LEISTUNGSBERICHT 2022

DIREKTION IKT&CYBER

UNSER HEER

Bundesministerium für Landesverteidigung

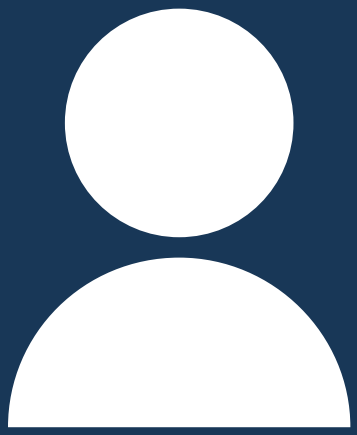
Die Bezeichnungen in diesem Leistungsbericht betreffen Männer, Frauen wie auch nichtbinäre und diversgeschlechtliche Personen gleichermaßen.

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

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.

Inhaltsverzeichnis

LEITUNG



GenMjr Ing. Mag. Hermann KAPONIG

Leitung Direktion IKT&Cyber

„Digitalisierung bedeutet vielmehr auch die Chance, die Prozesse im Rahmen der Transformation anzupassen oder sogar gänzlich neu aufzusetzen.“

Es ist mir eine große Freude den neuen Leistungsbericht der Direktion IKT&Cyber für das Jahr 2022 präsentieren zu dürfen. Wir haben uns entschlossen, diesen Leistungsbericht in einem neuen umfassenderen Setting vorzulegen. Dies erfolgt nun im Gegensatz zu den letzten Jahren, wo wir nur den Leistungsumfang der Organisationsbereiche des IKT&Cybersicherheitszentrums präsentiert haben.

Da wir auf Grund der Reorganisation seit 1. Juli 2021 auch diesen Fähigkeitsbereich im Ressort gebündelt haben, sind wir nun als Direktion IKT&Cyber im Rahmen der Generaldirektion Landesverteidigung (GDLV) breiter aufgestellt. Die Leistungsbereiche der Cyberkräfte (IKT-Truppe, Elektronische Kampftruppe, Cybertruppe, IKT-Provider und Informationskräfte) wurden überwiegend im Organisationsbereich der Direktion IKT&Cyber zusammengeführt. Dazu wurden die relevanten Aufgaben- und Organisationsbereiche der Zentralstelle/BMLV (die Aufgabe des Chief Digital Officer (CDO) und Chief Information Officer (CIO) und des Cyber- Koordinators, die Abteilung IKT- Planung [IKTPl] und die Abteilung Führungsunterstützung [FüU]), sowie der Streitkräfte (die J6-Abteilung [J6/SK], das Führungsunterstützungsbataillon 1 [FüUB1] und das Führungsunterstützungsbataillon 2 [FüUB2]), der Streitkräftebasis (die G6-Abteilung [G6/SKB], das IKT&Cybersicherheitszentrum (IKTCySihZ) und die Führungsunterstützungsschule [FüUS]), inklusive deren Hauptkanzleien, in der neuen Direktion IKT&Cyber zusammengeführt.

In der nunmehrigen Organisation der Direktion IKT&Cyber ist der Direktor IKT&Cyber gleichzeitig Chief Digital Officer (CDO) und Chief Information Officer (CIO) des BMLV, Kommandant der Cyberkräfte des Österreichischen Bundesheeres und Leiter des IKTCySihZ. Die Planungskomponente in Form der Abteilung IKT&Cyber Planung (IKTCyPl), die

Einsatzführungskomponente in Form der Abteilung IKT&Cyber-Einsatz (IKTCyE) wurden angepasst und die operativen Elemente mit dem IKTCySihZ, der FüUS und dem FüUB1 und dem FüUB2 übernommen. Die Reorganisationsmaßnahmen sind zum Zeitpunkt der Drucklegung noch im Laufen.

Wir wollen mit unserem Leistungsbericht 2022 nunmehr das breite Spektrum unseres Leistungsumfanges darstellen. Einige besondere Themen will ich im Rahmen meiner Ausführungen besonders hervorheben:

Digitalisierung im Bundesheer bedeutet die digitale Transformation ins 21. Jahrhindert sicherzustellen. Die Digitalisierung gilt als wesentlicher Treiber zur Weiterentwicklung der operationellen Fähigkeiten des Bundesheeres für Einsätze im In- und Ausland. Dies ist besonders wichtig, da wir im Ressort aktuell am Aufbauplan zum ÖBH2032+ arbeiten. Daher wurde dazu ein temporäres, so genanntes Cyber-Informations-Fähigkeitsboard (CIFB) gebildet, um die notwendigen Grundlagen in unserem Fähigkeitsbereich für die Streitkräfteentwicklung zum ÖBH2032+ aufbereiten zu können.

Gleichermaßen muss die digitale Transformation Beiträge für die Steigerung der Leistungsfähigkeit im Tagesbetrieb und damit der sogenannten Verwaltung mit sich bringen. Wo notwendig und zweckmäßig, sind hier auch bundesweite oder internationale Entwicklungen mit zu berücksichtigen. Um hier nationale Entwicklungen mit berücksichtigen zu können, arbeiten wir im Bund im Rahmen der „CDO-Task Force“ und IKT-Konsolidierung aktiv mit. Internationale Entwicklungen werden durch aktive Mitarbeit in bi- oder multinationalen Gremien berücksichtigt und in verschiedensten Übungsformaten konkret erprobt und geübt.

Digitalisierung ist in unserem Verständnis nicht nur das reine Umwandeln von analogen oder teildigitalisierten Prozessen in durchgängige digitale Prozesse. Digitalisierung bedeutet vielmehr auch die Chance, die Prozesse im Rahmen der Transformation anzupassen oder sogar gänzlich neu aufzusetzen. Idealtypisch sollten solche Prozesse durch den jeweiligen Prozesseigner angestoßen und gemeinsam mit dem Fähigkeitsbereich IKT & Cyber realisiert werden. Wir legen besonderen Wert darauf, dass auch im Zuge von Digitalisierungsmaßnahmen systemisch militärische Notwendigkeiten entsprechend berücksichtigt, den Notwendigkeiten der Cybersicherheit Rechnung getragen und Daten und Informationen zentral bereitgehalten und verfügbar gemacht werden. Am Ende des Tages muss Digitalisierung jedenfalls einen Mehrwert für die Organisation mit sich bringen.

Im Jahr 2022 wurden maßgebliche Schritte zur Bereitstellung wesentlicher Grundlagen gemacht. Im Rahmen der Bearbeitungen der Arbeitsgruppe „Digitalisierung und IKT“ (AG DIKT) wurden unter der Federführung unseres Datenschutzbeauftragten (DSB/BMLV), Ministerialrat Dr. Gerhard Bernardi und einer Vielzahl mit Experten und Mitarbeiter:Innen des gesamten Ressorts wesentlichen Strategien ausgearbeitet. Mittlerweile wurden eine neue Digitalisierungsstrategie, eine neue IKT-Strategie und eine neue IKT-Sicherheitsstrategie in Kraft gesetzt. Die Bearbeitungen zu einer neuen KI- Strategie (Künstliche Intelligenz) und einer neuen Datenstrategie sind bereits gestartet worden.

Auch wurde durch die Abteilung IKTCyPl eine neue Leitlinie für Informations- und Wissensmanagement (IWM) erarbeitet und mittlerweile verfügt. Die Arbeiten zu einer „Leitlinie Cyberverteidigung“ sind ebenfalls sehr fortgeschritten und in der Finalisierung. Zudem wurde ein Projekt "Individuelle Datenverarbeitung (IDV) und individuelle Anwendungsentwicklung (IAE)" gestartet, um u.a. Insellösungen wo zweckmäßig zusammenzufassen und zentral bereitzustellen.

Um den Digitalisierungsprozess abgestimmt weiter zu treiben und die notwendigen Mechanismen dazu zu entwickeln, wurde ein „Strategisches Lenkungsgremium“ auf höchster Ebene im Ressort etabliert. Aktuell wird dazu an der Ausplanung eines „Strategischen Unterstützungselements Digitalisierung“ gearbeitet.

Das Jahr 2022 hat im Rahmen der „auslaufenden COVID-Pandemie“ wieder zugelassen, dass im Bearbeitungsrhythmus einigermaßen Normalität eintreten konnte. So konnten wieder national und international Übungen, Veranstaltungen und Kooperationsmaßnahmen durchgeführt und wahrgenommen werden. So konnte ich wieder bei den „EU Cyber Commanders Strategic Conferences (CyCo)“, den „EU CIS Director/ Cyber Commanders Conferences“, oder den „NATO Cyber Commanders Foren (CCF)“ dabei sein. Die Fachtagungen im DACH-Format (DEUTSCHLAND, ÖSTERREICH, SCHWEIZ) wurden wieder durchgeführt. Die Kooperation mit der National Guard VERMONT/ USA konnte im Fachbereich gestartet werden.

Höhepunkt am Ende des Jahres war eine durch den Staatssekretär für Digitalisierung initiierte gesamtstaatliche Studienreise mit Staatssekretär Florian Tursky, MBA MSc und seinem Kabinett, Parlamentariern, den CDO‘s des Bundes und Verantwortlichen aus den Bundesländern nach TALLINN/ESTLAND, um sich hier „Best practices“ in verschiedensten Bereichen präsentieren zu lassen und Ideen für Digitalisierungsvorhaben in Österreich zu holen.

Auch konnte ich im Rahmen von Dienstaufsichten bei den Dienststellen der Direktion IKT&Cyber über das ganze Jahr Eindrücke von der Leistungsfähigkeit und Leistungsbereitschaft unserer Cyberkräfte in ganz Österreich gewinnen.

Besonders erfreulich war die erfolgreiche Durchführung einer Vielzahl von nationalen und internationalen Übungen im Fachbereich. Hier möchte ich besonders, auf die mit den Kameraden des „Kommando Cyber- und Informationsraum (KdoCIR)“ der Deutschen Bundeswehr gemeinsam durchgeführten internationalen Cyberübung „Locked Shields 2022 (LS22)“ hinweisen. Dabei haben wir sehr gut abgeschnitten und konnten trotzdem viel dazu lernen.

Auch die internationale Übung „Coalition Warrior Interoperability Exercise 2022 (CWIX22)“, die trinationale „Common Roof 2022 (CR22)“ im DACH-Format und die im Ressort durchgeführte Notkommunikationsübung konnten wesentlich zur Übung der Fertigkeiten und zur Weiterentwicklung im Fähigkeitsbereich beitragen.

Ein besonderes Highlight des Jahres war der Start des neuen „Fachhochschulstudiengangs Militärische IKT-Führung (FHStG MilIKTFü)“ an der Theresianischen Militärakademie. Nach langen und umfassenden Vorbereitungsmaßnahmen konnte der erste Lehrgang im Herbst mit einem überdurchschnittlichen Anteil an Kursteilnehmern gestartet werden. Ich gratuliere der Militärakademie zu diesem Erfolg. Er ist ein wesentlicher Baustein für die qualifizierte Nachwuchsgewinnung im Fachbereich.

Auch hat uns im gesamten Ressortbereich, aber insbesondere im Bereich der Direktion IKT&Cyber, die Prüfung des Rechnungshofs im BMLV zur „Organisation Cyber–Defence im BMLV“ ordentlich beschäftigt. Der Endbericht wird wohl in Kürze veröffentlicht.

Besonders erwähnen möchte ich auch die im Spätherbst durch uns durchgeführte 10. BWÜ (Waffenübung im Fachbereich) für über 70 Milizexperten im Rahmen der Direktion IKT&Cyber. Diese Übungen werden gerne angenommen, halten unsere Experten am aktuellen Stand der Entwicklungen und fördern letztlich den Teamgeist. Ich bin stolz auf unsere Experten aus der Wirtschaft und des öffentlichen Lebens, die in den verschiedensten Bereichen unseres Fachbereichs verwendet werden. Ich freue mich immer wieder über deren ungebrochene Bereitschaft aus ihrem zivilen Beruf heraustretend, an solchen Übungen oder bei Spezialaufträgen zur Stelle zu sein.

Personalgewinnung war schon 2022 ein Schwergewichtsthema. Wir hoffen, dass wir in allen Bereichen entsprechend aufwachsen können, um die Herausforderungen der Zukunft mit hochqualifizierten Mitarbeiter:Innen meistern zu können. Vor allem im Provider- und Cyberbereich hoffen wir mit den neuen RIVIT-Verträgen (Richtverwendungen für IT-Fachpersonal) in den folgenden Jahren entsprechend aufwachsen können.

In diesem Zusammenhang darf ich unserem Dienststellenausschuss IKT&CySihZ, mit dem Vorsitzenden ADir Erwin FINK, meinen besonderen Dank für die hervorragende Arbeit und dem konstruktiven Miteinander für die Mitarbeiter:Innen und die Organisation aussprechen.

Personell hat sich im Bereich der Direktion IKT&Cyber einiges getan. Ich möchte hier auszugsweise einige Personalentwicklungen anführen:

Mitte des Jahres haben wir die Abteilungsleiterin Org&LogAppl/Bereich Appl, Frau Sylvia KRAUT-GARTNER in den Ruhestand verabschiedet. Die Abteilung wird bis zur Ausschreibung interimistisch durch den Stellvertreter Herrn Chefanalytiker Ing. Martin BERNHARD geführt.

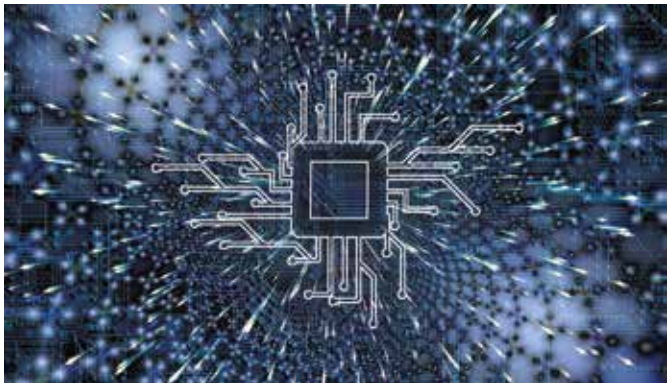
Auch haben wir Mitte 2022 den stellvertretenden Institutsleiter des IMG/IKTCySihZ (Institut für MilGeo-Wesen), Herrn Oberst Mag. Gerald GNASER in den Ruhestand verabschiedet. Ihm nachgefolgt ist mittlerweile nach erfolgtem Ausschreibungsverfahren Herr Oberst des höheren militärtechnischen Dienstes Mag. Dr. Tamino EDER, MBA.

Ende 2022 haben wir den Bereichsleiters IKT-Betrieb/IKTCySihZ, Herrn Hofrat Ing. Harald STEINDL, MSc in den verdienten Ruhestand verabschiedet. Der Bereich wird nun bis zur Ausschreibung interimistisch durch den Abteilungsleiter für Benutzerbetreuung, Herrn Mag. Peter BINDER geführt.

Wir konnten als Kommandounteroffiziers der Direktion IKT&Cyber, Herrn Vzlt Leopold RADLMAIR in unserem Kreis begrüßen.

Auch im Dienstbetrieb gab es einen Personalwechsel. So konnten wir als neue Kommandantin des Dienstbetriebs im IKT&CySihZ, Frau Oberleutnant Nadine FEURHUBER, BA begrüßen, die Herrn Major Mag (FH) Martin WIELAND gefolgt ist. Ihm wünschen wir für die Folgefunktion als S6/IKTCySihZ alles Gute.

Im Bereich der Führungsunterstützungsschule (FüUS) konnten wir als neuen Kommandanten im Rahmen der Truppenverwendung als Generalstabsoffizier, Herrn Oberst des Generalstabsdienstes Mag. Franz SITZWOHL begrüßen. Herrn Oberst Michael HOFFMANN, der die FüUS zuvor 18 Monate interimistisch geführt hatte, darf für seine Leistung herzlich gedankt werden.



Ein Highlight des Jahres 2022 für uns war, dass mit Herrn Gefreiten Georg Felber, ein Cyber-Grundwehrdiener des Militärischen Cyberzentrums (MilCyZ), zum Rekruten des Jahres 2022 gekürt wurde. Das war wohl eine höchst verdiente Auszeichnung für ihn als Person, aber auch eine gewisse Wertschätzung für unseren Funktionsbereich. Damit bestätigt sich unser System des Cyber-Rekruten im Bundesheer als echte Erfolgsgeschichte.

Das nächste Jahr wird für unseren Fachbereich nicht minder fordernd.

Neues Kommunikationssystem - Das klare Schwergewicht wird die Einführung des neuen „Tactical Communication Networks (TCN)“ im gesamten Bundesheer sein. Damit einher geht ein Technologiesprung in den Fähigkeiten des Bundesheeres, ist aber auch mit einer echten Herausforderung für das Personal verbunden.

„All in“ - Eine echte Herausforderung wird die NATO Cyberübung „Locked Shields 2023 (LS23)“. Da stellen wir uns übungstechnisch rein national, mit einem im Leistungsumfang und Dimension noch nie dagewesenen „Blue Team“, auf.

Digitalisierung und Aufbauplan 2032+ werden unsere Kräfte massiv fordern. Hoffentlich dürfen wir dazu bald auf gesicherte Strukturen zurückgreifen.

Abschließend darf ich mich bei allen Kommandanten, Leitern und Mitarbeiter:Innen herzlich für die gezeigten Leistungen im Jahr 2022 bedanken und sie gleichermaßen auch dazu auffordern, im folgenden Jahr mit ihrem Engagement, Wissen und Erfahrung ihren wesentlichen Beitrag für die Erhaltung und Weiterentwicklung Führungsfähigkeit unseres Bundesheeres beizutragen.

Allgemeine Vorstellung

Die Direktion IKT&Cyber stellt in der nunmehrigen Gliederung die Heimat der Cyberkräfte und der Informationskräfte dar. Damit ist einerseits eine zentrale Anlaufstelle für alle Belange im Bereich der Cyber- Truppe, der EloKa- Truppe, der IKT- Truppe und der Informationskräfte begründet worden und andererseits eine systemische Durchgängigkeit in den Fachbereichen etabliert worden.

Die Aufgaben der Direktion IKT&Cyber sind hierbei vollumfänglich erweitert worden, sodass eine einsatzorientierte und lückenlose Bearbeitung, Implementierung und Bereitstellung für die zukünftigen technologischen Trends, kommenden Übungen und Einsätze aus einer gemeinsamen Hand gewährleistet sind. Aufbauend auf diesem sich ergebenden Mehrwert steht hier die Digitalisierung der Streitkräfte unter Einbeziehung aller Stakeholder im Fokus.

Die neue Struktur der Direktion IKT&Cyber ermöglicht es somit, Vorhaben vom Anfang der Idee und des Bedarfes bis zum endgültigen Einsatz neuer Fähigkeiten in allen zugehörigen Waffengattungen zu begleiten und federführend in den Einsatz zu bringen. Damit wird die Direktion IKT&Cyber aber auch integraler Bestandteil der Kernprozesse der Landesverteidigung. Dieser Verantwortung bewusst, ist es auch das visionäre Ziel der Führung der Direktion hierbei federführend, innovativ und mutig im Rahmen technologischer Zyklen die Streitkräfte zu modernisieren.

Mit der Abteilung IKT und Cyber Planung ist ein zentraler Stakeholder in diesem Prozess in der Direktion verankert. Verantwortlich für die Entwicklung der Fähigkeitsbereiche IKT, Cyber, EloKa und der Informationskräfte werden die Grundsteine im Rahmen des Aufwuchses moderner, vernetzter und interoperabler, international einsatzfähiger Streitkräfte gelegt.

Mit der Abteilung IKT und Cyber Einsatz wurde auch der führungsverantwortliche Anteil der Cyber- und Informationskräfte in die Direktion gegliedert. Neben der Verantwortung zum Führen von Cyber Operationen und der Gestellung zum streitkräfte- übergreifenden operativen Kommando, ist die Abteilung wesentlich für die Führung im Fachbereich direktionsübergreifend verantwortlich.

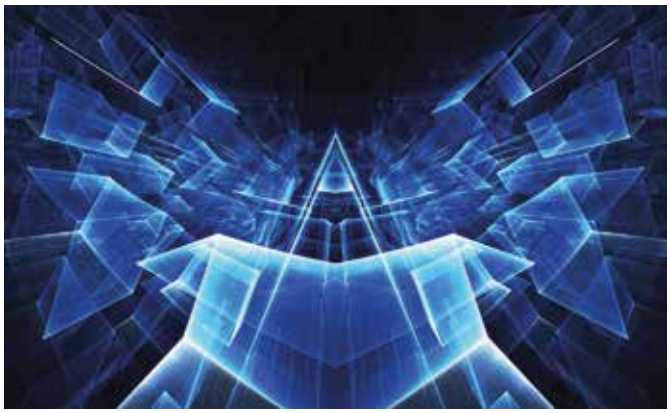
Der Mehrwert der Einsatzführung entsteht hierbei aus der strukturell gegebenen direkten Verknüpfung mit der planenden Abteilung zum Zwecke der Einsatzorientierung. Dabei können die Einsatzerfahrungen und –Erkenntnisse direkt zusammengeführt und die betroffenen Fähigkeiten rasch, effektiv und effizient weiterentwickelt werden.

Die Direktion IKT&Cyber ist aufgabentechnisch auch im Realisierungsmanagement verankert. Dabei ist das Element der IKT und Cyber Bereitstellung und Steuerung etabliert. Es bildet die Schnittstelle der planenden, beschaffenden und einsatzführenden Anforderungen zu den Technikern, Programmierern und Analytiker in den etablierten Bereichen des IKT und Cyber Sicherheitszentrum. In direkter Koordination mit der Direktion Rüstung werden hierbei die geplanten und beschafften Systeme nach den

Kundenvorgaben in die IKT Systeme des Bundesheeres implementiert. Als Zweitaufgabe ist dem Element eben jene Steuerung zugeordnet, die die vorhin erwähnte Koordinierung der Prozesse innerhalb der Direktion IKT&Cyber sicherstellen, bewerten und steuern soll.

Zusätzlich steht der Direktion IKT&Cyber die Führungsabteilung als zentrales Führungselement für die Aufgaben zur Verfügung. Grundsätzlich ausgerichtet, den Bereichen des IKT und Cybersicherheitszentrums die Verwaltung abzunehmen, sind ihr auch umfassende Aufgaben zur Führungsunterstützung innerhalb der Generaldirektion für Landesverteidigung zugeordnet.

Als direkter Ansprechpartner für den Support und die Leistungserbringer sind hier im speziellen die örtlichen Leitbediener und Hauptkanzleien der Direktionen zu sehen. Als ein wesentliches zentrales Element für die Generaldirektion wird durch die Führungsabteilung das übergreifende Wissens- und Informationsmanagement betrieben.



Neben diesen strukturellen Aufgaben gibt es aber auch noch weitere wichtige Aufgaben die seitens der Direktion IKT&Cyber sichergestellt bzw. wahrgenommen werden. So ist die Direktion durch den Leiter das oberste Gremium im Rahmen der Digitalisierung durch personelle Abbildung des CDO und CIO des Ressorts. Neben dem stetigen Ausbau der Cyber Verteidigung ist die Digitalisierung eines der Schwergewichtsprojekte die für eine zukünftige, moderne Ausrichtung der Streitkräfte forciert werden.

Den Kern der Direktion IKT&Cyber bilden aber die Bereiche des IKT und Cybersicherheitszentrums und die nachgeordneten Verbände, sowie die Führungsunterstützungsschule.

Durch diesen Dreiklang ergeben sich vor allem auf Anwenderebene wesentlichen Vorteile von einer raschen Adaption, über die einsatzorientierte Weiterentwicklung und mit gediegener Ausbildung hinterlegte Implementierung neuester Verfahren und Anwendungen. Dabei ist neben der Möglichkeit der direkten Kommunikation auch das gegenseitige Verständnis des Fachbereiches ein essentieller Mehrwert.

Zusammengefasst ist festzuhalten, dass die neue Gliederung der Direktion IKT&Cyber einen essentiellen Mehrwert, Zusammenwirken des Aufwuchses von fachspezifischen Fähigkeiten, deren technisch organisatorischer Entwicklung und deren schlussendlicher Einsatzrelevanz darstellt.

Der Verbund der planenden, militärstrategischen und operativen, sowie die kontinuierliche Einbeziehung der taktischen Ebenen und der Ausbildungsverantwortlichen bündelt hierbei die Kräfte und generiert Synergien in allen Phasen.

GenMjr
Ing. Mag. Hermann KAPONIG
Leiter Dion IKT&Cyber,
CDO/CIO/BMLV

ObstdG
Mag. Christof TATSCHL
ChdStb und stvKdt

Bgdr
Mag. Gerhard WEINER
ÜV IKTCyPl

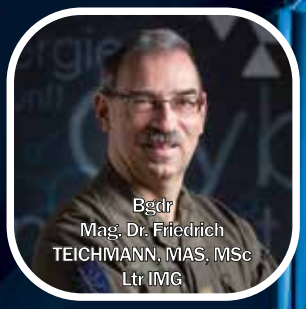
Bgdr
Mag. Arnold STAUDACHER
ÜV IKTCyE

ObstltdG
Mag.(FH) Christoph JEZEK
ÜV IKTCyBerStlg

Mag. Wolfgang HACKER
Ltr IKT-Te. CTO

HR
Ing. Harald STEINDL, MSc
Ltr IKT-Betr

Dipl-HTL-Ing. Lambert
SCHARWITZL, MA, MSc
Ltr MilCyZ



Bgdr
Mag. Dr. Friedrich
TEICHMANN, MAS, MSc
Ltr IMG

HR
Dipl.Ing. Gerald HOFMEISTER
Ltr Appl

Obst
Ernst BERTHOLD, MSD
Kdt FüUB1

Obst
Johannes NUSSBAUMER, MSD
Kdt FüUB2

ObstdG
Mag. Franz SITZWOHL
Kdt FüUS m.d.F.B.

Reorganisation und Herausforderungen

Die bereits 2021 begonnene Reorganisation und Aufstellung der Direktion IKT&Cyber wurde mit den Bearbeitungen am Beginn des Jahres 2022 abgeschlossen. Die Ausgangsbasis für die Struktur bildete die Vorgabe für die strukturellen Vorgaben und VBÄ-Umfang Ende November 2021. Die daraus resultierenden Bearbeitungen mündeten in die Version 5 Anfang des Jahres und in die Version 6, die schließlich den Abschluss der Bearbeitungen bildete. Dabei waren die vorrangigen Ziele, Prozesse beschleunigen (bei Digitalisierung & Cyber sind Geschwindigkeit und rasche hochqualitative Umsetzungen entscheidend!), Entscheidungen im Zuständigkeitsbereich treffen, klare Vermeidung von Duplizierungen der Aufgaben und Ausrichtung der Elemente auf die Leistungserbringung für den Einsatz, Projekte, Vorhaben und Übungen ausschlaggebend.

Der Kunstgriff, mit gleichbleibendem Personalstand die neue Struktur in der Leitungsebene abdecken zu können, war dazu mehr als nur eine Herausforderung, weil durch die zusätzlichen und umfangreichen Aufgaben auch neue Elemente möglichst aufkommensneutral gebildet werden mussten. Daher gab es auch Transfers von der Leitung in die technische Ebene und umgekehrt. Das wurde auch durch die Betrachtungen und Analysen im Zuge des begleitenden Controllings zur Reorganisation immer stringent unterstützt und es wurden auch die Leistungsziele, Produkte und Wirkungen der Organsiationselemente sehr ausführlich beschrieben.

Die gemeinsame Spitze im Ressort ist durch die Reorganisation sichtbar kleiner geworden, weil die Informationsübermittlung relativ schnell über die Besprechungssystematik im kleineren Gremium erfolgt. Was das Informationsmanagement betrifft, hat die Direktion IKT&Cyber dabei maßgeblichen Einfluss auf die Verdichtung wesentlicher Inhalte und Aussortierung von unwichtigen Dokumenten und Vorgängen im Schriftverkehr des Ressorts, getragen durch verstärkte Vorgänge zur inhaltlichen Rationalisierung.

Highlights

Der wesentlichste Benefit ergibt in der Direktion IKT&Cyber durch die Zusammenführung der Organisationselemente für Planung, Bereitstellung und Einsatz, weil das Zusammenwirken innerhalb der Direktion wirksam wird und positive Effekte auf die Umsetzung der Kernprozesse der militärischen Landesverteidigung hat, wenngleich die Steuerung mit minimalem Personalaufwand enorm schwierig zu bewältigen ist.

Obwohl die Systemabteilung IKTS als Anteil der Beschaffung im Kreislauf außerhalb der Direktion angesiedelt ist, führen gut funktionierende Abläufe durch ständige, gegenseitige Abstimmung, die sich aus den bisherigen langjährigen Prozessen weiterentwickelt haben, zu einer ausgesprochen kompakten Zusammenarbeit.

Im Vergleich dazu wird es ungleich schwieriger, die Digitalisierung ohne weitere Ressourcen ungebremst im Ressort forcieren zu können. Das ist eine Mammutaufgabe, wo vor allem die Direktion IKT&Cyber selbst über Gebühr gefordert sein wird, weil es ein erklärtes Kernziel ist, die Digitalisierung der Streitkräfte dahingehend massiv zu fördern und zu unterstützen.

Technische Übungen zur Einsatzvorbereitung

MIC 22 - Military Interoperability Conference 2022 (18 01 – 19 01 Technical Track)

Das erste Highlight des Jahres für die technischen Übungen bildete der Technical Track zur milCERT Interoperability Conference. Der Technical Track wurde über die Cyber Range Cybexer von LUXEMBURG aus gehostet und für die Teilnehmer hybrid abgewickelt.

Wie bereits im Vorjahr wurde das kleine Team mit einem Spitzenplatz am Podest belohnt und für den besten SITE REP ausgezeichnet.

LOCKED SHIELDS 2022 (19 04 – 22 04)

Die Übung "Locked Shields" ist die größte und komplexeste internationale Live-Fire-Übung zur Cyberverteidigung der Welt.

Sie wird seit 2010 vom NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) organisiert. An der Übung sind etwa 5500 virtualisierte Systeme beteiligt, die mehr als 8000 Angriffen ausgesetzt sind.

Neben der Sicherung komplexer IT-Systeme müssen die verteidigenden Teams (Blue Teams) auch bei der Meldung von Vorfällen, der strategischen Entscheidungsfindung und der Bewältigung forensischer, rechtlicher, medien- und informationsbezogener Herausforderungen effizient sein.

Dieses Jahr gab es ein Joint-Team ÖSTERREICH-DEUTSCHLAND, wobei das Forensik-Team in EUSKIRCHEN/DEUTSCHLAND vor Ort die Übung absolvierte, der größte Teil des Blue Teams nahm an der Übung jedoch von Wien aus online teil. Zusätzlich zum Blue Team wurden auch zur Übungsorganisation mehrere Teams nach Tallinn geschickt.
Die Teilnahme erfolgte durch MilCyZ, CERT, Cyber-GWD und Miliz praktisch in allen Subteams, Red Team, Yellow Team und White Team. Das Joint Team belegte den 7. Platz von insgesamt 24 Teams. Im Übungsumfang wurden insgesamt 4000 Systeme gegen 2500 Attacken verteidigt.

Für 2023 ist der Einsatz eines nationalen gesamtstaatlichen Blue Teams in der Größenordnung von etwa 90 Personen geplant und damit ist diese Übung eindeutig ein absolutes Schwergewichtsvorhaben der Direktion IKT&Cyber im neuen Kalenderjahr.

THORS HAMMER 2022 (19 04 – 07 05)

Die Teilnahme an der THORS HAMMER 22 (TH22) war ein weiterer wesentlicher Schritt für das Herstellen der Einsatzbereitschaft der CREW-Systeme. Erstmals konnte auch die Funktionalität des Systems HUSAR-CREW unter Einsatzbedingungen erfolgreich getestet werden.

Ebenso konnte die prinzipielle Wirksamkeit der CREW-Systeme gegen Drohnenfernsteuerungen nachgewiesen werden. Da in Österreich weder eine Testinfrastruktur (z.B. Mobilfunkbereich) noch die für eine Testung erforderlichen realen Bedrohungsmittel (z.B. in Konflikt- und Kriegsgebieten gefundene RCIED oder Bauteile) verfügbar sind, kann diese Anpassung und Überprüfung nur im internationalen Umfeld erfolgen. Das hat insofern besonders Bedeutung, als zum Ziel für die weiteren erforderlichen Maßnahmen die Ausstattung der EUBG2025 mit CREW-Systemen definiert wird und alle diesbezüglichen Ausbildungs- und Testvorhaben auf diese Absicht ausgerichtet werden.

Coaltition Warrior Interoperability Exploration Experimation, Examination, Exercise (CWIX) 2022 (07 06 – 24 06)

Österreich nahm heuer erstmals mit einer Remote Teststellung aus dem Nationalen FMN CIAV Battle Lab und daher nur mit einer kleinen Delegation vorort teil. CWIX bietet im Rahmen ihrer 4 X (in eXploration, eXperimentation, eXamination und eXercise) Gelegenheiten, in allen Phasen der Fähigkeitsentwicklung im Bereich C4ISR den Stand der Interoperabilität von Technik, Personal und Prozessen zu testen, zu validieren, zu verifizieren und zu üben. Alle festgelegten Übungsziele konnten erreicht werden.

Der gesamte Planungsprozess für die CWIX Serie und die dadurch mögliche Informationsgewinnung bedeuten auch für die gesamte Direktion IKT&Cyber eine sehr gute Gelegenheit gemeinsam mit internationalen Partnern planungs-, implementierungs- und betriebsrelevante Grundlagen im Bereich einsatzorientierter Systeme zu erarbeiten und aktiv an der Weichenstellung für kurz- und mittelfristige Vorhaben im IKT-Bereich mitzuwirken.

Neben der Übungstätigkeit und den FMN Aktivitäten wurde die CWIX 2022 daher insbesondere zur Marktforschung genutzt, weil man bei der CWIX IKT-Systeme im Testbetrieb abseits von Hochglanzprospekten beobachten und quasi die Programmierer der Firmen beim Beheben von Mängeln schwitzen sehen kann. Dabei konnte auch der Entwurf der Vorhabensabsicht und die Liste der Anforderungen für die Softwareablöse beim nationalen Führungsinformationssystem auf Plausibilität überprüft werden.

COMMON ROOF (CR) 2022 (03 10 – 21 10)

Die bereits seit langem in den Ländern Österreich, Deutschland und der Schweiz stattfindende multinationale Übung wurde dieses Jahr durch das Führungsunterstützungsbataillon 1 verantwortlich durchgeführt. In der Übung wurden die jeweiligen nationalen Einsatznetzwerke in ein gemeinsames multinationales Mission Network zusammengeführt und festgelegte betriebliche Abläufe und Prozesse anhand einem Szenario und einem Ablaufplan geübt und gleichzeitig evaluiert.

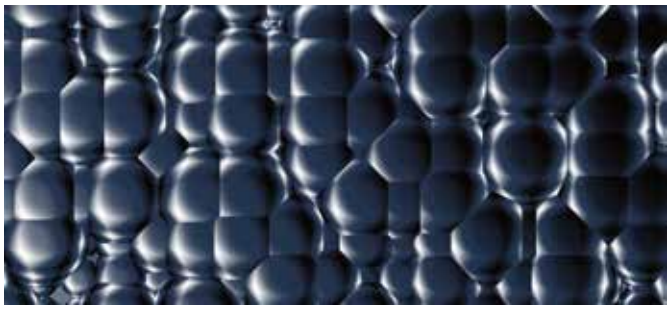
Das Hauptziel planen, errichten, betreiben und schützen eines verlegbaren, nationalen/multinationalen Einsatznetzwerkes nach den Vorgaben des Federal Mission Network ist auch ein wichtiger Schritt in der Vorbereitung der IT-Bedarfe der EUBG 2025.

Leistungsportfolio des Providers

Der Hauptwirkungsbereich der Analysen, der sich in der Leitungsebene immer stark auf die Dokumentation der Leistungsfähigkeit des Providers und die Planungsprognosen stützt, wurde sowohl in der Serviceentwicklung als auch in der Analyse der bestehenden Services durch die Arbeitsgruppe Digitalisierung und Informations- und Kommunikationstechnologie (AG DIKT) unterstützt. Auch 2022 bedurfte es ständiger Neubeurteilungen.

Dabei wirkte immer die Problematik einer ausgewogenen Schichtung der Aufträge mit, um das ständige Ressourcenfehl im Personal ausgleichen zu können.

Für die technischen Bereiche war auch das Jahr nach dem Beginn der Reorganisation nicht gerade einfach. Der Personalaufwuchs war mehr als überschaubar und im Jahresvergleich angesichts der angepeilten Aufwuchsziele weit unter dem beschriebenen Pfad. Der daraus entstandene Rückstau in der Serviceentwicklung, der zu einem nochmals erhöhten Arbeitsaufwand aufstieg, verstärkte die Notwendigkeit, Schwergewichte zu setzen und den Workflow wirklich zielgerichtet einzugrenzen und Arbeitspakete zu koordinieren.



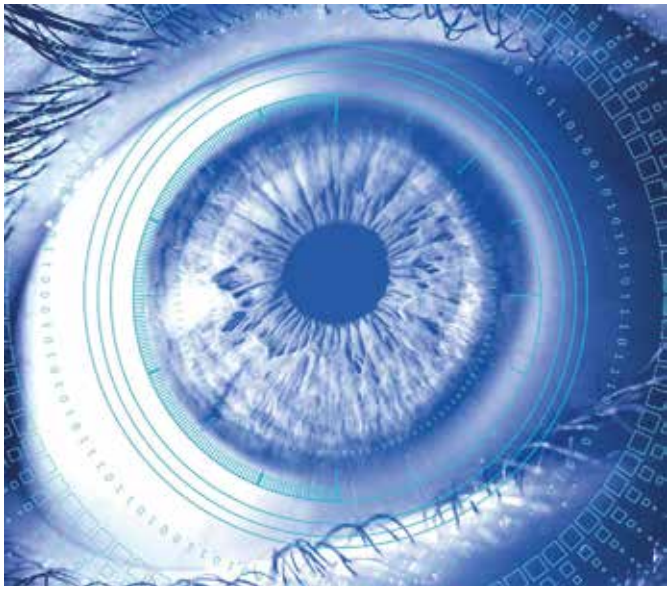
Mit Beginn 2022 setzte im I. Quartal daher ein umfassendes Deconflicting für die Service-Pipeline ein, um die bestehenden Aufträge auch mit Bedacht auf bestehende Verpflichtungen tatsächlich wirklich ausreichend bedienen zu können. Trotzdem gelang es auch 2022, etliche Vorhaben umzusetzen und bereits neue, umfangreiche Aufgaben in der Entwicklung zu beginnen.

Folgende Vorhaben wurden erfolgreich abgeschlossen:

- Entwicklungssvorgang zu Vorhaben „ÖBH-Klon Neu (Win10) + Endgeräte Umstellung der SMN auf Windows 10 und RHEL 7.x (Kamino)“
- Forschungsprojekt "HAMMONDORGEL“ (Ziel, ein Konzept eines Staatsgrundnetzes auszuarbeiten) seitens AIT, wo das BMLV in der Arbeitstgruppe durch IKTPl und IKT&CySihZ vertreten war
- CMS neu – „Bereitstellung eines neuen Content Management-Systems (COTS-Produkt) zur Ablöse der Eigenentwicklung Publish-Manager (PUMA)“
- Computer Assistiertes Testen - Ablöse CUT „Ersatz der SW zur psychologischen Eignungsprüfung“
- S2FIS „Ablöse bestehender dezentraler Access-Datenbanken zur Bearbeitung hochsensibler personenbezogener Daten im S2-Fachdienst“
- Bereitstellung einer 2 Faktor Authentifizierung für das IKT-Service Internet-Mailing (Webmail)
- Servicekatalog „Bereitstellung einer Web-Applikation zur Erfassung und Verwaltung des Servicekatalogs unter Berücksichtigung der Vorgaben der AG DIKT, Teilarbeitsgruppe IKT-Entwicklungsplanung“
- Ablöse Bilddatenbank
- Datenfunksoftware II Realisierungspaket 4
- Erprobung Arbeits- und Transportboot, Sturm- und Flachwasserboot Gehörschutz Bootsfunk; drahtlose INTERCOM

Projekte und Planungsaufgaben

Während in der ersten Jahreshälfte die hauptsächliche planungsmäßige Orientierung in Richtung Verfolgung der Realisierungsziele 2022 bis 2027, Überarbeitung der Kernprozesse, Mitarbeit in der AG Digitalisierung und IKT sowie Mitarbeit in den Hauptprojekten „Unser Heer“ ging, war die zweite Jahreshälfte bereits mit den beginnenden Arbeiten zum Fähigkeitsaufbau ÖBH 2032+ gekennzeichnet.



Maßgebliche Mitarbeit und Einflussnahme erfolgen in einer Vielzahl von Projektvorhaben im gesamten Ressort mit Mitarbeitern der eigenen Direktion, weil der Bereich IKT&Cyber auch als Querschnittsmaterie überall hineinwirkt.

Übersicht über die wesentlichen Projekte und Vorhaben:

- AG DIKT mit Teilarbeitsgruppen DIKTS, IKT-Entwicklungsplanung und Sicherheitspartnerschaft
- Unser Heer B-02 Schwerpunkt Cyber Defence
- Unser Heer A-06 Digitalisierung der Behördenverfahren
- Unser Heer A-02 Optimierung der Rahmenbedingungen für die Miliz
- Unser Heer B06 Drohnenabwehr
- Planspiel Schutzoperation und nachfolgende Bearbeitungen
- Aufbauplan ÖBH 2032+
- Weiterentwicklung der EloKa-Truppe
- Verbesserung der Autarkie des IKT-Systems ÖBH
- Erstellung Systembeschreibung IKT-System Einsatz
- PESCO CBRN SaaS
- Teilprojektgruppe IKT zu AW 169 LEONARDO
- Planungsleitlinie Direktion IKT&Cyber
- Cyber und Informationkräfte Fähigkeiten Board

Überprüfung des Rechnungshofs

Im zweiten Halbjahr kam zu den bereits umfangreichen Bearbeitungen in allen Spektren Planung, Einsatz und Bereitstellung der Überprüfungsauftrag eines Teams des Rechnungshofs. Der Überprüfungsauftrag erfolgte, die Gebarung des Bundesministeriums für Landesverteidigung hinsichtlich der Organisation der Cyber-Defence zu überprüfen. Die Durchführung zur Umsetzung wurde dabei an die Direktion IKT&Cyber mit umfassender Handlungsfreiheit delegiert, die Bearbeitung in Abstimmung mit Revision in sehr unbürokratischer und stets zuvorkommender Zusammenarbeit problemlos vorgenommen.

Die Bearbeitung begann mit einer Einweisung am 14.7. und wurde mit einer Sachverhaltsbesprechung mit dem Überprüfungsteam am 21.12. inhaltlich bereits weitgehend abgeschlossen. Die Einzelschritte dazu wurden auf Grundlage von Fragenkatalogen, Einzelanregungen und vor allem mittels Videokonferenzen in Form von Interviews der beteiligten Experten und Kontaktpersonen aller Dienststellen, die mit dem Überprüfungsauftrag in Verbindung standen, abgewickelt.

Die Themenfelder umfassten einen breit gefächerten Bogen mit rechtlichen Aspekten für Cyber Defence, nationalem und internationalem Handlungsrahmen, Entscheidungsprozessen, gesamtstaatlichem Mechanismus, Beteiligung des BMLV im Krisen- oder Einsatzfall, Zusammenarbeit mit anderen Ressorts, Aufgaben auf Bundesebene, politischem Rahmen für Cyberabwehr, internationalen Beteiligungen und Kooperationen, aktueller Organisationsänderung im BMLV, Beschreibung der Organisationseinheiten, Personalrekrutierung und Ausbildung, Mengengerüste, Forschung und Entwicklung im Cyber-Bereich, Bedrohungsbilder und Bedrohungsszenarien, Maßnahmen und Meldeprozesse, Koordinierungen, Einsatzvorbereitung, Einsatzpläne und Übungen, Kompetenzaufbau, Cybersicherheitpaket, Projektaufträgen, Statistiken und internationaler Zusammenarbeit.

Im Wesentlichen wurde die Aufbauorganisation der Direktion IKT&Cyber als gutes und geeignetes Konstrukt beurteilt und die einzelnen Expertisen in den Bearbeitungsfeldern äusserst positiv aufgenommen und verwertet. Sicher wurde das Überprüfungsteam durch die Vielzahl an Aufgabenfeldern und den umfangreichen Horizont der Mitwirkung im Cyber-Bereich sowie durch die sehr viel anders konfigurierten und umfassenderen Vorgänge - als vom einfachen Verwaltungshandeln gewohnt - am Anfang etwas überrascht.

Der intensive Informationsaustausch während der gesamten Überprüfung, der sich kontinuierlich weiterentwickelte, konnte aber ein sehr kompaktes und rundes Bild erzeugen und den Fokus für die richtigen Empfehlungen ziemlich gut schärfen. Gleichzeitig konnte auch der ursprünglichen Intention des Überprüfungsteams, die bisher kaum bekannten Aufgaben des BMLV in diesem Bereich viel genauer kennenzulernen und analysieren zu können, weitgehend Genüge getan werden. Der Abschluss der Überprüfung mit der Fertigstellung des Berichts wird 2023 bereits zeitnahe erwartet.

Forschung und Entwicklung

Forschungsumfeld

Auf Grund der stets steigenden Bedeutung von Technologie können Fähigkeiten in hohem Ausmaß nicht im eigenen Leistungsbereich gestemmt werden, sondern stützen sich im großen Ausmaß auf gemeinsame Forschungsprojekte und Kooperationen ab. Forschung ist der Impulsgeber für die Innovationsfähigkeit einer Organisation und schafft mittelbar auch einen hohen Reifegrad zur Herstellung der Grundlagen für die Fähigkeitsentwicklung der Streitkräfte.

