IKT&CySihZ

Leistungsbericht

2021

Cyberkräfte
connect-protect-inform

WIR SCHÜTZEN ÖSTERREICH.

bundesheer.at

UNSER HEER

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.

Inhalt

Bundesministerium für Landesverteidigung

Inhaltsverzeichnis

Bundesministerium für Landesverteidigung

Vorwort

IKT&CySihZ

Cyberforces

connect-protect-inform

cyber defence •

ensure command capabilities •

operation of all IT Services •

WIR SCHÜTZEN ÖSTERREICH.

bundesheer.at

UNSER HEER

Bundesministerium für Landesverteidigung

Kommandant IKT&CySihZ

IKT & Cybersicherheitszentrum

Sehr geehrte Leser und Leserinnen!

Letztes Jahr haben wir als „IKT und Cybersicherheitszentrum" (IKT&CySihZ) des Österreichischen Bundesheeres erstmalig einen Leistungsbericht über exemplarisch hervorzuhebende Vorhaben und Projekte im Jahr 2020 erstellt. Dies erfolgte einerseits mit der Zielsetzung, besondere Leistungen, die durch uns für das Verteidigungsressort geleistet wurden, transparent zu machen. Besonderes Anliegen war es auch darzustellen, was wir für die Weiterentwicklung der Einsatzbereitschaft unserer Soldaten im In- und Ausland beitragen. Genauso wie wir auch hinsichtlich der im Normbetrieb notwendigen Verwaltungsnotwendigkeiten unsere Leistungen abliefern. Zum anderen sollte der Leistungsbericht auch die Komplexizität unseres breiten Leistungsspektrums darstellen, aber auch die hohe Qualität, die Leistungsbereitschaft, wie die Leistungsfähigkeit unserer Mitarbeiter zum Ausdruck bringen. Natürlich war das nur ein Exzerpt dessen, was hier an Vorhaben, Projekten, Kurzfristaufträgen und normativem Tagesgeschäft geleistet wurde. Wir haben dazu viele Rückmeldungen erhalten. Der Leistungsbericht 2020 wurde durchwegs positiv aufgenommen, was uns darin bekräftigt hat, einen solchen Bericht des „IKT- und Cybersicherheitszentrums" auch für das Jahr 2021 zu verfassen.

Auch 2021 waren die Auftragsbücher des IKT&CySihZ wieder prall gefüllt und konnten entsprechend der Prioritätenreihungen abgearbeitet werden. Natürlich war das Jahr 2021 auch für das IKT&CySihZ primär durch die Covid-19 Pandemie gekennzeichnet. In einem ausgewogenen Mix, zwischen der Aufrechterhaltung der Führungsfähigkeit unseres Ressorts und Sicherstellung unseres Grundauftrages, wurde auf einen verträglichen und vertretbaren maximalen Schutz unserer Mitarbeiter gesetzt. Ich denke, dass wir diesen Spagat hervorragend gemeistert haben. Weiters haben uns die Herausforderungen im Cyberraum, wie auch die notwendigen Digitalisierungsmaßnahmen ordentlich beschäftigt.

Ich möchte mich bei dieser Gelegenheit herzlich bei den Kommandanten, Leitern, sowie den engagierten Mitarbeiter für die besonderen

GenMjr Ing. Mag. Hermann Kaponig

Leistungen im Jahr 2021 bedanken. Gleichzeitig wird auch den Vorgesetzten im Ressort für deren Unterstützung und die allfällige Anerkennung unserer Leistungen herzlich gedankt.

Auch Forschung und Entwicklung ist bei uns ein zentrales Thema. So haben wir uns natürlich auch in vielen Forschungsprojekten im Ressort, im Bund oder international zukunftsorientiert engagiert. Zudem haben wir aktiv unsere Beiträge in Strategie,- Konzept- und Fähigkeitsbearbeitungen eingebracht. Und wir haben uns in hochkarätigen Diskussionsforen oder Fortbildungen mit renommierten Experten und Unternehmen zur Weiterentwicklung im Fachbereich ausgetauscht, um uns zeitgerecht den zukünftigen Herausforderungen stellen zu können.

