motivenberichte und Vorhabensabsichten in den Waffengattungen Kommunikationstruppe und PsyOps-Trupp
- Vorschriftenerstellung und Fähigkeitenentwicklung
- Internationale Kurse im Bereich Informationsoperationen und Strategische Kommunikation (USA, DEU, TUR)
- Mitwirken bei internationalen Projekten, wie z.B. Countering Cognitive Warfare im Rahmen von Multinational Capability Development Campaign (MCDC)
- Erstellung nationaler Projokte wie z.B. Lagebild Zuarbeit beim Aufbau des FHQs im Rahmen des J10/InfoOps

opKomm

IT und Berufsmessen, Studienmessen und Firmeninformationstage an Schulen

Im Jahr 2025 war die Direktion 6 - IKT und Cyber bei zahlreichen Veranstaltungen und Schulbesuchen aktiv, um Schülerinnen und Schüler sowie die Öffentlichkeit über die vielfältigen Karriere- und Ausbildungsmöglichkeiten im Bereich IKT und Cyber zu informieren.

Die Events erstreckten sich von Recruiting Days und Firmeninformationstagen an verschiedenen HTLs bis hin zu großen Karrieremessen und Sicherheitskonferenzen.

Ein besonderer Fokus lag auf den Events an HTLs wie Wiener Neustadt, Ungargasse, Mödling, St. Pölten und vorallem unserer Partnerschule der HTL Spengergasse. Bei diesen Veranstaltungen präsentiert die Direktion 6 die Aufgaben und Möglichkeiten im IKT- und Cyberbereich, insbesondere den Cyber-Grundwehrdienst und stießen auf großes Interesse. Viele Schülerinnen und Schüler zeigten sich überrascht von der Modernität und Vielfalt der Angebote. Besonders erfreulich war die zunehmende Anzahl an weiblichen Interessentinnen, die sich über Karrieremöglichkeiten im Bereich IKT und Cyber sowie über die Möglichkeiten als Zivilistin oder im militärischen Bereich informierten.

Foto: HTL-Spengergasse, Bundesheer/Dion6

Foto: BeSt-Messe, Bundesheer/Dion6

Auch bei großen Karrieremessen wie der BeSt in Wien und der Jobmesse Austria in der Marx Halle Wien war die Direktion 6 - IKT und Cyber stark vertreten. An diesen Veranstaltungen nutzten Schülerinnen und Schüler, aber auch Familien und ältere Interessenten die Gelegenheit, sich über die breite Palette an Berufsmöglichkeiten im ÖBH zu informieren.

Darüber hinaus nahm die Direktion 6 an fachspezifischen Veranstaltungen wie der IT-SecX 2025 in St. Pölten teil, bei der sich Expertinnen und Experten aus dem Bereich IT-Security austauschten.

Auch zu erwähnen ist die Teilnahme an der IKT-Sicherheitskonferenz in Dornbirn (24.-26. Juni), bei der eine Partnerschaftsurkunde zwischen dem Bundesheer und dem Verein Austria Cyber Security Challenge unterzeichnet wurde.

Zudem pflegte die Direktion 6 enge Kontakte zu IT-HTLs in ganz Österreich. So fanden Besuche in der Stiftkaserne durch Schülergruppen der HTL Waidhofen a.d. Ybbs und der HTL Wels statt. Bei diesen Veranstaltungen bekamen die Schülerinnen und Schüler Einblicke in technische Innovationen wie z.B. den Einsatz von LibreOffice.

Im Zuge der engen Beziehungen zu IT-HTLs wurde auch ein Partnerschaftstreffen mit der HTL Spengergasse veranstaltet.


Foto: Locked Shields 25, BMLV/HBF

Internationale Übungen und sonstige Veranstaltungen

Internationale Zusammenarbeit stand im Fokus der Übung "Locked Shields 2025", der weltweit größten Cyber-Verteidigungsübung. Das österreichische StratKomm Team erreichte bei der Übung den 2. Platz von 17 internationalen Teams.

2025 fand der erste Workshop der Abteilung IKTBstg&NuMngt statt, bei dem die Digitalisierung der Streitkräfte und der Aufbau einer neuen Waffengattung "Informationsoperationen" diskutiert wurden. Diese Initiativen zeigen, dass das Bundesheer aktiv an der Weiterentwicklung seiner Fähigkeiten arbeitet, um zukünftigen Herausforderungen gerecht zu werden.

EscapeRoom Ausrückungen

Girls Day 2025 in der Maria-Theresien-Kaserne

Am 24. April 2025 öffnete die Maria-Theresien-Kaserne ihre Tore für den Girls Day. Mädchen und junge Frauen informierten sich über vielfältige Karrieremöglichkeiten im Bundesheer, wie z.B. als Gardesoldatin, Militärpolizistin oder im Bereich IKT und Cyber. Highlights waren der Flugsimulator, eine Fahrt im Dingo 2 und der neue Escape Room zum Thema Fake News. Die Veranstaltung zeigte deutlich das gestiegene Interesse junger Frauen am Bundesheer und an Cyber-Sicherheit.

Tage der offenen Tür und Cyber Days

In der JANSA-Kaserne (23.-26. April) und der HTL Rennweg (14.-16. Mai) wurden die Besucher mit dem Escape Room und Vorträgen zu Cyber-Sicherheit begeistert. Besonders bei jungen Schülern stieß das Angebot auf große Resonanz. Die direkte Ansprache und der praktische Bezug der Inhalte förderten den Dialog mit Schülern und Lehrern.

Große Events und Feste

Beim Donauinselfest (20.-22. Juni) und dem Schulfest "Hot in the City" (24.-26. Juni) in Wien zog der Escape Room tausende Besucher an.

Bei der "Level Up"-Messe in Salzburg (28.-29. Juni) und den Tagen der offenen Tür in Klagenfurt (1. Juli) und Spittal an der Drau (2. Juli) sowie dem Landesfeuerwehrjugendtreffen in Sigmundsherberg (Juli) war der Escape Room stets ausgebucht. Die Veranstaltungen boten eine Mischung aus Unterhaltung, Information und interaktiven Angeboten, die bei Besuchern aller Altersgruppen Anklang fanden.


Foto: Level Up, Bundesheer/Dion6


Foto: Nationalfeiertag 2025, Bundesheer/Dion6

Nationalfeiertag 2025 und Tag der Schulen

Am 26. Oktober feierte das Bundesheer sein 70-jähriges Jubiläum mit einer eindrucksvollen Leistungsschau in der Wiener Innenstadt. Auf dem Heldenplatz und weiteren Schauplätzen präsentierten die Direktion 6 modernste Ausrüstung, von Drohnen bis hin zu künstlicher Intelligenz. Die Themeninsel "Cyber, Forschung und Technik" begeisterte die Besucher mit innovativen Ausstellungsstücken wie Drohnen, autonomen Fahrzeugen und KI-Anwendungen.

Der "Tag der Schulen" am Heldenplatz, bei dem rund 7.000 Schülerinnen und Schüler aus Wien und Umgebung die Gelegenheit hatten, das Bundesheer kennenzulernen. Die jungen Besucher erlebten ein abwechslungsreiches Programm, darunter unseren Cyber Escape Room und interaktive Mitmachangebote.


Foto: Interview, Bundesheer/Dion6

Military Public Affairs (milPA)

Aktivitäten und Initiativen in Social Media, Printmedien und TV und Radio

Aus dem Bereich milPA ist besonders der Erfolg unserer 27 Kurzvideos aus der Reihe „Digital – ganz real" hervorzuheben. In jeder Folge wird ein Experte „im Schatten" über seine Tätigkeit interviewt und bisher konnten insgesamt 645.000 Nutzer auf Instagram, TikTok, Facebook und Youtube erreicht werden. Es hat sich um eine Comunity von ca 10.000 bis 15.000 Aufrufe innerhalb von 2 Tagen gefunden.

Auf unserer Webpage wurden die Mitarbeiterinnen und Mitarbeiter der Direktion, und natürlich auch alle anderen Interessierten, mit knapp 70 Beiträgen über intressante Projekte und Feierlichkeiten informiert.

Das Thema „Digitale Souveränität" hat im Jahr 2025 sehr hohes Medieninteresse erlangt und eine größere Anzahl von Interviewanfragen, darunter ZiB2 Spezial und Ö1 hervorgefufen. Zu diesem Thema waren darüber hinaus mehr als 15 Journalistenanfragen schriftlich zu beantworten.
Es ist auch für 2026 mit einem hohen Interesse an diesem Thema zu erwarten, da die Anerkennung unserer Experten bereits international nachgefragt wird.

Um dieser verstärkten Nachfrage gerecht zu werden organisierte InfoOps&opKomm ein 2 tägiges Interviewtraining, das sicherlich 2026 eine Wiederholung erfahren wird. Die Themen Informationsraum, KI, Space und Digitale Souveränität lassen auch im kommenden Jahr ein hohes Medieninteresse erwarten.

IKT Cyberplanung

Leiter IKTCyPl (m.d.F.b.): ObstdG Mag. Klaus JENSCHIK


Foto: BMLV/HBF

Als eingeteilter Leiter der Abteilung IKTCyPl konnte ich mich seit 01. Februar 2025 von den Fähigkeiten, der Energie, der Motivation und dem ausgezeichneten Fachwissen der Mitarbeiterinnen und Mitarbeiter überzeugen. Die drei Standorte der Abteilung Wien, Salzburg und Villach erleichtern die Kommunikation mit den Bedarfsträgern und den militärstrategischen und operativen Planungsstellen. Die Kooperation mit der Generaldirektion Präsidium (GDPräs) und der Gruppe Direktion Fähigkeits- & Grunsatzplanung (GrpDion-Fäh&GSPl) wurde durch die Dislozierung v.a im Amtsgebäude Rossau ermöglicht. Die räumliche Nähe zur Stift Kaserne erleichtert die Abstimmung mit der Führung der Direktion 6 - IKT und Cyber und dem IKT&CySihZ.

Wegen Verwendungsänderungen und Übertritt in den Ruhestand haben einige Mitarbeiter die Abteilung verlassen. Meist jüngere Mitarbeiterinnen und Mitarbeiter konnten für die Bereiche Systemarchitektur, elektronische Kampfführung (EloKa) und Administration gewonnen werden. Ein großes Personalfehl besteht weiterhin bei den Waffengattungen Psychologische Operationen (PsyOps)- und Kommunikationstruppe.

Höhepunkt 2025 war die Vorbereitung und Durchführung des Wargame Führungsüberlegenheit, mit den Teilaspekten Informations- und Entscheidungsüberlegenheit, im Juli. Dabei konnten die bisherigen Planungen überprüft und Erfahrungen zur Weiterentwicklung gewonnen werden. Basierend auf diesem Wissen konnten die Motivenberichte FüU- und Cyber-Truppe finalisiert werden. Die Erarbeitung einer einsatztauglichen ÖBH-Business Architektur wurde initiiert. Die Ausbildungssystematik von Offizieren, Unteroffizieren und zivilen Mitarbeiterinnen und Mitarbeitern im Fachbereich wird im Hinblick auf das Zielbild ÖBH2032+ weiterentwickelt.

Dieses Zielbild bedeutet auch eine klare Priorisierung der Bearbeitungen und die Abstützung auf internationale Kooperationen, v.a. im Fernmeldenetz (FMN)- und DACH-Format, externe Ressourcen und Milizexperten.

Routinemäßig erarbeiten wir Planungsdokumente als Grundlage für die nachfolgende, meist mehrjährige Realisierung der Fähigkeiten.

2025 waren dies (federführend oder mitwirkend) die Erstellung der Planungsgrundlagen für u.a. Raketenartilleriebatterie, bodengebundene Luftabwehr, Schützen- und Radpanzerflotte, Gefechtsstandsystem großer Verband, Joint Fire Support, ortsfeste und verlegbare Einsatzrechenzentren, EloKa-Zug- und -Kompanie.

Klare Ziele für uns bleiben die Entwicklung der Grundlagen für die Einsatzbereitschaft (Mission Cloud/ IKT-System Einsatz/ Cyber/ EloKa) – für die Streitkräfteplanung im Frieden und Einsatz (Plans Cloud) und eine moderne Verwaltung (Business Cloud) – im multinationalen Umfeld.

Besuch bei AIT am 30.September 2025

Die Abteilung IKT Cyberplanung besuchte im Wege der Kaderfortbildung am 30. September 2025 das Austrian Institute of Technology – AIT. Annähernd vollzählig wurden die Mitarbeiter der Abteilung vom Head of Center Dipl.-Ing. Helmut Leopold empfangen und durch den Vormittag geleitet. Das interessante Programm war gegliedert in die Vorstellung des AIT, der Projektlandschaft und konkreter Forschungsbereiche die aktuell behandelt werden. Als besonders interessant stellten sich die Themen zu Cybersecurity und Verschlüsselungstechnik heraus.

Für die Mitarbeiter der Abteilung IKT Cyberplanung gab es aufschlussreiche Diskussionen, die für die internen Planungsprojekte von hohem Nutzen waren. Dipl.-Ing. Leopold unterstrich mehrfach den Mehrwert und die Unterstützungsleistungen die durch das AIT dem BMLV zur Verfügung stehen. Ein großer Dank gilt dem Präsentatorenteam des AIT für die interessanten und aktuellen Inhalte und den angeregten Diskussionen und Einzelgesprächen.

Materialstruktur

IT-Materialstruktur

Im Zuge der „Strukturanpassung der Zentralstelle und Kommanden der oberen Führung im ÖBH", wurden einige Organisationspläne zunächst ohne Sachmittelteil verfügt. Das Schwergewichtig im Bereich IT-MatStrukt lag daher auf der Einarbeitung der noch fehlenden Daten in die IT-MatStrukt-Applikation als Grundlage für alle weiteren Bearbeitungsschritte der Abteilungen Strukturplan und Organisation.

Nachdem jedoch die ersten Direktionen erfolgreich eingearbeitet waren, folgten auch schon die ersten Evaluierungsanträge. In Summe erreichten die Abteilung IKTCyPl im Jahr 2025 an die 250 ELAK-Geschäftsstücke mit dem Betreff „Änderung der IT-MatStrukt" und sorgten dadurch für einen konstant hohen zusätzlichen Arbeitsaufwand.

Erfreulicherweise konnte mit 01. Oktober eine neue Verwaltungspraktikantin aufgenommen werden, die bereits nach kurzer Einschulungszeit bei der Bearbeitung der IT-MatStrukt tatkräftig mithelfen konnte.

Ein weiteres Schwergewicht lag bei der Umsetzung der geplanten Erhöhung der Anzahl an dienstlichen Smartphones (iPhones) im Ressort. Im Rahmen der o.a. zahlreichen Anpassungen der IT-MatStrukt konnte, in enger Abstimmung mit den POCs der jeweiligen Direktionen oder Abteilungen, die Summe der Smartphones bereits signifikant erhöht werden. Die Ebene „Referatsleiter" wurde in der IT-MatStrukt vollständig auf Smartphones umgestellt, teilweise konnten aber auch schon einige „Referenten" bei der Bearbeitung berücksichtigt werden. Die Priorität bei der Umsetzung lag neben den neugeschaffenen Direktionen 1-8 v.a. bei Schulen und Akademien.

Experten

IT-SECX 2025: Sicherheit neu gedacht – von der Straße bis ins Weltall

Am 2. Oktober 2025 verwandelte sich der Campus der FH St. Pölten erneut in einen Treffpunkt für Cybersecurity-Enthusiasten, Fachleute und Studierende. Die diesjährige IT-SECX – IT Security Community Exchange stand unter dem visionären Motto:

„To boldly secure what no one has secured before – from road to space security."

Grafik: IT-SecX, Obst Joachim KÖLL

Damit rückte die Konferenz jene sicherheitsrelevanten Bereiche in den Fokus, die zunehmend unser modernes Leben prägen – von vernetzten Verkehrssystemen bis hin zu weltraumbasierten Infrastrukturen.

Bereits die Eröffnung setzte ein starkes Zeichen: ObstdG Franz Sitzwohl beleuchtete in seinem Impulsvortrag die Herausforderungen und Chancen moderner Information Operations. Sein Beitrag zeigte eindrucksvoll, wie stark Informationsräume heute mit sicherheitspolitischen Realitäten verwoben sind – und wie relevant strategische Kommunikation im Zeitalter hybrider Bedrohungen geworden ist.

Parallel zur Hauptkonferenz fand erneut das etablierte Side-Event „Experten im Militär und BMLV meets FHSTP" statt. Dieses jährliche Format bringt hochkarätige Fachleute aus der Direktion 6, Angehörige der Führungsunterstützungsschule (FüUS) sowie Vertreterinnen und Vertreter des BMI mit Forschenden und Lehrenden der FH St. Pölten zusammen.

In einem eigenen, geschützten Bereich tauschten sie sich über Themen wie Künstliche Intelligenz, Cyber Defence, Security-Strategien und aktuelle technologische Entwicklungen aus.

Organisiert wurde dieses wertvolle Vernetzungsformat auch heuer wieder von Militärexperten der IKTCyPI und FüUS für eine reibungslose Durchführung sorgte. Die offene Gesprächskultur und der enge fachliche Austausch machten das Side-Event erneut zu einem Highlights der gesamten IT-SECX.

Mit ihrer Mischung aus hochaktuellen Themen, anwendungsorientierten Vorträgen und lebendigem Networking bestätigte die IT-SECX 2025 einmal mehr ihren Ruf als eine der bedeutendsten Security-Veranstaltungen des Landes.

Und eines steht bereits fest: Auch im kommenden Jahr wird die IT-SECX fortgesetzt – mit neuen Impulsen, neuen Ideen und erneut mit dem Ziel, die Zukunft der Cybersicherheit aktiv mitzugestalten.

Foto: IT-SecX, Obst Joachim KÖLL


Foto: Ausmusterung -Experten, Obst Joachim KÖLL

Erste Ausmusterung von Experten im Militär der Direktion 6 am Tag der Leutnante

Vom 26. bis 27. September 2025 fand an der Theresianischen Militärakademie der Tag der Leutnante statt. In diesem Jahr wurden in Wiener Neustadt 76 Berufs- und 46 Milizoffiziere, darunter neun Frauen, feierlich in die Truppe übernommen. Die Dion 6 war in diesem Jahr mit 5 Experten vertreten.

Im Laufe der letzten Monate bzw. Jahre wurden dazu die erforderlichen Seminare an der Landesverteidigungsakademie sowie die Erstellung einer fachspezifischen Hausarbeit (Expertise im Fachbereich) positiv absolviert. Abschließend erfolgte die Überstellung auf den Arbeitsplatz und Beförderung zum Oberleutnant des Expertendienstes (OltExp).

Schon in der Vorbereitung der Veranstaltung konnten wir die Kameradschaft und den Zusammenhalt stark wahrnehmen, denn es galt sämtliche Uniformbestandteile des Ausgangsanzuges inklusive Volldekoration (Ordensschnalle) vorzubereiten. Betreffend Ablauf der Tage bestand auch ein guter Kontakt zum Jahrgangssprecher der Fähnriche des Ausmusterungsjahrganges 2025 „Generaloberst Josef Roth", was die Vorbereitung erheblich erleichtert hat.

Militärisches Informationsmanagement zur Unterstützung der digitalen Souveränität

Im Kern besteht das Informations-management aus dem Erfassen von Daten und Informationen, dem Speichern (z. B. Datenbanken, Archive, Systeme), dem Analysieren und Verarbeiten (um Wissen zu generieren), dem Verteilen oder Übermitteln (an die richtigen Stellen, zur richtigen Zeit), dem gleichzeitigen Schützen (Vertraulichkeit, Integrität, Verfügbarkeit) und zu guter Letzt dem Löschen bzw. Unbrauchbarmachen (wenn Informationen nicht mehr gebraucht oder gefährlich werden).

Im militärischen Kontext bekommt das Informationsmanagement eine besondere Dimension, weil Informationen eine operative Ressource sind – ähnlich wie Munition, Treibstoff oder Personal.

Das militärische Informationsmanagement ist daher weit mehr als reine Datenverwaltung. Mit diesem Fokus lässt sich die Thematik wie folgt gliedern:

Grafik: Bundesheer

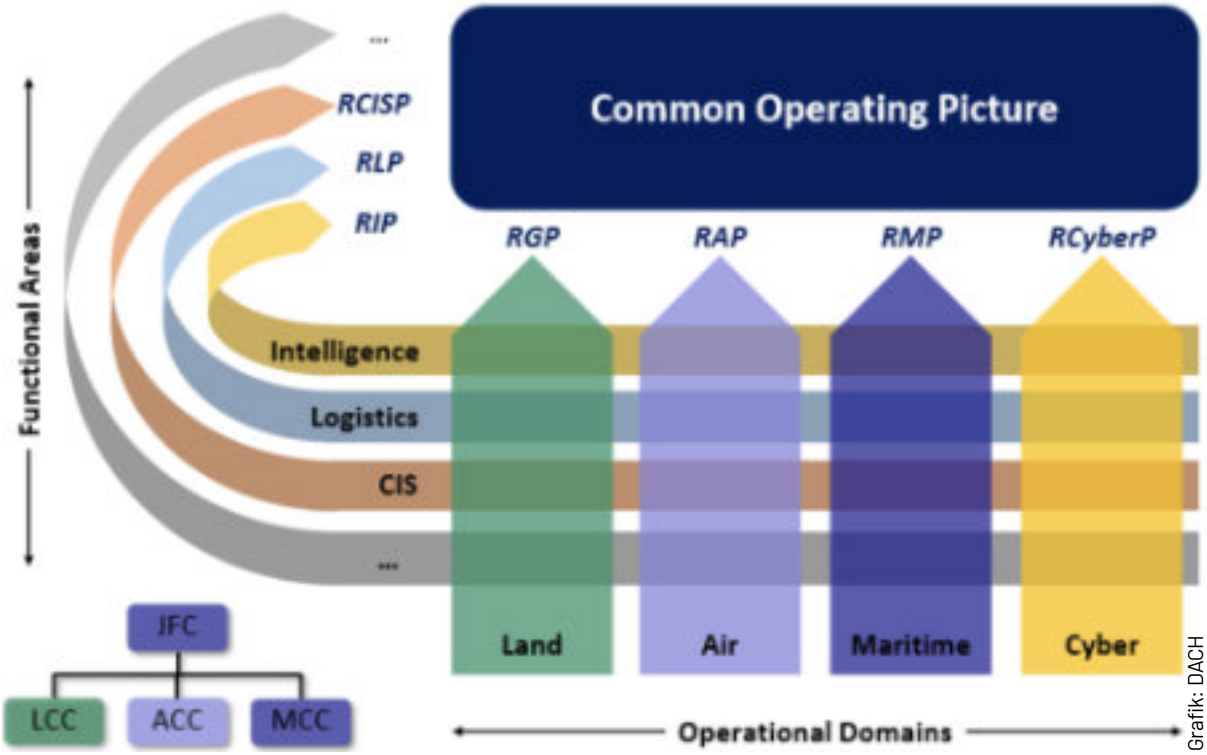
Die Informationssammlung beinhaltet sowohl den Anteil der Aufklärung (bestehend aus SIGINT1, HUMINT2, OSINT3, GEOINT4 usw.), die Überwachung von Kommunikationsnetzen, Sensoren und Drohnenbildern sowie das Sammeln von Lageinformationen (durch Meldeflüsse über die Chain of Command).

Eine Auswertung der Informationen erfolgt im Bereich der Informationsverarbeitung & Analyse. Entscheidend beim Erstellen von Lagebildern durch Aufbereitung und richtiger Interpretation der Daten (beispielsweise für Lagekarten in Operationszentren) ist eine korrekte Mustererkennung in den gewonnenen Informationen (z.B. Bewegungen von Truppen oder im Falle von Cyber-Aktivitäten) sowie die richtige Fusion unterschiedlicher Quellen zu einem schlüssigen Gesamtbild (COP5).

Eine rasche und zutreffende Informationsverteilung stellt sicher, dass der jeweilige Soldat (Kommandant) zur richtigen Zeit über die relevante Information zur Auftragserfüllung verfügt (z.B. durch Führungsinformationssysteme bzw. Battlefield Management Systems; BMS). Dabei ist auf korrektes Priorisieren, Filtern, Verdichten und bestmöglich richtiges Interpretieren dementsprechend Wert zu legen.

Bezüglich Schutz & Kontrolle der Daten sind wesentliche Aspekte der Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit sensibler Informationen nach den geltenden Bestimmungen der Geheimhaltung, Verschlüsselung und Zugriffsbeschränkungen zu realisieren. Schutz vor Desinformation, vor einem gegnerischem Cyberangriff oder vor gegnerischer Aufklärung (SIGINT) bieten unter anderem die Anwendung eines „Need-to-know"-Prinzips und die Verwendung aktueller Sicherheitsstrategien und –modelle wie Zero Trust (ZT) oder Methoden wie Data Centric Security (DCS), welche eine zeitgemäße Sicherung sensibler Informationen ermöglichen sollen.

Eine Besonderheit im militärischen Informationsmanagement stellen offensive Informationsoperationen (InfoOps) dar.



Grafik: DACH

Sie werden durch Psychological Operations (PSYOPS), durch Electronic Warfare (EW; durch Stören von Kommunikationskanälen), mit Cyberoperationen, oder durch Täuschung und Desinformation - mit dem klaren Ziel den Gegner zu verwirren, zu demoralisieren oder zu steuern – zur Anwendung gebracht. All diese Aspekte dienen der Führungsunterstützung. Dabei werden militärische Entscheidungsträger (Kommandanten) mit Informationen versorgt und deren Entscheidungsprozesse durch die Nutzung neuer Technologien (im „OODA-Loop": Observe – Orient – Decide – Act) unterstützt und beschleunigt.

Zusammengefasst ist Informations-management im Militär alles, was mit dem Erfassen, Verarbeiten, Verteilen, Schützen und Nutzen von Information zu tun hat – sowohl defensiv (eigene Informationssicherheit) als auch offensiv (gegnerische Informationen beeinflussen). Es reicht von IT-Infrastruktur über Nachrichtendienste bis hin zu Cyber- und Informationsoperationen und stellt eine wesentliche Voraussetzung zur Erreichung einer digitalen Souveränität von Streitkräften dar.

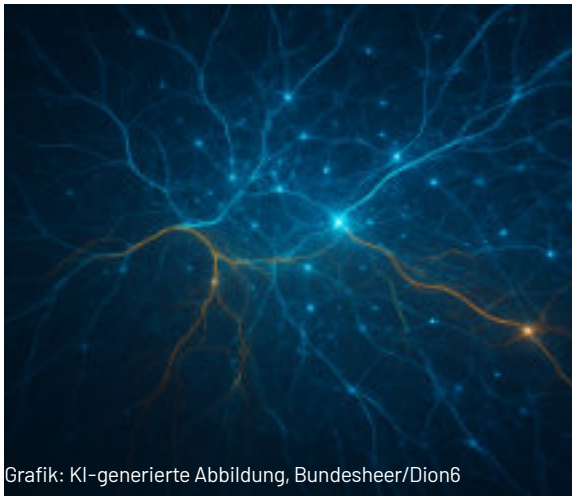
Zur Realisierung dieser Souveränität bedarf es nachfolgender vier Komponenten:

Datenhoheit und Datensicherheit

Streitkräfte müssen in der Lage sein, ihre taktischen, operativen und strategischen Daten zu schützen, zu speichern und zu analysieren, ohne auf (externe) Cloud-Dienste oder fremde Plattformen angewiesen zu sein.

Kontrolle über Technologien und Systeme

Eine Erreichung weitgehender Unabhängigkeit von fremden Technologien in Schlüsselbereichen wie Hardware, Software und Kommunikationsinfrastruktur ist anzustreben. In Fällen der diesbezüglichen Unmöglichkeit wäre zumindest eine eigene oder vertrauenswürdige Entwicklung und Wartung von Kommunikationssystemen (z. B. Funk oder Satellitenkommunikation), Führungsinformationssystemen, der dazugehörenden Sensorik und Waffensysteme mit IT-Komponenten und der eigenen Entwicklung und Anwendung künstlicher Intelligenz (und deren Datenmodellen sowie Algorithmen) anzustreben.



Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Besonders kritisch ist die Abhängigkeit von internationalen IT-Konzernen, etwa aus den USA oder China. Digitale Souveränität bedeutet, alternative Lösungen zu besitzen oder selbst entwickeln zu können – im besten Fall mit europäischen Partnern (im Zuge von z.B. EDA9-Projekten).

Cyberabwehr und Informationssicherheit

Die Erreichung und Erhaltung der Handlungsfähigkeit im Cyber- und Informationsraum ist die Fähigkeit, sich gegen Cyberangriffe, Sabotage und digitale Spionage zu verteidigen und gleichzeitig eigene Cyberoperationen durchzuführen. Dies umfasst auch den Schutz der eigenen Informationsressourcen gegen physische Spionage, Manipulation und Desinformation.

Interoperabilität und NATO- bzw. EU-Kompatibilität

Trotz Souveränität müssen Streitkräfte mit Partnernationen zusammenarbeiten können. Anzustreben ist eine Standardisierung und Kompatibilität, ohne Kontrollverlust über eigene Systeme. Das Ziel dabei ist die Erreichung einer Resilienz durch Redundanz und Interoperabilität innerhalb von NATO- und EU-Strukturen, ohne Abhängigkeit von einzelnen Akteuren. Digitale Souveränität darf nicht im Widerspruch zur Bündnisfähigkeit (NATO/EU) stehen – eine vernünftige Balance zwischen Eigenständigkeit und Integration ist nötig.

Digitale Souveränität ist für moderne Streitkräfte ein entscheidender Faktor zur Wahrung von Handlungsfreiheit, Resilienz und Einsatzfähigkeit. Sie bedeutet die Fähigkeit, Informationen, Datenflüsse und digitale Infrastrukturen unabhängig, sicher und kontrolliert zu beherrschen. Militärisches Informationsmanagement bildet dabei das Rückgrat; es stellt sicher, dass Informationen als Ressource zielgerichtet erfasst, verarbeitet, geschützt und für operative Entscheidungen nutzbar gemacht werden.

Aktuelle Bedrohungsanalysen führten national zu Überlegungen wie dem Aufbauplan 2032+, in welchem in naher Zukunft den Herausforderungen der hybriden Kriegsführung von wachsenden Sensor-Datenmengen und Cyber-Datenströmen, sowie regelmäßiger Cyber-Bedrohungen durch Systemanpassungen (Verwirklichung technologischer und systemimmanenter Fähigkeitsschritte, wie Adaptierung und Aufwuchs von Organisationsplänen) begegnet werden soll.

Eine Möglichkeit, diesen Herausforderungen gerecht zu werden, ist beispielsweise die Entwicklung eines Informations- und Kommunikationssystems für den Einsatz (IKTSysE) verbunden mit der Implementierung von ortsfesten und verlegbaren Einsatzrechenzentren (ofEReZ / vlgbEReZ). Dieses IKTSysE wird unsere Streitkräfte durch Resilienz gegenüber Ausfällen und Angriffen, Flexibilität beim Einsatz in unterschiedlichen Szenarien, Interoperabilität mit Partnernationen und Bündnisstrukturen, Autarkie bis zum Zeitpunkt der erforderlichen Synchronisation mit übergeordneten Systemen, Handlungsfreiheit durch jederzeit verfügbare, gesicherte Datenverarbeitung unterstützen und eine Erlangung von Führungs- und Informationsüberlegenheit begünstigen.

Im Rahmen unserer Kooperationen (DACH und FMN) wurden gemeinsam bereits wesentliche Voraussetzungen für die Realisierung solcher Fähigkeitsschritte erarbeitet und im Zuge unterschiedlichster Fachfortbildungen (wie beispielsweise dem Seminar Führungsunterstützung für Unteroffiziere an der Führungsunterstützungsschule) den künftigen Anwendern / Administratoren solcher Systeme zur Kenntnis gebracht.

Grafik: Bundesheer/Dion5


Foto: Bundesheer/Dion6

Zum Zwecke der Realisierung sind unter anderem die Schaffung ausbildungsmäßiger Voraussetzungen und umfangreiche Umstrukturierungs- und Beschaffungsvorgänge erforderlich. Diese wurden bereits erfolgreich angestoßen; diesbezügliche Informationsvorträge dazu bestätigen, dass ein direktionsübergreifendes Verständnis und Engagement hierzu besteht und weiterverfolgt wird.

Fazit

Militärisches Informationsmanagement ist ein Schlüsselfaktor für die digitale Souveränität moderner Streitkräfte. Die richtige Aufbereitung und Interpretation von Daten schafft ein konsolidiertes aktuelles Lagebild und versetzt den verantwortungstragendentragenden Kommandanten in die Lage, schnell und wirksam zu entscheiden (K-R-Z Kalkül).

Das im Aufbauplan 2032+ vorgesehene IKTSysE wird mit den Einsatzrechenzentren dazu beitragen, Informationsüberlegenheit auch in dynamischen Einsatzszenarien sicherzustellen. Innerhalb der Generaldirektion für Landesverteidigung (GDLV) erfolgen parallele Planungs- und Realisierungsschritte in Sinne einer direktionsübergreifenden Zusammenarbeit, um künftig sämtlichen IKT-Anforderungen der hybriden Kriegsführung in adäquater Ausprägung zu begegnen.

Architekturbearbeitungen

„Mit Architektur und internationaler Kooperation auf den Weg in die Zukunft“

Mit Umsetzung der Reform wurde 2025 innerhalb der Abteilung IKTCyPI das Referat Architektur geschaffen.

Der eingeteilte Referatsleiter wurde mit der Aufgabe betraut den Fähigkeitenbereich Architektur und Interoperabilität in der Abteilung aufzubauen.

Als erster Erfolg kann der Projektstart zur Einführung einer Enterprise Architektur im BMLV, (Kurztitel BEAM) verzeichnet werden. Architektur bedeutet die Vernetzung von Strategien, Prozessen, Technologien und Struktur, um Komplexität erfassbar und beherrschbar zu machen und agil auf neue Anforderungen reagieren und rasch adaptieren zu können.

Gemeinsam mit dem Projekt Team aus Mitarbeitern und Mitarbeiterinnen der IKTCyPI, IKTBstg&NuMngt sowie aus dem IKT&CySihZ werden in einer ersten (Ramp-up) Phase die Grundlagen und der Fahrplan für das Programm zur Umsetzung der nächsten Jahre festgelegt. Ziel ist es, Ebenen übergreifend die Architekturarbeit in der Planung, Entwicklung sowie Realisierung von Fähigkeiten zu etablieren und im BMLV zu verankern. Ein entscheidender Faktor hierfür sind die Erfahrungen aus bereits laufenden Projekten wie z.B. der Einführung des MTPz PANDUR EVO und dem Aufbau der Luftverteidigung, die aufgrund ihrer hohen Komplexität wertvolle Beiträge liefern.

Im Rahmen der Architektur und Digitalisierung kommen wesentliche Vorgaben und Rahmenwerke aus dem internationalen Umfeld. So ist das multinationale Programm „Federated Mission Networking (FMN)“ ein essentieller Treiber für die Interoperabilität zwischen unseren Teilstreitkräften. Das BMLV entsendet seine Experten und Expertinnen in unterschiedliche Arbeitsgruppen, um den internationalen Erfahrungsaustausch zu fördern und in den jeweiligen Gremien an den Spezifikationen mitzuwirken, die zur nationalen Umsetzung gelangen.
In der DACH-Kooperation Cyber werden in weiterer Folge gemeinsame interoperable, föderierte Fähigkeiten erarbeitet. Diese orientieren sich einerseits an FMN und anderseits an den DACH gemeinsamen Herausforderungen im Bereich der IKT, Cyber und EloKa. Sowohl die Beteiligung in FMN, als auch die DACH-Kooperation Cyber unterlaufen derzeit einen Umbruch, um Interoperabilität und internationale Zusammenarbeit stärker in unserer Organisation zu verankern und auf breitere Beine zu stellen.

Im Rahmen der Architektur und Digitalisierung kommen wesentliche Vorgaben und Rahmenwerke aus dem internationalen Umfeld. So ist das multinationale Programm „Federated Mission Networking (FMN)" ein essentieller Treiber für die Interoperabilität zwischen unseren Teilstreitkräften. Das BMLV entsendet seine Experten und Expertinnen in unterschiedliche Arbeitsgruppen, um den internationalen Erfahrungsaustausch zu fördern und in den jeweiligen Gremien an den Spezifikationen mitzuwirken, die zur nationalen Umsetzung gelangen. In der DACH-Kooperation Cyber werden in weiterer Folge gemeinsame interoperable, föderierte Fähigkeiten erarbeitet. Diese orientieren sich einerseits an FMN und anderseits an den DACH gemeinsamen Herausforderungen im Bereich der IKT, Cyber und EloKa. Sowohl die Beteiligung in FMN, als auch die DACH-Kooperation Cyber unterlaufen derzeit einen Umbruch, um Interoperabilität und internationale Zusammenarbeit stärker in unserer Organisation zu verankern und auf breitere Beine zu stellen.

Cyber

Kooperation CCDCoE und MoD ESTLAND:

Als zweckmäßig erwies sich die Teilnahme an der Conference on Cyber Conflicts (CYCON) in TALLINN/EST und als nationaler Vertreter bei den Steering Committees des Cooperative Cyber Defence Center 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: CCDCoE

Keynotes des Dir CCDCoE und des Präsidenten Estlands verstärken die Bedeutung der Cyber-Angriffe auf supply chains (amplification) sowie in Cloud Architekturen (ohne Segmentierung). Dies resultiert im steigenden Bedarf an humananalytischer Analyse in komplexer werdender Security Operation Cell (SOC)-Architektur. SOC-Tools mit Artificial Intelligence (AI)-basierter Technologie müssen die Reaktion darauf werden, um zeitgerechte Reaktionen auf erkannte und ausgenutzte Vulnerabilities zu ermöglichen. Dieser sicherheitshollistische Ansatz, Platformization of AI driven resilience, wird in der NATO-FMN Zero Trust-Architektur verfolgt:

Die Teilnahme des ÖBH am Übungsvorhaben Locked Shields im Mai 2025, unter Leitung des CCDCoE, wurde ff durch IKTCyE gesteuert und erstmalig in einer Stabsorganisation über den technischen Bedarf eines Blue-Teams hinweg mit strategischen und legistischen Analysen zur operativen Führung mit erweiterten Lagebildanteilen befähigt. Im Strategic Track wurden mit Unterstützung durch Direktion 6 - IKT und Cyber, Generaldirektion Verteidigungspolitik (GDVPol) und Vertretern des Bundesministeriums für Inneres (BMI) ansatzweise gesamtstaatliche Auswirkungen und Beratungleistungen der Übungsleitung eingebracht.