Laufende Projekte

FORTE-Projekte

Single Device for Multi Security Domains (SD4MSD)

SD4MSD

SINGLE DEVICE FOR MULTIPLE SECURITY DOMAINS

Für das Arbeiten in unterschiedlichen Sicherheitsdomänen im Gefechtsstand oder in (verlegbaren) Rechenzentren werden derzeit zumeist unterschiedliche Geräte für unterschiedliche Sicherheitsdomänen verwendet. Wesentlich zielführender, „gerätesparender“ und sicherer wäre der Einsatz von Datenendgeräten, die auch hardwareseitig so konzipiert sind, dass sie in unterschiedlichen Domänen eingesetzt werden können und somit eine echte Multidomänenfähigkeit mitbringen. Die bisherigen Ergebnisse des Forschungprojekts wurden bereits auf der IKT-Sicherheitskonferenz 2022 präsentiert und sind auch Grundlage des bereits nachfolgenden Projekts

FiBack - Finding Backdoors

Im BMLV werden „Closed Source“ Sicherheitssysteme, auch von Herstellern aus dem außereuropäischen Ausland eingesetzt. Es gibt immer wieder Hinweise, dass z.B. seitens diverser Akteure sogenannte „Backdoors“ in Systemsoftware, Firm - oder Hardware eingebaut werden. Für das Verteidigungs-Ressort ist es daher notwendig, geeignete Methoden und/oder Partner zum Aufspüren derartiger „Backdoors“ zu finden. In diesem Projekt wird dieser Prozess (teil-) automatisiert und damit die Möglichkeit geschaffen, mehr Komponenten zu prüfen. Hierbei werden Techniken und Methoden entwickelt und neue hybride Ansätze, welche die automatisierten Analysen mit Expertenwissen augmentieren um somit mehr und tiefer gehende und versteckte Sicherheitslücken zu finden, erarbeitet.

CONTAIN - Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten

Cyberbedrohungen haben das Potential, Unternehmen und ganze Lieferketten nachhaltig zu stören und die Wiederherstellung ist nicht einfach. Das Projekt CONTAIN zielt daher darauf ab, Bewusstsein für Themen des Incident Response und der nachfolgenden Prozesse zu steigern und Tools des Software Engineerings, sowie entsprechende Referenzprozesse zu definieren. Das zu entwickelnde Simulationsmodell dient der Identifizierung kritischer Prozesse, sowie etwaiger Ressourcen- und Kapazitätsengpässe, woraus relevante Möglichkeiten zur Optimierung von Prozessen abgeleitet werden.

SIDES - Signal Detection System

Ziel des Projektes ist die Erstellung einer Vorstudie zur Implementierung eines C4ISR-Spektrums-Klassifizierungsystem basierend auf Machine Learning Algorithmen. Dieses "Signal Detection System" (SiDeS) soll an einem bestimmten örtlichen Punkt das Funkspektrum empfangene Funksignale in einem großen Frequenzbereich detektieren, klassifizieren und identifizieren können, um so die kontextbezogene Analyse und Entscheidungsfindung des taktischen Kommandanten zu erleichtern.

Cat.B ANQuOR - Advanced Networking with Quantum Communications with Operational Relevance

Die derzeit reifste Anwendung der Quantenkommunikation ist Quantum Key Distribution (QKD), also die informationstheoretisch sichere Erzeugung und Verteilung kryptographischer Schlüssel mit quantenphysikalischen Methoden. Zweck des Projekts ist die Absicherung einer militärischen Kommunikationsverbindung zwischen einem Anschlusspunkt in einem ortsfesten militärischen Netzwerk und einem verlegten Gefechtsstand im Feld durch Quantum Key Distribution (QKD).

KIRAS-Projekte

SHIFT - Sichere Simulationstechnologien für cyber-physische Systeme (CPS)

Das Projekt zielt darauf ab, gezielte Trainingsumgebungen im Bereich CPS aufzubauen, kann einer Vielzahl an potentiellen Anwendern die Nutzung im Bereich ICS und Global Navigation Satellite System (GNSS) ermöglichen. Dies kann langfristig zu gezieltem Aufbau von Personal als auch zur Technologieentwicklung in Österreich beitragen. SHIFT leistet auch einen Beitrag zum Aufbau einer BMLV-spezifischen Cyber-Range.

CATCH-IN - Technologien und Konzepte zur Ortung und Verfolgung von Interferenzquellen

Die Abhängigkeit der sicherheitskritischen Infrastruktur oder zukünftiger Schlüsseltechnologien von globalen Satellitennavigationssystemen (GNSS) als Informationsquelle für Zeit und Ort wird in Zukunft weiter zunehmen. Die Folgen von Störungen im GNSS-Empfang können erheblichen wirtschaftlichen Schaden anrichten. Im Kontext eines bundesweiten Monitoringsystems für Frequenzstörungen zielt das Vorhaben auf Innovationen zum Schutz sicherheitskritischer Anwendungen ab. Dies erfolgt anhand der Fallbeispiele der GNSS Nutzung in der Luftfahrt sowie kooperative Systeme im Straßenverkehr. Gesamtziel ist eine deutliche Verbesserung des Wissensstandes über Auftreten von Interferenz, Jamming, Spoofing und, sowie gleichzeitig die Konzeptionierung und Darstellung von kostengünstigen Gegenmaßnahmen.

Abgeschlossene Projekte

Forschungsbereich FTB1 Cyber Sicherheit, - Verteidigung, Abwehr von Cyber-Bedrohungen

EMS Eye Bots - Scannen und Analyse im elektromagnetischen Spektrum

Gemeinsam mit dem UZEloKa des MilCyZ der Direktion IKT&Cyber wurden die Anforderungen an solche Sensoren erforscht und in weiterer Folge drei Demonstratoren für den mobilen Einsatz entwickelt und in Feldversuchen getestet. Untersucht wurden modernste SDR-Plattformen (Software Defined Radio), Spektrum-Analysatoren sowie zugehörige Antennen. Ergänzt wird der Sensor durch moderne Einplatinenrechner, Akkutechnologien sowie Verortungssensoren. Für die Feldmessungen wurden die ausgewählten Komponenten zu Sensoren inklusive Rechner, Stromversorgung und Gehäuse verarbeitet. Zur Analyse der Messdaten wurden zwei Softwarepakete zur Visualisierung umgesetzt und die Messergebnisse beschrieben.

Information Labelling - Automatisiertes Information-Labelling in heterogenen Führungsinformationssystemen mittels AI/KI

Entwicklung der fachlichen Anforderungen und der Konzeptionierung einer tragfähigen Systemarchitektur für automatisiertes Information-Labelling in heterogenen Führungsinformationssystemen für unterschiedliche Datentypen. Damit sollen Grundlagen für eine spätere prototypische Implementierung eines skalierbaren High Performance Sicherheitsgateways als Ansatz für das effiziente Zusammenwirken von Crypto-Binding Methoden und Methoden zur Online-Klassifikation zum Aufbau sicherer nationaler und europäischer Federated Mission Networks geschaffen werden. Ein neues Forschungsprojekt ist bereits in Planung mit Start ab 2023.

Militärisches Cyberlagebild User Interface (CIRP II)

Das Forschungsprojekt liefert sowohl grundlegende Anforderungen der Stakeholder als auch Grundlagen für die optimierte Gestaltung und Erstellung des User Interfaces zur quasi Echtzeitverarbeitung bzw. –darstellung des Cyberlagebilds, welches die Basis für ein möglichst in Echtzeit darstellbares Hybrides Lagebild bildet.
Ermittlung der Informationsanforderungen verschiedener Stakeholder zur Gewinnung einer effizienten, rollendifferenzierten Übersicht des Cyberlagebilds, Informationsaufbereitung und Visualisierung in den militärischen Cyberlagebild Dashboards. Entwicklung geeigneter Funktionalitäten zur Anordnung und Darstellung speziell im militärischen Cyber Sicherheits-Umfeld sowie prototypische Umsetzung.

FORTE-Projekte

CADSP - Cyber Attack Decision Platform

Das primäre Ziel des Projekts CADSP ist die wissenschaftliche Untersuchung, technische Konzeption und Validierung einer Cyber Attack Decision and Support Platform zur Detektion und Abwehr von Angriffen aus dem Cyberraum. Aufbauend u.a. auf dem Concept of Operations (CONOPS) BMLV-spezifischer Anwendungsfälle im Cyber Incident Reponse Bereich, soll im gegenständlichen Projekt die Grundlage für die Realisierung einer international führenden Cyber Attack Decision and Support Platform (CADSP) gelegt werden.

PIONEER (Interoperabilität und Digitalisierung von Aufklärungsprozessen)

Das Ziel Erstellung einer Systemarchitektur sowie von initialen Proofs-of-Concept (PoC) auf dem aktuellen Stand der Technik inkl. Methoden aus den Bereichen Softwaresysteme sowie Künstliche Intelligenz (Konsortium mit industrieller Leitung, BMLV in der Rolle des Bedarfsträgers).

KIRAS-Projekte

GIREKO - GNSS Interferenz Karte Österreich

Das Ergebnis einer Interferenz Landkarte für Österreich ist für das BMLV/ÖBH von hohem Interesse. Einerseits hat das BMLV den Auftrag zum Schutz kritischer Infrastruktur, andererseits ist das ÖBH selbst ein „kritischer GNSS Nutzer“ und noch stärker von Jamming und Spoofing betroffen. Durch die Testmessungen werden Erfahrungen gesammelt, welche Interferenzsignale in welcher Häufigkeit auftreten, und welche Charakteristika sie haben. Die Ergebnisse fliessen in die aktuelle Fähigkeitsentwicklung zu Navigation Warfare ein.

Sonstige Forschungsprojekte

Open QKD – „Quantum Key Distribution“

Quelle: openqkd.com

Unter der Konsortialführung des Austrian Institute of Technology (AIT) wurde QKD-Infrastruktur in Räumlichkeiten des BMLV/ÖBH und des Bundesrechenzentrums GmbH (BRZ) aufgebaut. Im Zuge des Projektes wurden entsprechende Glasfaserverbindungen zwischen den beteiligten Standorten errichtet, die Quantenrouter sowie Hardware Encryptoren in den Testräumlichkeiten installiert und konfiguriert. Die Einsatztauglichkeit der eingesetzten QKD-Infrastruktur konnte bestätigt werden.

QKD4Gov – „Einsatz von QKD zwischen Behördenstandorten in Wien“

Im Rahmen des österreichischen Förderprogramms für Sicherheitsforschung (KIRAS) wurde das Forschungsprojekt QKD4Gov – Einsatz von QKD zwischen Behördenstandorten in Wien – in enger Kooperation mit dem Bundeskanzleramt (BKA) und dem AIT umgesetzt. Es kam neben der QKD-Infrastruktur auch die Secret-Sharing-Technologie zum Einsatz, um neben dem Austausch (Data on Transit) auch die sichere Speicherung (Data at Rest) von sensiblen Daten zu Testen. Die Bereitstellung der Quantenrouter sowie der Secret-Sharing-Lösung erfolgte ohne Probleme. Der ausgewählte Use-Case konnte erfolgreich umgesetzt werden.

Permanent Structured Corporation

GMSCE - Geo-Meteorological and Oceanographic Support Coordination Element:

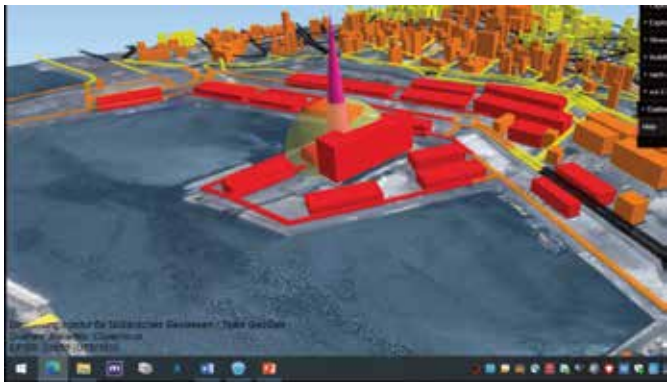
Projekt mit der Lead Nation DEUTSCHLAND, das zum Ziel hat, die Unterstützung von Missionen und Operationen durch GeoMETOC (Geospatial, Meteorological & Oceanographic) mittels einer Architektur zu verbessern, die die europäischen GeoMETOC-Fähigkeiten durch die Koordination und Verbesserung der Datenerfassung, einschließlich der Installation eines Geo-Data Infrastructure EU (GDI-EU), miteinander verbindet und erheblich steigert. Das hat große Vorteile für die Anteilnahme im Lagebild-Wirkungsverbund zur Auftragserfüllung im In- und Ausland.

DM_DRCP - Deployable Military Disaster Relief Capability Package:

Ziel ist es, eine auf Missionen zugeschnittene Task Force zu bilden, um Notfällen und außergewöhnlichen Ereignissen innerhalb und außerhalb des EU-Gebiets zu begegnen, Österreich hat dazu Teilnehmerstatus.

COHGI - Common Hub for Governmental Imagery:

Ziel und Zweck ist die Einrichtung einer gemeinsamen Drehscheibe zur Erleichterung des Austauschs von klassifizierten staatlichen Kartografien auf europäischer Ebene zwischen den Mitgliedstaaten sowie mit EU-Einrichtungen und fördert die Basis für GeoInfo-Produkte, Österreich hat dazu Teilnehmerstatus.



DoSA - Defence of Space Assets (DoSA):

Ziel dieses Projekts ist es, die operative Effizienz der EU im Weltraumbereich zu steigern, indem aktuelle und zukünftige Weltraumressourcen optimal genutzt werden. Österreich hat dazu Teilnehmerstatus.

AMIDA UT - Automated Modelling, Identification and Damage Assessment of Urban Terrain:

Das Hauptziel dieses Projekts ist es, ein automatisiertes System/Gerät/Tool für eine verbesserte und schnellere Kartierung und Identifizierung von Zielstrukturen zu schaffen.

EURAS - EU Radionavigation Solution :

Das Ziel ist die Entwicklung der EU-Militär-PNT-NAVWAR-Doktrin einschließlich der Galileo-Fähigkeiten, insbesondere des Public Regulated Service (PRS).

CBRN SaaS RSS - Chemical, Biological, Radiological or Nuclear Surveillance as a Service:

Das CBRN-Aufklärungs- und Überwachungssystem stärkt die Aufklärungs-, Überwachungs- und Fähigkeiten zum Incident Management gegen CBRN-Kampfmittel durch den Einsatz neuartiger unbemannter Sensoren und Systemverbesserungen. Das IKT&CySihZ ist dazu mit den IKT&Cyber-Spezialisten in der Expertengruppe vertreten.

Das Vorhaben wird vor allem in der 2. Phase mit der Überführung in eine gesamtheitliche Operationsführung aus dem Blickwinkel der Digitalisierung für die Direktion IKT&Cyber im Hinblick auf die Digitalisierung der Streitkräfte einen besonders hohen Stellenwert erhalten, weil es sozusagen als Vorzeigeprojekt gelten kann.

CDICC - Cyber and Information Domain Coordination Centre:

Ziel des Projekts „Cyber and Information Domain Coordination Centre“ ist die Entwicklung, Einrichtung und der Betrieb eines multinationalen Koordinierungszentrums für die Cyber und Informationsdomäne (CID) als ständiges multinationales militärisches Element. Im Ökosystem Cyber entwickelt sich das Projekt zusehends zu einer Drehscheibe, gegenüber den militärischen CERTs und der Military Planning and Conduct Capability (MPCC) bzw. den OHQs.

CRF - Cyber Ranges Federations:

Das Hauptziel besteht darin, die Leistungsfähigkeit der europäischen Cyber-Ranges zu verbessern, indem bestehende nationale Cyber-Ranges zu einem größeren Cluster mit mehr Kapazität und einzigartigen Diensten zusammengeschlossen werden. Dies ermöglicht es entsprechend die Fähigkeiten zu teilen und zu bündeln und die Qualität von Cyber-Trainings und -Übungen zu verbessern sowie die Föderation für Cyber-bezogene Forschungs- und Entwicklungszwecke zu nutzen. Österreich hat dazu ebenfalls Beobachterstatus.

Das Ziel „Errichten der nationalen militärischen Cyber Range“ ist in der Fähigkeitsentwicklung sehr weit oben angesiedelt und wird mit dem kommenden Personalaufwuchs hoffentlich endlich ausreichend forciert werden können.

Entwicklungstendenzen und Zielrichtungen 2023

Für die gesamte konzeptionelle Arbeit und inhaltliche Neuorientierung in der Direktion IKT&Cyber wird die bereits 2021 begonnene bereits sehr fundierte Grundlagenarbeit vertieft, der Umfang der Forschung und Entwicklung zeigt den Stellenwert im Ressort. Für 2023 und die Folgejahre sind bereits zahlreiche weitere prominente Forschungsvorhaben in der Pipeline.

FÜHRUNGSABTEILUNG

Bundesministerium für Landesverteidigung

ObstdG Mag. Christof TATSCHL

Führungsabteilung

Das Jahr 2022 war für die Führungsabteilung, neben ihren sowieso immer laufenden Koordinierungs- und Unterstützungsaufgaben für die Direktion IKT&Cyber und dem IKT&CySihZ, durch die weitere Unsicherheit einer fehlenden Organisationsstruktur, den sich verstärkenden drückenden Personalmangel, und der Notwendigkeit der zeitlich begrenzten Übernahme der direktionsweiten Koordinierung der Fähigkeitsplanungen für alle der Direktion IKT&Cyber zugewiesenen Waffengattungen auf den Weg zum ÖBH 2032+, eine große Herausforderung. Da es seit vielen Jahren für die Führungsabteilung keinen den Aufgaben angepassten Org-Plan gibt, weiterhin der Zeitpunkt des Abschlusses der Einnahme der Direktionen ungewiss ist, es keine für diese Aufgabe angepasste Stabsstrukturen gibt und dem zu Folge auch keine dazugehörigen eingeübten Prozesse abgerufen werden können, musste ein rasch wirksamer Ansatz gefunden werden, um dem Aufgabendruck vernünftig Herr werden zu können.

„Agile Führung erfordert es, die Wertschätzung zwischen allen Mitgliedern der Abteilung zu fördern und Toleranz und Fairness zu leben.“

In einer sich ständig änderten Organisation, deren begonnener Änderungsprozess seit vielen Jahren das Ergebnis der Änderung nie erlebt und auch niemals in die Konsolidierungsphase gelangt, kann ein streng hierarchischer Ansatz, wie im Militär unter Standardbedingungen üblich und durchaus erfolgreich angewandt, nicht mehr ausreichend funktionieren.
Zu den bereits genannten Rahmenbedingungen wirken auch Veränderungen aus der Gesellschaft und der hohe Digitalisierungsdruck auf die Kultur- und Prozessentwicklung unserer Organisation. Besonders neue und junge Mitarbeiter erwarten sich heute von ihrem Arbeitgeber und Arbeitsplatz andere Rahmenbedingungen, als noch vor 20 Jahren. Die Organisation ist einem ständigen Wandeln unterworfen, sieht sich aber den unflexiblen, starren Bereichen der staatlichen Verwaltung und ihren Vorschriften gegenübergestellt.

Der Zugang des ÖBHs zu seinen Mitarbeitern ist aus dieser Sicht nicht mitarbeiterzentriert, sondern verwaltungszentriert. Zudem wurden die neuen Direktionen so strukturiert, dass sie auf die wichtigsten Ressourcen und Stellschrauben einer Organisation, Mitarbeiter und Budget, keinen direkten Einfluss haben. In diesem Spannungsverhältnis ist es nicht immer leicht, alle Mitarbeiter gut mitzunehmen, die Prozesse richtig und rasch genug anzupassen und die Chancen der Digitalisierung ausreichend nutzen zu können.

Als Chef des Stabes der Direktion IKT&Cyber und Leiter der Führungsabteilung (betraut, bzw. Überleitungsverantwortlicher) musste ich, um die Chance auf Erfolg zu haben, das Wagnis eingehen, die grundlegende und vertraute Führungsphilosophie des in militärischen Organisationen stark verbreiteten Taylorismus in Richtung einer agilen Organisation verändern.

Der wichtigste und vielleicht riskanteste Schritt war es die Verantwortlichkeiten in der Führungsabteilung, soweit wie möglich, in der Hierarchie nach unten zu drücken. Die Selbstverantwortung der Referatsleiter, als auch den ihnen zugeteilten Mitarbeitern sollte so gut wie möglich gestärkt werden. Das bedeutet einerseits der endgültige Abschied von Micro-Management und andererseits mehr Verantwortungsdruck für die nächste Ebene. Ich bin überzeugt, dass in einer Abteilung mit dieser großen Fülle an verschiedenen Aufgaben, deren Aufgabenerfüllung Auswirkungen auf alle Ebenen des ÖBHs haben können und die für die Führung und Unterstützung eines äußerst vielschichtigen Betriebes wie der Direktion IKT&Cyber verantwortlich ist, am Ende des Tages keine andere Wahl bleibt.

Mit dieser Maßnahme steigt der Bedarf einer klaren Zielausrichtung und Kommunikation der Ziele auf allen Ebenen und es bedarf einer klaren Kunden- und Ergebnisorientierung. Wir haben daher verstärkt die Bedarfe der uns angewiesenen Bereiche analysiert und versucht auf diese, soweit es unsere Ressourcen möglich machen, einzugehen. Für den Vorgesetzten bedeutet dies, dass er weniger in der Prozesskontrolle wirksam sein kann.

Dieser Ansatz würde bei einer so großen Abteilung gar nicht mehr möglich sein. Vielmehr müssen sich die Vorgesetzten aller Ebenen in der Abteilung, einschließlich des Abteilungsleiters selbst, fast ausschließlich der Ergebniskontrolle widmen. Der Vorgesetzte übernimmt immer mehr die Beraterrolle für seine unterstellten Führungskräfte, während er vor allem die Ziele formuliert und Leitlinien vorgibt. Die Ergebnisorientierung bedingt, dass man Erfolgsfaktoren definieren muss, die gemessen werden können und klar kommuniziert werden. Das ist ein Prozess, der noch zu schärfen sein wird.

Ein weiterer wichtiger und für die generellen Organisationsgewohnheiten ungewöhnlicher Schritt ist die Anwendung von und die Verpflichtung zum Transparenzprinzip. Aus meiner Sicht lässt der Durchdringungsgrad dieses Prinzips direkte Rückschlüsse auf die Reife einer Organisation zu. Unter Anpassung einer im IKTCySihZ genutzten Software für den IT-Service Ticketverwaltung wurde ein KANBAN-Board eingerichtet mit dem alle in der Abteilung laufenden Aufgaben, die ein Zusammenwirken bedürfen, oder besonders ressourcenfordernd sind, für alle Mitarbeiter der Abteilung sichtbar gemacht.

Dieser Prozess befindet sich erst in der Erprobungsphase, soll aber nach erfolgreicher Implementierung in der Abteilung auch auf die „Stakeholder“ der Führungsabteilung ausgerollt werden. Als Stakeholder sind hier z.B.: die Führung der Direktion, aber auch die der Direktion IKT&Cyber unterstellten Bereiche gemeint, die durch diese Einsicht sehen und verstehen können, wie ihre Anliegen behandelt und priorisiert werden, welche Schwierigkeiten es unter Umständen gibt und wie weit Aufgaben schon erledigt wurden.

Obwohl durch die rasch aufeinanderfolgenden Umgliederungszyklen, die es seit vielen Jahren der Organisation nicht erlauben zur Ruhe zu kommen, von der Führung des Bundesheeres bereits hohe Flexibilität und Veränderungsbereitschaft abverlangt wird, habe ich mich nach eingehender Beurteilung nicht gescheut, durch die notwendigen internen Anpassungen, den Führungskräften der Abteilung noch mehr Flexibilität und Anpassungsbereitschaft abzuverlangen, indem wir neue Wege in der Führung und des Zusammenarbeitens zu gehen versuchen.

Damit das funktionieren kann, ist es wichtig die Wertschätzung zwischen allen Mitgliedern der Abteilung zu fördern und Toleranz und Fairness zu leben. Das ist vielleicht eines der schwierigsten umzusetzenden Prinzipien, kann aber durch die Anwendung von offener, angepasster und ehrlicher Kommunikation befördert und umgesetzt werden.

Mit den neuen strategischen Vorgaben für die Landesverteidigung, den neuen Budgetzahlen, der Ausrichtung der Planungen auf ÖBH 2032+ und der verfügten Realisierungsziele ist für die Direktion IKT&Cyber im Bereich der Planung ein besonderer Lastfall eingetreten. Es war zu entscheiden, ob mit den alten Strukturen und Prozessen das Auslangen gefunden werden kann, oder ob unter Ausnutzung der Möglichkeiten der Implementierung der Prinzipien einer agilen Organisation eine höhere Leistungserbringung zu erwarten sein würde. Angesichts der Bedeutung der gestellten Planungsaufgabe, verbunden mit der einzigartigen Chance das ÖBH in die Digitalisierung zu bringen, ist das höhere Risiko

durch temporäre Struktur- und Prozessänderung zu akzeptieren. Nach eingehender Beurteilung der eigenen Planungsressourcen wurde zudem klar, dass aufgrund des geringen Personalrahmens der IKTCyPl und der bereits jetzt bestehenden hohen Auslastung nur durch klare Schwergewichtsbildung und enge Erfolgskontrolle, die gestellten Aufgaben erfolgversprechend umgesetzt werden können.

Mit den nun stark geänderten finanziellen Rahmenbedingungen für die Folgejahre bedarf es einer umfassenden Neubeurteilung der Umsetzung jedes einzelnen Realisierungszieles. Die nun vorliegenden Budgetzahlen ermöglichen es somit, auch teilweise stillgelegte Projekte, die aufgrund fehlender Ressourcen hintangehalten wurden, aber für das Führungssystem ÖBH im Einsatz unerlässlich sind, neu zu bewerten, zu priorisieren und vollinhaltlicher sowie zukunftsträchtiger aufzustellen.

Daher habe ich als Chef des Stabes der Direktion IKT&Cyber, in Umsetzung der Vision und der Leitlinien, des Direktors der Direktion IKT&Cyber, nach eingehender Beurteilung, gemeinsam mit den zuständigen Führungskräften in der Abteilung, dem Direktor vorgeschlagen, die Prinzipien einer agilen Organisation auf die Fähigkeitenentwicklung in unseren Bereich anzuwenden. Nach der entsprechenden Anleitung und Genehmigung durch den Direktor wurde das Cyber Information Fähigkeiten Board (CIFB) ins Leben gerufen, das in einem agilen Ansatz alle Kräfte der Direktion zur Erfüllung der gestellten Planungsaufgaben zur Umsetzung der Vision ÖBH 2032+ erarbeiten soll.

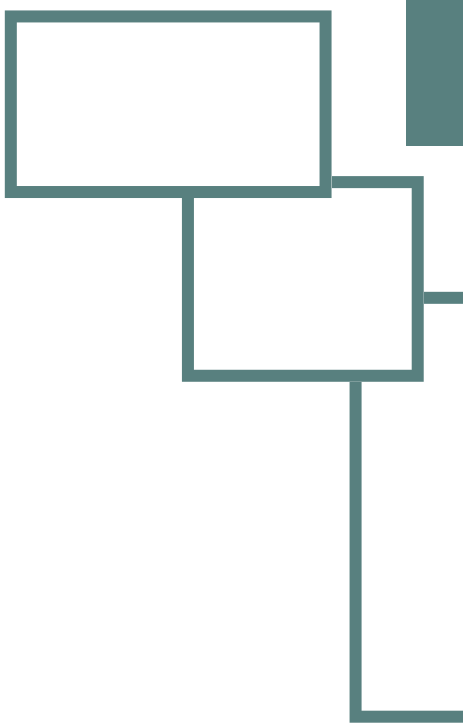
Es muss hier nochmals betont werden, dass eine solche Umstellung, während einer nicht abgeschlossenen Umgliederung von allen Mitarbeitern höchste Anstrengungen und Flexibilität erfordert.

Die Leiter, Fachoffiziere und alle betroffenen Mitarbeiter müssen auf diesem Weg mitgenommen werden. Führungskräfte müssen ihre Rolle anpassen und vor allem für die nächste Ebene unterstützend wirken und ihre Fachkompetenz voll einbringen. Vorgesetzte müssen die Kultur der Veränderung vorleben und die Vision und die Ziele des gesamten Unternehmens tragen.

In Vorbereitung auf diese Herausforderung hat die Führungsabteilung bereits zwei Mal ein sehr erfolgreiches Teamtraining mit klarem Fokus auf die Personalentwicklung, Organisationsentwicklung und Zusammenarbeit unter der äußerst professionellen Betreuung von ADir Oliver Jeschonek (Zentrum für Menschenorientierte Führung und Wehrpolitik, Referat „Coaching, Mediation & Teamentwicklung“) und seinen Co-Trainern abgehalten.

Die Reise hat natürlich erst begonnen. Der Aufbau und die Bearbeitung des äußerst komplexen Projekts CIFB, das Eintauchen in eine agile Organisationsentwicklung wird dem Planungsteam Direktion IKT&Cyber und dem dazugehörige Team Führungsabteilung die Chance geben sich positiv weiter zu entwickeln. Der Beginn des CIFB hat die Orientierungsphase überwunden und bereits positive Ergebnisse gezeigt und es wird spannend werden, was ich dem geneigten Leser im Leistungsbericht 2023 über den Ablauf des Projektes berichten werden kann.

Ich sehe der Aufgabe und der Entwicklung positiv entgegen, da die gezeigte Leistung der beteiligten Mitarbeiter, ihr Interesse und Neugier auf Neues verbunden mit höchster Flexibilität mir Mut gemacht und Zuversicht gegeben haben. Die Mitarbeiter und ihr Engagement sind die Stärke der Führungsabteilung und versprechen einen erfolgreichen Kurs. Dafür möchte ich und muss ich jedem einzelnen Mitarbeiter und Mitarbeiterin meinen besonderen Dank aussprechen.



Moderne militärische Führung

Moderne militärische Führung stellt hohe Anforderungen an die Führungskräfte, die sich mit immer komplexeren und dynamischen Herausforderungen auseinandersetzen müssen. Diese Herausforderungen umfassen sowohl konventionelle als auch nicht-konventionelle Bedrohungen, die sich auf den Informationsraum, Cyberspace und den Weltraum erstrecken. Um erfolgreich zu sein, müssen militärische Führungskräfte in der Lage sein, schnell auf sich ändernde Umstände zu reagieren und Entscheidungen zu treffen, die auf einer umfassenden Analyse von Daten und Informationen basieren.

Auf dem modernen Gefechtsfeld finden sich eine Vielzahl von Akteuren; Staatliche Akteure wie Militärische Einheiten aus multinationalen Kontingenten oder Polizei und Ordnungskräfte, Nichtstaatliche Hilfsorganisationen wie das Rote Kreuz, Supranationale Hilfs- Organisationen wie UNHCR, aber auch zivile Firmen, die als Vertragspartner oder aus eigenen Interessen am Gefechtsfeld teilnehmen.

Moderne Informationssysteme ermöglichen einen schnellen Datenaustausch. Ziel ist es, durch geeignete Informationssysteme den Entscheidungsfindungsprozess zu unterstützen und durch bedarfsgerechte Informationsaufbereitung soweit es geht zu verkürzen. Hierbei ist insbesondere der Zugriff auf Informationen aus vielen relevanten Quellen zu achten. Von daher ist besonderes Augenmerk zu richten auf die Interoperabilität. Dies betrifft nicht nur technische Interoperabilität, sondern auch die geistige Interoperabilität mit den eigenen Systemen und Prozessen sowie die der jeweiligen Mission Partners. Das verlangt ein hohes Maß an technischer Expertise und geistiger Flexibilität von den militärischen Kommandanten auf allen Führungsebenen.

Des Weiteren sind moderne Waffensysteme immer komplexer zu bedienen. Dies liegt unter anderem auch an einem hohen Maß an Automatisation, welche zur Verkürzung von Befehlszyklen genutzt wird. Die Einhaltung von verschiedenartigen rechtlichen Bestimmungen aus lokalen bis internationalen Rechtsquellen sowie unterschiedlichen Sicherheitsbestimmungen, Normen und Vorgaben bedingt auch ein komplexes Management von Berechtigungen und Zugriffskontrollen.

Kommandanten aller Ebenen müssen diese Berechtigungen durch geeignete Systeme herstellen und verwalten. Das verlangt ein hohes Maß an vernetztem und kritischem Denken. Ein weiterer wichtiger Aspekt moderner militärischer Führung ist die Fähigkeit, den Nutzen von Technologie und Innovationen zu erkennen und sie entsprechend zu nutzen. Dazu gehört eine umfassende Kenntnis der Informations- und Cyber-Kriegsführung, die Fähigkeit, Datenanalyse und künstliche Intelligenz zu nutzen, sowie die Fähigkeit, komplexe Probleme zu lösen und Entscheidungen unter unsicheren und sich schnell ändernden Umständen zu treffen.

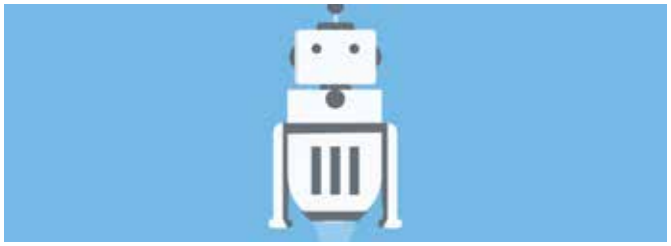
Um auf diese Anforderungen vorbereitet zu sein, ist es wichtig, dass militärische Organisationen und Schulungseinrichtungen sicherstellen, dass ihre Führungskräfte die notwendigen Fähigkeiten erwerben und auf dem neuesten Stand halten. Regelmäßige Schulungen und Weiterbildungen, die sich auf die neuesten Entwicklungen und Herausforderungen in der militärischen Führung konzentrieren, sind entscheidend, um sicherzustellen, dass die Führungskräfte in der Lage sind, schnell auf sich ändernde Umstände zu reagieren und erfolgreich in einer immer komplexeren und dynamischen Umgebung zu operieren.

Zusammenfassend lässt sich feststellen, dass militärisches Handeln in allen Räumen der Kriegsführung, Wasser, Luft, Land, Information und Cyber stets gleichzeitig stattfindet. Daher ist die moderne militärische Führung eine komplexe und dynamische Disziplin, die hohe Anforderungen an die Führungskräfte stellt und ein hohes Maß an technischem und systemischem Verständnis von Kommandanten aller Ebenen verlangt. Die Fähigkeit, schnell auf sich ändernde Umstände zu reagieren und komplexe Entscheidungen zu treffen, ist entscheidend für den Erfolg auf dem modernen Gefechtsfeld.

Referat Personalverwaltung

Nach der herausfordernden Einnahme der derzeitig geplanten Organisationsstruktur im Jahr 2022, lag das Schwergewicht wieder auf den Tätigkeiten als Standeskörper vorrangig für das IKT&CySihZ. Gleichzeitig mussten auch die der Direktion IKT&Cyber nachgeordneten sowie neu hinzugekommene, ministerielle Organisationselemente serviciert werden. Fehlende Vorgaben, nach der Einnahme der virtuellen Organisation und eine Änderung der Dienstbehördenzuständigkeiten, Mitte des Jahres, kamen erschwerend hinzu.

Durch Dienstzuteilungen und Militärperson auf Zeit (MZ) Aufnahme konnte das Referat Personalverwaltung personell aufwachsen und die Aufgaben effizienter bewältigen. Nur so war der Spagat zwischen der „Beratertätigkeit", der Personalplanung einerseits sowie die Personalbetreuung andererseits zu schaffen. Erste Erfolge durch gestraffte Prozessabläufe konnten bereits erzielt werden.



Das Hauptaugenmerk lag im Jahr 2022 einmal mehr auf der Personalgewinnung, die sich im Licht des österreichweiten IT-Fachkräftemangel, zunehmend als schwierig gestaltet. Eine wesentliche Erleichterung konnte in Zusammenarbeit mit den Bereichen Sicherheit und BetrOrg im Herbst 2022 erreicht werden. AÜG-Mitarbeitern (Mitarbeiter nach dem Arbeitsüberlassungsgesetz) konnten rascher aufgenommen werden. In der Zeit von Oktober bis Dezember 2022 wurden mehr als 10 AÜG-Mitarbeiter aufgenommen. Insgesamt konnte der Besetzungsgrad des IKT & Cybersicherheitszentrum auf 84 % angehoben werden.

Durch die Zuweisung von Personalwerbebudget wurden die Werbemaßnahmen an Schulen, Berufsmessen etc. ermöglicht. Daraus resultieren positive Rückmeldungen und die Anzahl der Initiativbewerbungen nicht nur für den Cybergrundwehrdienst sondern auch für die Bereiche Technik, Applikationen, IMG, Betrieb und das Militärische Cybersicherheitszentrum steigen an. Mit RIVIT – Richtverwendung in der IT-soll die Attraktivität des Bundes als Arbeitgeber gesteigert werden. Es wurde ein erster Schritt gesetzt das IT-Entgelt an die privatwirtschaftlichen Gehälter anzupassen. Gerade die letzten Jahre haben gezeigt, dass bei den Generationen X,Y,Z nicht mehr nur der finanzielle Aspekt bei der Jobsuche im Vordergrund steht.

Viel mehr sind, neben einem spannenden Aufgabengebiet, die Bereiche Familie, Work-Life-Balance, vergünstigtes Essen, die Möglichkeit des Homeoffice etc. ein wichtiger Faktor für die Bewerber und damit können wir in der Direktion IKT&Cyber durchaus punkten.

Militärische Sicherheit

Schulung der Sicherheitsbeauftragten der Direktion IKT&Cyber durch die IDC (IDCheck)-Academy der Österreichischen Staatsdruckerei

Im Zuge einer eintägigen Fortbildung der Sicherheitsbeauftragten erfolgte ein Schulungsprogramm für sichere Ausweiskontrollen. Im Rahmen der Schulung „ID-Check 2022" vermitteln die OeSD-Sicherheitsexperten detailliertes Theorie- und Praxiswissen über die wichtigsten Merkmale unterschiedlicher Ausweise.

Ziel der Ausbildung war es, dass die Teilnehmer die gängigsten Sicherheitsmerkmale bei internationalen ID-Dokumenten erkennen und diese auf dessen richtige Ausführung in einem Schnell-Check überprüfen. Neben den gängisten international verwendeten Sicherheitsmerkmalen wurde auch auf das Erkennen von wichtigen Details der Offset- und der auch gut fühlbaren Stichtiefdrucktechnologie unter Zuhilfenahme des Fadenzählers eingegangen. Die Unterscheidung von Laser- und Tintenstrahldruck (Inkjetdruck) wurde ebenfalls im Fokus auf die Erkennung von damit gefälschten ID-Dokumenten gelehrt und musste anhand von Lernbehelfen im Rahmen der praktischen Abschlussprüfung von den Kursteilnehmern erkannt und korrekt zugeordnet werden.

Ein Herzstück des Schulungsprogramms war die Wissensvermittlung und praktische Übung der „10 goldenen Regeln beim Check von internationalen ID-Dokumenten“, in dem Fokus auf den gesamtheitlichen Schnellcheck-Prozess eines dem Sicherheitspersonal noch unbekannten ID-Dokuments gelegt wurde.

Durch die IDC-Abgleichmethode in Verbindung mit dem nationalen bzw. internationalen IDC-Schnellcheck-Tool wurde über den Aufbau und den Ablauf der IDC-Aktionskette informiert. Sollte eine tiefergehende Analyse eines ID-Dokuments durchgeführt werden müssen, wurden weitergehende Vergleichsmittel (z.B. Datenbanken mit Informationen zu ID-Dokumenten) geschult und aber auch dessen Grenzen in der Abgleichmethode den Kursteilnehmern dargelegt. Jeder Teilnehmer entwickelte ein situationsbezogenes Bewusstsein für den richtigen und zielgerichteten Einsatz der IDC-Dokumentenkontrollmethode und der IDC-Abgleichmethode.

Weiters wurde Basiswissen bezüglich der in ID-Dokumenten (Reispässe, Personalausweise, ...) eingesetzten Hochsicherheits-Chips und deren speziell entwickelte Technologie sowie ein Überblick über die in diesem Sektor eingesetzte Kryptographie (u.a. QR-Codes und deren Einsatzgebiete, Ausblick in die Zukunft) vermittelt.

Nach einer Trainings Session sowie einer theoretischen und praktischen Wissensüberprüfung, in der die Ausbildungsinhalte praxisnah angewendet werden konnten, erfolgte die Zertifikatsverleihung durch die Staatsdruckerei.

Durch diese Ausbildung konnte eine Awareness der Sicherheitsbeauftragten bezüglich Achtsamkeit für das Erkennen von manipulierten oder gefälschten Ausweisdokumenten/ID-Dokumenten geschaffen bzw. geschärft und mit viel Detailwissen aus der Praxis angereichert werden.

Betriebsorganisation und Wirtschaftsversorgung

Die Administration der Einkaufsagenden in den verschiedensten Spektren im IT-Bereich oder für die verschiedensten Versorgungsgüter wurde in insgesamt ca. 900 Vorgängen über Einkaufsakte, Beschaffungsanträge, Einleitungen zur Beschaffung/Vertragsänderung, Kreditkarten- oder BBG-Beschaffungen oder Beschaffungen von Versorgungs- und Wirtschaftsgütern aus dem zentralen und dezentralen Budget durchgeführt.

Gleichzeitig werden durch die Budgetstruktur ca. 400 gültige Service-, Bereitstellungs- oder Abrufverträge für die Sicherstellung des IT-Betriebes administriert, verrechnet und laufend aktualisiert, an die 1000 Rechnungen, 80 Vertragsanpassungen, 1000 Abrechnungen für die Leiharbeiter sind nur einige Zahlen und Fakten dazu. Die Betriebsorganisation ist unter anderem das Administrationselement für die Leiharbeiter im Zuständigkeitsbereich und musste ca. 120 externe Mitarbeitervorgänge erledigen [aufnehmen, kündigen oder verrechnen]. Die BetrOrg&Wi führte im vergangenen Jahr ca. 2.000 MIS-Buchungen für die gesamte Dienststelle durch.

Die Betriebsorganisation deckt auch den Aufgabenbereich Datenschutz ab. Ein Teilbereich davon sind Datenschutzauskünfte. Dabei hat jeder österreichische Staatsbürger das Recht, Auskunft über seine Daten, die beim ÖBH gespeichert sind, zu erhalten. Hierbei wurden im Jahr 2022, ca. 15 Datenschutzanfragen erledigt. Dabei kam es zu keiner Überschreitung der gesetzlich vorgeschriebenen Frist von vier Wochen für die Beantwortung der Auskunft. Das Jahr 2022 war durch eine geringe Anzahl an Auskünften gekennzeichnet, der Durchschnitt der letzten zehn Jahre betrug 40 Auskünfte pro Jahr. Des Weiteren wird auch der Aufgabenbereich Qualitätsmanagement von der Betriebsorganisation abgedeckt.

Logistik

Im Zuge des Jahres 2022 wurden im Bereich der Logistik in der Optimierung der Logistikprozesse und der Zusammenarbeit mit den Bereichen deutlich merkbare Erfolge erzielt trotz nach wie vor spärlicher Besetzung an fachausgebildeten Logistikpersonal. Um nach inzwischen 8 Jahren an unzureichender logistischer Aufteilung der Verwaltung von Truppennummern und dem daraus resultierenden Mehr an Arbeit Herr zu werden wurden im vergangenen Jahr erfolgreich ein neuer derzeit in Ausbildung befindlicher Lagermeister, ein auszubildender Fahrzeug-Unteroffizier (FzUO) sowie 2 Militärperson auf Zeit - Charge (MZCh) als Nachschubsgehilfe (NGeh) rekrutiert.

Nach einem notwendigen Nachjustieren in der Personalplanung im Bereich der Abdeckung des IKTBetr konnte in Verbindung mit dem Mitarbeiter, dem ehem. Bereichsleiter und der Versorgungsführung ein Modell zur Übergabe der Materialverwaltungszuständigkeit im Zuge der in diesem Jahr folgenden Inventuren erschlossen werden.

Der ursprünglich geplante Mitarbeiter für diesen Bereich arbeitet jetzt Expertise gerecht im Bereich der Konfigurationslogistik und Fremdversorgung als Sachbearbeiter.

Weiters konnte im eigenen Bereich in stundenlanger selbst Aneignung von fehlender Expertise auf Grund von Kompetenzabgang der Konfigurationsablauf wieder auf Schiene gebracht werden ohne Jahre auf Kurse warten zu müssen.
Dasselbe trifft auf Tätigkeiten des Karteimittelführers (KMF), Sachbearbeiter S4 (SBS4) sowie die des Lagermeisters (LgrMst) zu.

Das logistische Tagesgeschäft hat sich im Bereich des IKT&CySihZ über die Jahre zu einem Konglomerat an Sonderfällen verwandelt, was höchst lösungsorientiertes Handeln, Flexibilität, enormen Mehraufwand und hochoptimiertes Zeitmanagement abverlangt. Der Bereich der Logistik hat es dennoch möglich gemacht unzählige Projekte, spontane Akutfälle an der Tagesordnung und „normale“ Termingeschäfte trotzdem meist zeitgerecht erledigt zu haben.

In Bezug auf Inventuren konnte 2022 neben den periodisch jährlichen Inventuren die TN 3775 MilCyZ und große Teilbereiche von IKTTe TN 3773 gem Jahresinventurplan erfolgreich abgeführt werden.

Infrastruktur

Der RefLtr Vers&S4 bzw Ltr Log&Infra&DBetr versah 2022 gem provisorischem OrgPlan Direktion IKT&Cyber die Agenden des POC Infra IKT&CySihZ als auch in neuer Organisation GDLV die Funktion des ONV/Infra/Direktion IKT&Cyber (oberster Nutzervertreter Infra) und somit begleitend zuständig für Baubedarfe aller nachgeordneten Verbände (Vbd) und Baumaßnahmen der Fernmeldesystemräume (FMSysR) als Hausherr gem Betreibenserlass.

2022 hielten sich die abgeschlossenen Baumaßnahmen, abgesehen von der Adaptierung der

Führungszentrale Direktion IKT&Cyber, in beschedenen Grenzen, war jedoch bestimmt von großen Bauplanungen. In WIEN erfolgten Planungen für den Umbau STIFT Kaserne Obj 5 sowie in der STARHEMBERG Kaserne war die Errichtung einer Cyber Range das dominante Thema, in VILLACH die Planung der Großkaserne neu mit Implementierung FüUB1, sowie St JOHANN das Durchsetzen der Errichtung und Adaptierung der Elektronikwerkstatt (EloWkSt) FüUB2 mit Baubeginn 2023.

Dienstbetrieb

2022 stand im Zeichen des Wechsels der Führung, wobei der langjährige Kdt Dienstbetrieb Mjr WIELAND Martin das Kommando an Frau Olt FEURHUBER Nadine übergab.

Olt Nadine FEURHUBER

Die routinemäßige Dienstleistung des Dienstbetriebes umfasste die Betreuung und Verwaltung der CyberGWD des IKT&CySihZ, die Bearbeitung der Belange Infra im Bereich Kleinbaumaßnahmen, sowie die Sachbearbeitung des KABA Schließsystems. Brandschutzprävention und Verantwortung/Kontrolle über die Waffenkammer gehörten zu Nebenaufgaben, die 2022 ordnungsgemäß abgearbeitet wurden.