Natürlich haben wir auch Zeit gefunden, unsere Partnerschaft mit der HTBLVA Spengergasse weiter aufrecht zu erhalten und weiter zu entwickeln. Besonders stolz sind wir auf die Weiterentwicklung und den Aufbau eines Pools an Informationsoffizieren für die Cyberkräfte.

Was im Jahr 2021 ziemlich merklich weniger erfolgt ist, waren natürlich Covid-19-bedingt die Auslandsaktivitäten, von Übungen beginnend bis hin zu Teilnahmen an internationalen Veranstaltungen. Die eine oder andere internationale Cyberübung, oder die trinationale Interoperabilitätsübung „Common Roof" (CR21) oder die „Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX21) haben dennoch stattfinden können. Das Treffen der „EU- CIS & Cyber Commander" hat zumindest virtuell ausgetragen werden können. Letztlich hat der beträchtliche Wegfall internationaler Aktivitäten aber den Fokus auf unsere Kernaufgaben schärfen lassen.

Lassen sie mich jedoch einige Besonderheiten des Jahres 2021 explizit hervorheben.

Mit großer Freude darf ich in Erinnerung bringen, dass im Jahr 2021 für unser integriertes Team „SMN.mobile" im Zuge der Matineé „Militär des Jahres" ein Special Award 2021 an unser Team höchst engagierter Mitarbeiter vergeben wurde. Das war Anerkennung höchster Ausprägung für unsere Experten, die es mit einem Tool ermöglicht haben, dass die Ressortangehörigen mit den dienstlichen Notebooks, unter Einhaltung unserer Sicherheitsrichtlinien, auch im Teleworking und Homeoffice außerhalb des Dienstortes deren Aufträgen entsprechen konnten. Mit diesem selbst entwickelten Software-Tool konnten wir die zuvor nur in geringer Zahl im Ressort nutzbaren „Secure VPN GovNet Boxen" als Hardware-Lösung nun in großer Dimension und auch höchst kostengünstig ablösen.

Besonders zu erwähnen ist auch, dass unser „Militärisches Cyberzentrum" (MilCyZ) in der Funktion MilCERT (Militärisches Computer Emergency Readiness Team) des BMLV, bei der letztjährig erstmalig stattgefundenen EU-Übung „MIC21" (MilCERT- Interoperability Conference) höchst erfolgreich teilgenommen hat. Organisiert wurde diese neue Übungsreihe durch die European Defence Agency (EDA). Gleich bei der Premiere dieser europaweiten Cyber-Übung, konnte durch unser MilCERT der dritte Platz in der Gesamtwertung für Österreich erreicht werden. Darüber hinaus wurde die Spezialwertung "Situation Reports" durch das österreichische Team gewonnen und das MilCyZ erhielt dafür einen "Special Award" überreicht.

Ich bin stolz, solche Experten mit höchster Fachkompetenz und tollem Teamgeist in unseren Reihen zu wissen.

Ein besonderes Anliegen ist es mir, bei dieser Gelegenheit unserem vormaligen Vorsitzenden des Dienststellenausschusses, Herrn Vizeleutnant Helmut Pröll, als Personalvertreter für dessen langjährige Arbeit mit seinem Team zu danken. Unser langjähriger Dienststellenausschuss-Vorsitzender ist Mitte des Jahres in den verdienten Ruhestand übergetreten. Ich wünsche ihm für seinen neuen Lebensabschnitt, wie seinem Nachfolger Herrn Amtsdirektor Erwin Fink für sein Wirken, alles herzlich Gute.

Sehr geehrte Leser und Leserinnen! Gewähren Sie mir einen kleinen Rückblick auf die organisatorischen Veränderungen im Jahr 2021.