Für das BMLV bedeutend ist die Kooperation, um Erkenntnisse in die Fähigkeitsentwicklung der Cyber-Truppe für das ÖBH und in Zusammenwirken mit EU sowie NATO einfließen lassen zu können. Dazu ist es wertvoll bei Strukturreformmaßnahmen des CCDCoE, bei Entwicklungsbedarfen der Nationen (im Program of Work) bei den dazu nötigen Abstimmungen zu gültigen Vertragsgrundlagen mit CCDCoE und MoD Estland und Übungsvorhaben aktiv mitzuwirken.

Fähigkeitsentwicklung Cyber-Truppe

Umsetzungsmaßnahmen finden sich in der Planung zur Fähigkeitenentwicklung der Cyber-Truppe in Abstimmung mit dem Zielbild ÖBH2032:

- Die Planungsgrundlagen aus dem Motivenbericht Cyber-Truppe sind mit Realisierungsansätzen in den Entwicklungslinien beim Fähigkeitenworkshop der Cyber-Kräfte dargestellt worden.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

- Szenarienbasiert für einen möglichen Einsatz der Cyber-Truppe wurde beim Wargame Fühungsüberlegenheit der verfahrensmäßige Bedarf zur Unterstützung mit Wirkmitteln im Cyber-Raum eingebracht.

- Die spezifische Weiterentwicklung von IKT-Sicherheitstechnischen Realisierungsmaßnahmen ist in der Vorhabensabsicht Informationssicherheitsmanangementsystem des BMLV und ÖBH beschrieben worden.

- Umsetzungsmaßnahmen iZm mit den zuständigen Fachabteilungen Org und IKTS für die nötige SOC-Fähigkeit und die Cyber Range wurden mit einer Strukturerweiterung des MilCyZ und ausrüstungsmäßiger Beschaffung von Sicherheitstools bzw. Hardware erreicht.

Grafik: Bundesheer/Dion6

„Ohne Verbindung keine Führung – stets gültig“

In den vergangenen Jahren ist das IKT-System des Bundesheer unter anderem im Bereich der verlegbaren IKT-Infrastruktur modernisiert worden. Verbindungsmittel die hohe Bandbreiten ermöglichen wurden flächendeckend in Form des Tactical Communication Network (TCN) der Truppe zugeführt, um eine ununterbrochene Führungsfähigkeit des ÖBH zu ermöglichen. Im Zuge mehrerer Großübungen in den letzten Monaten konnte die Einsatztauglichkeit des TCN wiederholt unter Beweis gestellt werden. Somit konnte ein weiterer Meilenstein auf dem Weg zu einer breitbandigen Datenkommunikation auf allen Ebenen erreicht werden. Dies konnte durch hohes Engagement von Experten aus diversen Dienststellen aus dem beschaffenden, bereitstellenden und technischen Bereich bewerkstelligt werden. Mit der gerade beginnenden Auslieferung des Soldatenfunkgerätes an die Truppe erreicht die digitale Kommunikation auch die unterste taktische Ebene, die Gruppe. Dennoch gibt es noch Verbesserungspotential im Bereich breitbandige Datenkommunikation im mobilen Bereich. Mit der beginnenden Einführung eines Datenfunkgerätes (TDR), interoperabel mit europäischen Funksystemen durch die Nutzung der europäischen Wellenform ESSOR, wird diese Lücke in den nächsten Jahren geschlossen. Mit dem TCN und dem TDR wird schlussendlich die breitbandige Datenkommunikation von Gefechtsstand bis auf Ebene Gruppe sichergestellt.

Wargame Führungsüberlegenheit

Im Juli 2025 fand in Salzburg das Wargame Führungsüberlegenheit (WG FüÜlg) statt. Es fügte sich in eine Reihe von verschiedenen Wargames auf strategischer Ebene zum Bewerten einer Basisfähigkeit anhand eines fiktiven Zukunftsszenarios. Dabei sollten vor allem die bisher erarbeiteten Grundlagen zur Umsetzung des Zielbildes ÖBH2032+ in den Bereichen Führungsunterstützung (FüU), elektromagnetische Kampfführung (EloKa), Kampfführung im Cyberraum und die Services im Weltraum überprüft und vertieft werden. Der Fokus der Betrachtung lag auf dem Führungs-, ISTAR-, Wirkungs- und Unterstützungsverbund (FIWU) des mobilgemachten ÖBH2032+ auf der strategischen Ebene bis zur Brigade/Bataillon. Ergänzt wurde das Wargame durch die Vorstellung des IKT-Systems Einsatz sowie einer Leistungsschau der IKT- und Cyber-Systeme. Das Schwergewicht der Bearbeitungen lag auf der Berücksichtigung der FüU-Struktur inkl. der IT-Provider/Rechenzentren (ReZ) sowie des Joint Fire Support (JFS), der Luftverteidigung, des ISTAR-Verbundes, der EloKa sowie der Domänen Cyber- und Weltraum jeweils basierend auf dem Zielbild ÖBH2032+.

Insgesamt wurden drei Arbeitspakete bearbeitet, wobei die Grundlagen und die Ausgangslage vorgestaffelt verteilt wurden.

- Lagebild und Ersteinsatz der Führungsunterstützung im mobilgemachten Bundesheer – SG ist der Führungsverbund,
- Lagefortsetzung – SG ist der ISTAR-Verbund.
- 2. Lagefortsetzung – SG ist der Wirkungs- & Unterstützungsverbund.

In einem abschließenden Arbeitspaket erfolgt die Präsentation der Ergebnisse an den Chef des Generalstabes inklusive Folgerungen und weiterführender Maßnahmen. Die erarbeiteten Antworten auf die Frage „Ist die derzeit geplante Führungsunterstützung in der Lage, das mobilgemachte ÖBH2032 in der Militärischen Landesverteidigung zu unterstützen?“ führten zum Erkennen des Anpassungsbedarfs und zu Ableitungen von weiterführenden Maßnahmen im Bereich der FüU, EloKa, Cy, IT-Provider und Space Services für alle beteiligten Organisationseinheiten und darüber hinaus für das Schaffen der erforderlichen Rahmenbedingungen.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Die Umsetzung dieser Maßnahmen erfolgt nun in einem weiteren Schritt im Zusammenwirken der beteiligten Dienststellen und Organisationseinheiten.

EloKa - Neue Mittel für das ÖBH

Die aktuellen Entwicklungen in den Krisengebieten weltweit zeigen deutlich, wie sich das Gefechtsfeld der Gegenwart entwickelt hat. Die elektromagnetische Kampfführung – sei es in Form von Steuersignalen von Drohnen oder die Übermittlung von Videosignalen direkt von der Front über unterschiedlichste Verbindungsmittel an die Bedarfsträger – gewinnt mehr und mehr an Wichtigkeit und rückt damit zunehmend in das Interesse von modernen Armeen.

Um diesem Umstand Rechnung zu tragen wird im Zuge des Aufbauplans ÖBH 2032+ die Truppe mit modernsten Mitteln ausgerüstet.

Die Beschaffungen von hochwertigen Erfassungssystemen sowie leistungsfähigen Störsystemen wird vorangetrieben, um diese so rasch als möglich der Truppe zuzuführen. Die Fähigkeiten des ÖBH das Elektromagnetische Spektrum bestmöglich ausnützen zu können geht aber weit über die Beschaffung von technischen Komponenten hinaus. Vielmehr muss in den kommenden Monaten und Jahren das Bewusstsein geschaffen werden, dass die Waffengattung EloKa alle anderen Domänen durchdringt – nicht nur bildlich gesprochen.

IT-Informations-Freiheits-Gesetz-Service (IFG-Service)

Mit Wirkung vom 01.09.2025 trat das „Informations Freiheits Gesetz" (IFG) in Kraft. Das IFG sieht einerseits die Möglichkeit des Bürgers mittels Anfrage zu konkreten Informationen der Verwaltung zu kommen und andererseits die proaktive Veröffentlichung von Verwaltungsvorgängen vor.

Damit war der Bedarf im Ressort gegeben ein Werkzeug zur Unterstützung der Verwaltung, konkret des Referates Bürgerservice des BMLV, bei der proaktiven Freigabe von Informationen (Erlässe, Verträge, etc.) zu planen.

Das IFG-Service konnte innerhalb kurzer Zeit mittels strukturierter Erhebung der Anforderungen der Bedarfsträger durch IKTCyPI und der Umsetzung sowie Programmierung durch das IKT&CySihZ, konzipiert und bereitgestellt werden.

Die, mittels des sogenannten IFG-Service, freigegebenen Informationen werden auf der IFG-Plattform des Bundesrechenzentrums bereitgestellt.

Grafik: IFG-Service, Bundesheer/Dion6

„Datennetz der Medizin" (DaMe)

Aufgrund der Novellierung des Gesundheitstelematikgesetzes 2025 bestand der Bedarf bei all jenen militärmedizinischen Stellen und Stellungshäusern, welche einen Austausch von Patientendaten und Befundungen mit zivilen Ärzten haben, diesen neu auszuplanen. Bis dato erfolgte die Übertragung von Patientendaten und Befundungen mittel FAX oder am Postweg. Die Verwendung von FAX-Geräten zur Übertragung dieser Daten wurde mittels oben angeführten Gesetz mit 01.01.2025 verboten. Daher ist dringlich eine adäquate elektronische Übertragungsmöglichkeit im Sinne der Sicherstellung der Vorgaben der Datenschutzgrundverordnung (DSGVO) sicherzustellen. Nach Durchführung der Erhebung der Bedarfe durch IKTCyPI in Zusammenarbeit mit dem IKT&CySihZ und den Bedarfsträgern der Direktion 8, konnte für die sichere verschlüsselte Übertragung der Patientendaten und Befundungen eine zivile Lösung gefunden werden. Diese wird nach Einkauf in die bestehenden Prozesse implementiert.

„He(e)r mit Geschichte"

H(e)er mit Geschichte ist ein Kooperationsprojekt zwischen dem BMLV und dem Austrian Centre for Digital Humanities and Cultural Heritage (ACDH-CH). Das Ziel des Vorhabens ist die systematische Erfassung, Kontextualisierung und Beforschung von militärhistorischen und kulturwissenschaftlich relevanten Ereignissen und zugehörigen Jubiläen bzw. Gedenktagen sowie die Bereitstellung der Forschungsdaten und -ergebnissen. Neben der Nutzung durch das BMLV bzw. andere Einrichtungen der öffentlichen Verwaltung, sollen die Daten insbesondere für Forschungsvorhaben zum Kulturerbe Österreichs verwendbar sein sowie zur Information für die interessierte Öffentlichkeit dienen.

IKTCyPI hat bei diesem Vorhaben ebenfalls bei der Erhebung der Anforderungen der Abteilung Zielgruppenkommunikation unterstützt und die Realisierung durch das IKT&CySihZ veranlasst. Aufgrund der Mitarbeit der Planungsabteilung vom Beginn des Projekts wird dieses innerhalb kürzester Zeit zur Zufriedenheit aller Beteiligten realisiert werden.

IKT Cybereinsatz

Leiter IKTCyE: Bgdr Mag. Arnold STAUDACHER


Foto: BMLV/HBF

Die Abteilung IKTCyE wirkt auf der operativen Ebene an der Schnittstelle zwischen den einsatzverantwortlichen Direktionen 1 und 2 und den eigenen Verbänden und Dienststellen und sorgt sowohl für die Sicherstellung der jeweiligen Bedarfe als auch für die fachliche Weiterentwicklung der Kompetenzen in den Waffengattungen der Direktion 6. Dabei kann wiederum auf ein arbeitsintensives Jahr 2025 zurückgeblickt werden. Neben den substantiellen Beiträgen bei den In- und Auslandseinsätzen konnten über 30 nationale und multinationale Übungen und Vorhaben bewältigt werden.

Folgende Vorhaben bildeten das Schwergewicht:

Alle 3 großen Auslandskontingente KFOR, EUFOR ALTHEA und UNIFIL wurden auf das neue Tactical Communication Network umgerüstet. Dieses erhielt ein wesentliches Software - Upgrade, welches in einer großen IKT Betriebsübung auf dessen Einsatztauglichkeit überprüft wurde. Mit diesen Maßnahmen konnte die Systemeinführung bei der Truppe, welche ein Arbeitsschwergewicht der letzten Jahre war, erfolgreich zum Abschluss gebracht werden.

Die Beschäftigung mit den Herausforderungen der „Hybriden Bedrohungen" und der „Abwehr von Drohnen" wurde bei der Multinationalen Cyberverteidigungsübung „Locked Shields 25" (gemeinsam mit den Niederlanden (NLD) und der US National Guard Vermont) bzw. bei der EloKa D-A-CH Übung „Alpine Jam 25" intensiviert. Ebenfalls gemeinsam mit unseren Nachbarn wurde erstmalig bei der D-A-CH Übung „Common Roof 25" das in Einführung befindliche Führungsinformationssystem HeadQuarter „SITAWARE" erprobt.

Die Fähigkeit des ÖBH zur „Black Out" Notkommunikation konnte durch die Ausrollung von modernen SAT Telefonen auf alle Kasernen und Liegenschaften sowie durch Ausstattung der Militärkommanden mit dem neuen Kurzwellengerät „FALCON III" wesentlich verbessert werden.

Die Beteiligung an den Wargames „Mobilmachung", „Führungsunterstützung" und „Luftverteidigung" sowie am Vorhaben „FHQ" brachten wertvolle Erkenntnisse für die Umsetzung des Aufbauplanes ÖBH2032+ im eigenen Bereich.

FüU/IKT Auslandskontingente

Auch 2025 galt es primär, die Herausforderung der Aufbringung des benötigten Fachpersonals für die Auslandskontingente AUTCON/UNIFIL, AUTCON/KFOR und AUTCON EUFOR/ALTHEA zu bewältigen.

Wie schon 2024, war das AUTCON/UNIFIL im Libanon stark von der äußerst angespannten Sicherheitslage und der Herausforderung der häufig ausfallenden bzw. verschobenen Folgeversorgungen beeinflusst. Trotz dieser herausfordernden Umfeldbedingungen ist es gelungen, die TCN-Umstellung plangemäß durchzuziehen und somit das PACE-Konzept für dieses Kontingent vollständig umzusetzen.

Zusätzlich wurde die Qualität der Sozialkommunikation des AUT WLAN im Camp Naqoura, durch Maßnahmen im Bereich der IKT Sicherheit sowie durch die Verdichtung und Erweiterung des Empfangsbereichs wesentlich verbessert. Für AUTCON EUFOR/ALTHEA wurden Mobile Device Management (MDM) Lizenzen beschafft, um Erfahrungswerte bei der IT-mäßigen Verwaltung der national beschafften Mobiltelefone zu sammeln. Auf Grund des äußerst positiven Feedbacks wird diese Anwendung nun auch für das AUTCON/KFOR vorgesehen.

Durch die Schaffung eines IKT-Gerätepools bei der Auslandseinsatzbasis können ab 2025 nun erstmals alle österreichischen Kontingente und bei Bedarf auch Einzelpersonen sowie Ausbildungspersonal rasch und unkompliziert mit der erforderlichen IKT Ausstattung des ÖBH versorgt werden. Darauf aufbauend wurden alle Missionen im BMLV ELAK abgebildet und einheitliche HCL-Notes sowie E-Mail-Adressen zugordnet.

TCN-Umstellungen im Ausland

Das absolute Schwergewicht bei den Auslandseinsätzen lag im Jahr 2025 in der technischen Umstellung der 3 großen Auslandsmissionen AUTCON/EUFOR/ALTHEA, AUTCON/UNIFIL und AUTCON/KFOR von der Integrierte Fernmeldeinfrastruktur (IFMIN) auf das moderne Tactical Communication Network (TCN). Mit dieser Umstellung wurde die veraltete IFMIN-Infrastruktur, welche über 35 Jahre in Betrieb war, sowohl im In- als auch im Ausland außer Dienst gestellt.

Foto: Bundesheer/Dion6

Beteiligte Einheiten und Personal

An der Umstellung waren insgesamt 20 Soldaten und Zivilbedienstete aus folgenden Einheiten beteiligt:

- IKT Cybereinsatz (IKTCyE)
- IKT-Betrieb (IKTBetr)
- Militärisches Cyberzentrum (MilCyZ)
- Führungsunterstützungsbataillon 1 (FüUB1)
- Kommando 7. Jägerbrigade (Kdo7.JgBrig)
- Stabsbataillon 7 (StbB7)
- Heereslogistikzentrum Graz (HLogZ G)
- Radarbataillon (RadB)

Herausforderungen

Die Umstellung stellte unerwartete Herausforderungen dar, da die veraltete, teils Jahrzehnte alte ortsfeste Verkabelung in den Camps weiterhin genutzt werden musste. Da ein solcher Einsatz von TCN zuvor nicht getestet worden war, mussten die Teams flexibel reagieren und Lösungen vor Ort entwickeln. Die dabei gewonnenen Erfahrungen sind von großem Wert für zukünftige Einsätze und Übungen des Österreichischen Bundesheeres (ÖBH).

Durchführung und Bedingungen

Trotz schwieriger Bedingungen wurde die Umstellung planmäßig und zur vollsten Zufriedenheit der Nutzer durchgeführt.

Um die Kontingente möglichst wenig zu behindern, fanden die Arbeiten unter Zeitdruck über Wochenenden und oft bis spät in die Nacht statt. In einigen Fällen mussten die Teams bei Temperaturen von bis zu 40°C arbeiten.

Vorteile der TCN-Umstellung

Die Umstellung auf TCN stellt nun eine moderne digitale IKT Anbindung nach Österreich mit folgenden wesentlichen Vorteilen sicher:

- Erhöhte Bandbreite: Die Bandbreite für die Rückwärtsverbindung nach Österreich wurde um das 3-fache gesteigert.
- Moderne Telefonie: Jeder SMN-Teilnehmer kann nun via Softphone telefonieren - eine deutliche Verbesserung der Kommunikationsmöglichkeiten.
- Zukunftsfähigkeit: Die Implementierung bildet die Grundlage für die Verwendung zukünftiger Anwendungen wie FüIS HQ oder BMS Frontline, welche zZt. in Beschaffung sind.

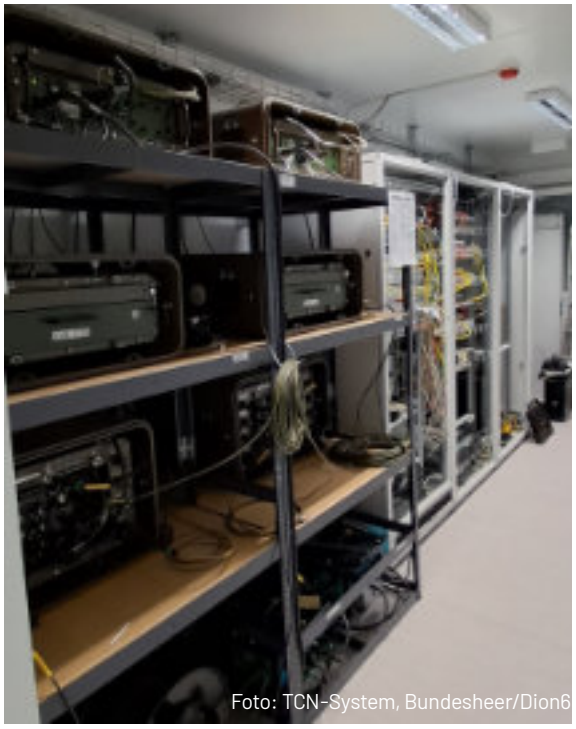


Foto: TCN-System, Bundesheer/Dion6

Foto: TCN-System, Bundesheer/Dion6

Fazit

Die TCN-Umstellung bei den Auslandsmissionen war ein wichtiger Schritt zur Modernisierung der Kommunikationsinfrastruktur des ÖBH. Trotz einiger unerwarteter Herausforderungen wurde das Projekt erfolgreich und planmäßig abgeschlossen. Die Umstellung bringt nicht nur eine Modernisierung, sondern ist zugleich auch ein wichtiger Baustein für die Digitalisierung.

TCN-Systemtestung

In der 41. und 42. Kalenderwoche 2025 wurde das System Tactical Communication Network (TCN) einem technischen Belastungstest unterzogen.

Das System TCN befand sich bis Ende des Jahres 2025 in der Einführungsphase. Um einen ordnungsgemäßen Übergang in die Nutzungsphase 2026 sicherstellen zu können war es notwendig, das Netzwerk einer Testung unter maximaler Auslastung zu unterziehen.

Die Notwendigkeit wurde nochmals durch die Tatsache verstärkt, dass Ende August das, durch die Vertragsfirma bereitgestellte, sogenannte Update 3A durchzuführen war. Dieses Update beinhaltet neben Neuerungen im Routing auch einige neue Funktionalitäten, die zu überprüfen waren.

Die Gesamtleitung wurde durch die Abteilung IKTCyE übernommen. Die technische Testleitung wurde durch das IKTCySihZ / IKTTe wahrgenommen. Unterstützt wurde dabei durch die Bereiche IKT-Betrieb und Applikationen.

Das bedeutete, dass ein Drehbuch mit einem Umfang von ca. 250 Seiten zu erstellen war. Die verwendete Testmatrix umfasste ca. 20.000 Datensätze zur zeitlichen Koordinierung des Ablaufes der 100 Techniktests auf den eingebundenen Vermittlungseinheiten. In der Nestumgebung wurden über 100 taktische Router über verschiedenste Einbindungs- und Verbindungsmöglichkeiten in einem österreichweiten Netz zusammengefasst. Über 250 Personen sorgten für einen möglichste reibungslosen Testbetrieb.

Um die Steuerung der einzelnen Vorhaben bestmöglich koordinieren zu können wurden 6 Teilnetze gebildet. Die Hauptstandorte bildeten die Teilnetze Linz/Hörsching (Platz der Testleitung, Kommando Luftunterstützung (Kdo LuU) und 4. Panzergenadierbrigade (4.PzGrenBrig) und Klagenfurt/Villach (7.JgBrig und FüUB1).

Die weiteren Netze wurden in Mautern (3.JgBrig), Absam (6.GebBrig), Zeltweg (LRÜ) und St. Johann im Pongau (FüUB2) betrieben. Weitere Standorte waren mit einzelnen Systemen eingebunden.

Herstellerseitig wurde das Vorhaben durch Vertreter der Firma CANCOM unterstützt. Die Entwicklerfirma BITTIUM reiste aus Finnland an um mit der Expertise ihrer Mitarbeiterinnen und Mitarbeiter zur Seite zu stehen.

Das System TCN konnte grundsätzlich alle geforderten Anforderungen erfüllen. Geringfügige Arbeiten sind dennoch notwendig und werden in nächster Zeit realisiert.

Die Systemtestung war gekennzeichnet durch hohes Engagement auf allen Ebenen. Ohne die gezeigte Performance des eingesetzten Personals wäre ein derart herausforderndes Vorhaben nicht realisierbar.

Zusammenfassend ist aus Sicht der Gesamtleitung festzuhalten, dass einem Übergang in die Nutzungsphase nichts im Wege steht.

Foto: TCN-Systemtestung, Bundesheer/Dion6

Notkommunikationsübung - Effektive Einsatzbereitschaft sichern!

2025 fand unter Federführung des Referates Informationsübertragung (InfoÜ) der Abteilung IKTCyE im Frühjahr erneut eine Notkommunikationsübung statt.

Das angenommene Übungsszenario war ein großflächiger Stromausfall in Europa (Blackout).

Eine reale Gefahr, wie der Vorfall in Spanien und Portugal gezeigt hat. Am 28. April 2025 gingen in Spanien und Portugal die Lichter aus. 18 Stunden sollte es dauern, bis die Stromversorgung auf der Iberischen Halbinsel wiederhergestellt war. Dabei fiel die öffentliche elektrische Energieversorgung komplett aus und konnte erst in mehreren Stufen wiederhergestellt werden. Die Ursachen: Netzüberlastung, fehlende Reserven und technische Schwächen – ein Warnsignal für ganz Europa, das dafür sorgen muss, dass das Licht nicht ausgeht. Die „Störung" war im europäischen Verbund die größte Störung seit mehr als 20 Jahren. Das Blackout in Spanien zeigt: „Systemstabilität ist eine wachsende Herausforderung"

Foto: Einlagensteuerung, Bundesheer/Dion6

Foto: Funk-Pinzgauer FüUS, Bundesheer/Dion6

Die zunehmende Komplexität des Europäischen Verbundnetzes durch fortschreitende Digitalisierung, durch extreme meteorologische Lagen infolge des Klimawandels, sowie durch gesellschaftliche Bedrohungen wie Cyberattacken und Terrorismus erhöhen die Wahrscheinlichkeit eines Blackouts. Umso wichtiger ist daher die Vorbereitung und praktische Erprobung einer Notkommunikation.

Über Hundert Experten im Bereich der Kurzwelle (KW) und Ultrakurzwelle (UKW) errichteten und betrieben österreichweite, autarke und datenfunktionsfähige Führungsnetze unter Einbindung der Verbände und Dienststellen der Direktionen. Die vorhandenen Abläufe und festgelegten Prozesse zur Sicherstellung einer permanenten Kommunikation bei Katastrophenfällen, wie einem mehrtägigen großflächigen Stromausfall, werden dabei überprüft und evaluiert. Die Autarkie der Stromversorgung für die führenden Kommanden und die Funktrupps erhält dabei besondere Bedeutung.

Durch die gebildete Einlagensteuerung, bestehend aus Vertretern der Abteilung IKTCyE und der IKT-Truppe, wurden nach einem vorbereiteten Drehbuch während der Übung mehr als 200 Meldungen bzw. Sprüche abgesetzt, davon konnten 94% ordnungsgemäß übertragen und bearbeitet werden.

Es konnten erneut wertvolle Erkenntnisse für die Gewährleistung einer stabilen Notkommunikation für das Österreichische Bundesheer (ÖBH) gewonnen werden.

DACH Rahmenübung COMMON ROOF 2025

Im Zeitraum vom 06.10.2025 bis 17.10.2025 fand im Rahmen der DACH-Kooperation „Digitalisierung" die trinationale Übung COMMON ROOF 2025 (CR25) statt.

Grafik: Common Roof

Diese Übung zielte im Wesentlichen auf die Interoperabilität innerhalb der D-A-CH Nationen ab und das Schwergewicht lag in der Bereitstellung und dem Betrieb von IT-Einsatzservices in einem Einsatznetzwerk. Die Übung CR25 bezweckte einerseits die Umsetzung der Fähigkeitsziele gem. der IKT- und Digitalisierungsstrategie und schaffte anderseits die Voraussetzungen zur Verbesserung der Zusammenarbeits- und Führungsfähigkeit militärischer Stäbe in Kommanden bei grenzüberschreitenden Einsätzen.

Das taktische Übungsszenario handelte in einem fiktiven Kontinent unter Berücksichtigung mehrerer fiktiver Staaten und Bündnisse. Die Brigade AUT wurde im Rahmen der militärischen Landesverteidigung eingesetzt.

Die Einsatzführung erfolgte in einem taktischen HQ im Führungsinformationssystem (FüIS) „SitaWare", welches durch das Kommando Cyber der Schweizer Armee für Österreich bereitgestellt wurde. Aufgrund der Tatsache, dass das FüIS im ÖBH erst in Einführung ist, konnten für ein multinationales Einsatzszenario bereits schon Erfahrungen gesammelt werden.

Zielsetzung Digitalisierung:

- Die Führungsaufgaben in einem Brigadestab werden mit Führungsinformationssystemen wahrgenommen.
- Die Führungsüberlegenheit wird durch die Verfügbarkeit von zeitverzugslosen und medienbruchfreien digitalen Lagebildern erreicht.
- Das digitale Lagebild wird mit Nachbarn und anderen einsatzrelevanten Akteuren ausgetauscht und die taktischen Entscheidungsfindungsprozesse sind untereinander abgestimmt.

Dabei wird der Operateur im Sinne der Digitalisierung im Zusammenwirken mit der IKT sensibilisiert.

Zielsetzung FüU-Truppe:

- Der FüU-Einsatz ist in enger Abstimmung mit den jeweiligen taktischen Bedürfnissen geplant und die hierzu erforderlichen Planungsdokumente sind erstellt und verfügbar.
- Eine serviceorientierte Betriebsführung gewährleistet die vernetzte Einsatzführung von digitalisierten Streitkräften.
- Standardisierte Verfahren für den Betrieb von gemeinsamen militärischen Führungsnetzwerken sowie das Informations- und Wissensmanagement sind am Gefechtsstand implementiert und werden bei der Übung weiterentwickelt.

Die Erkenntnisse aus den Übungen fließen sowohl in die Anpassung und Weiterentwicklung der Führungsprozesse als auch in die Fähigkeitsentwicklung der Führungsunterstützungstruppe in allen Entwicklungslinien (Vorschriften, Pers. und Mat. Struktur/Organisation, Ausbildung und Infrastruktur) ein.

Es waren an der digitalen Einsatzführung des Brigadestabes aus der Schwarzenberg-kaserne in Wals insgesamt 35 Übungsteilnehmer beteiligt. Die Übung wurde erfolgreich durchgeführt und hat gezeigt, dass die Digitalisierung der Führungsaufgaben im Brigadestab einen wesentlichen Beitrag zur Effizienz und Effektivität leistet. Das ist die Grundvoraussetzung für die Sicherstellung der Führungsüberlegenheit in einem Einsatzstab.


Foto: Einsatzführung, Bundesheer/Dion6

Grafik: Locked Shields

Locked Shields 2025 – 15 Jahre der weltweit größten Cyberabwehrübung

Im Mai 2025 fand die Locked Shields 2025 statt, die größte und anspruchsvollste Live-Cyber-Verteidigungsübung der Welt. Ausgerichtet vom Cooperative Cyber Defence Centre of Excellence (CCDCOE), brachte diese Übung über 4.000 Teilnehmerinnen und Teilnehmer aus 41 Nationen zusammen. Gleichzeitig feierte sie ihr 15-jähriges Jubiläum als einzigartiges Trainingsformat.

Die Vorbereitung umfasste den Aufbau der IT-Infrastruktur, das Kennenlernen der zu schützenden Systeme sowie die Integration von Experten aus verschiedenen Ländern sowie zivilen Partnern.

Die Teilnehmer mussten unter hohem Zeitdruck nicht nur technische, sondern auch strategische Entscheidungen treffen. Diese beinhalteten rechtliche, kommunikative und politische Aspekte – Fähigkeiten, die in realen Krisensituationen entscheidend waren. Der Fokus lag auf dem Schutz kritischer Infrastrukturen, der Verfügbarkeit militärischer Systeme und der strategischen Entscheidungsfindung unter realistischen Krisenbedingungen.

Foto: Locked Shields Arbeitsplätze, BMLV/HBF

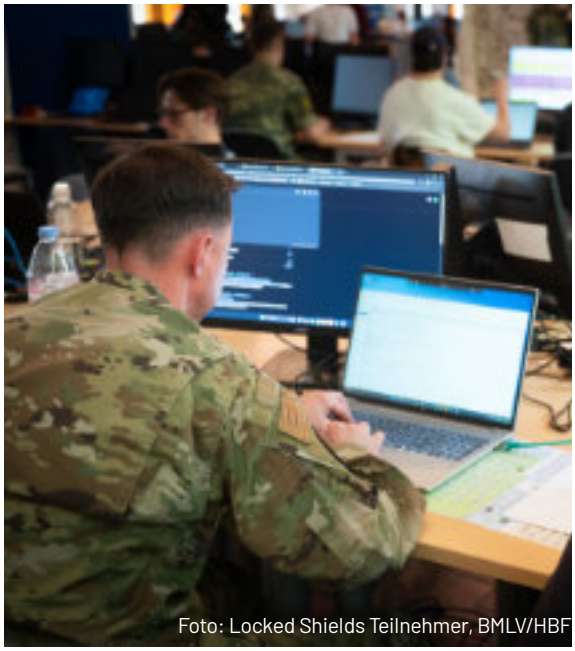


Foto: Locked Shields Teilnehmer, BMLV/HBF

Die Übung konzentrierte sich auf lebenswichtige Dienste wie Stromversorgung, Wasser und 5G-Infrastruktur sowie militärische Systeme, etwa für Luftverteidigung oder taktische Kommunikation. Die Szenarien waren an aktuellen geopolitischen Herausforderungen angelehnt. Die Locked Shields bot eine realistische Umgebung, in der nationale und internationale Cyberverteidigungsteams (Blue Teams) zivile und militärische IT-Systeme sowie kritische Infrastrukturen vor intensiven Cyberangriffen schützten. Insgesamt waren über 8.000 virtualisierte Systeme mehr als 8.000 Angriffen ausgesetzt.

Österreich nahm mit einem hochqualifizierten Team teil. Neben den heereseigenen Cyber- und Informationsspezialisten gehörten hierzu Cyberexperten aus den Niederlanden und der National Guard Vermont (USA). Ebenso verstärkten Spezialisten aus der kritischen Infrastruktur das über 100 Personen starke multinationalen Blue Team in Österreich.

Die Locked Shields 2025 unterstrich die Bedeutung internationaler Zusammenarbeit in der Cyberabwehr und zeigte Österreichs aktiven Beitrag zur Stärkung der europäischen und globalen Cyberresilienz.

D-A-CH EloKa Übung ALPINE JAM 2025

Ungewöhnliche Ruhe herrschte von 4. bis 14. August 2025 auf dem Truppenübungsplatz Hochfilzen. Grund dafür war nicht etwa eine vermeintliche Sommerpause auf dem Schieß- und Übungsplatz, vielmehr wurden die Einrichtungen für eine weitgehend geräuscharme Übung zum Thema „Kampf im elektromagnetischen Spektrum" genutzt.

Auf Einladung und unter Übungsverantwortung der Abteilung IKTCyE trafen sich Techniker und EloKa-Fachpersonal des Bundesheeres sowie aus Deutschland und der Schweiz zur D-A-CH Übung Alpine Jam 25. Zweck des Vorhabens war die Überprüfung der Wirksamkeit von CREW-Systemen („Jammer") gegen funkferngezündete Sprengfallen (RCIED – Radio Controlled Improvised Explosive Devices) sowie gegen Mini- und Microdrohnen mit dem Ziel, die Systeme an die aktuellen Bedrohungsszenarien anzupassen und somit die Effektivität zu optimieren.

Die durch die drei DACH-Nationen bei dieser Übung eingesetzten unterschiedlichen Störsysteme mussten dabei auf zwei genormten Teststrecken ihre Wirksamkeit gegen mehr als 20 verschieden Drohnentypen sowie ca. 30 unterschiedliche RCIED-Auslöseeinrichtungen unter Beweis stellen.

Foto: ALPINE JAM 2025, Bundesheer/Dion6

Der Signalerfassung und die Vermessung mit unterschiedlichen Messmittel - einschließlich des ERFOS-Systeme – sowie der präzisen Dokumentation der Ergebnisse kommen bei derartigen Übungsvorhaben entscheidende Bedeutung zu.

Das Fundament für den Erfolg solcher Vorhaben bildet die jahrelange bewährte Zusammenarbeit mit den DACH-Partnern im Fachbereich „Elektromagnetische Kampfführung".


Foto: ALPINE JAM 2025 DV-Day, Bundesheer/Dion6

Diese Partnerschaft basiert auf gegenseitigem Vertrauen sowie Offenheit und ist von der Überzeugung geprägt, dass der Schutz der eigenen Soldaten die oberste Prämisse des eigenen Handelns darstellt und diese gemeinsamen Anstrengungen rechtfertigt.

Zuletzt erbringt diese Übung auch den Beweis, dass der Joint-Gedanke die eigenen Bemühungen trägt und die Planung sowie Durchführung einer Übung über die Grenzen von Direktionen hinweg möglich ist. Neben der Eloka-Kompanie (EloKaKp) des FüUB2, welche die Hauptlast der Übungsdurchführung zu tragen hatte, und dem Unterstützungselement-EloKa (UZEloKa) unterstützten Dienststellen aus den Direktionen 1, 2 und 4 (StbB7, JgB8, Luftaufklärung, HLogZ WIEN) sowie – als Zeichen der bewährten interministeriellen Zusammenarbeit – auch Vertreter der Fernmeldebehörde das Vorhaben. Letztendlich war eine erfolgreiche Übung nur durch gemeinsame Bemühungen sicherzustellen.

Und nach dem Motto des Abteilungsleiters IKTCyE „Tue Gutes und sprich darüber" wurden zahlreichen wesentlichen Entscheidungsträgern, Kommandanten und Fachpersonal der drei Nationen im Rahmen eines VIP-Day die Bedeutung der Thematik, die Herausforderungen und erste Übungserkenntnisse nähergebracht.

Form, Umfang und Ablauf der Übung Alpine Jam 25 haben sich bewährt – die nationalen Übungsziele wurden erreicht. Die gewonnenen Erkenntnisse sowie der enorme Mehrwert der internationalen Zusammenarbeit, des Erfahrungs- und Wissensaustausches sowie die Bedeutung der Interoperabilität in den technisch schnelllebigen Szenarien „Counter Remote Controlled Improvied Explosive Devise (RCIED)" und „Counter Unmanned Aerial Vehicle (UAV)" haben die drei Nationen bestärkt, die Übungsserie Alpine Jam im Jahr 2027 fortzusetzen und weiterzuentwickeln.