Referat Informations- und Wissensmanagement und Kanzleidienst

Nach der herausfordernden Einnahme der derzeitigen Organisationsstruktur im Jahr 2021, konnte sich das Referat IWM&KzlD wieder voll auf die Kerngeschäfte konzentrieren. Die nachfolgende Darstellung soll einen Überblick über die erbrachten Leistungen im Jahr 2022 geben:

Bei den Einsätzen/Übungen DAEDALUS22, G7-Gipfel (ELMAU), der AIRPOWER22 und der AIREX22 wurde das Informationsmanagement geplant, angeordnet, kontrolliert und gesteuert. Hierzu wurde zudem Personal des Referats für die Durchführungsphasen in die Einsatzstäbe abgestellt. Ebenso wurde bei der COMMON ROOF 22, die SG-Übung der Cyberkräfte 2022, personell unterstützt. In den Nachbereitungsphasen wurden zum Zwecke des Wissenserhalts strukturierte Datensicherungen vollzogen.

Quelle: Liferay

Mit November 2021 stand das neue Content Management System (CMS) Liferay DXP für alle Anwender des SMN zur Verfügung. Hierzu wurde unter Federführung des Referats eine Nutzerrichtlinie erstellt und bereitgestellt, um den mit Mai 2022 festgelegten ÖBH-weiten Umstieg zu gewährleisten. Zudem wurde ein erheblicher Beitrag zum bereitgestellten Handbuch samt Intranet-Site geleistet und mehrere Provider-Schulungen durchgeführt. Auch der Intranet-Auftritt der Direktion IKT&Cyber wurde konzipiert, umgesetzt und wird laufend betreut, sodass aktuelle Informationen über das gesamte Leistungsspektrum der Direktion abrufbar sind.

In Bezug zum BMLV-ELAK sind nebst durchgeführten Schulungen zur effektiven und effizienten Geschäftsfallbearbeitung und einer Initiative in Zusammenarbeit mit ZGK, Präs und KonkrPersAdminNG zur Eindämmung der Informationsflut, vor allem die Ausrollung des BMLV-ELAK in den Auslandsmissionen AUTCON KFOR, EUFOR ALTHEA, UNIFIL und zu Kleinmissionen erwähnenswert. Dies brachte erhebliche Vorteile in Bezug auf die einfache Verarbeitung nationaler, einsatzrelevanter Geschäftsfälle bis zur Klassivifierungsstufe E (KlasStu E), das Führen der KTB und der spezifischen Informationsbereitstellung innerhalb der Missionen.

Mit Jänner 2022 wurde das Projekt IDV (individuelle Datenverarbeitungsanwendungen) gestartet, dessen Zweck es ist, sowohl den Bestand als auch den Bedarf

an IDV-Anwendungen innerhalb des ÖBH zu erheben, um deren Nutzen und Anwendbarkeit unter Einbindung der OrgEt des BMLV/ÖBH zu beurteilen bzw. zu priorisieren.

Außerdem wird nebst der Bereitstellung einer geeigneten Entwicklungsumgebung auch eine neue IDV-Richtlinie für das Ressort erstellt werden.
In weiterer Folge sollen als notwendig beurteilte Anwendungen (im Zuge des Projekts „IDV-Ablöse“) unter Vermeidung von Redundanzen und in konsolidierter Form zur unmittelbaren und raschen IT-Unterstützung der Bedarfsträger ÖBH-weit zur Verfügung gestellt werden.

Der abgeschlossene Erhebungsumfang umfasst 89 Meldungen mit insgesamt 793 gemeldeten Anwendungen. Das Erhebungsergebnis erlaubt es, den Bedarf der gesamten Organisation einzuschätzen, um passgenaue Lösungen zu finden.

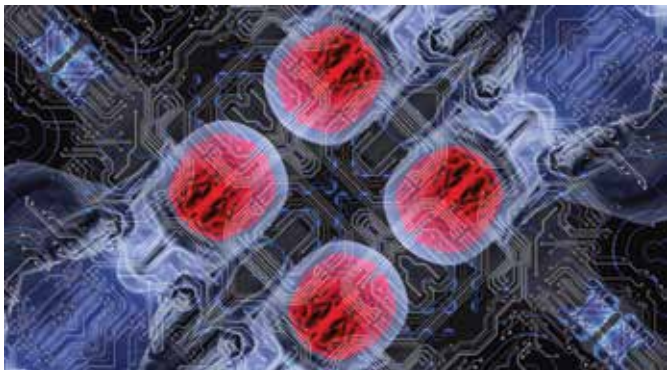
Aufgrund der Vielzahl an Aufgaben, kann hier nicht jede Leistung (bspw. das Postfach-Management im IBM-NOTES, die Entwicklung und Bereitstellung einer Jahres-Vorhabens-Übersicht im IBM-NOTES OE Kalender, die vielen Rollenvergaben im BMLV-ELAK, ...) näher beschrieben werden, aber zur Sichtbarmachung der Leistung der Hauptkanzleien der Direktion IKT&Cyber an vier Standorten.

Referat Informationstechnologie und Führungsunterstützung

Nach der herausfordernden Einnahme der derzeitig geplanten Organisationsstruktur im Jahr 2022, lag der Fokus auf den zukünftigen Kernaufgaben: Sicherstellung der direktionsbezogenen Führungsunterstützung und die Standortbetreuung der IKT- Systeme sowie die dafür vorgesehene System- und Netzwerkadministration für die Generaldirektion und Führungsunterstützung für die GDLV. Zur Aufgabenerfüllung ist das Referat IT&FüU auf vier Standorte aufgeteilt.

Mitte des Jahres wurde der Lehrsaal 107 durch das Ref IT&FüU übernommen und technisch aufgerüstet. Damit ist die Basis für die zukünftige Funktion des Raumes als multifunktionaler Besprechungsraum und als Lagezentrum für den Einsatzstab Cyber gelegt.

Im Herbst 2022 wurden die drei Systemadministratoren und Leitbediener (SysAdmin&LB) am Standort BELGIER Kaserne sowie das S6 Fachpersonal des Standortes Stiftkaserne in das Ref IT&FüU integriert. Die Integration des Standortes SCHWARZENBERG Kaserne erfolgt im Jahr 2023. Zur Unterstützung der Ausbildung wurden IT Grundkurse für Milizexperten durchgeführt. Weiters wurden Bedienstete der GDLV durch Schulungen im neuen CMS sowie im ELAK 4.0 auf den neuesten Stand gebracht.



In Graz wurden durch die Dion1 zwei BLACKOUT-Übungen angeordnet und durchgeführt. Diese Übungen brachten wesentlichen Erkenntnisse für den Notbetrieb der BELGIER Kaserne und notwendige Adaptierungen der Infrastruktur. Ein wichtiger Teilbereich dieses Notbetriebs beinhaltet die Maßnahmen des Troubleshootings der IKT–Systeme bei Wiederhochfahren, im Notbetrieb sowie bei der Rückführung in den Normbetrieb durch die begleitenden Maßnahmen der SysAdmin&LB.

Gegen Ende des Jahres wurde ein Prototyp eines Kanban-Boards basierend auf ITSM realisiert, welches 2023 in den Echtbetrieb übergeführt wird. Das Ziel ist es, die Aufgabensteuerung der Führungsebene der FüAbt effektiver und zielgerichteter zu gestalten.
Aufgrund der Vielzahl an Aufgaben, kann hier nicht jede Leistung angeführt werden, die im Laufe des Jahres durchgeführt wurden. Exemplarisch werden einige Punkte aus dem vielfältigen Bearbeitungsportfolios des Referats angeführt:

- umfangreicher Vorort-Service an den Standorten für die GDLV
- Beratungsleistungen in Angelegenheiten der FüU für die GDLV
- Unterstützung der Reformbearbeitungen für die Direktion IKT&Cyber
- technische Begleitung der S6 Fachbesprechung als hybride Veranstaltung

Operative Kommunikation und Personalwerbung

Die Direktion IKT&Cyber war im Jahr 2022 in der Öffentlichkeitsarbeit sehr aktiv und hat eine Vielzahl an Veranstaltungen besucht. Ziel war es, Werbung für den Cyber-Grundwehrdienst zu machen und Personal für die technischen Bereiche zu werben sowie das Image der Cyberkräfte zu fördern. Die Highlights des Jahres waren die „LEVEL-UP“ Gaming Messe in Salzburg, die Dreharbeiten mit Oscarpreisträger Ruzowitzky, sowie der Nationalfeiertag.

Rekrut des Jahres

2022 siegte in der Kategorie "Rekrut des Jahres" Gefreiter Georg FELBER aus Niederösterreich. Er hat seinen Grundwehrdienst als "Cyber-Grundwehrdiener" im Militärischen Cyberzentrum im Referat "Codeanalyse und technische Forensik" in Wien abgeleistet. Er zeigte seine beeindruckende Expertise bei der Analyse komplexer Malware-Probleme aus aktuellen Angriffen auf die Systeme des Österreichischen Bundesheeres.

Im Zuge seiner Tätigkeit gelang es ihm auch, eine bedeutende Schwachstelle in einem auf künstlicher Intelligenz basierenden Analysesystem aufzuzeigen. Besonders hervorzuheben ist, dass sich Gefreiter FELBER mit seinem Team im Rahmen der "Austrian Cyber Security Challenge" gegen Mitkonkurrenten in seiner Klasse behaupten und den Sieg einfahren konnte.

Platz 2 ging an den ebenfalls nominierten Gfr Elias HOHL, welcher wie Gfr FELBER ebenso im Militärischen Cyberzentrum der Direktion IKT&Cyber seinen Cyber-Grundwehrdienst leistete.

Gfr Georg FELBER

Gfr Elias HOHL

Cyber-Grundwehrdienst; ein Erfolgsmodell

Das IKT-spezifische Angebot des Cyber-Grundwehrdienstes fand seine Ursprünge im Jahr 2014. Seit diesem Zeitpunkt sind kontinuierlich ca. 90 Cyber-Grundwehrdiener jährlich in der Direktion IKT&Cyber bzw. den Vorgängerorganisationen im Einsatz. Durch die steigende Bekanntheit bei Wehrpflichtigen sind die begrenzten verfügbaren Plätze sehr beliebt und schnell gefüllt. Aufgrund dieser Entwicklung wird ab 2024 das System von „First Come, First Served“ auf „Best of the Best“ umgestellt. Dadurch wird den bestqualifizierten Grundwehrdienern ermöglicht, in dem einzigartigen und interessanten Umfeld der Direktion IKT&Cyber mitzuwirken.

Durch die besondere Positionierung des Cyber-Grundwehrdienstes ist die Wertschätzung der Fähigkeiten der Grundwehrdiener sehr hoch, was sich auf die Arbeitsmoral sowie die Ergebnisse der jeweiligen Projekte sehr positiv auswirkt. So wird aus dem Gedankengang „Wir sind hier NUR Grundwehrdiener“ eher das Verständins „Wir verstehen uns als Teil eines großen Teams!“.

Zu den Vorteilen des Cyber-Grundwehrdienstes zählen auch die vielseitigen Einsatzmöglichkeiten innerhalb der Direktion: Cyber-Gehilfe, Informations- und Dokumentationsgehilfe, Netzwerktechniker, Programmierer, IKT-Sicherheitsexperte sowie Grafik-/Medientechniker.

Informationsoffiziere

Eine neue Initiative im Jahr 2022 war die Einführung des Systems der Informationsoffiziere. Diese Mitarbeiter repräsentieren neben ihren Tätigkeiten in der Direktion IKT&Cyber diese bei Veranstaltungen zur Personalwerbung und Imagepflege. Dazu fanden zwei Fortbildungen statt, um sie für ihre Aufgabe optimal vorzubereiten. So wurden über 20 Veranstaltungen durch Informationsoffiziere besucht.

Dieses Engagement hat sich ausgezahlt, denn die Direktion IKT&Cyber hat auf den Veranstaltungen einen sehr guten Eindruck hinterlassen. Es wurde viel über den Cyber-Grundwehrdienst und Jobangebote gesprochen, aber auch der Austausch mit anderen Experten im Bereich der IKT war wichtig.

Die Partnerschaftspflege mit der HTL Spengergasse konnte mit mehreren gemeinsamen Veranstaltungen gepflegt werden, während bei zwei weiteren HTLs die ersten Events zu einer möglichen Partnerschaft stattfanden. Die Traditionstage von FüUS, FüUB1 und FüUB2 rundeten das Angebot der operativen Kommunikation ab.

Durch die Teilnahme an all diesen Veranstaltungen und die Arbeit der Informationsoffiziere hat die Direktion IKT&Cyber ihre Bekanntheit erhöht und zeigte, dass sie ein moderner und attraktiver Arbeitgeber ist. Die Direktion IKT&Cyber blickt auf ein erfolgreiches Jahr 2022 zurück und freut sich darauf im Jahr 2023 die bestehenden Initiativen, Partnerschaften und auf weitere innovative Projekte.

Der Informationsraum

Informationsoperationen und der Informationsraum sind in der heutigen schnelllebigen Welt von großer Bedeutung. Sie beziehen sich auf die Verwaltung und Nutzung von Informationen, um Ziele und Interessen zu erreichen.

Informationsoperationen beziehen sich auf die gezielte Verbreitung von Informationen, um Einfluss auf die Meinungen und Entscheidungen von Individuen und Gruppen zu nehmen. Dies kann sowohl positiv als auch negativ sein. Positive Informationsoperationen beziehen sich auf die Verbreitung von wahren und nützlichen Informationen, während negative Informationsoperationen Falschinformationen und Desinformation verbreiten.

Ein wichtiger Aspekt von Informationsoperationen ist die Nutzung von sozialen Medien und Online-Plattformen, um die Verbreitung von Informationen zu beschleunigen und zu verstärken. Dies ermöglicht eine schnelle und effektive Verbreitung von Informationen, andererseits kann es auch zur Verbreitung und Verstärkung von Falschinformationen und Desinformation führen.

Informationsraum bezieht sich auf den Bereich, in dem Informationen verarbeitet, gespeichert und genutzt werden. Dies umfasst sowohl physische als auch digitale Räume. Der digitale Informationsraum hat in den letzten Jahren an Bedeutung gewonnen, da immer mehr Informationen online gespeichert und genutzt werden. Einerseits ermöglicht es einen schnellen und einfachen Zugriff auf Informationen, andererseits kann es auch zur Überwachung und Kontrolle von Individuen und Gruppierungen führen.

Ein weiterer Aspekt von Informationsoperationen ist die Verwendung von psychologischen und sozialen Techniken, um die Meinungen und Entscheidungen von Individuen und Gruppen zu beeinflussen. Dies kann von Regierungen, staatlichen Organisationen, aber auch von privaten Unternehmen und Einzelpersonen durchgeführt werden.

Ein Beispiel für den Einsatz von Informationsoperationen im Krieg ist die Verwendung von psychologischer Kriegsführung (PSYOPS) um die Moral und den Willen des Feindes zu schwächen. Dies kann durch die Verbreitung von Gerüchten und durch gezielte Beeinflussung von Individuen und Gruppen durch verschiedene Medien und Kanäle erreicht werden.

Im Rahmen von Friedensmissionen können Informationsoperationen eingesetzt werden, um die Öffentlichkeit über humanitäre Hilfe zu informieren und um die Zusammenarbeit und Unterstützung der Bevölkerung zu gewinnen. In diesem Kontext kann auch gezielte Kommunikation genutzt werden, um extremistische Ideologien und Gewalt zu bekämpfen.

Beim Einsatz von Informationsaktivitäten ist stets das Zusammenwirken mit anderen Wirkmitteln in allen Domänen der Kriegsführung anzustreben. Insbesondere ist hier die Verwendung von Methoden der elektronischen Kampfführung (EloKa) zu beurteilen, um die Kommunikation des Feindes zu stören oder zu unterbrechen. Auch Cyber-Angriffe können eingesetzt werden, um die Kommunikations- und Informationssysteme des Feindes zu stören oder zu zerstören.

Es ist wichtig, die Auswirkungen von Informationsoperationen zu verstehen und zu beurteilen, um sicherzustellen, dass sie im Einklang mit den moralischen und rechtlichen Standards und im Interesse der nationalen Sicherheit eingesetzt werden.

Bgdr Mag. Gerhard WEINER

Abteilung IKT&Cyber Planung

„Die besondere Anforderung liegt in der Planungsleistung zur Fähigkeitsentwicklung in den Domänen Land und Luft, wo der Bedarf an IKT und IT, sowie der Digitalisierung insgesamt, permanent einzubringen ist.“

Das Jahr 2022 war von zahlreichen Herausforderungen geprägt; ausgehend von einer bis Redaktionsschluss dienstrechtlich unveränderter Besetzung von Arbeitsplätzen der Bediensteten in der Altorganisation waren mit derselben Anzahl von Mitarbeitern nicht nur die bestehenden, sondern auch neue Aufgaben wahrzunehmen.

Neben der auch bisher zugeordneten Fähigkeitsentwicklung in der Domäne Cyber, somit den Waffengattungen IKT, elektronische Kampfführung (eloKa) und Cyber ist IKTCyPl nunmehr auch zuständig für die Domäne des Informationsumfeldes mit den Waffengattungen Kommunikations-Truppe (Komm-Tr) und Psychologische Kampfführungs-Truppe (PsyOps-Tr). Die Zuordnung der Fähigkeitsentwicklung für die Domäne Weltraum ist in Aussicht genommen.

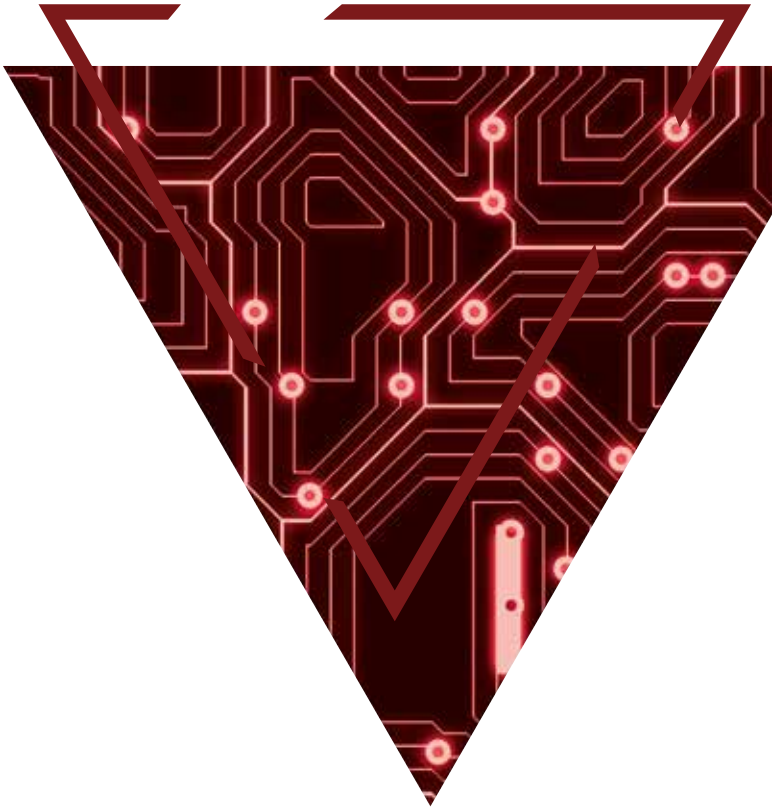
Aufbauorganisatorisch bestand die Herausforderung, die fachdienstliche Zuordnung zur Dion Fäh&GSPl (Aufgabe der Koordination der Fähigkeitsentwicklung) mit der organisatorischen Unterstellung unter die Direktion IKT&Cyber in Einklang zu bringen. Getreu dem Leitspruch „Wo ein Wille da ein Weg“ gelang es zunehmend unter Nutzung von Synergien aus dem Bereich der Direktion IKT&Cyber auch diese Herausforderung zu meistern.

Erhebliche personelle Ressourcen waren zur Entwicklung von Strategien im Rahmen der Arbeitsgruppe DIKT aber auch zur Unterstützung des Überleitungsverantowortlichen Direktion IKT&Cyber in dessen Funktion als Chief Digital Officer abzustellen.

Aber auch im eigenen Zuständigkeitsbereich waren wesentliche Grundlagenbearbeitungen zu leisten. Elementar für die Entwicklung der Waffengattung Cyber wurde eine Leitlinie Cyber Verteidigung erstellt, Autarkieerfordernisse im Bereich der Sicher-

stellung von IT-Services in mil. Liegenschaften führten zur Erteilung eines umfassenden Projektauftrages durch die Ressortleitung; hier sollen 2023 wesentliche Sachverhalte aufbereitet und durch die Ressortleitung die erforderlichen Entscheidungen getroffen werden.

Der UKRAINE-Krieg führte zu einer politischen Neubewertung jener Ressourcen, die dem ÖBH (hinkünftig) zur Verfügung gestellt werden sollen. Das bedeutete ein intensives und zeitkritisches Beurteilungsverfahren für die Fähigkeitsentwicklung aller zugeordneten Waffengattungen, wo unter zugrunde Legung des zu erreichenden Zielzustandes 2032 die dafür erforderlichen Aufbauschritte mit Schwergewicht auf die Entwicklungslinie Invest festzulegen waren.



Besonders gefordert sind wir bei der ständigen Beitragsleistung zur Fähigkeitsentwicklung in den Domänen Land und Luft, wo der Bedarf an IKT und IT, der Digitalisierung insgesamt, permanent einzubringen ist. Das erfordert eine kontinuierliche und intensive Begleitung der Abteilung StruktPl, indem eine Einbindung von Experten bereits auf Prozessebene stattfindet.

Die Fähigkeitsentwicklung per se wurde durch den Überleitungsverantwortlichen der Direktion IKT&Cyber zum Schwergewicht der Direktion IKT&Cyber erklärt und durch die Implementierung des Cyber Informations Fähigkeits Boards (CIFB) manifest. Die grundsätzlichen Bearbeitungen sollen mit Mitte 2023 abgeschlossen werden, die erarbeiteten Grundlagen sollen dann „in der Linie“ also durch IKTCyPl weiter ausgeplant werden.

Es wird daher 2023 darauf ankommen, dass diese Bearbeitungen maßgeblich durch Mitarbeiter der Abteilung gestaltet werden, personelle Engpässe durch Unterstützungsleistungen der Direktion IKT&Cyber kompensiert werden und danach planmäßig der weitere Ausbau der Abteilung voranschreiten kann.

Wegen der derzeitigen personellen Zersplitterung der Mitarbeiter wird die personelle Zusammenführung aller planerischen Elemente der GDLV unter dem Schirm der IKTCyPl samt der Etablierung eines schlagkräftigen Teams eine der wesentlichsten Zielsetzungen 2023 darstellen.

Beschreibung der Aufgaben

Die Angelegenheiten und Aufgaben der Abteilung IKTCyPl wurden mit der Aufgabenzusammenstellung zur Dienstanweisung der Generaldirektion für Landesverteidigung mit Juni 2022 verfügt.

Die Abteilung IKTCyPl ist für die Fähigkeitsplanung der Waffengattungen der Domänen Cyber und Informationsumfeld federführend zuständig und damit neben der Abteilung Struktur Planung eine der beiden fähigkeitsplanenden Dienststellen. Abgeleitet von den zentralen Prozessen der Landesverteidigung trägt die Abteilung wesentlich im Kernprozess Streitkräfte entwickeln bei. Bereits im verteidigungspolitischen Managementprozess erfolgen die Szenarienableitungen unter entscheidender Mitwirkung der Expertise der Fähigkeitsplaner der Abteilung.

Die Angelegenheiten, die federführend zugeordnet sind, erstrecken sich über die Beurteilung, die Entwicklung, die Vorhabensbeschreibung, die Prioritätenfestlegung bei der Realisierung und die Begleitung bis zur Realisierung. Insbesondere die querschnittlich betrachteten Bereiche der Kommunikationstechnologie und der Informationstechnologie betreffen alle Waffengattungen (damit auch der Domänen Land und Luft) und sind gesamtheitlich zu beurteilen. Hierbei gibt es eine enge Kooperation mit der Abteilung StruktPl, wo unsere Fähigkeitsplaner frühzeitig bei allen Planungsvorhaben eingebunden werden.

Die Abarbeitung der mannigfaltigen Aufgaben spiegelt sich nur teilweise in der Struktur und Personalzuordnung der Abteilung wieder. Die technologischen Entwicklungen der letzten zehn Jahre erfordern auch einer regelmäßigen Anpassung der Strukturen in immer kürzer werdenden Zyklen.

Die mit Schwergewicht zu behandelnden Angelegenheiten der Weiterentwicklungen der konkreten Waffengattungen müssen durch virtuelle Personalmaßnahmen abgedeckt werden.

Betroffen davon sind die Weiterentwicklungen der militärischen Fähigkeiten sowie der Aufgabenstrukturplanung der Cyber-Tr, der EloKA-Tr, der Komm-Tr und der PsyOps-Tr. Parallel dazu erfolgen die Weiterentwicklungen der Enterprise Architektur und der allgemeinen Digitalisierung im Ressort. Im Rahmen des Telekommunikationsgesetzes und des Frequenz- und Spektrummanagement erfolgt das behördliche Wirksamwerden innerhalb der Organisation und als Schnittstelle zu anderen Ressorts und Organisationen.

Grundsätzlich wird die gesamte Fähigkeitsplanung im Verantwortungsbereich der Domäne Cyber und Informationsumfeld von zahlreichen nationalen und internationalen Vorgaben und Kooperationen beeinflusst. Die Zuarbeit durch die Abteilung erfolgt bei der Erstellung der Planungsziele, der Fähigkeitskataloge oder der Fähigkeitsbedarfe und mündet in einer Weisung zur Priorisierung und Realisierung. Die Mitarbeiter der Abteilung IKTCyPl erstellen für deren zugeordnete Waffengattung Motivenberichte und Vorhabensabsichten. In der Querschnittsbetrachtung der Kommunikation / der Informationstechnologie erfolgt die Mitwirkung bei allen Vorhaben aller Waffengattungen. Diese umfassenden Aufgaben machen eine permanente und intensive Zusammenarbeit mit der Abteilung StruktPl erforderlich.

Im Bereich der allgemeinen Streitkräfteplanung erfolgt die Mitwirkung und das Einbringen von Expertise aus den federführenden Domänen durch die Mitarbeiter bei der Aufbauplanung des Bundesheeres für den Zeitraum der kommenden zehn Jahre. Die Planungsannahmen und Vorgaben resultieren dabei aus den Beurteilungen zu den Szenarien der planungsleitenden Schutzoperation. Des Weiteren werden zusätzlich Projekte begleitet und geleitet deren Zielerreichung eine umfassende Zusammenarbeit mehrere Dienststellen erfordert.

Eine Weiterentwicklung und transparente Steuerung der Bewältigung dieser Aufgabenbereiche setzt das Vorhandensein der wichtigsten Ressource in der Planung voraus – der Personalressource.

Digitalisierungsvorhaben

Die Digitalisierung ist in allen Bereichen des Lebens angekommen. Die Veränderungsprozesse werden in Industrie, Wirtschaft und Gesellschaft mit rasanter Geschwindigkeit vorangetrieben.

Die Entwicklungen im Bereich digitaler Technologien und die damit einhergehende Vernetzung von Sensoren, IT-Systemen, Applikationen, Assets mit integrierter digitaler Technologie und menschlichen Akteuren hat und wird den Daten und Informationsaustausch zwischen Menschen und Maschinen zeitlich erheblich beschleunigen. Informationen sind zunehmend ortsunabhängig, mobil und in nahezu Echtzeit verfügbar.

Reale und virtuelle Welten rücken immer näher zusammen und erreichen einen immer höheren Grad der digitalen Vernetzung. Informationen können schneller gewonnen, analysiert und bewertet werden. Darauf basierend können Entscheidungen zielgerichteter und verzugslos getroffen werden.

Digitalisierung ist heute in Industrie und Wirtschaft der zentrale Faktor bei der Transformation der Wertschöpfung. Bei der digitalen Transformation werden Produkte, Services, Prozesse und ganze Geschäftsmodelle digitalisiert. Dies führt zu einem Wandel in den Abläufen der Gesamtorganisation und wird die Art und Weise, wie das BMLV Leistungen erbringt oder Wirkungen erzielt, durch den Einsatz fortschrittlicher digitaler Technologien grundlegend verändern.

Durch den Herrn Generalsekretär und den ChGStb wurde die Arbeitsgruppe DIKT (Digitalisierung und IKT) eingerichtet. Auftrag war die Entwicklung einer Digitalisierungsstrategie sowie einer darauf ausgerichteten IKT- und IKT-Sicherheitsstrategie. Die Arbeitsgruppe wurde durch die IKTCyPl breit und mit hoher Priorität unterstützt. Die verfügte Digitalisierungsstrategie definiert die strategischen Ziele und Vorgaben des Ressorts als verbindliche Grundlage für den digitalen Transformationsprozess des Ressorts und läutet aus strategischer Sicht den Veränderungsprozess ein.

Die Möglichkeiten moderner Technologien und die damit verbundenen Bedrohungspotentiale stellen eine komplexe Herausforderung für den Einsatz in allen Einsatzdomänen und für die Aufgabenerfüllung des Ressorts im Allgemeinen dar. Während der Bedarf an digitalen Technologien und Modernisierungsprogrammen stetig steigt, wächst auch die Angriffsfläche für Bedrohungen der Cyber-Sicherheit. Die Dynamik der technologischen Veränderungen und des Bedrohungsumfeldes erfordern grundlegende Veränderungen im Ressort.

Die digitale Transformation muss als querschnittliche Aufgabe in alle Prozesse der Entwicklung und Weiterentwicklung des Ressorts integriert werden. Dies wird aus technischer und methodischer Sicht durch die IKTCyPl sowie die Direktion IKT&Cyber insgesamt umfassend zu unterstützen sein.

Internationale und gesamtstaatliche Kooperationen

Internationale Kooperationen

Die IKTCyPl nimmt an gesamtstaatlichen und internationalen Kooperationen teil. Wesentliche und ressourcenintensive Aktivitäten werden nachfolgend dargestellt:

Federated Mission Network (FMN)

FMN wurde durch das North Atlantic Council Anfang 2015 gestartet. FMN bietet den konzeptionellen Rahmen für die Zusammenführung von Menschen – Prozessen – Technologien um "Federated Mission Networks" für multinationale Operationen zu planen, vorzubereiten, zu errichten, zu betreiben sowie wieder rückzubauen. Im Zentrum stehen die durch IKT zu unterstützenden militärischen Prozesse und Verfahren. Der Ansatz zur „Vernetzten Operationsführung (NetOpFü)" im multinationalen Rahmen wird konsequent umgesetzt. FMN ist aus nationaler Perspektive betrachtet der "Key Enabler" für die nationale Fähigkeiten Entwicklung interoperabler Kräfte für multinationale Einsätze.

Deutschland-Österreich-Schweiz (DACH)

Die DACH Kooperation FüU/IT wurde 2014 ins Leben gerufen und zielt auf eine konkrete Umsetzung der FMN Vorgaben in einem DACH-Mission Network ab. Seit 2017 wird jährlich eine gemeinsame Übung (Common Roof) durchgeführt, die der gemeinsamen Verifikation und Validierung der definierten Fähigkeiten sowie der Ausbildung des eingesetzten Personals dient. 2022 wurden die Bearbeitungen innerhalb der DACH Kooperation konsequent weitergeführt. Das Schwergewicht des Jahres lag aus Sicht der Fähigkeitsentwicklung weiter im Bereich der IT-Betriebsführung sowie auf der Übung Common Roof. Ab 2023 orientiert sich die DACH Kooperation zunehmend an den gemeinsamen Herausforderungen der digitalen Transformation der Streitkräfte. Dazu wurden im Kontext der Digitalisierung mehrere Fähigkeiten-Cluster gebildet, welche ab Februar 2023 ihre Bearbeitungen aufnehmen.

Gesamtstaatliche Kooperationen

Im Rahmen interministerieller Gremien treffen die Chief Digital Officer Task-Force (CDO-Task-Force) und Chief Information Officer CIO (IKT-Bund) der Bundesministerien zusammen. Dabei werden im gesamtstaatlichen Kontext Gesetzestexte, Strategien und Referenzdokumente erarbeitet, sowie konkrete interministerielle Projekte wie z.B. die IKT-Konsolidierung des Bundes beschlossen. Im gesamtstaatlichen Gremium für Bund, Länder, Städte und Gemeinden (BLSG) erfolgen jene Abstimmungen, um Synergien zwischen den föderalen Strukturen im IKT-Bereich sicherzustellen. Mit der Aufgabe des CDO und CIO ist der Überleitungsverantwortlicher der Direktion IKT&Cyber betraut. IKTCyPl unterstützt den CIO nachhaltig bei dessen Aufgaben, nimmt an den Bearbeitungen in zahlreichen Arbeitsgruppen teil und bringt fachliche Expertise unter Einbindung von Experten ein.

Fähigkeitsentwicklung

Fähigkeitsplanung

Die Abteilung IKTCyPl ist für die Fähigkeitsplanung der Domänen Cyber und Informationsumfeld federführend zuständig und damit neben der Abt StruktPl, eine der beiden fähigkeitsplanenden Dienststellen. Die Entwicklung der Fähigkeiten konkret in den Waffengattungen IKT-Tr, EloKa-Tr, Cyber-Tr, Komm-Tr und PsyOps-Tr basiert auf den militärstrategischen Vorgaben und den internationalen Kooperationsfeldern. Um auch international zusammenwirken zu können, ist die Implementierung von Standards und der Beitrag bei internationalen Entwicklungen entscheidende Voraussetzung.

Einen wesentlichen Bereich der Fähigkeitsentwicklung stellen die Querschnittsbearbeitungen dar, die übergreifend über alle Waffengattungen aller Domänen wirksam werden. Hierzu zählt vor allem der Kommuniktaionstechnologie- (KT-) sowie der Informationstechnologie- (IT-) Bereich, Digitalisierung per se aber auch Ausbildung und Forschung durch Vernetzung mit internationalen Arbeitsgruppen. Folgend werden Themen, die im vergangenen Jahr bearbeitet wurden näher dargestellt.

Experten im Militär

IKTCyPl ist Leitstelle für alle Militärexperten der Bereiche IKT und Cyber. Sie steuert und koordiniert ÖBH-weit ca. 70 Militärexperten der Bereiche IKT & Cybersicherheit & Informationssicherheitsmanagement (IKT&CySih&InfoSihMngt), IKT, IKT-Risikomanagement (IKTRiskMngt), Informationsmanagement & Wissensmanagement (InfoMngt&WM) und Geologische Wissenschaften (GeoWiss).

Davon sind ca. 50 Experten direkt beim MilKdo WIEN beordert. Hauptbedarfsträger dieser Experten ist die Direktion IKT&Cyber, ca. 20 weitere Experten sind bei Ämtern und Verbänden des ÖBH beordert.

Militärexperte ist eine Person, die über facheinschlägiges Wissen verfügt, das im ÖBH nicht oder nicht ausreichend vorhanden ist. Unter dieser Prämisse gilt es, Milizsoldaten und Milizsoldaten zu identifizieren, die für den Fähigkeiten-Erhalt wie auch für die Fähigkeiten-Entwicklung nutzbar gemacht werden. Der Nutzen soll für beide Seiten eine Win-Win-Situation darstellen.

Dieses Wissen soll aber nicht nur der Direktion IKT&Cyber, sondern auch dem gesamten Ressort / ÖBH zur Verfügung gestellt werden. Folgerichtig wurde 2022 eine Militärexperten-Plattform im SMN entwickelt, die voraussichtlich ab dem III. Quartal 2023 operativ gestellt werden wird. Darauf sind alle IKT- und Cyber- und GeoWiss-Experten mit deren Fähigkeitsprofilen und Kompetenzen dargestellt. Jeder Bedarfsträger des ÖBH kann dort für seinen Bedarf den geeigneten Experten finden und mit diesem unmittelbar in Kontakt treten.

Vom 21. – 25. November 2022 fand eine BWÜ der Experten der Direktion IKT&Cyber statt. Ziel war die Zusammenführung der, bei den Experten vorhandenen Skills, mit dem tatsächlichen Wissensbedarf der Fachbereiche der Direktion IKT&Cyber. Bei diesem Skill-matching konnten zahlreiche „Treffer“ erzielt werden, indem konkrete Projekte definiert und identifiziert werden konnten und einzelnen Experten hinsichtlich deren Mitwirkung zugeordnet wurden. Da der IT- und Cyber-Bereich grundsätzlich sehr dynamisch ist, liegt die besondere Herausforderung darin, die richtigen Experten zu den prioritären Bearbeitungen der Direktion IKT&Cyber und des gesamten ÖBH zu finden und zielgenau zuzuordnen.

Die Experten BWÜ, perfekt organisiert von der Leitstelle IKTCyPl hat sich erstmals in den Fachgruppen neu organisiert und den Arbeitsplan für 2023 festgelegt.

"Ohne Experten aus der Miliz, müsste das BMLV teure Expertisen von "Consultern" zukaufen, welche das Militär nicht verstehen. Das Expertensystem ist einzigartig im europäischen Vergleich." meint MjrdhmfD Prof. Mag. CERNE, MBA Experte für DX+RM.

Battlefield Management-System (BMS)

Nachdem die Planungen für die Beschaffung eines BMS für die Führungsebenen vom kleinen Verband / von der Kompanie abwärts, mit einer Schnittstelle zum Führungsinformationssystem, bereits 2021 abgeschlossen waren, erfolgte seitens IKTCyPl Anfang 2022 eine intensive Mitwirkung bei der Erstellung der Leistungsbeschreibung, die von der Abteilung IKTS federführend wahrgenommen wurde. Die Ausschreibungsunterlagen konnten dort finalisiert werden, die Ausschreibung steht unmittelbar vor der Bekanntgabe.

Führungsinformationssystem-Software (FüIS-SW) neu

Die Vorhabensabsicht für die Beschaffung einer neuen Software für das FüIS des ÖBH, die zur Verwendung in den Stäben ab Bataillon aufwärts vorgesehen ist, konnte bis Ende 2022 insoweit finalisiert werden, als das Dokument nach einer internen Abstimmungen voraussichtlich im ersten Quartal 2023 in das Genehmigungsverfahren gehen kann. Grund für die Erneuerung der Software ist die erforderliche Ablöse der Software PHÖNIX/FüIS, die wegen bevorstehender Technologiesprünge der internationalen Standards für Führungsinformationssysteme notwendig geworden war.

Interoperabilität & Teilnahme an der Coalition Warrior Interoperability Exercise (CWIX) 2022:

Zur Sicherstellung, dass die nationalen einsatzorientierten IT-Systeme auch die geforderten internationalen Standards erfüllen und mit den Systemen anderer Nationen interoperabel sind, nimmt das ÖBH seit 2010 regelmäßig an der CWIX teil. Im Jahr 2022 erfolgte die Teilnahme erstmals unter wesentlicher Abstützung auf das Personal sowie die IKT-Services aus dem nationalen Battle Lab in der AG Stiftgasse, vor Ort waren in BYDGOSZCZ/POLEN am NATO Joint Forces Trainings Centre nur wenige Teilnehmer anwesend.

Die Teststellung diente vornehmlich der Überprüfung der (richtigen) Implementierung und der Funktionalität der Core Services im Battle Lab.

Alle Services müssen die Spezifikationen, die gemeinsam im Federated Mission Networking Framework (siehe unten) erarbeitet wurden, erfüllen und sind später für die Übernahme in das IKT-System/Einsatz vorgesehen. So wird einerseits national die Streitkräfte und Waffengattungen übergreifende Zusammenarbeitsfähigkeit im Führungsverbund sicher gestellt und andererseits die Interoperabilität bei multinationalen Missionen ermöglicht.

Teilnahme als „Affiliate“ im Federated Mission Networking (FMN) Framework (seit 2016):

Zur Sicherstellung von Funktionalität und Interoperabilität des nationalen IKT-System/Einsatz beteiligt sich das ÖBH im Rahmen des FMN Frameworks an nachstehenden Arbeitsgruppen, in denen unter Einbringung von erheblichen personellen Ressourcen arbeitsteilig Expertise eingebracht wird; dabei werden Entscheidungen im Konsens aller FMN Affiliates getroffen:

Operational Coordination Working Group (OCWG):

Definition der operationellen Anforderungen und Priorisierung sowie Beschreibung der, durch IKT-Systeme zu unterstützenden Prozesse als Grundlage für „Procedural Instructions“ bei der Spezifikation.

Capability Planning Working Group (CPWG):

Spezifikation der IKT-Services unter Einbeziehung bereits existierender Standards mittels „Service Instructions“ und „Procedural Instructions“ in sogenannten Spirals (aktuell Bearbeitung Spiral 5)

Coalition Interoperability Assurance and Validation Working Group (CIAV):

Überprüfung der Spezifikationen auf technische Umsetzbarkeit und Testbarkeit vor finaler Akkreditierung in einer FMN Spiral

Erstellung von standardisierten Test Cases und Use Cases im Interoperability Core Tool (IO-Core Tool) (Repository) für die akkreditierten Spezifikationen. Das Repository kann und soll von allen Affiliates bei Teststellungen im Rahmen der CWIX, bei FMN CIAV Events und sogar bei nationalen Übungen (z.B. Common Roof) verwendet werden, um Messbarkeit und Vergleichbarkeit von Testergebnissen sicher zu stellen.

Planung und Abwicklung von Events für Verifikation und Validierung in der CIAV Testumgebung. Dabei erfolgt eine Abstützung auf das Combined Federated Battle Laboratory Network (CFBLNet - NATO SECRET), das die nationalen FMN Service Stacks in den Battle Labs vernetzt. Unterstützung von Verifikation und Validierung von IKT-Services im Rahmen der Übung CWIX.

Change and Implementation Coordination Working Group (CPWG):

Hier erfolgt die Festlegung der Joining, Membership und Exit Instructions für FMN Instanzen für jede Spiral FMN Change-Management und Dokumentation der FMN Baseline als Katalog aller IKT-Service Produkte der Affiliates, die nach einem nationalen Request for Change (RfC) formal einen standardisierten Verifikations- und Validierungsevent mit mindestens 3 Partnern bestanden haben und in einem von den CIAV National Leads akkreditierten Bericht als nachweislich interoperabel befunden wurden.

Multinational CIS Security Management Authority Working Group (MCSMA):

Dient zur Sicherstellung, dass die CIS-Security Anforderungen für Bereitstellung und Betrieb von IKT-Services eingehalten werden und dass Einsatznetzwerke über entsprechende Sicherheitsakkreditierungen verfügen.

Informationstechnologie

Das Referat Informationssysteme (InfoSys) in der Abteilung IKTCyPl ist in seinem Themenbereich breit aufgestellt. Als Enabler für die IKT reichen Aufgaben über die Planung von Fach- bzw. Führungsinformationssysteme sowie sonstige Informationssysteme und Standardsoftware in allen Netzen, der Beschreibung von Anforderungen bis zur Weiterentwicklung durch Beiträge zum Change-Management, Updates und Upgrades und der Begleitung der Prozesse zur Realisierung/Einführung.

Besonderes Augenmerk liegt aktuell auf den Bereichen eines modernen Aufklärungs- Führungs- und Wirkungsverbunds und den IT-Services in einem IKT-System Einsatz sowie der netz- und domänenübergreifenden Bereitstellung und Nutzung von Daten und Informationen. Im Rahmen der Herausforderungen der Digitalisierung ist das Referat in die Prozesse anderer Domänen/Direktionen eingebunden, um konkrete Anforderungen abzuleiten und Vorschläge zur Realisierung beizubringen. Mit der Beteiligung an Konferenzen im Federated Mission Networking (FMN) findet ein laufender internationaler Austausch statt, der eine Ausrichtung entlang der eigenen nationalen Ambitionen erlaubt. Gemeinsam mit Deutschland und der Schweiz werden im Rahmen der DACH Kooperation „Digitalisierung“ Fähigkeiten entwickelt, die im Rahmen der Übung COMMON ROOF validiert wurden und in Teilen als Ausgangsbasis für die Entwicklung des IKT-System Einsatz zum Tragen kommen.

Informationsumfeld

Mit dem im Jahr 2017 verfügten und bis heute weiterhin gültigen Militärstrategischen Konzept (MSK) wurde die taktische Struktur der Informationskräfte, die aus den Waffengattungen der Kommunikations- und der Psychologischen PsyOpsTr bestehen, festgelegt. Die Fähigkeitsentwicklung dieser Waffengattungen soll, sofern ein im Rahmen der Zentralstellenorganisation (ZSO) zu systemisierendes Referat innerhalb der IKTCyPl auch realisierst werden kann, von diesem dauerhaft wahrgenommen werden.

Hinsichtlich der Fähigkeitsplanung der Informationskräfte innerhalb des zukünftigen Österreichischen Bundesheeres (ÖBH) 2032+ gab es die Vorgaben und Rahmenbedingungen, dass der Gleichzeitigkeitsbedarf der Waffengattungen und ihrer Elemente sich auf die Schutzoperation auszurichten hat und dass die Fähigkeitsentwicklung der Informationskräfte priorisiert ist. Die Kooperation mit der Deutschen Bundeswehr führte dazu, dass hinsichtlich der Abdeckung des Gleichzeitigkeitsbedarfs auf der unteren taktischen (takt) Ebene eine weitestgehend gleiche Ablauf- und Aufbauorganisation erzielt werden konnte.
Das Planungsdokument PsyOps-Tr auf der unteren taktischen Ebene ist in Bearbeitung und stellt den strukturell erforderlichen Aufwuchsplan an Arbeitsplätzen dar. Das Planungsdokument für die Komm-Tr wird in Abstimmung mit der inhaltlich dafür zuständigen Stelle zu bearbeiten sein. Bis auf Weiteres wird der Gleichzeitigkeitsbedarf im Anlassfall mit einer Truppenteilung aus der „Friedensstruktur“ abgedeckt werden.

Das Arbeitsjahr 2022 war vor allem damit geprägt, Beiträge und Rückmeldung zu grundsatzplanerischen Dokumenten zu verfassen. Diese umfassten z.B. die Beiträge zum Querschnittskonzept Einsatz im Informationsumfeld, zum Fähigkeitskatalog Informationskräfte, zur Verfahrenstafel Informationskräfte und zur Task List PsyOps-Tr, zu den aktuellen Realisierungszielen und zu den Thesenpapieren Komm- und PsyOps-Tr.