Mit 1. Juli 2021 wurde im Verteidigungsressort auf oberster und oberer Ebene eine weitere Organisationsänderung in Angriff genommen. So wurde in der Initialisierungsphase mit der „Generaldirektion für Landesverteidigung" (GDLV) eine neue Gliederung mit neun Direktionen für die jeweiligen Fähigkeitsbereiche aufgesetzt. Der Fähigkeitsbereich „IKT und Cyber" wurde in der neuen „Direktion 6 IKT und Cyber" gruppiert. Dazu erfolgte in der „Direktion 6 IKT und Cyber" eine Fähigkeitsbündelung nahezu aller Cyberkräfte (IKT-Truppe, Cyber-Truppe, EloKa-Truppe). Das bedeutete, dass die Führungsunterstützungsschule (FüUS), das Führungsunterstützungsbataillon 1 (FüUB1) und das Führungsunterstützungsbataillon 2 (FüUB2) der „Direktion 6 IKT und Cyber" zugeordnet wurden. Darüber hinaus wurden die BMLV-Abteilung IKT-Planung (IKTPl) und die BMLV-Abteilung Führungsunterstützung (FüU) der „Direktion 6 IKT und Cyber" eingegliedert. Zudem wurden die Joint 6-Abteilung der Streitkräfte (J6/KdoSK) und die Generalstabsabteilung 6 der Streitkräftebasis (G6/KdoSKB) der neuen „Direktion 6 IKT und Cyber" unterstellt. Als weitere neue Aufgaben wurden dem künftigen Direktor IKT und Cyber die Funktionen des „Chief Information Officers" (CIO/BMLV) und des Chief Digital Officers (CDO/BMLV) zugeteilt. Des Weiteren wurde entschieden, dass der „Direktion 6 IKT und Cyber" nicht nur die Domäne Cyber, sondern auch das Informationsumfeld mit seinen Waffengattungen Psycological Operations-Truppe (PsyOps-Truppe) und Kommunikations-Truppe (Komm-Truppe) als Aufgabe zugeordnet wird.

Im III. und IV. Quartal 2021 waren nach Anpassungen der zugeordneten Aufgaben und Angelegenheiten somit sämtliche Prozesse und Produkte im Fähigkeitsbereich zu analysieren, Duplizitäten zu eliminieren und Schnittstellen zu berücksichtigen.

Zu Redaktionsschluss dieses Berichts waren die Organisationplan-Bearbeitungen noch im Laufen. Nach Verhandlung und späterer Verfügung der Organisationspläne soll 2022 die personelle Überleitung in die neue Struktur erfolgen.

Nachdem eine unterjährige Neuorganisation begonnen wurde, habe ich mich entschieden den Leistungsbericht 2021 auch noch auf Basis der gültigen Organisation, mit Fokus auf die Organisationselemente des „IKT und Cybersicherheitszen-

trums", wie schon im Jahr 2020 aufzusetzen. Der Leistungsbericht 2022 wird nach Verfügung der Organisationspläne und der personellen Einnahme auf Basis der neuen Organisation erstellt werden. Darin werden wir dann zusätzlich auch auf die Leistungen der Abteilungen IKTCy-Planung und IKTCy-Einsatz, wie auch der Führungsunterstützungsschule und der beiden Führungsunterstützungsbataillone, eingehen.

Sehr geehrte Leser und Leserinnen! Lassen sie mich ein wenig Ausblick nehmen. Alles spricht von Digitalisierung, viele meinen damit aber lediglich den Transfer von analogen Medien in die digitale Welt. Das ist natürlich viel zu kurz gegriffen. Digitalisierung ist auch oftmals mit massiven Änderungen der Prozesse verbunden und muss letztlich medienbruchfrei technisch umgesetzt werden. Erst damit wird ein wirklicher Mehrwert für die Organisation erzeugt. Manche vermeinen, dass das dann schon die IKT-Spezialisten machen werden. Und ich sage nein – nicht nur, denn Digitalisierung der Streitkräfte für den Einsatz oder die Digitalisierung der Verwaltung für die Sicherstellung und Verbesserung des Normbetriebs geht uns alle an. Wenn wir also erfolgreich Digitalisierungsmaßnahmen setzen wollen, sind alle Fachbereiche gefordert, deren Vorstellungen einzubringen, allfällige Prozessänderungen zu veranlassen und manchmal auch die notwendigen gesetzlichen Begleitmaßnahmen dazu zu starten. Gemeinsam können wir dann technische Lösungen finden und wirkliche Digitalisierungsmaßnahmen für das 21. Jahrhundert realisieren.

MISSION

Wir sind das Herzstück der Cyberkräfte und stellen die Führungsfähigkeit des Österreichischen Bundesheeres sicher.