IKT-Sicherheit & Bedrohungslage Cyber

Das Referat IKT-Sicherheit & Bedrohungslage Cyber (IKTSih&BedrLCy) innerhalb der Abteilung IKTCyE hat den Auftrag die periodischen IKT-Sicherheitsüberprüfungen bei den Missionen des ÖBH durchzuführen. In der Leitlinie zur IKT-Sicherheit im Ressortbereich des BMLV ist die Überprüfung der technischen, organisatorischen, infrastrukturellen und personellen Absicherungsmaßnahmen angeordnet.

Foto: Mitarbeiter bei IKTSih-Maßnahmen, Bundesheer/Dion6

Zu diesem Zweck wurden 2025 vier IKT-Sicherheitsüberprüfungen bei den Missionen KFOR, EUFOR/ALTHEA (halbjährlich) und UNIFIL (einmal im Jahr) durchgeführt.

Die IKT-Sicherheitsüberprüfung in den Auslandseinsätzen ist ein Prozessschritt in der Cyber-Sicherheit um klassifizierte Daten und Systeme vor Bedrohungen zu schützen. Durch regelmäßige Überprüfungen können potenzielle Schwachstellen identifiziert und behoben werden, um Sicherheitslücken zu minimieren. Eine effektive IKT-Sicherheitsüberprüfung gewährleistet die Einhaltung von nationalen und internationalen Compliancemaßnahmen.

Eine proaktive Sicherheitskultur im Bundesheer gewährleistet die Resilienz von IKT-Systemen und Services gegenüber Bedrohungen.

Foto: Unsachgemäße Verkabelung, Bundesheer/Dion6

Im Zuge der Umsetzung der IKT-Sicherheitsmaßnahmen wurden auch Auf- und Umbauarbeiten von IKT Systemen bei Auslandsmissionen (z.B. TCN-Umbau) sicherheitstechnisch begleitet. Im Zuge der Absicherung von IKT-Systemen und Schutz der Informationen wurden auch Kryptosysteme für Vertraulich und Geheim österreichweit und in allen Missionen ausgetauscht.

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

Cyber Dokumentations- und Informationszentrum (CDIZ) in Graz

Das CDIZ Graz wurde 2024 vom Referat IKT-Sicherheit & Bedrohungslage Cyber (IKTSih&BedrLCy) implementiert, um die für die Analyse von Cyberbedrohungen notwendigen Daten gezielt verfügbar machen zu können.

2025 erfolgte eine Weiterentwicklung sowohl in personeller, technischer als auch infrastruktureller Hinsicht, um die Leistungsfähigkeit dieses Elements zu erhöhen.

Das Team des CDIZ Graz besteht aus Grundwehrdienern und Chargen, die Führung und Steuerung erfolgt durch das Referat IKTSih&BedrLCy.

In Zusammenarbeit mit dem Cyber Dokumentations- und Forschungszentrum (CDFZ) Wien werden cyber-relevante Informationen aus unterschiedlichen Quellen gesammelt und strukturiert in Datenbanken abgelegt.

Auf Grundlage dieser Daten werden Lagebeiträge und sowohl periodische als auch spezifische Abfragen und Berichte generiert und den jeweiligen Bedarfsträgern bereitgestellt.

Grafik: CDIZ, Bundesheer/Dion6

Budget und Personal

Leiter Budg&Pers: ADir RgR Doris ZELEZNY

Mittlerweile liegt der Abschluss der Reorganisation der Direktion 6 – IKT und Cyber und die damit einhergehende Gründung des Referats Budget und Personal ein Jahr zurück. Auch wenn die Reorganisation im personellen Bereich ausreichende Planungssicherheit gebracht hat, so waren die letzten Monate dennoch von vielen Herausforderungen geprägt, die von Seiten aller Beteiligten ein hohes Maß an Engagement, Flexibilität und Anpassungsfähigkeit erfordert haben. Dazu gehörten unter anderem die Anpassung an neue organisatorische Strukturen und Prozesse, sowie die Sicherstellung einer reibungslosen Zusammenarbeit zwischen dem IKT und Cybersicherheitszentrum und der Direktion 6 – IKT und Cyber als Leitungselement.

Die Vakanz der Referatsleitung des Referats Personalverwaltung und Öffentlichkeitsarbeit des IKT und Cybersicherheitszentrum war eine besondere Herausforderung, da die Leitung dieses Referats vorübergehend durch das Referat Budget und Personal übernommen wurde. Die zusätzlich anfallenden Arbeiten konnten durch die hohe Flexibilität und das starke Engagement aller Beteiligten bewältigt werden, was auch die Zusammenarbeit zwischen den beiden Referaten weiter gestärkt hat.

Mit der nun erfolgten Besetzung der vakanten Referatsleitung ist diese zusätzliche Belastung weggefallen. Nichts desto trotz wird seither die Zusammenarbeit zwischen den beiden Referaten eng und effektiv ausgestaltet, um ein reibungsloses Funktionieren hinsichtlich sämtlicher Personalbelange gewährleisten zu können.


Foto: BMLV/HBF

Dieses Jahr hat jedenfalls gezeigt, wie wichtig es ist, als Team zusammenzuhalten, damit auch zukünftige Ziele konsequent umgesetzt und Veränderungen bewältigt werden können.

„Unsere Mitarbeiterinnen und Mitarbeiter sind der Schlüssel zu unserem Erfolg. Im letzten Jahr ist es uns, durch Förderung der Kreativität, gegenseitige Wertschätzung und gute Zusammenarbeit gelungen, dass sich die Bediensteten langfristig mit dem Unternehmen identifizieren.“

Personal

Entwicklungen innerhalb des Referats Budget und Personal

Im laufenden Jahr konnten im Referat Budget und Personal Entwicklungen verzeichnet werden, die sowohl zur Stabilisierung der Arbeitsfähigkeit als auch zur Weiterentwicklung der Personalprozesse beigetragen haben.

Ein zentraler Erfolg war die Übernahme einer Personalbearbeiterin in ein unbefristetes Dienstverhältnis. Dadurch konnte erstmalig ein Besetzungsgrad von 100% erreicht werden. Diese Vollbesetzung wirkt sich auf die Aufgabenwahrnehmung innerhalb des Referats positiv aus: Zuständigkeiten konnten klar verteilt, Bearbeitungszeiten verkürzt und verlässliche Vertretungsregelungen etabliert werden. Zudem bietet die personelle Verstärkung gleichzeitig die Möglichkeit neue Initiativen zu starten und bestehende Prozesse weiter zu optimieren. Als verwaltungsvereinfachende Optimierungen können beispielhaft die dienstlich veranlasste Verlängerung der nicht regelmäßigen Telearbeit, sowie die Einführung eines allgemeinen Postfaches, das die kontinuierliche Bearbeitung personalrelevanter Vorgänge gewährleisten soll, genannt werden.

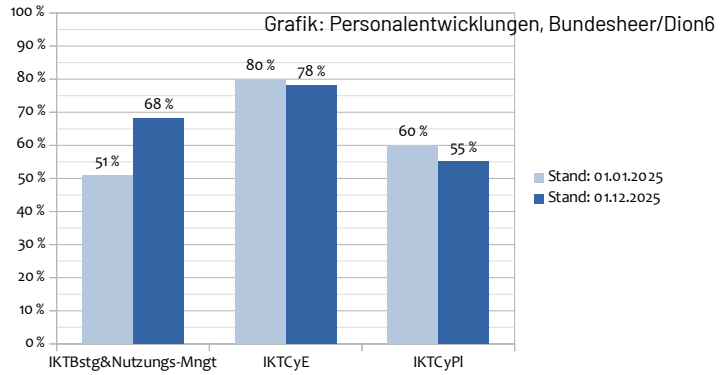
Dennoch wurde im Jahresverlauf erneut deutlich, dass das Fehlen eines Bewerbungsmanagement-Systems einen erheblichen organisatorischen Mehraufwand verursacht. Bewerbungen müssen weiterhin manuell erfasst, sortiert und verwaltet werden, was den Bewerbungs- und Auswahlprozess sehr langwierig macht. Ein digitales System, das dabei hilft, die Bewerbungen professionell zu verwalten, würde die Abläufe wesentlich effizienter gestalten, den Auswahlprozess beschleunigen und die Kommunikation mit den Bewerbern erleichtern. Zusätzlich wäre ein digitaler Bewerberpool wünschenswert, da mit einem solchen eine schnelle und effiziente Besetzung vakanter Positionen ermöglicht werden könnte, da bereits vorqualifizierte Kandidatinnen und Kandidaten zur Verfügung stehen. Damit könnte die Qualität der Personalgewinnung nachhaltig gestärkt werden.

Insgesamt zeigt das Jahr sowohl positive Entwicklungen als auch Herausforderungen auf, die in den kommenden Monaten weiterverfolgt werden müssen.

Um weiterhin den künftigen Zielen gerecht werden zu können, bedarf es jedenfalls enormer Anstrengungen.

Personelle Entwicklungen innerhalb der Direktion 6 - IKT und Cyber

Auch innerhalb der drei Abteilungen der Direktion 6 - IKT und Cyber konnten personelle Entwicklungen festgestellt werden. Trotz vermehrter Pensionsabgänge und bestehender Kontingent- und Aufnahmebeschränkungen konnte der Personalstand stabil gehalten und teilweise sogar erhöht werden.



Budget

Aufgrund der Nationalratswahlen wurde im Herbst 2024 kein Entwurf eines Bundesfinanzgesetztes 2025 vorgelegt, daher begann das Jahr 2025 mit einen Budgetprovisorium. Der tatsächliche Beginn der Freigabe des Budgets erfolgte im Juli 2025.Die Vorgaben des Ressorts, massiv in der Verwaltung einzusparen, wirken sich auch auf die Direktion 6 - IKT und Cyber nachhaltig aus. Dies betrifft auch den gesamten Aufbau und die Weiterentwicklung für die Ausrichtung auf ÖBH 2032+.

Die knappen Budgetmittel in den Bereichen der Inlands- und Auslandsdienstreisen führte im dritten Quartal 2025 zu massiven Einschränkungen. Auch die kommenden Jahre werden durch die massiven Einsparungen der Budgetmittel geprägt sein. Eine Priorisierung der Übungen und Vorhaben ist notwendig um zum Einen die vorgegebenen Ziele zu erreichen und gleichzeitig einen Fähigkeitenverlust zu vermeiden. Die restriktive Handhabung der Bugetmittel wirkt sich auch auf den Personalaufwuchs der Direktion 6 - IKT und Cyber aus.

Frauenbeauftragte

Das Jahr der Frauenbeauftragten 2025 war von Weiterbildung im Bereich Gleichstellung geprägt.
Ein Pilotkurs zum Thema Selbstverteidigung für Zivilbedienstete, als auch das Seminar Grundlagen der Gleichstellung sowie eine interne Schulung zu Dienstpflichten für Beamte und Vertragsbedienstete erweiterten das Wissen rund um das Thema Gleichstellung und Sexuelles Fehlverhalten im ÖBH.

In der Direktion 6 - IKT und Cyber gibt es insgesamt 4 Ansprechpartnerinnen wenn es um das Thema geschlechtliche Diskriminierung oder sexuelles Fehlverhalten geht:

- OR Mag. Helene Kautz (Dion6 & IKT&CySihZ)
- Lt Ines Kloiböck, BA (FüUS)
- OStWm Eva Lindbichler (FüUB2)
- StWm Elisabeth Jobst (FüUB1)

Einen großen Teil des Jahres unterstützte VB Marion Jansky das Team in Wien, bei der wir uns dafür recht herzlich bedanken möchten. Mit großer Motivation üben die Mitarbeiterinnen dieses Ehrenamt der Frauenbeauftragten aus, da ihnen der Einsatz für Gleichbehandlung und ein wertschätzendes Miteinander ein besonderes Anliegen ist. Für sie ist es sehr wichtig Unterstützung bei Problemen zu leisten, zuzuhören und Lösungen zu finden. So manche von ihnen konnte Ihren ersten "Einsatz" erfolgreich abschließen - eine Bestätigung für alle, diesen Weg mit Engagement fortzusetzen!

Mit Stand 05.12.2025 betrug der Anteil an weiblichen Mitarbeitern in der Direktion 6 - IKT und Cyber und IKT&CySihZ 14,73%. Betrachtet man die letzten Jahre ergibt dies, unter anderem aufgrund des erfolgreichen Recruitings, wieder eine positive Tendenz. Was trägt nun zu einer hohen Diversität im Personalstand bei und durch welche Maßnahmen wird das in unserem Ressort und damit auch in unserer Direktion gesteuert:

- Diversity Management als Instrument zur gezielten Wahrnehmung, Wertschätzung und Nutzung der Vielfalt aller Bediensteten und zur entsprechenden Verteilung von Ressourcen und Belastungen zwischen Gruppen
- Diskriminierungen aus Gründen des Geschlechts, der Rasse, der ethnischen Herkunft, der Religion oder der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung sind zu bekämpfen
- Frauenförderung erfolgt im BMLV gemäß dem Frauenförderungsplan (Frauen sind aktiv zu fördern, wenn sie unterrepräsentiert sind)
- Bundes-Behinderteneinstellungsgesetz

Oft wird der Punkt Wahrnehmung und Wertschätzung angesprochen, der auch viel mit Kommunikation zu tun hat. Um diese Kommunikation zu fördern gab es erstmals auf Initiative von OR Mag. Kautz ein informelles Treffen aller weiblichen Bediensteten des Standortes Stiftgasse. Denn Kennenlernen seines Gegenüber und Kommunikation ist einer der Grundsteine für ein respektvolles und wertschätzendes Miteinander.


Grafik: KI-generierte Abbildung, Bundesheer/Dion6


Grafik: KI-generierte Abbildung, Bundesheer/Dion6

BUNDESGESETZBLATT
FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2023 **Ausgegeben am 24. August 2023** **Teil II**

246. Kundmachung der Bundesministerin für Landesverteidigung betreffend den Frauenförderungsplan für das Bundesministerium für Landesverteidigung

Aufgrund des § 11a des Bundes-Gleichbehandlungsgesetzes (B-GlBG), BGBl. Nr. 100/1993, zuletzt geändert durch das Bundesgesetz, BGBl. I. Nr. 205/2022, wird verlautbart:

Frauenförderungsplan des Bundesministeriums für Landesverteidigung für den Zeitraum vom 1. September 2023 bis 31. Dezember 2025

Inhaltsverzeichnis

Präambel

(1) Das Bundesministerium für Landesverteidigung (BMLV) gibt ein klares Bekenntnis zur Gleichstellung von Frauen und Männern im Bundesdienst ab.

(2) Gemäß Bundes-Gleichbehandlungsgesetz besteht die rechtliche Verpflichtung, einer bestehenden Unterrepräsentation von Frauen entgegenzuwirken (Frauenförderungsgebot). Eine Unter-repräsentation von Frauen ist dann gegeben, wenn der Anteil der Frauen im Bereich der jeweiligen Dienstbehörde in einer Verwendung oder Funktion unter 50 Prozent liegt. Die Dringlichkeit der beruflichen Förderung von Frauen ergibt sich aus dem jeweiligen Ausmaß der gegenwärtigen Unterrepräsentation.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

IKT&Cybersicherheitszentrum

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

Es ist mir eine besondere Freude, als bestellter Leiter des IKT&CySihZ dieses Vorwort zu schreiben. Das IKT&CySihZ hat nicht nur als eigener „IT-Provider im Haus" eine Sonderstellung im Ressort, sondern mit dem Schwerpunktthema Digitalisierung des modernen Gefechtsfeldes die wahrscheinlich spannendste und wichtigste Rolle bei der Fähigkeitsentwicklung zu ÖBH2032+. Dies wird umso herausfordernder, da die technischen Entwicklungszyklen speziell im Bereich IT, Cyber, EloKa oder Space eine unheimliche Geschwindigkeit verzeichnen, die ein modernes Heer zumindest in den Grundzügen parallel entwickeln muß, um die Führungsfähigkeit zu gewährleisten bzw. die Information Superiority im Einsatzraum zu erlangen.

Trotz der relative Größe des IKT&CySihZ und seiner ausgezeichneten Mitarbeiter war das IKT&CySihZ auch 2025, zumindest in Teilbereichen, bis zur Grenze der Leistungsfähigkeit gefordert. Die konkreten Projekte sind in den einzelnen Fachbereichen ausführlich beschrieben, können aber in 5 Hauptgruppen unterteilt werden:

- IKT-Betrieb stabil und sicher durchführen (vom Nutzer bis zu den Serverfarmen, von Usability bis zum Notfallmanagement)
- IKT-Sicherheit und Cyberabwehr 24/7 durchführen und regelmäßig üben bzw. evaluieren (vom Audit über Zulassungen der IKT-Systeme bis zum technischen Lagebild Cyber)
- IKT/Geo/Space/EloKa Portfolio (Service und Projekte) abstimmen und entsprechend der Vorgaben (Nutzungsrichtlinien, Betriebsvorgaben, SLA) „in-time" und „in-budget" umsetzen
- Weiterentwicklung der gesamten IKT-Landschaft (z.B. Bundesheer online, digitale Souveränität, IKT-Ausstattung PANDUR, Vernetzung ISTAR bis zu Joint Warfare) um ein modernes IKT-System dem Ressort zur Verfügung zu stellen
- moderne/aktuelle Entwicklungen wie z.B. EloKa-Fähigkeiten, Space Services und KI (künstliche Intelligenz) implementieren


Foto: BMLV/HBF

Alle diese Bereiche müssen gem. dem Zielbild ÖBH2032+ bestmöglich „militarisiert" und insbesondere durch Miliz (speziell für die Durchhaltefähigkeit) Einsatztauglich (inkl. 24/7) ausgerichtet werden.


Foto: BMLV/HBF

Führungsabteilung

ObstdG Ing. Mag. Guido KRAUS

Das Jahr 2025 war geprägt mit dem weiteren Aufwuchs des IKT&Cybersicherheitszentrum (IKT&CySihZ) in personeller Sicht wie auch bei den Fähigkeiten im Zusammenhang mit dem Aufbauplan ÖBH 2032+.

Dabei hat die Führungsabteilung (FüAbt), die mit Juni 2025 einen neuen Leiter erhielt, die notwendigen Unterstützungen und verwaltungstechnischen Rahmenbedingungen sichergestellt.

Dazu wurde auch das Übungsvorhaben „Locked Shields 2025", das mit internationaler Beteiligung in einem eigenen Übungssetting durchgeführt wurde, maßgeblich durch Elemente der FüAbt unterstützt.

Mit 01.10.2025 wurde zusätzlich ein neuer Organisationsplan (OrgPl) verfügt, der den Referaten der FüAbt eine notwendige Anpassung speziell der Fachkräfte ermöglicht, um den Aufwuchs des IKT&CySihZ auch weiterhin bestmöglich unterstützen zu können.

Dieser Aufwuchs bedeutete auch eine räumliche Erweiterung der verschiedenen Fachbereiche des IKT&CySihZ, welche mit Masse ebenso aus der FüAbt heraus geplant und bewirtschaftet wurde und 2026 weiter koordiniert wird.

Diese Veränderung betraf auch verschiedene Teilbereiche der FüAbt, sodass deren Diensträumlichkeiten teilweise verlegt und adaptiert werden mussten. Dabei hat das betroffene Personal den ordnungsmäßigen Dienstbetrieb aufrecht erhalten und damit wieder ihre Flexibilität unter Beweis gestellt.

Personalverwaltung

Im Jahr nach der umfassenden Umstrukturierung ist das IKT&CySihZ nun vollständig eigenständig und organisatorisch klar von der Direktion 6 getrennt. Diese Neuausrichtung bildete die Grundlage für eine deutliche Professionalisierung des Zentrums. Im Jahr 2025 konnte die interne Struktur weiter gefestigt werden: Mit der Einsetzung einer neuen Referatsleiterin (RefLtr) für die Personalverwaltung (S1) sowie der Übernahme einer zusätzlichen Sachbearbeiterin wurde der Personalbereich nachhaltig gestärkt. Diese personellen Erweiterungen steigern nicht nur die organisatorische Leistungsfähigkeit, sondern tragen auch langfristig zur Stabilität und Weiterentwicklung bei.

Ein besonderes Highlight stellte die Teilnahme zweier Referentinnen aus den Referaten Budg&Pers (Dion6) sowie PersVerw&ÖA an der internationalen Cyber-Verteidigungsübung „Locked Shields 2025" dar. Diese zweiwöchige Übung brachte hochqualifizierte Fachkräfte aus verschiedenen Nationen zusammen und bot eine ausgezeichnete Plattform für Wissensaustausch, Netzwerkbildung und die praktische Anwendung aktueller cyberverteidigungsspezifischer Verfahren. Erstmals kam dabei auch das neu entwickelte Personalmeldesystem zum Einsatz, eine vom Fachbereich Applikationen eigens programmierte Software, die eine vollständige digitale Erfassung und Auswertung aller Teilnehmenden ermöglichte. Durch diesen technologischen Fortschritt konnte der gesamte Meldeprozess erheblich beschleunigt, standardisiert und insgesamt effizienter gestaltet werden. Zugleich leistet das System einen wesentlichen Beitrag zur fortschreitenden digitalen Weiterentwicklung.

Noch weitere Gründe forderten die Personalverwaltung im Jahr 2025 deutlich stärker und sorgten für eine weit höhere Auslastung als im Vorjahr. Diese waren vor allem mehrere Erweiterungen in den Organisationsplänen, die in verschiedenen Bereichen zusätzliche Planstellen geschaffen haben. Dadurch erhöhte sich die Zahl der Ausschreibungen spürbar im Vergleich zu 2024. Vor allem externe Bekanntmachungen führten zu einem deutlichen Anstieg an Bewerbungen. Hinzu kam eine Zunahme an Anfragen im Zusammenhang mit dem Grundwehrdienst sowie eine steigende Zahl an Initiativbewerbungen.

Besonders stark bemerkbar machten sich die höheren Bewerbungszahlen für Praktikumsstellen, insbesondere im Rahmen des Sommerpraktikantenkontingents. Diese Entwicklungen machen deutlich, dass das IKT&CySihZ sowohl als Arbeitgeber als auch als Dienstleister zunehmend an Attraktivität gewinnt und gleichzeitig seine Rolle als moderne, wachsende und technologisch geprägte Dienststelle weiter ausbaut.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Ausbildung und Miliz (Ausb&Miliz)

Das „hybride" Referat Ausb&Miliz gehört gemäß Orgplan zum IKT&CySihZ/FüAbt. Tatsächlich ist das Referat in Doppelverwendung, daher die Bezeichnung „hybrid", weil die Direktion 6 - IKT und Cyber kein in irgendeiner Form abgebildetes Ausbildungselement hat und somit gemäß Geschäftsordnung verantwortlich ist, sämtliche Aufträge hinsichtlich Ausbildung und Miliz der Direktion 6 - IKT und Cyber zu erfüllen. Der Aufgabenbereich des Referats ist auf Grund der Hybridität weit gestreut und erfordert die Bearbeitung der Themenbereiche der klassischen Stabsarbeit S3, S5 und S7.

Die Tätigkeiten und der Verantwortungsbereich des Ref Ausb&Miliz sind die Abwicklung von

- Ausbildungen im Inland an zivilen Ausbildungsstätten
- Ausbildungen im Inland an militärischen Ausbildungsstätten/Laufbahnkurse.
- Ausbildungen im Ausland an zivilen und militärischen Ausbildungsstätten. Diese werden auf Basis Entsendung gem. KSE-BVG, Abs1 Z2 durchgeführt.
- Besuche in Österreich (BiÖ) für Ausbildungen
- BiÖ allgemein (Bilaterale Besuche..., etc.)
- Auslandsdienstreisen (ADR) aller Arten; hierzu gehören NATO-ADR, EDA-ADR, WFE-ADR und ADR-allgemein
- NATO Travelorder (NATO Marschbefehle)
- Milizangelegenheiten: Befüllung des Miliz-OrgPl, Beorderungen bei Direktion 6 - IKT und Cyber und IKT&CySihZ, Bearbeitung von freiwilligen Meldung zu Milizübungen, freiwillige Waffenübung (fWÜ), Funktionsdienst (FD), freiwillige Milizarbeit (fMA), Sperrung auf dem Arbeitsplatz, Beantragungen auf Zuweisung eines Übungsverbands, Erwirken von Einberufungsbefehlen, Bearbeitung und Mitarbeit bei Planung von Milizübungen etc.

Derzeit ist das Referat nicht voll besetzt, sodass die Aufgabenfelder und Bearbeitungslast flexibel zugeordnet werden müssen.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Versorgung & Infrastruktur (Vers&Infra)

Die Eigenversorgung läuft gemäß den vorgegebenen logistischen Abläufen zufriedenstellend, die Zusammenarbeit mit den Bereichen hat sich aufgrund des Kennenlernens der zugeteilten Nachschuborgane mit den zivilen Bedarfsträgern erheblich verbessert.

Der neue Orgplan für die FüAbt wurde mit 01.08.2025 erlassen und aufgrund umsichtiger Personalplanung und logistischer Ausbildung konnten alle zusätzlich genehmigten Arbeitsplätze (API) mit Fachpersonal besetzt werden. Die Fachausbildung an der Heereslogistikschule (HLogS) erfolgt erst nach Einteilung auf den Arbeitsplatz und wird im Herbst 2026 für alle neu eingeteilten Versorgungsorgane abgeschlossen werden.

Für die Bereiche und Abteilungen der Dion6 wurde unter Federführung (ff) des Referates Vers&Infra ein den Bedürfnissen angepasster Orgplan Sachmittelteil erarbeitet und im Oktober 2025 der IKTCyPl und der Org zur Prüfung und Genehmigung vorgelegt.

Die geplanten Inventuren erfolgten gemäß vorgelegtem Inventurplan an Direktion 4, Schwergewicht 2025 war die Inventur des Bereichs Applikationen, um die geordnete Übergabe an den neuen Geräteverwalter gemäß Materialwirtschaftsweisung 123/4 vollziehen zu können.

Die Fremdversorgung (FV) & Konfigurationslogistik (KonfigLog) 2025 war gekennzeichnet durch die Neuorganisation der Logistik durch die Direktion 4. Die Direktion 6 - IKT und Cyber konnte die Versorgung eigenständig unter Anbindung an das IKT&CySihZ sicherstellen. IKTCyE sind mit ihren Teilen in Salzburg und Graz in der Versorgungsdurchführung den jeweiligen Militärkommanden zugewiesen.

Die Fremdversorgung unterstützte die Cyberübung „Locked Shields 2025" mit Personal und Gerät von FüUB1 und FüUB2 und stellte die Arbeits- und Einsatzbereitschaft für über 150 Teilnehmer unter ff IKTCyE sicher.

Im Zuge des Bedarfes von Crypto-Geräten NCAS, ASECOS und SINA Boxen wurden 2025 vereinzelt Konfigurationen vorgenommen und den Bedarfsträgern im ÖBH aus dem IKT-Sonderlager übergeben.

Auch 2025 verlangten laufende Einsätze und Übungen erhebliche IKT-Gerätebewegungen von speziell konfigurierten Funkgeräten und Mobiltelefonen aus dem IKT-Sonderlager.

Die Funktion von IKT & Fernmeldesystem-Räumen im ÖBH war durch den Ausfall des strategischen Anlagenraumes IFMIN in einer Kaserne nach einem Hochwasser nur eingeschränkt gegeben. Der Notbetrieb wurde unter ff IKTCyE und IKTBetr mit Telecom A1 provisorisch wieder hergestellt und das Militärkommando Niederösterreich sowie die Stellungskommission angebunden. Im März 2025 erfolgte eine IKT-Konferenz zur Errichtung eines neuen Anlagenraumes mit zusätzlicher Implementierung des Telekommunikationsverband (TKV). Der Bau, Einrichtung und Inbetriebnahme wird im 1. Quartal 2026 unter ff IKTS und Begleitung IKTBetr fertiggestellt werden, die Aufräumarbeiten im zerstörten IFMIN Bunker dauern nach wie vor an und werden mit Kräften Dion4, IKTBetr und MilKdo NÖ bis Ende 1. Quartal 2026 zum Abschluss gebracht.

Schwergewicht 2025 war auch die Autarkie in der Stift-Kaserne, Anbindung der Stromversorgung an das Objekt 6, Errichtung der Zusatztanks und Umstellung der Löschanlage von Halon zu C2.

Das 4. Obergeschoß (OG) des Objektes 10 Wirtschafts- und Unterkunftsgebäude (WUG) wurde der Direktion 6 - IKT und Cyber seitens Direkton 7 zugesprochen und in Eigenregie adaptiert. Der Raumgewinn eines Stockwerkes umfasst Platz für 30 Cyberrekruten und Bürofläche für 30 Mitarbeiter. Mit der Fertigstellung und Bezug von Teilen IMG und FüAbt wird Mitte 2. Quartal 2026 gerechnet.

Weiters unterstützte das Referat Versorgung die infrastrukturellen Anpassungen in der Stift-Kaserne, um die notwendigen Erweiterungen der verschiedenen Organisationseinheiten sicherzustellen.

2025 stand der Fokus für die Übernahme/Übergabe von logistischem Fachpersonal aufgrund zeitnaher Versetzung in den Ruhestand, Ausscheiden von Mitarbeitern und genereller Personalfluktuation.

Gleichzeitig konnten 3 weitere Versorgungs-Mitarbeiter die Ausbildung zum Nachschubsunteroffizier (NUO) an der HLogS besuchen, weiteres Fachpersonal deren Aus-Fort- und Weiterbildung erfolgreich durchlaufen und bis Ende des Jahres umfangreiche Bildungsprogramme abschließen.

Die Rekrutierung weiterer Personen aus dem Grundwehrdienst und der Privatwirtschaft erfolgte 2025 weiterhin erfolgreich und garantiert die Abdeckung von personellen Abgängen und Bedeckung des Aufwuchses gemäß OrgPl FüAbt neu.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6


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.

Neben diesen Tätigkeiten lag das Schwergewicht 2025 in der Weiterentwicklung von einsatzorientierten Fähigkeiten durch die Teilnahme an der CWIX 2025 und der Übernahme des National Lead für diese Übungsreihe.

Ebenso wird die Einführung der neuen Führungsinformationsservices mit dem SitaWare Headquarters und Frontline und der IKT-Systeme für die unterschiedlichen Varianten des Mannschaftstransportpanzers PANDUR durch den Bereich Applikationen tatkräftig unterstützt.

Weiters wurde die IDV-Anwendung COPiD durch die Webanwendung „Personalmeldesystem Einsatz" ersetzt, die u.a. zur Generierung von Personalmeldungen in laufenden Einsätzen verwendet wird.

Um für die Streitkräfte zukünftig genügend Personal rekrutieren zu können, wurde das Projekt „Digitalisierung Wehrdienst" initiiert, das die Stellungspflichtigen schon frühzeitig mittels modernen digitalen Medien über die Karrieremöglichkeiten im ÖBH informiert.

Entwicklung und Start Audit DGMN 2.0

Aufbauend auf die über Jahrzehnte gesammelten Erfahrungen im Bereich Betriebssysteme, Informationsmanagement, Softwareverteilung etc. wurde die Konzeption von DGMN 2.0 gestartet und in Abstimmung mit MilCyZ entwickelt.

Im Zuge der Weiterentwicklung galt es ua. folgende Anforderungen zu erfüllen:

- Migrationsszenario
- Berücksichtigung von zukünftigen Anforderungen im ÖBH
- Neudesign und Implementierung eines Rollenkonzeptes in eine neugeschaffene Domaine.

Gemeinsam mit MilCyZ wurden bereits erste erfolgreiche Entwicklungsaudits durchgeführt.

Interoperables Zutrittsmanagement (iZMS) & Küchenmanagement-Systems (KMS)

Im Jahr 2025 konnte sowohl das Pilotprojekt iZMS als auch das Rollout und die Abnahme von KMS erfolgreich umgesetzt und abgeschlossen werden.

Im Bereich von iZMS wurden neben den umfangreichen Funktionstests insgesamt vier unterschiedliche Hersteller mit zwei unterschiedlichen Kartentechnologien in das Abnahmesystem integriert und in einem aus drei Standorten bestehenden Gesamtsystem implementiert.

Im Bereich des KMS wurden neben den zahlreichen zusätzlichen funktionellen Anforderungen vor allem diverse Schnittstellen und Automatisierungsschritte implementiert.

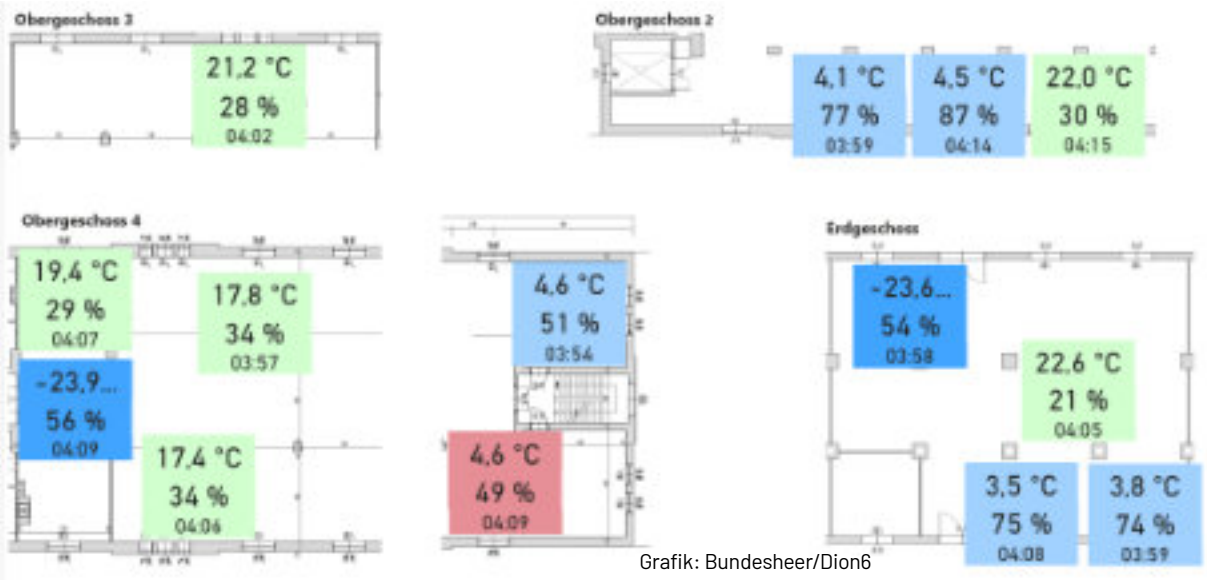
Vorbereitungen für die Beschaffung eines medizinischen Informationssystems (MEDIS)

Gemeinsam mit der Direktion 8 und Abteilung IKT-Systeme wurden im Jahr 2025 die erforderlichen Unterlagen für die Einleitung einer Ausschreibung wie Leistungsbeschreibung und -verzeichnis samt Bewertungskriterien etc. erarbeitet.

Sonstige Projekte und Vorhaben (Auszug)

In den diversen weiteren zahlreichen IKT-Services im DGMN wurden unterschiedlichste Anforderungen implementiert und die Systeme weiter ausgebaut. So wurden im Bereich Low-Range-WAN (LoRaWAN) unterschiedlichste Temperaturüberwachungen mit Alarmierung und Transportüberwachung realisiert. Des weiteren wurden unterschiedlichste Services in die Auswerte- und Management-Plattform PowerBI eingebunden.

Grafik: LogoDGMN, Bundesheer/Dion6



Grafik: Bundesheer/Dion6

Informationsfreiheitsgesetz-Service (IFG-Service)

Mit Inkrafttreten des Informationsfreiheitsgesetz (IFG), samt Vollzugsverpflichtung ab dem 01.09.2025, besteht das Recht auf individuellen Zugang zu Informationen.

Gefordert ist u.a. die proaktive Bereitstellung von Dokumenten im allgemeinen öffentlichen Interesse gemäß Informationsfreiheitsgesetz 2025.

Im BMLV wurde hierfür das Service „IFG-Service" zur Freigabe dieser Dokumente implementiert.

Grafik: IFG-Service, Bundesheer/Dion6

Wird im Zuge der Aktenbearbeitung im BMLV-ELAK festgestellt, dass ein oder mehrere Dokumente dieses Akts für die Öffentlichkeit von Interesse sind, kann dem Akt ein Antrag zur Freigabe dieser hinzugefügt werden. Der Antrag beinhaltet die Metadaten des Datensatzes, diese können über ein Formular nachbearbeitet werden.

Der Akt mit den freizugebenden Dokumenten darf nicht klassifiziert und/oder keine Datenschutz-Markierung aufweisen. Nach Genehmigung des Aktes wird der entsprechende Antrag in das IFG-Service zur weiteren Bearbeitung durch GDPräs eingebracht.

Eine Erweiterung der Begutachter um weitere Experten, wie z.B.: Datenschutzbüro (DSBür) oder Abwehramt (AbwA), ist vorgesehen.

Durch Sichtung und Bewertung der Dokumente werden diese nun zur Veröffentlichung freigegeben oder zurückgewiesen.

Nach erfolgter Freigabe werden die Dokumente an das Portal „data.gv.at" übergeben.

Schwerpunkt Einsatzorientierung

Ein wichtiger Schwerpunkt der Abteilung Informationsmanagement&Büroautomation war auch im Jahr 2025 die Einsatzorientierung durch die Bereitstellung von Core-Services gemäß den Vorgaben der Federated Mission Networking (FMN) Initiative:

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

Hierbei gilt 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 FMN müssen erfüllt sein
- Einsatztauglichkeit/Truppentauglichkeit: Nutzung und Betrieb der IT-Services durch die Truppe im Einsatzraum müssen möglich sein.

Diese Core-Services wurden bei der internationalen Interoperabilitätsübung CWIX2025 (Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise) getestet.

Munition Ausbildungsgebühren

Das zentrale Web-Service Munition Ausbildungsgebühren (MunAusbGeb) dient dazu, den Munitionsbedarf laut Gebührenerlass zu melden, prüfen und die entsprechenden Zuweisungen anzuordnen.