Cyberverteidigungsleitlinie

Die Cyberverteidigung ist ein gesamtstaatlicher Prozess unter der Federführung des BMLV und umfasst daher alle Maßnahmen zur Vorbereitung, Aufrechterhaltung und Wiederherstellung der Handlungsfähigkeit im Rahmen einer souveränitätsgefährdenden bzw. –verletzenden Handlung. Wiewohl Grundlagen zur Entwicklung der Waffengattung Cyber, die ja in der Frage der Cyberverteidigung eine Hauptrolle spielt, bereits seit mehreren Jahren vorliegen, wurde die Österreichische Strategie für Cyber Sicherheit (ÖSCS) als wesentliches Rahmendokument zur Einbettung der militärischen Fähigkeiten in einen gesamtstaatlichen Ansatz der Republik im Jahr 2021 verfügt.

Nun gilt es auch unter besonderer Berücksichtigung der aktuellen weltpolitischen Lage (UKRAINE Krieg seit Februar 2022 andauernd) rasch Festlegungen auf militärstrategischer Ebene zu treffen, die es erlauben, auf einer gesicherten Grundlage die Voraussetzungen für die Fähigkeitsentwicklung der Cyber Truppe zu treffen. Dabei spielt der Anlassfall der militärischen Cyber Verteidigung eine besondere Rolle, weil hier der Bedarf an erforderlichen Fähigkeitsträgern bestmöglich abgeleitet und konkretisiert werden kann.

Cyber-Verteidigung stellt einen Teilbereich der militärischen Landesverteidigung dar und ist als Aufgabe dem ÖBH zugeordnet. Dies ist per Gesetz unter anderem in Form der militärischen Landesverteidigung (milLV) oder der Assistenzleistung durch Artikel 9a iVm 79 B-VG sowie im WG §2 (1) definiert. Daher hat das Bundesheer in Ableitung von den zu erwartenden militärischen Anlassfällen (Schutzoperation etc.) Struktur, Kräfte und Mittel zur Verteidigung im Cyber-Raum bereit zu halten. Diese Bereithaltung erfordert auch die Einsatzvorbereitung in Friedenszeiten.

Planung Weltraum

NAVIGATION WARFARE TESTUNG am TÜPl SEETALER ALPE im Mai 2022

Die Direktion IKT&Cyber lud zu einer internationalen Satelliten-Navigations-Vermessung inklusive „Navigation Warfare“ ein und über 40 namhafte Experten trugen zum Erfolg der Veranstaltung bei.

In Koordination mit nationalen und internationalen Forschungspartnern, sowie mit Behörden (insbesondere der nationalen Frequenzbehörde sowie AustroControl) und Institutionen der Europäischen Union (u.a. die Weltraumbehörde EUSPA, die Europäische Verteidigungsagentur EDA, das EU-Satelliten-Zentrum in Madrid) wurden die Signale der verschiedenen Globalen-Navigation-Satelliten-Systeme (GNSS) aufgezeichnet und analysiert: USA-GPS, Europa-GALILEO, russisches GLONASS und chinesisches BEIDOU.

In der Woche 24. bis 26. Mai wurden unter der Leitung von Brigadier Dr. Friedrich TEICHMANN (Leiter IMG und POC operative Weltraumservices für das BMLV) diese Satellitensignale insbesondere hinsichtlich sicherer PNT (Position Navigation-Timing) Lösung am Gelände des TÜPl Seetaler Alpe bei realen Bedingungen umfassend getestet und ausgewertet. Die konkrete Umsetzung der Messkampagne erfolgte durch das Referat Navigation des IMG, das in bewährter Weise durch Milizexperten unterstützt wurde. Die teilnehmenden Fachexperten kamen neben Österreich aus den Niederlanden, Italien, Slowenien und Spanien und waren neun verschiedenen akademischen Institutionen wie z.B. der TU GRAZ zuzuordnen.

Für die einsatzrelevante Auswertung der PNT-Lösungen wurde ein anwenderorientierter Szenarien-Katalog herangezogen (z.B. verschiedene Entfernungen oder Abstrahlungskriterien), der weitere Erkenntnisse zum Aufbau der militärischen Fähigkeit „Navigation Warfare“ und die taktischen Möglichkeiten, ähnlich „Electronic Warfare“ für Jamming (entspricht einer Blockade einer PNT-Lösung) und Spoofing (bedeutet eine Verfälschung der PNT-Lösung) liefern soll.

Auch der Militärkommandant der Steiermark, Brigadier Mag. Heinz ZÖLLNER, konnte sich vor Ort ein Bild von den technischen Möglichkeiten, insbesondere dem GNSS-Monitoring sowie der im Aufbau befindlichen offensive Navigation Warfare Fähigkeit der Direktion IKT&Cyber/IMG durch Jamming und Spoofing von Lokation und Zeit machen.

Bundesministerium für Landesverteidigung

Bgdr Mag. Arnold STAUDACHER

Abteilung IKT&Cyber Einsatz

„Die Zusammenarbeit mit anderen Bereichen der Direktion IKT&Cyber ist insbesondere hinsichtlich der Kernaufgaben der Abteilung, aber auch hinsichtlich der Beitragsleistung zur Fähigkeitsentwicklung der Cyberkräfte von enormer Wichtigkeit.“

Die Zusammenarbeit mit anderen Bereichen der GDLV erfolgt vor allem im Hauptprozess „Streitkräfte einsetzten und führen“ sowie im Rahmen der Vorhabensplanung und unterjährigen Anpassung und Koordinierung aller Vorhaben des ÖBH. In diesem Sinne gestaltet sich auch die Zusammenarbeit innerhalb der Direktion IKT&Cyber, wobei jedoch hier auch der Beitrag zur Fähigkeitsentwicklung der Cyberkräfte im abgelaufenen Jahr von enormer Wichtigkeit war. Im gegenständlichen Bericht wird auf die Leistungen in verschiedensten Einsätzen, Übungen und Vorhaben der Cyberkräfte im abgelaufenen Jahr 2022 eingegangen.

Der Jahresbeginn war noch geprägt von den Einschränkungen aufgrund der Corona Pandemie und wesentliche Vorhaben – wie beispielsweise die Luftraumsicherungsoperation anlässlich Weltwirtschaftsforum in DAVOS (WEF DAVOS) – wurden verschoben bzw. gänzlich abgesagt.

Ab 24 02 22 war dann der Angriffskrieg RUSSLANDS gegen die UKRAINE ein wesentlicher Prägungsfaktor für die Cyberkräfte. Die kriegsbedingten Auswirkungen im Cyberraum führten zu einer erhöhten Wachsamkeit und Aktivität durch IKTCyE und MilCyZ sowohl innerhalb der Direktion IKT&Cyber (insbesondere hinsichtlich Lagebilderstellung) als auch im gesamtstaatlichen und europäischen Rahmen (vor allem im Rahmen von Operative Koordinierungsstruktur (IKDOK)). Bereits ab März wurde die Einsatzbereitschaft bei EUFOR/ ALTHEA deutlich erhöht und die FüUKp/KPE verstärkt die Mission bis dato mit zusätzlichen IKT Trupps.

Bei den Auslandseinsätzen des ÖBH war die erste Jahreshälfte von der Übernahme der Führung der EU Trainingsmission in MALI durch AUT – und somit durch eine deutliche IKT Verstärkung in diesem Einsatzraum geprägt. Zusätzlich konnte im Jahr 2022 die IKT Ausstattung bei KFOR und EUFOR ALTHEA

(neue VCN Mobilfunkgeräte und Ausstattung mit neuer Mission Secret Hardware bei KFOR, Errichten von zusätzlicher Gefechtsstandsinfrastruktur, teilweise Ausstattung mit SILENTEL Kommunikation und Anbindung der Mission an das SMN bei EUFOR ALTHEA) erneuert und verbessert werden.

Bei den Assistenzeinsätzen im Inland leisteten zahlreiche Soldaten der Cyberkräfte einen Beitrag, hier sind insbesondere die Beteiligung mit einer AssKp/FüUB2 in Kärnten im 2. Quartal 2022, die Beteiligung an der Bewachung von Botschaften in der Bundeshauptstadt sowie – zumindest in der 1. Jahreshälfte die Unterstützung beim „Contact Tracing“ zu erwähnen. Zudem wurde im Mai und im Juni d. Jahres die Führungsunterstützung für die beiden Luftraumsicherungsoperationen anlässlich „WEF DAVOS/CHE“ und „G7 Gipfel in ELLMAU/DEU“ sichergestellt.

Im Gegensatz zu den beiden vorangegangenen Jahren war das Jahr 2022 ab dem II. Quartal dann auch wieder von zahlreichen Übungen im In- und Ausland sowie von Vorhaben geprägt. Die Cyberkräfte unterstützten insbesondere die Übung der Landstreitkräfte „European Mountain Thunder“ (6. JgBrig, Raum Tirol) und die „Airpower22“ der Luftstreitkräfte in ZELTWEG und haben zum Erfolg dieser Vorhaben des ÖBH beigetragen.

Als eigene SG Vorhaben konnten die multinationalen Übungen „Locked Shields 22“ gemeinsam mit DEU durch das MilCyZ, „Thors Hammer22“ in SWE durch die EloKa Truppe sowie „Common Roof 22“ in VILLACH durch die IKT Truppe mit dem FüUB1 an vorderster Front erfolgreich durchgeführt werden. Diese und viele andere Vorhaben werden in weiterer Folge in diesem Kapitel noch näher beschrieben.

Die Abteilung IKTCyE ist die Einsatzkomponente der Direktion IKT&Cyber. Sie ist für die Führungsunterstützung, die elektronische Kampfführung und für die Kampfführung im Cyberraum bei allen Einsätzen des Bundesheeres verantwortlich. Ihr sind folgende Aufgaben zugeordnet:

- Gesamtverantwortung innerhalb der Direktion IKT&Cyber über alle Angelegenheiten des Einsatzes der Cyberkräfte des ÖBH sowie diesbezüglich in der gesamtstaatlichen und internationalen Zusammenarbeit.
- Angelegenheiten der operativen Einsatzplanung und Einsatzführung zur Sicherstellung der Führungsunterstützung (FüU) bei Einsätzen des ÖBH.
- Angelegenheiten der Informationsübertragung (verlegbares und mobiles Fernmeldesystem ÖBH (FMSysÖBH)) bei Einsätzen, Übungen und Vorhaben der Streitkräfte (SK).
- Angelegenheiten der Informationssysteme und der Informationsverarbeitung bei Einsätzen, Übungen und Vorhaben des ÖBH.
- Angelegenheiten der elektronischen Kampfführung und der netzwerkorientierten Operationen und Operationen im Cyberraum im Rahmen der operativen Einsatzplanung und Einsatzführung.
- Angelegenheiten der einsatzbezogenen IKT-Sicherheit und des Cyberbedrohungsbildes.
- Wahrnehmung der militärstrategischen Einsatzkoordination, der Einsatzgrundlagen und Einsatzauswertung für den Fachbereich IKT&Cy.

Die Abteilung IKTCyE gliedert sich in folgende Elemente:

- Abteilungsleitung
- Referat Führung und Planung
- Referat IKT Sicherheit und Bedrohungslage Cyber
- Referat Informationsübertragung
- Referat Informationssysteme und Informationsverarbeitung
- Referat Cyber und Elektronischer Kampf
- Referat Einsatzgrundlagen IKT und Cyber

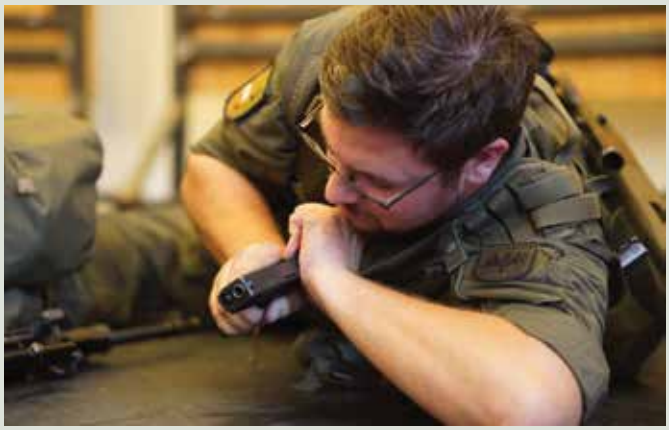
Die Führungsspanne der Abteilung umfasst hinsichtlich aller Einsatzvorbereitungs-, Einsatz- sowie Übungsbelange die FüUS, FüUB1, FüUB2, MilCyZ, IKTBetr sowie das IMG. Die Zusammenarbeit mit anderen Bereichen der Direktion IKT&Cyber ist insbesondere hinsichtlich der Kernaufgaben der Abteilung, aber auch hinsichtlich der Beitragsleistung zur Fähigkeitsentwicklung der Cyberkräfte von enormer Wichtigkeit. Im gegenständlichen Bericht wird auf die Leistungen dieser Elemente in verschiedensten Einsätzen, Übungen und Vorhaben eingegangen.

Im Jahr 2022 wurde unter ff des Referates Informationsübertragung (InfoÜ) mit der Installierung einer „Notkommunikation über Kurzwelle (KW) für das ÖBH bei unvorhersehbare Netzausfällen“ begonnen. Dazu wurden autarke und datenfunkfähige Führungsnetze KW/UKW österreichweit für das gesamte ÖBH geplant und die Umsetzung im September befohlen.

Eine erste Evaluierung bzw. Überprüfung der „Notkommunikationsnetze“ wurde im Zuge einer Alarmübung Anfang Dezember durchgeführt. Dabei lag das Hauptaugenmerk auf die Sicherstellung und Erhaltung der Führungsverbindung für die Kommanden.

Führungs-unterstützungs-schule

Die Führungsunterstützungsschule (FüUS), als Heimat der Cyberkräfte, betreut seit 2017 Kräfte aus den Waffengattungen Cyber, Elektronische Kampfführung (EloKa) und Informations- und Kommunikationstechnologie (IKT). Im Jahr 2022 wurden dabei, analog zu den Vorjahren, unterschiedlichste Lehrgänge, Laufbahnkurse, Seminare und sonstige Vorhaben abgehalten. Höhepunkte waren dabei die Realisierung der 1. Sonderwaffenübung für FüUS-Milizteile, die Ausbildung von zwei Einrückungsterminen an Grundwehrdienern, ua. für Streitkräftebasis (ET 02/2022) sowie die Direktion 4 (ET 06/2022). Herausforderung für das Lehrelement war die Abwicklung des ET 10/2022 mit 93 GWD und die parallele Ausbildung der Cyber GWD in Stärke von 59 GWD.



Teilnehmer der Sonderwaffenübung

Neue Führung der FüUS

Oberst des Generalstabsdienstes (ObstdG) Mag. Franz Sitzwohl wurde mit Wirksamkeit vom 1. November 2022 im Rahmen einer Truppenverwendung für die Dauer eines Jahres mit der Funktion des Kommandanten der FüUS beauftragt. Am 7. November 2022 wurde hierzu das Kommando der FüUS im Zuge eines Festaktes vom vorgesetzten Kommandanten, Generalmajor Mag. Hermann Kaponig, offiziell an ObstdG Sitzwohl übergeben. Im Zeitraum von Juni 2021 bis zur Ablöse war der stellvertretende Kommandant, Oberst Michael Hoffmann, mit der Führung der FüUS beauftragt und konnte so eineinhalb Jahre zur Entwicklung beitragen.

ObstdG Sitzwohl ist ausgebildeter Infanterist und war zuletzt im Rahmen eines Auslandseinsatzes als Kommandant des 46. Kontingents im Kosovo tätig. Gemeinsam mit dem Kader der FüUS wird er sich im kommenden Jahr den Herausforderungen in den Bereichen Digitalisierung, IKT, EloKa und Cyber stellen.

Kommandoübergabe an ObstdG SITZWOHL

Offiziers- und Unteroffiziersaus-, -fort- und -weiterbildung

72 Curricula unterstreichen die Diversität der Ausbildung, welche von der FüUS zu beachten ist. Die Reichweite erstreckte sich über Inhalte der oa. Waffengattungen und resultierte in der Lehre und Ausbildung von Kadersoldaten für:

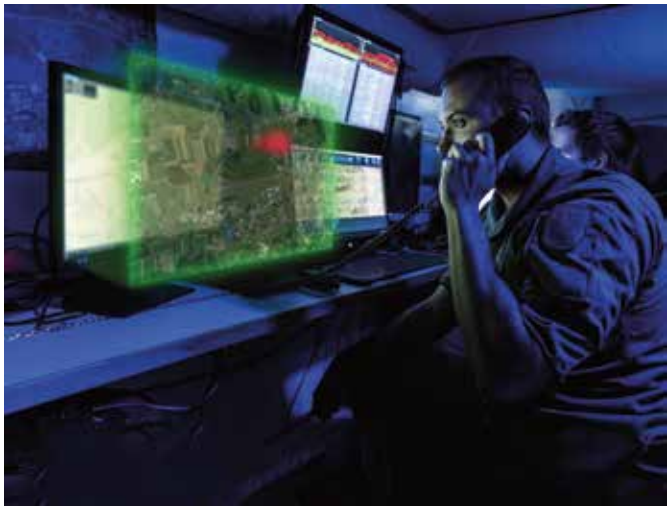
- Kaderanwärterausbildung 2 (KAAusb2): 23 Wochen mit 43 Teilnehmern.
- KAAusb2/Umschuler: 17 Wochen mit 19 Teilnehmern.
- Kaderausbildung 5 (KAusb5): 12 Wochen mit 40 Teilnehmern.
- Militärakademiker: 33 Wochen mit 10 Teilnehmern.
- Lehrgang Grundlagen für Waffengattungsfremde: 16 Wochen mit 4 Teilnehmern.
- Weiterbildung S6: 6 Wochen mit 6 Teilnehmern.

Im Rahmen von Ausbildungslehrgängen betreffend IKT Sicherheit, Leitbediener und Datennetzwerke wurden insgesamt 213 Teilnehmer ausgebildet. Im Lehrgang Grundlagen EloKa für die Landstreitkräfte und Spezialeinsatzkräfte wurden insgesamt 40 Personen ausgebildet.

In Summe wurden an der FüUS im Jahr 2022 ca. 17.000 Ausbildungs-Personentage geleistet. Dabei wurden mehr als 800 Kaderangehörige im Rahmen von 72 Ausbildungsvorhaben ausgebildet.

Diese Leistungsbilanz war nur durch Unterstützung und enge Zusammenarbeit mit IKTCyE, FüUB1 und FüUB2 sowie allen FüU-Kompanien der Brigaden möglich. Die FüUS bedankt sich an dieser Stelle für die gute Zusammenarbeit und Unterstützung.

Erstmals startete 2022 an der TherMilAk der Studiengang „militärische IKT Führung“ mit 22 Fähnrichen. Dieser neue Lehrgang wird den modernen Erfordernissen der Offiziersausbildung in den Waffengattungen IKT und Cyber gerecht und wird künftig die darauf aufbauende Ausbildung an der FüUS prägen.



Einsatzvorbereitungen

Die FüUS führte 2022 im Rahmen der internationalen Einsätze KFOR (Kosovo), EUFOR (Bosnien) und UNIFIL (Libanon) mit jeweils zwei Rotationen im Jahr, insgesamt 12 Wochen die Einsatzvorbereitung im Bereich Führungsunterstützung durch. Für jeweils zwei Wochen wurden dabei, in Abstimmung und Zusammenarbeit mit der Abteilung IKTCyE, sowie FüUB1 und FüUB2, durchschnittlich etwa fünf Teilnehmer auf die Aufgaben der S6-Gruppe, Leitbediener, Vermittlungssystem und Kommunikationszentren (COMCEN) für den Auslandseinsatz vorbereitet.

TCN und KW-System

Eine Zäsur im Rahmen der künftigen FüU-Ausbildung stellt die Implementierung des Tactical Communication Network (TCN) dar. Durch die im Jahr 2023 startende Einführung von TCN wurden sowohl die Ausbildungslandschaft als auch infrastrukturelle Herausforderungen an der FüUS nachhaltig gestaltet. Systemtests, neue Curricula sowie eine komplette Neugestaltung von Ausbildungsgängen waren erforderlich. Dazu wurden Zieldefinition, Lehrgangsplanung und Curriculaerstellung stets unter intensiver Einbindung des bereits geschulten Fachpersonals der Truppe durchgeführt.

Funkstelle mit Band - MMO-Antenne

Zu Beginn des Jahres 2022 wurde die zweite Firmenschulung für Betriebslehrpersonal abgeschlossen, gefolgt von einer ersten Felderprobung des Datenfunkanteils im April.

Einen Höhepunkt bildete die erste, rein durch FüUS und Truppe durchgeführte Schulung am System für weiteres, 24 Personen umfassendes, Fachpersonal. Weitere Erprobungen im Juli zur Feststellung der Reichweiten und Bandbreiten des Datenfunks und im September zur Arbeitsweise am Gefechtsstand bildeten den Abschluss des praktischen, feldmäßigen Wissenserwerbs. Das durchwegs intensive TCN-Jahr 2022 endete mit zwei taktischen Fortbildungen für den Ausbildungskader im November und der dreitägigen Firmenschulung für Netzmanagementlehrpersonal im Dezember.

Die Einführung des neuen Kurzwellensystems Harris (KWSys Harris) erforderte drei Systemschulungen in der Dauer von jeweils 15 Ausbildungstagen mit 14 Teilnehmern und zwei Seminare KW-Planung mit je 10 Tagen Ausbildungsdauer und 4 Absolventen.

Ausbildung an der Splitbox des Datenfunkgerätes

Nachdem das Kurzwellenfunksystem Landstreitkräfte (KWFuSys LaSK) immer breiter zur Truppe ausgerollt wird, erforderte dies im Jahr 2022 drei Systemschulungen für das künftige Betriebspersonal.

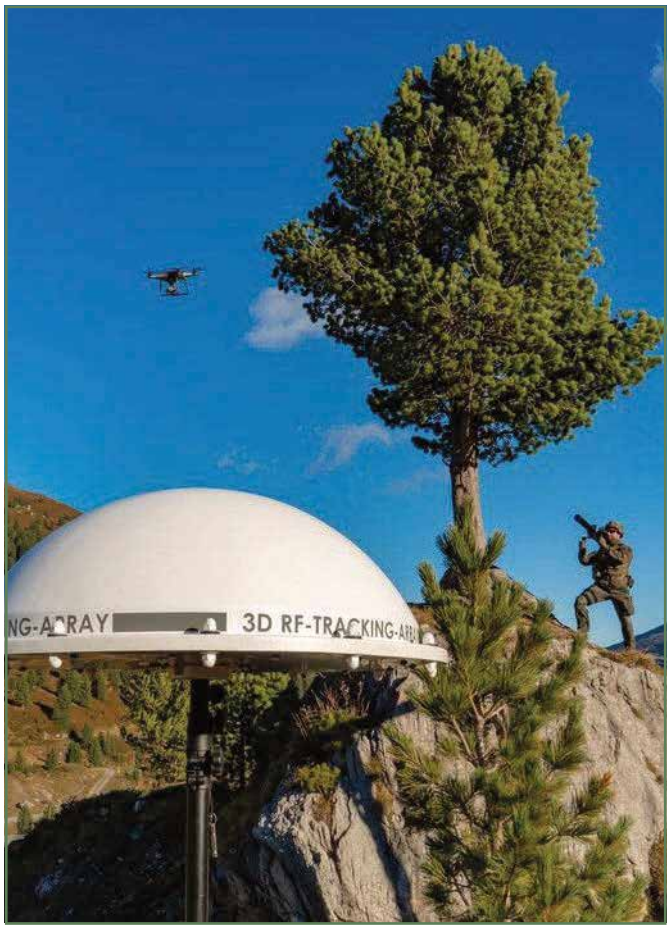
Jede dieser Systemschulungen umfasst 15 Ausbildungstage und deckt den Ausbildungsbedarf von 14 Teilnehmern. Darauf aufbauend wurden zwei Seminare für Planungspersonal an der FüUS im Umfang von je 10 Ausbildungstagen und je 4 Absolventen durchgeführt. Außerdem wurde mit den curricularen Grundlagen der Grundstein für die folgende Regelausbildung am KWFuSys LaSK gelegt.

Internationale & nationale Vernetzungen

International beschreitet die FüUS weiter Neuland, was jedoch die Aussichten zur Erreichung der vollen Interoperabilität der Cyberkräfte bietet. Dieses Netzwerk an Möglichkeiten im nationalen und internationalen Bereich gilt es laufend zu intensivieren.

Teilnahme an der Schieß- und Lehrübung der TherMilAk

Darin ist auch der vermehrte Austausch von Lehr- aber auch Ausbildungspersonal inkludiert. Im DACH-Rahmen, mit Deutschland und Schweiz, wurden zahlreiche Ausbildungen im Zuge von Lehrgängen und Seminaren durchgeführt. Diese reichen von der KAAusb2 bis hin zur FachAusb StbO/S6. Dabei wurden insgesamt 19 internationale Ausbilder sowie 67 internationale Kursteilnehmer an die FüUS abgestellt.



Einsatz Elektronischer Drohnenabwehr

Neben den vermehrten internationalen Abstellungen an der FüUS wurde auch erstmalig die Alpentriode in Österreich durchgeführt. Das Konzept der Alpentriode wurde bereits 2015 in einer Kooperation mit Deutschland und Schweiz entwickelt. Das Ziel der einwöchigen Ausbildung war den anderen Nationen das Österreichische taktische Planungsverfahren im Bereich der Führungsunterstützung zu präsentieren. Anhand eines multinationalen Szenars wurde dies danach durch alle beteiligten Nationen zur Anwendung gebracht.

National wurde im Jahr 2022 die Umstellung der Taktikausbildung im Bereich der Planung des Einsatzes mit neuen Organisationselementen und die Implementierung der TCN-Systeme im ÖBH intensiviert.

Hierzu wurden die Kooperationen mit Akademien und Schulen weiter gesteigert, um im Bereich der Taktikausbildung (FüLG, StbLG, GStbLG etc.) die neuesten Erkenntnisse aus Sicht der Führungsunterstützungszentrale zu vermitteln. Dies wurde unter anderem mittels Mobile Training Teams (MTTs) umgesetzt.

Elektronische Drohnenabwehr (ELDRO)

Das ELDRO-Element kann auch im Jahr 2022 auf zahlreiche Übungen und Einsätze zurückgreifen. Um beispielsweise zukünftige Einsätze zu erleichtern, wurden bereits zu Beginn des Jahres, in Zusammenarbeit mit dem BMI, Vermessungsflüge im Raum Wien durchgeführt, um Detektionsreichweiten verschiedenster Aufstellungsplätze präzise festlegen zu können.

Elektronische Drohnenabwehr

Des Weiteren wurde das Element bei zahlreichen Veranstaltungen im Rahmen der Öffentlichkeitsarbeit zum Einsatz gebracht, um in diesem Zusammenhang vor allem auf die Aktualität der Problematik bei der Handhabung handelsüblicher Drohnen aufmerksam und der Bevölkerung bewusst zu machen, dass es seit 2017/18 ein funktionierendes Schutzschild gegen diese Bedrohung im ÖBH gibt.

Darüber hinaus wurde zeitweise Personal für die Mitwirkung der Erprobung neuer Systeme (HENSOLDT & RHEINMETALL) abgestellt, um die Fachexpertise des seit 2017 bestehenden ELDRO-Elements mit einwirken lassen zu können. Neben zahlreichen weiteren Übungen (Schutzschild BWÜ JgB8, URBAN HERMES etc.) kann der Einsatz im Zuge der „Airpower22“ hervorgehoben werden.

Im Rahmen der Großveranstaltung kam es zu einer Vielzahl an Drohnendetektionen, welche unter anderem durch Gegenmaßnahmen erfolgreich bekämpft werden konnten. Das herausfordernde Jahr wurde mit einem Assistenzeinsatz an der Grenze Burgenland abgeschlossen. Ziel dieses Einsatzes war eine Grenzraumüberwachung durch das ELDRO-Element herzustellen und die Anzahl der Drohnenflüge im Grenzbereich fest zu stellen.

Führungs-unterstützungs-bataillon 1

Beorderte Waffenübung 2022

Vom 27 06 bis zum 02 07 22 fand eine Beorderte Waffenübung bei den Villacher Fernmeldern statt. Aufgrund des „Rückstaus“ der letzten Jahre wurden knapp 170 Milizsoldaten in die Lutschounig-Kaserne einberufen. Die Milizionäre wurden auf 4 Züge aufgeteilt, wobei bei der Einteilung auf die bisherige Vorerfahrung und auf die Anzahl an bisher abgeleisteten Truppenübungen Rücksicht genommen wurde. Nach Kenntnisauffrischung im Bereich Waffen und Schießdienst, im Nahkampf sowie im Bereich der Kampfmittelabwehr einschließlich Verlegung auf den Truppenübungsplatz Marwiesen zum „Scharfschießen“ zu Beginn der BWÜ, stand der Rest der Milizübung ganz im Zeichen der Führungsunterstützung mit Ausbildung an den Fernmeldegeräten.

Alle gestellten Aufgaben konnten von den Milizsoldaten ohne nennenswerte Probleme oder Friktionen gelöst werden. Ein Wettschwimmen, welches aufgrund der hohen Temperaturen kurzfristig angeordnet wurde, rundete eine gelungene Waffenübung ab. Am Kameradschaftsabend tauschten die Soldaten die Erlebnisse der letzten Tage kameradschaftlich aus. Am Samstag, als letzter Programmpunkt gab es abschließendes Antreten, bei dem Auszeichnungen verliehen, Beförderungen durchgeführt und auch Milizsoldaten aus dem Milizstand entlassen werden konnten. Alles im allen war es eine gelungene Woche für alle Teilnehmer.

LWL Bautrupp bei der BWÜ FüUB1

Luftraumsicherungsoperation DÄDALUS 2022

Von 22 05 – 26 05 22 sicherte das Österreichische Bundesheer anlässlich des Weltwirtschaftsforum in Davos (Schweiz) verstärkt den österreichischen Luftraum, täglich starteten Militärpiloten in die vorgegebenen Einsatzgebiete. Dazu wurde ein Flugbeschränkungsgebiet über Teile Vorarlbergs und Tirols errichtet. Mehr als 1.000 Soldatinnen und Soldaten sowie 20 Luftfahrzeuge, zehn Flächenflugzeuge und zehn Hubschrauber, sorgen für die Sicherheit der Veranstaltung und schützen die örtliche Bevölkerung vor Gefahren aus der Luft.

Damit die Luftfahrzeuge alle für den Luftverkehr notwendigen Messdaten und Informationen bekamen, errichteten die Führungsunterstützungssoldaten ein breitbandiges Datennetz. Die Sicherstellung der Funktionalität und der hohen Qualität von allen benötigten Datenleitungen erfüllten die Cyberkräfte problemlos. So unterstützte die 2.FüUKp, zur Bewältigung der gestellten Aufgaben mit Richtfunktrupps. Während der gesamten Übung konnten die Villacher Fernmelder alle Aufträge friktionslos erfüllen und damit einen wesentlichen Beitrag zum erfolgreichen Verlauf der Luftraumsicherungsoperation leisten.

European Mountain Thunder 2022

Relaisstelle bei der LRSiOp Daedalus 22

Die "European Mountain Thunder 2022" ist ein internationales Übungsvorhaben, das von 09 05 – 20 05 22 in den Tuxer Alpen am Truppenübungsplatz Wattener Lizum stattfand. Neben Österreich beteiligten sich Montenegro, Spanien und Tschechien an der Übung. Außerdem wurden im Rahmen der Partnerschaft für den Frieden (PfP) internationale Militärbeobachter aus Italien, Schweden, Kroatien, Rumänien, Slowenien und der Tschechischen Republik entsandt.

Die "European Union Pooling and Sharing Mountain Training Initiative" bezeichnet eine Ausbildungsplattform, die das Ziel verfolgt, die Einsatzfähigkeiten europäischer Gebirgstruppen gemeinsam weiterzuentwickeln. Das Österreichische Bundesheer übernimmt dabei die Führungsrolle.

Das FüUB1 setzte vor allem Datenfunktrupps mit alpiner Erfahrung zur Bewältigung der gestellten Aufträge und Aufgaben ein, galt es doch alle Kommunikationserfordernisse der übenden Truppen innerhalb und außerhalb des taktischen Rahmens umfangreich abzudecken und ein in alle Richtungen stabiles Funknetz für die übenden Soldaten sicherzustellen. 30 Soldaten der 2. FüUKp, eingegliedert in der Gebirgsbrigade, lösten alle sich im Hochgebirge stellenden Herausforderungen ohne Probleme und konnten so einen wichtigen Teil zum Erfolg der multinationalen Gebirgsübung beitragen.

Trinationale “D-A-CH” IKT Übung Common Roof 2022

Im Zeitraum von 03 10 22 bis 21 10 22 fand in den Ländern Österreich Deutschland und der Schweiz die multinationale Übung Common Roof 22 (CR22) statt. Diese Übung zielte auf die Interoperabilität innerhalb D-A-CH (Deutschland-Austria- Schweiz) Community ab und der Fokus lag in der Bereitstellung eines trilateralen Führungsnetzes für Einsätze im Rahmen der grenzüberschreitenden Katastrophenhilfe und der gemeinsamen Abwehr von Bedrohungen im Cyber Raum. Dabei wurden die jeweiligen nationalen Einsatznetzwerke in ein gemeinsames multinationales Mission Network zusammengeführt und festgelegte betriebliche Abläufe und Prozesse anhand einem Szenario und einem Ablaufplan geübt und gleichzeitig evaluiert.

Analyse im Subordinate Service Management and Control Element (SSE)

Die Verantwortlichkeit der Übungsdurchführung der CR22 lag beim FüUB1, bei dem die nationale Übungsleitung inklusive der Netzwerküberwachung des österreichischen Anteiles im multinationalen Netzwerk lag.

Durch das Errichten und Betreiben eines „Subordinate Service Management & Control Elements“ (SSE) am Standort in Villach, führten die Soldaten die beabsichtigten Erprobungen gemeinsam mit Deutschland und der Schweiz durch und überprüften somit alle interoperablen Fähigkeiten in den Bereichen Betriebsführung, Netzsteuerung und Netzwerküberwachung eines nationalen Einsatznetzes in einem multinationalen Verbund.

Techniker aus allen Bereichen der Direktion IKT&Cyber bei den letzten Vorbereitungen

Führungs-unterstützungs-bataillon 2

Das FüUB2 ist seit 1. Juli 2021 truppendienstlich der Direktion IKT&Cyber unterstellt. Das FüUB2 gliedert sich in ein Bataillonskommando mit Stabskompanie, drei Führungsunterstützungskompanien, eine FüUKp für elektronische Kampfführung und eine FüUKp für Kaderpräsenzeinheiten. Zusätzlich betreibt das FüUB2 ein dezentrales Cyberschulungszentrum für die Ausbildung von Cyber-GWD für Westösterreich und bildet GWD für ein Cyber Dokumentations- und Informationszentrum aus, welche fachdienstliche Aufträge des Abwehramtes bearbeiten.

Ausbildung der Grundwehrdiener und Einsatzbereitschaft des FüUB2

Im Jahr 2022 wurden bei drei Einrückungsturnussen insgesamt ca. 350 GWD ausgebildet. Zusätzlich wurden ca. 50 Cyber-GWD durch unser dezCSZ geschult. Damit haben, seit der Aufstellung des dezCSZ2 im Juni 2015, 350 Cyber-GWD diese Fachausbildung beim FüUB2 absolviert. Bei drei Kf-Kursen konnten in diesem Jahr über 100 GWD die Führerscheinklasse „C“ erfolgreich abschließen, mehr als 60 GWD für das FüUB2 und über 50 externe Fahrschüler aus dem Koordinierungsbereich der 6.GebBrig.

Zur Zielüberprüfung der Teilkontingente im Verband sowie zum Erhalt und zur Verbesserung der eigenen Fähigkeiten führte das FüUB2 im Jahr 2022 zwei Alarmübungen durch. Hierbei war das Ziel, jeweils den präsenten Einrückungstermin im letzten oder vorletzten Ausbildungsmonat, die StbKp, die FüUkp (eloKa) und das Bataillonskommando (Bkdo) in den Übungsablauf einzubinden. Von 01. bis 03. März wurden hierbei die Fähigkeiten des ET 10/21 überprüft. Von 11. bis 13. Oktober war der ET 06/22 der 2.FüUKp im Rahmen eines Schutzszenarios gefordert.

Assistenzeinsätze im Inland

Das FüUB2 war im zweiten Quartal 2022 der formierungsverantwortliche Verband für eine Kompanie im Rahmen des sicherheitspolizeilicher Assistenzeinsatz (sihpolAssE) Migration/hsF, gem. § 2 Abs. 1 lit. b. WG 2001 im Verantwortungsbereich des Militärkommandos Kärnten. Die Hauptkräfte dafür wurden durch die 1.FüUKp mit ihrem Kader und den Rekruten aus dem Einrückungsturnus Oktober 2021, auf Basis des Funktionsdienstes im Modell „6+3“, gestellt.
Unter der Einsatzführung des Lagezentrums des Militärkommandos Kärnten zählten zu den Aufgaben dieser Assistenzkompanie: Die Zusammenarbeit mit der Landespolizeidirektion Kärnten, Grenzkontrollen zu Slowenien, Ausgleichsmaßnahmen zu Italien und die ständige Überwachung des grenznahen Raumes. Zusätzlich wurden im Rahmen des AssE COVID, § 2 Abs. 1 lit. c. WG 2001, die Bezirksverwaltungsbehörden zur Pandemiebekämpfung unterstützt und die Einhaltung der COVID-19 -Einreiseverordnung an definierten Grenzübergängen überprüft.

Im Rahmen des Assistenzeinsatzes Contact-Tracing bei der BH St. Johann im Pongau wurde von Jahresbeginn bis zum 15. April 2022 bei den Containment-Maßnahmen der Gesundheitsbehörden mitgewirkt. Das FüUB2 stellte durchgehend vier Soldaten für diesen Einsatz. Zur Sicherstellung der Entlastung der LPD Wien waren im Rahmen des sihpolAssE Objektschutz Wien von 28. März 2022 bis 04. Juli 2022 permanent zwei Soldaten des FüUB2 im Einsatz.

Leistungen im Auslandseinsatz

Aufgrund der Lageentwicklung, hervorgerufen durch den Angriff Russlands in der Ukraine, beurteilte das Operation Headquarter (OHQ) Operation ALTHEA die Notwendigkeit der Entsendung der Reservekräfte zu EUFOR/ALTHEA. Die Alarmierung der Intermediate-Reserve-Kräfte erfolgte am 23. Februar 2022. Bereits am 26. Februar wurde der Österreichische Anteil dieser Truppen, bestehend aus InfKp, IKTTrp und EOD- Element, entsandt. Zur Sicherstellung der Verbindung von den Kompanien zur Tactical Operation Cell des MNBN, befanden sich bis zum Jahresende dauerhaft acht Soldaten der FüUKp/ KPE als IKTTrp im Auslandseinsatz.

Unterstützung von Vorhaben der Streitkräfte

Im Zuge der Selbstevalurierung (SEL2) ABCAbwKp/KPE, durchgeführt in der 7. und 8. Kalenderwoche im Tritolwerk, konnte die 1.FüUKp mit der Gestellung eines Funkzuges, der die Verbindungen der Übungsleitung sowie der zu evaluierenden Kompanie sicherstellte, seine Fähigkeiten unter Beweis stellen. Bei der NEL2 der PzGrenKp/KPE in Allentsteig wurde von der 42. Kalenderwoche bis zur 46. Kalenderwoche mit einem Funktrupp unterstützt.

Anlässlich des G7-Treffens in Elmau (Deutschland) waren Teile der 3.FüUKp im Rahmen einer Luftraumsicherungsoperation eingesetzt. Dazu wurde ein Flugbeschränkungsgebiet über Teilen Tirols errichtet, um die örtliche Bevölkerung vor Gefahren aus der Luft zu schützen. Auch hier konnte mit Hilfe unserer präsenten IKT-Kräfte eine kompetente Unterstützung zur Bereitstellung eines aktuellen Luftlagebildes gewährleistet werden.

Die 3.FüUKp stellte im Juli mit ihren in der Waffengattung IKT-Truppe bestens ausgebildeten Grundwehrdienern das Führungsnetz für die eingesetzten Kräfte bei der Ausbildungsübung „Eisenerz 2022“ sicher. Eine Besonderheit dabei war die Zusammenarbeit der IKT-Truppe mit Elementen der Luftstreitkräfte, da aufgrund des Geländes im Übungsraum die Relaisstandorte teilweise nur per Luft erreichbar waren.

UKW-Relais bei der MilAK Übung „Eisenerz 2022“ am Erzberg

Unter dem Kommando der Theresianischen Militärakademie übten von 11. bis 22. Juli im Großraum Eisenerz über 1.000 Soldatinnen und Soldaten. Bei diesem Manöver konnten die Fähnriche der Militärakademie gemeinsam mit Milizsoldaten und Grundwehrdienern unter anderem die Themen „Angriff“ und „Schutz“ oder Scharfschießen im freien Gelände üben.

Multinationale EloKa Übung „Thors Hammer 22“

Die Spezialisten für den Bereich „Force Protection“ unserer EloKaKp waren von 19. April bis 7. Mai in Schweden bei der internationalen Übungsserie „Thors Hammer“ eingesetzt. Diese Übung bezweckt die Testung von technischen Systemen zur Unterdrückung bzw. Störung von funkgezündeten improvisierten Sprengkörpern (CREW-Systeme: Countering Radio Controlled Improvised Explosive Devices – Electronic Warfare) unter Einsatzbedingungen als Maßnahme zum Truppenschutz. Das nationale Ziel, die Überprüfung der Einsatzbereitschaft und technischen Interoperabilität mit den relevanten Einsatzpartnern mit Fokus auf die EU-Battlegroup 2025, konnte erreicht werden.

Übungsteilnehmer THORS HAMMER

Airpower 22

Bei der größten Airshow Europas, der AIRPOWER 22, welche von 2. bis 3. September am Fliegerhorst Hinterstoisser in Zeltweg stattfand, waren wiederum unsere Experten der EloKaKp im Einsatz. Die EloKaKp bildete das Kernelement des ÖBH innerhalb des „Interministeriellen Ortungsverbundes“ (IMOV) und war für die Schaffung der technischen Voraussetzungen als auch für die Sicherstellung der taktischen Einsatzleitung verantwortlich.

Die Hauptaufgabe dabei war, die Überwachung des Elektromagnetischen Umfeldes (EMU) sicher zu stellen um zielgerichtete Maßnahmen bei unrechtmäßiger oder sicherheitsgefährdender Nutzung des EMU zu setzen. Dadurch konnten Bedrohungen wie die Inbetriebnahme von nicht genehmigten Sendern/Empfängern, das Mithören und Stören von militärischen und/oder zivilen Funkfrequenzen und eine missbräuchliche Nutzung von militärischen und/oder zivilen Frequenzen erkannt, gepeilt und geortet werden. Das Kaderpersonal der EloKaKp hat durch seine profunde Vorbereitung, Planung und Durchführung entscheidend zum reibungslosen und sicheren Ablauf der AIRPOWER 22 beigetragen. Die 2022 erbrachten Leistungen des FüUB2 zeigten wiederum das besondere Engagement, die hohe Professionalität und den Einsatzwillen aller Angehörigen des Verbandes.

Die hohe Qualität der Auftragserfüllung ist ein eindeutiger Beleg für die Nachfrage der Fähigkeiten des FüUB2 und seiner Soldatinnen und Soldaten. Was immer der Dienst von uns verlangt, wir werden stets unser Bestes geben, um unsere Aufträge rasch und effektiv zu erledigen, mit einem geregelten und ordentlichen Dienstbetrieb und hoffentlich immer zur Zufriedenheit unserer Vorgesetzten.

Militärisches Cyberzentrum

Das Militärische Cyberzentrum innerhalb der Direktion IKT&Cyber, hat den Auftrag, die Sicherheit des Ressorts im IKT-, Cyber- und EloKa-Umfeld zu gewährleisten. Es agiert in diesem Rahmen als technische Speerspitze des ÖBH in der Domäne Cyber. Um diese Aufgabe erfüllen zu können, ist regelmäßige Ausbildung und geeignetes Training erforderlich. Nur so können die vielfältigen Herausforderungen gemeinsam gemeistert werden.

Zu diesem Zweck werden Jahr für Jahr unzählige personenspezifische Ausbildungen, welche den speziellen Bedarf der einzelnen Mitarbeiter in ihrer jeweiligen Funktion erforderlich sind, absolviert. Damit erhält jeder Mitarbeiter für sich jene Schulungen, die für das Erbringen der täglichen Leistungen erforderlich sind. Sei es der Überblick über ein neues, spezifisches Fachgebiet, eine vertiefende Schulung zu einem bestimmten Produkt oder Werkzeug, oder zur persönlichen Entwicklung. Doch das ist nicht genug. Die vielfältigen Anforderungen an das MilCyZ, den immer ausgeklügelteren und neuesten Angriffstechniken standhalten zu können, ist lange keine Einzelleistung mehr. Nur im Team können hochkomplexe Cyber-Angriffe erkannt sowie rasch und effektiv abgewehrt werden. Dazu bedarf es regelmäßiger gemeinsamer Übungen, um das fachspezifische Wissen der Einzelpersonen im Team optimal verbinden und einsetzen zu können.

„MilCERT Interoperabilitätskonferenz“ (MIC) der EU

Von 17. bis 19. Februar 2022 fand die insgesamt erst zweite "milCERT Interoperabilitätskonferenz (MIC) der Europäischen Union im technischen Bereich" statt. veranstaltet wurde sie von der European Defence Agency (EDA) organisiert. Ziel dieser Übungsserie ist es, die Kommunikation und Zusammenarbeit und somit das Vertrauen unter den europäischen milCERTs zu stärken. Im jahr 2022 nahmen 200 Experten aus 19 Mitgliedstaaten teil. Das österreichische Team nahm mit 10 Personen teil, und leistete dabei rund 30 Personentage.

Dazu werden im Rahmen einer technischen Cyber-Defence-Übung Angriffe auf ein virtuelles Netzwerk durchgeführt, welche von den jew. milCERTs im eigenen Zuständigkeitsbereich zunächst erkannt und analysiert werden müssen. Die Erkenntnisse sollen einerseits in ein „nationales“ Lagebild, den so genannten „Situational Report“ (kurz: SITREP) einfließen und von der Übungsleitung bewertet werden. Über diesen SITREP wird im militärischen Umfeld die Führung über aktuelle Situationen informiert, um stets eine aktuelle Lageübersicht zu haben, und ggf. steuernd eingreifen zu können. Andererseits müssen aus den Detailanalysen Angriffsindikatoren (Spuren, welche die Angreifer im System hinterlassen haben) erkannt, aufbereitet und mit den anderen Teams geteilt werden. Die Informationsverteilung ist einer der Schlüsselfaktoren in der modernen Cyber-Verteidigung. Nur so ist es möglich, ein gemeinsames Lagebild zu erhalten.