Wir wahren in Zusammenarbeit mit relevanten staatlichen Akteuren die Hoheit im Informationsraum mit Schwergewicht Cyberraum und verteidigen diesen im Krisenfall.

Wir gewährleisten die Verfügbarkeit, Integrität und Vertraulichkeit der Daten des Ressorts.

Wir stellen den durchgehenden Betrieb der IKT-Services und die Aufbereitung der Umwelt- und Umfeldbedingungen im In- und Ausland sicher.

Wir beraten Entscheidungs- und Bedarfsträger in allen relevanten Aufgabenstellungen der Cyberdomäne.

Expertenwissen, Innovationfähigkeit und Erfahrung ermöglichen uns, interoperable und den Sicherheitserfordernissen entsprechende Produkte bereit zu stellen.

VISION

connect

Wir stellen die Handlungsfähigkeit unserer Soldaten am digitalisierten Gefechtsfeld sicher.

Wir ermöglichen den Einsatz künstlicher Intelligenz und autonomer Systeme.

protect

Wir stellen den durchgängigen und permanenten Schutz der Informationen, Daten und Systeme für unsere Soldaten und die Angehörigen der Landesverteidigung sicher.

inform

Wir liefern signifikante Beiträge zum Wissensmanagement der Führung und zur Informationsüberlegenheit im Einsatzraum.

Bundesministerium für Landesverteidigung

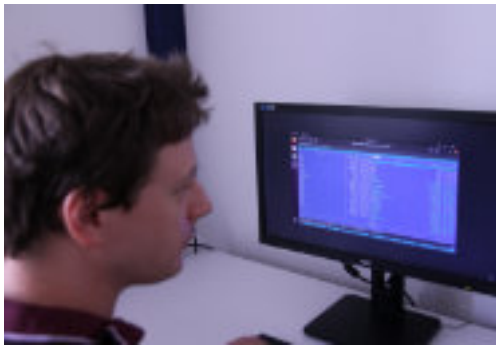
Highlights und Forschung

Bundesministerium für Landesverteidigung


IKT&CySihZ
Cyberkräfte
wir sind cyber
WIR SCHÜTZEN ÖSTERREICH.
bundesheer.at
UNSER HEER
Bundesministerium für Landesverteidigung

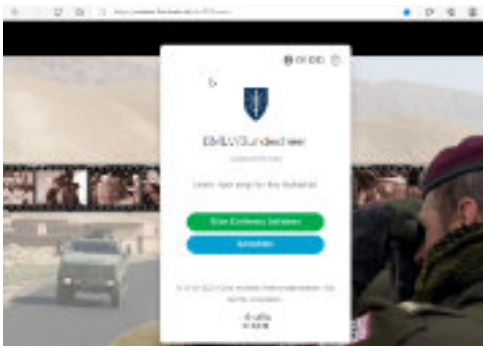
Highlights

Cyber Bedrohungen:
Cyber-Bedrohungen zählen mittlerweile zu den größten Risiken für den öffentlichen und privatwirtschaftlichen Sektor. Um für den Ernstfall gerüstet zu sein, nützen die Experten der Direktion 6 IKT und Cyber die nationalen und internationalen Trainingsmöglichkeiten. Neben nationalen Übungen zur Erprobung gesamtstaatlicher Prozesse im Falle eines IKT-relevanten Notfalles, wurde auch international sowohl auf operativer als auch strategischer Ebene die Koordination mit anderen militärischen Computer Emergency Response Teams (CERT), geübt.
(Mehr dazu ab Seite 73)