Das Service MunAusbGeb umfasst folgende Module:

Gebührenerlass

Der Gebührenerlass wird durch Waffensysteme & Munition (WSM) gepflegt. Darin werden jährlich aufgrund der Ausbildungsvorhaben die Ausbildungs-munitionsgebühren (wie viel von welcher Munition für einen bestimmten Zweck) festgelegt.

Bedarfsmeldung Bedarfsträger

Basierend auf dem Gebührenerlass meldet jede Organisationseinheit (OrgEinheit), welche Ausbildungsvorhaben (wie viele Personen/ Waffen/...) durchgeführt werden. Unter Berücksichtigung des noch vorhandenen Bestands ergibt sich daraus der Munitionsbedarf für das Ausbildungsjahr.

Prüfung und Zusammenfassung Bedarfsmeldung durch übergeordnete OrgEinheit

Die Bedarfsmeldungen werden entlang der MunAusbildungsHierarchie jeweils von den übergeordneten OrgEinheiten geprüft und zusammenfasst.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Zuweisung durch WSM

WSM weist den obersten OrgEinheiten aufgrund des gemeldeten Bedarfs unter Berücksichtigung vorhandener Deposite, Prioritäten und Mangellage Munition zu. Gegebenenfalls werden auch Ablieferungsaufträge ausgesprochen. Es kann auch angegeben werden, dass eine bestimmte Munition erst später (nach Lieferung durch die Firma) zugewiesen wird.

Zuweisung durch übergeordnete OrgEinheit

Die übergeordnete OrgEinheit weist die erhaltene Munition aufgrund des gemeldeten Bedarfs ihren untergeordneten OrgEinheiten zu.

Abwicklung Später-Zuweisung

Die im Rahmen der 1. Zuweisung durch WSM und übergeordnete OrgEinheiten angekündigten Zuweisungen aus Firmenlieferungen werden umgesetzt.

Die Module „Gebührenerlass“, „Bedarfsmeldung Bedarfsträger“ und „Prüfung und Zusammenfassung Bedarfsmeldung durch übergeordnete OrgEinheit“ werden aktuell durch Anwender getestet. Die anderen Module werden bis Ende Q2/2026 umgesetzt.

Personalapplikationen

Die Abteilung Personalapplikationen ist der zentrale Personaldatenprovider des österreichischen Bundesheeres und steht für Digitalisierung und eGovernment im BMLV.

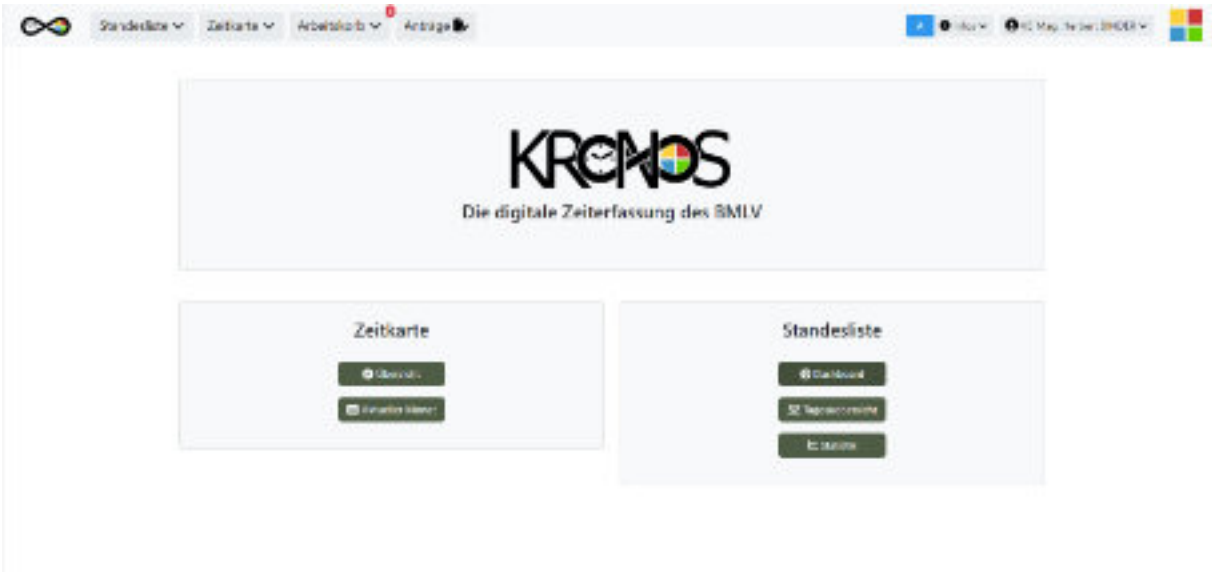
Die Erfolgsgeschichte von bundesheeronline konnte auch im Jahr 2025 fortgesetzt werden, bundesheeronline wurde mit dem österreichischen Verwaltungspreis 2025 in der Kategorie, "Innovatives Servicedesign und digitale Services" ausgezeichnet.

Die Auszeichnung erfolgte insbesondere aufgrund des direkten Kommunikationskanals zwischen Antragsteller und zuständigen Referenten („Chat") und der transparenten Darstellung des Bearbeitungsstatus. Die Akzeptanz als auch die Erfordernis wird eindrucksvoll durch die hohe Anzahl an bereits registrierten Anwendern (ca. 70.000) dokumentiert. Das IT-Service bundesheeronline wird um weitere Verfahren ständig erweitert, unter anderem ist aktuell die Verlässlichkeitserklärung (VLE), diverse freiwillige Meldungen sowie die Datenschutzauskunft bereits in Erprobung.

Das Projekt „Digitalisierung Wehrdienst", eng verwoben mit bundesheeronline ermöglicht in Phase I die freiwillige digitale Vorabteilnahme von Stellungspflichtigen am Stellungsprozess und soll bereits Ende Jänner 2026 in der Muster-Stellungskommission Kärnten erprobt werden. Die zielgruppengerechte Kommunikation als auch der zeitgemäße digitale Auftritt soll zur Attraktivitätssteigerung des Bundesheeres beitragen.

Der Probebetrieb zu KRONOS-Zeiterfassung konnte im Jahr 2025 erfolgreich beendet werden. Mit dem Erlass der neuen Zeitordnung ist für alle Anwender mit einer personifizierten SMN-Chipkarte die Teilnahme verpflichtend. Es sei erwähnt, dass bereits im Probebetrieb die meisten Dienststellen des BMLV KRONOS freiwillig genutzt haben. Dies spricht für die hohe Qualität der Anwendung sowie den erkennbaren Nutzen für den Bediensteten, den Vorgesetzten und in weiterer Folge der Personalverwaltung. KRONOS entwickelt sich weiter zum zentralen Mitarbeiter-Dashboard. Aktuell wird bereits bei ausgewählten Dienststellen der persönliche Arbeitskorb sowie die Integration der WEB-Standesliste in KRONOS erprobt.

Foto: Übergabe Verwaltungspreis, BMLV/HBF



Grafik: KRONOS, Bundesheer/Dion6

Der persönliche Arbeitskorb ermöglicht die nachweisliche Benachrichtigung der Bediensteten und vermeidet die Erstellung von Arbeitslisten. Nach erfolgreicher Integration des PAAN-Antragswesen kann KRONOS über das BMLV-Stammportal bereitgestellt werden und dadurch über private Devices sowie im DGMN genutzt werden.

Grafik: Logo PMSE, Bundesheer/Dion6

Personalmeldesystem Einsatz (PMSE) wurde im Jahr 2025 erfolgreich erprobt und ist ab November 2025 als Ersatz von COPID bei Inlandseinsätzen und -übungen verpflichtend zu nutzen.

Die Integration mit den bestehenden Personal-applikationen bzw. die Nutzung der bereits vorhandenen Daten, ist das Erfolgsgeheimnis der neuen Anwendung.

Auch hier dokumentieren die hohen Nutzungszahlen bereits in der Erprobungsphase die Akzeptanz und den Bedarf an Digitalisierung.

Neue Anwendungen im Bereich Personalapplikationen werden bereits ausschließlich in WEB-Technologie bereitgestellt, mit dem Projekt "Digitalisierung Wehrdienst" werden nun auch Bestandsapplikationen technologisch erneuert und in WEB-Technologie entwickelt.

Der Leitsatz von PersAppl ist, Daten am Entstehungsort (Bedienstete, Wehrpflichtige, Bürgerinnen und Bürger) nur einmal erfassen zu lassen und gegebenenfalls medienbruchfrei über Schnittstellen weiterzuverarbeiten.

CWIX 2025

CWIX ist die größte IKT-bezogene Veranstaltung der NATO und ihrer Partnernationen.

2025 waren 3250 Personen aus 40 Nationen sowie NATO-Organisationen und dem EU-Military Staff registriert.

Es wurden mehr als 400 militärische IKT-Systeme unterschiedlicher Entwicklungsstufen und Reifegrade im multinationalen Verbund getestet.

Grafik: Logo CWIX, NATO

Foto: CWIX25 Teilnehmer AUT, Bundesheer

Das österreichische Kontingent war auf beiden Standorten im polnischen Bydgoszcs, dem NATO Joint Force Training Center (JFTC) und einem Flugfeld der Polnischen Streitkräfte präsent.

Ein erheblicher Teil der Tests konnte jedoch auch von dem aus Wien angebundenen AUT Battle Lab durchgeführt werden. Das Schwergewicht lag dabei auf der Vorbereitung zur Zertifizierung von IKT-Services des ÖBH im Rahmen des FMN, das seit Jahren das Leitprogramm für die Zusammenarbeitsfähigkeit der Nationen, aber auch zwischen Domänen und Waffengattungen für Joint- und Multi Domain Operations, ist.

Die Teststellungen waren in 18 sogenannten Focus Areas organisiert. Eine davon, GeoMetOc-Service, wurde von einem Mitarbeiter des Instituts für Militärisches Geowesen erfolgreich geleitet. Der, durch die Abteilung Einsatzapplikationen gestellte Experte in der Focus Areas Joint Intelligence, Surveilance and Reconnaissance (JISR), konnte als Focus Area Analyst einen wichtigen Beitrag leisten. Somit konnten wertvolle Informationen und Erkenntnisse für die nationale Fähigkeitsentwicklung gewonnen werden.

Führungsinformationservice „SitaWare"

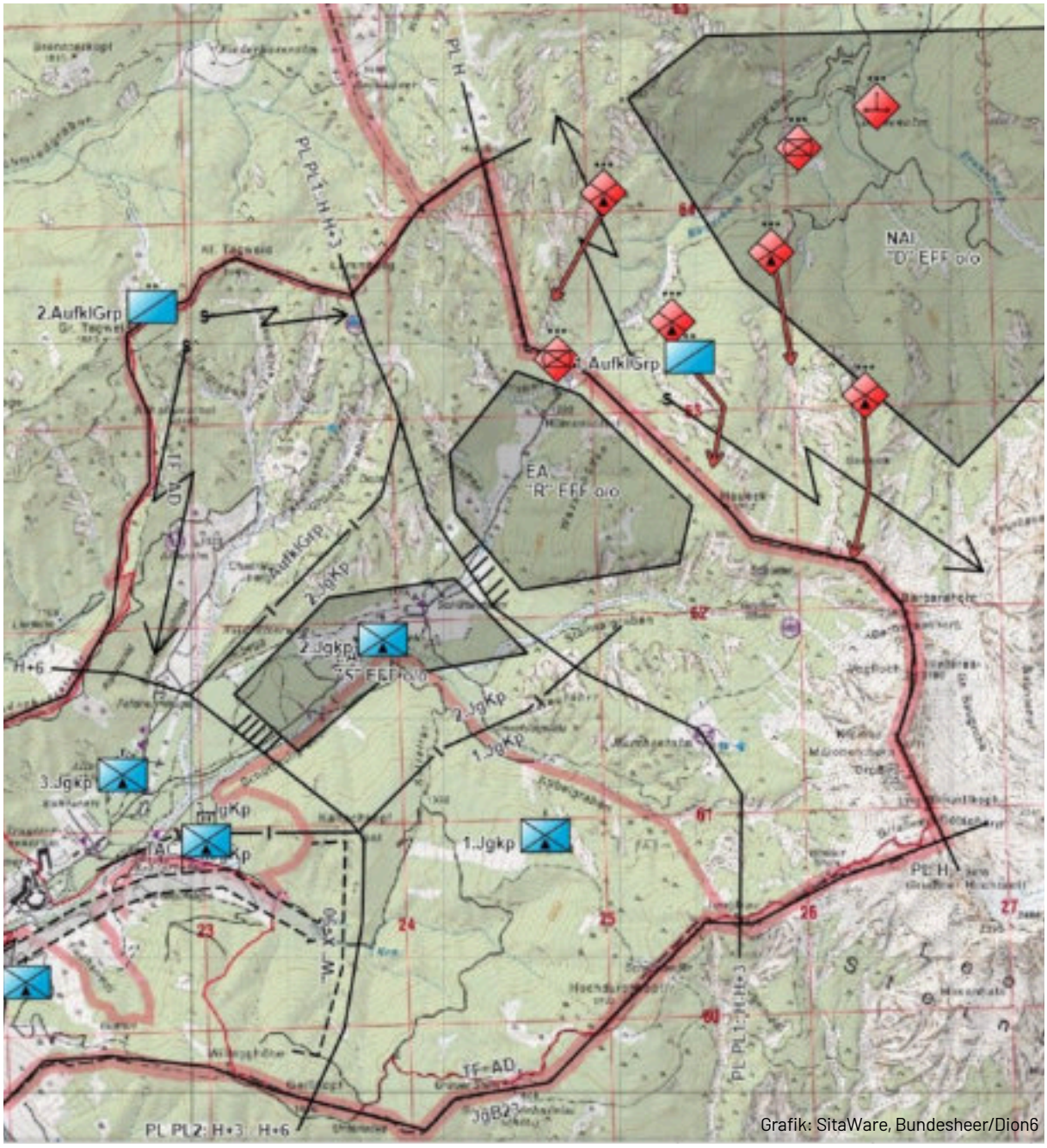
Die mit Ende 2024 beschaffte Software-Suite SitaWare der Firma Systematic wird derzeit in die Systemlandschaft des ÖBH technisch integriert und gleichzeitig werden die militärischen Planungsprozesse hinsichtlich der digitalen Unterstützungsmöglichkeiten evaluiert und optimiert. Gemeinsam mit der Herstellerfirma wurde die erste Implementierung des Systems erfolgreich durchgeführt.

Damit konnten den Akademien, Theresianische Militärakademie (TherMilAk) und Landesverteidigungsakademie (LVAk), jeweils eine Instanz im zentralen Rechenzentrum bereitgestellt werden. Erste Funktions- und Leistungstests fanden im Rahmen der Übung „Waldviertel" auf einer TCN-Server Ausstattung statt.

Im Laufe des Jahres startete die Zusammenarbeit mit der IKTTe zur Entwicklung von automatisierten Bereitstellungsprozessen. Ziel ist es, die Einführung und Aktualisierung der Systeme künftig vollständig automatisiert und einheitlich durchführen zu können.

Im zweiten Halbjahr 2025 wurde zudem eine Power-User-Gruppe unter der Leitung von IKTCyE eingerichtet. Ihre Hauptaufgabe liegt in der Erstellung von Standard Operating Procedures (SOP) für den praktischen Einsatz der Software-Suite.

Ab dem zweiten Quartal 2026 wird darüber hinaus eine eigene Ausbildungsumgebung für SitaWare Headquarters für bestimmte Standorte zur Verfügung stehen.



Grafik: SitaWare, Bundesheer/Dion6


Foto: BMLV/HBF

IKT-Technik

Leiter IKTTe & CTO des BMLV: Mag. Wolfgang HACKER

Im Jahr 2025 wurde neben der Erhaltung und Weiterentwicklung der bereits eingeführten Systeme / Plattformen / Services intensiv an der Umsetzung der Vorgaben aus dem Zielbild ÖBH2032+ gearbeitet, wobei der Schwerpunkt auf der Schaffung eines durchgängigen System of Systems lag.

Dieses System ermöglicht die Integration verschiedener Teilsysteme zu einem kohärenten Gesamtsystem, das die Anforderungen moderner militärischer Operationen erfüllt.

Durch die systematische Nutzung von Cloud-Technologien in den Verarbeitungsebenen Edge, Fog und Cloud soll hinkünftig eine effiziente und effektive Bereitstellung des IKT-Systems des Österreichischen Bundesheeres ermöglicht werden.

Ein besonderes Highlight war das Aufsetzen einer internen Machine Learning Operations (MLOps)-Plattform, welche die Bereitstellung von Künstlicher Intelligenz (KI)-Services ermöglicht.

Insgesamt kann das Jahr 2025 als ein erfolgreiches Jahr bewertet werden. Die umgesetzten Maßnahmen tragen dazu bei, die IKT-Infrastruktur zukunftssicher zu machen und die Kernaufgaben des BMLV/ÖBH effektiv zu unterstützen.

PANDUR IKT-Labor

Im Juni 2025 wurde das Pandur IKT-Labor eröffnet. Mit der Beschaffung von 225 PANDUR Evo sind neben der Ausarbeitung der Konzepte für den IKT-Einsatz auch praktische Überprüfungen notwendig geworden.

Schrittweise werden beginnend vom digitalen Interkomm-System die Systeme mit Blick Zielausstattung aufgebaut, konfiguriert und im Verbund getestet.

Dabei wird von Anfang an die Truppe mit eingebunden, um hier mit den Bedarfsträgern gemeinsam rasch zu Erkenntnissen zu gelangen.

Durch die Einstellmöglichkeit eines PANDURs mit fliegender Verkabelung gibt es einen Handlungsspielraum, der im reinen Laborbetrieb nicht möglich ist.

Ferner soll die Verzahnung verschiedener Systeme unter Laborbedingungen erprobt werden. Denn die Pandur-Flotte sowie andere Gefechtsfahrzeuge bedürfen des Zusammenspiels dieser Komponenten genauso wie das IKT-System Einsatz im Großen.

Perspektivisch ist dieses Labor damit als Teil des notwendigen Zentrums für Integration, Prozessvalidierung und Testung (ZIPT) zu sehen.

Einführung Interkomm-System Chelton TacG2, der Nachfolger der Cobham VIC-3-0

Das TacG2 ist ein softwaredefiniertes, digitales Interkomm-System, das sich im Bezug zur technischen Konzeption und Design stark am Vorgänger, der im ÖBH eingeführten VIC-3-0, orientiert. Das Design der Stationen erlaubt eine Umrüstung von Fahrzeugen mit VIC-3-0 Installation auf eine Lösung mit der TacG2 ohne mechanische Adaptation der Montagepunkte und unter Weiternutzung wesentlicher Teile der Verkabelung der VIC-3-0.

Eine „Voice over IP" Fähigkeit erlaubt den Aufbau und Annahme von VoIP Rufen zu externen Teilnehmer, internen Einzelteilnehmern sowie einer Interkomm Sprachgruppe. Selektivrufe und Konferenzgespräche mit Sprachteilnehmern der Interkomm sowie Funkgeräten stehen ebenfalls zur Verfügung.

Durch Vertreter des Bereiches IKT-Technik (IKTTe) erfolgte in Abstimmung mit dem Hersteller die Sprach- und Datenintegration aller Truppenfunksysteme sowie des Hochfrequenz-Funk (HF) Kurzwellenfunksystem. Zudem wurden die aktuellen Panzerfunk (PzF) Headsets (HS) sowie die in Testung befindlichen Muster der neuen Headset Systeme für Kampfhelme und PzF HS entsprechend für eine optimale Kommunikation angepasst. Der Zulauf und die Güteprüfung des neuen TacG2 Interkom Lösung erfolgt noch bis Mitte 2026.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Foto: TCN-Update, Klaus UNTERBUCHBERGER

Tactical Communication Network (TCN)-Update 3A/Systemtest

Im Zeitraum vom 25.05. – 05.09.2025 erfolgte das Firmware Update am Fernmeldesystem TCN auf eine neue Version. Diese Version deckt alle geforderten technischen Anforderungen der Leistungsbeschreibung ab. Die Umstellung auf das Protocol Independent Multicast (PIM)-Multicastprotokoll ermöglicht es 5 definierbare Multicast-Areas zu betreiben, wobei die Synchronisierung der Sprachteilnehmer ausschließlich im jeweiligen Multicast-Area erfolgt und damit andere Multicast-Areas nicht gestört bzw. durch den Synchronisierungsvorgang belastet werden.

Zur Feststellung der vollständigen Leistungserfüllung der technischen Aspekte der Leistungsbeschreibung und zur Überprüfung der Performance des TCN-Systems wurde ein Systemtest durchgeführt.

Zu diesem Systemtest wurden 106 Vermittlungseinheiten verteilt auf ganz Österreich unter Einbindung aller Brigaden zusammengezogen.

Es wurden 99 Testfälle in einem Drehbuch und einer Testmatrix unter der Federführung von Vertreter der Systembetreuung TCN definiert und von den Operatoren der Vermittlungen durchgeführt. Der Systemtest wurde positiv abgeschlossen.

Military Air Surveillance and Acquisition Radar System Short Range Radar (MARS SRR)

Das MARS SRR wird als Teilsystem der Nachfolge des Aufklärungs – und Zielzuweisungsradarsysteme (AZR) beschafft. Das MARS SRR-System wird in 2 Varianten eingeführt werden.

Die Variante 1 ist ein System, das mit einem Wechselaufbau auf einem „PickUp"-Kfz montiert ist, um eine hohe Mobilität sicherzustellen. Es besteht die Möglichkeit das Radarsystem bis zu einer Fahrgeschwindigkeit von 60 km/h zu betreiben.

Die Variante 2 ist ein System, welches auf einem 3-Bein montiert wird und somit einen Einsatz im urbanen Raum z.B.: auf Flachdächern und dergleichen sehr flexibel ermöglicht.

Das Radarsystem besteht aus 4 hochmodernen starren Full-Active Electronically Scanned Array (AESA)-Radarantennen, welche gemeinsam eine volle Rundumsicht ermöglichen. Das System ist auf eine mittlere Reichweite ausgelegt, wobei Flugobjekte mit einem sehr kleinen Radarquerschnitt (z.B.: Micro Drohnen) bis in einer kurzen Entfernung detektiert werden können.

Da das MARS SRR ein Software Defined Radar ist, besteht die Möglichkeit das Radarsystem an diverse Einsatzanforderungen zeitnah anzupassen und kann daher auch als Multi-Mission-Radar eingesetzt werden.

Grafik: MARS SRR, Bundesheer/Dion6

Einführung Libre-Office

Im Jahr 2025 ist das Thema der „digitalen Souveränität" sehr stark in das Interesse von Bürgern, Medien, Regierungen und öffentlichen Stellen gerückt.

Der Bereich IKT-Technik (IKTTe) als Provider der Infrastruktur vom Datacenter bis zum Endgerät, vom Truppenfunk bis zum Videokonferenzsystem und vom Konfigurationsmanagement bis zur Entwicklungsinfrastruktur legt seit je her, stets besonders darauf Wert, Unternehmensdaten auf eigenen Systemen zu verarbeiten und zu speichern. Als Mittel zur Zielerreichung wird sehr häufig Open Source Software eingesetzt. Die allgemeine Verfügung des Quellcodes „minimiert das Risiko, in Abhängigkeit von einzelnen Anbietern zur geraden genauso wie die Gefahr in politische Querelen verwickelt zu werden" wird schon 2020 in der Open Source Software Strategie der EU-Kommission für 2020 – 2023 als Vorteil angeführt. In diesem Sinne wurde 2025 der „Leitfaden für den Einsatz von Open Source Software in der Bundesverwaltung" durch das Bundeskanzleramt (BKA), Bundesministerium für Justiz (BMJ) und der Direktion 6 - IKT und Cyber insbesondere IKTTe erarbeitet und veröffentlicht. Der Leitfaden stellt eine fundierte zielgerichtete Information für IT-Verantwortliche der Bundesverwaltung zur Open Source Software dar!

Als konkretes umgesetztes Vorhaben zur digitalen Souveränität erlangte die Einführung von LibreOffice im BMLV/ÖBH sehr große nationale als auch internationale Anerkennung. Der Produktwechsel zu LibreOffice, nach über 30 Jahre, erzeugte viele Anfragen zum Projekt und zum Produkt. Für die Zusammenarbeit mit Externen wird, wenn es unbedingt erforderlich ist und technisch möglich ist, in Ausnahmefällen Microsoft Office eingesetzt.

LibreOffice wurde eingeführt, um die Unabhängigkeit des BMLV/ÖBH zu stärken und „zu funktionieren, wenn nichts mehr geht". Das Einsparen von Budgetmittel war nicht der Auslöser für das Vorhaben.

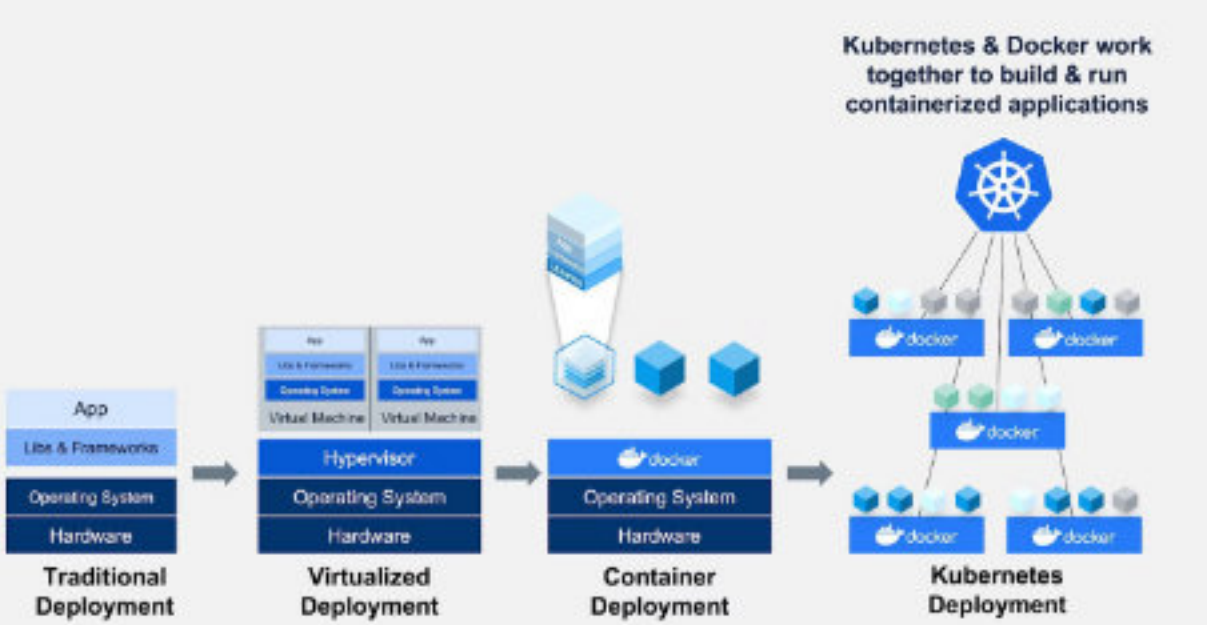
Für das BMLV/ÖBH war stets klar, dass für Wartung und Entwicklung kostenpflichtige Unterstützungsleistung erforderlich werden wird. In Summe wurden bisher etwa 5 Personenjahre in die Weiterentwicklung von LibreOffice investiert.

Alle Codebeiträge wurden als Open Source Code an das LibreOffice übergeben und werden heute von vielen Millionen von LibreOffice Nutzern verwendet.

Foto: LibreOffice Stand NFT25, Bundesheer/Dion6

LibreOffice Conference Budapest 2025 ELTE IK

Grafik: Logo LibreOffice Conferenzce, LibreOffice



Grafik: Cloud Plattform, Docker

Cloud Plattform

In der heutigen schnelllebigen Welt der Technologie spielt die Cloud Plattform eine zentrale Rolle, um Unternehmen flexibel, skalierbar und zukunftssicher aufzustellen.

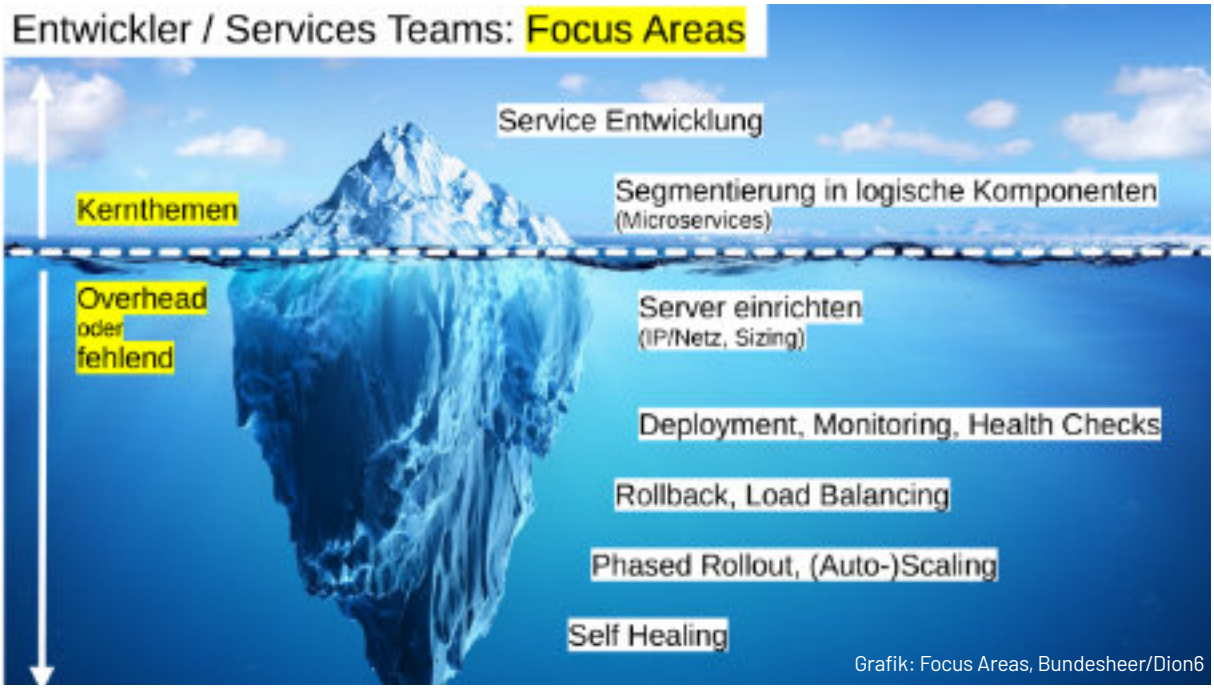
Ein zentraler Bestandteil dieser Entwicklung ist die Container-Technologie, die im Vergleich zu virtuellen Maschinen (VMs) zahlreiche Vorteile bietet.

Während Entwickler und Verantwortliche für Virtuell Machine-basierte Services von der Betriebssystemkonfiguration bis hin zur Lifecycle Prozessen der Applikation zahlreiche Fragestellungen zu beantworten haben, ermöglichen Container es sich ganz auf die Kernthemen der Applikation — in der nachfolgenden Visualisierung jene Punkte über der Wasseroberfläche — zu fokussieren.

Durch die Nutzung von Kubernetes als Container Orchestrator bzw. Cloud Plattform profitiert man von einer weitreichenden Standardisierung der Prozesse, wie etwa:

- Deployment, Update, und ggf. Rollback von Applikationsversionen
- Konfiguration und Change Management, vollständig deklarativ
- Observability: Logs, Metrics und Traces können zentral bereitgestellt werden
- Self-Healing bei Service Problemen: Restart von leichtgewichtigen Containern, eingebaute Status Checks, ...
- Self-Healing bei Infrastruktur Problemen: automatische Reaktion auf ausgefallene Kubernetes Nodes, sowie Scaling bei veränderter Nutzerlast.

Die erfolgreiche Implementierung von Cloud-Native-Lösungen, die positive Resonanz auf unsere Workshops und die kontinuierliche Weiterentwicklung der Cloud Plattform unterstreichen die erfolgreichen Schritte, die das ÖBH in Richtung einer zukunftssicheren IT-Infrastruktur unternommen hat.



KI@ÖBH-2025 - ein Rückblick

Im Bereich von Künstliche Intelligenz (KI) und Machine Learning (ML) stand das Jahr 2025 im Zeichen der Migration der laufenden Artificial Intelligence (AI) Services wie dem "AI chat", "AI translator" oder die "AI document assistance" auf neue, leistungsstarke Graphics Processing Unit (GPU)-Server speziell für künstliche Intelligenz.

Dabei ist es sinnvoll, sich auf die frei verfügbaren technischen Lösungen zu verlassen, die weit verbreitet und zuverlässig im industriellen Einsatz sind.

Das bringt allerdings einen wesentlichen technologischen Wandel mit sich, denn mit dem Blick auf die zukünftigen Anforderungen an die IT des ÖBH waren große Schritte in Richtung "cloud-native" Technologien und die "Kubernetes" Plattform nötig, die anhand der KI Services erprobt und festgelegt worden sind. Dies hat wesentliche Fortschritte mit wertvollem Wissensgewinn erbracht.

Fortgesetzte Aktualisierungen und die Hilfe für Mitarbeiter des Ressorts durch den "VBL-Chat", der aktuell 1396 Verlautbarungsblätter in natürlichsprachlicher Dialogform für alle im internen Netz erschließbar macht, haben dem verantwortlichen Team sowohl erfreuliche als auch hilfreiche Rückmeldungen eingebracht.

Damit ist der Blick nun auf die weitere Verbesserung und die Ermöglichung von Services zur Unterstützung der Mitarbeiter gerichtet.

Grafik: KI VErwendungen, Bundesheer/Dion6


Foto: BMLV/HBF

Militärisches Cyberzentrum

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

Das Jahr 2025 war für das MilCyZ geprägt von einer dynamischen Bedrohungslage im Cyberraum und einer Zunahme professioneller, KI-gestützter Cyberangriffe. Neue Angriffsvektoren wie personalisierte Phishing-Kampagnen, Supply-Chain-Angriffe und Ransomware mit Double-Extortion-Taktik, Zero-Day-Exploits, staatlich geförderte Cyberangriffe und Social Engineering wurden adressiert.

Unser Fokus stand daher in der kontinuierlichen Weiterentwicklung unserer Cyber-Verteidigungssysteme. Dennoch ist absehbar, dass die Herausforderungen im Jahr 2026 weiter zunehmen und uns der Umbau des Heeres auf ÖBH2032+ massiv fordern werden.

Die Teilnahme an internationalen Cyberübungen und die Fortführung der InnoVision-Eventreihe unterstrichen die Bedeutung von Teamwork, Innovation und strategischen Partnerschaften für die Bewältigung zukünftiger Herausforderungen im Cyberraum.

Die Aktivitäten des Cyber Rapid Response Teams (CRRT) haben einmal mehr unterstrichen, wie wichtig eine rasche und präzise Reaktion auf cyberspezifische Bedrohungen ist. Die Fortschritte im Bereich des technischen Fähigkeitenaufbaus in der Elektronischen Kampfführung zeigen, dass wir auch in diesem zentralen Bereich auf dem richtigen Weg sind.

Das MilCyZ wird sich auch 2026 auf eine proaktive Cyberresilienz konzentrieren, IT-Sicherheit konsequent in KI-Einführung und Cloud-Betrieb zu integrieren und adaptive Verteidigungsmechanismen mit menschlicher Aufsicht zu verbinden. Nur so kann die Sicherheit digitaler Infrastrukturen auch unter sich wandelnden Bedrohungen gewährleistet werden.

Cyber Exercises – Planung, Vorbereitung & Organisation

Im Jahr 2025 hat das Militärische Cyber-Zentrum nicht nur an einer Vielzahl von Cyber-Defence-Übungen teilgenommen, sondern zudem maßgeblich zur Planung, Organisation und Durchführung selbst beigetragen.

Diese Übungen waren entscheidend für die Vorbereitung auf zukünftige Herausforderungen und die Weiterentwicklung der Kompetenzen im Umgang mit Cyberbedrohungen. Darüber hinaus konnten hierbei wichtige Fähigkeiten für die weitere Verwertung innerhalb der Cyber Range ÖBH erarbeitet werden.

Grafik: LS25 Teilnehmer, Bundesheer/Dion6

Eine dieser Übungen, war die Cyber Coalition, bei welcher die Koordination und Zusammenarbeit zwischen der NATO, ihren Alliierten und Partnern im Mittelpunkt steht. Nach vielen Jahren wurde das Österreichische Bundesheer erneut zur Übung eingeladen und konnte maßgebliche Beiträge leisten.

Die Übung bietet Gelegenheit, spezifische Ziele im Bereich der Cyberraum-Operationen in einem Multi-Domain-Umfeld zu üben.

Durch die Kombination von technischen und nicht-technischen Koordinierungsaspekten, Prozessen und der Zusammenarbeit aller Teilnehmer können Fähigkeiten und Funktionalitäten der nationalen und multinationalen Cyber-Defence weiter verbessert werden.

Darüber hinaus wurde im Rahmen des KIRAS Forschungsprojekts „CONTAIN" ein Incident Response Framework für Cyber-Bedrohungen in transnationalen Lieferketten entwickelt. Zur Validierung und Verbesserung der Forschungsergebnisse wurde dieses im Rahmen einer Cyber Defence Übung erprobt.

Das Framework ermöglichte es, Strategien und Maßnahmen zur Bekämpfung von Cyberangriffen auf komplexe Lieferketten zu erarbeiten und zu testen. Die Ergebnisse tragen daher maßgeblich dazu bei, die Resilienz gegenüber transnationalen Cyberbedrohungen zu stärken.

Einen Kernbereich stellte die Teilnahme an der Locked Shields in drei der Organisationsteams dar.

Hierbei konnte der Beitrag für das Training von Blue Teams (Anm.: Defensive Cyber-Verteidungskräfte) von unterschiedlichen Funktionen erreicht werden: Green Team (Infrastruktur), Red Team (Angreifer) und Yellow Team (Situational Awareness). Die Übung bietet als die größte Live-Fire Cyber Defence Übung eine einzigartige Plattform, um die eigenen Fähigkeiten in stark umkämpften Umgebungen zu trainieren. Hierbei steht die Verteidigung einer fiktiven Nation und deren kritischen Infrastrukturen im Vordergrund.