Insbesondere dieser standardisierte Informationsaustausch stellt den Kern dieser Übungsserie dar. Denn auch die Qualität der mit den anderen Teilnehmern geteilten Daten und Informationen über die zentrale „Malware Information Sharing Platform“ (MISP) wird bewertet.

Scoreboard der Übung "MIC22" in Brüssel, Quelle: https://eda.europa.eu/news-and-events/news/2022/01/26/second-eda-live-cyber-exercise-for-military-certs-concluded

Das österreichische Team erlangt auch 2022 zum zweiten Mal in Folge den Sieg in der Spezialwertung „Best SITREP“ und konnte hinter Finnland den zweiten Platz in der Gesamtwertung erreichen.

Im Juni kamen die Leiter der jew. milCERTs in Brüssel für den zweiten Teil der Übung zusammen. Dabei konnten die Teamleiter untereinander Erfahrungen austauschen, und sich näher kennenlernen um das notwendige Vertrauen zu stärken. Darüber hinaus wurden Lehren aus dem technischen Teil der Übung gezogen.

Dies dient dazu, die bestmögliche Unterstützung der Teams zur Zusammenarbeit und zum Informationsaustausch gewährleisten zu können.

Luftraumsicherungsoperation „Daedalus 2022“ anlässlich WEF DAVOS

Das MilCyZ nahm 2022 erstmalig mit zwei Personen und einem Gesamtaufwand von 20 Personentagen aktiv an dieser Luftraumsicherungsoperation teil, um

- den Bedarf betr. Cyber-Lagebild und LRSiOp-relevanten Informationen im Detail zu erheben, und so die österr. Luftstreitkräfte künftig besser unterstützen zu können;
- Awareness-Vorträge im Zusammenhang zwischen den Domänen Cyber und Luft abzuhalten, und so das Bewusstsein betr. Gefahren im Cyber-Raum für das aktiv beteiligte Personal und die Leitungsebene der LRÜ zu stärken; sowie
- aktuelle Beiträge für die Lagebesprechungen zu liefern.

Dabei war es möglich, die Teilnehmer in bestimmte Stabsfunktionen während der LRSiOp in ihrer Cyber Awareness fortzubilden und die Sensibilität vor allem im Bereich von Phishing-Angriffen zu steigern.

Eurofighter bei einem Übungsflug

Luftraumsicherungsoperation anlässlich G7 Gipfel ELMAU (DEU)

Im Juni fand die Luftraumsicherungsoperation (LRSiOp) anlässlich des G7-Gipfels in ELMAU, Deutschland, statt. Dabei unterstützen die österreichischen Luftstreitkräfte, die deutschen Behörden und die Luftwaffe bei der Luftraumsicherung des Konferenzgebietes auf österreichischer Seite. Das MilCyZ hat hierzu erstmalig mit einer Person und einem Gesamtaufwand von 12 Personentagen in Analogie und mit demselben Zweck zur zuvor erwähnten „DAEDALUS 22“ aktiv teilgenommen.

Dabei konnten wertvolle Erkenntnisse für eine künftig verbesserte Unterstützung der Luftstreitkräfte im Einsatzfall gewonnen werden. Diese fließen in regelmäßige und anlassbezogene Cyber-Lagebilder ein, welche somit künftig gezielt für den Bedarf der Luftstreitkräfte aufbereitet werden können.

„AIRPOWER22“

AIRPOWER22 STEIERMARK

Im Rahmen der Großveranstaltung AIRPOWER22 hat das MilCyZ heuer erstmalig mit 1 Person und einem Gesamtaufwand von 4 Personentagen, zzgl. Mehrdienstleistungen, aktiv teilgenommen. Dabei wurde im Einsatzstab mitgearbeitet, um für etwaige Cyber-Angriffe rasch vor Ort sein zu können und umgehend geeignete Gegenmaßnahmen koordinieren zu können. So gäbe es starke Auswirkungen auf die Veranstaltung, wenn etwa lokale Systeme (Videowalls, Lautsprecheranlagen) gehackt werden würden und dadurch etwa eine Massenpanik ausgelöst werden würde. Noch schlimmer, sollten aufgrund von Cyber-Angriffen etwa die lokalen Luftraum-Überwachungs- oder Flugfunk-Systeme ausfallen. Dann wäre das Leib und Leben der Piloten oder des Publikums gefährdet, könnten die Flugmanöver oder der gesamte Flugbetrieb nicht mehr koordiniert werden.

Darüber hinaus war das Ziel, analog zu den LRSiOps DAEDALUS und anlässlich des G7-Gipfels Elmau, Details zu den Abläufen und Bedarfen der Stabselemente und durchführender OEt/Personen zu erheben, um auch hier den Bedarf für künftige AIRPOWER Veranstaltungen, aber auch vergleichbarer Einsätze, im Bereich Lagebild-relevanter Informationen aus dem Cyber-Raum durch das MilCyZ gezielt bereitstellen zu können.

Cyber Übung “Cracking the Shell”

Durch eine internationale Partnerschaft mit Estland, haben die Cyber-Spezialisten auch außergewöhnliche Trainingsmöglichkeiten. So wurde von 19. bis 23. September 2022 mit 8 Personen und rund 40 Personentagen intensiv geübt. Dabei wurde von den Trainern vermittelt, was für Möglichkeiten Angreifer in modernen IKT-Systemen zur Verfügung stehen, und welche Angriffstechniken sie einsetzen. Dies erlaubt es den Experten des MilCyZ beide Seiten kennenzulernen, und so die Systeme bestmöglich abzusichern.

Einerseits übt das BMLV-eigene „Red Team“ (IKT-Sicherheitsauditoren und Penetrationstester), wie sich ein Angreifer durch das Netz bewegen kann. Dadurch wird es möglich vergleichbare Vorgehensweisen zu testen, und so auch komplexe Angriffsvektoren identifizieren zu können. Schließlich ist es erst nach der Erkenntnis über Lücken in den eigenen Systemen möglich, diese einer Lösung zuzuführen und somit bestmöglich abzusichern. Dann nämlich können diese erkannten Schwachstellen von echten Angreifern nicht mehr ausgenützt werden.

Andererseits erhält auch das „Blue Team“ (jene Personen, welche Cyber-Sicherheits- und Erkennungssysteme des BMLV/ÖBH aufbauen und tagtäglich nützen bzw. verbessern) Einblick in die Arbeitsweisen von Angreifern. Somit können sie in der Prävention, durch Entwicklung und Aufbau geeigneter Sicherheitssysteme viele Angriffstechniken bereits in der Designphase berücksichtigen, und so von vornherein Gegenmaßnahmen ergreifen. Darüber hinaus ist die Erkennung und die Reaktion auf erkannte Angriffe oder Angriffsversuche gezielter möglich, da die von Angreifern gewählten Angriffstechniken auch den Verteidigern bereits bekannt sind. Somit können rasch gezielte Maßnahmen ergriffen werden, um Angreifer bereits in einer frühen Phase zu bekämpfen.

Dies gilt freilich für den Fall, dass sie es über die hohen Schutzmaßnahmen des BMLV/ÖBH schaffen. Meist scheitern Angriffe bereits in einer frühen Phase.

EloKa Übung „THOR’S HAMMER 2022“ in SWE

Im zweiten Quartal 2022 nahm das Unterstützungszentrum Elektronische Kampfführung (UZEloKa) im Rahmen des österreichischen Kontingents mit zwei Vertretern bei der EXERCISE THOR'S HAMMER 2022 (TH22) in SCHWEDEN teil. Ein wesentliches Ziel war die Überprüfung der Countering Radio Controlled Improvised Explosive Devices Electronic Warfare (CREW) -Systeme gegen aktuelle internationale Radio Controlled Improvised Explosive Devices (RCIED) - Bedrohungen.

Die Abteilung UZEloKa war im Schwergewicht auf einer multinationalen Teststrecke, welche durch die Beteiligung von Technikern und EloKa-Fachpersonal aus DEUTSCHLAND, den NIEDERLANDEN und ÖSTERREICH betrieben wurde, eingesetzt. Es konnten wieder wertvolle Erkenntnisse für das österreichische System gewonnen werden, die der Verbesserung der Wirkung und Funktion dienen. Zusätzlich konnte bei dieser Übung, gemeinsam mit den Instandsetzungselementen des CREW-Systems, erfolgreich bei der Entwicklung von Testroutinen für CREW-Systemen mitgearbeitet werden.

Im Gesamten dienen all diese Anstrengungen dem Schutz unserer Soldaten gegen RCIEDs im Einsatzraum.

Am internationalen Besuchertag konnte sich eine Abordnung der Direktion IKT&Cyber, mit Vertretern von Kommando, IKT Cyber Einsatz und UZEloKa, über die nationale und internationale Leistungsfähigkeit von Systemen gegen RCIEDs machen. Es war ein konkretes Beispiel, wie wichtig die aktiv gelebte internationale Kooperation in diesem speziellen Bereich der EloKa ist.

Luft-Boden Übung „Adriatic Strike 2022“ in SLO

Ebenfalls im zweiten Quartal 2022 nahm das UZEloKa mit einem Vertreter an der EXERCISE ADRIATIC STRIKE 2022 in SLOWENIEN teil. Es wurde die Funktion eines EloKa-Trainers ausgeübt, bei dem die Expertise als EloKa-Fachpersonal sowie als Stabsoffizier wesentliche Erfordernisse waren. Die internationale Übung hatte, unter Beteiligung einer Vielzahl von Partnerstaaten und der Einbindung von unterschiedlichsten Luftfahrzeugen, wie Kampfflugzeugen, Hubschraubern und unbemannten Luftfahrzeugen (UAVs), zum Ziel ein realistisches und komplexes Joint Terminal Attack Controller (JTAC)-Training zur Luftnahunterstützung zu ermöglichen. Bei den Luftstreitkräften kommen seit vielen Jahren eine Vielzahl von EloKa-Systemen zum Einsatz.

Das bereits wiederholte Einbringen der Fachexpertise bei dieser sich wiederholenden Übung zeigt den hohen Ausbildungsstand des Spezialisten des UZEloKa. Es kann genau durch diese Art multinationaler Kooperation der Erfahrungsausbau für künftige Einsätze weiterbetrieben werden.

EDA Projekt MICNET

Um die EU-weite Zusammenarbeit im Bereich der Cyber-Sicherheit zu verbessern wurde durch das EDA-Projekt MICNET der Grundstein für ein gemeinsames Cyber-Vorfallsmanagement gelegt. Das Projekt soll es den milCERTs der EDA-Mitgliedstaaten ermöglichen Informationen, Angriffsinformationen sicher mit den Verbündeten auszutauschen, um eine wirksamere Cyber-Verteidigung und die Verbesserung der Resilienz in allen Mitgliedstaaten zu erhöhen.

Mulitnationale Cyber Verteidigungsübung „Locked Shields 22“ (LS22)

Die multinationale Übung "Locked Shields" ist die seit 2012 jährlich stattfindende weltweit größte Live-Fire Cyber-Defence-Übung der Welt und ist für das MilCyZ die wichtigste Übung im Jahr. Über 2000 Cyber-Experten üben dabei „im militärischen Drill“ die Abwehr von Cyber-Angriffen in einer simulierten hochkomplexen Netzwerkumgebung.

Locked-Shields-Organisatoren vor dem simulierten Stromnetz von „Berylia“; Quelle: https://www.bundesheer.at/cms/artikel.php?ID=11341

Hier werden zwei Wochen lang die Fähigkeiten nationaler, ziviler und militärischer IT-Systeme zum Schutz lebenswichtiger Dienste und kritischer Infrastrukturen getestet. Dies wird erreicht, indem eine Reihe realistischer, groß angelegter Cyberangriffe simuliert wird.

„Red vs. Blue“

Die "Locked Shields" ist eine Übung von Red Teams (Angreifer) gegen Blue Teams (Verteidiger), wobei der Fokus auf den Blue Teams liegt. 2022 traten 24 Teams bestehend aus über 2.000 Teilnehmern aus 32 Nationen an. Rund 5500 virtualisierte Systeme waren dabei mehr als 8.000 Cyber-Angriffen ausgesetzt.

Szenario

Dem Szenario zufolge verschlechterte sich die Sicherheitslage in dem fiktiven Inselstaat Berylia im nördlichen Atlantik aufgrund einer Reihe koordinierter

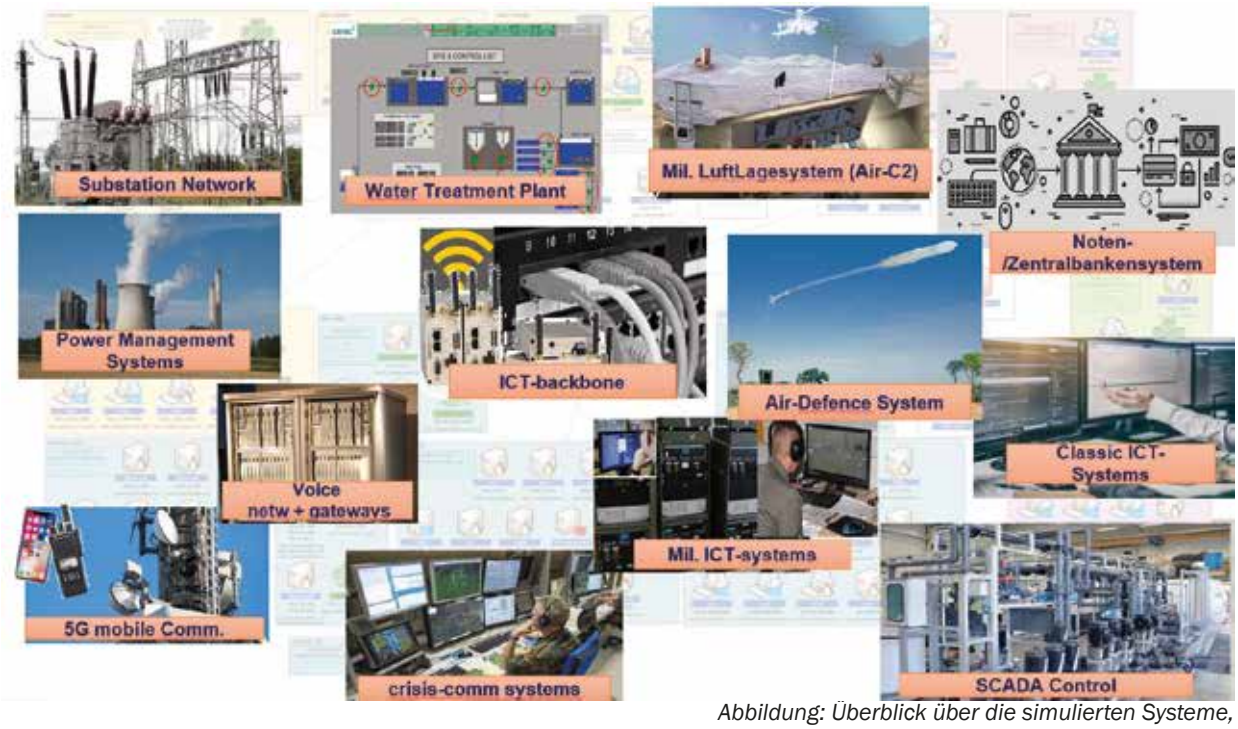


Abbildung: Überblick über die simulierten Systeme, welches es im Rahmen LS22 zu verteidigen galt. Quelle: Eigene / CCDCOE

Cyber-Angriffe auf dortige militärische und zivile IT-Systeme, letztere aus dem Bereich kritischer Infrastruktur. Diese Angriffe führten zu schwerwiegenden Störungen des Betriebs von Regierungs- und Militärnetzen, der Kommunikation, der Wasseraufbereitungssysteme sowie des Stromnetzes und schließlich zu öffentlichen Unruhen und Protesten. Zum ersten Mal beinhaltete die Übung die Simulation des Reservemanagements und der Finanznachrichtensysteme einer Zentralbank.

Das Besondere an der Übungsserie „Locked Shields“: Die Soldatinnen und Soldaten wurden mit "Live Fire" konfrontiert. Das bedeutet, dass die Teilnehmenden in Echtzeit Cyber-Angriffe erkennen und abwehren mussten.

Locked Shields-Mitarbeiter des Organisationsteams in einer der wenigen ruhigen Minuten. Quelle: https://www.bundesheer.at/cms/artikel.php?ID=1134.

Hinzu kommt „militärischer Drill“, indem der Druck extrem hoch ist, um ein sehr hohes Stressniveau zu erzeugen und die Verteidiger damit für den Ernstfall vorzubereiten. In der „heißen“ Phase der Übung, welche lediglich zwei Tage umfasst, passieren Angriffe, welche sonst üblicherweise über Monate hinweg realistisch sind.

Das Österreichische Bundesheer war bei der Übung durch das Militärische Cyberzentrum in einem multinationalen Joint-Team gemeinsam mit Deutschland vertreten. Die Herausforderung bestand darin, dass die Akteure in beiden Ländern stationiert und durch Videokonferenzen und Chat geführt werden mussten.

Eine gemeinsame Teilnahme von einem Standort aus wurde, u.a. aufgrund der COVID-Situation, vermieden. Andernfalls hätte es passieren können, dass eine Vielzahl der Cyber-Experten beider Länder zeitgleich ausfallen.

Veranstalter und Ergebnis

Geleitet und ausgerichtet wurde die Übung vom NATO "Cooperative Cyber Defense Center of Excellence" mit Sitz in Tallinn, Estland.

Gewonnen hat das Team aus Finnland, das österreichisch-deutsche Team konnte sich unter den Top 10 platzieren.

IKT-Betrieb

Im Ressort laufen Projekte zur Steigerung des Autarkiegrades, um die Auftragserfüllung auch in einer Krisensituation zu gewährleisten. Die Frage „Stell dir vor es geht das Licht aus. Sag was würdest du dann tun?“ aus dem Film „Hallo Dienstmann“ im Jahr 1952 - obwohl diese Frage damals in einem anderen Zusammenhang gestellt wurde - eröffnet sich gegenwärtig in einem anderen Kontext ganz neu und erfordert umfangreiche Beurteilungen und Bearbeitungen für die Aufrechterhaltung des Betriebes der IKT-Services durch alle Bereiche und Abteilungen der Direktion IKT&Cyber. Im Bereich IKT-Betrieb (IKTBetr) wurde mit der Ausarbeitung von Varianten zur Erhöhung der Autarkie für die Anbindung der Liegenschaften begonnen und im nächsten Jahr fortgesetzt.

Im Jahr 2022 wurden nach pandemiebedingter Einschränkung in den vergangenen Jahren wieder mehr Übungen durch die Truppe mit IKT-Einbindung durchgeführt. Schwerpunkte für den IKT-Servicebetrieb setzten im Jahr 2022 wieder die Luftraumsicherungsoperation DAEDALUS22 und die AIRPOWER22.

Impression von der AIRPOWER22

Bei anderen Vorhaben wie der Einführung des Tactical Communication Network (TCN) und dem Telekommunikationsverbund (TKV) als Ersatz für bestehende Systeme wird entweder die Auslieferung an die Truppe (TCN) vorbereitet oder an der Installation und Inbetriebnahme von Pilotstandorten (TKV) gearbeitet.

Dabei sind nicht nur technische Herausforderungen zu bewältigen, sondern auch etliche Abläufe und Aufgaben neu zu identifizieren, abzustimmen und festzulegen.

Zukünftig stellt das TCN einen Teil der Basisinfrastruktur für das IKT-System Einsatz (IKTSysE) dar. Aktuell wird an der Systemarchitektur IKTSysE und an der Organisation der Betriebsprozesse gearbeitet. Ausgestattet u.a. mit verlegbaren und ortsfesten Rechenzentren und Servern für unterschiedliche Einsatzszenarien soll das IKTSysE grundsätzlich durch die Truppe autark betreibbar sein. So ein komplexes System erfordert neue Rollenbilder bei der Truppe und in den Bereichen der Direktion IKT&Cyber, um IKT-Services mit den zugehörigen Betriebsprozessen für den eigenen Bedarf und die Zusammenarbeit mit internationalen militärischen Partnern zu betreiben.

Der TKV als Ersatz für den Nebenstellenverbund Österreich (NVÖ) wird im ortsfesten Bereich auch betrieblich neue Funktionalitäten zur Verfügung stellen. Mit den Contact Center- und der Unified Communication Services eröffnen sich für Anwender, Bediensteten im IKT-Support und in der Telefonvermittlung völlig neue Möglichkeiten. Anwender werden über eine ihnen zugeordnete Rufnummer an Ort ihrer jeweiligen Dienstverrichtung erreichbar sein, es können spezielle Support-Teams unabhängig vom jeweiligen Dienstort, gebildet werden und ähnliches wird für die im Rahmen der Krisenkommunikation eingesetzten Bediensteten möglich werden.

Auch im Bereich der ortsfesten und mobilen Kommunikation hat sich im Jahr 2022 einiges getan - mehr dazu auf den folgenden Seiten.

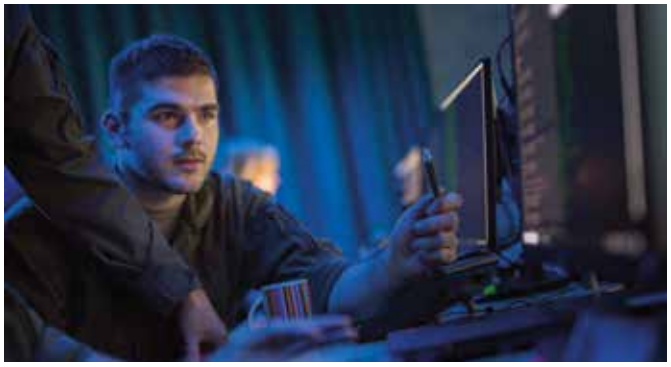
IKT-Unterstützung für Übungen, Einsätze, Kongresse und Symposien

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

Die Abteilung Betriebsführung koordiniert, steuert und überwacht bei Übungen und Einsätzen des ÖBH die

Einbindung der verlegbaren IKT-Truppensysteme in betrieblichen Belangen und stellt nach der Einbindung die Nutzung der IKT-Services für selbige sicher.

Zur Steuerung und Überwachung des ofFMSysÖBH wird in der Abteilung Betriebsführung das funktionale Element der Systemsteuerung gebildet.



Die Systemsteuerung setzt sich aus den für die jeweiligen Teilsysteme des ofFMSysÖBH zuständigen Systemingenieure (SysIng), sowie aus den für den operationellen Betrieb verantwortlichen Funktionen in der Betriebsführungs- und –überwachungszentrale (BÜZ) zusammen. Die BÜZ ist georedundant an 2 Standorten ausgeführt. Bei Bedarf werden zusätzlich weitere Kräfte aus den anderen technischen Bereichen der Direktion IKT&Cyber in die Systemsteuerung eingebunden, um auch bei komplexen Störungen rasch eine Lösung zu erarbeiten.

Aufgrund der COVID-Lage fanden Anfang des Jahres 2022 keine Vorhaben statt. Auch das Weltwirtschaftsforum in DAVOS (WEF DAVOS) wurde nicht wie geplant im Jänner abgehalten, sondern in den Mai 2022 verschoben. Die Luftraumsicherungsoperation (LRSiOp) DAEDALUS22 im Rahmen des WEF DAVOS konnte am Ersatztermin erfolgreich im Raum VORARLBERG/TIROL durchgeführt werden und stellte auch für die Systemsteuerung wie auch die Jahre zuvor eine besondere Herausforderung dar. Bei solch bedeutenden Vorhaben wird von der Systemsteuerung zusätzlich benötigter Support von den technischen Bereichen der Direktion IKT&Cyber angefordert und auch eingesetzt.

Alle, kurzfristig während der LRSiOp DAEDALUS22 Bedarfe konnten im Rahmen der IKT-Unterstützung in enger Zusammenarbeit mit dem Bereich IKTTe in der Direktion IKT&Cyber bearbeitet werden. In dem einen oder anderen Fall wurden Steuerungsmaßnahmen zusammen mit der Netzsteuerung der Truppe Umgehungslösungen eingesetzt, um Einschränkungen bei der Verfügbarkeit von IKT-Services rasch und bedarfsgerecht wieder zu beheben. Dies war zuletzt deshalb möglich, weil bereits bei der Netzplanung erforderliche Redundanzen berücksichtigt wurden.

Auch für die bereits im Juni 2022 unweit der österreichischen Staatsgrenze stattfindende LRSiOp im Raum TIROL im Rahmen des G7-Gipfel in ELMAU/DEU wurde IKT-Unterstützung von der Systemsteuerung bereitgestellt.

Insgesamt im Jahr 2022 von der Systemsteuerung 35 Vorhaben im Rahmen der IKT-Unterstützung betreut. Die Zusammenarbeit der Systemsteuerung mit der Truppe wurde von beiden Seiten als sehr gut bezeichnet. Als SG konnten die bereits oben erwähnten Vorhaben „LRSiOp Daedalus 22“, LRSiOp G7“ sowie die Auslandsübungen der Streitkräfte und die „Airpower 22“ mit Erfolg unterstützt werden.

Im Rahmen der Leistungsschau am Nationalfeiertag wurden am Heldenplatz in WIEN erstmals von der FüUS Komponenten des Tactical Communication Networks (TCN) präsentiert. Für die Einbindung der verlegbaren Systeme am Heldenplatz wurde durch das IKT-Service des Heeres Logistikzentrums WIEN ein Truppenanschaltepunkt (TAP) durch Umbau eines nahegelegenen Truppenanschaltekastens errichtet. Die Steuerung und Überwachung des TAP erfolgte durch die Systemsteuerung.
Ziel und Zweck der Ausstattung der Truppe mit dem oben angeführten, neuen System TCN ist der Ersatz nach 30-jährigen Betrieb für

- Integrierte Fernmeldeinfrastruktur (IFMIN)
- Datennetzwerk verlegbar
- verlegbares Richtfunksystem (vlgbRiFuSys)
- verlegbares Local Area Network (vlgbLAN)

durch ein militärisches IP basierendes IKT-System mit inkludierten Services für die Übermittlung von Sprache und Daten.

Die Vermittlungseinheiten (VmiE) im TCN sind in unterschiedlicher Ausprägung entweder in Shelter, Wechselaufbauten bzw. in geschützten/ungeschützten Führungsfahrzeugen eingebaut oder können aber auch in Gefechtsstandzelten und Gebäuden aufgebaut werden.

TCN ist für den Einsatz im In- und Ausland vorgesehen, entweder mit Rückwärtsverbindung in das ofFM-SysÖBH oder im autarken Betrieb.

Die Vernetzung bis in die Führungsebene Einheit ermöglicht den Einsatz unterschiedlicher IKT-Services auch in dieser Ebene. Diese neuen Möglichkeiten erfordern künftig den Ausbau der Betriebsorganisation, um die neuen Herausforderungen auch hinsichtlich Service Management gerecht werden zu können.

Ein weiteres Schwergewicht in der Aufgabenerfüllung des Bereiches IKTBetr stellt die Leistungserbringung durch den Serviceschwerpunkt Internet (SSP INTERNET) bei verschiedenen Veranstaltungen durch Beistellung, Support und Betrieb von speziell für den Zweck konfigurierter IKT dar.

Je nach Bedarf werden bei Veranstaltungen wie der IKT-Sicherheitskonferenz, bei Konferenzen und Symposien mit nationalen und internationalen Teilnehmern in Österreich, in Kasernen zur Nutzung des Internet durch Rekruten, bei speziellen Ausbildungsvorhaben und Einsätzen WLAN-Router mit mehreren Access-Points eingesetzt, um lokal den Betrieb eines Netzwerkes mit Internet-Anbindung zur Verfügung zu stellen. Bei den größten Veranstaltungen wurden auf diese Weise gleichzeitig mehrere tausend Anwender in verschiedenen Netzen versorgt.

IKT-Sicherheitskonferenz 2022

Durch die Bediensteten im SSP INTERNET als Teil der Direktion IKT&Cyber wird im Tagesgeschäft der Anwender-Support für Internet-Services wie e-Mailing, Webmail, Browsing und verschlüsselte Sprachtelefonie - im letzten Fall auch für Anwender in anderen Ressorts - für jede Art von dienstlichem IKT-Endgerät erbracht. Aufgrund der querschnittlichen Thematik in diesem speziellen Themengebiet steht der SSP Internet nicht nur den Bediensteten im Ressort, sondern auch Anwendern in anderen Ressorts, wenn diese das IKT-Service verschlüsselte Mobiltelefonie nutzen, zur Verfügung.

Telekomminikationsverbund (TKV)

Durch die Einstellung des Hersteller-Supports für die Komponenten des „Nebenstellenverbundes-Österreich“ (NVÖ) wurden die Telefonanlagen im NVÖ ausschließlich durch ressorteigenes Personal gewartet und im Anlassfall mit Komponenten von Anlagen, die abgebaut wurden, instandgesetzt. Eine weitere Folge des herstellerseitigen End of Life bzw. End of Service für diese Produkte war, dass bei einer Organisationsänderung die Rufnummern der Nebenstellen entsprechend der neuen Struktur angepasst werden konnten.

Endgeräte im TKV

Nach mehrjähriger Vorbereitung, Ausschreibung, Zuschlag und Vertragsabschluss werden nunmehr alle bestehenden Anlagen ersetzt. Aufgrund des Ankaufes dieses modernen Systems können dem Anwender viele zusätzliche IKT-Services, zur Verfügung gestellt werden. Vor Zuschlag der Leistungen an den Bieter wurde das angebotene System im Rahmen eines Tests vor Zuschlag (TVZ) eingehend geprüft. Besonders intensiv wurden die Software und die neuen Endgeräte getestet. Die Spezialisten des Bereiches MilCyZ untersuchten das angebotene Gesamtsystem auf Sicherheitslücken, um wie geplant den Anwendern ein zertifiziertes IKT-System zur Verfügung zu stellen. Core-Funktionalitäten wie zentrale Vermittlung und Contact Center

Funktionalität inklusive IVR, Accounting sowie Reporting waren ebenfalls ein grundlegender Bestandteil des TVZ. Im Rahmen des TVZ waren alle technischen Bereiche der Direktion IKT&Cyber gefordert, da ein Zusammenwirken aller Services für eine erfolgreiche Überprüfung der geforderten Funktionalitäten erforderlich war. Der TVZ konnte mit Jänner 2022 abgeschlossen werden.

Die weiteren Monate im Jahr 2022 waren ausgefüllt mit Planungsarbeiten, der Ausarbeitung von Grundlagen und mit intensiver Zusammenarbeit der Techniker sowohl im Resort als auch mit den Technikern des Auftragnehmers, um eine zentrale Vorgabe umzusetzen - es soll sich für den Anwender so wenig wie möglich in den Bereichen Rufnummern, Wählsystematik, Nutzung der Teilnehmerfeatures etc. ändern, um von Beginn an eine hohe Akzeptanz zu erreichen. Für die erfolgreiche Abwicklung dieses sehr umfangreichen Projektes wurden Arbeitsgruppen für Netzwerktechnik, Software-Implementierung, Infrastruktur, Betriebskonzept, Endgeräte, Rollout sowie für Benutzerbetreuung und Ausbildung gebildet, deren Ergebnisse unter Führung der Projektleitung koordiniert zur Umsetzung gelangen.

Gegen Ende des Jahres 2022 konnten die ersten Pilotlokationen mit den neuen Anlagen und den neuen Endgeräten ausgestattet werden. Geplant ist mit den Pilotinstallationen bis zum Start des österreichweiten Rollouts im Jahr 2023 hinreichend Erfahrungen beim Betrieb und in der Nutzung zu sammeln und allfällige Fehler in der Konfiguration zu finden und zu beheben.

Aktuell wird noch an der sehr komplexen Aufgabe - Implementierung der Software für die Nutzung der Unified Communication (UC) Services in den Pilotstandorten - gearbeitet. Um die oa. Teilbereiche in zeitlicher Abstimmung mit der Implementierung des TKV durch eigenes Personal abdecken zu können bzw. in den eigenverantwortlichen Betrieb gehen zu können, wurden mehrere Workshops mit allen involvierten Dienststellen bzw. mit dem Auftragnehmer durchgeführt und ein Ausbildungsplan für Lehrpersonal, Techniker verschiedener Ebenen sowie für die Bediensteten in der Vermittlung entwickelt.

Im Themenbereich Ausbildung wurden für die unterschiedlichen Rollen/Personengruppen (Betriebspersonal, Techniker, Supportpersonal, etc.) inhaltlich zugeschnittene Ausbildungslehrgänge definiert. Abzustimmen war auch die zeitliche Abfolge bzw. Priorisierung, um während der Implementierung TKV das erforderliche Know-How beim Personal schon zur Verfügung zu haben. Am Anfang werden alle Ausbildungslehrgänge durch den Auftragnehmer durchgeführt, bis sich das ressorteigene Lehrpersonal an der Führungsunterstützungsschule (FüUS) das notwendige Wissen aneignen konnte, um als interne Ausbildungsstätte für die Bediensteten die entsprechenden Kurse abzuhalten.

Eine Neuerung und erhebliche Verbesserung in der internen, aber auch externen Kommunikation stellt die Skill-basierte Verwendung von Automatic Call Distribution (ACD) inklusive Interactive Voice Response (IVR) dar.

Hiermit wird dem Benutzer künftig die volle Contact Center (CC) Funktionalität zur Verfügung stehen. Dieses Paket an IKT-Services im TCN ermöglicht beispielsweise die Vorschaltung einer IVR (Interactive Voice Response) bzw. Skill basierendes Routing eines Anrufes, um zielgerichtet und rasch die Verbindung mit einer auf das konkrete Anliegen spezialisierten Mitarbeiterin bzw. Mitarbeiter - unabhängig von deren bzw. dessen Dienstort - herzustellen. Auch für die Krisenkommunikation des Ressorts (Betrieb eines Callcenters bei Großveranstaltungen bzw. bei außergewöhnlichen Vorkommnissen im Zuständigkeitsbereich des BMLV) soll in Zukunft die Komponente der Sprachsteuerung IVR (Interactive Voice Response) zum Einsatz kommen.

Um die dafür notwendigen Abläufe prozessgesteuert im TKV bereitzustellen, wurden die zugehörigen Stammdaten erhoben sowie zu den Prozessen passende Call Flows z.B. für die Vermittlung von Gesprächen, die Kontaktierung des IKT-Supports, für die Krisenkommunikation des Ressorts entwickelt und implementiert.

Die Verwendung von UC Clients und dem damit verbundenen One-Number-Concept wird dem Anwender neue Möglichkeiten bieten, z.B. wird der Anwender künftig selbst entscheiden, auf welchem Endgerät im TKV er unter seiner Teilnehmernummer erreichbar sein wird. Eine wesentliche Qualitätssteigerung im Bereich der ortsunabhängigen Erreichbarkeit der Bediensteten bei z.B. Telearbeit oder auf Dienstreise.

Die großen Herausforderungen im Rahmen der Realisierung und des Rollouts des TKV stellen die Konfiguration der Netzwerkinfrastruktur, die IKT-spezifischen Sicherheitseinstellung an den Schnittstellen zu anderen Systemen aber auch die schrittweise Umstellung der Telefonzentrale auf den TKV, im während der Umstellungsphase parallelen Betrieb zweier Systeme dar. Die Aufgabenstellung dabei ist, die Standorte, abhängig vom Fortschritt der Realisierung des TKV, entsprechend aufzuschalten bzw. das Personal rechtzeitig und zum richtigen Zeitpunkt zu schulen.

Innerhalb des Bereiches IKTBetr werden in den kommenden Monaten die Themen der Betriebsführung und die Absolvierung erforderlicher Schulungen durch das Betriebspersonal und -Vermittlungspersonal wesentlich sein, um erfolgreich den TKV zu betreiben.

Aus Sicht des Bereiches IKTBetr verläuft bisher die Implementierung TKV planmäßig. Die Zusammenarbeit mit allen involvierten Organisationseinheiten bzw. Bearbeiter gestaltet sich sehr effektiv und produktiv.

Mobile Kommunikation im Jahr 2022

Der Großteil der Telekommunikationsdienstleistungen im BMLV - national und international - wird durch Services von nationalen Providern bereitgestellt. Diese Dienstleistungen umfassen das Kommunikationsspektrum von mobiler Kommunikation, über internationale Datenverbindungen, bis hin zu Internetservices via Satellit.

Um zeitgemäße Kommunikationsmöglichkeiten effizient nutzen zu können, wurde ein Vorhaben durch die Abteilung IKTS eingeleitet, um die Anbindung der militärischen Liegenschaft künftig auf Basis „Lichtwellenleiter Technologie“ an einen zivilen Provider herzustellen. Alle angeführten Kommunikation- und Datenservices erfordern mittelfristig Bandbreiten bis zu Gigabit pro Sekunde. Die derzeitigen Kapazitäten bzw. die notwendige Anbindungsinfrastruktur in den Liegenschaften muss adaptiert bzw. von Grund auf geändert werden.

National werden Datennetze, abseits des ortfesten Richtverbindungsnetzes (ofRVN), auf Basis Ethernet-Services in unterschiedlichen Bandbreiten zu militärischen Liegenschaften betrieben. Diese „Point to Multipoint“ (PtMP) Dienstleistungen werden sowohl im sicheren militärisches Netz (SMN) als auch im Tactical Communication Network (TCN) zur Verbindung der IKT-Systeme und der Liegenschaften errichtet.

Im Vorhaben selektives WLAN für Rekruten (selWLAN Rekr) werden Internet-Services zur Nutzung mit privaten Endgeräten in militärischen Liegenschaften in Kombination mit WLAN in mehr als 70 Liegenschaften zur Verfügung gestellt. Um zukunftsweisend dynamisch Bandbreiten zur Verfügung zu stellen, wurden gemeinsam mit Abteilung IKTS Vertragsanpassungen ausgearbeitet und umgesetzt.

Im Rahmen der Übersiedelung der Bundeshandelsakademie für Führung und Sicherheit (BHAK), auf Grund der Generalsanierung der DAUN-Kaserne in Wiener NEUSTADT, wurde das Schülerwohnheim mit beigestellten LTE-Routern ausgestattet. Um dem IKT-spezifischen Schutz der Schüler und des Lehrpersonals zu verbessern wurde gemeinsam mit dem Vertragspartner eine Lösung ausgearbeitet und in der Folge mittels Regeln in den Firewalls für die LTE-Router umgesetzt. Zudem wurden die Komponenten einem internen und externen Audit unterzogen, um die geforderten Schutzziele zu überprüfen.

Neben den terrestrischen Services nehmen die Satelliten gestützten Kommunikationsmittel im Rahmen der militärischen Kommunikation für Sprach- und schmalbandige Datenservices einen hohen Stellenwert ein. Mit einem Provider wurde eine besondere Form der Sprachkommunikation mittels Push to Talk (PTT) realisiert. Dabei ist es möglich, weltweit kurze Gespräche via Satellit mit Teilnehmern in der Sprechgruppe wie mit einem herkömmlichen Funksprechgerät im verschlüsseltem Modus zu führen.

Für die mobile Sprachkommunikation im sicherheitspolizeilichen Assistenzeinsatz (SihPolAssE) und bei anderen Assistenzleistungen des Bundesheeres werden hauptsächlich BOS-Endgeräte verwendet, um auch die Kommunikation mit anderen Blaulicht- und Sicherheitsorganisationen zu gewährleisten. Der neue Mehrzweckhubschrauber „AW169“ wird, weil dieser auch im Rahmen von SihpolAssE eingesetzt wird, daher mit einem airborne BOS-Endgerät ausgestattet. Bei der Implementierung des airborne BOS-Endgerätes in die Kommunikationseinrichtungen des Hubschraubers und bei der Konfiguration des Bedienteils sind die luftfahrtspezifischen Vorgaben einzuhalten. Durch die Aufteilung dieses BOS-Endgerätes in eine Steuereinheit und eine „Transceiver“-Einheit müssen beide Komponenten mit einer speziellen Software parametriert werden, um einerseits die Luftfahrtspezifika einzuhalten und um andererseits dem speziellen Bedarf der Piloten gerecht zu werden.

verschiedene BOS-Endgeräte

Um während der AIRPOWER22 (AP22) den hohen Bedarf an mobilen Kommunikationsmiteln abzudecken, wurden mehr als 600 BOS-Endgerate und mehr als 200 Mobiltelefone eingesetzt. Im Bereich BOS wurden dafür auf den Geräten und im System 20 Sprechgruppen eingerichtet, um einen reibungslosen Funkverkehr mit allen Beteiligten ohne gegenseitige Blockaden aufgrund der intensiven Nutzung sicherzustellen.

Das Erheben des Bedarfs, die Festlegung der Sprechgruppen, die Konfiguration und der lokale Anwender-Support war eine riesige Herausforderung für alle beteiligten Bediensteten im Führungsgrundgebiet 6/AP22. Mit dem technischen und organisatorischen Know How der Bediensteten konnte in diesem Bereich ein wesentlicher Beitrag zum sicheren Ablauf der AP22 erbracht werden.

Institut für Militärisches Geowesen

Hochgebirgslandelehrgänge der Luftstreitkräfte (HGLLG)

Übergabe von Karten für HGLLG Sommer 2022

Im Referat Daten & Systeme des IMG gibt es seit Jahren zwei Fixpunkte im Sommer und im Winter – den Hochgebirgslandelehrgang der FIFIATS.

Aufgabe des IMG ist es dabei, die von vielen Stellen eingebrachten Landeerlaubnisse, Überflugseinschränkungen und Landeverbote zu einer analogen Karte zusammenzuführen und diese dann für alle Systeme in den LFz auch in digitaler Form zu konvertieren und bereit zu stellen.

Durch stetiges Einarbeiten von Feedback sowohl der Bedarfsträger, als auch durch die gute Kontaktpflege zu den Datendistributoren (z.B. Ämter der Landesregierungen, Nationalparkverwaltungen, Österreichische Bundesforste (ÖBF)) kommt es zu laufender Qualitätsverbesserung und somit Steigerung der Zufriedenheit unserer Bedarfsträger.

"Coalition Warrior Interoperability Exercise 2022" in POL (CWIX22)

CWIX-Teilnehmer des Bereichs GeoMetOc

Die CWIX ist eine jährlich stattfindende Übung der NATO mit dem Fokus auf Interoperabilität von Command and Controll Information Systems (C2IS) und findet im Joint Forces Training Center der NATO in BYDGOSZCZ statt.

An der Übung nehmen jährlich mehr als 1200 Personen aus rund 45 Nationen teil. Nach mehrjähriger Pause hat wieder ein Vertreter des IMG im Geo-Fachbereich der Übung teilgenommen. Hauptzweck ist hier das Üben des Austausches von Geoinformationen wie Karten, Satellitenbildern u.ä.

Ursprünglich sollte ein Militärgeograf lediglich als Analyst für diesen Bereich teilnehmen, auf Grund des Ausfalls eines Mitgliedes der französischen Delegation musste er jedoch die Leitung des gesamten Bereiches Geospatial, Meteorologie und Ozeanographie übernehmen.

Aufgrund der langjährigen Erfahrung des IMGs konnte diese Aufgabe zur vollsten Zufriedenheit aller Teilnehmer im Fachbereich, immerhin rund 40 Personen aus 15 Nationen, erfüllt werden.

„SURVEX 2022" mit mobilem Geo Element in CZE

Im März 2022 befand sich das mobile Geoelement (GeoOps) des IMG mit 4 Mitarbeitern auf Übung in Bechyne, CZE. Diese internationale Vermessungsübung findet unter der Schirmherrschaft der Multinational geospatial Support Group (MN GSG) statt. Vertreten sind sechs Nationen: AUT, CAN, CZE, DEU, ESP und LTU. Die Schwerpunkte der Übung liegen auf der Interoperabilität der Vermessungsteams, Austausch von Know-how und internationale Vernetzung.

Mobiles Geo Element bei der FüSim Ausbildung der 3. JgBrig (BSE) in WEITRA

Die 3. Jägerbrigade (Brigade Schnelle Kräfte (BSK)) übte Ende April 2022 mit ausländischen Armeen am Führungssimulator in Weitra. Diese Übung wird durch drei Mann des Mobilen Geoelements / IMG mittels Einsatz der VR- Brille und 3D- Modellierung unterstützt. Pionierkräfte beurteilten das Gelände für den Einsatz der Pionierbrücken zur Überschreitung der Kamp. Dabei wurde BORIS (Browser-based Orientation in Space) und milGeoVA (VirtualReality-Anwendung) vom Pionieroffizier der Brigade eingesetzt. Beides sind Technologien zur virtuellen 3D-Geländedarstellung und werden am IMG betrieben.

„Langen Nacht der Forschung“ an der TherMilAk in Wr. Neustadt

Am Freitag, dem 20. Mai 2022, ging die zehnte „Lange Nacht der Forschung“ in ganz Österreich über die Bühne. Die heimische Wissenschaftsgemeinde machte dabei live ihre Arbeit aus nächster Nähe erlebbar. Mit rund 2.500 Programmpunkten an 280 Standorten war die zehnte Ausgabe der "Langen Nacht der Forschung" die größte Veranstaltung zur Wissenschaftsvermittlung im gesamten deutschsprachigen Raum.

Erstmals mit dabei auch die Theresianische Militärakademie, die das IMG zur Teilnahme einlud.

An sieben Stationen wurden Einblicke in Forschungsprojekte des Bundesheeres und von Partnern ermöglicht. Gleich zwei davon wurden vom IMG erfolgreich betrieben:

- GIS mit BISS: Schutz von Personal vor Beeinträchtigung durch gefährliche Fauna und Flora in Einsatzräumen
- Visual Analytics im militärischen Georaum

Rund 400 Besucher kamen zwischen 17.00 und 23.00 Uhr in die „Burg“. Führungen, Workshops, Vorträge, Live-Präsentationen und bei Experimenten zum Zuschauen, Mitmachen und Staunen bot die Lange Nacht der Forschung in der Militärakademie für alle etwas: Für Wissenschaftsprofis und solche, die es werden wollen, für Abenteuerlustige und Neugierige, für Um-die-Ecke-Denker, für Tüftler, für kleine und große Entdecker und für alle, die es ganz genau wissen wollten.

Richtig ausgefüllte Forscherpässe konnten von Kindern und Jugendlichen gegen Experimentiersets eingetauscht werden. Erwachsene konnten mit einem richtig ausgefüllten Forscherpass an einer Verlosung exklusiver Preise teilnehmen.