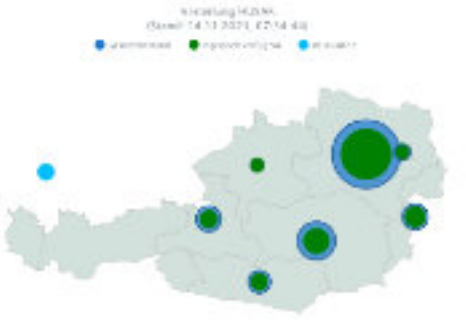


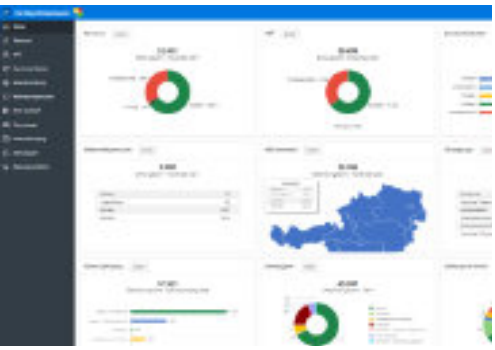
MAVE 4.0
Das MAVE-System (Multi Anti Virus Engine) ist eine Eigenentwicklung des MilCyZ zur Prüfung des Datenverkehrs auf Schadsoftware. In der Version 4.0 werden, unter anderem, erstmalig Technologien zur Anomalie-Erkennung via Künstlicher Intelligenz (KI) & Machine Learning eingesetzt.
(Mehr dazu ab Seite 74)

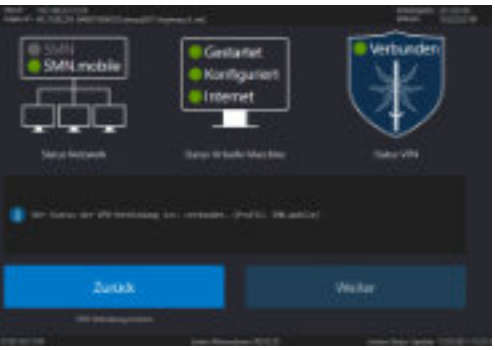
TCN:
Das Vorhaben TCN (Tactical Communication Net) wurde 2021 gem. den Planungen abgearbeitet: Im März 2021 wurde die Ausbildungsanlage an der Führungsunterstützungsschule (FüUS) installiert, sowie Referenzsysteme im IKT&CySihZ in Betrieb genommen. Im September 2021 hat an der FüUS die erste Schulung (techn. Systemeinweisung) stattgefunden. Im Oktober 2021 wurde die „Train The Trainer" Ausbildung durchgeführt und danach mit der Schulung der Operatoren an der FüUS begonnen. Ende Juli 2021 wurde die 1. Teillieferung bereitgestellt und im November 2021 wurde zusammen mit dem Auftragnehmer die Güteprüfung der gelieferten Komponenten gestartet. Die Durchführung eines umfassenden Systemtests ist für 2022 geplant.
(Mehr dazu ab Seite 58)



VKSng:
Das Jahr 2021 hat die größte Erweiterung und Umstellung für das System VKS13 seit dem Bestehen mit sich gebracht. Durch die Einführung von VKS13 am Arbeitsplatz wurde die Infrastruktur für bis zu 2.000 gleichzeitige Teilnehmer an Videokonferenzen mit den ortsfesten VKS13-Anlagen sowie untereinander geschaffen. Der nun vollzogene Umstieg auf virtuelle Konferenzräume bringt eine Reihe zusätzlicher Features mit sich (z.B.: „Hand heben", „Chat"). Mit der Einführung eines Passcode-Schutzes für alle virtuellen Konferenzräume Anfang 2022 wird dieser wichtige Schritt abgeschlossen.
(Mehr dazu ab Seite 58)







Logistische Verfügbarkeitsmeldung (LogVerfM):
Mit der logistischen Verfügbarkeitsmeldung wurde eine Möglichkeit geschaffen für definierte Systeme bzw. Geräte in einem übersichtlichen Diagramm einen raschen Gesamtüberblick über Anzahl, technischen Zustand und Standort zu bekommen.
(Mehr dazu ab Seite 46)

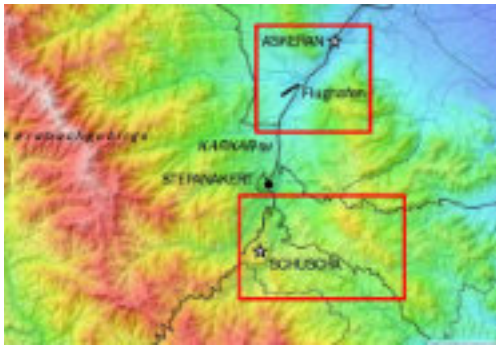
Combined Federated Battle Laboratories Network (CFBLNet):
In der STIFT Kaserne wurde der AUT CFBLNet Point of Presence mit einer NATO SECRET Zulassung in Betrieb genommen. Erstmals konnten Interoperabilitätstests aus einer Lokation in Österreich über ein hochsicheres internationales Test- und Entwicklungsnetz durchgeführt werden.
(Mehr dazu ab Seite 54)