Zudem wurde die jährliche Cyber Range Exercise (CRX25) des MilCyZ erstmalig in Kooperation mit der Cyber Range des Österreichischen Bundesheeres durchgeführt. Diese Übung bietet die Möglichkeit, die Expertise der eigenen Fachkräfte einzubinden und innovative Technologien in einer realistischen Umgebung zu testen. Die Veranstaltung eigener Cyber Defence Übungen ermöglicht es, gezielt auf die Bedarfe der Fähigkeitsplanung des MilCyZ einzugehen und diese zu verbessern.

Insgesamt führen die laufenden Teilnahmen an der Organisation von Cyber Übungen, die Fähigkeiten im Bereich Cyber-Defence ganzheitlich zu verbessern. Die enge internationale Zusammenarbeit, die Integration modernster Technologien und der Fokus auf realistische Szenarien haben die Voraussetzungen geschaffen, um zukünftigen Herausforderungen im Cyberraum erfolgreich begegnen zu können. Darüber hinaus entstehen durch diese internationale Form der Zusammenarbeit Kooperationen, welche über die reine Teilnahme als Training Audience weit hinaus gehen.

Übungs- & Einsatzinfrastruktur – Cyber Range & CRRT Kits

Für die Cyber Range ÖBH konnten 2025 erste Erfolge bei der Implementierung erzielt werden, wodurch die Grundlagen für eine zukunftsfähige Trainings- und Simulationsumgebung für den Cyberraum gelegt wurden. Zudem wurden die ersten Prototypen für Übungsvorhaben entwickelt und bereits in Übungsvorhaben, wie der Locked Shields und der Cyber Coalition, erprobt. Diese werden zukünftig für realistische Trainings- und Simulationsszenarien weiterentwickelt und eingesetzt.

Darüber hinaus konnten wichtige Synergien zwischen einsatzrelevanten Fähigkeiten und der Cyber Range identifiziert werden, wodurch die CRRT Toolkits als Einsatzinfrastruktur für verlegbare Einsätze der Cyber Defence weiterentwickelt werden konnten. Die Cyber Range kann hierdurch neben der Simulationsfähigkeiten der Cyber Defence, auch wichtige Akzente als ortsfestes Reachback setzen. Beide Systeme wirken somit gemeinsam und verbessern hierdurch die Cyber Defence Fähigkeiten des ÖBH maßgeblich. Ein erster Prototyp dieses Aufbaus konnte auch bereits im Rahmen der Locked Shields 2025 erfolgreich erprobt werden. Eine Evaluierung dieses Aufbaus konnte das Potenzial einer interdisziplinären Vorgehensweise hervorheben und unterstreicht die Bedeutung von Kooperation im Rahmen der Cyber Defence. Hierdurch konnten Fähigkeiten im MilCyZ gebündelt und entsprechende Herausforderungen effizient bewältigt werden.

Die Cyber Range ÖBH ist damit nicht ausschließlich als Trainingsumgebung etabliert, sondern zudem die Grundlage für die Cyber-Waffen-Automatisierung und Resilienzsimulationen im Cyber Raum. Diese Fähigkeiten liefern neben fachspezifischen Spezialtrainings, auch Möglichkeiten der schnellen Einsatzvorbereitung, der Analyse potentieller Bedrohungen sowie Gefechtstestungen defensiver Maßnahmen im Cyberraum. Durch diese Entwicklungen konnte die Resilienz des BMLV/ÖBH weiter gestärkt werden, was angesichts der stetig zunehmenden Bedrohungen im Cyberraum von besonderer Bedeutung ist.

Grafik: Übungs- & Einsatzinfrastruktur, Bundesheer/Dion6


Foto: CSA-Partnerschaft, BMLV/HBF

Partnerschaft Cyber Security Austria

Die Partnerschaft mit Cyber Security Austria wurde heuer im Rahmen der IKT-Sicherheitskonferenz in Dornbirn mit der Urkundenüberreichung feierlich besiegelt. Gemeinsamen Aktivitäten im kommenden Jahr sieht man mit Freude entgegen.

Prozesslandkarte MilCyZ

Die Prozesslandkarte (PLK) ist im MilCyZ ein Managementinstrument, das wesentliche Prozesse in einer übersichtlichen Darstellung abbildet. Dadurch werden Zusammenhänge, Wechselwirkungen sowie Verantwortlichkeiten klar zugeordnet.

Als Orientierungshilfe dient die PLK um Optimierungspotentiale zu erkennen und die strategische Unternehmenssteuerung zu unterstützen. Prozesse gewährleisten, dass wiederkehrende Aufgaben einheitlich und effizient durchgeführt werden.

Dies ist in der Cybersicherheit entscheidend, um auf Bedrohungen schnell und systematisch reagieren zu können.

Ein zusätzliches Mapping auf internationale Standards wie das NIST 2.0 Framework schafft Synergien zu anderen Bereichen sowie die Identifikation von Lücken.

InnoVision Fokusgruppenmeetings 2025

Im November 2024 fand das InnoVision-Kick-off-Event des Militärischen Cyberzentrums statt, das den Grundstein für diese erfolgreiche Reihe legte. 2025 wurden zwei Fokusgruppenmeetings durchgeführt, die sich jeweils auf unterschiedliche Schwerpunkte der Cyberverteidigung konzentrierten:

Mai: Fokus auf das militärische Cyberlagebild der Zukunft

Im Mai standen die aktuellen Entwicklungen und Herausforderungen im Bereich des Cyberlagebilds im Mittelpunkt. Experten aus Wirtschaft, Industrie und Bedarfsträgern des BMLV und weiteren sicherheitsrelevanten Ressorts wie BKA und BMI diskutierten Lösungsansätze, um an innovativen Ideen für den Umgang mit den zunehmenden Cyberbedrohungen zu erarbeiten. Die Keynote von FH-Prof. Mag. Wolfgfang RÖMER, einem renomierten österreichischen Innovationsexperten, regte zum Nachdenken an und inspirierte die Teilnehmenden über den Tellerrand zu schauen und zu denken

November: Fokus auf Security Operations Center (SOC)

Am 17. November 2025 lag der Fokus auf dem Security Operations Center (SOC), konkret einem mobilen, hierarchischen SOC. Die Teilnehmer tauschten sich in aktiven Arbeitsgruppen zum Thema aus und führten spannende Diskussionen zu den präsentierten Fragestellungen.


Foto: Innovision, Bundesheer/Dion6

Foto: Innovision Arbeitsgruppen, Bundesheer/Dion6

Prof. Dr. Thomas MONZ, einer der führenden europäischen Quantenforscher, von der Uni Innsbruck leitete mit einer spannenden Keynote in das Thema ein. Auch hier wurden innovative Ideen entwickelt, die den Weg für zukünftige Forschungsprojekte ebnen sollen.Das Herzstück der InnoVision liegt in ihrem strukturierten und kollaborativen Ansatz. In den Fokusgruppen-Workshops erarbeiten Kleingruppen, bestehend aus Experten verschiedener Bereiche an spezifischen Fragestellungen.

Foto: Innovision Ausarbeitung, Bundesheer/Dion6

Anschließend stellt jede Gruppe, die gezielt als potentielles Konsortium zusammengestellt wurde, ihre Ergebnisse in einem kurzen Pitch vor. Diese Pitches fassen die Kernidee der Gruppe zusammen und machen sie für alle Teilnehmer verständlich und nachvollziehbar.

Die entwickelten Lösungsansätze aus dem InnoVision-Fokusgruppenmeeting werden im Nachgang detaillierter ausgearbeitet.

Bis Mai 2026 soll zu jeder Idee ein detailliertes Exposé entstehen, das als Grundlage für die Umsetzung von einem Forschungsprojekt dient.

Wie geht es weiter?

Im Juni 2026 erwartet uns eine InnoVision, die voller innovativer Ideen und spannender Präsentationen zu den Themen "Cyberlagebild" und "Security Operations Center (SOC)" steckt.

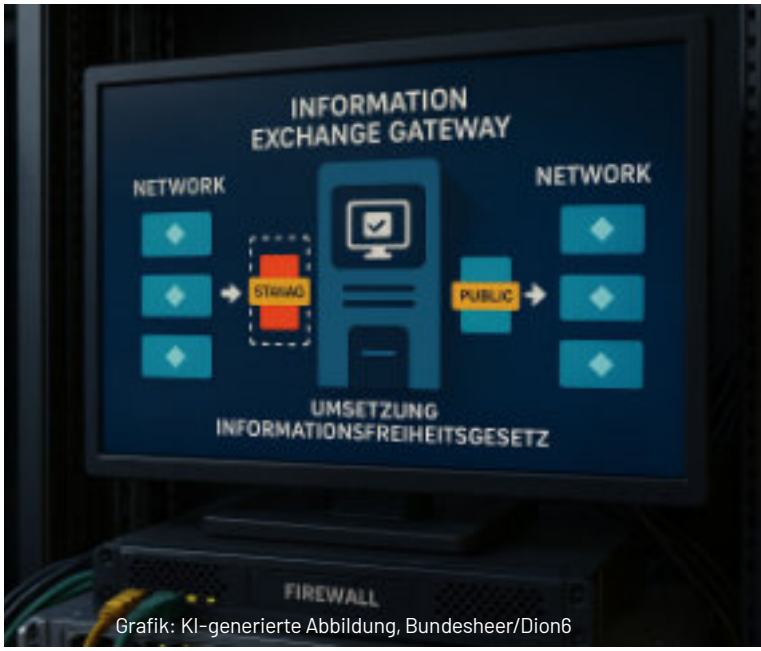
Eine ausgewählte Fachjury entscheidet über die Siegerprojekte und somit über die nächsten Forschungsprojekte für den gezielten Fähigkeitenaufbau im Bereich Cyberverteidigung.

IFGIEG mit Labeling nach STANAG

Durch das am 1. September 2025 in Kraft getretenen Informationsfreiheitsgesetz (IFG) ergeben sich auch neue Herausforderung für IT-Systeme. Einerseits soll Bürgerinnen und Bürgern der Zugang zu diesen Informationen erleichtert werden, während gleichzeitig sensible Daten weiterhin geschützt bleiben müssen. Um diesen Anforderungen gerecht zu werden, wurde ein spezielles Information Exchange Gateway (IEG) konzipiert, welches durch unterschiedliche Schutzmechanismen, wie bspw. Segmentierung, Policy Enforcement und Transportverschlüsselung, als zusätzliche Sicherheitsebene innerhalb der IKT-Architektur des BMLV fungiert. Das vollständig in Eigenentwicklung realisierte "IFGIEG" stellt zudem eine standardisierte Schnittstelle dar, die anhand von integriertem Labeling Dokumente automatisiert nach Schutzbedarf prüft und dadurch den Informationsfluss kontrollieren kann. Zum Einsatz kommen dabei vertrauenswürdige Sicherheitslabel gemäß NATO-Standardisierungsabkommen (STANAG 4774/4778), wodurch auch die Anforderungen an einen militärischen Datenaustausch der Zukunft erfüllt werden können.

Schadcode-Erkennung durch KI- & ML-Analysen

Die Multi Anti Virus Engine (MAVE) ist eine Eigenentwicklung des MilCyZ und wird im BMLV als eines der zentralen Sicherheitselemente zur Prüfung des Datenverkehrs auf Schadsoftware eingesetzt. Seit der Version 4.0 werden dabei zusätzlich zu klassischen signaturbasierten und heuristischen Verfahren auch Künstliche Intelligenz (KI) und Machine Learning (ML) Technologien zur Erkennung und Abwehr von Schadsoftware eingesetzt. Dieser Ansatz wurde im vergangen Jahr weiter ausgebaut. Neue KI- und ML-gesteuerte Analysen ermöglichen eine bessere Bewertung von potentiell gefährlichen Dateien und mittels Deep Neural Networks werden Modelle trainiert die Malware aufgrund einer holistischen Repräsentationen erkennen können. Darüber hinaus wurde in Kooperation mit der FH St. Pölten das Projekt SCRIPTS-GPT initiiert, dessen Ziel es ist, potenziell schädliche Makros in Dokumenten zu identifizieren und zu beschreiben. Im Mittelpunkt stehen dabei CPU-optimierte Large-Language-Models, die auch auf leistungsschwacher Hardware zuverlässig und effizient betrieben werden können.



Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Cybersecurity: Anpassungen und Fortschritte in der militärischen Einsatzumgebung

Die Neuausrichtung der Sicherheitsanforderungen

Im letzten Jahr wurden die Fähigkeiten zur Ausarbeitung systemspezifischer Sicherheitsanforderungen neu auf die Herausforderungen der militärischen Einsatzumgebung ausgerichtet. Durch Erkenntnisse aus aktuellen internationalen Konflikten wurde deutlich, dass auch das Österreichische Bundesheer auf neue Bedrohungen reagieren muss. Die Anpassung von IKT- (Information and Communication Technology) und OT- (Operational Technology)-Systemen sowie IT-gestützten Waffensystemen an diese Herausforderungen ist eine der wichtigsten Voraussetzungen für die erfolgreiche Einsatzbereitschaft.

Ein besonderer Fokus liegt dabei auf der Stärkung der IKT-Architektur im Einsatzraum. Systeme wie das Tactical Communication Network (TCN), die Einführung des PANDUR-Systems oder die Modernisierung der IT-getützten 35mm FLAk bilden die Grundlage für zuverlässige und gegen Cyberangriffe resiliente Systeme.

Die Rolle des milCyZ bei der Systementwicklung

Die aufwändigen Beitragsleistungen in der Konzeption der durch das IKT- und Cybersicherheitszentrum zu entwickelnden Systeme haben maßgeblich dazu beigetragen, ein einheitliches Gesamtbild der IKT-Sicherheitsarchitektur zu schaffen. Durch diese Bemühungen können neue Systeme und Dienstleistungen effizient entwickelt werden, bei denen Sicherheit von Beginn an geplant und integriert ist. Dieser Ansatz unterstützt nicht nur die Entwicklung neuer Technologien, sondern auch die langfristige Sicherheit der militärischen Infrastruktur.

Sicherheitsexperten im Einsatz: Penetration Testing und Compliance Checks

Die Sicherheitsexperten des Österreichischen Bundesheers haben im letzten Jahr wieder wichtige Beiträge zur Stärkung der Verteidigungsfähigkeit der IKT-Systeme geleistet. Durch Penetration Testing, Compliance Checks, Akkreditierungen und sicherheitstechnische Abnahmen konnten zahlreiche Sicherheitslücken und Gefährdungen aufgedeckt und behoben werden. Die Ergebnisse dieser Bemühungen tragen maßgeblich zur erfolgreichen Einsatzbereitschaft und zur Sicherheit der Streitkräfte bei.

Die Zukunft der Cybersecurity im militärischen Kontext wird weiterhin von der Fähigkeit abhängen, sich an neue Herausforderungen anzupassen und innovative Lösungen zu entwickeln. Das Österreichische Bundesheer ist mit den getroffenen Maßnahmen gut auf diesen Weg vorbereitet.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Locked Shields

Seit 2012 nimmt das MilCyZ fast jährlich an der Cyberübung „Locked Shields" teil. Organisator ist das NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Die Übung gehört zu den weltweit anspruchsvollsten im Bereich der Cybersicherheit. 2025 verlegten für die Teilnahme rund 40 Cyber- und InfoOps-Experten der Partner Niederlande und US National Guard sowie rund 110 Experten aus Österreich für 2 Wochen an einen Standort in Wien.

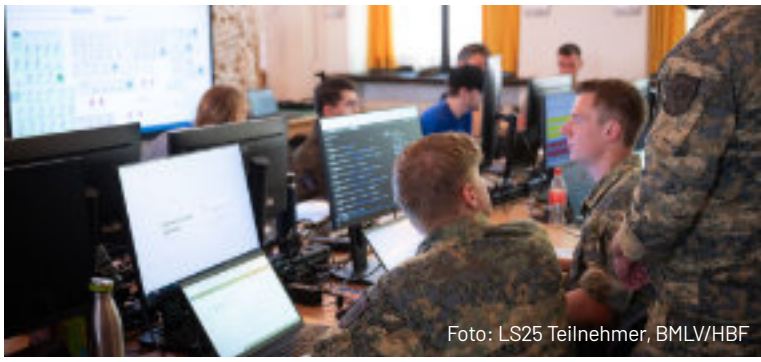


Foto: LS25 Teilnehmer, BMLV/HBF

„Locked Shields" zielt darauf ab, die Reaktionsfähigkeit und Verteidigungsstrategien gegen reale Cyberbedrohungen zu testen. Dabei werden groß angelegte Cyberangriffe auf kritische Infrastrukturen simuliert, bei dem über 2000 Cyberexperten aus 40 Nationen in 20 Teams gegeneinander antreten.

Die Blue Teams müssen als Verteidiger ihre Infrastruktur schützen und Services verfügbar halten, während sie gleichzeitig versuchen, die Angreifer zu identifizieren und deren Aktivitäten zu stoppen. Die Herausforderung bestand darin, vielfältige 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. Nur so kann eine schnelle und effektive Abwehr gewährleisten werden.


Foto: LS25 Internationaler Teilnehmer, BMLV/HBF

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.

Das Red Team (mit Unterstützung von Österreichischen Experten), das die Angriffe simulierte, nutzte eine breite Palette von Taktiken, von klassischen Angriffen bis hin zu komplexeren, schwer erkennbaren Bedrohungen wie Zero-Day-Exploits. Das AUT-NLD-USA-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 PsyOps/InfoOps) im Griff zu haben und auf etwaige Medienanfragen zu reagieren sowie proaktiv im Informationsraum zu agieren.

Die Teilnahme an „Locked Shields" ermöglichte den Teilnehmern 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 Cyberherausforderungen noch besser vorbereitet zu sein. Erstmalig kam dabei das Cyber-Rapid-Response-Toolkit Österreichs zum Einsatz.

Aktivitäten des CRRT (Cyber Rapid Response Team)

Schnelle Reaktionsfähigkeit als Schlüssel

CRRTs sind spezialisierte Einheiten, die im Falle schwerwiegender, komplexer und hochdynamischer Cyberangriffe schnell und effektiv reagieren. Dabei kann im Anlassfall etwa kritische Infrastruktur geschützt und die Folgen von Cyberbedrohungen zu minimiert werden. Diese Fähigkeit ist von entscheidender Bedeutung. Das PESCO CRRT-Netzwerk (von dem Österreichische Spezialisten Teil sind) hat in den vergangenen Jahren bei mehreren Einsätzen und Übungen unter Beweis gestellt, wie schlagkräftig es ist. Seit 2024 leistet auch Österreich wertvolle Beiträge dazu.

Einsätze und Übungen des CRRT im Jahr 2025

- Teilnahme an der Cyber-Übung „Cyber Fortress" in Luxemburg im Rahmen von PESCO CRRT
- Teilnahme an einer Spezialausbildung für „Industrielle Kontrollsysteme" in Belgien, im Rahmen von PESCO CRRT

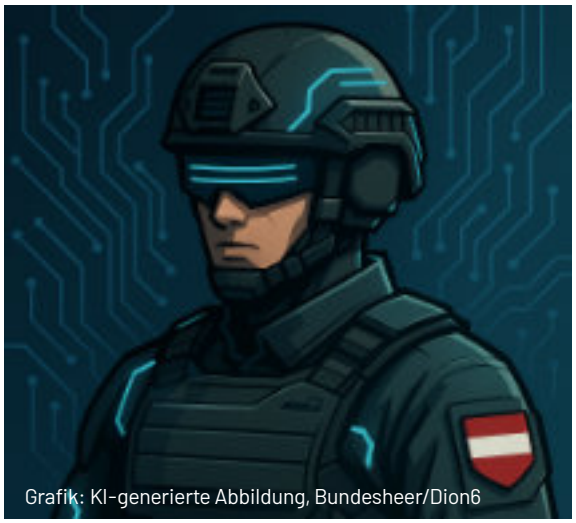
Innerhalb Österreichs / in eigenen Systemen gab es 2025 glücklicherweise keinen Anlassfall für das CRRT. Es wurde jedoch mehrfach eine Aktivierung überlegt.


Grafik: KI-generierte Abbildung, Bundesheer/Dion6

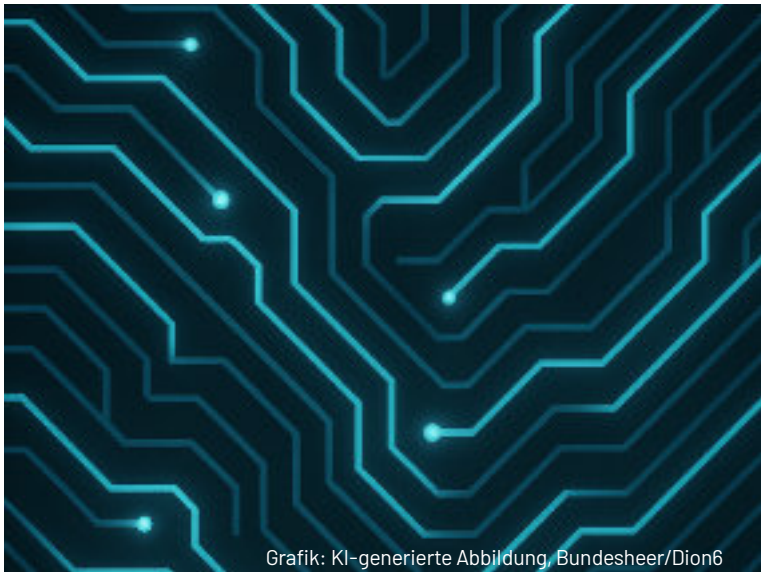
Qualifiziertes Personal und spezialisierte Ausrüstung

Die Wirksamkeit eines CRRT hängt nicht nur von einer schnellen Reaktionszeit ab, sondern auch und vor allem von der Qualität des eingesetzten Personals und der verfügbaren Ausrüstung. Die erforderliche Spezialausrüstung ist inzwischen beschafft worden und steht den Teams als IOC zur Verfügung. Dennoch bleibt die Rekrutierung und Ausbildung von hochqualifizierten Cybersicherheitsexperten eine Herausforderung. Die Organisationspläne hinken dem Bedarf hinterher, was eine angemessene Besetzung der notwendigen Planstellen verzögert. Dies reduziert auch die Schlagkraft der Ausrüstung, da diese derzeit aufgrund knapper Ressourcen in die vorgesehene und erforderliche Einsatzkonfiguration gebracht werden kann.

Die Mitgliedschaft im EU PESCO CRRT stärkt nicht nur die Fähigkeit des Österreichischen Bundesheeres, auf Cyberangriffe schnell und gezielt zu reagieren. Sie fördert darüberhinaus die europäische Zusammenarbeit in der Cybersicherheit. Moderne Ausrüstung ist inzwischen verfügbar, doch bleibt die Gewinnung und Ausbildung qualifizierter Experten eine zentrale Herausforderung. Die Fortschritte in diesem Bereich sind entscheidend, um die Ambitionen des Österreichischen Bundesheeres in der Cyberdomäne langfristig umsetzen zu können. Vor allem aber, um bestmöglich auf den nächsten Ernstfall vorbereitet zu sein.



Grafik: KI-generierte Abbildung, Bundesheer/Dion6



Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Technischer Fähigkeitenaufbau in der Elektronischen Kampfführung

Die Abteilung Unterstützungszentrum EloKa (UZEloKa) ist durch die eingesetzte und sich rasch ändernde Technologie konfrontiert und begegnet den Herausforderungen dieses technisch umfangreichen Aufgabengebietes mit einem bestmöglichen Fähigkeitenaufbau. Dieser stützt sich unter anderem auf laufende Ausbildungen, regelmäßige Teilnahme an militärischen Übungen und eine internationale fachliche Kooperationen.

Die Waffengattung „Elektronische Kampfführung" (EloKa) des österreichischen Bundesheeres, in internationalen Kontext auch „Electronic Warfare" (EW), umfasst militärische Maßnahmen unter Ausnutzung der elektromagnetischen Strahlung.

Nationale Ausbildungen für Messgeräte in den Technologiebereichen Kommunikation und Radar für Signalanalysen stellen eine wichtige Grundlage dar, um dann in der Folge zur Verbesserung der eigenen EloKa-Systeme beizutragen.

Die sich rasch ändernde Technologie erfordert zusätzlich eine internationale Zusammenarbeit, um gegen die, weltweit in Einsatzräumen verwendeten Bedrohungen und Techniken, vorgehen zu können.

Die nun mehrjährige multinationalen Kooperation als Partnernation in zwei Arbeitsgruppen der "Aerospace Capability Group 3 on Survivability" in der "NATO Air Force Armaments Group" ermöglicht einen einsatzrelevanten Austausch auf einer fachlich technischen Ebene. 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.

Die "Sub-Group 2 on Self-Protection Measures for Joint Services Airborne Assets" beschäftigt sich mit dem Selbstschutz von Luftfahrzeugen.
Das UZEloKa konnte bei unterschiedlichen multinationalen Übungen und internationalen Veranstaltungen einsatzrelevante Erkenntnisse gewinnen. Eine der vielen Aktivitäten ist die Teilnahme an der internationalen technischen Veranstaltung „Waveform Development Olympiad“ (WDO) bei der der Arbeitsfokus auf dem Wissensaustausch zu neuen Bedrohungen und den erforderlichen Gegenmaßnahmen, Erfahrungsaustausch zu EloKa-Systemen und der Verbesserung der Mess- und Testverfahren sowie der Signal- und Bedrohungsanalyse.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6


Foto: BMLV/HBF

IKT-Betrieb

Leiter IKTBetr:
HR Mag. Peter BINDER, M.Sc. MSc

Der demografische Wandel stellt alle IT Organisationen vor tiefgreifende Veränderungen. Mit dem Ausscheiden der Babyboomer geht wertvolles Erfahrungswissen verloren. Dokumentationen sind oft lückenhaft, Wissen steckt in Köpfen statt in Systemen, wodurch riskante Abhängigkeiten entstehen. Hier ist die Leitung gefordert. Wissen muss gesichert werden und Strukturen müssen zeitgerecht angepasst werden.

Gleichzeitig verschärft der Fachkräftemangel die Lage. Die jüngere Generation ist kleiner, digitaler geprägt und erwartet moderne Tools, flexible Arbeitsweisen und sinnvolle Aufgaben. Routinetätigkeiten wirken oftmals wenig attraktiv. Der Generationenwechsel erfordert daher mehr als Neueinstellungen, es braucht organisatorische und technologische Erneuerungen.

Hier wird Künstliche Intelligenz zum Schlüssel. Sie kann Wissen erfassen, strukturieren und für alle verfügbar machen. Intelligente Systeme unterstützen weniger erfahrene Mitarbeitende und kompensieren Wissensverlust. Zugleich automatisiert KI Standardaufgaben, etwa durch Chatbots, Self Services oder Ticketklassifizierung. Das steigert die Effizienz, entlastet Teams und schafft Raum für anspruchsvollere Tätigkeiten.

Mit der Einführung von KI verändern sich auch die Rollenbilder: Automatisierung, Wissensmanagement und Datenkompetenz werden zentral. Der Abschied erfahrener Mitarbeitender eröffnet Chancen zur Modernisierung. Entscheidend ist, den Wandel zeitgerecht, aktiv und gemeinsam zu gestalten, hier muss Vertrauen aufgebaut werden, Ängste müssen minimiert und Standards etabliert werden, Weiterbildung ist zu fördern.

So entsteht gemeinsam ein moderner, resilienter und attraktiver Fachbereich, bereit für die neuen Herausforderungen.

IT-Sicherheit & Frequenz Schlüsselwesen (ITSihFrqSchlW)

Die Abteilung ITSihFrqSchlW leistete auch im Jahr 2025 als Dienstleister einen wesentlichen Beitrag, für die Bedarfsträger in Österreich, für die Unterstützung bei Übungen im In- und Ausland, sowie bei der Einführung von Systemen, Umbauarbeiten bei bestehenden Anlagen und im Rahmen der Supporttätigkeit durch die einzelnen Referate über ihr Fachwissen und persönlichem Einsatz einen wesentlichen Beitrag, um den Herausforderungen gerecht zu werden und einen wesentlichen Beitrag zur Erreichung der gesteckten Ziele zu erreichen.

Sehr viele Tätigkeiten laufen automatisiert im Hintergrund ab – ohne viel Aufsehen zu erregen und sind zur Norm geworden. Sei es das einspielen von Updates/Upgrades, löschen von Einträgen, Änderungen sowie Fehlerbehebungen in Systemen und diversen Infrastrukturen – all diese Tätigkeiten sind Aufgaben welche täglich und/oder in regelmäßigen Abständen abgearbeitet werden. Die Verteilung von Geheimunterlagen gem. den betrieblichen Vorgaben, die Anpassung und Evidenthaltung der zu beteilenden Dienststellen, sowie die rasche Zuteilung von Ersatzschlüsselunterlagen bei Bloßstellung von Schlüsselunterlagen ist ein Teil der umfassenden Tätigkeiten, welche in das Tagesgeschäft der Abteilung fallen.

Eine außergewöhnliche Aufgabe in diesem Jahr war die fachmännische Demontage von über 200 Stück Kryptogeräten, um diese einer thermischen Vernichtung zuführen zu können. Durch diese Tätigkeit konnten mehrere tausend Euro eingespart werden – welche sonst an eine Firma zu bezahlen gewesen wäre.

Berechtigungsmanagement: Austausch der Chipkarten auf 700.000 Serie

Mit Erhalt der neuen Chipkarten der Serie 700000 Ende Dezember 2024 wurde umgehend mit der Initialisierung der 40000 Chipkarten (CK) begonnen und Anfang Jänner 2025 startete die Umstellung auf die neue Serie. Die dezentralen Ausstellungsstellen/Dienststellen wurden so rasch als möglich mit der neuen Serie beteilt, um den Austausch der fehleranfälligen alten Serie vor Ort voranzutreiben.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Im Bereich Berechtigungsmanagement wurden alle Änderungsanträge, Änderungswünsche und abgegebene defekte CK im Rahmen des Tagesgeschäftes durch die neue Serie ersetzt.

Die Zielsetzung, alle Bedarfsträger so rasch wie möglich auf die neue Chipkartenserie umzustellen, konnte bis Ende Juli 2025 abgeschlossen werden. Gleichzeitig zum Austausch auf die neue Serie erfolgten auch im Chipkartenverwaltungsprogramm (ZBS) die erforderlichen Orgplananpassungen, Neuanlagen von Verwaltungsstellen, Umgliederungen, Abgabenvorschreibungen, Änderungen der OrgPosNr, Eintragungen bei den Kennungen, um die Chipkarten auch ordnungsgemäß zuweisen zu können. All diese Tätigkeiten konnten trotz eines Personalengpasses durchgeführt werden und seit Ende August wurde, nach Zugang eines Militärperson auf Zeit - Charge (MZCh) mit der Rücknahme, Kontrolle und Inaktivsetzung der abgelieferten CK der Serie 600.000 begonnen. Ziel dieser Tätigkeit ist es, bis Ende des Jahres alle CK der Serie 600.000 aus dem System genommen zu haben.

Frequenzmanagement

Neben dem Tagesgeschäft der Frequenzanforderungen, sowie der daraus resultierenden Frequenzzuteilung für Übungen im In- und Ausland durch Teile ÖBH bzw. ausländischer Übender in Österreich, stellte die Trilaterale Übung „TRIAS 25" am Truppenübungsplatz Allentsteig, die größte Herausforderung in der Frequenzkoordinierung in diesem Jahr dar.

Übung TRIAS 25

Durch die Schweizer Armee erfolgte ein Frequenzantrag für die Teilnehmer aus der Schweiz sowie Deutschland gem. den internationalen gängigen Abläufen und Normen bei der NARFA AUT (National Radio Frequency Agency), disloziert beim IKTBetr.

Die Teilnehmer aus Österreich beantragten die benötigten Frequenzen direkt beim IKTBetr gem. den intern geltenden Richtlinien.

Der Umfang der Anträge für die verschiedenen Fu- Systeme umfasste Frequenzanforderungen über das gesamte Frequenzspektrum. Nach Vorlage der ersten Anträge, basierend auf der Übungsanlage, den verschiedenen Fu-Systemen sowie den technischen Parametern und den in Österreich für den im Übungsraum Allentsteig zur Verfügung stehenden Frequenzen erfolgte eine Überarbeitung der Frequenzanträge durch die Schweiz in Zusammenarbeit mit der NARFA AUT. Die Probleme der Verfügbarkeit von Frequenzen zur Abdeckung des Bedarfes für die Fu-Systeme beschränkte sich im wesentlichen auf den VHF- Bereich. Nach anpassen und ausreizen sämtlicher technischer Möglichkeiten und viel Rechenarbeit, konnten die Plannungs- Tools der Fu- Systeme mit den notwendigen Frequenzen beteilt werden, um, wenn auch eingeschränkt, die erforderlichen Fu- Netze bilden zu können.

Für die restlichen Fu- Systeme konnten aufgrund der technischen Parameter und der geringeren Anzahl von Frequenzen eine rasche und unkomplizierte Zuteilung getroffen werden.

Durch die gute Zusammenarbeit, Fachwissen im Frequenzmanagement, sowie technische Systemkenntnis konnte mit dem Frequenzmanager der Schweizer Armee die Frequenzplanung angepasst und der Fernmeldeeinsatz sichergestellt erden.

Folgende Fu- Systeme in den verschiedenen Frequenzbereichen waren im Rahmen der Übung eingesetzt und wurden mit den nötigen Frequenzen beteilt:

- HF-Funk im Übungsraum, sowie eine HF-Rückwärtsverbindungen in die Schweiz
- VHF-Truppenfunk im Fixkanalbetrieb sowie im Hoppinbetrieb
- VHF-Funk im Flugfunkbereich
- UHF-Funk
- Richtfunk im Übungsraum
- Mehrere Drohnensysteme in verschiedenen Frequenzbereichen

Foto: Übung TRIAS 25, BMLV/Daniel Trippolt

NDA (National Distribuion Authority):

Die NDA (National Distribuion Authority) ist verantwortlich für die Verteilung und Nachweisführung von Kryptomaterial der NATO innerhalb des ÖBH.

Unter dem Begriff Kryptomaterial werden sowohl Kryptogeräte als auch Kryptoschlüssel verstanden. NATO-Kryptogeräte werden als CCI (Controlled Cryptographic Item) eingestuft und unterliegen daher besonderen Bestimmungen hinsichtlich Verteilung, Verwahrung und Transport.

Ein wesentlicher Beitrag zur Auftragserfüllung der NDA war im Jahr 2025 die Durchführung einer österreichweiten Gesamtinventur, die vier Monate in Anspruch nahm und ohne besondere Vorkommnisse abgeschlossen werden konnte.

Von März bis April 2025 führte die NDA die jährliche Schulung des COMSEC Personals durch. An der Schulung 2025 nahmen an den Standorten Wien, Zeltweg, Salzburg und Hörsching insgesamt 12 Crypto Custodians und 70 COMSEC User teil.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Betriebsführung

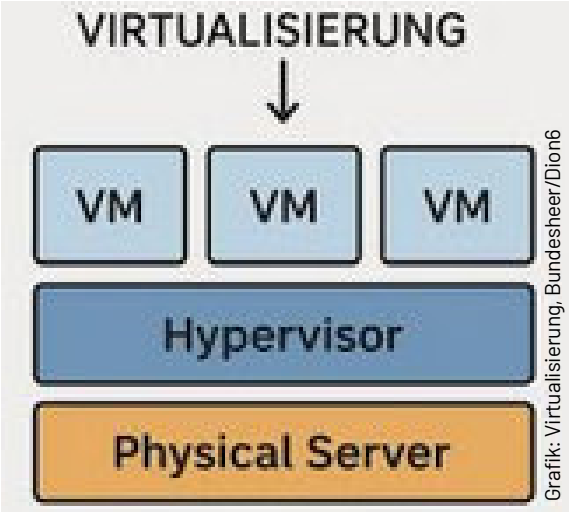
Zentrales Backupsystem

„IBM Storage Protect" (ehemals IBM Spectrum Protect) ist eine Software für Datensicherung und Wiederherstellung, Aufbewahrung und Wiederverwendung im Bereich VM's, Datenbanken, Anwendungen, Dateisystemen, SaaS-Workloads und Containern, welche seit den 90iger Jahren im österreichischen Bundesheer eingesetzt wird. Daten können in cloudbasierten Objektspeichern und lokalen Speichern (zB.: IBM Storage FlashSystem) und auf physisches Band kopiert werden.

Das Produkt kommt zur Datensicherung/Wiederherstellung in der Direktion 6 - IKT und Cyber für unsere Produktion-, Test- und Entwicklungssysteme, sowie auch im Abwehr- und Heeresnachrichtenamt zum Einsatz. Um einen reibungslosen Betrieb gewährleisten zu können, bedarf es eines laufenden aufwendigen Upgrades des Systemes. Im Jahr 2025 konnten 2 Mitarbeiter des Referates IKTBetrieb/Betriebsführung/Systemorganisation und Betriebstechnik IT (OrgBetrTelT) das Abwehramt erfolgreich auf die neue Version umstellen.