Multinationalen LuSK Übung „FIRE BLADE 2022“ in HUN

Im Juni 2022 fand am Luftwaffenstützpunkt Pápa in Ungarn die dreiwöchige Übung FIRE BLADE 2022 statt. An der von der Europäischen Verteidigungsagentur (European Defence Agency – EDA) organisierten Übung nahmen rund 550 Soldaten aus fünf Nationen (Belgien, Österreich, Slowakei, Slowenien und Ungarn) mit 25 Luftfahrzeugen (20 Hubschrauber und fünf Flächenflugzeuge) teil. Die Planung und Durchführung der Übungsvorhaben wurde durch ein internationales Mentorenteam mit Helicopter Tactic-Instruktoren aus den Niederlanden, Österreich und Schweden unterstützt.

Das Hauptaugenmerk der mittlerweile 16. Übungsausgabe lag auf der Verbesserung der Interoperabilität auf taktischer Ebene. Dadurch sollten internationale Einsätze im Verbund besser vorbereitet und koordiniert werden können. Unter anderem wurden Szenarien wie Such- und Rettungseinsätze, Luftnahunterstützung, Konvoi-/Hubschrauberbegleitung, Aufklärung und Überwachung, medizinische Evakuierung und die Evakuierung von Verletzten trainiert.

Das österreichische Kontingent wurde bei der nationalen Missionsplanung durch einen Offizier des IMG unterstützt, der die österreichischen Piloten bei den jeweiligen Übungsplanungen mit gedruckten missionsspezifischen Papierkarten sowie mit digitalem Kartenmaterial und Geodaten für die jeweiligen Positions- und Navigationssysteme in den Cockpits zur praktischen Missionsdurchführung versorgte.

TherMilAk Übung „ERZBERG 2022“

Das IMG unterstützte mit zwei Mitarbeitern und zwei Milizoffizieren / Experten Mitte Juli 2022 das Vorhaben NIKE zur Fähigkeitsentwicklung des ÖBH im urbanen Raum mit Schwergewicht auf unterirdischer Infrastruktur.

Im Zuge dieser Unterstützungsleistung wurden Totalstation und Laserscanner zur Geodatenerfassung eingesetzt, um ein 3D-Modell für Einsatzplanung und Einsatzführung zu erstellen. Die Datenerfassung fand dafür am „Zentrum am Berg“, einem untertägigen Forschungszentrum der Montanuniversität Leoben am steierischen Erzberg, statt und lieferte ca. 1 Mrd. Laserpunkte (LAS-Format).

In der Nachbereitung werden diese Punkte u.a. ausgedünnt, in Dreiecksflächen umgebildet und als 3D-Objekt dem Bedarfsträger zur Verfügung gestellt.

AIRPOWER 2022

Im Zuge der AIRPOWER 22 unterstützte das mobile Geo-Element (mblGeoEt) des IMG mit unterschiedlichen Kartenprodukten den Veranstalter in der Planungs- und Durchführungsphase.

Dabei spannte sich der Bogen an Produkten von der kleinformatigen Schenkeleinsatzkarte über großmaßstäbige Bildkarten über den ganzen Veranstaltungsraum mit all seinen Infrastruktureinrichtungen bis hin zu topographischen Karten, die das gesamte Aichfeld und Räume darüber hinaus abdeckt; neben analoger Produkte, auch im System PHÖNIX/Lage verfügbar.

Neben den militärischen Nutzern aus dem Bereich der Luft- und Landstreitkräfte wurden Kartensätze u.a. an EKO/Cobra, BPK Murtal und den zuständigen Feuerwehreinheiten übergeben.

Während der Durchführungsphase konnte der Gefechtsstand des mbIGeoEt in den Räumlichkeiten der LuAufklSta/Aussenstelle LOXZ betrieben werden, wo sämtliche Manipulation der analogen Karten durchgeführt wurden. Etwaige Anpassungen der Kartenprodukte durch Lageänderung konnten abgestützt auf das DGMN vor Ort sichergestellt und mittels mobilem Plotter in Kleinstauflage sofort produziert werden.

Auch dieses Jahr war das IMG mit dem mbIGeoEt ein verlässlicher Partner der AIRPOWER.

„PROJEKT TIEFENRAUSCH“ AM OÖ. TRAUNSEE im September 2022

Der Klang der Erde - genau das war es, wonach sich das Kurier-Medienhaus in Kooperation mit Partnern, v.a. mit dem ÖBH, in einer der wohl aufwendigsten österreichischen TV-Produktionen des Jahres 2022 auf die Suche machte.
Mit dem LIVE-Projekt Tiefenrausch begaben sich Promis gemeinsam mit wissenschaftlichen Experten in einem U-Boot an den tiefsten Punkt des Traunsees, um Klänge hörbar zu machen, die noch niemand gehört hatte.

Das einzigartige Projekt wurde neben Pionieren aus MELK und Jagdkommando-Soldaten aus WR. NEUSTADT auch durch drei Mitarbeiter des IMG unterstützt: Bgdr Dr. TEICHMANN, Militärgeograph ObstdhmtD Mag. HEISSL und Militärgeologe HERDA, MSc waren einige Tage in EBENSEE und TRAUNKIRCHEN vor Ort um u.a. zwei zentrale Fragen zu beantworten:

- Wie sieht der Traunsee am Ostufer unter der Wasseroberfläche aus? Um diese Frage zu beantworten, tauchte der Militärgeologe des IMG mit dem U-Boot erstmals entlang des Abhanges Richtung Seegrund: Erkenntnis: Eine steile Felswand reicht von der Wasseroberfläche bis fast zum Seegrund. Lediglich am Grund befindet sich eine dünne Schlammschicht.

- Wie tief ist der Traunsee tatsächlich? Ein Militärgeograph des IMG verifizierte mit einem Tauchgang die tiefste Stelle und deren Lage im Traunsee: 191m. Festgestellt wurde dies mit den Bordinstrumenten des U-Bootes und einer Unterwasserdrohne. Grundlage des Vorhabens war das amtliche Kartenwerk des IMG und die Expertise des MilGeo-Fachdienstes.

Insgesamt ein gelungenes Projekt mit dem sich das ÖBH in einer einmaligen Kulisse großartig präsentieren konnte. Für das IMG brachte es einen unschätzbaren Wissensgewinn v.a. in den Bereichen Bathymetrie und Unterwasser-Geologie.

Der Promi-Ansturm war enorm und der nationale und lokale „Medienrummel“ dementsprechend.

Durchführung der Navigation Warfare Übung am Truppenübungsplatz Seetaler Alpe

Das Referat Navigation führte in der ersten Oktoberwoche 2022 eine Übung zu Navigation Warfare auf dem TÜPl SA durch.

Neben internen Dienststellen sowie nationalen Forschungspartnern wie Joanneum Research, Accurision oder TU Graz beteiligten sich auch internationale Gäste an der Übung. So durfte man verschiedene Dienststellen der Deutschen Bundeswehr sowie Teilnehmer des EU-SatCen und EDA in der Steiermark willkommen heißen. Ein großes Dankeschön gebührt der Fernmeldebehörde, die auf Amtshilfe an dieser Übung teilnahm und neben der Frequenzüberwachung auch fachliche Beitrage in den Diskursen beisteuerte.

zivile Partner unterstützen das IMG im Zuge von KIRAS und FORTE Forschungsprojekten beim technischen Aufbau der Fähigkeit. Abstimmungen sind für Kalibrierungen unerlässlich.

Organisatorisch wurde der gesamte Übungsablauf mit fixen Terminen geplant. So begann jeder praktische Übungstag mit einem Briefing, womit alle Teilnehmer über den geplanten Tagesablauf informiert wurden, und endete mit einem Debriefing, wo die Tageserfahrung, Verbesserungsvorschläge und etwaige weitere Sachverhalte diskutiert wurden. Im Anschluss daran fand täglich eine Teamleiterbesprechung statt um den nächsten Tag vorzuplanen und somit die durchzuführenden Tests zu fixieren.

Auch die GWD des IMG unterstützen die Messreihe und protokollieren eifrig die Auswirkungen auf Empfangsgeräte.

Im Zuge des praktischen Parts der Übung wurden verschiedene Spoofing und Jamming Tests mit unterschiedlichen Sendern und Empfängern durchgeführt. Diese wurden einerseits im Nahbereich, als auch im Fernbereich durchgeführt mit Wirkrichtung geschütztem Talkessel, sodass eine Störung außerhalb des Truppenübungsplatzes nicht möglich ist.

Übungsaufbau mit prüfendem Blick der Fernmeldebehörde um die ca. 1km entfernten Messfahrzeuge nicht zu intensiv zu bestrahlen.

Der theoretische Teil war geprägt von Fachdiskursen zu Forschungsprojekten und dem weiteren Entwicklungspfad dieser noch jungen Waffengattung Navigation Warfare.

Kameraden der DBw sind ebenso interessiert an unseren Aussendungen und verfolgen das Geschehen auf deren Monitoring- und Aufzeichnungsstationen.

Ein Übungserfolg konnte sowohl aus österreichischer Sicht, als auch aus internationaler Sicht verbucht werden.

13. HELICOPTER TACTICS SYMPOSIUM 2022

Vom 14. bis 16. November 2022 nahm das IMG am 13. Helicopter Tactics Symposium 2022 der EDA, national organisiert durch die österreichischen Luftstreitkräfte, in der SCHWARZENBERG-Kaserne teil.

Dabei stellte das IMG seine Kompetenz im Bereich der 3-dimensionalen Geländedarstellung in Form eines Informationsstandes mit Live-Demo nicht nur den internationalen Teilnehmern des Symposiums vor, sondern genauso Teilen der Luftstreitkräfte und der IKT&Cybereinsatz-Kräfte des Bundesheeres.

Es wurde sowohl das System BORIS (Browser-based Orientation in Space), wie auch die milGeoVA (eine Virtual Reality-Anwendung) anhand ausgewählter Szenarien vorgestellt und als Ausgangspunkt für intensive Fachgespräche genutzt.

Thematisch kreisten diese Gespräche um die Themen der Interoperabilität, serviceorientierte Architekturen, Anwendungsfelder und Abgrenzung einzelner Anwendungen.

Speziell im Austausch mit den internationalen Teilnehmern des Symposiums hat sich dem IMG die Möglichkeit geboten, seine Kompetenz und Fähigkeiten im 3D-Bereich im internationalen Nutzerkreis zu verorten.

Durchführung der 10. BWÜ der Milizexperten Direktion IKT&Cyber von 21.11.22 bis 25.11.22

Alle zwei Jahre üben die Experten „Direktion IKT&Cyber /Institut für Militärgeographie“ im Rahmen einer BWÜ. Ende November fand diese zum insgesamt 10. Mal statt. Die Experten des IMG sind über die Jahre zu einem eingespielten Team zusammengewachsen und stellen regelmäßig ihre Fähigkeiten und auch ihre Durchhaltefähigkeit unter Beweis.

Die Übungsleitung wurde erneut in bewährter Weise von ObstdhmtD i.R. Mag Gerald GNASER wahrgenommen. Dieser unterstrich die Wichtigkeit der Führungsgrundsätze des ÖBH.

Am Dienstag erfolgte das Scharfschießen am Schießplatz in Stammersdorf an der Pistole P80.

Am Mittwoch erfolgte die Verlegung zur TherMilAk, wo das NIKE-UT-Projekt, an dem das IMG beteiligt ist, vorgestellt wurde.

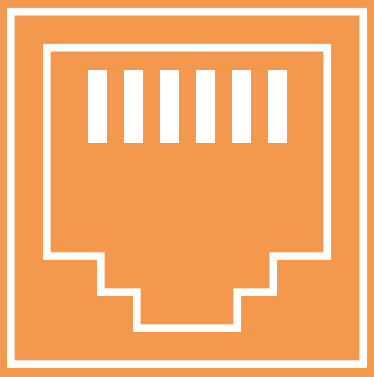
Am Nachmittag fanden Fachvorträge statt; so berichteten beispielsweise MA des IMG über ihre jeweiligen Erfahrungen im Ausland und Milizexperten des IMG über ihre Fachrichtungen und Forschungsergebnissen.

Am Donnerstagvormittag begrüßten Ltr IMG Mag. Dr. Teichmann, MSc MAS und stvLtr IMG Mag. Dr. Tamino EDER die MilGeo-Experten, am Nachmittag wurde gemeinsam eine Arbeitsplatzbeschreibung für einen Arbeitsplatz eines Militärgeologen ausgearbeitet.

Am Abend lud ObstdhmtD i.R. Mag. Gerald GNASER im Restaurant Musil zu einem Gemeinschaftsabend, wo Ehrungen und Auszeichnungen stattfanden.

Am Freitag, dem letzten Tag, wurde ObstdhmtD i.R. Mag. Gerald GNASER durch den Ltr Direktion IKT&Cyber GenMjr Ing. Mag. Hermann KAPONIG wegen seiner großartigen und ehrenhaften Leistungen gebührend gewürdigt und schließlich unter standing ovations aller Anwesenden verabschiedet.

Der Übungsleiter ObstdhmtD i.R. Mag. Gerald GNASER



ObstltdG Mag.(FH) Christoph JEZEK

Abteilung IKT&Cyber Bereitstellung

„Wir selbst erfinden gerade das Unternehmen und deren Abläufe neu, alles von Hybridität, Multi-Domain Warfare, Digitalisierung über Führungsgrundsätze bis hin zu neuen Geschäftsfeldern, Wertschöpfungsketten, Aufgaben und Verantwortlichkeiten wird diskutiert.“

Als Leiter des Referats der IKT und Cyber Bereitstellung darf ich auf ein herausforderndes Jahr 2022 zurückblicken. Nicht nur die zahlreichen Vorhaben, Projekte und täglichen Herausforderungen haben uns permanent vorangetrieben, sondern auch die neuen Strukturen und deren zu entwickelnden Prozesse. Dabei darf ich vorweg auf die nachfolgenden Seiten verweisen, in denen die einzelnen Aufträge, Aufgaben und Herausforderungen der Bereiche dargestellt sind, die im abgelaufenen Kalenderjahr mit viel Aufwand und Engagement entwickelt, betrieben und umgesetzt wurden.

Die Grundidee der IKT und Cyber Bereitstellung wurde insofern definiert, um eine interne, nach internationalen militärischen und zivilen IT- Standards ausgerichtete Planung und Koordinierung der Bereiche Applikationen, IKT-Technik, IKT-Betrieb, Militärisches-Cyber-Zentrum sowie dem Institut für militärisches Geowesen zu etablieren. Dabei ist eine der wesentlichen Aufgaben ein übergeordnetes Architekturmanagement im Rahmen der Digitalisierung für das IKT System des ÖBH zu entwerfen, zu implementieren und langfristig zu betreiben.

Das visionäre Ziel ist es, die aufgrund erforderlicher Erhaltungs- bzw. Weiterentwicklungsmaßnahmen getroffenen, Entscheidungen, Planungen, Beschaffungen oder Technologieentwicklungen immer ganzheitlich anhand deren Auswirkungen auf die militärische Einsatzführung und den militärischen Nutzen zu betrachten. Dazu soll neben einem modernen IT- Service Management auch ein effizientes Vorhabens- und Projektmanagement prozessual zur Ressourcensteuerung aufgebaut werden.

Die größte Herausforderung war aber, und diese nehmen wir auch in Teilen in das folgende Jahr mit, die langfristige Implementierung und Etablierung

der neu aufgestellten Bereitstellung als das zentrale Element in der Direktion IKT&Cyber. Wir selbst erfinden gerade das Unternehmen und deren Abläufe neu, alles von Hybridität, Multi- Domain Warfare, Digitalisierung über Führungsgrundsätze bis hin zu neuen Geschäftsfeldern, Wertschöpfungsketten, Aufgaben und Verantwortlichkeiten wird diskutiert. Im Bereich der IKT und Cyber Bereitstellung wird ebenfalls altes analysiert, bei Bedarf umgebaut oder gar neu aufgestellt. Aktuell gibt es hierfür kaum definierte Prozesse und viele Dinge passieren nach Gefühl. Wenn wir weiterwachsen und effizient bleiben wollen, kann das so nicht bleiben.

"Am Arbeitsplatz müssen wir den Usern ganz unideologisch die Werkzeuge bereitstellen“

Mit der organisatorischen Abbildung des Referates IKT und Cyber Bereitstellung innerhalb der Direktion IKT&Cyber wurde nunmehr jenes Element geschaffen, welches sich primär mit der Umsetzung der planerischen Vorgaben und der Implementierung beschaffter Systeme beschäftigt. Damit soll sichergestellt werden, dass einerseits sich die einzelnen Komponenten militärisch betrachtet in ein nutzbares, effizientes und für den Einsatz ausgerichtetes System integrieren und andererseits die notwendigen, betrieblichen Sicherheitsstandards systematisch eingehalten und weiterentwickelt werden.

Wesentlich für die Bereitstellung ist jedoch die service- und kundenorientierte Herangehensweise als der IKT-Provider für die Streitkräfte. Daher stehen für uns Service und Kundenorientierung im Vordergrund und definieren in allen unseren Handlungen die obersten Ziele. Die Bereitstellung als das zentrale Servicemanagement für die IKT im österreichischen Bundesheer hat sich daher das Ziel gesetzt, sich als ein zuverlässiger IT- Dienstleister zu positionieren und zu etablieren.

Dazu wollen wir adäquate, Schnittstellen- bezogene, normative Prozesse entwickeln und einführen. Weil das aber zumeist als bürokratisch, komplex oder zu modern für das System verschrien ist, müssen wir vorerst mit großen, zumeist persönlichen Widerständen rechnen. Daher ist auch unser Leitspruch, dem User jene Werkzeuge bereitzustellen, die er zur täglichen Aufgabenerfüllung im Frieden und Einsatz, im In- und Ausland benötigt.

Unser Ziel ist erst dann erreicht, wenn alle Mitarbeiter, Vorgesetzten und Nachgeordneten merken, dass uns die neuen Systeme und Prozesse wirklich voranbringen und die tägliche Arbeit effizienter gestaltet. Die von uns erdachte Vision zur Digitalisierung wird somit eine Herausforderung in der Implementierung, eine Herausforderung in der Umsetzung und eine Herausforderung in der Akzeptanz der Nutzer darstellen. Im Endeffekt gilt es aber, den Prozess im Team mit allen weiterzuentwickeln und damit Bedenken und Sorgen auszuräumen.

Schlussendlich ist aber auch die Ressourcensteuerung eine zentrale Herausforderung, derer wir uns im kommenden Jahr stellen werden müssen. Die Quantität und Vielfältigkeit der Aufgaben, sowie lange Ausbildungszeiten, einhergehend mit den technologischen Weiterentwicklungen und den immer größer werdenden Bedrohungen im IKT und Cyber Bereich zwingen uns auch die Ressourcen- und Personalfrage in Abhängigkeit der erfüllbaren Aufgaben zu betrachten.

Schwergewichtsbildungen und Priorisierungen von bestimmten Vorhaben und Aufträgen werden schlussendlich eine sichere, aber eingeschränkte Weiterentwicklung und Betrieb garantieren. Die vollumfängliche, funktionale, militärisch sichere, qualitativ entsprechende Umsetzung aller Vorhaben wird aber nur dann gelingen, wenn wir adäquates Personal rekrutieren, zielgerichtet aus- und weiterbilden können und vor allem langfristig im Bereich halten können.

Ich bin zuversichtlich, dass wir den Weg, den wir beschritten haben, im nächsten Jahr noch weiter festigen können. Denn erst durch unseren gemeinschaftlichen Weg wird es möglich sein, die Komplexität der Bereitstellung im Rahmen der Digitalisierung zu fassen und die neuen Aufgaben und unsere Vision derart zu kombinieren, dass daraus ein potenter Mehrwert für die Organisation entsteht.

Auch haben wir alle Werkzeuge, Verfahren und Prozesse etabliert, die uns diesen Weg ermöglichen werden. Ich freue mich daher gemeinsam mit meinen Mitarbeitern der IKTCyBstg und den Bereichen des vormaligen IKTCySihZ diesen steinig anmutenden Weg weiter fortzuschreiten.

Applikationen

Neben der Sicherstellung von Erhaltung und Betrieb der ca. 130 IT-Services für die der Bereich Applikationen technisch serviceverantwortlich ist, lag der Schwerpunkt im Jahr 2022 im Voranbringen der Digitalisierung, Autarkie von IKT-Services und den großen Vorhaben der Direktion IKT&Cyber (z.B. Digitalisierung Behördenverfahren, Tactical Communication Network TCN, Telekommunikationsverbund TKV, IKT-System Einsatz, etc.).

Einen großen Nutzen für alle Anwender bringen die durch Personalapplikationen bereitgestellte Standesliste, sowie der elektronische Antrag auf Erholungsurlaub, Zeitausgleich und Pflegefreistellung dar. Diese werden im nächsten Jahr durch die zentral bereitgestellte Zeitkarte ergänzt.

Auch 2022 erfolgte wieder die Unterstützung von Übungen und Einsätzen mit den erforderlichen IT-Services. Dabei ist vor allem die Interoperabilitätsübung CWIX hervorzuheben, die in Polen statt findet und an der nun erstmals auch aus dem AUT Battle Lab des Bereichs Applikationen in der STIFT Kaserne teilgenommen werden konnte.

Die individuelle Datenverarbeitung (Anwendungsentwicklung durch die Zentralstelle und Truppe) wird, nicht zuletzt aufgrund der Ablöse von MS-Office durch Libre-Office, unter Federführung des Bereichs Applikationen auf komplett neue Beine gestellt.

Die bereits 2021 im dynamisch gesicherten Militärnetz (DGMN) bereitgestellte Sicherheitszone miltärisches Gesundheitswesen wird laufend ausgebaut (z.B. Einbindung verschiedener medizinischer Geräte) und stellt nun die Grundlage für das neu umzusetzende Medizin-Informationssystem (MEDIS) dar.

Der Bereich Applikationen unterstützt die Fähigkeitsplanung und –evaluierung, im Zuge dessen wurde ein Prototyp eines Fähigkeitsevaluierungssystems umgesetzt. Dieser wurde gut angenommen und stellt die Basis für weitere Bearbeitungen dar.

24/7-Verfügbarkeit von PS-NT

Im Zuge der Autarkiebestrebungen des BMLV wurde die Anforderung gestellt, dass auch die einsatzwichtigen und unternehmenskritischen IKT-Services auf der zentrale EDV-Anlage des BMLV (ZEDVA, u.a. PS-NT, ORGIS, ZBS) zumindest 14 Tage lang rund um die Uhr bereitgestellt werden sollen.

Im Zuge der Systemerhaltung wurden die Betriebsabläufe (u.a. Batchverarbeitung, Inbetriebnahme) so angepasst, dass die IKT-Services der ZEDVA nun rund um die Uhr technisch verfügbar sind. Die Anwender können nun jederzeit die Personalapplikationen des BMLV nutzen.

PAAN-Zeitmanagement - Zeitkarte

Bedienstete des BMLV sollen eine digitale Zeitkarte bereitgestellt bekommen. In der ersten Ausbaustufe soll die Zeitkarte im SMN für Anwender mit eigener Chipkarte verfügbar sein.

KRONOS

Unter Nutzung der bereits vorhandenen Daten wird in moderner Web-Technologie dem berechtigten Bediensteten eine moderne Zeitkarte bereitgestellt.

Im Sinne der Digitalisierung sollen künftig Informationen nur noch einmal erfasst werden und in den jeweiligen IKT-Services automatisiert weiterverarbeitet werden (u.a. PERSIS, PAAN-Mehrdienstleistungsabrechnung, WEB-Standesliste). Die digitale Zeitkarte ist ab 12/2022 an ausgewählten Dienststellen im Probebetrieb und wird sukzessive weiter ausgerollt werden.

Die Integration und Erweiterung um notwendige Funktionalitäten erfolgt schrittweise analog dem PAAN-Antragswesen (u.a. Antrag auf Erholungsurlaub über die Ich-Rolle).

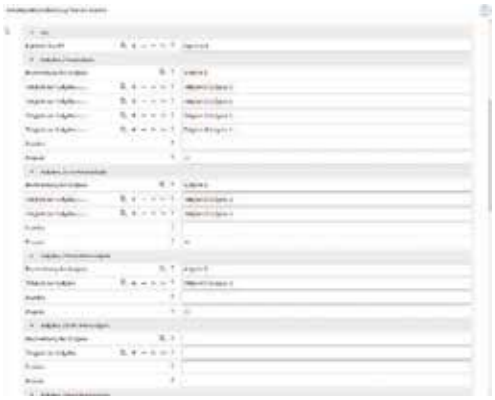
ZAMS – zentrales Ausbildungsmanagementsystem

Im Ausbildungsbereich werden aktuell unterschiedliche Insellösungen (u.a. KURSIS, LISy) verwendet. Eine zentrale Applikation zur Verwaltung und Steuerung im Ausbildungswesen ist aktuell im BMLV nicht vorhanden. Mit Erteilen des Projektauftrages für ZAMS soll die Ablöse von KURSIS und der erste Schritt in Richtung zeitgemäße IT-Unterstützung im Ausbildungsbereich gesetzt werden.

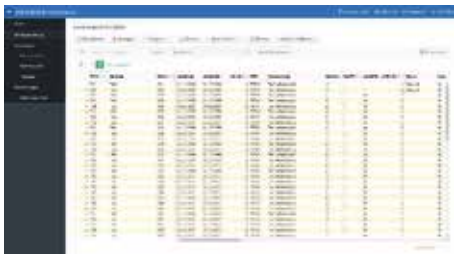
Im Jahr 2022 wurde ein Prototyp auf Basis der im eGovernment-Projekt ‚Digitalisierung der Behördenverfahren' verwendeten Technologie errichtet. Im 1. Quartal 2023 wird KURSIS durch eine zentrale WEB-Anwendung abgelöst werden.

Die Kursinformationen stehen dann BMLV-weit in einer zentralen Anwendung für alle berechtigten User immer aktuell zur Verfügung. LISy, das Lehrgangsinformationssystem der HLogS wurde durch das bestehende IKT-Service EPR – Eignungsprüfung abgelöst. Mittlerweile werden automatisiert die Ergebnisdaten zu Kursen vom IKT-Service EPR in das IKT-Service PERSIS (Personalinformationssystem des BMLV) eingebracht. Schrittweise werden weitere erforderliche Funktionalitäten ausgerollt.

Arbeitsplatzinformationssystem (APLIS)



Die Ablöse einer dezentralen, in Microsoft Access entwickelten IDV-Anwendung zur workflowgesteuerten Verwaltung von Arbeitsplatzbeschreibungsdokumenten mit der zusätzlichen Integration eines hierarchischen Berechtigungssystems und der Möglichkeit zum Archivieren der fertigen Arbeitsplatzdokumente in der Datenbank.

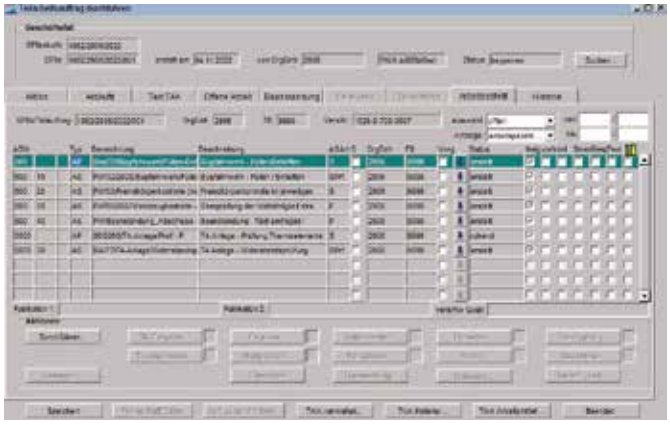


Nach einer umfangreichen Analyse der bestehenden Anwendung (beginnend Q3/2021) und Fertigstellung Detailspezifikation (Q4/2021) wurde am 25.04.2022 die erste APLIS Release 22.4 bereitgestellt. Bis zum Ende des Jahres 2022 wurden bereits weitere 5 Releases (aktuell 22.9) mit neuen Funktionen und Änderungen gem. weiterer Anforderungen der Fachabteilung bereitgestellt.

LOGIS-Materialerhaltung

Auf Grund der unterschiedlichsten Systeme die im ÖBH betrieben und daher auch einer Materialerhaltung unterzogen werden müssen, ist es eine Herausforderung einen einheitlichen Materialerhaltungsprozess zu etablieren.

2022 wurde hauptsächlich im Lz-Bereich vieles für einen einheitlichen und einfachen Ablauf der Materialerhaltungsprozesse investiert. So wurden Begriffe vereinheitlicht, Wertlisten vereinfacht und vor allem prozesssteuernde Eingaben so konzipiert, dass der Materialerhaltungsprozess für alle Systeme gleich ist.



Die Oberflächen wurden so umgestaltet, dass die gesamte Information übersichtlich dargestellt wird. Das betrifft vor allem die Durchführung Arbeitsauftrag /Teilauftrag bzw. Arbeitspakt/Arbeitsschritt. Die Feldvorbelegung wurde optimiert und beim Erstellen eines Arbeitsauftrages aus einem Wartungskatalog werden etwaige Dokumente mit in den Arbeitsauftrag übernommen.
Diese Maßnahmen erleichtern in Zukunft die Einführung neuer Systeme in LOGIS und vor allem in die Materialerhaltung wie z.B.: die neuen Hubschrauber LEONARDO AW169.

Interoperabilitätsübung CWIX am AUT CFBLNet

Federated Mission Networking

Die Interoperabilität des Bundesheeres im IKT-Bereich wird maßgeblich durch die Beteiligung am FMN (Federated Mission Networking) bestimmt. Im Zuge von Tests und multilateralen Übungen muss die Zusammenarbeitsfähigkeit der IKT-Services des Bundesheeres nachgewiesen bzw. geübt werden.

Mit dem neu errichteten AUT Battle Lab in der Stiftskaserne steht dem Bundesheer ein Testsystem mit Anschluss an das internationale Testnetzwerk CFBLNet (Combined Federated Battle Laboratories Network) zur Verfügung.

Im Juni 2022 wurde erstmals an der internationalen Großübung CWIX (Coalition Warrior Interoperability Exercise) mit einer "remote" Teststellung aus dem eigenen Battle Lab erfolgreich teilgenommen. Die AUT Delegation am NATO Joint Forces Training Center in Polen konnte damit deutlich verkleinert werden.

Neues Erfassungs- und Ortungssystem - Interministerieller Ortungsverbund AIRPOWER 22

Die Aufklärung im "elektromagnetischen Spektrum" (gemeint ist damit der Frequenzbereich unterhalb des langwelligen Infrarot) ist ein wesentliches Element der elektronischen Kampfführung (EloKa). Mit dem neuen Erfassungs- und Ortungssystem ERFOS steht dem Bundesheer ein modernes Sensorsystem zur Verfügung, das in das bestehende EloKa-Aufklärungssystem zu integrieren ist.

In Zusammenarbeit der Abteilung Einsatzapplikationen mit dem Führungsunterstützungsbataillon 2 wurde ERFOS kommunikations- und informationstechnologisch in den Interministeriellen Ortungsverbund IMOV eingebunden und bei AIRPOWER 22 erstmalig zum Einsatz gebracht. Im IMOV-Lagezentrum wurden die Sensordaten des BMLV, des BMI und der Fernmeldebehörde zusammengeführt, visualisiert und ausgewertet.

BMLV-ELAK 2022

Auch im Jahr 2022 wurde der BMLV-ELAK weiterentwickelt, es wurden Anwenderanforderungen umgesetzt und erforderliche Anpassungen aufgrund der sich laufend ändernden organisatorischen und technischen Rahmenbedingungen durchgeführt.

Konkret erfolgten 3 BMLV-ELAK Upgrades mit denen 420 Punkte umgesetzt wurden (u.a. parallele Bearbeitung von Dokumenten des Akts während des Einsichtsverkehrs, Mustereingangsstücke/-erledigungen, Start Libre-Office-Integration). Außerdem wurde 2022 eine BMLV-ELAK-Anwenderzufriedenheitsbefragung durchgeführt.

Ergebnis der Anwenderzufriedenheitsbefragung war, dass sich sämtliche abgefragten Kernfaktoren (Funktionsumfang, Design, Performance und Struktur) Vergleich zum Ergebnis 2018 verbessert haben.

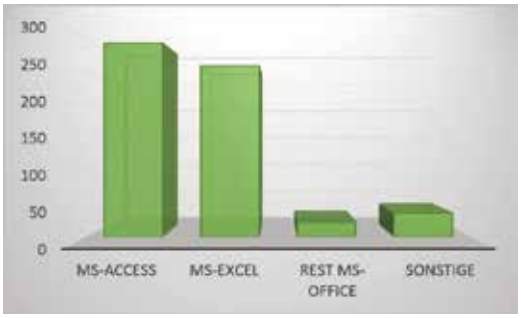
Bewertung Kernfaktoren in Schulnoten

Auch bezüglich der Benutzbarkeit (Usability) zeigt sich mit 84,1% positiven Rückmeldungen ein überdurchschnittlich guter Wert.

Die Durchführung der Anwenderzufriedenheitsbefragung 2022 wurde von den Benutzern sehr gut aufgenommen. Die rund 1.200 konstruktiven Kommentare werden im Rahmen des Change-Managements berücksichtigt.

Individuelle Datenverarbeitung (IDV) NEU

Unter individueller Datenverarbeitung (IDV) werden Anwendungen verstanden, die durch die Truppe und die Zentralstelle selbst entwickelt wurden. Basierend auf einer Erhebung im Frühjahr 2022 wurde festgestellt, dass der Großteil der IDV-Anwendungen in MS-Access und MS-Excel implementiert ist.



Code-Basis der IDV-Anwendungen

Aufgrund der geplanten Ablöse von MS-Office durch LibreOffice ist es unbedingt erforderlich, sämtliche in MS-Access oder MS-Excel entwickelten IDV-Anwendungen durch Alternativen abzulösen, die nicht auf MS-Access oder MS-Excel basieren.

Außerdem muss eine neue IDV-Entwicklungsumgebung bereitgestellt werden nachdem MS-Access für IDV-Entwicklungen nicht mehr zur Verfügung steht.

Die Ergebnisse der IDV-Erhebung wurden bewertet und analysiert. Es wurden die beiden neuen Projekte „IDV-Ablöse“ und „Software-Portfolio Truppe“ gestartet, mittels denen die Umsetzung der Ablöse der vorhandenen IDV-Anwendungen in MS-Excel/MS-Access durch bestehende, angepasste oder neue zentrale IT-Services erfolgen wird.

Betreffend die neue IDV-Entwicklungsumgebung erfolgte eine Evalierung von Low-Code/No-Code-Entwicklungsumgebungen am Markt. Ergebnis war, dass diese für den Anwendungsfall der IDV-Anwendungen im BMLV/ÖBH derzeit nicht geeignet sind. Daher wird seitens Direktion IKT&Cyber ein eigenes IDV-Entwicklungsservice bereitgestellt werden, das auf den Programmiersprachen Java und dem Angular Framework basieren wird.

In einer Reihe von Workshops wurde mit der Sichtung der vorhandenen IDV-Anwendungen und der Anforderungserhebung begonnen.

Für die effektive Zusammenarbeit wurde eine IDV-Entwickler-Community gegründet, die sich gerade in Aufstellung befindet. Um den mannigfaltigen organisatorischen und rechtlichen Herausforderungen zu begegnen, wurde mit der Konzeption und dem Design von Prozessen, Richtlinien und Regelungen begonnen.

IOT – LoRaWAN Smart Waste - eAWK

Das Internet of Things (IoT) ist aus unserem Leben nicht mehr wegzudenken und erfährt immer größere Verbreitung. Parallel dazu haben sich moderne, effiziente und kostengünstige Vernetzungs- und Übertragungsmöglichkeiten entwickelt und etabliert.
Long Range Wide Area Network (LoRaWAN) ist ein standardisiertes Funknetz, das die drahtlose Vernetzung von batteriebetriebenen Geräten verschiedenster Art (IoT-Geräte wie Gewichts- und Füllstandsensoren, Luftgütesensoren u.v.a.m.) ermöglicht. Die Daten dieser Geräte werden verschlüsselt und ressourcenschonend auch über weite Distanzen übertragen und zentral gesammelt.

Die Abteilung Bauwesen-Applikationen hat im Jahr 2021 das Projekt „Smart Waste“ initiiert. Die Messung der Abfallmasse und der Füllstände der Lebensmittelabfalltonnen und die Auswertung dieser Daten ermöglichen die Entwicklung und Setzung von Maßnahmen, um die Speiseabfälle laut EU-Vorgabe bis 2030 um 50% zu reduzieren.

Dieses Projekt hat sich im Jahr 2022 seiner „Serienreife“ genähert. Mit dem Pilotprojekt „Smart Waste+“ wurde der Horizont auf den Siedlungsabfall erweitert. Im eAWK werden die Ziele der Abfallwirtschaft für die einzelne Liegenschaft zur Umsetzung der Vorgaben des Green Deal und des Kreislaufwirtschaftspakets für die nächsten Jahre definiert.

Sicherheitszone militärisches Gesundheitswesen

Die im Jahr 2021 im DGMN geschaffene „Sicherheitszone Militärisches Gesundheitswesen“ (SihZo MilGesW) stellt eine auf die Anforderungen der Medizin ausgerichtete gemanagte zentrale Systemlandschaft zur Verfügung. Die Infrastruktur des DGMN bildet die Basis für diese in sich geschlossene Umgebung, für die es mittlerweile eine genehmigte Datenschutzfolgeabschätzung existiert. Die SihZo MilGesW erfüllt damit alle datenschutzrechtlichen Bestimmungen. Gesundheitsdaten sind besonders schutzwürdige Daten – auch diesem Umstand wird selbstverständlich Rechnung getragen.

Nach der Einbindung einiger medizinischer Systeme und Geräte – wie z.B. des Radiologie-Informationssystems (RIS) – haben wir begonnen, die Voraussetzungen für die Implementierung weiterer Gerätschaften („Modalitäten“) zu schaffen. Nach einem „Best of Breed-Ansatz“ (für jeden Bereich soll die jeweils „beste“ Lösung ausgewählt werden) wird ein IT-Service „Medizin-Informationssystem“ (MEDIS) entstehen. Dieses System ist ein Pendant zu zivilen Krankenhaus-Informationssystemen (KIS) und soll möglichst alle Anforderungen des militärischen Gesundheitswesens erfüllen. Dazu gehören der Patient (Stammdaten, Aufnahmedaten), der Fall (Anlassfall einer Untersuchung oder Behandlung) und der Befund (Ergebnis einer Untersuchung) sowie jeweils damit zusammenhängende Items (Diagnostik, Medikation, Operation, Pflege etc.).

Analyse und Visualisierung von Geschäftsdaten

Viele IT-Services dienen unter anderem dem Zweck, zu messen, zu wiegen, zu zählen oder Geld zu buchen und zu überweisen. Dabei entsteht eine große Menge an Daten.

Leistungen

Die Abteilung BauWAppl hat daher vor Jahren die bis dahin manuell durchgeführte zentrale Sammlung dieser Daten automatisiert. In weiterer Folge entstand die Forderung nach der Aufbereitung und Visualisierung der gesammelten Daten.

Digitalisierung in Betreuungseinrichtungen

Das ÖBH betreibt über 100 Betreuungseinrichtungen – entweder unter hoheitlicher oder unter privatrechtlicher Verwaltung. Sie alle führen ihre Gebarung auf individuelle Art und Weise: vom händisch geführten Kassabuch über Excel-Sheets bis zur selbstprogrammierten Access-Datenbank.

Leistungen

Die Abteilung BauWAppl hat aufgrund einer Anregung der Theresianischen Militärakademie (TherMilAk) Möglichkeiten gesucht, den Geschäftsbetrieb der Betreuungseinrichtungen zu modernisieren, zu vereinheitlichen sowie effizienter und damit wirtschaftlicher zu machen.

IKT-Technik

Im Bereich IKTTe wurde 2022 ein Wertesystem von den Führungskräften ausgearbeitet und im Rahmen einer Bereichsbesprechung unter Anwesenheit aller Mitarbeiter des Bereiches vorgestellt und eingeführt.

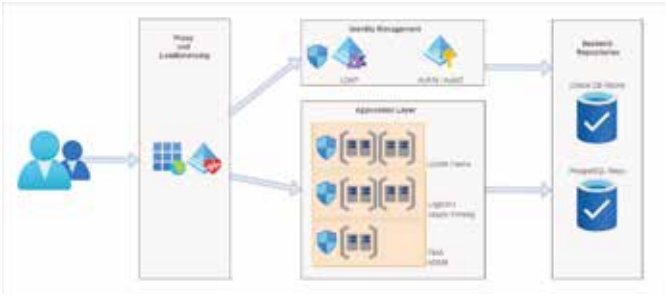
Die Eckpfeiler des Wertesystems sind Professionalität, Loyalität und respektvoller Umgang. Für Klarheit im Wertesystem sorgen die konkreten Beschreibungen der Eckpfeiler.

Mit Anfang Jänner 2022 wurde die neue Richtlinie zur Umsetzung der IT-Sonderverträge verlautbart. Ziel der Richtlinie ist die Modernisierung der Richtverwendungen in der IT (RIVIT) sowie die Steigerung der Attraktivität des Bundes als Arbeitgeber für IT-Spezialisten durch die Optimierung der Anstellungsverfahren und Anpassung des Gehaltsansätze für IKT-Spezialist. In Zusammenarbeit mit Vertreter der Abteilung Organisation in der Zentralstelle sowie externen Spezialisten wurde der bestehende Organisationsplan in das neue RIVIT-Schema übergeführt. Im nächsten Schritt erfolgt die Aufnahme der über externe Dienstleister beschäftigten Mitarbeiter sowie die Überleitung bestehender interessierter Mitabeiter:innen in das neue Schema.

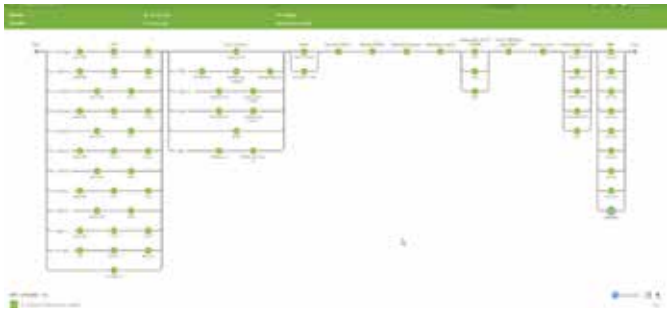
Im Rahmen der Weiterentwicklungen und Aktualisierungen wurde im Jahr 2022 besonders die Infrastruktur für das Logistische Informationssystem (LOGIS) durch das Referat Integrationssoftware komplett erneuert. Die dafür zu berücksichtigende Infrastruktur ist breit gefächert und umfasst Komponenten wie Applicationserver, Webserver, Loadbalancer, Server Firewalls und Cluster-Konfigurationen. Neben der Bereitstellung der Applikationen übernimmt diese Infrastruktur auch eine Vielzahl anderer Aufgaben. Diese reichen von der Authentifizierung von Anwendern, der Autorisierung für den Zugriff auf Produkte bis hin zur Lastverteilung von Services. Für die Umstellung auf das aktuelle Red Hat Enterprise Linux 8 (RHEL8) Betriebssystem wurden alle diese Server neu installiert, konfiguriert und aktualisiert!

Dabei wurden die Installation, die Konfiguration, die Überwachung sowie weitere laufend durchzuführende administrative Tätigkeiten schrittweise automatisiert und auch automatisiert getestet. Auch das Einspielen von Security Patches oder Änderungen zwecks Fehler-

behebung sind auf diesem Weg jetzt rascher möglich und können vor dem produktiven Rollout automatisiert getestet werden.



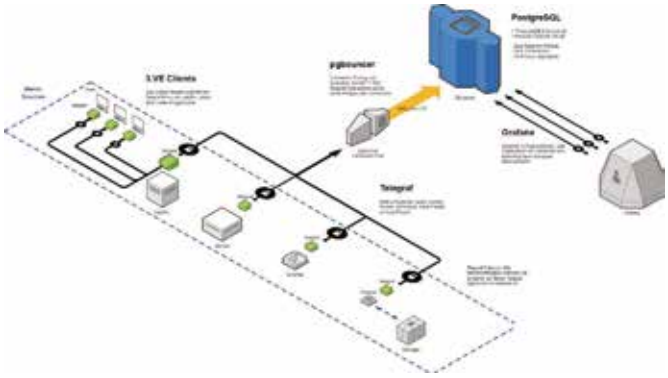
Aufgrund der hervorragenden Vorbereitung wurde für die Umstellung und Erweiterung der Funktionalität nur eine Downtime von insgesamt einer Stunde benötigt!



LOGIS CI Pipeline

Als weiterer Schwerpunkt des Jahres konnte die Abteilung technische Querschnittsaufgaben (TQA) die Infrastruktur für das IKT-Lagebild - Monitoring und Metrics Collection (METIS) - deutlich verbessern. Es werden Kennzahlen für die gesamte SMN Infrastruktur in einer noch nie dagewesenen Qualität und Quantität gesammelt, ausgewertet und auch dargestellt werden!

Die METIS Infrastruktur wurde 2022 im Backend vollständig von InfluxDB Timeseries Databases auf PostgreSQL + TimescaleDB Extension umgestellt. Die im Bild visualisierte Infrastruktur deckt nun alle SMN Windows Clients, SMN linux Kamino Server sowie andere inkludierte Systemkomponenten (Cisco Switches, ...) ab:



Aktuell werden in METIS Test u. Prod Umgebungen alle 15 Sekunden Rohdaten in die Datenbank geschrieben, um derzeit ca. 80 Kennzahlen zu errechnen. Die Erweiterung des Systems auf Services, Applikationen, etc. ist jederzeit möglich. METIS bietet eine breite Auswahl an vorgefertigten Telegraf Metriken, um Messwerte, Kennzahlen o.ä. zu erfassen, ggf. aufzubereiten und durch Grafana Dashboards sowohl Echtzeit als auch historische Daten zu visualisieren. In weiterer Folge ist geplant, eine „METIS-Appliance“ für das IKT-System Einsatz bereitzustellen, um der IKT-Truppe eine effiziente und effektive Möglichkeit zur Betriebsführung zu geben.

Im Bereich der Radartechnik war das Jahr 2022 geprägt durch den Abschluss des Vorhabens „Upgrade Long Range Radar (LRR) inkl. dem Deployable Air Defence Radar (DADR)“. Sämtliche Radarstationen sowie das verlegbare Radarsystem DADR sind technisch angepasst und teilweise umgebaut worden, um die international vorgeschriebenen technischen Anforderungen für den Betrieb des MODE 5 (Modus verschlüsselt – Sekundärradar) zu erfüllen.