Neues Intranet mit dem Content Management System (CMS) Liferay DXP:
Am 27.10.2021 wurde das neue Intranet basierend auf dem Content Management System Liferay DXP in Betrieb genommen. Dies stellt einen Meilenstein sowohl für die Ersteller, als auch für die Nutzer von Intranet-Inhalten dar.
(mehr dazu ab Seite 51)

Personal Management (PersMgmt)-Dashboard:
Der obersten Führung des BMLV werden mit dem PersMgmt-Dashboard aussagekräftige Kennzahlen rund ums Personal in moderner Art und Weise bereitgestellt.
(Mehr dazu ab Seite 44)

SMN.mobile:
Im September 2020 wurde das IKT&CySihZ mit der priorisierten Realisierung von SMN.mobile – der softwarebasierten Nachfolgelösung der GovNetBox – beauftragt. Im März 2021 wurde die Auslieferung plangemäß gestartet und im April 2021 abgeschlossen. SMN.mobile wurde von den Experten des IKT&CySihZ „erfunden" und entwickelt. Neben immensen Einsparungen gegenüber einer Commercial off the Shelf (COTS) Lösung bietet SMN.mobile ein sehr hohes Sicherheitsniveau (Zulassung für NATO RESTRICTED und EINGESCHRÄNKT), besonderen Benutzerkomfort und die unlimitierte Verfügbarkeit auf SMN Geräten. Durch den Wegfall von zusätzlicher Hardware (GovNetBox) konnte die Nutzung des SMN sowohl im Einsatz, bei Dienstreisen oder im Rahmen der Telearbeit wesentlich vereinfacht werden.
Das Team wurde mit dem „Special Award INNOVATION Wir machen das Bundesheer Digital" ausgezeichnet.
(Mehr dazu ab Seite 30 und 58)

Einsatz Virtual-Reality (VR)-Brille (3D Modellierung):
Den Einsatzraum in all seiner Komplexität rasch zu erfassen, ist essentiell für eine erfolgreiche Auftragserfüllung. Als zeitgemäße und zweckmäßige Ergänzung zur klassischen Karte speziell in der Geländedarstellung kommt Virtual Reality zum Einsatz.
(Mehr dazu ab Seite 97)



MilGeo-Analyse Bergkarabach (Experten IMG+LVAk):
Die gegenständliche MilGeo-Analyse befasst sich mit dem Einsatzgebiet Bergkarabach bzw. den Kriegshandlungen zwischen Armenien und Aserbaidschan im Zeitraum September bis November 2020. Im Fokus steht der Faktor Raum resp. die Möglichkeiten und Einschränkungen für die taktischen Einsatzarten Angriff und Verteidigung. Seitens IMG wurden in Zusammenarbeit mit der Aktivkomponente sowie Experten der Miliz relevante Geo-Faktoren beurteilt und als Entscheidungsgrundlage für weitere taktische Erkenntnisse aus dem Konflikt zur Verfügung gestellt.
(Mehr dazu ab Seite 96)

Gefährliche Fauna, Übergabe Datenbank an Deutsche Bundeswehr:
Am 3. November 2021 übergab nach der Einladung des österreichischen Militärattachés in Deutschland, Brigadier Mag. Christian Platzer, der Leiter des Institutes für Militärisches Geowesen, Brigadier Mag. Dr. Friedrich Teichmann, die Datenbank „Gefährliche Fauna" an die Bundeswehr. In dieser werden zahlreiche Tierarten, wie beispielsweise Schlangen, Skorpione, Spinnen, Stechmücken und deren Vorkommen in möglichen Einsatzräumen dargestellt.
Die Datenbank „gefährliche Fauna" enthält neben der Beschreibung der Tierarten auch die geographischen Aspekte und Details zu den entsprechenden Lebensräumen und Verhaltensweisen der Tiere, die für Menschen potenziell gefährlich sind. Im Kommando Sanitätsdienst der Bundeswehr VI 2 (Kdo SanDstBw VI 2) wird diese Datenbank weiterentwickelt und mit medizinischen Informationen zu den Gifttieren ergänzt.
(Mehr dazu ab Seite 22 und 96)