IBM Storage Protect im SMN

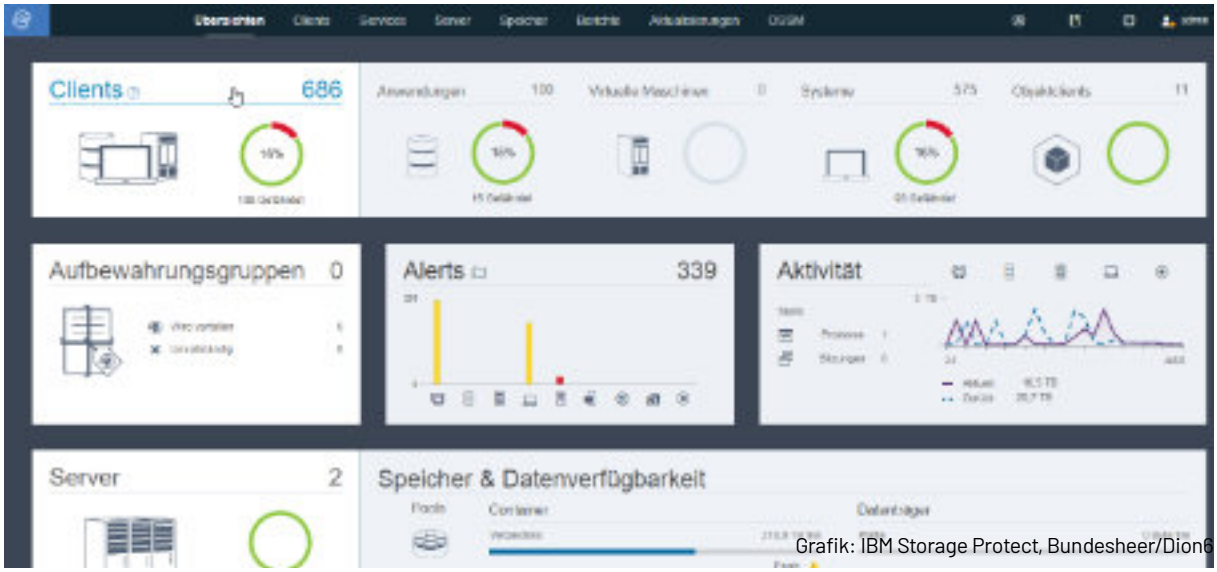
Liegenschaftsserver dienen u.a. als Fileserver und auch „pass through server" zu den Services.



Grafik: Virtualisierung, Bundesheer/Dion6

Aufgrund gewachsener Anforderungen ist diese Technologie basierend auf einer alten Systemsoftware (RHEL) veraltet und eine neue Infrastruktur war damit unabdingbar. Im Jahr 2025 konnten einige Mitarbeiter aus dem Referat IKTBetrieb/BetrFü/SysOrgBetrTelT bei der Umstellung auf eine neue Serverstruktur, aufgebaut auf einem physischen Server und darauf existierende mehrere virtuelle Komponenten, zu einem Teil mitgestalten.

Dies war ein notwendiger Schritt und gewährleistet alle weiteren Updates von RHEL und auch anderen SW-Paketen.



Grafik: IBM Storage Protect, Bundesheer/Dion6

Benutzerbetreuung

Das Jahr 2025 war für die Abteilung Benutzerbetreuung wieder geprägt von mannigfaltigen Herausforderungen, welche durch den Zusammenhalt und die Kompetenz der Mitarbeiterinnen und Mitarbeiter allesamt erfolgreich bewältigt werden konnten.

Hierbei stachen vor allem die Schlagwörter TCN (Tactical Communications Network) und TKV (Telekommunikationsverbund) heraus.

Im Bereich TCN unter der Federführung Referat BenBeIT-West und Teilmitwirkung Benutzerbetreuung IT-Süd (BenBeIT-Süd) wurden folgende TCN-Teilprojekte umgesetzt und durchgeführt:

TCN-Umstellung

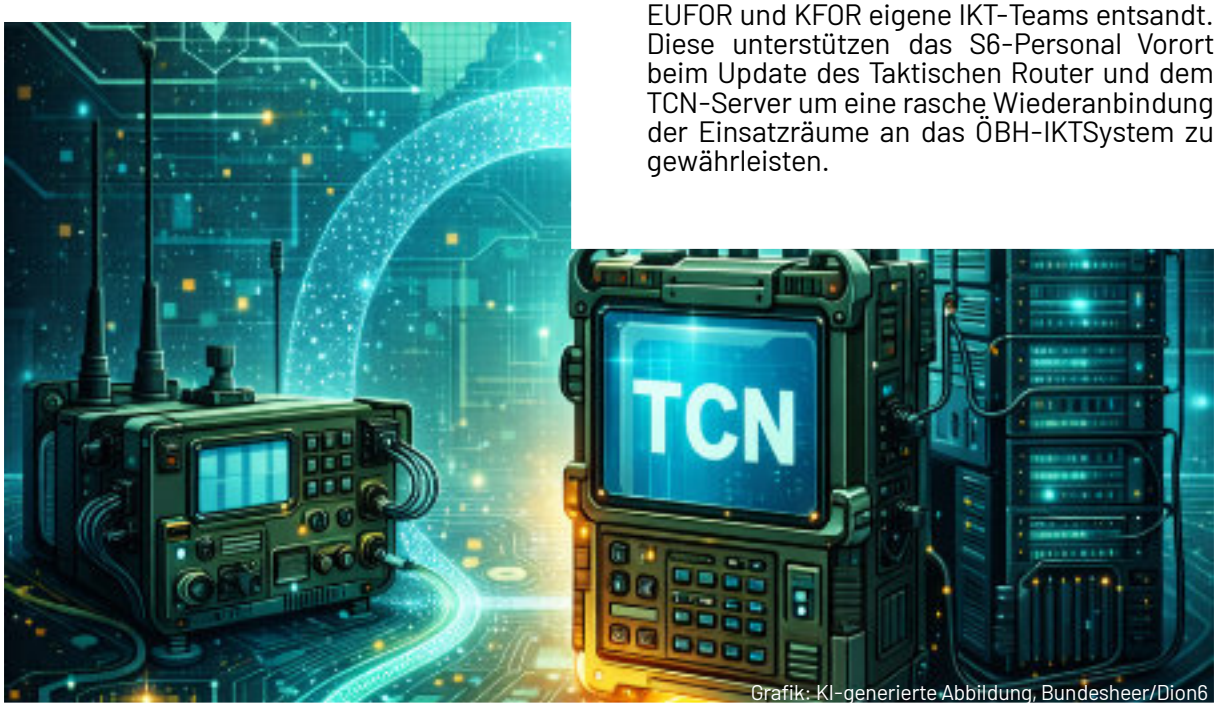
Im ersten Halbjahr 2025 wurden die Einsatzlokationen EUFOR Bosnien, UNIFIL Libanon und KFOR Kosovo unter der technischer Leitung BenBeIT-West auf das neu im ÖBH eingeführte TCN-System umgestellt. Dabei wurden alle Netzwerkkomponenten durch TCN taugliche Geräte ersetzt und sämtliche Netzwerk-Verteiler adaptiert.

Als besondere Herausforderung galt die Aufrechterhaltung der ständigen Einsatzfähigkeit der vor Ort eingesetzten Truppen. Dies konnte Basierend auf einer sorgfältigen Planung und Koordinierung letztlich auch gelingen. Hinsichtlich der neu eingesetzten Technologie und der mit hergehenden Unerfahrenheit der Anwender, wurde ebenso ein großes Augenmerk auf die technische Dokumentation und die Schulung der eingesetzten Truppe gelegt. Letztendlich ist es gelungen den Auftrag mitsamt allen technischen, zeitlichen, klimatischen und organisatorischen Herausforderungen zu erfüllen.

TCN 3A Update

Beim bislang größten Update der noch jungen Geschichte des TCN Systems, konnte BenBe (federführend IT-West) einen großen Beitrag zum Gelingen beisteuern. Während ein Groß der Geräte durch die Truppe upgedatet wurde, koordinierte BenBeIT-West zeitlich vorgegebene Abläufe und erwies sich erneut als kompetenter Ansprechpartner bei technischen und organisatorischen Herausforderungen. Speziell die Auslandslokationen stellten eine große Herausforderung dar.

Hierzu wurden in die Einsatzräume UNIFIL, EUFOR und KFOR eigene IKT-Teams entsandt. Diese unterstützen das S6-Personal Vorort beim Update des Taktischen Router und dem TCN-Server um eine rasche Wiederanbindung der Einsatzräume an das ÖBH-IKTSystem zu gewährleisten.



Grafik: KI-generierte Abbildung, Bundesheer/Dion6

TCN-Systemtest nach Update 3A:

Nach dem erfolgreichen Abschluss des Software-Updates wurden die Systemstabilität sowie die technische und betriebliche Einsatzbereitschaft umfassend überprüft. Im Zuge einer breit angelegten Testphase befanden sich mehr als 100 Systeme gleichzeitig im Netz und waren über unterschiedlichste Anbindungsvarianten im gesamten Bundesgebiet miteinander vernetzt. Dabei wurden an die 99 Tests zu Funktionalität, Bandbreitenauslastung und Systemstabilität durchgeführt. Die gewonnenen Erkenntnisse wurden ausgewertet und dokumentiert. Es wurden auch noch Systemfehler gefunden, welche nun durch die Vertragsfirma weiter analysiert werden. Die BenBeIT-West war dabei ein Bestandteil der Systemtest-Leitung und wirkte bei der Erstellung der Testabläufe und der Durchführung der System-Testung mit.

Im Rahmen der Einführung des BMS (Battle Management System des ÖBH) kam es für BenBeIT-Süd zu einer ersten Ausbildung in der Anwendung „Sitaware HQ" mit einem Ausblick auf Funktionalität und Möglichkeiten des Software-Pakets.

Umstellung auf TKV

Das Projekt TKV wird flächendeckend in ganz Österreich umgesetzt und bedeutet die Ablöse des mittlerweile in die Jahre gekommenen NVÖ (Nebenstellenverbund Österreich).

Hierbei werden in einem ersten Takt die Liegenschaften LAN-konsolidiert, anschließend die Anwender mit den neuen Softphones (telefonieren über das SMN-Notebook) bzw. einem neuen Hardphone ausgestattet. Liegenschaften, in welchen sich Elemente der Benutzerbetreuung oder Vermittlungen befinden, werden ebenfalls auf jeweils eigene Softwareprodukte umgestellt. Erste Elemente der Benutzerbetreuung wie das Service Schwerpunkt MTM in Linz und das Service Schwerpunkt Internet in Innsbruck wurden bereits umgestellt, sowie ein Vermittlungsstandort in Klagenfurt.

Ziel ist es, bis Jahresende 2025 sämtliche Referate der Benutzerbetreuung sowie alle Vermittlungen ö-weit in den TKV eingebunden zu haben.

Große Standorte wie Wien, Graz und Salzburg bedürfen aufgrund ihrer Komplexität besonderer Vorbereitung und werden Zug um Zug umgestellt.

Abschluss Serverrollout

Nachdem im Jahr 2024 sämtliche inländischen Server durch neue, aktuelle und leistungsstarke Hardware ersetzt wurden, wurden im ersten Halbjahr 2025 die Server der Auslandslokationen ebenfalls ausgetauscht, womit das Serverrollout als erfolgreich beendet betrachtet werden kann. Ebenso wurden sämtliche Server auf die aktuelle Version upgedated.

LibreOffice für BMLV ELAK und Übernahme von 1st-Level-Support

Im Zuge der bevorstehenden Ablöse von Microsoft Office durch das Opensource-Produkt LibreOffice wurde dieses in einem ersten Schritt verpflichtend für die Erstellung von Dokumenten in BMLV ELAK implementiert. Hierbei wird der 1st-Level-Support durch die Referate der Benutzerbetreuung gestellt, welche als Anlaufstelle für Fragen, etwaige Probleme und Verbesserungsvorschläge fungieren. Dies dient der Vorbereitung und Einarbeitungsmöglichkeit der Anwenderinnen und Anwender bis zum Zeitpunkt der Ablöse durch LibreOffice. Sämtliche Anfragen konnten hier entweder einer sofortigen Lösung zugeführt werden bzw. wurden als Verbesserungsvorschlag weitergeleitet.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

First-Level Support ELAK

Der ELAK stellt die zentrale digitale Plattform für die Aktenverwaltung im BMLV dar. Dadurch wird ein sicherer, zuverlässiger und effizienter Betrieb ermöglicht. Gleichzeitig trägt der ELAK maßgeblich zur Vereinfachung und Beschleunigung der behördlichen Kommunikations- und Arbeitsprozesse bei.

Durch regelmäßige-Updates werden kontinuierlich Benutzerwünsche umgesetzt sowie technische und funktionale Modernisierungen eingeführt. Diese Maßnahmen tragen wesentlich zu einer effizienteren und benutzerfreundlicheren Arbeitsweise bei.

Sämtliche Anfragen und Anliegen konnten hierbei erfolgreich beantwortet und zu einem positiven Abschluss gebracht werden.

Zusätzlich zum Support des BMLV ELAK unterstützt das SSPIT ZentrS die Anwenderinnen und Anwender bei Anfragen zum Stammportal und hilft auch im Rahmen des 1st-Level-Supports bei Fragen beim Erstellen von Intranetseiten (CMS).

Service Schwerpunkt Eurofighter (SSP IT EF)

Wie schon im Jahr 2024 hat sich das Team des SSP IT EF den Aufgaben im Zuge des Ground-Supports erfolgreich gestellt. Der Service Schwerpunkt Eurofighter erbringt hierbei einen wichtigen Beitrag zum erfolgreichen Flugbetrieb des Eurofighters.

So wurden u.a. zur Entlastung der Controller Militärflugleitung Zeltweg eine FOS (Forward Operation Site) in Linz Hörsching und in Klagenfurt eingerichtet und in weiterer Folge betrieben.

Ebenso unterstützte der Service Schwerpunkt Eurofighter das Luftzielschießen „Air to Air Gunnery mittels der Bereitstellung einer Rückwärtseinbindung des Eurofighter-Netzes ESS mit UTNC, welches in Grosseto (Italien) stattfand.

Im Herbst 2025 findet die Übung Tigermeet (Portugal) im Rahmen einer NATO Übung statt. Dazu haben die Vorbereitungen bereits im Jänner 2025 begonnen.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Service Schwerpunkt IT Mail Terminmanagement

Das Team des SSP MTM betreute im Jahr 2025 rund 17.000 Benutzer bei allen Anliegen bzw. Problemen rund um HCL Notes SMN und Internet-Mailing (Webmail). Der Schwerpunkt lag dabei auf der Unterstützung der Anwender bei Fragen zur Bedienung von Notes, Passwortproblemen, zu Mail- und Kalenderfunktionen.

SSP IT Internet & Mail Terminmanagement

Das Team des SSP Internet betreute im Jahr 2025 sämtliche Anwender des BMLV im In-und Ausland und im Rahmen von Einsätzen, Übungen und Veranstaltungen in den Themenbereichen Internet, BitBox, SMN-Mobile, Mailing, WLAN, mobile Endgeräte (iPhone/iPad), und verschlüsselte Smartphone-Kommunikation (Silentel/Threema).

Während des gesamten Jahres wurden umfangreiche Tests (teilweise mit dem Hersteller) und Abstimmungen mit anderen Ministerien hinsichtlich der geplanten Ablöse Silentel/Threema durchgeführt.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6


Foto: BMLV/HBF

Institut für Militärisches Geowesen

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

Das Jahr 2025 war für das Institut für Militärisches Geowesen, durch den Abgang des Leiters Brigadier Dr. Teichmann und durch die Betrauung mit der Führung des Stellvertreters, eine Weichenstellung.

Einerseits wurden die Agenden für externe Schnittstellen (nationale sowie internationale Partner) übergeben und andererseits wurde der Führungswechsel intern im MilGeo-Dienst auf strategischer sowie operativer Ebene abgeschlossen. Das bedeutet, dass sich die Ausrichtung des Fachdienstes - bedingt durch den Motivenbericht „zentraler Provider“ und des neuen MilGeo Fachkonzeptes – auf die Entwicklung von geforderten Fähigkeiten verlagert.

In diesem Zusammenhang sei hier zum Beispiel die Flexibilität zur Lagebildverdichtung mittels Drohnen oder die rasche Bereitstellung von MilGeo-Daten für C4ISR-Systemen genannt.

Eine weitere strategische Entscheidung für den MilGeoD ist das Herauslösen des NavWar-Anteils aus dem OrgPlan des IMG. Mit diesem Schritt ist der Weg frei für den Aufbau einer eigenen Abteilung Space Services.

Mit viel Freude und Engagement blickt das gesamte IMG auf die Herausforderungen des kommenden Jahres 2026.

Verleihung des Großen Ehrenzeichens für Verdienste um die Republik Österreich

Am 08.01.2025 wurde auf Entschließung des Herrn Bundespräsident Dr. Alexander Van der Bellen an Herrn Hofrat Mag. Werner Heriszt, IMG/Referatsleiter Daten, Systeme & Services das Große Ehrenzeichen für Verdienste um die Republik Österreich verliehen.

Die feierliche Überreichung nahm der mit der Führung betraute Leiter IKTCySihZ und vormalige Leiter des IMG, Bgdr Dr. Friedrich Teichmann, im Rahmen der Eröffnung der diesjährigen MilGeo-Fachdienstbesprechung in Wien vor.

Foto: Übergabe Großes Ehrenzeichen, Bundesheer/Dion6

SKEV Winterspiele Maria Alm 15.- 17.01.2025

Vom 15.01. - 17.01.2025 fanden in Maria Alm die 56. Winterspiele des SKEV (Sportklub des Bundesamtes für Eich- und Vermessungswesen / BEV) statt, zu denen das IMG im Zuge der bereits 17-jährigen bestehenden Partnerschaft ebenfalls eingeladen war.
Um die wichtigen Kontakte zum Bundesamt für Eich- und Vermessungswesen weiter zu stärken, nahmen insgesamt drei Teilnehmer des IMG an den Bewerben teil und unterstützten die Organisation mit einem Löffelgericht im Rahmen der Öffentlichkeitsarbeit!

Dabei konnte die Mannschaft des IMG den 1. Platz im Skilanglauf klassisch Mannschaftswertung erringen.

Foto: SKEV Winterspiele, Bundesheer/Dion6

ÖK50 - Neue Kartengrafik

Die vom Bundesamt für Eich- und Vermessungswesen (BEV) gemeinsam mit dem Institut für Militärisches Geowesen (IMG) herausgegebene Österreichische Karte 1:50 000 - UTM (ÖK50) ist das topographische Grundkartenwerk Österreichs. Im Laufe der Jahre wurde die ÖK50 zwar immer wieder leicht angepasst, aber Produktion und Zeichenschlüssel wurden nie grundlegend verändert.

Die zeitgemäßen Anforderungen an die Nutzung der kartographischen Modelle in verschiedenen analogen und digitalen Medien können mit diesen rasterbasierten Daten nicht mehr adäquat erfüllt werden. Zudem ist die Notwendigkeit für effizientere Prozesse in der digitalen Produktion, die höhere Genauigkeit und die raschere Aktualisierung der Daten nur durch einschneidende Erneuerungen erreichbar.

Das Kartographische Modell 1:50 000 mit dem daraus abgeleiteten Kartenwerk ÖK50 wurde daher umfassend neu konzipiert und die gesamte Kartenerstellung im BEV auf modernste Verfahren umgestellt. Der weiterhin hohe Informationsgehalt der staatlichen Kartenwerke sowie eine verbesserte Lesbarkeit sollen auch in Zukunft das effiziente Arbeiten mit der Karte als Planungsgrundlage sichern und die Orientierung im Gelände garantieren.

Grafik: ÖK50, Bundesheer/Dion6

Das neue kartographische Vektormodell für den Maßstab 1:50 000 (KM50-V) beinhaltet mit diversen Attributen versehene Kartenobjekte und wird nun wie die kartographischen Folgemodelle in einem Geo Informationsservice (GIS) geführt. Überdies erfolgt die Erstellung des KM50-V auf Grundlage der Objekte des Digitalen Landschaftsmodells (DLM) in einem hochgradig automatisierten Verfahren, die sehr arbeitsintensiven Abläufe der Kartenherstellung wurden in einen automationsunterstützten digitalen Prozess übergeführt.

Bilaterales Arbeitstreffen Austria - Italy

Das Istituto Geografico Militare (IGM) aus Florenz / Italien beehrte das IMG mit einem mehrtägigen Arbeitsbesuch in Wien.

Von 11. bis 13. März 2025 wurde ein bilaterales Treffen mit der Delegation aus Italien abgehalten. Gegenstand dieser Besprechung waren neben dem allgemeinen Informationsaustausch im Fachbereich MilGeo noch Themenschwerpunkte wie die zukünftige strategische Ausrichtungen der MilGeo-Dienste, moderne 3D-Visualisierungsmöglichkeiten und die Bearbeitungen von Militärischen Landesbeschreibungen. Zusätzlich wurde die bestehende bilaterale Vereinbarung diskutiert und mögliche Adaptierungen eingeleitet. Es wurde auch eine Gegeneinladung der Italiener an das IMG ausgesprochen.

AFDRU-Einsatz in der Slowakei im März 2025

Nach einem Ausbruch der Maul- und Klauenseuche in einem Rinderzuchtbetrieb im grenznahen Bereich zur Slowakei hilft die österreichische Katastrophenschutzeinheit Austrian Force Disaster Relief Unit (AFDRU) mit Personen-, Kfz- sowie Infrastrukturdekontamination.

Das IMG stellte am 25. März 2025 dem Kontingent Satellitenbilder, Lage- und Anfahrtskarten zur Verfügung und unterstützte bis 7. April 2025 den Einsatz durchgehend mit einem Reach-Back Element.

AFDRU-ÜBUNG auf SARDINIEN (ITA)

Die AFDRU-Elemente des GFFF-V (Ground Forest Fire Fighting with Vehicle; Waldbrandbekämpfung am Boden mit Fahrzeugen) übten seit 8. April 2025 im multinationalen Verbund auf der italienischen Insel Sardinien.

46 Männer und Frauen - darunter ein Offizier des IMG, zwölf Fahrzeuge und 250 Tonnen Gerät machten sich am 5. April 2025 auf den Weg zur EU-Zertfizierungsübung für die Fähigkeiten zur Waldbrandbekämpfung – ein weiteres spezialisiertes Element im europäischen Katastrophenschutzmechanismus.

Das IMG stellte auch hier vorgestaffelt der übenden Truppe umfangreiches Kartenmaterial zur Verfügung und unterstützte während der einwöchigen Übung mit einem Reach-Back-Element in Wien.

Foto: AFDRU-Übung, Bundesheer

Foto: AFDRU-Truppe, Bundesheer

Navigation Warfare Test- und Versuchsreihe

Von 2. bis 6. Juni 2025 lud das Referat Navigation zur Navigation Warfare Test- und Versuchsreihe am Truppenübungsplatz Seetaler Alpe ein.

Diese regelmäßig stattfindenden Übungswochen dienen der praktischen Erprobung und Weiterentwicklung offensiver u0nd defensiver Maßnahmen im Bereich Navigation Warfare (NavWar). Dabei werden Stör- und Täuschsysteme (Jamming & Spoofing) getestet, neue Verfahren validiert und bestehende Fähigkeiten unter realitätsnahen Bedingungen überprüft.

Foto: NavWar-Testreihe, Bundesheer/Dion6

Wargame "Führungsüberlegenheit" 2025 - Leistungsschau IMG

Im Zuge des Wargames "Führungsüberlegenheit" Anfang Juli 2025 hatte auch das IMG die Möglichkeit der obersten militärischen Führung des Bundesheeres und dem Führungs- und Fachpersonal aus dem Führungsgrundgebiet 6 seine Fähigkeiten und Fähigkeitsvision für 2032+ darzustellen.

Dies erfolgte im Rahmen einer Leistungsschau, in der unterschiedliche bestehende Fähigkeiten vorgeführt und relevante Zukunftstechnologien aus der Industrie ausgestellt wurden. Das IMG konnte dabei seine bestehenden interaktiven und immersiven Produkte zur 3D-Geländedarstellungen inklusiv des Nutzungsprozesses von BORIS, VRANZ und ALOIS präsentieren.

Kampfmittelsuche und Blindgängerdokumentation am TüPl Lizum/Walchen (TüPl LW)

Seit nun mehr 10 Jahren unterstützt das IMG das Projekt Kampfmittelsuche und Blindgängerdokumentation am TÜPl LW. Durch eine fundierte digitale Dokumentation mittels Geographischem Informationssystem (QGIS) werden die abgesuchten Flächen und sämtliche Blindgängerfunde mit zahlreichen Zusatzinformationen (Attributen) räumlich dokumentiert.

Die Dokumentation dient im Anschluss dem Kommandanten für die Bewertung der Flächen in Rote, Gelbe und Grüne Zonen um so die Sicherheit während militärischer Nutzung und touristischer Nutzung (83 km Wanderwege und 45 km Skirouten) zu gewährleisten.

Foto: TüPl LW, Bundesheer/Dion6


Foto: GWD Abschlussmarsch, Bundesheer/Dion6

Orientierungsmarsch der GWD des IKT&CySihZ

Mit vollem Einsatz und hoher Motivation sind die Grundwehrdiener des IKT- & Cybersicherheitszentrums des Einrückungstermines 02/2025 unter Leitung von Frau Oberleutnant Deak sowie Unterstützung vom Institut für militärisches Geowesen zum letzten Mal zu einer Übung im Gelände ausgerückt. Dieser Abschlussmarsch stellte nicht nur einen bedeutenden Teil der körperlichen Ausbildung dar, sondern förderte auch den Zusammenhalt und das kameradschaftliche Miteinander innerhalb der Gruppe.

Die Rekruten, von denen mittlerweile die meisten bereits zum Gefreiten befördert wurden, hatten den Auftrag, im Rahmen eines Orientierungsmarsches in Gruppenstärke von Payerbach Reichenau/ Hirschwang über den Knappenhof auf dem Törlweg das Otto-Schutzhaus zu erreichen.

2. Basislehrgang Space & Security 2025

Von 30. Juni bis 4. Juli 2025 fand an der FüUS die zweite Ausgabe des Basislehrgangs Space & Security im Rahmen des Truppenoffizierslehrgang (TrOLG) der Militärischen IKT-Führung (Mil-IKTFü) statt. Ergänzend nahmen auch Vertreterinnen und Vertreter der Direktion 2 / Luftraumüberwachung (LRÜ), der FüUS selbst, des Referats Navigation sowie des TÜPl Bruckneudorf teil. Erstmals wurde der Kurs im Pilotversuch auch ministerienübergreifend geöffnet. Dadurch war auch das Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI) vertreten.

MilGeo-Übung MERCATOR

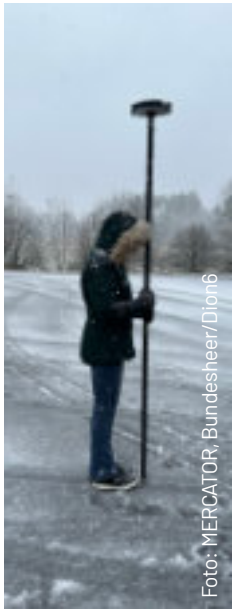


Foto: MERCATOR, Bundesheer/Dion6

Im November 2025 fand die MilGeo-Übung MERCATOR 2025 des IMG im Raum ALLENSTEIG statt. Ziel dieser Übung war die Erstellung dreier Roadbooks für Haupt- und Alternativ-Strecken zwischen Bahnhof WURMBACH und UTA STEINBACH, die Erstellung von Detaildarstellungen des Bahnhofes, der UTA und der Brücke über den TAUERBACH, sowie der schriftlichen Ausarbeitung einer Regionsbeschreibung des WALDVIERTELS.

Während der Erhebungsphase wurden die beiden Geo Support Teams des IMG durch einen Drohnentrupp der Heerestruppenschule unterstützt, wodurch in weiterer Folge Luftbildkarten und 3D-Modelle erstellt werden konnten. Zeitgleich zu den Erhebungstrupps im Raum ALLENTSTEIG wurde durch ein Reachback-Element zeitnahe zur Datenerhebung bereits Geoprodukte erstellt.

Die Erkenntnisse aus der MERCATOR 2025 steigern die qualitativen und quantitativen Fähigkeiten und Fertigkeiten des IMG im Bereich der kleinräumigen Lagebildverdichtung. Dieses Wissen fließt in die Gestaltung der Übungsvorhaben des IMG im Jahr 2026 ein und bilden das Fundament der Milizübung im Herbst 2026.

LEO2VLEO geht in die Umsetzung

Am 22. Juli 2025 fand bei der Europäischen Verteidigungsagentur (EDA) in Brüssel das Kick-off-Meeting zum Projekt „LEO2VLEO – Military Crisis Response Satellite Constellation" statt. Mit diesem offiziellen Projektstart wurde ein bedeutender Meilenstein für die europäische Sicherheits- und Verteidigungspolitik im Bereich Weltraumtechnologie gesetzt. Das EDA Cat.B Forschungsprojekt LEO2VLEO ist eine Initiative der EDA in Zusammenarbeit mit den Verteidigungsministerien der Niederlande und Österreich. Ziel ist die Entwicklung, den Bau, und der Betrieb einer militärischen Satellitenkonstellation, welche die Fähigkeit besitzt, aktiv zwischen dem Low Earth Orbit (LEO) (ca. 500 km Höhe) und dem Very Low Earth Orbit (VLEO) (ca. 300 km Höhe) zu manövrieren.

European Union Military Geospatial Capability Board - Meeting in Salzburg

Das diesjährige European Union Military Geospatial Capability Board (EUMGCB) - Meeting wurde vom 03.09. bis 05.09.2025 in der Schwarzenbergkaserne abgehalten. Veranstalter dieses Meetings war der EUMS (European Military Staff) unter der Leitung von Oberstleutnant Ilka Ocker.

Insgesamt waren 51 Teilnehmer von Mitgliedsstaten der EU, von Organisationen aus der Geodatenbranche sowie NATO-Verbänden anwesend. Der gewonnene Überblick des aktuellen Standes anderer Nationen und Organisationen in Bezug auf Fortschritte in der Geodatenakquise und -verarbeitung sowie der kommunikative Austausch des IMG mit diesen Organisationen und Staaten war sehr aufschlussreich und wertvoll. Das IMG war neben der Teilnahme am Meeting für die Organisation des Events und der Schaffung einer gemütlichen Atmosphäre sowie funktionierenden Rahmenbedingungen zuständig.

Besuch des Herrn Generalsekretär (HGS)

Am Donnerstag, den 09. Oktober 2025, besuchten Herr Generalsekretär Dr. Arnold Kammel und Frau Kommissär Mag. Anna-Maria Roth das Institut für Militärisches Geowesen (IMG). Ziel des Besuchs war die Einweisung des Herrn Generalsekretärs in die Tätigkeiten des IMG. Das IMG bedankte sich herzlich bei HGS Dr. Kammel und Frau Kmsr Mag. Roth für ihren Besuch und das Interesse an den Tätigkeiten und Projekten des Instituts.

Tag der Schulen 2025

Beim diesjährigen Tag der Schulen am 22. Oktober 2025 am Wiener Heldenplatz war auch das IMG mit vollem Einsatz für den Bereich Space Services des Österreichischen Bundesheeres im Einsatz.

An ihrem Stand gelang es den beiden, vielen neugierigen Schülerinnen und Schülern einen spannenden Einblick in die Welt der Space Services zu geben – von den zentralen Aufgaben bis hin zur Bedeutung des Weltraums für das Bundesheer. Das große Interesse und die vielen Fragen zeigten, wie faszinierend dieses Thema für junge Menschen ist.

Lehrgang Tief- und Großbohrlochsprengungen

Von 20.10. bis 31.10.2025 fand der Lehrgang Tief- und Großbohrlochsprengungen an der Heerestruppenschule (HTS)/Insititut der Pioniere (InstPi) mit sechs Teilnehmern statt. Zur Ausbildung gehören neben der Sprengtechnik auch das Erwerben von Grundkenntnissen der Geologie sowie das Bestimmen von Gesteinseigenschaften im Feld.

Das IMG unterstützte das Ausbildungsvorhaben mit der Abhaltung von Unterrichten zu den Themen Militär-, Ingenieurs- sowie Hydrogeologie und vermittelte theoretische und praktische Kenntnisse der Gesteinsbestimmung.

Foto: Tief- und Großbohrlochsprengungen, Bundesheer/Dion6

Führungsunterstützungsbataillon 1

Kommandant FüUB1: Obst Ernst BERTHOLD, MSD

Ein Jahr des Erfolgs und der Innovation.

Während die Zeit unaufhaltsam voranschreitet, möchte ich auf die bemerkenswerte Reise zurückblicken, die wir im Jahr 2025 gemeinsam unternommen haben. Es war ein Jahr, geprägt von bedeutenden Erfolgen, Innovationen und steigender Einsatzbereitschaft. Das Führungsunterstützungsbataillon 1 hat nicht nur die Erwartungen erfüllt, sondern sogar übertroffen und damit ein solides Fundament für zukünftige Unternehmungen geschaffen.

Im abgelaufenen Jahr haben wir unsere IT-Infrastruktur erfolgreich modernisiert und somit die Effizienz und Sicherheit erhöht. Die Einführung des neuen verlegbaren Fernmeldesystems TCN (Tactical Communikation Network) ist abgeschlossen und die restlichen Komponenten des ausgeschiedenen Systems IFMIN (integrierte Fernmelde Infrastuktur) sind bereit zur Rückgabe und Verwertung. Dieses Projekt war von zentraler Bedeutung, um unsere Systemlandschaft zu optimieren und sicherzustellen, dass wir an der Spitze der technologischen Entwicklung bleiben.

Im Mittelpunkt dieser Erfolge stand das Personal unseres Verbandes, die Soldaten und Soldatinnen des Führungsunterstützungsbataillon1. Jedes einzelne Mitglied hat mit Engagement und Fachwissen maßgeblich dazu beigetragen, Herausforderungen zu meistern und Ziele zu erreichen.

Das Projekt Großkaserne Villach hat Fahrt aufgenommen, der Rohbau ist fertiggestellt, die neue Zufahrt ist im Bau befindlich und die Fertigstellung des Projektes mit 2028 ist realistisch.

Im kommenden Jahr stehen wir vor neuen Herausforderungen. Wir werden unter anderem die Planungen für die Integration einer völlig neu aufzustellender Kompanie für Elektronische Kampfführung vorantreiben, um unsere Fähigkeiten weiter zu stärken.

Dieses Jahr war für das FüUB1 in vielerlei Hinsicht ein sehr forderndes. Zusammengefasst kann jedoch resümiert werden, dass die gestellten Aufträge abgearbeitet und die für 2025 gesteckten Ziele erreicht wurden.


Foto: BMLV/HBF

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.

30. Jahre Partnerschaft

Am 16.05.25 fand am Rathausplatz in Villach die Jubiläumsfeier der 30 jährigen Partnerschaft unseres Bataillons mit der Stadt Villach statt. Die Partnerschaft des FüUB1 (damals Fernmeldebataillon 1) wurde am 09.05.95 durch den damaligen Bataillonskommandanten Oberst Günther Janda mit dem Bürgermeister von Villach Helmut Manzenreiter begründet.

Ziel dieser Partnerschaft ist die Stärkung der gegenseitigen Beziehungen zwischen militärischen und zivilen Organisationen sowie die Förderung von gegenseitigem Verständnis der Aufgaben und Tätigkeitsbereichen der Partnerorganisation. Durch das Zusammenwirken von Bundesheer, Wirtschaft und öffentlicher Hand soll das Vertrauen und die Akzeptanz der militärischen Landesverteidigung erhöht werden.

Um den partnerschaftlichen Charakter der Veranstaltung besonders zu betonen wurde als musikalische Einstimmung ein Platzkonzert der Militärmusik Kärnten unter der Leitung von Oberst Dietmar Pranter durchgeführt.

Beim militärischen Festakt waren neben den Soldaten des Bataillons auch Traditionsverbände aus dem regionalen Umfeld mit angetreten.

Als militärisch Höchstanwesenden konnten wir den Militärkommandanten von Kärnten Brigadier Mag. Philipp Eder, bei uns begrüßen.

Als zivilen Höchstanwesenden konnte der Landtagspräsident Ing. Reinhart Rohr bei der Veranstaltung beiwohnen.

Sowohl der Kommandant des FüUB1, Oberst Ernst Berthold MSD, als auch Bürgermeister Günther Albel betonten in ihren Ansprachen die positiven Synergieeffekte dieser fruchtbaren Partnerschaft.

Der Militärkommandant betonte in seiner Rede insbesondere die Nachhaltigkeit und die Relevanz von Werte in einer solchen Partnerschaft und die Wichtigkeit diese innerhalb einer sich dem Wertewandel zuwendenden Gesellschaft, zu bewahren.

Als Höhepunkt der Veranstaltung wurden gegenseitig Partnerschaftsgeschenke ausgetauscht und dem Bürgermeister wurde aufgrund seiner wohlwollenden Verdienste um das Bataillon die Auszeichnung „Ehrenfunker“ verliehen.

Anschließend an den Festakt luden der Bürgermeister und der Bataillonskommandant auf Kostproben aus der Gulaschkanone ins Rathaus ein.

Foto: Partnerschaftsurkunde, Bundesheer/Dion6


Foto: Richtfunkverbindung, Bundesheer/Dion6

Übung DÄDALUS 2025

Das Weltwirtschaftsforum findet vom 20.01. bis einschließlich 25.01.25 im idyllischen Bergort Davos statt. Hier treffen sich die Mitglieder der Stiftung, aus den Bereichen der Politik, Wirtschaft, Wissenschaft und Medien um über aktuelle globale Fragen zu diskutieren.

Aufgrund der Grenznähe von Davos, erging auch diese Jahr das Ersuchen der Schweiz die Überwachung des österreichischen Luftraums im betroffenen Gebiet zu verstärken.

Aufgrund dieses Gesuches stellt das österreichische Bundesheer mehr als 1.000 Soldaten, 11 Flächenflugzeuge und 9 Hubschrauber bereit. Diese sorgen für die Sicherheit bei der Veranstaltung und schützen die örtliche Bevölkerung vor möglichen Gefahren aus der Luft.

Bei dieser „Cross-Boarder Operation" werden zivile Luftfahrzeuge beobachtet, begleitet und lückenlos an die Luftwaffe der anderen Nation übergeben. Ein Waffengebrauch ist in der benachbarten Nation nicht erlaubt.

Das FüUB 1 war bei dieser Übung mit einer Führungsunterstützungskompanie 1 (FUKp1) vertreten. Ihre Aufgaben war die Sicherstellung eines verlässlichen Datennetzes und Kommunikationsnetzes, welches für einen reibungslosen Flugbetrieb von entscheidender Relevanz ist.