Zur Detektion und Bedrohungsbewertung von militärischen Luftfahrzeugen im internationalen Luftraum innerhalb der Reichweite der Weitbereichsradarsensoren (ca. 450 km) müssen die Radargeräte mit einem Mode 5 Empfänger ausgestattet sein. Die Zertifizierung / Zulassung durch die entsprechende internationale Behörde wird 2023 starten und spätestens aber 2024 abgeschlossen werden.

Anfang 2022 wurde die Beschaffung eines Nachfolgesystems für das Aufklärungs- und Zielzuweisungsradar (AZR) inkl. der Zieldatenempfänger (ZDE) durch die Bildung einer Arbeitsgruppe gestartet. Es wurde auf Basis der Vorhabensabsicht begonnen eine technische Leistungsbeschreibung für die einzelnen Hauptkomponenten zu erstellen. Derzeit findet ein Request for Information (RfI) an interessierte industrielle Radarhersteller statt. Nach Einlangen der Antworten werden im Jänner 2023 die Herstellerfirmen für eine Firmenpräsentation eingeladen, um im Anschluss die Leistungsbeschreibung finalisieren zu können.

2022 wurde der „Test vor Zuschlag“ (TvZ) im Rahmen des Projektes Telekommunikationsverbund (TKV) durchgeführt. Im Zuge der Bearbeitungen wurden vom Audit-Team des Militärischen Cyber Zentrums (MilCyZ) Schwachstellen identifiziert. Sicherheitsoptimierungen wurden in Zusammenarbeit mit dem Hersteller unmittelbar umgesetzt. Das professionelle Vorgehen sowie die hohe Kompetenz der IKT-Spezialisten hat nicht nur innerhalb des Ressorts, sondern ganz besonders auch beim Anbieter und der internationalen Community großen Respekt und Anerkennung für die Direktion IKT&Cyber gebracht.

Im September wurde die Rechenzentrumskomponenten des Systems in Betrieb genommen und im Anschluss wurden drei Pilotstandorte ausgestattet und in Betrieb genommen. Im nächsten Schritt erfolgt die Zulassung des Systems sowie die Vorbereitung der Ausrollung der ersten Liegenschaften im Jahr 2023.

Die SW wurde einer Güteprüfung unterzogen und zur Auslieferung freigegeben. Die Beschaffung von neuen Soldatenfunkgeräten wurde abgeschlossen. Die erste Liefertranche wird im Juni 2023 erwartet. Das ÖBH hat 10 Stk eines der modernsten Truppenfunkgeräte, ein SW-defined-Radio, leihweise zur Verfügung. Diese hochmodernen Funkgeräte (TDR...Tactical Data Radio) wurden einerseits im Labor umfangreichen Tests unterzogen und andererseits im Feld getestet. Erprobungen und Tests werden 2023 fortgesetzt. Ziel ist es, ein TDR in das Tactical Communication Network (TCN) zu integrieren.

Eine hohe Auftragslage bei knappen Personalressourcen sowie Lieferengpässen der Hersteller stellen die Verantwortlichen für die LAN-Konsolidierung vor große Herausforderungen, da die Konsolidierung in den lokalen Netzwerken eine Voraussetzung für die Auslieferung des TKV-Systems darstellt.

Mitarbeiter der Abteilung Hardware und System Software (HW&SysSW) wurden mit der Einführung von LibreOffice beauftragt. LibreOffice ist ein leistungsstarkes Open Source Office-Paket, das ohne Aktivierung oder Cloudservices betrieben werden kann. Weltweit wird es von mehreren hundert Millionen Nutzern verwendet. Darunter sind Unternehmen, Behörden, Blaulichtorganisationen und auch Armeen. In Österreich wird LibreOffice u.a. seit Jahren erfolgreich im Justizministerium eingesetzt.

Außerhalb ist die freie Office-Suite z.B. in der Deutschen Verwaltung als Teil eines alternativen souveränen IT-Arbeitsplatzes vorgesehen.

Im SMN ist LibreOffice seit langer Zeit verfügbar. Viele Anwender haben es innerhalb von „Browser in the Box“ bereits unter Linux verwendet. Aktuell ist LibreOffice auf mehr als der Hälfte der SMN- PCs oder -Notebooks installiert. Im ÖBH-Paket befinden sich schon heute Mustervorlagen und viele für den Dienst hilfreiche Cliparts und Erweiterungen. Mit der SMN-weiten Einführung 2023 werden die ÖBH-spezifischen Ergänzungen fortgesetzt. Geplant ist eine Erweiterung u.a. um hochqualitatives Kartenmaterial des Instituts für Militärisches Geowesen (IMG) und neue dem Corporate Design entsprechende Vorlagen. Mittelfristig wird es mit LibreOffice innerhalb des SMN möglich werden, dass mehrere Personen gleichzeitig an einem Dokument arbeiten.

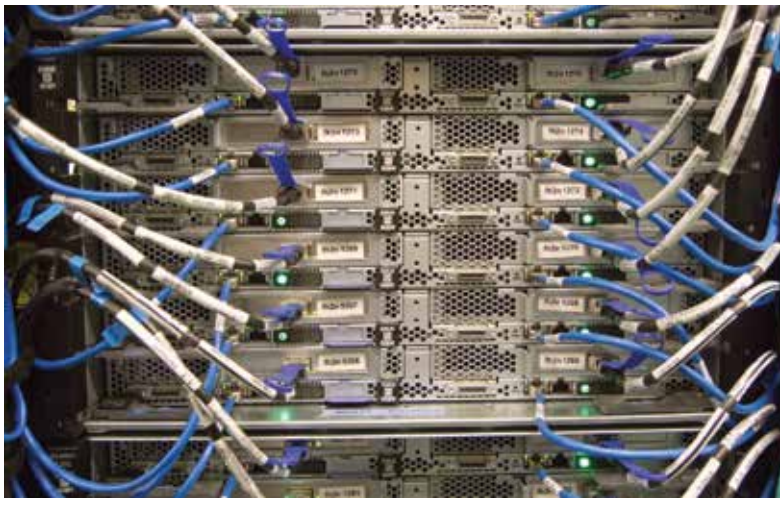
Beginnend mit 2023 wird auf die Verwendung von LibreOffice in den zentralen Applikationen umgestellt. Die Vorbereitung laufen auf Hochtouren! Einige LibreOffice Nutzer haben sicher schon die ersten Vorboten der Anpassungen entdeckt. Ende 2024 wird die Umstellung abgeschlossen werden. Microsoft Office 2016 wird zunächst parallel zu LibreOffice verfügbar bleiben. Neuere Microsoft Office Versionen werden zukünftig bedarfsorientiert für spezielle Formen der Zusammenarbeit mit externen Stellen bereitgestellt werden.

Anwendungsfall Dokumente & Präsentationen			Format/Werkzeug
ÖBH	→	Extern	Grundsätzlich PDF
ÖBH	↻	Extern	Gleiches Werkzeug nach Vereinbarung
ÖBH	←	Extern	PDF, OOXML, ODF, TXT, RTF,....

Zur Unterstützung der SMN - Anwender stehen seit Mitte 2022 die LibreOffice Website (https://cms.intra.bmlv.at/web/libre-office) mit Umstiegshilfen, Handbüchern und Links zu weiteren Informationen im WWW zur Verfügung. Die Benutzerbetreuung des IKTBetr hilft darüber hinaus wie gewohnt bei Fragen zum neuen Werkzeug weiter. Auch die Forenfunktionalität des neuen CMS wird zum Einsatz kommen.

Zur selbstständigen Wissensaneignung werden „Fasttrack“ Videos Anfang 2023 veröffentlicht. Diese Videos unterstützen bei der raschen Einarbeitung in LibreOffice und vermitteln Produktvorteile und effiziente Lösungswege für laufende Aufgabenstellungen.

Zur Vervollständigung des Unterstützungsangebots werden weiterhin Informationsschreiben erstellt und VTCs mit dem S6-Fachpersonal durchgeführt. Ersten Online-Befragungen zufolge schätzt das S6-Personal, dass etwa die Hälfte der Kollegen bereits über brauchbare LibreOffice Kenntnisse verfügen. Jenen Anwendern, die noch keinen Kontakt mit dem zukünftigen Office haben, gilt das Angebot LibreOffice vom Leitbediener am eigenen AP installieren zu lassen und spätestens im Februar 2023 nach der Veröffentlichung der Lernvideos mit der Vorbereitung für den rasch näherkommen Umstieg 2023 zu beginnen.



In den vergangenen Jahren wurden massive Anstrengungen zur erfolgreichen Einführungen von Virtualisierungstechnologien sowie der Einführung von Automatismen für die Bereitstellung von IKT-Technologien im Rechenzentrum unternommen. Zur gleichen Zeit wurde auch der alte Serverklon durch den neuen KAMINO-Serverklon abgelöst. Die Ziele dieser Ablöse waren klare Zuständigkeiten für instal-

lierte Services zu schaffen, die Nachvollziehbarkeit von Änderungen zu erhöhen, klare Releasezyklen vorzugeben und damit ein durchgehendes Lifecyclemanagement des KAMINO-Serverklon sicherzustellen.

Mit der dringend erforderlichen Erneuerung der Liegenschaftsserver-Infrastruktur wurde im Zuge der Vorbereitungen der Einsatz von Virtualisierungstechnologie auf Liegenschaftsservern mit höchster Priorität betrieben. Im Zuge des Vorhabens TCN (Tactical Communication Network) wurde es klar, dass für das TCN-Managementsystem (TCNM) zwingend Virtualisierung erforderlich war und daher vorab mit Priorität zu implementieren war. Im Rahmen von TCN und als Vorgriff zur Hardware-Erneuerung der Liegenschaftsserver konnte somit ein Proof of Concept in Bezug auf die Einführung von Virtualisierungstechnologie auf den Liegenschaftsservern erfolgreich umgesetzt werden.

Des Weiteren wurde das Konzept „Backup-to-Disk für Liegenschaftsserver“ umgesetzt. Hierbei handelt es sich um eine Funktionalität, bei der die Sicherungsdaten nicht auf Datenkassetten, sondern auf Festplatte geschrieben werden. Dies hat eine hohe Priorität für Liegenschaftsservern, da das Sichern und Zurückspielen von Daten mittels Datenkassetten und eigenem Bandlaufwerk fehleranfällig ist. Es wurde das Sicherungs- und Wiederherstellungskonzept für den Liegenschaftsserver NEU in Richtung „Backup-to-Disk“ überarbeitet. In Zukunft erfolgt eine Sicherung der Daten der Liegenschaftsserver auf eine zentrale Infrastruktur. Die Datensicherung erfolgt vollautomatisch zuerst lokal auf Festplatte am Liegenschaftsserver und wird danach vollautomatisch auf die zentrale Infrastruktur in der STIFT Kaserne repliziert. Dieser Schritt war notwendig da festgestellt wurde, dass mindestens 25 % der täglichen Bandsicherungen fehlerhaft oder nicht durchgeführt werden.

Für das Sichern und Wiederherstellen von Daten ist eine Netzwerkverbindung zur zentralen Infrastruktur in der STIFT Kaserne erforderlich. Die Verfügbarkeit des Netzwerkes ist österreichweit nahezu durchgehend gegeben. Fast alle Netzausfälle erfolgen geplant und sie werden als Wartungsaktivitäten entsprechend angekündigt. Die Wahrscheinlichkeit des Netzausfalls wird als wesentlich geringer als das Risiko eines Datenverlusts aufgrund einer mangelnden Datensicherung vor Ort beurteilt. Für den zwingenden Bedarf einer lokalen Sicherung werden entsprechende Datenträger zur Verfügung gestellt.

Damit diese Konzepte und Neuerungen umgesetzt werden können, sind nicht nur motivierte ausgewiesene Experten als Mitarbeiter und die entsprechende Zeit erforderlich, sondern auch eine neue Server-Hardware. Aufgrund COVID19 und den damit verbundenen weltweiten Lieferschwierigkeiten von IKT-Komponenten konnte das Ziel, die Ablöse der alten Liegenschaftsserver bis Ende 2022 abzuschließen, nicht erreicht werden. Die Lieferung der neuen Serverhardware wird mit Anfang 2023 erfolgen. Der Termin der Ablöse wird sich daher bis Ende 2023 strecken. Die Liegenschaftsserver werden in den Größen X-LARGE, LARGE, MEDIUM und SMALL beschafft.

Die Liegenschaftsserver X-LARGE und LARGE sind Rack-Server. Die Liegenschaftsserver MEDIUM und SMALL, welche den Großteil der Server ausmachen, sind normale Standmodelle. Bei der Beschaffung der neuen Liegenschaftsserver wurden auch die Erneuerung der unterbrechungsfreien Stromversorgungen (USV) und die Server-Racks für die Rack-Server berücksichtigt.

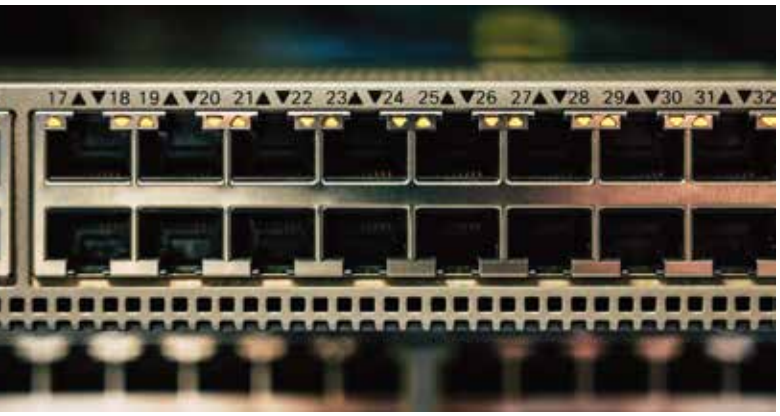
Die verbleibenden Herausforderungen für die neuen Liegenschaftsserver und dem neuen KAMINO Serverklon sind organisatorischer und weniger technischer Natur. Es sind die Installationsvoraussetzungen vor Ort sicherzustellen, die Abstimmungen für das RollOut durchzuführen, die Hardware-Zuweisungen logistisch vorzubereiten und die Umstellungen sowie Inbetriebnahmen zu koordinieren.

Durch die notwendig gewordene Ablöse der vorhandenen zentralen Bandrobotorsysteme in Verbindung mit der Erhöhung der Bandbreite im Netzwerk hat sich heuer die Möglichkeit eröffnet, eine asynchrone Datenspiegelung umzusetzen und somit die Auslagerungssicherung – Verbringung von Bänder an einen dritten Standort - abzulösen. Es wurde das Siche-

rungs- und Wiederherstellungskonzept für die Sicherung der Daten der zentral betriebenen Services mit der Funktionalität „Backup-to-Disk für die zentrale Infrastruktur“ dahingehend überarbeitet. Dadurch erfolgt im Rahmen der Erneuerung der vorhandenen zentralen Bandrobotorsysteme eine Erweiterung zu Backup/Recovery-Systeme bestehend aus Servern, Datenspeichersystemen Bandrobotorsystemen und einem Storage Area Network (SAN).

Mit den neuen Backup/Recovery-Systemen sind somit nicht nur kürzere Backup- und Recovery-Zeiten, sondern auch das asynchrone Spiegeln von Backupdaten über große Distanzen möglich. Für die Umsetzung der asynchronen Datenspiegelung wurden daher ein zusätzliches Backup/Recovery-System für einen dritten Standort mitbeschafft.

Auch hier gab es aufgrund COVID19 und den damit verbundenen weltweiten Lieferschwierigkeiten von IKT-Komponenten einen Lieferverzug. Dieser fiel aber weniger verzögernd aus, da es sich bei den Komponenten der Backup/Recovery-Systeme Großteils nicht um IKT-Massenware handelt. Die Inbetriebnahme und Abnahmetests sind im Laufen, danach erfolgt die Migration der Daten von den alten zentralen Bandrobotorsystemen auf die neuen Backup/Recovery-Systeme und nach Verfügbarkeit der erforderlichen Bandbreite die asynchrone Datenspiegelung auf einen dritten Standort.



Zusätzlich zur Überarbeitung der Sicherungs- und Wiederherstellungskonzepte und die Einführung der Funktionalität „Backup-to-Disk“ sowohl für dezentrale Server als auch für die zentrale Infrastruktur sind zumindest noch exemplarisch folgende Vorhaben zu erwähnen:

- die Beschaffung, Implementierung, Auditierung, Zulassung und Inbetriebnahme (Anfang 2023) eines S3 kompatiblen Object Store
- das Update auf zwei RHEL8 Minor Releases und die Bereitstellung von RHEL9 ab Verfügbarkeit
- die Anpassung, Erneuerung und Orchestrierung des gesamten IKT-Ökosystems KAMINO bestehend aus Test- und Entwicklungsinfrastruktur für die Klon- und Klonmodul-Entwicklung und der Managementumgebung, d.h. die Überarbeitung der gesamten Continuous Integration und Continuous Deployment Umgebung in Hinblick auf den neuen KAMINO Serverklon

Auf der Liste der erforderlichen technischen Neuerungen im Bereich IKTTe stehen noch einige interessante Punkte hinter denen sich besondere technische Herausforderungen verbergen und wofür in den nächsten Jahren hoffentlich auch Zeit sein wird. Denn diese Liste ist mehr. Sie ist eine Wunschliste. Es geht dabei nicht nur um technische Neuerungen, sondern auch um den Spaß an Neuem, um die Lust an Veränderungen und um das erfüllende Gefühl eine Vision in eine Strategie und in die Realität umzusetzen, um damit die Ansprüche eines modernen IKT-Providers zu erfüllen.

Die Rekrutierung von Personal, die Einführung neuer sowie Erhaltung und Weiterentwicklung bestehender IKT-Infrastruktur, der Radarsysteme, der Funkgeräte im mil. Bereich sowie systemnaher Software wird alle Mitarbeiter des Bereiches IKT-Technik fordern. Trotzdem werden ausgewählte, wichtige Themenbereiche wie zum Beispiel „Quantum Key Distribution (QKD), Künstliche Intelligenz (KI), Zero Trust Architektur (ZTA) durch die Umsetzung von konkreten Projekten bzw. der Mitwirkung in verschiedenen Arbeitsgruppen und Forschungsprojekten im kommenden Jahr bearbeitet werden.

Die Mitarbeiter des Bereiches IKTTe bedanken sich für die außerordentlich gute Zusammenarbeit.

Militärisches Cyberzentrum

MiCNET, Notfall- und Krisenmanagement, CyberRange, Cybersicherheitszyklus

MiCNET

In den vergangenen Jahren führte die Direktion IKT&Cyber im Rahmen eines European Defence Agency (EDA) -Projektes Live-Fire-Cyberübung durch, die speziell der Verbesserung der europäischen Zusammenarbeit zwischen den nationalen Computer-Notfallteams (CERTs) der Mitgliedstaaten diente. An der Übung nahmen mehr als 200 Experten aus 17 EDA-Mitgliedstaaten und der Schweiz teil, die alle von ihren Arbeitsorten aus miteinander verbunden waren. Die Veranstaltung bestand sowohl aus einem technischen Teil, in dem das Vorfallsmanagement im Vordergrund stand, als auch aus einem strategischen Teil, in welchem die internationale Kooperation zwischen der Leitungsebene der milCERTs diskutiert wurde.

Quelle: https://eda.europa.eu/

Das Ziel der Übung war es unter anderem, militärische CERTs zusammenzubringen und die Dynamik des Vorfallmanagements zu beobachten. Wobei der besondere Schwerpunkt auf dem Informationsaustausch, einem Schlüsselfaktor der modernen Cyberverteidigung lag. Während die europäischen Länder bei der Einrichtung von Mechanismen und Verfahren für den Informationsaustausch zwischen zivilen CERTs weit vorangekommen sind, sind solche Kooperations- und Kommunikationskanäle im militärischen Bereich viel weniger entwickelt, auch aufgrund der hohen Sensibilität der Informationen. Angesichts dessen haben viele Beteiligte die Notwendigkeit geäußert, die in zivilen Kreisen angewandte Praxis des Informationsaustauschs auch auf militärische CERTs und deren Operationen auszuweiten. In der neuen EU-Cybersicherheitsstrategie, die im Dezember 2021 veröffentlicht wurde, wird hervorgehoben, dass diese Initiative dazu beitragen würde, die Zusammenarbeit zwischen den Mitgliedstaaten erheblich zu verbessern. Daher beteiligt sich die Direktion IKT&Cyber an dem EDA-Cat A Projekt „Military Computer Emergency Response Team Operational Network (MICNET)“, welches im November 2022 von 18 Nationen unterschrieben wurde.

Hauptziele des Forschungsprojektes

Vertrauensbildende Maßnahmen

Um Konflikte aufgrund von Fehleinschätzungen oder einer falschen Risikowahrnehmung und die Eskalation einer Krisensituation, die schließlich zu einem bewaffneten Konflikt führen würde, zu verhindern, nutzen die EU-Staaten "vertrauens-, transparenz- und sicherheitsbildende Maßnahmen" als Instrument für Verhandlungen.

Wenn man nicht zuerst Vertrauen gewinnt, wird man die nachfolgenden Ziele nicht erreichen können. Mit den vorhandenen begrenzten Ressourcen und Strukturen einen Kreis des Vertrauens zwischen der milCERT-Gemeinschaft durch die Dynamisierung einer jährlichen Übung auf technischer/operativer Ebene zu schaffen, um die Ausbildung, die Verbindungen und die bessere Erfassung und Gestaltung der nachfolgenden Ziele durch den Prozess der Lessons Learned (LL) zu erhöhen.

Vertiefung des Informationsaustausches

Es gibt keine Einheitslösung für die verschiedenen Cyberverteidigungsorganisationen innerhalb der EDA, so dass jede Organisation ihre grundlegenden Erkenntnisse zum Eigenschutz selbst definieren muss, unabhängig davon, ob es sich um technische Informationen oder Erkenntnisse über eher operative Verhaltensweisen oder Trends handelt.
Die systematische Weitergabe der richtigen Informationen zur richtigen Zeit an die richtigen Beteiligten ermöglicht einen wirksameren Cyberschutz und eine effektivere Reaktion. Dies ist ein grundlegendes Instrument, um das Umfeld zu bewerten und sich folglich besser zu schützen.

Verstärkung der Zusammenarbeit

Die Zusammenarbeit zwischen den EU-Einrichtungen ist eine der Hauptprioritäten, um eine wirksamere Cyber-Verteidigung und eine effizientere und kohärentere Reihe von Initiativen zur Entwicklung der Fähigkeiten in allen Mitgliedstaaten zu ermöglichen.

Notfall- und Krisenmanagement

Notfallhandbuch

Um im Falle einer Cyber-Krise besser auf den Ernstfall vorbereitet zu sein hat das MilCyZ im Frühjahr 2022 einen Schwerpunkt auf Business Continuity Management (BCM) gelegt. Dabei wurde ein neues Notfallhandbuch für den geregelten Ablauf und die Einberufung entsprechender besonderer Aufbauorganisationen in IT-Sicherheitsvorfällen erstellt.

Das Notfallhandbuch wurde auf Basis gängiger IT-Sicherheitsstandards erstellt und für das MilCyZ adaptiert um auch spezielle Erfordernisse militärischer Organisationen abdecken zu können.

Ziel des Handbuches ist es, einen koordinierten Ablauf bei einem auftretenden IKT-Sicherheitsnotfall zu gewährleisten und die Rahmenbedingungen eines solchen Ablaufes klar zu definieren.

Quelle: BSI-Standard 200-4, S. 16

Dabei wurde die Einsatzorganisation in drei organisatorische Ebenen unterteilt:

- Operative Notfall-Teams aus den betroffenen Fachbereichen
- Notfallentscheidungsgremium als strategisches Entscheidungselement bei einem Notfall
- Notfallstab als leitendes und koordinierendes operatives Element

Mit der Stabsarbeit im Rahmen der besonderen Einsatzorganisation wird sichergestellt, dass alle vorhandenen Kompetenzen in der Direktion gebündelt werden. Durch das besetzte Notfallentscheidungsgremium und dem Notfallstab ist es möglich, in kurzer Zeit wichtige Entscheidungen zu treffen, um den Verlauf des Notfalles positiv zu beeinflussen. Dies stärkt die Handlungskompetenz, was in einem Notfall unumgänglich ist.

Nach der Verfügung des Notfallhandbuches wurde die Einberufung auch erfolgreich mit allen involvierten Leitern in Form einer Alarmierungsübung erfolgreich absolviert.

Stabsübung Krisenmanagement

Um neben dem Notfall auch auf eine mögliche Cyber-Krise vorbereitet zu sein, führte die Direktion IKT&Cyber Anfang des Jahres auch eine Stabsübung zur Erprobung der Prozesse und den Aufbau der Stabsinfrastruktur im Falle einer Cyber-Krise durch. Als Ausgangsszenario wurde damals der Beginn des Ukraine-Krieges und deren Auswirkung auf das BMLV und Österreich genommen. Hierfür wurde in den Räumlichkeiten der AG-Stiftgasse ein Krisenstab der Direktion IKT&Cyber aufgebaut um einerseits ein einheitliches Cyber-Lagebild zu erstellen und andererseits die Prozesse auf einen möglichen Ernstfall anzupassen.

Truppenübungsplatz in der Cyber-Domäne

Zunehmende digitale Vernetzung, Cyberattacken und hybride Konflikte erfordern eine permanente Aus- und Weiterbildung für Cyberexperten, -führungskräfte und –truppen.

Zivile und militärische Einsatzorganisationen simulieren regelmäßig ihre Einsatzfälle im Rahmen physischer Übungen, um stets für den Ernstfall gerüstet zu sein.

Dieses Erfordernis besteht freilich auch in der Domäne Cyber, allerdings braucht es hier ein virtuelles Pendant zum klassischen Truppenübungsplatz:

Eine sogenannte Cyber Range ist eine virtuelle Umgebung innerhalb derer Cyberangriff und Cyberverteidigung geübt, als auch neue Technologien erprobt werden können, ohne real existierende Systeme zu gefährden. Typischerweise werden real existierende Systeme (Netzwerke, Applikationen, Tools, bis hin zu Supervisory Controll and Data Acquisition (SCADA) - Software) in eine Cyber Range kopiert und die angrenzende Netzwerk- und Internetstruktur simuliert.

Das Militärische Cyberzentrum ist derzeit an mehreren einschlägigen Forschungsprojekten beteiligt, nutzt bisher aber nur Cyber Ranges von Drittanbietern. Naturgemäß können dadurch nicht alle Anforderungen des Österreichischen Bundesheers abgebildet werden.

Daher wurde 2022 neben der Mitarbeit in laufenden Forschungskooperationen vom MilCyZ eine Roadmap zur Errichtung einer eigenen Cyber Range des Österreichischen Bundesheeres erstellt welche auf militärische Erfordernisse ausgerichtet ist. Die personellen und materiellen Grundsteine sind gelegt, sodass 2023 der Beginn der operativen Umsetzung erwartet werden darf:

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

Cybersicherheitszyklus

Im Militärischen Cyberzentrum werden die Elemente einer umfassenden IT-Security und Cyber Defence verzahnt umgesetzt. Einzelne Teilfunktionen, die sich aktuell im Aufbau befinden (wie z.B. Rapid Response Teams (RRT), Cyber Range), werden dabei nicht vergessen, sondern laufend mitgedacht. Einer der wesentlichen Eckpfeiler dieses ganzheitlichen Cybersicherheitsansatzes stellen die 5 Kernfunktionen des NIST Cybersecurity Framework (CSF) dar. Der Cybersicherheitsleistungskatalog und die entsprechenden Tools des MilCyZ können den einzelnen Elementen des CSF Katalogs wie folgt zugeteilt werden:

IDENTIFY –BMLV IKT-Sicherheitsstatus: Das Leistungsspektrum der Organisationselemente CySihMgmt (ISMS, IKT-Risikomanagement und Grundlagen, Cyber-Tüpl) und Sih-Konzepte & InfoSih (Audit und Pentesting, Zulassung, Richtlinien und Policies) sowie SihOpZ (Cyber Lagebild, Schwachstellenmanagement) greifen in der Kernfunktion IDENTIFY ineinander.

PROTECT – Angriffe verhindern: Hauptverantwortlich in der Kernfunktion PROTECT sind die MilCyZ Elemente IKTCySihTe (für die technische Realisierung und Eigenentwicklungen) und Sih-Konzepte & InfoSih (konzeptionelle Anteile).

https://bit.ly/3kGv8HU

DETECT – Cyber Angriffe erkennen: Neben präventiven Maßnahmen betreibt das MilCyZ auch ein umfassendes Sicherheits-Logging und Sicherheits-Monitoring System. So können Anomalien, Angriffsversuche und erfolgreiche Angriffe möglichst frühzeitig erkannt werden. Hier ist insbesondere das Organisationselement SihOpZ (zentrales Sicherheitslogging und -monitoring) federführend tätig. IKTCySihTe bringt Sicherheitssensorik mit ein.

RESPOND – Cyber Angriffe abwehren: Das MilCyZ deckt die Behandlung aller Eskalationsebenen eines Cybersicherheitsvorfalls ab. Werden Reaktionsteams entweder „vor Ort“ oder in Lagezentren benötigt, werden Liasion Elemente oder Rapid Reaction Teams entsendet.

Unter der Führung des Elements SihOpZ (Incident-handling, Lagebild) ist hauptsächlich das Element CySihTe (Analyse von Cyberwaffen, technische Forensik, anlassbezogene Entwicklung von IT-Sec-Sensoren und Effektoren) gefordert. Sih-Konzepte & InfoSih unterstützt bei der Abwehr anlassbezogen mit umfassender Red Teaming Erfahrung. Bei größeren Vorfällen (Notfall / Krise) unterstützt CySihMgmt mit Notfallmanagement sowie (gesamtstaatlicher) Krisen-managementliasionfunktion.

RECOVER: Im Rahmen der Wiederherstellungsphase können die Experten des MilCyZ mit Verbesserungsmaß-nahmen zur Erhöhung der Resilienz und der Cybersicherheit unterstützen. Auch hier sind potentiell alle MilCyZ-Organisationselemente involviert. Lessons Identified und Lessons Learned fließen in alle Funktions-elemente des ganzheitlichen Sicherheitsansatzes hinein.

Die Implementierung des Cybersicherheitszyklus erfordert die personelle und technische Realisierung eines umfangreichen Fähigkeitenspektrums.

Cyberverteidigungsmatrix

Zur Darstellung von notwendigen Fähigkeiten im Bereich der Cyberverteidigung kann Abbildung 2 als Basis dienen.

Diese Rollen- und Fähigkeitenmatrix ist die Grundlage für den Aufbau eines umfassenden Fähigkeitenframe-works für die Cyberverteidigung im Jahr 2023. Dieses Framework wird es auch erlauben, Fähigkeitenprofile, die in spezifischen Einsatzumgebungen und Organisa-tionelementen benötigt werden, modular abzuleiten um die Cyber-Truppe fähigkeits- und aufgabenspezi-fisch aufbauen zu können.

milCPS - Military Cyber Protection System

Das “Military Cyber Protection System” (milCPS) wird schrittweise georedundant ausgebaut. Dazu werden am Standort des Zentralen Ausweichsystems (ZAS) in mehreren Phasen verschiedene Komponenten der „Defence Technology“ in Betrieb genommen. Mit einem Zeithorizont von mehreren Jahren ist geplant, den gesamten Technologie-Stack am Standort des ZAS autark einsetzen zu können. So soll denkbaren künftigen Bedrohungen (sowohl im Cyberraum als konventionell) wirksam begegnet werden können.

Webproxy

Die im milCPS eingesetzte Webproxy Lösung hat das Ende der technischen Lebensdauer erreicht. Um das Schutzniveau zur Absicherung der ausgehenden HTTP und HTTPS Zugriffe zum Internet und anderen externen Netzen am Stand der Technik zu halten ist eine Ablöse erforderlich.

Aufgrund der besonderen Sicherheitsanforderungen und der hohen Integrationstiefe mit anderen Cybersi-cherheitssystemen, ist der Herstellerwechsel eine besondere technische Herausforderung. Der Webproxy ist einer der wichtigsten Sensoren zur Erkennung und Abwehr link- und browserbasierter Angriffe.

EDRS - Endpoint Detection and Response System

Das in den letzten beiden Jahren eingeführte „Endpoint Detection and Response System“ (EDRS) konnte sich heuer erstmals im scharfen Schuss bewähren. Durch den Einsatz des Systems konnte ein Cyberangriff auf ein IKT-System entdeckt werden, der ohne EDRS höchstwahrscheinlich unerkannt geblieben wäre. Durch den gezielten Einsatz der Response Fähigkeiten des Systems konnte der Angriff auf ein einziges System beschränkt und vollständig aufgeklärt werden.

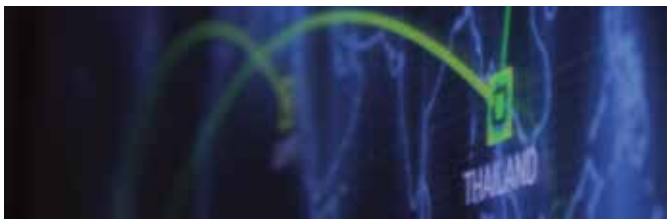
UTNC - Universal Tactical Network Connector

Der Prototyp des „Universal Tactical Network Connector“ (UTNC) bietet eine kryptographisch gesicherte Rückwärtsverbindung für verlegte Einheiten im In- und Ausland. Das System kann dabei unterschiedliche Kommunikationskanäle nutzen (Internet, Satellit, ...) und ist für Truppentauglichkeit, einfache Handhabung und als „Light-Weight“ Lösung für gute Transportierbarkeit ausgelegt. Die erfolgreiche Erprobung erfolgte bei mehreren nationalen und internationalen Einsätzen des ÖBH.

Threat Broker

Ziel des Projekts „Threat Broker“ ist es technische Informationen über Cyber Bedrohungen aus unterschiedlichen Quellen zu aggregieren und zu normalisieren. Dabei werden offene und kommerzielle Informationsquellen genauso genutzt, wie das Eigenaufkommen aus der Sensorik des ÖBH, sowie nationaler und internationale Partner. Diese Informationen werden im Zuge des Projekts aber nicht nur für Analysen zur Verfügung gestellt, sondern derart aufbereitet, dass sie in den Sensoren und Effektoren des „Defence Technology Stacks“ des ÖBH direkt weiterverarbeitet werden können.

Distributed Denial of Service Attack - DDoS



Da die Kernprozesse des ÖBH so gestaltet sind, dass sie auch ohne verfügbares Internet funktionieren, hatte Schutzbedarf vor Distributed Denial of Service (DDoS) Angriffen bisher keinen besonderen Stellenwert.

Dennoch ist im letzten Jahr eine Zunahme von DDoS Angriffen aufgefallen, die nicht auf eine reine Überlastung der Netzwerkkapazitäten abzielen, sondern versuchen die Webanwendungen auf Applikationsebene zu überlasten. Im Zuge dieser Analysen ist es gelungen, die Fähigkeiten zur Abwehr bzw. zur Verzögerung solcher „Layer 7 DDoS“ Angriffe entscheidend zu verbessern.

Kryptographie in Eigenentwicklung

Im Rahmen der Verarbeitung sowie bei der Übermittlung von klassifizierten Informationen in IKT-Systemen sind besondere Sicherungsmaßnahmen und Schutzvorkehrungen zu treffen. Seit 2005 wird im BMLV dazu ein eigens entwickeltes ÖBH-Kryptosystem eingesetzt, welches den Schutz solcher sensiblen Informationsinhalte bis zu hohen Klassifizierungsstufen vor Kompromittierung gewährleistet. In dem 2022 durchgeführten Rollout der neuen Software-Version wurde auch die Hardware auf moderne Technologie-Standards aktualisiert. Somit konnte nicht nur die Rechenleistung für die Krypto-Operationen erhöht werden, sondern es wurden auch zusätzliche TEMPEST-Sicherheitsvorkehrungen getroffen. Dadurch wird nun die kompromittierende elektromagnetische Strahlung der Kryptosysteme minimiert, sodass eine Rekonstruktion der Informationen anhand einer Abstrahlung nicht mehr möglich ist.

Darüber hinaus wurde mit GPG4BMLV eine Anwendung zum Ver- und Entschlüsseln von Dateien bis zur Klassifizierungsstufe "EINGESCHRÄNKT/RESTRICTED" im Sicheren Militärischen Netz (SMN) entwickelt. Dieses verwendet die universelle Krypto-Engine wie beispielsweise GnuPG (GNU Privacy Guard) und ist somit uneingeschränkt kompatibel mit allen anderen Programmen, die den OpenPGP-Standard nach RFC 4880 implementieren. Dadurch wird ein sicherer und uneingeschränkter Datenaustausch auch mit externen Partnern ermöglicht. Als besondere Herausforderung im Rahmen der Übermittlung von verschlüsselten Dateien gestaltet sich die Überprüfung auf Schadcode. GPG4BMLV verwendet dazu die Eigenentwicklung Multi AntiVirus Engine (MAVE), welche nach dem Entschlüsselungsvorgang automatisiert aufgerufen wird und die Datei erst nach erfolgreicher Prüfung dem Anwender zur weiteren Bearbeitung zur Verfügung stellt.

TIP, Einsatz-SOC, RRT, CR22

Die Direktion IKT&Cyber als zentraler IKT-Provider ist im Rahmen der Bereitstellung in nahezu alle IKT-Projekte eingebunden. Abhängig vom konkreten Umfang eines neuen IKT-(Teil-)Systems, sind mehr oder weniger Fachbereiche und –Abteilungen eingebunden. Aufgrund stetig steigender Sicherheitsanforderungen werden auch immer mehr IKT-Services und IKT-Fähigkeiten in die Systeme der Sicherheitsoperationszentrale (SihOpZ) als Teil des MilCyZ, eingebunden. Dies umfasst folgende Fähigkeiten:

- Angriffserkennung mit Hilfe des Kernsystems „SIEM“ (Security Information and Event Management),
- Schwachstellen-Management mit Hilfe eines Schwachstellen-Management-Systems und einer zugehörigen Schwachstellen-Datenbank, sowie dem
- Cyber-Lagebild mit dem gerade in Entwicklung befindlichen „CyMIS“ (Cyber Melde- und Informationsservice), welches künftig ein Ebenengerechtes Lagebild im Cyber-Raum liefern wird.

Das MilCyZ baut zudem gerade ein System zur Sammlung und Verarbeitung von Bedrohungsinformationen („TIP“, Threat Intel Platform) auf. Dieses ermöglicht es bei der Prävention von Cyber-Angriffen, aber auch bei der Angriffserkennung und –Analyse künftig besseren Kontext zu schaffen. Somit können bekannte Bedrohungen (z.B. bekannte Schadsoftware, bekannte Angreifer-Infrastruktur) schneller blockiert oder erkannt und geeignete Gegenmaßnahmen getroffen werden. Das System wird über den Jahreswechsel 2022/2023 produktiv gehen.

Darüber hinaus wird das MilCyZ künftig auch dezentrale Services bereitstellen, welche die IKT-Sicherheit von Teilsystemen auch abseits zentraler Infrastruktur gewährleisten bzw. im Anlassfall Wiederherstellung unterstützen. Dazu zählen folgende Vorhaben:

Einsatz-SOC:

Das Einsatz-SOC („Security Operations Centre“) wird künftig als dezentrales SOC-Element mit dem IKT-System Einsatz gekoppelt Anwendung finden. Dazu bietet es die Möglichkeit, Angriffe auch in den dezentralen, ggf. autark agierenden Systemanteilen, erkennen und Erstmaßnahmen zur Eindämmung ergreifen zu können. Dies trifft z.B. auf schnell zu verlegende Einsatzsysteme, auch im Ausland, zu, bevor etwa eine Rückwärtsverbindung zu den zentralen IKT-Systemen hergestellt werden kann. Derzeit befindet sich das Vorhaben in Analyse, ist jedoch abhängig vom – ebenfalls noch in Analyse befindlichen – IKT-System Einsatz und dem zugehörigen verlegbaren Rechenzentrum.

Weiters hat die Sicherheitsoperationszentrale (SihOpZ) im Rahmen der DACH-Übung „COMMON ROOF 22“ (CR22) erneut die zentralen Komponenten zur Angriffserkennung („SIEM“) im SOC-Element bereitgestellt. Ergänzend wurde 2022 auch ein Element zur Automatisierung und zum Verwalten der Vorgänge („SOAR“, Security Orchestration, Automation and Response) hinzugefügt. Darüber war es den Übungsteilnehmern in der SOC-Zelle möglich, etwaige erkannte Angriffe in einer Art Ticket im Kontext zu betrachten, Tätigkeiten zu dokumentieren und eine geeignete Gegenmaßnahme zu ergreifen. In weiteren Iterationen der Übungsserie werden die Prozesse und Integrationen der verschiedenen Sicherheitssysteme stetig vertieft werden.

Rapid Response Teams Cyber:

Es wird eine Fähigkeit aufgebaut, um im Anlassfall mit reaktiven Kräften abgesetzte IKT-(Teil)Systeme zu analysieren und etwaige Cyber-Angreifer in dem betroffenen System zu bekämpfen, um im Anschluss wieder einen sicheren Betrieb gewährleisten zu können. Dies gilt einerseits für dezentrale IKT-Systemanteile des BMLV, bzw. auch wenn gesamtstaatlich ein Assistenzeinsatz im Cyber-Raum für andere Ministerien oder im Bereich der kritischen Infrastruktur ausgerufen werden sollte. Dazu baut das MilCyZ Infrastruktur und technische Fähigkeiten auf und laufend aus, um im Ernstfall Unterstützung bieten zu können.

Sicherheitskonzepte & Sicherheitsaudits

Auch im Jahr 2022 hat die Abteilung Sicherheitskonzepte & Informationssicherheit in zahlreichen Vorhaben und Projekten die Sicherheit bereits in der Konzeptions- und Designphase von Systemen durch direkte Mitwirkung erhöhen können.

Durch diese frühzeitige Beitragsleistung ist sichergestellt, dass ein System in seiner Realisierungsphase schon sämtliche sicherheitstechnischen Anforderungen erfüllen kann, wodurch die sicherheitstechnische Abnahme und ggf. Zulassung des Systems deutlich effizienter und mit weniger Bedarf an nachträglichen Korrekturen durchgeführt werden kann.

Im Rahmen von IKT-Sicherheitsaudits werden neben Eigenentwicklungen auch immer wieder Produkte überprüft, welche auch außerhalb des BMLVs eingesetzt werden. Werden dabei Schwachstellen gefunden, die sich nicht aus der verwendeten Konfiguration, sondern auf das Produkt selbst beziehen, werden diese selbstverständlich an den Hersteller weitergegeben, so dass dieser für all seine Kunden eine abgesicherte Lösung bereitstellen kann.

Im vergangenen Jahr wurden für folgende Lösungen Schwachstellen gemeldet:

- In einer Unified Communication Umgebung wurden mehrere gravierende Schwachstellen gefunden, die in Kombination zu einer kompletten Übernahme der betroffenen Server führen hätte können. Der Hersteller wurde informiert, hat bereits mehrere der Schwachstellen behoben und arbeitet weiter intensiv mit dem MilCert zusammen um die verbleibenden zu mitigieren.

- In einem Content Management System (CMS) und dessen Plugins wurden Schwachstellen gefunden, welche es einem authentifizierten Benutzer erlauben, Code in den Browsern von Administratoren und anderen Benutzern auszuführen, und sich so schließlich ihre Daten zu stehlen und sich ihre Rechte zu verschaffen. Die Kommunikation mit dem Distributor ist am Laufen, damit auch diese Schwachstellen behoben werden können.

- In einem weit verbreiteten Videokonferenzsystem konnten unterschiedliche Schwachstellen identifiziert werden. Gleich mehrere davon erlauben es einem authentifizierten Benutzer die Datenbank auszulesen. Der Angreifer kann dadurch sensible Informationen erlangen, unter anderem die Namen der Benutzer und Administratoren, sowie deren Passworthashes. Damit könnte er in weiterer Folge die Passwörter offline knacken und sich auf diese Weise den vollen Zugriff auf das Videokonferenzsystem sichern, um so unbemerkt Besprechungen zu belauschen.

Eine weitere Schwachstelle führt dazu, dass authentifizierte Benutzer der Weboberfläche am Betriebssystem unberechtigt Dateien lesen und schreiben können. Die Schwachstelleninformationen sind über den Distributor an den Hersteller übermittelt worden.

Fähigkeitenausbau der Elektronischen Kampfführung

In der Abteilung UZEloKa konnten die Fähigkeiten bei der Signalanalyse von Signalen im Elektromagnetischen Umfeld (EMU) ausgebaut werden. Diese Fähigkeitenerweiterung, die durch gezielte Systemschulungen und laufende Fortbildungen die Expertise des Fachpersonals auf dem aktuellen Stand der Technik hält, stellt ein wesentliches Element der Analyse und Bewertung von Informationen in der Waffengattung Elektronische Kampfführung (EloKa) dar.

Mit dem heurigen Jahr wurde die Abteilung UZEloKa mit der Entwicklung und dem Aufbau eines EloKa-Lagebildes beauftragt.

Als Teil der Cyberkräfte ist es für die Waffengattung EloKa ein Lagebild des EMU in dem Lageinformationen mit Bezug zur Nutzung und Nutzern des EMU aus unterschiedlichen Bereichen des ÖBH, Lagemeldungen verarbeitet werden, die Erstellung einer EloKa-Lagekarte und das Bereitstellen von Fachbeiträgen.

Damit soll der kritische Informationsbedarf von militärischen Entscheidungsträgern hinsichtlich des Einsatzes sämtlicher Nutzer des EMU, der EloKa-Truppe und etwaigen Fähigkeitsdefiziten gedeckt werden.

Forschungs- und Entwicklungsprojekte

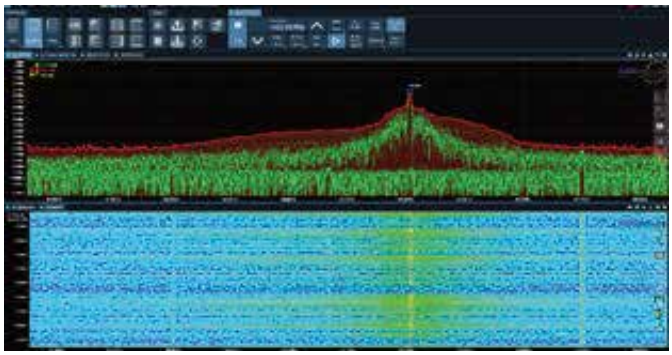
Im zweiten Quartal 2022 konnte das rund eineinhalb Jahre dauernde Projekt „EMS Eye Bots - Scannen und Analyse im elektromagnetischen Spektrum“ gemeinsam mit dem Forschungspartner JOANNEUM RESEARCH erfolgreich zum Abschluss gebracht werden.