Ö Militärkarte 1:300 000 mit Politischen Bezirken:
Diese Sonderkarte im Format 200x100 cm beinhaltet auf Basis des maßstäblich etwas verkleinerten Kartenwerkes „Österreichische Karte 1:250 000" (das standardmäßig aus 12 Einzelblättern besteht) eine Übersicht über die Politischen Bezirke Österreichs inklusive deren Bezeichnungen auf einem Blatt.
(Mehr dazu ab Seite 107)

Ausgewählte Forschung und Entwicklung

Die hier vorgestellten Projekte bieten einen Einblick in unsere Forschungstätigkeiten, sind jedoch nur ein Auszug aus unserem breitgefächerten Forschungsengagement.

SD4MSD:
Mit dem Projektpartner AIT (Austrian Institute of Technology) sowie der Firma MUSE Electronics GmbH wurde die Umsetzung des Projekts Single Device for Multiple Security Domains (SD4MSD) gestartet. Das Forschungsprojekt wird aus Mitteln des FORTE-Forschungsprogramms der Forschungsförderungsgesellschaft (FFG) finanziert und läuft vom 01.01..2021 bis zum 31.12.2022. Ziel des Projektes ist es, einen Proof-of-Concept Prototypen zu entwickeln und diesen im Rahmen von „Feldtests" zu validieren. Die Ergebnisse dieser Evaluierung werden in einer zweiten Iteration in ein verfeinertes Systemkonzept einfließen. Ferner werden Penetrationstests durch Sicherheitsforscher durchgeführt, um die Erfüllung der nichtfunktionalen Sicherheitsanforderungen zu überprüfen.
(Mehr dazu ab Seite 62)

Explore AI:
Mit der FH-St. PÖLTEN wurde ein Forschungsprogramm mit dem Namen: „explore AI" durchgeführt. Das Thema Artificial Intelligence (AI) entwickelt sich derzeit schnell weiter und spielt in immer mehr Anwendungen eine wichtige Rolle. Für den militärischen Bereich wird AI daher in naher Zukunft sowohl neue Herausforderungen als auch Chancen bieten, jedoch ist der tatsächliche Einfluss von AI-Technologien auf das Militärwesen, und speziell dem Cyber-Bereich, derzeit noch nicht erforscht. Im Rahmen dieses Projekts wurde mit Hilfe des Werkzeugs der explorativen Szenarienanalyse untersucht, in welchen Gebieten AI großen Einfluss haben wird und wo es sich für das BMLV lohnt, wesentliche Ressourcen zu allokieren.
(Mehr dazu ab Seite 73)

Forschungsmarkttag:
Auch 2021 fand an der Theresianischen Militärakademie in Wiener Neustadt der Forschungsmarkttag statt, diesmal unter dem Motto „Digitalisierung–Vorbereitung auf künftige Einsatzszenarien". Das IKT&CySihZ war mit 3 von insgesamt 10 Forschungsprojekten vor Ort vertreten. Konkret wurden die Forschungsergebnisse folgender Projekte anschaulich präsentiert: milGeoCoopSandbox–Nutzung von Extended-Reality-Technologien als Beitrag zur umfassenden Lagebilddarstellung, GIS mit BISS–Force Health Protection und Health Promotion für den militärischen Einsatzraum Afrikas sowie EMS Eye Bots–Scannen und Analyse im elektromagnetischen Spektrum.
(Mehr dazu ab Seite 76 und 98)