Für die 3. FüUKp beginnen die Vorbereitungen für diese Luftraumsicherungsoperation bereits in den Sommermonaten des Vorjahres. Hier werden die Aufstellungsplätze erkundet und die benötigten Verbindungsrelationen erprobt.

Die Cybersoldaten sind bereits eine Woche vor Beginn des Forums im Einsatzraum und errichten die geforderten Kommunikationsverbindungen. Diese dienen der Einbindung von diversen Luftraumüberwachungssystemen.

Alle gestellten Aufgaben konnten erfüllt werden und damit konnte ein wesentlicher Beitrag zum Erfolg der Luftraumsicherungsoperation Dädalus geleistet werden.

Kaderanwärterausbildung 2

Aufgrund der dichten Ausbildungslage an der Führungsunterstützungsschule in Wien, wurde ein Teil der Kaderanwärterausbildung 2 beim Führungsunterstützungsbataillon 1 abgehalten.

Die 1. FüUKp bekam den Auftrag diese Ausbildung zu planen und im Anschluss durchzuführen. Planungen begannen bereits Sommer 2024. Hier stützte man sich auf bereits gewonnene Erkenntnisse der Truppenschule hinsichtlich Dienstplangestaltung und Normierung von Abläufen. Ebenso mussten sich Ausbilder auf Unterrichte und Lehrinhalte vorbereiten, um Auszubildenden ausreichend auf künftigen Aufgaben eines Gruppenkommandanten vorzubereiten.

Anfang Februar startete die bis Ende März dauernde Kaderanwärterausbildung 2. Die 39 Kursteilnehmer kamen aus dem gesamten Bundesgebiet aus unterschiedlichsten Einheiten des Bundesheers. Es wurden zwei Züge mit verschiedenen Schwerpunkten eingeteilt. Ein Zug fokussierte sich auf die leitungsungebunde Fernmeldesysteme und im Gegenzug vertiefte man sich im anderen Ausbildungszug auf leitungsgebunden Übertragungsmöglichkeiten. Zu Beginn mussten die Auszubildenden sehr viel Zeit im Lehrsaal verbringen, den Praxis muss auf guter Theorie beruhen. Hier erlernte man Sicherheitsbestimmungen und den richtigen Umgang mit Fernmeldegeräten.

Foto: Ausbildung an Fernmeldesystemen, Bundesheer/Dion6

Foto: Fernmelder, Bundesheer/Dion6

Die Inhalte wandelten sich in der Kursdauer fortlaufend Richtung praktischer Anwendung und die Soldaten übernahmen Aufgaben eines Gruppenkommandanten und führten ihre Trupps laut ihren erhalten Aufträgen.

Zum Kursende hin legten die Kursteilnehmer eine schriftliche Prüfung, zu ihrem theoretischen Wissen ab. Bei der praktischen Prüfung erhielten die Prüflinge einen umzusetzenden Auftrag über Errichten und Betreiben eines Funktrupps oder das Herstellen und Halten einer kabelgebundenen Leitung. Dies mussten alle Teilnehmer und ihre Trupps unter Einsatzbedingungen durchführen.

Alle 39 angetreten Soldaten konnten diese Teilprüfung auf ihrem Weg zum Unteroffizier positiv abschließen und ihre weiterführende Ausbildung an der Führungs-unterstützungsschule in Angriff nehmen.

TCN Lehrgänge

Mit dem Jahr 2023 wurde das neue Fernmeldesystem Tactical Communication Network (TCN) im Österreichischen Bundesheer eingeführt.

Wie bei jeder neuen Systemeinführung erfordert es eine gediegene Einschulung der Bediener, um das System in den Einsatz zu bringen und um es durch gezielte Gerätewartung einsatzbereit zu halten. Weiters müssen die Gruppen- und Truppenkommandanten in der Lage sein, Grundwehrdiener auf diesen Geräte auszubilden.

In erster Linie wurden die Systemschulungen und dazugehörigen Kurse an der der Führungsunterstützungsschule in Wien durchgeführt. Allen voran wurde der Basislehrgang TCN in der Starhemberg-Kaserne abgehalten. Nach einem intensiven Jahr wurde der Basislehrgang neu beurteilt und geplant. Man kam zu dem Entschluss, die Dauer von drei auf vier Wochen zu erhöhen und einige der Lehrgänge an die Truppe auszulagern. Daher bekam die Netzsteuerungsgruppe des FüUB 1 den Auftrag Kurse zu planen und abzuhalten.


Foto: TCN-Systemschuldung, Bundesheer/Dion6


Foto: TCN-Systemschulung, Bundesheer/Dion6

Am 10.02.25 startete ein Basislehrgang mit zehn Teilnehmern aus dem gesamten Bundesgebiet. Bei diesem Kurs geht es um Vermittlung von Basiswissen, welches vom Einheitskommandanten bis zum Truppenkommandanten jeder haben sollte.

Zu Beginn lag das Hauptaugenmerk auf Theorie. Der Lehrgang wurde mit fortschreitendem Wissen der Teilnehmer immer praxisorientierter. Zum Abschluss mussten sich die Teilnehmer einer schriftlichen sowie praktischen Prüfung unterziehen, welche alle Soldaten positiv bestanden hatten.

Im Anschluss daran begannen zwei Gruppenkommandanten Lehrgänge. Alle Teilnehmer des Informations-Kommunikationstechnologie Lehrgangs legten ihre Ausbildung vertiefend auf das Vermittlungssystem und auf das Einrichten eines Gefechtsstandes ab. Beim Gruppenkommandanten Lehrgang der Netzgruppe lag das Schwergewicht auf Errichten und Betreiben eines Datenfunksystems im Band IV-Bereich. Auch bei diesem Lehrgang konnten alle Teilnehmer einen positiven Abschluss erzielen.

Nach nur einer Woche Pause für die Ausbilder der Netzsteuerungsgruppe startete der 2.Basislehrgang TCN mit zehn Teilnehmern. Auch hier konnten alle Auszubildenden ihr Wissen bei der Abschlussprüfung unter Beweis stellen.

TCN Umstellung Ausland

Die Umstellung auf das neue Telekommunikationssystem TCN macht bei der Grenze des Bundesgebietes nicht halt. Alle Führungsunterstützungselemente im Bundesgebiet sind bereits auf das neue TCN System umgestellt. Die Ausbildung der Grundwehrdiener, Kaderanwärter und Spezialisten auf dem Telekommunikationssektor verläuft nunmehr zur Gänze auf dem neuen System. Nun kann man auch die Erneuerung der Systeme bei den sich im Ausland befindlichen Teilen des Österreichischen Bundesheeres als abgeschlossen betrachten.

Die Erneuerung auf TCN Systemkomponenten bei den Auslandsbasen im Kosovo, Bosnien und Libanon erforderte logistisches, fachliches und elektronisches Know How. Für die Meisterung der logistischen Herausforderungen der tonnenschweren Fracht wurden Teile der Heereslogistikzentren aus Klagenfurt, Graz und Salzburg herangezogen, um Geräte an ihren Bestimmungsort zu verbringen. Fachliche sowie elektronische Kompetenz aus der Direktion 6 konnte zusammengezogen werden, um diese Problemstellung zu lösen.

Das Führungsunterstützungsbataillon 1 war von Beginn der Umstellung an vorderster Front miteinbezogen. Bereits bei den ersten Erkundungsmaßnahmen in den jeweiligen Einsatzräumen konnten Soldaten der Elektronischen Werkstatt und der Netzsteuerung ihre Fachexpertise miteinbringen.

Hier erfolgte streng militärisch eine Lagebeurteilung und eine Erhebung des Gerätebedarfs. Nach dieser Beurteilungsphase stand der praktischen Arbeit vor Ort nichts mehr im Wege.

Je nach Einsatzraum und der vor Ort erforderlichen Arbeiten stellte das FüUB1 Teams in der Stärke von 11 – 18 Personen zusammen und diese verlegten dann zu den jeweiligen Kontingenten. Vor Ort erfolgte ein Austausch der alten gegen neue FüU Geräte. Nach dem Abbau verpackten die Teams die Altgeräte und die Logistikzentren führten dies durch. Alle neuen Systeme konnten friktionsfrei errichtet, programmiert und in Betrieb genommen werden. Ergänzend führte man bei weiterverwendeten Komponenten eine Materialerhaltung durch, Kabel wurden auf ihre Verbindungsfähigkeit überprüft, bei Bedarf gereinigt oder ausgetauscht. Auch verschiedenste Verteilerschränke mussten erneuert und neu verkabelt werden.

Nach Beendigung des Austauschs verbauten die Teams 47 Stück SSW, 5 Stück ATA, 6 Stück MSW und über 600 Stück Patchkabel in verschiedensten Längen.

Somit sind, nach Finalisierung aller Arbeiten die Telekommunikationsverbindungen für unsere Auslandskontingente innerhalb alle Einsatzräume des österreichischen Bundesheeres sichergestellt und eine Rückwärtsverbindung nach Österreich ständig leistungsfähig aufrecht.

Foto: TCN-Umstellung AUsland, Bundesheer/Dion6

Führungsunterstützungsbataillon 2

Kommandant FüUB2: Obst Johannes NUSSBAUMER, MSD


Foto: BMLV/HBF

Im Jahr 2025 stand das FüUB2, zusätzlich zu den üblichen Aufgaben und Herausforderungen, vor der Aufgabe, den Abgang von Personal vor allem auch den von Offizieren zu kompensieren. Zahlreiche Einsätze bei Vorhaben im In- und Ausland sowie die Standby-Phase für die EU-Battlegroup (BG2025) forderten den Verband.

Das FüUB2 wirkte beim Erreichen der vollen Einsatzreife (FOC) unseres neuen verlegbaren, hochmodernen, internetbasierenden taktischen Kommunikationssystems „Tactical Communication Network" (TCN) erfolgreich mit. Bei der Luftraumsicherungsoperation DÄDALUS im Jänner konnten die gewonnenen Radardaten über das TCN erfolgreich in die Einsatzzentrale Basisraum nach St. Johann im Pongau übertragen werden. Dadurch gewährleisteten wir mit unseren präsenten IKT-Kräften eine kompetente Unterstützung zur Bereitstellung des aktuellen Luftlagebildes. Ein weiterer wichtiger Weg zur FOC des TCN bedeutete der Einsatz des FüUB2 bei der Ausbildungsübung WALDVIERTEL25. Dabei errichtete und betrieb das FüUB2 das Führungsnetz für die gesamte Übung unter vorgestaffelter Einrichtung und Einbindung sämtlicher Gefechtsstände über das TCN bis auf Kompanieebene. Das FüUB2 stellte bei dieser multinationalen Ausbildungsübung die reibungslose Kommunikation und Vernetzung der beteiligten Kräfte sowie die Führungsfähigkeit der übenden Verbände sicher. Die WALDVIERTEL25 war somit auch für das FüUB2 eine ausgezeichnete Möglichkeit einsatznah zu üben und die Bedürfnisse im IKT-Bereich zu gewährleisten. Der Abschluss für eine endgültige Bewährung des TCN als Einsatznetzwerk des ÖBH erfolgte mit der IKT-Betriebsübung und einer umfassenden Systemtestung im Oktober.

Unsere FüUKp/EloKa setzte ihren Kompetenzaufbau in diesem Jahr erfolgreich fort. Bei den Übungen TRIAS25 und WALDVIERTEL25 wurden unter Einsatz der Erfassungs- und Ortungssysteme (ERFOS) das elektromagnetische Spektrum überwacht und gegnerische Funksignale aufgespürt und ausgewertet. Damit konnte eine Erweiterung der Fähigkeiten in der Waffengattung erreicht und eine erste Einsatzbereitschaft (IOC) des ERFOS für zukünftige Aufgaben des ÖBH sichergestellt werden. Bei der Übung ALPINE JAM 25 mit dem Ziel der Erprobung elektronischer Gegenmaßnahmen gegen funkgesteuerte improvisierte Sprengkörper (RCIED) am Truppenübungsplatz Hochfilzen konnten wir mit Experten aus Deutschland und der Schweiz, eine Optimierung der Wirksamkeit der CREW- und Drohnenabwehr-Systeme gegen die Steuerungen von Mini- und Microdrohnen erfolgreich erproben.

Mit den unbefristet beorderten Kameraden der Miliz wurden heuer zwei beorderte Waffenübungen (BWÜ) im FüUB2 durchgeführt. Bei diesen BWÜ erfolgten Ausbildungen für Einsatzaufgaben im Inland. Dabei wurden die Grundschießfertigkeiten, die Ausbildungen im Bereich mobiler Fernmeldesysteme mit Schwergewicht UKW, im Bereich TCN und Einweisungen in die EloKa durchgeführt, um die ausbildungsmäßigen Voraussetzungen für die Einteilung in der Einsatzorganisation sicherzustellen.

Wie schon in der Vergangenheit intensiv geschehen, gilt es, parallel zu den laufenden Aufgaben, Maßnahmen zur Personalgewinnung zu setzen. Einerseits ist es notwendig, das im Bestand befindliche Personal zu halten und andererseits mehr junges Personal zu werben. Wir sind wie bisher gefordert, unseren Beitrag zur Personalgewinnung aktiv zu leisten. Die Ausbildungen in unseren Waffengattungen und den Funktionen in den Einheiten, die professionelle Auftragserfüllung bei den Übungen und im sicherheitspolizeilichen Assistenzeinsatz an der Staatsgrenze, eine engagierte und unterstützende Stabsarbeit im Bataillonskommando sind Zeugnisse unserer Kompetenz, Verlässlichkeit und Leistungsfähigkeit. Danke an meine Soldatinnen, Soldaten und Bediensteten des FüUB2 für diesen Korpsgeist!

Einsatz der 2. FüUKp im Rahmen der Luftraumsicherungsoperation DAEDALUS25

Das Weltwirtschaftsforum (WEF) in Davos stellt jedes Jahr eine bedeutende Plattform für hochrangige politische, wirtschaftliche und gesellschaftliche Gespräche dar. Um einen reibungslosen Ablauf dieses globalen Gipfeltreffens zu gewährleisten, wurde die 2. Führungsunterstützungskompanie (2. FüUKp) mit dem Einrückungstermin 10/24 sowie dem zugehörigen Kader aus dem FüUB 2 eingesetzt.

Bereits Mitte November 2024 begannen die Vorbereitungen für die Luftraum-sicherungsoperation DAEDALUS25 mit dem I. und II. IKT-Zug (IKTZg) der 2. FüUKp. Diese Phase umfasste insbesondere fachspezifische Ausbildungsmaßnahmen sowie die genaueste Planung und Bereitstellung der erforderlichen Ausrüstung. Ein entscheidender Bestandteil war die fundierte Ausbildung der Grundwehrdiener des ET 10/24, die bereits seit Dezember 2024 im Rahmen der Basisausbildung 2/3 wesentliche Fachkenntnisse im Bereich des Kabelbaus und dem Einrichten eines Gefechtsstandes erworben hatten.

Diese erworbenen Fähigkeiten konnten nun praktisch angewandt werden. Der Fokus der Vorbereitungsphase lag insbesondere auf der Herstellung der Einsatzbereitschaft und der Verlegung der Kommunikationsinfrastruktur in die vorgesehenen Einsatzräume. Am Dienstag, den 14. Januar, verlegte die 2. FüUKp in Richtung Operationsraum Bregenz, wo nach der Ankunft sofort die ersten Maßnahmen zur Errichtung der Gefechtsstände und des Netzes eingeleitet wurden. Ein zentraler Bestandteil der Operation war die Einrichtung der Gefechtsstände im Bereich des Radarbataillons sowie die Unterstützung der Fliegerstaffel in Hohenems.

Ein wesentlicher technischer Schwerpunkt lag auf der Verlegung von Lichtwellenleitern (LWL) zwischen den Aufklärungs- und Zielzuweisungsradaren (AZR) und den Richtfunksystemen. Beispielsweise hierbei der Standort Sulzberg, bei dem eine Doppelleitung LWL in der Länge von 2 Kilometern errichtet wurde. Währenddessen arbeiteten die Kadersoldaten und die Grundwehrdiener im Kommandogebäude Oberst Bilgeri an der Einrichtung der Gefechtsstände und der Einbindung der Kommunikationssysteme.

Foto: Netz-Trupp BIV am Pfänder, Eva Lindbichler

Ein besonders wichtiger Aspekt hierbei war die Zusammenarbeit zwischen dem I. und II.IKTZg. Letzterer war für die Einbindung weiterer Fernmeldestellen (FMSt) verantwortlich. Parallel dazu war der IKT-Bautrupp intensiv damit beschäftigt, weitere LWL-Verbindungen im Einsatzraum unter Berücksichtigung aller Sicherheitsbestimmungen zu errichten.

Besonders im Bereich des Flugplatzes Hohenems war dies eine Herausforderung, da hier während der Operation ein hohes Flugaufkommen herrschte. Nach erfolgreichem Abschluss aller wesentlichen Maßnahmen meldete der I.IKTZg am 17. Januar die vollständige Einsatzbereitschaft. Von diesem Zeitpunkt an lag der Fokus auf der täglichen Überprüfung und Instandhaltung der Infrastruktur, um eine durchgehende Verbindung zu den Gefechtsständen zu gewährleisten.

Mit dem offiziellen Beginn der Operation am 20. Januar wurde das gesamte System unter realen Einsatzbedingungen getestet. Ein besonderer Schwerpunkt lag dabei auf der Überwachung der Kabelstrecken, um mögliche Beschädigungen frühzeitig zu erkennen um sofortige Instandsetzungsmaßnahmen durchführen zu können.

Foto: Netz-Trupp BIV am Vögel, Richard Mulder

Die DAEDALUS25 war bis zum Ende des Einsatzes am 24. Jänner eine äußerst anspruchsvolle, aber ebenso erfolgreiche Operation. In diesem Rahmen konnte das Kader und die Grundwehrdiener der 2. FüUKp ihr Wissen und erlerntes Können im Bereich Tactical Communication Network (TCN) eindrucksvoll unter Beweis stellen. Die enge Zusammenarbeit zwischen den verschiedenen Einheiten, die präzise Planung und die disziplinierte Umsetzung aller Maßnahmen führten zu einer reibungslosen Operationsdurchführung.

Damit wurde ein bedeutender Beitrag zur Sicherung des Weltwirtschaftsforums 2025 in Davos geleistet.

Fernmelde Betriebsübung der FüUKp/KPE + Scharfschießen der FüUKp/KPE

Führungsunterstützungskompanie /Combat Service Support Battalion (CSSBN)

In der 10. Kalenderwoche fand die erste Zusammenziehung von Teilen der FüUKp(KPE) im Jahr 2025 in der Krobatinkaserne in St. Johann im Pongau statt. Zweck der Zusammenziehung war es, eine Fernmeldebetriebsübung (FMBetrÜb) mit dem Tactical Communication Network (TCN) durchzuführen und zu überprüfen, ob die Fernmeldesystem einsatzbereit sind.

Dazu wurde die Vermittlungseinheit großer Verband (GVE) über den Truppenanschaltepunkt (TAP) in der Krobatinkaserne in das ortsfeste Fermeldesystem (ofFMSys) gebracht. Der IKTBauTrp stellte im Anschluss eine Singlemode Lichtwellenleitung (SM LWL) von der GVE zum Lehrsaal her, wo sich der Gefechtsstand der FüUKp befand. Im Lehrsaal wurden die restlichen Vermittlungseinheiten (VmiEinh)in Betrieb genommen. An diesen beiden Systemen wurden dann sämtliche Telefone, Switches und andere Komponenten des Gefechtsstand-Einrichtesatzes der GVE, der Systeme und des Zusatzgerätes angeschlossen. Zweck dessen war es, die Zertifikate der Geräte zu erneuern und die Systeme abzugleichen. Da das TCN-System laufend upgedatet wird, ist es notwendig, in periodischen Abständen die einzelnen Komponenten zu überprüfen um sicherzustellen, dass es nach einem Update zu keinen Komplikationen gekommen ist.


Foto: SAT-Anlage, Bundesheer

Parallel dazu wurde die Woche zur Aufrechterhaltung der Einsatzbereitschaft des Personals der FüUKp genutzt. Hierzu fand am Dienstag eine Leistungsüberprüfung „Allgemeine Kondition" statt und am Mittwoch wurde eine Hauptdichteprüfung mit der neuen mobilen Prüfanlage durchgeführt. Des Weiteren wurde die Woche genutzt um diverse Belehrungen abzuarbeiten.

Ein weiteres Ziel der FMBetrÜb war es, neu eingeführte Systeme wie z.B. den Truppenanschaltepunkt Adhoc verlegbar (TAP-A-vlgb) zu überprüfen und zu testen um dadurch neu Erkenntnisse zu gewinnen. Außerdem wurde ein Truppenanschaltepunkt Satellitenanlage verlegbar (TAP-S-vlgb) über den Remote Terminal Europe (RTE) verwendet und hinsichtlich der Bandbreite von ca. 20 Megabits per Second (mbps) Leistung überprüft.


Foto: Neue Ausrüstungsteile der KPE, Bundesheer

Sollte die EUBG ausgelöst werden und sich das CSSBN in einem Einsatzraum befinden, ist es natürlich auch wichtig, Sozialkommunikation (Internet/WLAN für soziale Kommunikation) für die Truppe bereitstellen zu können. Dazu verfügt die FüUKp über 2 Module "Internet via Sat". Diese können über Sat-Terminals offene WLANs bereitstellen, welche dann von den Soldaten genutzt werden können. Das trägt wesentlich zur Aufrechterhaltung der Moral bei.

Unterstrichen wurde die Wichtigkeit der FMBetrÜb mit einer Fachaufsicht durch die Direktion 6. Diese wurde intensivst dazu genutzt der Direktion 6 ein aktuelles Lagebild über den materiellen und personellen Zustand der FüUKp zu vermitteln und weitere Vorhaben zu besprechen.

Um die Einsatzbereitschaft zu erhalten wurde weiters in der 17.KW ein Scharfschießen durch die FüUKp/KPE durchgeführt. Schwergewicht dabei war die Handhabung der neuen ballistischen Schutzweste, des taktischen Laser/Lichtmoduls und der neuen Nachtsichtbrille 3D. Dementsprechend wurde auch die Bekämpfung von Zielen bei Dunkelheit trainiert und gemeistert.

Übung WALDVIERTEL 25

Von 16. bis 27. Juni 2025 führte die Theresianische Militärakademie gemeinsam mit der 4. Panzergrenadierbrigade am Truppenübungsplatz Allentsteig die Ausbildungsübung Waldviertel 25 durch. Um die vielfältigen Verbindungsrelationen sicherstellen zu können, war das Führungsunterstützungsbataillon 2 gefordert. Dabei war neben den eigenen Elementen wie dem Bataillonskommando, der 1. Führungsunterstützungskompanie, der verminderten Stabskompanie sowie der Führungsunterstützungskompanie für elektronische Kampfführung auch die Führungsunterstützungskompanie des Panzerstabsbataillons 4 in das Führungsunterstützungsbataillon eingegliedert.

Als zentraler Bestandteil zur Steuerung sämtlicher betriebstechnischer Maßnahmen im verlegbaren und mobilen Bereich, wurde auch ein Central Network Operations Center aus Elementen der Netzsteuerung sowie der S6-Gruppe des Führungsunterstützungsbataillons 2, gebildet.

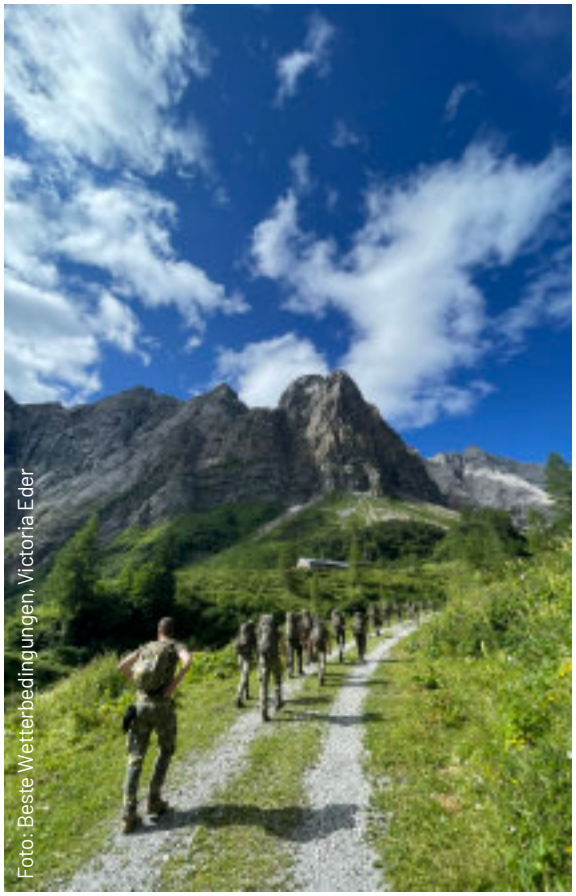


Foto: Beste Wetterbedingungen, Victoria Eder

Alpinausbildung des ET02/25 „Wer auf alten Wegen steigt, trägt neues Wissen weiter“

Im Anschluss an die Ausbildungsübung WALDVIERTEL 25 führte die 1. Führungsunterstützungskompanie in der 28. Kalenderwoche eine Alpinausbildung im Raum Lienz durch.


Foto: Klettersteig „Weg der 26er“, Victoria Eder

Bei verbesserten Wetterbedingungen verlegte die Kompanie am Dienstag in die Franz-Joseph-Kaserne. Am Mittwoch stand eine Alpintour zum Wolayersee auf dem Programm. Nach einem langen, aber landschaftlich beeindruckenden Aufstieg über das Valentintörl, teilte sich die Kompanie in zwei Gruppen auf: Die 1. Gruppe nahm den anspruchsvollen Klettersteig „Weg der 26er“ zur Hohen Warte in Angriff, während die 2. Gruppe weiter zur Wolayerseehütte wanderte und dort die historischen alpinen Stellungen erkundete.

Der Donnerstag stand ganz im Zeichen der Geschichte: Erkundet wurden unter anderem die Cellon-Stollen – ehemalige Kriegsstollen, die heute als Klettersteig genutzt werden.


Foto: Alter Versorgungsstollen als Klettersteig, Victoria Eder

Historisch betrachtet war die sogenannte „Cellonschulter“ eine Schlüsselstellung am Plöckenpass und Schauplatz heftiger Kämpfe zwischen Österreich-Ungarn und Italien während des Ersten Weltkriegs. Österreichische Soldaten meißelten sich damals Meter für Meter durch den Fels, um mit den Cellon-Stollen eine beschusssichere Verbindungslinie unter schwerstem Feindfeuer zu schaffen.

Während sich die 1. Gruppe unterirdisch durch den Klettersteig der Cellon-Stollen hocharbeitete, begab sich die 2. Gruppe auf den Kleinen Pal, der sich auf der gegenüberliegenden Talseite befindet. Dort errichteten einst beide Kriegsparteien entlang der Hänge Stellungen, die stellenweise nur wenige Meter voneinander entfernt lagen.

Die Gruppe besuchte das gut erhaltene Freilichtmuseum, das noch heute vom Verein Dolomitenfreunde betreut wird. Im Anschluss folgte eine abschließende Führung im Museum „1915–1918" in Kötschach-Mauthen, das sich mit dem Gebirgskrieg in den Karnischen Alpen beschäftigt.

Für die Grundwehrdiener des ET 02/25 war die Alpinausbildung zweifellos eine anspruchsvolle, aber ebenso prägende Erfahrung, die ihnen auch über den Dienst hinaus in Erinnerung bleiben wird.

Foto: Wohlverdiente Pause, Victoria Eder

Foto: Traumhafte Aussicht, Victoria Eder

Führungsunterstützungsschule

Kommandant FüUS: ObstdG Mag. Franz SITZWOHL, MSc

Die Vielfalt an Vorhaben der FüUS im Jahr 2025, inklusive neuer Ausbildungsvorhaben, Forschung und Erprobung, erforderte die volle Professionalität, nicht nur unseres Ausbildungspersonals sondern auch unserer Verwaltung und Logistik. Im Rahmen des Neujahrsempfangs sowie während unterschiedlichster Kaderfortbildungen versuchten wir die Herausforderung im Cyber- und Informationsraum zu beleuchten. Mittlerweile ist die FüUS in der Lage diese Events live im Intranet bereitzustellen. Die Teilnahme an Übungen mit Teilnehmern und Stabstrainern war 2025 besonders herausfordernd, denn es wurde erstmals der Generalstabslehrgang von allen unseren Waffengattungen (IKT, Cyber, EloKa, Kommunikation und PsyOps) beübt sowie betreut.

Neben den Herausforderungen von Desinformation wächst die Bedeutung von Künstlichen Intelligenz (KI) im militärischen Kontext. Die unterschiedlichen Formen von KI bieten einerseits große Chancen für das ÖBH, stellen uns aber auch vor erhebliche Herausforderungen. Es liegt in unserer Verantwortung, diese Technologien umsichtig einzusetzen, um die militärische Effizienz zu steigern, ohne dabei die ethischen und sicherheitstechnischen Fragen außer Acht zu lassen. Dabei ist auch die FüUS gefordert, mit seinen neuen Waffengattungen, den Cyber- und Informationsraum besser abzusichern.

Das Jahr 2025 war, neben den bisherigen Aufgaben der FüUS, geprägt von der Implementierung des Stabsbereiches J10 – Strategische Kommunikation (StratCom). Auf militärstrategischer Ebene werden diese Aufgaben von der Direktion Kommunikation wahrgenommen, während künftig J10 StratCom auf operativer Ebene im FHQ eine zentrale Rolle spielen wird. Ziel ist es dabei, die Planung und Umsetzung von Kommunikationsmaßnahmen der Kommunikations- sowie PsyOpsTruppe während militärischer Operationen zu koordinieren. Dazu wurde im Juni 2025, gemeinsam von FüUS mit der NATO-Schule Oberammergau, der Workshop „Grundlagen Strategische Kommunikation", abgehalten um Kenntnisse zu StratCom, Informationsoperationen, Psychological Operations und Military Public Affairs zu vertiefen.


Foto: BMLV/HBF

Die Höhepunkte unseres heurigen Traditionstages war die Überreichung der Ehrenringe der Führungsunterstützung in GOLD an GenMjr Hermann KAPONIG und ObstdG i.R. Horst TREIBLMAIER sowie die Begründung einer Partnerschaft mit dem AMRS. Der Amateurfunkverein des ÖBH, der AUSTRIAN MILITARY RADIO SOCIETY (AMRS), arbeitet bereits seit Jahren mit der FüUS und ist nun offiziell unser Partner.

Kommandant Fernmeldestelle: Eine fordernde militärische Ausbildung

Diese neue militärische Kommandantenausbildung ist ein intensiver Lehrgang, der angehende Kommandanten auf eine der technisch und taktisch anspruchsvollsten Positionen innerhalb der IKT-Truppe vorbereitet. Besondere Bedeutung wird dabei auf die Gefechtstechnik gelegt. Die Ausbildung schließt mit der Stabsunteroffiziersausbildung ab und befähigt den Teilnehmer die Aufgaben des Kommandanten einer Fernmeldestelle im nationalen Einsatz und im Frieden auszuüben und die funktionsspezifischen Aufgaben sowohl im nationalen als auch im internationalen Einsatz wahrzunehmen. Darüber hinaus wird Einblick in stabsdienstliche Aufgaben in einem Stab kleiner Verband genommen.

Die Ausbildung umfasst ein breites Spektrum an Inhalten, die die Soldaten auf ihre zukünftigen Aufgaben vorbereiten. Dazu gehören:

- Grundlagen Cyberkräfte Ebene Fernmeldestelle,
- Waffen- & Gerätefachausbildung Ebene Fernmeldestelle,
- Führen & Aufgaben in Frieden und Einsatz Ebene Fernmeldestelle.

Foto: Sicherungs- & Erkundungselement, Bundesheer/Dion6

Foto: Netz-Trupp beim Aufbau, Bundesheer/Dion6

Die Ausbildung erfolgt stufenweise und beginnt mit theoretischen Unterweisungen im Bereich der Cybergrundlagen sowie Befehlsgebung. Die theoretisch Erlernten Inhalte werden danach praktisch am Gerät präsentiert und geübt.

Auf dem Simulationssystem CATT, können die Soldaten in simulierten Gefechtsszenarien ihre Kompetenz und taktischen Fähigkeiten unter Beweis stellen, sowie die neu erlernten Befehlsformate stressfrei üben.

Ab der 2 Ausbildungswoche wird die Ausbildung ins Gelände verlegt. Besonders im Bereich der Gefechtstechnik müssen die Soldaten schnelles und präzises Handeln unter Druck beweisen.

Im Verlauf des Lehrgangs werden mehrfach jeweils zwei Fernmeldestellen, eine Führungseinrichtung sowie eine Übertragungseinrichtung bezogen, errichtet und betrieben.

Ein wesentlicher Bestandteil der Ausbildung ist die Befehlsgebung, die durch neu definierte Befehlsformate geregelt wird. Die Befehlsformate sind essenziell für das Beziehen und den Betrieb einer Fernmeldestelle.

Alpentriode 2025: Multinationale Zusammenarbeit auf hohem Niveau

Vom 11. bis 16. Mai 2025 fand in Österreich die multinationale Übung Alpentriode statt. Hier arbeiteten IKT-Truppen aus Österreich, Deutschland und der Schweiz eng zusammen, um Führungs- und Kommunikationsverfahren zu vertiefen, moderne Systeme zu erproben und die Kameradschaft zu stärken.

Am Sonntag wurden die Gäste aus Deutschland und der Schweiz herzlich empfangen. In entspannter Atmosphäre entstanden erste Kontakte und die Basis für eine erfolgreiche Woche.

Am Montag lag der Fokus auf technischer Ausbildung. Nach der Einführung in österreichische Fernmeldesysteme folgte die Einweisung in das Führungsinformationssystem SitaWare. In praktischen Übungen konnten sich alle Teilnehmer intensiv mit den Systemen vertraut machen. Gemeinsame Abende stärkten zudem den Teamgeist.

Am Dienstag startete das multinationale Planungsverfahren. In gemischten Teams wurden komplexe Lagen bearbeitet; SitaWare kam erstmals im praktischen Einsatz für Lageführung, Planung und Kommunikation zum Zug. Die Zusammenarbeit in trinationalen Teams funktionierte vorbildlich.

Foto: Alpentriode, Bundesheer

Foto: Alpentriode, Bundesheer

Der Mittwoch stand im Zeichen der Kameradschaft: Nach einer Führung im Heeresgeschichtlichen Museum folgte eine Schnitzeljagd durch die Wiener Innenstadt. Ein gemeinsames Abendessen im Prater rundete den Tag ab.

Am Donnerstag wurde das Planungsverfahren fortgesetzt und die Teams vertieften die Anwendung von SitaWare sowie Lagebeurteilung und Entscheidungsfindung im multinationalen Kontext.

Mit einem gemeinsamen Rückblick endete die Übung. Die Teilnehmer waren begeistert von der hohen fachlichen Qualität, praxisnaher Systemanwendung und dem kameradschaftlichen Austausch.

Desinformation: Herausforderungen für die Informationssicherheit

Desinformation stellt eine große Herausforderung für die Informationssicherheit dar. Am 29. April 2025 widmete sich eine Kaderfortbildung der FüUS diesem aktuellen Thema. Die Veranstaltung bot vielseitige Einblicke von Experten. OR Michael Suker vom CDFZ der Landesverteidigungsakademie hob hervor, dass hybride Bedrohungen spezifische militärische Vorbereitungen erfordern. Deepfakes werden gezielt eingesetzt, um durch manipulierte Audio-, Video- und Textdokumente sowie gefälschte Satellitenbilder und Geodaten Verwirrung zu stiften und strategische Fehlentscheidungen zu provozieren.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

Laut OR Suker sind selbst moderne KI-Systeme derzeit noch nicht in der Lage, Desinformation zuverlässig zu erkennen. Fact-Checking-Organisationen übernehmen daher eine wichtige Rolle, um Falschinformationen manuell zu kennzeichnen. Die schnelle Verbreitung in sozialen Medien erschwert die Bekämpfung zusätzlich.

Obstlt Lothar Riedl zeigte anhand von Beispielen wie „Love Scam“ und gezielten Falschmeldungen, wie Fake News sowohl im privaten als auch öffentlichen Bereich Einfluss nehmen. Auch das Wahlverhalten wird zunehmend durch Desinformation beeinflusst. Im hybriden Krieg dient sie der Manipulation der öffentlichen Meinung und der Untergrabung staatlicher Glaubwürdigkeit.

ObstdG Franz Sitzwohl erläuterte die Unterschiede zwischen Fehlinformation, Desinformation und Falschinformation. Entscheidend ist die Täuschungsabsicht eines Absenders. Satire und Parodie sind davon zu unterscheiden. Desinformation liegt vor, wenn Manipulationsversuche nachweisbar sind, oft mit erfundenen oder verkürzten Statistiken. Gerüchte verbreiten sich laut Studien sechsmal schneller als Wahrheiten. Organisationen setzen zunehmend auf „Prebunking“, also vorbereitete Gegenmaßnahmen im Fall eines Desinformationsvorfalles. Es wird geraten, Bilder und Videos sowie Quellen kritisch zu prüfen, um nicht selbst Teil von Desinformationskampagnen zu werden.

Framing in der Kommunikation

In der digitalen Medienwelt spielt nicht nur was berichtet wird eine Rolle, sondern vor allem wie Informationen dargestellt werden. Die Art der Darstellung – häufig als Framing bezeichnet – kann beeinflussen, wie Informationen interpretiert werden. Framing ist ein zentrales Konzept der Kommunikationswissenschaft und spielt eine wichtige Rolle bei der öffentlichen Meinungsbildung.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6


Foto: Itsuo Inouye für Associated Press im Irak-Krieg 2003

Framing beschreibt den Vorgang, bei dem bestimmte Aspekte einer Realität hervorgehoben und andere ausgeblendet werden, wodurch Interpretationen strukturiert werden. Nach Robert Entman umfasst Framing vier Elemente: Problemdefinition, Ursachenzuschreibung, Lösungszuschreibung und explizite Bewertung. Frames sind somit Perspektiven, die bestimmte Informationen betonen und andere ausblenden.