Das Projekt EMS Eye Bots beschäftigte sich mit der Forschungsfrage, wie Aktivitäten im Elektromagnetischen Umfeldes (EMU) mit kostengünstigen Standardbaugruppen erfasst werden können.

Langfristig gesehen könnten Sensoren in Zukunft in vielfacher Ausführung in einem Sensornetz zur mobilen Erfassung des EMU mitgeführt werden und zur eigenen Informationsverdichtung auf dem Gefechtsfeld beitragen.

Das Fehlen von Kommunikationskanälen oder die fremdgesteuerte Nutzung des EMU kann, speziell in hybriden Bedrohungsszenarien, die eigenen Fähigkeiten massiv einschränken, wodurch sich der Bedarf des Schutzes der eigenen Kräfte und der Bedarf der frühzeitigen Bedrohungserkennung ergeben.

Die Ergebnisse und gesammelten Erfahrungen dienen einerseits als Basis für die Miniaturisierung der Sensoren und andererseits als Grundlage für die Erforschung wie die verschiedenartigen Daten effizient weiterverarbeitet und einer optimalen Visualisierung zur Erkennung von Änderungen zugeführt werden können.



Die Eigenentwicklung der Abteilung UZEloKa zur Signaldarstellung und Simulation von Signalen wird stetig betrieben, um dem Stand der Technik zu entsprechen. Diese findet beispielsweise bei der Bedrohungssimulation für die Countering Radio Controlled Improvised Explosive Devices Electronic Warfare (CREW)-Systeme des ÖBH eine einsatzrelevante Anwendung.

Eine weitere Eigenentwicklung der Abteilung UZEloKa ist der Prototyp einer RCIED Datenbank im SMN die mit dem dritten Quartal 2022 den Probebetrieb aufnahm. Es sollen im Wesentlichen technische Informationen von RCIED zentral durch das UZEloKa an die Bedarfsträger des ÖBH bereitgestellt werden.

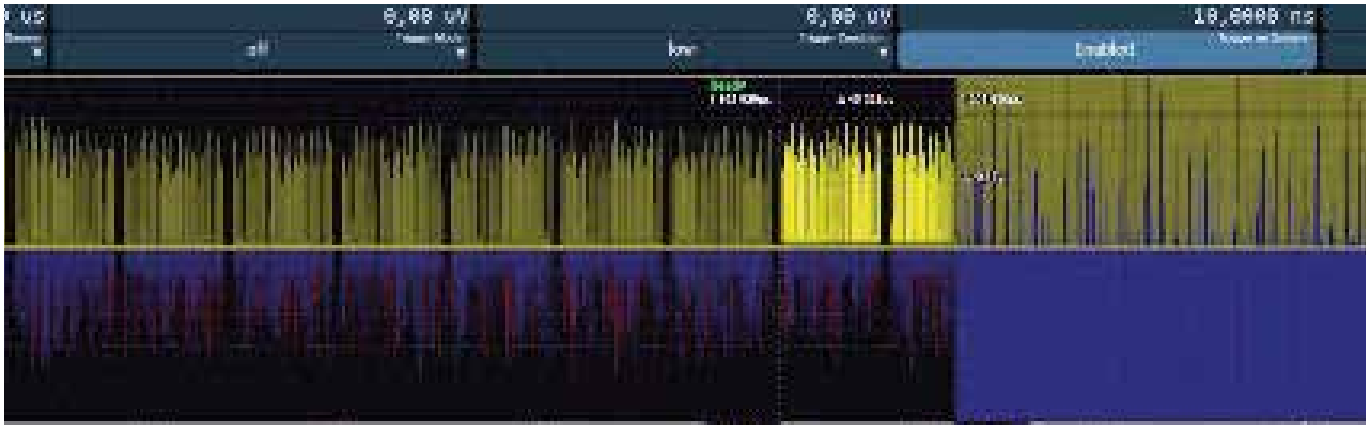
Diese herausfordernde Aufgabe ermöglichte einen sehr wertvollen Erfahrungsgewinn der die weiteren Planungen für den künftigen Fähigkeitenaufbau bei der Informationsbereitstellung in der Waffengattung EloKa, einer der Kernaufgaben des UZEloKa, darstellt.

Projektarbeit

Eine weitere Aufgabe des UZEloKa stellt die EloKa-Bewertung von Systemen dar. Hier wird aus Sicht der EloKa, und unter dem Einbeziehen von Auswirkungen, sowie dem Verhalten im EMU bewertet. Ebenfalls werden neue Systeme auf Implikationen auf die Waffengattung EloKa beurteilt.

Dies soll den Bedarfs- und Entscheidungsträgern einen Überblick vermitteln, um die EloKa-relevanten Eigenschaften, bei beispielsweise Einsätzen, Übungen und Beschaffungen, mitbeurteilen zu können.

Im Jahr 2022 geschah dies beispielsweise bei dem Projekt Tactical Data Radio (TDR) und konnte im Rahmen der Beschaffung des Hubschraubers AW169 begonnen werden.



Institut für Militärisches Geowesen

Mitarbeiter am IMG im April 2022

Internationale Zusammenarbeit auf Ebene EU und NATO-PfP

Das IMG nimmt regelmäßig als Vertreter Österreichs an Veranstaltungen auf NATO- und EU-Ebene teil, die die Steuerung und Koordinierung der Aktivitäten im Fachbereich sicherstellen. Aus strategischen Dokumenten der jeweiligen Institutionen leiten sich die Erfordernisse ab, die zur Auftragserfüllung essentiell sind. Vor allem im Bereich NATO-PfP deckt das IMG hier seinen Informationsbedarf was zukünftige Entwicklungen und Interoperabilitätserfordernisse betrifft. Im Jahr 2022 wurden beschickt:

- NATO Geospatial Board am HQ NATO
- Geospatial Requirements Working Group in Arnhem/NLD und bei HQ SHAPE
- EU Geospatial Board in Luxemburg/LUX
- PESCO Projekt EU GeoMetoc Support Coordination Element (GMSCE)

Natürlich waren bei allen diesen Treffen die Entwicklungen im Osten Europas ein Thema und es wurden auch entsprechende Ableitungen getroffen. Im vergangenen Jahr konnte mit der Verabschiedung der NATO Geo-Policy das höchste Grundlagendokument im Fachbereich auf NATO-Ebene finalisiert werden. Heuer wurde, nach mehrjährigem Bearbeitungsprozess durch die Mitgliedsstaaten, das European Union Concept for Geospatial Support for European Union Crisis Management and European Union Common Security Defence Policy Military Operations and Missions verfügt.

NATO Geospatial Board

Mit der Allied Joint Doctrine for Geospatial Support konnte die NATO dieses Jahr ein weiteres wichtiges Grundlagenpapier in den Genehmigungsprozess bringen. Zum Jahresabschluss ist die Bearbeitung des Technical Agreements für Projekt GMSCE zur Unterschriftsreife gelangt. Dieses Papier regelt die Abwicklung eines von Seiten EU artikulierten Bedarfes an GeoInfo-Produkten.

PARTNERSEMINAR 2022

Am 13. September 2022 konnten der Gruppenleiter Vermessung HR DI GOLD des BEV und eine der Partnerschaftsbeauftragten vom IMG OR Mag. KAUTZ im Rahmen des Partnerseminars 2022 die Urkunde zum 15jährigen Bestehen aus den Händen des designierten Generalstabchefs GenMjr Mag. Rudolf STRIEDINGER entgegennehmen.

Begründet wurde diese Partnerschaft zwischen IMG und BEV am 17.09.2007 von Bgdr Dr. Mang und Präsident DI Hochwarter um die enge fachliche Zusammenarbeit zu unterstreichen und die beiden Organisationen, die im k.k. Militärgeographischen Institut gemeinsame Wurzeln haben auf diese Weise wieder zusammen zu führen.

Es ist eine gelebte Partnerschaft die nicht nur vom fachlichen Austausch lebt, sondern auch von Freundschaften, die durch Partnerschaftsveranstaltungen entstanden sind.

WISSENSCHAFTSKOMMISSION am IMG

Basislehrgänge GIS

Einer der Basislehrgänge GeoInformationsSysteme am IMG

Im ÖBH bekommt die Verarbeitung geocodierter Daten auch außerhalb des MilGeo-Dienstes einen immer höheren Stellenwert. Um die Mitarbeiter dieser Projekte adäquat in die GIS Software (QGIS) einzuschulen, werden seitens IMG/IMG RefD seit 5 Jahren 1-wöchige „Basislehrgänge GIS“ unter der Leitung von OR Mag. KAUTZ angeboten. 2022 fanden zwei dieser Kurse am IMG statt und es wurden insgesamt 35 Mitarbeiter aus den Bereichen LuAufkl, LuU, MilKdoT und JaKdo vom GIS – Geosupportteam (KAUTZ, FÜRPASS, PRUZSINSZKY) des IMG erfolgreich geschult.

Referatsklausur Daten & Systeme – Iselsberg 22

Das Referat Daten & Systeme des IMG hielt vom 26.-30.09.22 seine jährliche Referatsklausur, diesmal im SemZ ISELSBERG ab. Dieses Jahr lag das Schwergewicht auf der durch die ständig steigende Anzahl an Plattformen und der durch das Ref Daten & Systeme zu unterstützenden Services, zuletzt etwa der leichten Mehrzweckhubschrauber (IMzHS) LEONARDO, umfassenden Abstimmung der Geodatenstruktur und der Systeme untereinander sowie auf der Neuausrichtung des Workflows und einer Evaluierung und weiteren Festigung des Qualitätsmanagements.

Geländeeinweisung im Gschlößtal durch die Mitarbeiter der NP-Verwaltung Hohe Tauern.

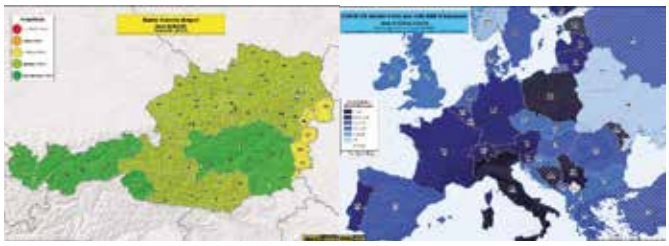
Konkrete Aufgaben waren u.a. die Übersicht, Qualitätsmanagement, Durchführung Lessons learned - lessons identified und daraus abgeleitet Optimierung der prioritären Auftragserfüllung der laufenden Projekte des Referates, die Jahresplanung für Projekte 2023 (insbes. Übungsteilnahmen des Referats), die Umstellung auf ArcGISPro bzw. QGIS in puncto Regelungsbedarf, Zeitrahmen und Abstimmung mit anderen Abteilungen Direktion IKT&Cyber, die Planungen zur Erstellung einer Metadatenbank mittels GeoNetworks, die neue GUI des GeoWebService „WebView“ sowie die Besprechung und Geländeeinweisung mit Vertretern des Nationalpark Hohe Tauern betreffend HGLLG 2023 und darüber hinaus.

Die direkte Zusammenarbeit mit der NP-Verwaltung Hohe Tauern ist für die Erstellung des Geodatenbestandes für den HGLLG unerlässlich.

COVID-19 Kartenproduktion

Die COVID-19 Pandemie ist ein Thema, das auch im Jahr 2022 weiterhin vom IMG bearbeitet wurde. Im Verlauf des Jahres sind rund 250 Karten erstellt worden, welche einerseits die Entwicklung der 7-Tages Inzidenz pro 100.000 Einwohner sowohl für Österreich als auch in Europa wiedergeben und andererseits die

aktuelle Schaltung der „Corona-Ampel“ abbilden. Die Veröffentlichung der Karten mit den jeweiligen Inzidenzzahlen erfolgt am Wochenbeginn sowie zur Mitte der Woche, jene mit der gegenwärtigen Ampel-Situation am Ende der Woche.



Diese Karten leisten im BMLV nach wie vor einen wichtigen Beitrag zu der Beobachtung und Beurteilung der COVID-19 Situation in Österreich.

Militärkarten Inland

Vom Institut für Militärisches Geowesen (IMG) werden die eingesetzten Kräfte beim Assistenzeinsatz an der Staatsgrenze im BURGENLAND, neben der standardmäßigen Versorgung mit den Topographischen Kartenwerken 1 : 50 000 und 1 : 250 000, mit maßgeschneidertem Kartenmaterial des Einsatzraumes unterstützt. Großer Bedarf an MilGeo-Produkten bestand in diesem Jahr insbesonders auch am Truppenübungsplatz BRUCKNEUDORF. Es wurden Militärkarten diverser Maßstäbe (Lagerpläne 1 : 5 000, TÜPl-Karten 1 : 10 000 und 1 : 25 000 sowie die Übersichtskarte 1 : 50 000) aktualisiert, nachgedruckt und bereit-gestellt, sodass die Versorgung der übenden Truppen mit aktuellem Kartenmaterial gewährleistet ist.

Ausschnitt aus der Topographischen Karte „AssE Burgenland 1 : 25 000“

Militärkarten Ausland

Aufgrund der aktuellen Lageentwicklung in der UKRAINE stehen die Überarbeitung von vorhandenem Kartenmaterial und die Erstellung von Spezialkarten im Fokus. Die aktuellen Produkte sind inhaltlich und kartographisch vielfältig und decken einen großen Maßstabsbereich ab.

Ausschnitt aus der Thematischen Karte „Ukraine 1 : 1 000 000“

Deren Erstellung ist, meist aufgrund der zeitlichen Rahmenbedingungen, oft herausfordernd. Es wurden zahlreichen Bedarfsträger innerhalb des BMLV und, im Zuge von Unterstützungsleistungen, das Innenministerium (BMI) sowie die Stabstelle Flüchtlingskoordination im Bundeskanzleramt (BKA) mit Karten versorgt.

Militärische Landesbeschreibungen (MLB) / Militärische Geoinformationen (MGI)

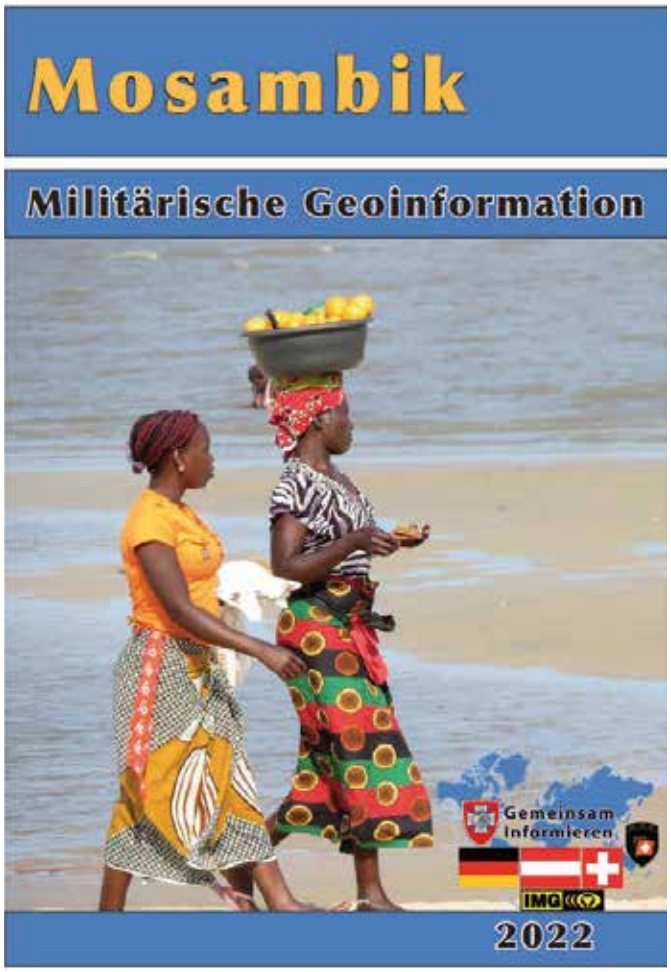
Für ausgewählte Krisengebiete der Erde und (potenzielle) Einsatzräume des ÖBH erstellt Direktion IKT&Cyber/IMG Militärgeographische Landesbeschreibungen (MLB) und Militärische Geoinformationen (MGI).

Diese landeskundlichen Informationen stellen einen allgemeinen Überblick über das jeweilige Land zu verschiedenen Themengebieten dar (. Sie dienen militärischen Planern als Bearbeitungs- und Beurteilungsunterlage sowie Soldaten als Einstiegsinformation bei einem Einsatz.

Aufbau und Gliederung von MLB und MGI sind deckungsgleich, ein Unterschied besteht lediglich im beteiligten Kreis von Autoren bzw. Dienststellen. Während die MLB ein rein österreichisches Produkt unter Beteiligung verschiedener Dienststellen des Bundesheeres (IMG, IFK, MilMed etc.) ist, entsteht eine MGI im Rahmen einer seit dem Jahr 2010 permanent laufenden Kooperation der militärischen Geodienste aus Deutschland, Österreich und der Schweiz („D-A-CH“).

Direktion IKT&Cyber/IMG, ZGeoBW (Zentrum für Geoinformationen der Bundeswehr) und die Schweizer Armee wirken an der Erstellung der Schriftenreihe „Militärische Geoinformation“ (MGI) arbeitsteilig zusammen.

Eine Koordinierungsgruppe, bestehend aus Mitgliedern der Geodienste dieser drei Partnerstaaten, trifft sich halbjährlich nach dem Rotationsprinzip zu Arbeitstreffen in Deutschland, Österreich und der Schweiz, wo konzeptionelle, inhaltliche und organisatorische Fragestellungen bearbeitet werden.



Coverbild der MGI Mosambik 2022

Koordinierung, Kartographie, Lektorat und Layoutierung werden dabei federführend von Direktion IKT&Cyber/IMG wahrgenommen. Sämtliche MLB/MGI sind im Intranet auf der Seite des Militärischen Geowesens in der Rubrik „Geoinformationen“ - „Länderinformationen“ unter folgendem Link abrufbar: https://cms.intra.bmlv.at/web/img
Im Kalenderjahr 2022 werden folgende MLB/MGI bearbeitet:

- MLB Zypern (Neubearbeitung)
- MGI Mosambik (Neubearbeitung)
- MGI Niger (Aktualisierung der Ausgabe 2014)
- MLB Bosnien-Herzegowina (Neubearbeitung)

MILITÄRGEOLOGIE

Die steigende Anzahl an militärgeologischen Unterstützungsleistungen, zeigt die Notwendigkeit der Fähigkeitenentwicklung in diesem Bereich deutlich.

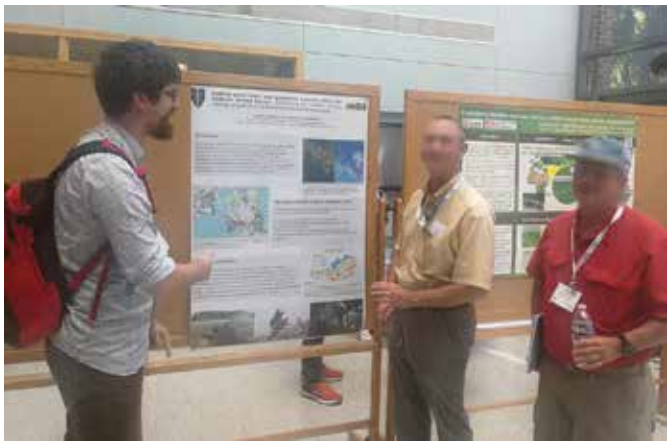
Ob Vorbereitungen auf die Bewältigung von Naturgefahren, Geländeanalysen für die Einsatzvorbereitungen im In- und Ausland sowie Untersuchungen des Untergrundes für den täglichen militärischen Dienstbetrieb: Geologische Expertise ist vorhanden!

Ausgewählte Produkte der Militärgeologie:

- Militärgeologische Stellungnahmen
- Digitale und Vorort Gelände Analysen
- Multispektrale Satellitenbildauswertung im Bereich Geologie und Bodenkunde
- Geologische, hydrologische und bodenkundliche Einsatzraumbeschreibungen
- Geologische Karten, Grafiken und Modelle
- Forschungsbeiträge zu geowissenschaftlichen Fragestellungen

14TH CONFERENCE OF MILITARY GEOSCIENCES

Bei der "14th Conference of Military Geosciences" einer internationalen geowissenschaftlichen Konferenz in Charleston, USA präsentierte das Institut für Militärisches Geowesen militär-geologische Fachbeiträge. Neben dem enormen Erkenntnisgewinn für die eigene Auftragserfüllung stärkt diese Teilnahme auch die internationale Zusammenarbeit.



Bundesministerium für Landesverteidigung

Stichwortverzeichnis

1-9

1st Level Support	Erste Anlaufstelle für IKT-Probleme
2nd Level Support	Zweite Ebene für spezifischere IKT-Probleme
24/7	24 Stunden am Tag, sieben Tage die Woche

A

AAB	Aufklärungs- und Artilleriebataillon 3
AAG21	„Air to Air Gunnery" (Luft-Luft Schieß-Übung)
ABCIS	Atomar-Biologisch-Chemisches Informationsssystem
ABNA	Airgapped Bastion Network Austria (physisch isoliertes Netzwerk)
AbwA	Abwehramt
Accesspoints	Zugangspunkte zu Netzwerken
AddOn	Erweiterung
AI	Artificial Intelligence (künstliche Intelligenz)
AIT	Austrian Institute of Technology (Außeruniversitäre Forschungseinrichtung in Österreich
All Flash	Schnelle Speichertechnologie (nichtflüchtig, behält Speicher trotz Abschaltung)
AMZ	Arbeitsmedizinisches Zentrum
APEX	Application Express (Webbasierte Softwareentwicklungs-umgebung)
Appl	Abteilung Applikation
Application Level Firewalling	Netzwerksicherheitskomponente auf Anwendungsebene
Arbeitsplatzfixes	Fehlerbehebungspunkte von Softwareproblemen
ArcGIS	Geoinformationssystem-Software
ARWT	Amt für Rüstung und Wehrtechnik
ASECOS	System zur verschlüsselten Übertragung von Daten
AssE	Assistenzeinsatz
Audit	Überprüfung
AÜG	Arbeitskräfteüberlassungsgesetz
AUT	Austria
AUTCON	Austrian Contingent (Kontingent im Auslandseinsatz)
AUVA	Allgemeine Unfallversicherungsanstalt

B

Backbone	Rückgrat (Hauptleitungen) von Netzwerken
BACnet	Building, Automation and Control Networks (Netzwerkpro-tokoll für Gebäudeautomation
BACtwin	Building, Automation and Control Twin (Digitaler Zwilling)

BandlibrarySystem	Bandbibliothek zur Datenspeicherung auf Magnetbändern
BatchFenster	Konsolenfenster des Betriebssystems
BBG	Bundesbeschaffungsgesellschaft
BenBe	Benutzer-Betreuung
Big Data	Große komplexe Datenmengen
Bitbox	Browser in the Box (Browser in virtueller Maschine, um Angriffe auf das Host-System zu verhindern)
BK/C	Bundeskriminalamt/Abteilung Cyber Crime and Competence Center
BKA	Bundeskanzleramt
Blackhawk	Transporthubschrauber S-70 der Firma Sikorsky
BlueScreen	Fehleranzeige nach schwerwiegendem Problem im Betriebssystem
BMDW	Bundesministerium für Digitalisierung und Wirtschaftsstandort
BMEIA	Bundesministerium für europ. und intern. Angelegenheiten
BMI	Bundesministerium für Inneres
BMLRT	Bundesministerium für Landwirtschaft, Regionen und Tourismus
BMLV	Bundesministerium für Landesverteidigung
BMS	Battlefield Management System
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
Bruteforce	Methode, unerlaubten Zugriff auf IT-Systeme zu erlangen
BRZ	Bundesrechenzentrum
BV Meldung	Meldung Besonderer Vorfälle
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
BVT/CSC	BVT/Cyber-Security-Center
BWÜ	Beorderten-Waffenübung

C

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

CISDefence	Computer and Information Systems Defence
CKM	Cyberkrisenmanagement
CKMS	Chipkarten-Management-System
CMS	Content Management System
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CO-IServices	Community of Interest Services (Interessensgemeinschaft)
COMEX	Communication Exercise 20
COMMON ROOF	Internationale Übung für Interoperabilität im DACH Raum
COMSEC	Communication security
Content Disarm and Reconstruction	Technologie um Schadsoftware aus Daten zu entfernen
Core-Services	Kerngruppe wichtiger Anwendungen (z.B. E-Mail, VPN, etc.)
Covid-19	SARS CoV-2 Virus („Corona-Pandemie“)
CR	Common Roof (Übung)
CST	Custodial Support Team
Custom App	Angepasste Applikation
CWIX	Coalition Warrior Interoperability Exercise
Cybär	Maskottchen IKT&CySihZ
CyberTruppe	Militärisches Element zur Beherrschung des vollen Spektrums des Kampfes in Computernetzwerken
Cyberabwehr	Abwendung von Attacken auf Netzwerke und Computersysteme
Cyberangriff	Gezielte Attacke auf größere Rechnernetzwerke, spezifisch wichtiger Infrastruktur
Cyberbedrohung	Bedrohungen im Cyberraum (Cyber Kriminalität, Identitätsmissbrauch, Cyberangriffe oder der Missbrauch des Internets)
Cyberdomäne	Dimension der militärischen Einsatzführung, wie Land, Luft, See oder Weltraum
Cyberkoordinator	Steuerungsorgan der Cyberdömane des BMLV auf strategischer Ebene
Cyberkräfte	Teilstreitkraft des ÖBH zur Beherrschung sämtlicher taktischen Maßnahmen zum Schutz der militärischen Netze
Cyberkriminalität	Straf- oder verwaltungsstrafrechtlich relevante, normierte Angriffe aus dem Cyberraum
Cyberkrise	Eskalationsstufe von Cybervorfällen, ausgerufen durch den BMI (NISG §3 Abs.22, §24)
Cyberlage	Darstellung der Eigenlage des ÖBH im Cyberraum und als Teil des militärischen Gesamtlagebildes
CyberOps	Cyber-Operations (Handlung im Cyberraum)
Cyberraum	Der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab
Cybersicherheit	Gesamtheit aller Technologien, Prozesse und Vorgehensweisen , die Netzwerke, Computer, Programme und Daten vor Angriffen, Schäden oder unerlaubten Zugriffen schützen sollen
Cyberverteidigung	Gesamtheit aller Maßnahmen zum Schutz vor Cyberangriffen und zur Erhöhung der Cybersicherheit
Cybervorfälle	Böswilliges oder versehentlich herbeigeführtes Ereignis, das die Cybersicherheit eines Informationssystems oder die Sicherheit der verarbeiteten Informationen gefährdet oder Sicherheitsrichtlinien, Sicherheitsprozesse oder Nutzungsbedingungen verletzt

D

DACAN	distribution and accounting agency NATO
DACH	Deutschland-Österreich-Schweiz
DADR	Deployable air defence radar
DAEDALUS	Luftraumsicherungsoperation
Datenfunksoftware	Software zur Übertragung von Daten über Funk
Dashboard	Visualisierung von Daten
Data Loss Prevention	Maßnahme zum Schutz der Vertraulichkeit von Daten
DBMS	Datenbank Management System
DDoS	Distributed Denial of Service
DGIWG	Defence Geospatial Information Working Group
DGMN	Dynamisches gesichertes Militärnetz
DhFMO	Diensthabender Fernmeldeoffizier
DhSys	Diensthabendes System
Dienstenetz	Logische Segmentierung des Trägernetzes (Leitung, Router) Netzwerkverkehr wird für unterschiedliche Kunden über ein und dieselbe Netzinfrastruktur logisch von einander getrennt und geroutet. Für jeden Kunden wird das Netz spezifisch abgesichert und verschlüsselt. Es werden somit mehrere Kundenentze zur Verfügung gestellt.
Digitaler Zwilling	Digitale Repräsentanz eines materiellen oder immateriellen Objekts/Prozesses aus der realen Welt in der digitalen Welt
Digitalisierung	Umwandlung von analogen Werten in informations-technisch verarbeitbare Daten
dpi	Dots per inch (Drucktechnische Auflösung)
DSB	Datenschutzbeauftragter

E

E-Mail	Electronic Mail (Digitale Post)
early life support	Lösung von operativen Problemen während der Anlaufphase
EDA	European Defence Agency
EDRS	Endpoint Detection Response System
EFA	Europäisches Forum Alpbach
Ego-Perspektive	Ansicht, als wäre man die jeweilige Person
Einsatz	Tätigwerden des ÖBH zur Erfüllung seiner verfassungsgesetzlich verankerten Aufgaben lt. §2 Abs.1 Wehrgesetz
ELAK	Elektronischer Akt (unterscheide BMLV-ELAK und ELAK im Bund)
EloKa	Elektronische Kampfführung
EloKa-Truppe	Elektronische Kampfführungs-Truppe
Emotet	Computer Schadsoftware
EOW	EU Operations WAN (Europaweites gesichertes Netzwerk)
ePAT	Elektronisches Patienten Informations System

EPR	Eignungsprüfung
ERGIS	Ergänzungsinformationssystem
ESS	Employee Self Service
ETB	Elektronisches Telefonbuch
Ethernet	Kommunikationsstandard für Software und Hardware in einem kabelgebundenen Netzwerk
EU Battle Groups	European Union Battle Groups
EUBG	European Union Battle Groups 2020
EUCH	European Challenge 2020 (Cyber-Übung)
Eurofighter Typhoon	Abfangjäger des Österreichischen Bundesheeres
EUTM	European Training Mission
Explore AI	Forschungsprojekt über den Einfluss von künstlicher Intelligenz auf das Militärwesen im österreichischen Kontext
Extranet	Erweiterung des Intranets, welches nur für eine festgelegte Gruppe an Nutzern zugänglich ist

F

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

G

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

H

Hardware	Physische Komponenten in der IT
Headset	Kopfhörer mit Mikrofon
HF	High Frequency (Hohe Frequenz)
HGG	Heeresgebührengesetz
HGLLG	Hochgebirgslandelehrgang
HLogZ	Heereslogistikzentrum
HNaA	Heeresnachrichtenamt
Homeoffice	Büroarbeit am Wohnort
Hotline	Heißer Draht (Telefonischer Auskunfts- und Beratungsdienst)
HPA	Heerespersonalamt
HTBLVA	Höhere technische Bundes Lehr- und Versuchsanstalt
HTS	Heerestruppenschule
HTTP	Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol Secure
Hybride Bedrohungen	Einsatz von konventionellen und unkonventionellen Methoden durch staatliche und nichtstaatliche Akteure in koordinierter Weise, ohne die Schwelle eines offiziell erklärten Krieges zu erreichen.

I

i3VE-Smartphone	iPhones speziell gesichert für das sichere militärische Netz
Identity Awareness	Identitätsbewusstsein
IDU	Integrated Display Unit (Displayeinheit für Luftfahrzeuge)
IFC	Industry Foundation Classes (ISO-Standard zur digitalen Beschreibung von Gebäudemodellen)
IFF	Identification Friend/Foe (Freund-Feind-Erkennung)
IKDOK	Innerer Kreis der operativen Koordinierungsstruktur
IKT	Informations- und Kommunikationstechnologie (Überbegriff aller computer- und netzwerkbasierten Technologien, als auch der verbundenen Wirtschaftsbereiche)
IKT-Truppe	Truppenteil der Cyberkräfte
IKTBetr	IKT-Betrieb (Bereich des IKT&CySihZ)
IKTCyPl	Planungsabteilung IKT&Cyber für die GDLV
IKTPl	Abteilung IKT-Plan im BMLV
IMM	Informationsmodul Miliz
Inbound	Eingehend (Datenübertragung)
Incident	Vorfall
Incident Handling Process Post Incident	Bewältigung von Vorfällen
Incident Response	Reaktion auf Vorfälle
InfluxDB	Datenbankmanagementsystem
Information Protection Node	Lösung zum Klassifizieren und/oder zum Schutz von Daten
INMARSAT	Satellitenkommunikationssystem
InstFl/FlFlATS	Institut Flieger/Flieger- und Fliegerabwehrtruppenschule
Intrusion Detection and Prevention	System zur Erkennung und Verhinderung von Angriffen
IP-Netzwerke	Internet Protocol Netzwerke
IRIDIUM	Satellitenkommunikationssystem
ISK	Informationssicherheitskommission
ISMS	Information Security Management System
IT	Informationstechnologie
ITSM	IT-Service-Management
iZMS	Interoperables Zutrittsmanagementsystem

J

J5	Abteilung für Planung auf Ebene höherer Kommanden
J6	Abteilung für IKT-Belange auf Ebene höherer Kommanden
Jamming	Stören von Signalen (Störsender)

JGSWG	Joint Geospatial Working Group
JITSI	Open Source Videokonferenzsoftware

K

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

L

Labelling	Markieren/Beschriften von Daten/Objekten
LAN	Local Area Network (Lokales Netzwerk)
Legic	Chipkartentechnologie
Leonardo	Leichter Mehrzweck-Hubschrauber des ÖBH
LFG	Luftfahrtgesetz
LI/LL	Lessons Identified/Lessons Learned
Liferay DXP	PuMa-Ablöse (neues CMS)
Loadbalance	Lastverteilung in Netzwerken
Lockdown	Eine Ausgangssperre oder Absperrung bzw. Versiegelung von Gebäuden und Bereichen
LOD	Low Altitude Danger (Unterer Luftraum, Flugbeschränkungsgebiet)
Log	Dokumentationsdaten von Änderungen/Ereignissen
LOGIS	Logistikinformationssystem
Look-and-Feel	Aussehen und Bediengefühl
LOR	Low Altitude Restricted (Unterer Luftraum, Flugbeschränkungsgebiet)
LRR	Long Range Radar
LRSiOp	Luftraumsicherungsoperation
LSF	Liste staatlicher Funk
LTE	LongTermEvolution (Mobilfunkstandard 3.9)

Lu/Lu Schießen	Luft-Luft-Schießen
LuAufklESt	Luft Aufklärungseinsatzstelle
LVId	Landesverteidigungs-Identifikationsnummer
LWL	Lichtwellenleiter
LZ	Lagezentrum

M

Malware	Schadsoftware
Matchbox	Virtueller Übungsraum
MAVE	Antischadsoftware-Programm
mblGeoEt	Mobiles Geo-Element
MD	Military Domain (Netzwerk im ÖBH)
Metadaten	Strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten
Metrics Collection	Metadaten-Sammlung
Metrik	Kennzahlen/Metadaten
Memorandum of Understanding	Vereinbarung zwischen zwei oder mehreren Parteien
MGI	Militärische Geoinformation
Mifare	Chipkartentechnologie
MIGIS	Militärisches Geoinformationssystem
MilAk	Militärakademie
MilCERT	Military Computer Emergency Readyness Team
milCPS	military Cyber-Protection System (Militärisches Cybersicherheitssystem)
MilGeo	Militärisches Geowesen
milGeoVA	Militärisches Geowesen Virtual Analysis
MILIS	Militärisches Informationssystem
Miliz	Streitkräfte, die zum größten Teil/vollständig aus Wehrpflichtigen im Bedarfsfall aufgestellt werden
Milizexperten	Experten aus verschiedenen Wissensgruppen aus dem Milizstand
MIMZ	Militärisches Immobilien Management Zentrum
MISP	Malware Information Sharing Platform (Plattform für Bedrohungsinformationsaustausch)
Mission Network	Einsatznetzwerk
MissionPlanningSystem	System zur Planung von Einsätzen
MLB	Militärische Landesbeschreibung
MLU	Midlife Upgrade
Mode S/Mode 5	Modus selektiv/Modus verschlüsselt (Sekundärradar)
Motion-Sickness	Bewegungskrankheit
Mountain Training Initiative	Europäische Ausbildungsinitiative zur Verbesserung der Gebirgseinsatzfähigkeit

MoVe	Mobilität in der Verwaltung (Zentrale Steuerung aller Dienstkraftfahrzeuge der Ministerien)
Moving-Map-Systeme	Navigationssystem (Aktuelle Position wird immer in der Mitte der Karte anstatt als Koordinaten angezeigt
MPC	Mid Planning Conference
MPH FTCN	Future Tactical Communication Network
MPR	Microwave Packet Radio
MSK17	Militärstrategisches Konzept 2017
MSS	Microwave Service Switch
MTM	Mail- und Termin Management
Multiplexing	Prozess des MUX
MUX	Multiplexer analoge/digitale Selektionsschaltung, bei der aus mehreren Eingängen ein Ausgang geschaltet werden kann

N

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

O

ÖBH	Österreichisches Bundesheer (Streitkräfte der Republik Österreich, dem die militärische Landesverteidigung obliegt und nach den Grundsätzen eines Milizsystems einzurichten ist)
ObstdG	Oberst des Generalstabsdienstes
ODU	Outdoor Unit (Außeneinheit)
OE	Organisationseinheit
Öffentlichkeitsarbeit	Management der öffentlichen Kommunikation von Organisationen gegenüber ihren internen/externen Anspruchsgruppen
ofFMSys	Ortsfestes Fernmeldesystem
ofRVN	Ortsfestes Richtverbindungsnetz
OGC	Open Geospatial Consortium
ÖMKFL	Österreichische Militärkarte Flieger
Open Source	„Offene Ressource" (Software für jedermann lizenzfrei zugänglich, Quellcode öffentlich verfügbar)
OpKoord	Operationskoordination
Oracle	Amerikanisches Soft- und Hardwareunternehmen

ORF	Österreichischer Rundunk
Org	Organisation (Abteilung im BMLV)
ORGIS	Organisationsplan Informationssystem
Orgplan	Organisationsplan
ORS	Ortsfeste Radarstation
Orthofotos	Verzerrungsfreie und maßstabsgetreue Abbildung der Erdoberfläche aus Luft- oder Satellitenbildern abgeleitet
Outbound	Ausgehend

P

PAAN	PERSIS Automationsunterstütze Abrechnung von Nebengebühren
Pandemie	Neue, zeitlich begrenzte, weltweite, starke Ausbreitung einer Infektionskrankheit mit hohen Erkrankungszahlen
PersA	Personalabteilung A im BMLV
PersAppl	Personal Applikationen
PERSIS	Personalinformationssystem
PGBACKREST	Post Gre Backup Restore
Phishing	Beschaffung persönlicher Daten anderer unwissender Personen
PIONEER	InteroPerability and DIgitization Of INtelligencE GathEring PRocesses ;)
PKI	Public Key Infrastructure (System, das digitale Zertifikate ausstellen, verteilen und prüfen kann)
Plug and Play	Anschließen und loslegen
PM-Bund	Personalmanagement des Bundes mit SAP
PostgreSQL	Freies objektrelationales DBMS
PrK	Präsidentschaftskanzlei
ProofofConcept	Funktionsbeweis eines ersten Prototypen
PS-NT	Personalsysteme Neue Technologie
PTC	Pre Travel Clearance
PTMP	Point To Multi Point
PTT	Push to Talk (Direktsprechverbindung im Funksprechverkehr)
PuMa	Publish Manager

Q

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

R

Radar	Radio Detection and Ranging (funkgestützte Ortung und Abstandsmessung)
RadStlg	Radarstellung
Ransomware	Schadprogramm mit Verschlüsselungsfähigkeit

Rasterbildform	Pixelbasiertes Bild
RCID	Resistive Capacitive Identification
RCIED	Radio Controlled and improvised explosive Device (funkausgelöste improvisierte Sprengkörper)
Rechenzentrum	Gebäude/Räumlichkeit in dem/der die zentrale Rechentechnik einer oder mehrerer Unternehmen/Organisationen untergebracht ist
redundant	Mehrfach vorhanden
Release	Veröffentlichung
Reputationsdatenbanken	Datenbank vertrauenswürdiger Quellen
Requests for Change	Anfrage für Änderungen
RHEL	Red Hat Enterprise Linux (Linux basiertes Betriebssystem)
RiFu	Richtfunk
Ripple	Sammlung mehrerer Schwachstellen in einer weit verbreiteten Architektur von Kommunikationsprotokollen
RIPTIDE	Resilient Position Navigation and Timing Testing for Defence
Rollout	Veröffentlichung neuer 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
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
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

Daten & Fakten

Leistungsdaten


> 20.000 PC's bzw. Notebooks weltweit (bis GEHEIM)


> 600 Software-Produkte


> 1.000 Server


> 1.000 Smartphones


> 50.000 Datenbankentabellen


~ 90 TB Netto in zentralen Datenbankmanagementsystemen (DBMS)


~ 2.150 Switches


~ 230 Router


~ 260 ofRVN-Elemente


~ 1.700km Funkstrecken im ofRVN


~ 50 Funkfelder im ofRVN


~ 30 LWL-Strecken im ofRVN

Software und Support


Informationsversorgung von mehr als 17.000 User


Bereitstellung von über 100 IT-Services mit hoher Verfügbarkeit


Bewirtschaftung von mehr als 3,5 Mio. Personendaten


> 10 Mio. Anwendertransaktionen und 1 Mio. Geschäftsfälle pro Jahr in der Logistik


Verarbeitung von über 1 Mio. Akten und mehr als 2 Mio. Eingangsstücken pro Jahr


2022 wurden ca. 30.000 Incidents aufgenommen


Die Lösungsrate betrug 97 %


ca. 2.700 Sites und über 10 Millionen Zugriffe pro Monat im IT-Service PUMA/Intranet


Mehr als 24 Millionen Mails pro Jahr im IT-Service Mailmanagement


~ 3.000 Controller (Gebäudeautomation)


~ 50.000 Zutrittsmedien (ZMS)


Mehr als 6.700.000 tatsächliche Verpflegsteilnahmen (gesamtes ÖBH)

Personal


Besetzungsgrad: 79%


Personalverfahren: ca. 2.600

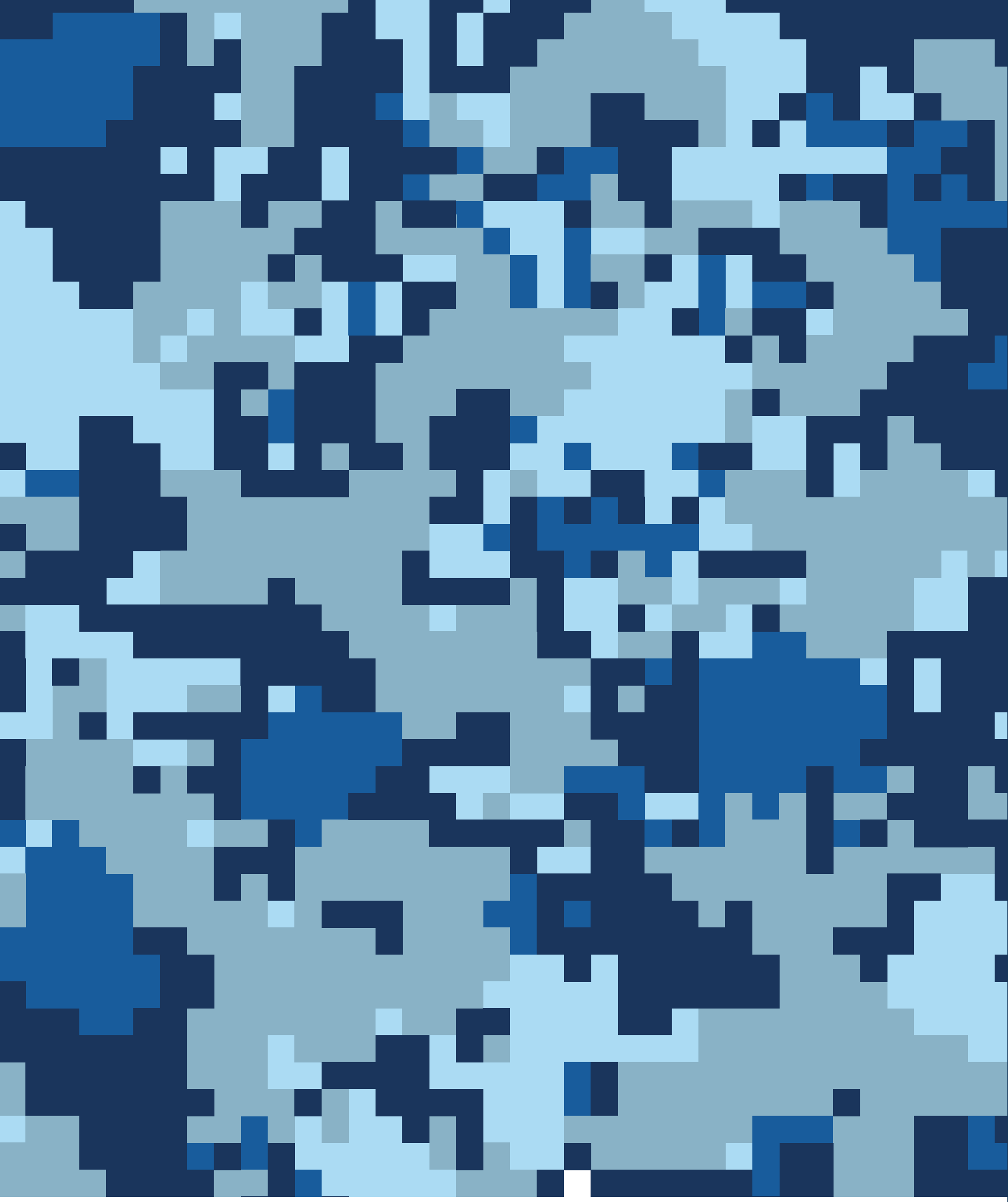
Altersstruktur: 18J - 30J = 19% | 30J - 50J = 39% | > 50J = 42%


Frauenanteil: 13%


ca. 90 neue Cyberrekruten im Jahr
Kontinuierlich ca. 30 Cyberrekruten im Einsatz

Logistik


Materialbewegungen auf VersNr Ebene: 3,4 Mio.



IMPRESSUM:

Amtliche Publikation der Republik Österreich
Bundesministerium für Landesverteidigung

Medieninhaber, Herausgeber und Hersteller:
Bundesministerium für Landesverteidigung
Roßauer Lände 1, 1090 Wien

Inhalt und Redaktion: Direktion IKT&Cyber
Idee, Konzeption und Gestaltung: Roland Pachler, Michael Kriehebauer
Layout: Michael Kriehebauer, Roland Pachler
Satz: Michael Kriehebauer, Benjamin Borenich
Fotos: Bundesheer, Direktion IKT&Cyber, soweit nicht ausdrücklich anders gekennzeichnet

Bundesministerium für Landesverteidigung