In der öffentlichen Debatte konkurrieren verschiedene Akteure darum, welche Deutungsrahmen sich durchsetzen. In der Medienpraxis zeigt sich Framing durch Wortwahl, Bildauswahl, Reihenfolge der Fakten und Kontextualisierung. Diese Mechanismen sind Teil journalistischer Arbeit. Problematisch wird es, wenn sie in manipulativer Absicht eingesetzt werden. Fake News nutzen häufig emotionale Darstellungsweisen, um Aufmerksamkeit zu erzeugen und bestehende Einstellungen zu verstärken. Framing kann beeinflussen, wie Informationen eingeordnet werden, bevor eine sachliche Bewertung erfolgt. Falsche Frames bleiben oft haften, auch wenn sie später widerlegt werden. In sozialen Medien werden Frames durch Wiederholung und Algorithmen verstärkt. Dies kann das Vertrauen in journalistische Angebote beeinträchtigen; Begriffe wie „Lügenpresse“ stehen für eine wachsende Skepsis gegenüber etablierten Medien.

Visuelles Framing, etwa durch Bildausschnitte, kann die Wahrnehmung beeinflussen – wie das häufig zitierte Beispiel eines US-Soldaten im Irakkrieg zeigt (siehe Foto). Framing nutzen nicht nur Medien, sondern auch Politik, PR und Regierungen – entscheidend ist, dies zu erkennen und kritisch zu reflektieren. Transparenz, Medienbildung und Faktenprüfung sind wichtig, um Desinformation und verzerrten Darstellungen entgegenzuwirken. Die Fähigkeit, Frames zu analysieren, wird zur Schlüsselkompetenz in einer Demokratie.

Grafik: KI-generierte Abbildung, Bundesheer/Dion6

LAGE PINZGAU

In der 5. Kalenderwoche 2025 führte die 6. Gebirgsbrigade eine umfassende Planungsübung zur Optimierung des taktischen Planungsprozesses durch. Beteiligt waren Angehörige des FGG6 der Brigaden, die S6-Gruppen der fünf Bataillone sowie der Führungs- und Stabslehrgang Miliz-Offizier der Führungsunterstützungsschule. Zwei Offiziere der FüUS leiteten diese Übung, einer übernahm die Führung des Brigadestabes, der andere betreute die Bataillonsstäbe.

Diese Übung basiert auf einer Lage im Verantwortungsbereich der Brigade. Die Standschützenkaserne bot dafür eine realitätsnahe Umgebung. Nach einer theoretischen Einführung startete das Planspiel. Es umfasste einen Angriff im Rahmen einer Schutzoperation unter anspruchsvollen Bedingungen im gebirgigen Gelände. Der gegnerische Verband agierte irregulär und setzte sowohl konventionelle als auch unkonventionelle Mittel zur Verteidigung ein.

Zunächst wurden die Bataillonsstäbe schrittweise in den Planungsprozess eingebunden. Ab Mittwoch erfolgte die Planung parallel auf Brigade- und Bataillonsebene, mit Schwerpunkt auf der Konzeption und Koordination der Kommunikationsverbindungen der angreifenden Truppe.

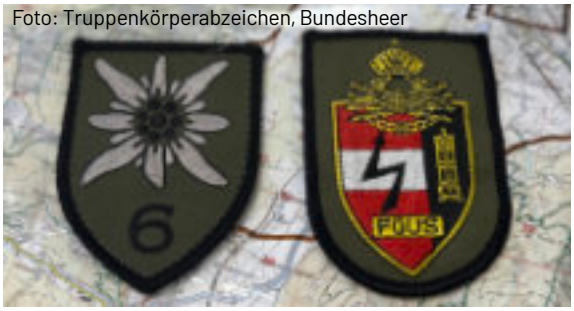


Foto: Truppenkörperabzeichen, Bundesheer

Der Chef des Stabes (COS), gespielt von der FüUS, setzte verbindliche Zeitvorgaben für die einzelnen Zwischenbesprechungen. Die Ergebnisse wurden jeweils den Kommandanten präsentiert, analysiert und optimiert.

Die Übung zeigte den hohen Ausbildungswert der Teilnahme von Lehrgangsteilnehmern an realen Stabsprozessen. Wesentliche Erkenntnisse waren die erforderliche Bereitstellung aller erforderlichen Materialien, die Kooperation mit den Bereichen S2 und Kampfunterstützung sowie die gestaffelten Planungsverfahren der Brigade und seiner Bataillone. Aufgrund der gewonnenen Erkenntnisse plant die FüUS, dieses Ausbildungsformat weiter auszubauen und künftig ein mobiles Trainer-Team für alle Brigaden des Österreichischen Bundesheeres bereitzustellen. Dabei sollen zukünftige Lagen noch stärker an die spezifischen Herausforderungen der jeweiligen Brigade angepasst werden.


Foto: Planspielteilnehmer, Bundesheer

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 Softwareentwicklungs-umgebung)
Appl	Abteilung Applikation
Application Level Firewalling	Netzwerksicherheitskomponente auf Anwendungsebene
Arbeitsplatzfixes	Fehlerbehebungspunkte von Softwareproblemen
ArcGIS	Geoinformationssystem-Software
ARWT	Amt für Rüstung und Wehrtechnik
ASECOS	System zur verschlüsselten Übertragung von Daten

AssE	Assistenzeinsatz
Audit	Überprüfung
AÜG	Arbeitskräfteüberlassungsgesetz
AUT	Austria
AUTCON	Austrian Contingent (Kontingent im Auslandseinsatz)
AUVA	Allgemeine Unfallversicherungsanstalt

B

Backbone	Rückgrat (Hauptleitungen) von Netzwerken
BACnet	Building, Automation and Control Networks (Netzwerkprotokoll für Gebäudeautomation
BACtwin	Building, Automation and Control Twin (Digitaler Zwilling)
BandlibrarySystem	Bandbibliothek zur Datenspeicherung auf Magnetbändern
BatchFenster	Konsolenfenster des Betriebssystems
BBG	Bundesbeschaffungsgesellschaft
BenBe	Benutzer-Betreuung
Big Data	Große komplexe Datenmengen
Bitbox	Browser in the Box (Browser in virtueller Maschine, um Angriffe auf das Host-System zu verhindern)
BK/C	Bundeskriminalamt/Abteilung Cyber Crime and Competence Center
BKA	Bundeskanzleramt
Blackhawk	Transporthubschrauber S-70 der Firma Sikorsky
BlueScreen	Fehleranzeige nach schwerwiegendem Problem im Betriebssystem
BMDW	Bundesministerium für Digitalisierung und Wirtschaftsstandort
BMEIA	Bundesministerium für europ. und intern. Angelegenheiten
BMI	Bundesministerium für Inneres
BMLRT	Bundesministerium für Landwirtschaft, Regionen und Tourismus

Stichwortverzeichnis

BMLV	Bundesministerium für Landesverteidigung
BMS	Battlefield Management System
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
Bruteforce	Methode, unerlaubten Zugriff auf IT-Systeme zu erlangen
BRZ	Bundesrechenzentrum
BV Meldung	Meldung Besonderer Vorfälle
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
BVT/CSC	BVT/Cyber-Security-Center
BWÜ	Beorderten-Waffenübung

C

C4	Cyber Crime and Competence Center (nationale Koordinierungs- und Meldestelle zur Bekämpfung von Cyberkriminalität)
CAD	Computer-Aided-Design (Rechnerunterstütztes Konstruieren)
Carrier-Ethernet	Erweiterung von Ethernet für Telekommunikation
CCI	Controlled cryptographic Item
CFBLNet	Combined Federated Battle Laboratories Network (Netzwerk zum simulieren von Trainingsumgebungen)
ChangeManagement	Laufendes umfassendes Veränderungsmanagement
Chat	digitale Umgebung zum Nachrichtenaustausch
ChdStb	Chef des Stabes
Chipkarte	Mittel zur Authentifizierung
CIO/CDO	Chief Informational Officer/Chief Digital Officer (strategische Position in der Führungsebene im Bereich IT)
CIRP	College International pour la Recherche en Productique (Internationale Akademie für Produktionstechnik)
CISDefence	Computer and Information Systems Defence
CKM	Cyberkrisenmanagement
CKMS	Chipkarten-Management-System

CMS	Content Management System
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CO-IServices	Community of Interest Services (Interessensgemeinschaft)
COMEX	Communication Exercise 20
COMMON ROOF	Internationale Übung für Interoperabilität im DACH Raum
COMSEC	Communication security
Content Disarm and Reconstruction	Technologie um Schadsoftware aus Daten zu entfernen
Core-Services	Kerngruppe wichtiger Anwendungen (z.B. E-Mail, VPN, etc.)
Covid-19	SARS CoV-2 Virus („Corona-Pandemie")
CR	Common Roof (Übung)
CST	Custodial Support Team
Custom App	Angepasste Applikation
CWIX	Coalition Warrior Interoperability Exercise
Cybär	Maskottchen IKT&CySihZ
CyberTruppe	Militärisches Element zur Beherrschung des vollen Spektrums des Kampfes in Computernetzwerken
Cyberabwehr	Abwendung von Attacken auf Netzwerke und Computersysteme
Cyberangriff	Gezielte Attacke auf größere Rechnernetzwerke, spezifisch wichtiger Infrastruktur
Cyberbedrohung	Bedrohungen im Cyberraum (Cyber Kriminalität, Identitätsmissbrauch, Cyberangriffe oder der Missbrauch des Internets)
Cyberdomäne	Dimension der militärischen Einsatzführung, wie Land, Luft, See oder Weltraum
Cyberkoordinator	Steuerungsorgan der Cyberdömane des BMLV auf strategischer Ebene
Cyberkräfte	Teilstreitkraft des ÖBH zur Beherrschung sämtlicher taktischen Maßnahmen zum Schutz der militärischen Netze
Cyberkriminalität	Straf- oder verwaltungsstrafrechtlich relevante, normierte Angriffe aus dem Cyberraum
Cyberkrise	Eskalationsstufe von Cybervorfällen, ausgerufen durch den BMI (NISG §3 Abs.22, §24)

Stichwortverzeichnis

Cyberlage	▶ Darstellung der Eigenlage des ÖBH im Cyberraum und als Teil des militärischen Gesamtlagebildes
CyberOps	▶ Cyber-Operations (Handlung im Cyberraum)
Cyberraum	▶ Der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab
Cybersicherheit	▶ Gesamtheit aller Technologien, Prozesse und Vorgehensweisen , die Netzwerke, Computer, Programme und Daten vor Angriffen, Schäden oder unerlaubten Zugriffen schützen sollen
Cyberverteidigung	▶ Gesamtheit aller Maßnahmen zum Schutz vor Cyberangriffen und zur Erhöhung der Cybersicherheit
Cybervorfälle	▶ Böswilliges oder versehentlich herbeigeführtes Ereignis, das die Cybersicherheit eines Informationssystems oder die Sicherheit der verarbeiteten Informationen gefährdet oder Sicherheitsrichtlinien, Sicherheitsprozesse oder Nutzungsbedingungen verletzt

D

DACAN	▶ distribution and accounting agency NATO
DACH	▶ Deutschland-Österreich-Schweiz
DADR	▶ Deployable air defence radar
DAEDALUS	▶ Luftraumsicherungsoperation
Datenfunksoftware	▶ Software zur Übertragung von Daten über Funk
Dashboard	▶ Visualisierung von Daten
Data Loss Prevention	▶ Maßnahme zum Schutz der Vertraulichkeit von Daten
DBMS	▶ Datenbank Management System
DDoS	▶ Distributed Denial of Service
DGIWG	▶ Defence Geospatial Information Working Group
DGMN	▶ Dynamisches gesichertes Militärnetz
DhFMO	▶ Diensthabender Fernmeldeoffizier
DhSys	▶ Diensthabendes System
Dienstenetz	▶ Logische Segmentierung des Trägernetzes (Leitung, Router) Netzwerkverkehr wird für unterschiedliche Kunden über ein und dieselbe Netzinfrastruktur logisch von einander getrennt und geroutet. Für jeden Kunden wird das Netz spezifisch abgesichert und verschlüsselt. Es werden somit mehrere Kundenentze zur Verfügung gestellt.

Digitaler Zwilling	Digitale Repräsentanz eines materiellen oder immateriellen Objekts/Prozesses aus der realen Welt in der digitalen Welt
Digitalisierung	Umwandlung von analogen Werten in informationstechnisch verarbeitbare Daten
dpi	Dots per inch (Drucktechnische Auflösung)
DSB	Datenschutzbeauftragter

E

E-Mail	Electronic Mail (Digitale Post)
early life support	Lösung von operativen Problemen während der Anlaufphase
EDA	European Defence Agency
EDRS	Endpoint Detection Response System
EFA	Europäisches Forum Alpbach
Ego-Perspektive	Ansicht, als wäre man die jeweilige Person
Einsatz	Tätigwerden des ÖBH zur Erfüllung seiner verfassungsgesetzlich verankerten Aufgaben lt. §2 Abs.1 Wehrgesetz
ELAK	Elektronischer Akt (unterscheide BMLV-ELAK und ELAK im Bund)
EloKa	Elektronische Kampfführung
EloKa-Truppe	Elektronische Kampfführungs-Truppe
Emotet	Computer Schadsoftware
EOW	EU Operations WAN (Europaweites gesichertes Netzwerk)
ePAT	Elektronisches Patienten Informations System
EPR	Eignungsprüfung
ERGIS	Ergänzungsinformationssystem
ESS	Employee Self Service
ETB	Elektronisches Telefonbuch
Ethernet	Kommunikationsstandard für Software und Hardware in einem kabelgebundenen Netzwerk
EU Battle Groups	European Union Battle Groups
EUBG	European Union Battle Groups 2020

Stichwortverzeichnis

EUCH	European Challenge 2020 (Cyber-Übung)
Eurofighter Typhoon	Abfangjäger des Österreichischen Bundesheeres
EUTM	European Training Mission
Explore AI	Forschungsprojekt über den Einfluss von künstlicher Intelligenz auf das Militärwesen im österreichischen Kontext
Extranet	Erweiterung des Intranets, welches nur für eine festgelegte Gruppe an Nutzern zugänglich ist

F

Fauna	Tierwelt
FEG	Forterhaltungsgebühr
Fertigungsklausel	Festlegung von Unterschriftsberechtigungen und Formulierungen
FFT Proxy	Friendly Force Tracking Proxy
FGP	Abteilung für Fahrzeuge, Geräte und persönliche Ausrüstung
Fibre	Glasfaser
Firewall	Netzwerksicherheitskomponente
First-Line-of-Defence	Erste Verteidigungslinie
FM-Planung	Fernmelde-Planung
FMN	Federated Mission Networking
FMSysÖBH	Fernmeldesystem ÖBH
FNMS	Funknetzmanagementsystem (Software)
Force Provider	IKT-Fähigkeiten des ÖBH, die Bedarfsträgern nicht zur Verfügung stehen, sind zentral beim IKT&CySihZ bereitzuhalten
FORTE	Österreichisches Verteidigungsforschungsprogramm
FORTE CADSP	Forschungsprojekt Cyber Attack Decision and Support Platform
FOSSGIS	Free & Open Source Software for GeoInformationSystems
Frq&SchlW	Frequenz- und Schlüsselwesen
Führungsmittel	Systeme, Geräte und technische Verfahren mit denen erforderliche Informationen gewonnen, verarbeitet, gespeichert und übertragen werden, um die eigene Führung sicherzustellen und die gegnerische zu beeinträchtigen

FüSim	Führungssimulator
FüU	Führungsunterstützung
FüUB	Führungsunterstützungsbataillon

G

G6	Generalstabsabteilung 6
GA-Funktionsliste	Gebäude-Automations Funktionsliste
Galileo-PRS	Galileo Public Regulated Service
Gebäudeautomation	Überbegriff für Überwachungs-, Steuer- und Regelungseinrichtungen in Gebäuden
GeoMetOc-Syndicate	Geospacial Meteorological and Oceanographic Syndicate
GeoOps	Geographic Operations (Geooperationen)
GIS	Geografisches Informations System
Global Mapper	GIS Software-Komplettlösung
GNSS	Global Navigation Satellite System
GOB	Geschäftsfallorientierte Bearbeitung
Goldhaube	Passives Element der österreichischen militärischen Luftraumüberwachung (primär und sekundär)
GovCERT	Governmental Computer Emergency Readyness Team
GovNetBox	Hochsichere VPN-Lösung für bestimmte Geheimhaltungsstufen
GPS	Global Positioning System
Grafana	Programm zur graphischen Darstellung von Daten
Grundwehrdienst	Pflicht eines jeden österreichischen Staatsbürgers, der als tauglich eingestuft ist
GStb	Generalstab
GUI	Graphical User Interface (grafische Benutzeroberfläche)
GWD	Grundwehrdiener/-dienst
GWS	GeoWebService

Stichwortverzeichnis

H

Hardware	Physische Komponenten in der IT
Headset	Kopfhörer mit Mikrofon
HF	High Frequency (Hohe Frequenz)
HGG	Heeresgebührengesetz
HGLLG	Hochgebirgslandelehrgang
HLogZ	Heereslogistikzentrum
HNaA	Heeresnachrichtenamt
Homeoffice	Büroarbeit am Wohnort
Hotline	Heißer Draht (Telefonischer Auskunfts- und Beratungsdienst)
HPA	Heerespersonalamt
HTBLVA	Höhere technische Bundes Lehr- und Versuchsanstalt
HTS	Heerestruppenschule
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hybride Bedrohungen	Einsatz von konventionellen und unkonventionellen Methoden durch staatliche und nichtstaatliche Akteure in koordinierter Weise, ohne die Schwelle eines offiziell erklärten Krieges zu erreichen.

I

i3VE-Smartphone	iPhones speziell gesichert für das sichere militärische Netz
Identity Awareness	Identitätsbewusstsein
IDU	Integrated Display Unit (Displayeinheit für Luftfahrzeuge)
IFC	Industry Foundation Classes (ISO-Standard zur digitalen Beschreibung von Gebäudemodellen)
IFF	Identification Friend/Foe (Freund-Feind-Erkennung)
IKDOK	Innerer Kreis der operativen Koordinierungsstruktur
IKT	Informations- und Kommunikationstechnologie (Überbegriff aller computer- und netzwerkbasierten Technologien, als auch der verbundenen Wirtschaftsbereiche)

IKT-Truppe	Truppenteil der Cyberkräfte
IKTBetr	IKT-Betrieb (Bereich des IKT&CySihZ)
IKTCyPl	Abteilung IKT Cyberplanung für die GDLV
IKTPl	Abteilung IKT-Plan im BMLV
IMM	Informationsmodul Miliz
Inbound	Eingehend (Datenübertragung)
Incident	Vorfall
Incident Handling Process Post Incident	Bewältigung von Vorfällen
Incident Response	Reaktion auf Vorfälle
InfluxDB	Datenbankmanagementsystem
Information Protection Node	Lösung zum Klassifizieren und/oder zum Schutz von Daten
INMARSAT	Satellitenkommunikationssystem
InstFl/FIFlATS	Institut Flieger/Flieger- und Fliegerabwehrtruppenschule
Intrusion Detection and Prevention	System zur Erkennung und Verhinderung von Angriffen
IP-Netzwerke	Internet Protocol Netzwerke
IRIDIUM	Satellitenkommunikationssystem
ISK	Informationssicherheitskommission
ISMS	Information Security Management System
IT	Informationstechnologie
ITSM	IT-Service-Management
iZMS	Interoperables Zutrittsmanagementsystem

J

J5	Abteilung für Planung auf Ebene höherer Kommanden
J6	Abteilung für IKT-Belange auf Ebene höherer Kommanden

Stichwortverzeichnis

Jamming	Stören von Signalen (Störsender)
JGSWG	Joint Geospatial Working Group
JITSI	Open Source Videokonferenzsoftware

K

Karten	Darstellung eines räumliches Gebildes auf einer Fläche
KBC	Kapsch Business Com (Unternehmen)
KdoFüU&CD	Kommando Führungsunterstützung und Cyber Defence
KdoSK	Kommando Streitkräfte
KdoSKB	Kommando Streitkräftebasis
KFOR Chief Geo	Kosovo Forces (Höchster Geograph der KFOR)
KI	Künstliche Intelligenz
Klon	Identische Kopie (des Betriebssystems)
Klonstraße	Aufreihung vieler Geräte auf denen das geklonte Betriebssystem installiert wird
Krypto	Kryptographie (Wissenschaft der Verschlüsselung von Informationen; Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind)
KURSIS	Kursinformationssystem
KUWEL	Kurzwelle Land

L

Labelling	Markieren/Beschriften von Daten/Objekten
LAN	Local Area Network (Lokales Netzwerk)
Legic	Chipkartentechnologie
Leonardo	Leichter Mehrzweck-Hubschrauber des ÖBH
LFG	Luftfahrtgesetz
LI/LL	Lessons Identified/Lessons Learned

Liferay DXP	PuMa-Ablöse (neues CMS)
Loadbalance	Lastverteilung in Netzwerken
Lockdown	Eine Ausgangssperre oder Absperrung bzw. Versiegelung von Gebäuden und Bereichen
LOD	Low Altitude Danger (Unterer Luftraum, Flugbeschränkungsgebiet)
Log	Dokumentationsdaten von Änderungen/Ereignissen
LOGIS	Logistikinformationssystem
Look-and-Feel	Aussehen und Bediengefühl
LOR	Low Altitude Restricted (Unterer Luftraum, Flugbeschränkungsgebiet)
LRR	Long Range Radar
LRSiOp	Luftraumsicherungsoperation
LSF	Liste staatlicher Funk
LTE	LongTermEvolution (Mobilfunkstandard 3.9)
Lu/Lu Schießen	Luft-Luft-Schießen
LuAufklESt	Luft Aufklärungseinsatzstelle
LVId	Landesverteidigungs-Identifikationsnummer
LWL	Lichtwellenleiter
LZ	Lagezentrum

M

Malware	Schadsoftware
Matchbox	Virtueller Übungsraum
MAVE	Antischadsoftware-Programm
mblGeoEt	Mobiles Geo-Element
MD	Military Domain (Netzwerk im ÖBH)
Metadaten	Strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten
Metrics Collection	Metadaten-Sammlung

Stichwortverzeichnis

Metrik	Kennzahlen/Metadaten
Memorandum of Understanding	Vereinbarung zwischen zwei oder mehreren Parteien
MGI	Militärische Geoinformation
Mifare	Chipkartentechnologie
MIGIS	Militärisches Geoinformationssystem
MilAk	Militärakademie
MilCERT	Military Computer Emergency Readyness Team
milCPS	military Cyber-Protection System (Militärisches Cybersicherheitssystem)
MilGeo	Militärisches Geowesen
milGeoVA	Militärisches Geowesen Virtual Analysis
MILIS	Militärisches Informationssystem
Miliz	Streitkräfte, die zum größten Teil/vollständig aus Wehrpflichtigen im Bedarfsfall aufgestellt werden
Milizexperten	Experten aus verschiedenen Wissensgruppen aus dem Milizstand
MIMZ	Militärisches Immobilien Management Zentrum
MISP	Malware Information Sharing Platform (Plattform für Bedrohungsinformationsaustausch)
Mission Network	Einsatznetzwerk
MissionPlanningSystem	System zur Planung von Einsätzen
MLB	Militärische Landesbeschreibung
MLU	Midlife Upgrade
Mode S/Mode 5	Modus selektiv/Modus verschlüsselt (Sekundärradar)
Motion-Sickness	Bewegungskrankheit
Mountain Training Initiative	Europäische Ausbildungsinitiative zur Verbesserung der Gebirgseinsatzfähigkeit
MoVe	Mobilität in der Verwaltung (Zentrale Steuerung aller Dienstkraftfahrzeuge der Ministerien)
Moving-Map-Systeme	Navigationssystem (Aktuelle Position wird immer in der Mitte der Karte anstatt als Koordinaten angezeigt
MPC	Mid Planning Conference

MPH FTCN	Future Tactical Communication Network
MPR	Microwave Packet Radio
MSK17	Militärstrategisches Konzept 2017
MSS	Microwave Service Switch
MTM	Mail- und Termin Management
Multiplexing	Prozess des MUX
MUX	Multiplexer analoge/digitale Selektionsschaltung, bei der aus mehreren Eingängen ein Ausgang geschaltet werden kann

N

NAFRA	national radio frequency agency
NATO	North Atlantic Treaty Organization
NavWar	Navigation Warfare (Kriegsführung über Navigation)
NCAS	National Crypto Algorithm System (Verschlüsselung von international klassifizierten Daten zur Übertragung)
NDA/MoD	National Distribution Authority/Ministry of Defence
Network Deception Lösung	Sicherheitsstufe in Netzwerken zusätzlich zu Firewalls
NGIF	NATO Geospatial Information Framework
NISG	Netz- und Informationssystemsicherheitsgesetz
NSA	national security agency
NVÖ	Nebenstellenverbund Österreich

O

ÖBH	Österreichisches Bundesheer (Streitkräfte der Republik Österreich, dem die militärische Landesverteidigung obliegt und nach den Grundsätzen eines Milizsystems einzurichten ist)
ObstdG	Oberst des Generalstabsdienstes
ODU	Outdoor Unit (Außeneinheit)
OE	Organisationseinheit

Stichwortverzeichnis

Öffentlichkeitsarbeit	Management der öffentlichen Kommunikation von Organisationen gegenüber ihren internen/externen Anspruchsgruppen
ofFMSys	Ortsfestes Fernmeldesystem
ofRVN	Ortsfestes Richtverbindungsnetz
OGC	Open Geospatial Consortium
ÖMKFL	Österreichische Militärkarte Flieger
Open Source	„Offene Ressource" (Software für jedermann lizenzfrei zugänglich, Quellcode öffentlich verfügbar)
OpKoord	Operationskoordination
Oracle	Amerikanisches Soft- und Hardwareunternehmen
ORF	Österreichischer Rundunk
Org	Organisation (Abteilung im BMLV)
ORGIS	Organisationsplan Informationssystem
Orgplan	Organisationsplan
ORS	Ortsfeste Radarstation
Orthofotos	Verzerrungsfreie und maßstabsgetreue Abbildung der Erdoberfläche aus Luft- oder Satellitenbildern abgeleitet
Outbound	Ausgehend

P

PAAN	PERSIS Automationsunterstützte Abrechnung von Nebengebühren
Pandemie	Neue, zeitlich begrenzte, weltweite, starke Ausbreitung einer Infektionskrankheit mit hohen Erkrankungszahlen
PersA	Personalabteilung A im BMLV
PersAppl	Personal Applikationen
PERSIS	Personalinformationssystem
PGBACKREST	Post Gre Backup Restore
Phishing	Beschaffung persönlicher Daten anderer unwissender Personen
PIONEER	InteroPerability and DIgitization Of INtelligencE GathEring PRocesses ;]

PKI	Public Key Infrastructure (System, das digitale Zertifikate ausstellen, verteilen und prüfen kann)
Plug and Play	Anschließen und loslegen
PM-Bund	Personalmanagement des Bundes mit SAP
PostgreSQL	Freies objektrelationales DBMS
PrK	Präsidentschaftskanzlei
ProofofConcept	Funktionsbeweis eines ersten Prototypen
PS-NT	Personalsysteme Neue Technologie
PTC	Pre Travel Clearance
PTMP	Point To Multi Point
PTT	Push to Talk (Direktsprechverbindung im Funksprechverkehr)
PuMa	Publish Manager

Q

QGIS	Freies Open Source Geographisches Informationssystem der Firma QGIS
QR-Code	Quick-Response Code (zweidimenionale Darstellung der binären Codes von ASCII-Zeichen)

R

Radar	Radio Detection and Ranging (funkgestützte Ortung und Abstandsmessung)
RadStlg	Radarstellung
Ransomware	Schadprogramm mit Verschlüsselungsfähigkeit
Rasterbildform	Pixelbasiertes Bild
RCID	Resistive Capacitive Identification
RCIED	Radio Controlled and improvised explosive Device (funkausgelöste improvisierte Sprengkörper)
Rechenzentrum	Gebäude/Räumlichkeit in dem/der die zentrale Rechentechnik einer oder mehrerer Unternehmen/Organisationen untergebracht ist
redundant	Mehrfach vorhanden
Release	Veröffentlichung
Reputationsdatenbanken	Datenbank vertrauenswürdiger Quellen

Stichwortverzeichnis

Requests for Change	Anfrage für Änderungen
RHEL	Red Hat Enterprise Linux (Linux basiertes Betriebssystem)
RiFu	Richtfunk
Ripple	Sammlung mehrerer Schwachstellen in einer weit verbreiteten Architektur von Kommunikationsprotokollen
RIPTIDE	Resilient Position Navigation and Timing Testing for Defence
Rollout	Veröffentlichung neuer Softwareprodukte und die Verteilung an Kunden sowie die Integration in bestehende Systeme
Router	Netzwerkgerät, das Daten zwischen mehreren Netzwerken weiterleitet (trennt Netzwerke)
Routing	Wegfindung im Netzwerk zur nächsten Station eines Datenpaketes
ROZ	Restricted Operation Zones
RRT	Rapid Response Team (Schnell einsatzbereites Team)
RSM	Resolute Support Mission
rugged und tempest NB	Gehärtete Notebooks
RüstPol	Abteilung für Rüstungspolitik im BMLV
RWARE	Retrieval Ware (Metadatensuchmaschine)
RZ	Rechenzentrum
RZL-Plan	Ressourcen-, Ziel- und Leistungsplan

S

SAA	Security Accreditation Authority (Akkreditierung von Informations- und Kommunikationstechniksystemen)
SAN	Storage Area Network
Sandbox	Software-Testumgebung; Isolierter Bereich ohne Auswirkung auf die Umgebung
Schlüsselarbeitskräfte	Für den Betrieb essentielle Arbeitskräfte
Schlw	Schlüsselwesen
SCPC Mode	Single Channel per Carrier Mode (Ein Kanal pro Gerät)

SD4MSD	Single Device for Multiple Security Domains (Ein Endgerät für verschiedene Sicherheitsstufen)
SDH	Synchrone Digitale Hierarchie
SecOps	Security Operations
Security Patches	Sicherheits-Updates
selWLANRekr	Selektives WLAN für Rekruten (IKT-Service)
SIEM	Security Information and Event Management (Echtzeitanalyse von Sicherheitsalarmen; lokal oder als Cloudservice)
sihpolAssE	Sicherheitspolizeilicher Assistenzeinsatz
Silentel	App für sichere mobile Kommunikation (NATO zugelassene Lösung für klassifizierten Sprach- und Datenaustausch)
SIM-Karte	Subscriber Identity Module Karte (Chipkarte, die zur Identifikation des Nutzers in ein Mobiltelefon eingesteckt wird)
SK	Streitkräfte
SKB	Streitkräftebasis
SMIR	Spectrum Management Repository (Software)
SMN	Sicheres Militärisches Netz
SMN.mobile	Ablöse der GovNetBox; mobiler VPN-Zugang in das SMN
SMS	Short Message Service (Kurznachrichtendienst)
Software	Sammelbegriff für Programme und die zugehörigen Daten
Spam	Unerwünschte, massenhaft per E-Mail oder auf ähnliche Weise versandte Nachrichten
Spoofing	Verschleierung oder Vortäuschung; Täuschungsmethoden zur Verschleierung der eigenen Identität
Sport	Körperliche Betätigung
SSD	Solid State Drive (schnelle Festplatte ohne bewegliche Teile)
SSP	Service Schwerpunkt
SSP ZABL	SSP zentrale Anwenderbetreuung LOGIS
SSP ZS	SSP zentrale Services
SSRS	System Specific Security Requirements (Systemspezifische Sicherheitsanforderungen)
Stammportal	Plattform zur Selbstverwaltung für Mitarbeiter des Bundes

Stichwortverzeichnis

STANAG	Standardisation Agreement - NATO
standalone	Alleinstehendes (IT-)Produkt
SUB	Sicherheitsunbedenklichkeitsbescheinigung
SW	Software
SWIFT BLADE	Multinationale Hubschrauber-Übung
Switch	Umschalter, Weiche (Kopplungselement in Rechnernetzwerken)

T

TA	Technical Agreement
Tablet	Tragbarer flacher, leichter Computer mit Bildschirm der durch Eingaben mit den Fingern reagiert
Tachymeter	Gerät zur Horizontalrichtung- Vertikalwinkel- und Schrägstreckenbestimmung
TAP	Truppenanschaltpunkte
TCN	Tactical Communication Network
TDM	Time Division Multiplexing (Methode zur Übertragung von Datenströmen)
te/tak Fähigkeiten	Technische/Taktische Fähigkeiten
TEC	Technologiegespräche Forum Alpbach
TechnologieStack	Datenökosystem (Liste aller Technologiedienste zum Erstellen/Ausführen einzelner Anwendungen)
Teilmobilmachung	Teilmobilisierung der Streitkräfte (Einberufung von Teilen der Miliz)
Teiltauglichkeit	Ableistung des Grundwehrdienstes mit leichten körperlichen Einschränkungen, „Grundwehrdienst nach Maß“
Teleworking	Regelmäßiges Arbeiten an einem anderen Arbeitsplatz als das Gebäude des Arbeitgebers
TFS	Truppenfunksystem
Threat Intelligence	Informationsbeschaffung über Bedrohungen und Bedrohungsakteure im Cyberraum
Threat Response	Erkennung, Untersuchung und Reaktion auf Schadsoftware im Netzwerk
TIGER MEET	NATO Luftraumüberwachungsübung, an der nur Einheiten mit Tiger im Namen oder Wappen teilnehmen dürfen
Timeseries Database	Zeitreihendatenbank (Datenbank für das Speichern und die Analyse von Zeitreihen wie z.B. Sensordaten)

TKV	Telekommunikationsverbund
TLZ	Technisch logistisches Zentrum
TN	Truppennummer
topographisch	Natürliche Erdoberfläche mit ihren Höhen, Tiefen, Unregelmäßigkeiten und Formen
Tracker	Drohnensystem des ÖBH
Tunneling	Virtueller abstrahierter Übertragungsweg
TÜPl	Truppenübungsplatz
TvZ	Test vor Zuschlag

U

UHF	Ultra High Frequency (Ultra hohe Frequenz)
UNFICYP Force Cartographer	United Nations Peacekeeping Force in Cyprus (Militärkartograf im Auslandseinsatz auf Zypern)
UNIS	IT-Unterstützung der Auslandseinsatz-Planung, Verwaltung und Besoldung
Updates	Software-Aktualisierungen
URL	Uniform Resource Locator (Standard für die Adressierung einer Website)
UseCase	Anwendungsgebiet
USV	Unterbrechungsfreie Stromversorgung
UZEloKa	Unterstützungszentrum EloKa

V

VbÜb	Verbandsübung
VersNr	Versorgungsnummer
VFR/IFR	Visual Flight Rules / Instrument Flight Rules (Sichtflugregeln / Instrumentenflugregeln)
VHF	Very High Frequency (Sehr hohe Frequenz)
Visual Computing	Grafische Datenverarbeitung
Visualisierung	Umwandlung abstrakter Daten in eine grafische, visuell erfassbare Form

Stichwortverzeichnis

VKS13	Videokonferenzsystem 13
vlgbFMSys	Verlegbares Fernmeldesystem
vlgbRZ	Verlegbares Rechenzentrum
VM	Virtuelle Maschine (virtuelle Umgebung zur Simulation von IT-Geräten, PC am PC)
VO Funk	Vollzugsordnung für den Funkverkehr
VPN	Virtual Private Network (gesicherte Netzwerkverbindung mithilfe von Tunneling)
VR	Virtual Reality (Virtuelle Realität - meist mit Vollvisierbrille)
VR-Sickness	Überkeit hervorgerufen durch die Verwendung einer VR-Brille (vergleichbar mit Seekrankheit)
VSAT	Very Small Aperture Terminal (Satellitenempfänger und Sender mit Antennen für satellitengestützte Kommunikation)
VTA	Verpflegsteilnehmer-Erfassung und bargeldlose Abrechnung
VTC	Video-Tele Conference (Videokonferenzsystem)
VULN	Vulnerability (Verwundbarkeit)
Vulnerability Monitoring	Überwachung von Schwachstellen

W

WAF	Web Application Firewall (Netzwerksicherheitskomponente gegen Angriffe aus dem Internet)
WarRoom	Kommandozentrale
Warfare	Operationen von Streitkräften
Web	„Netz" (meist Internet)
WEBEX	Videokonferenzsoftware
Webproxy	Vermittelnde Kommunikationsschnittstelle in einem Netzwerk
Webshop	Einkaufsplattform im Internet
Windows 10	Microsoft Betriebssystem
WLAN	Wireless-LAN (Kabelloser Zugang zu Netzwerken über Access-Points)
World in miniature navigation	Navigation des Standpunktes durch Verschieben der Person im Modell

WPTT	Wireless Push-To-Talk (Drahtlose Sprechtaste)
WSM	Abteilung Waffensysteme und Munition

X

XIRIS	Extended Integrated Reporting Infrastructure System (Anwendung zum Erstellen von Auswertungen von Daten aus anderen Anwendungen)

Z

ZBS	Zentrales Berechtigungs System
ZEDVA	Zentrale-Elektronische-Daten-Verarbeitungs-Anlage
ZentDok	Zentraldokumentation
Zerologon	Software-Schwachstelle
ZGeoBW	Zentrum der Geoinformationen der Bundeswehr
zIaaS	Zentrale Infrastructure as a Service
ZMS	Zutrittsmanagementsystem
ZTA	Abteilung im BMLV für Zentrale Technische Angelegenheiten

Bundesministerium für Landesverteidigung

IMPRESSUM:
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, soweit nicht ausdrücklich anders gekennzeichnet
Hersteller & Druck: Heeresdruckzentrum, 1030 Wien

Produziert nach den Richtlinien des Österreichischen Umweltzeichens

Platzhalter für Zertifizierungslogo