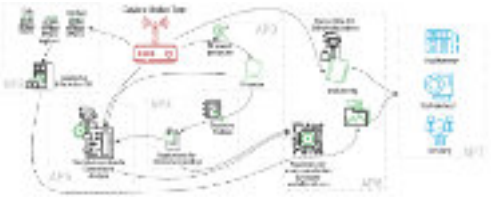
EMS EYE BOTS:
Das Projekt EMS Eye Bots beschäftigt sich mit der Forschungsfrage, wie Aktivitäten im EMS mit kostengünstigen Standardbaugruppen erfasst werden können. Damit soll in weiterer Folge eine Grundlage für die fortlaufende militärische Planung, ein Beitrag zum Cyber-Lagebild bzw. EloKa-Lagebild geschaffen werden, welches auf modularen, reproduzierbaren, kostengünstigen, frei verfügbaren und mobil einsatzbaren Komponenten basiert. Das Unterstützungszentrum Elektronische Kampfführung des Militärischen Cyberzentrums der Direktion 6 IKT und Cyber bearbeitet gemeinsam mit JOANNEUM RESEARCH dieses Forschungsprojekt.
(Mehr dazu ab Seite 76)

Forte:
Das Verteidigungsforschungsprogramm FORTE dient inhaltlich in erster Linie dem Erhalt und Ausbau der militärischen Innovationsfähigkeit. Im Gegensatz zum derzeitigen System der Forschung im ÖBH (Auftragsforschung und ressortinterne Forschung) wird FORTE als klassisches Forschungsförderungsprogramm im Bereich der Wettbewerbsforschung betrieben - mit der Besonderheit, dass das Programm in der Verantwortung des BMLRT steht und von diesem finanziert wird, während das BMLV die notwendige thematische Expertise liefert. Damit stellt FORTE eine gemeinschaftliche Umsetzungsaufgabe für BMLRT und BMLV dar.
(Mehr dazu ab Seite 55 und 73)

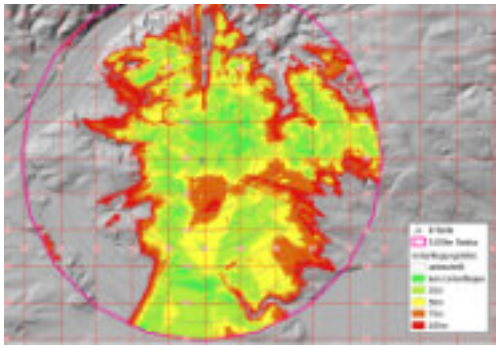
IFC Roundtrip mit Plangrafiken:
Ziel des Forschungsprojekts „IFC Roundtrip mit Plangrafiken" war es, das digitale Gebäudemodell zwischen unterschiedlichen Softwarelösungen auszutauschen und weiterzubearbeiten. Durch den IFC Roundtrip konnte außerdem die beherrschende Stellung des Marktführers gebrochen werden. Die vorhandenen Daten konnten mittels eines interoperablen Formats in eine andere Software übergeführt werden. Damit konnte deren Werterhalt sichergestellt werden. Nach Änderungen des Gebäudemodells können die einzelnen Plangrafiken wie Brandschutz-, Fluchtweg-, Bestandsplan automationsunterstützt abgeleitet werden. Grundlage ist das interoperable Austauschformat „Industry Foundation Classes". Auf dieser Basis wurden neun Bedingungen für die Nutzung des Standards formuliert. Das Forschungsprojekt hat bewiesen, dass der Roundtrip möglich ist und dass die Wertverluste vermeidbar sind, wenn Bauherren von den Softwarekonzernen die Weiterbearbeitbarkeit der erfassten Daten unabhängig von der eingesetzten Softwarelösung fordern.

OPENQKD:
OPENQKD (Quantum Key Distribution) ist ein EU-Forschungsprojekt unter der Federführung vom AIT (Austrian Institute of Technology). Durch Integration in bestehende Sicherheitsarchitekturen und Netzwerke soll das Bewusstsein für die Reife der Technologie geschaffen werden. Für das Projekt wird ein „QKD-Netzwerkknoten" inkl. Server zur Abarbeitung von Testfällen im IKT&CySihZ errichtet. Der Testpartner für das BMLV ist in diesem Projekt die Bundesrechenzentrums GmbH. Ferner wurde die Infrastruktur so ausgelegt, dass auch das Forschungsvorhaben QKD4Gov unterstützt werden kann, welches Mitte 2021 genehmigt wurde. Hierfür wird ein weiterer „QKD-Netzwerkknoten" installiert und betrieben, um eine Verbindung mit dem Bundeskanzleramt (BKA) und dem Bundesministerium für Inneres (BMI) aufzubauen.

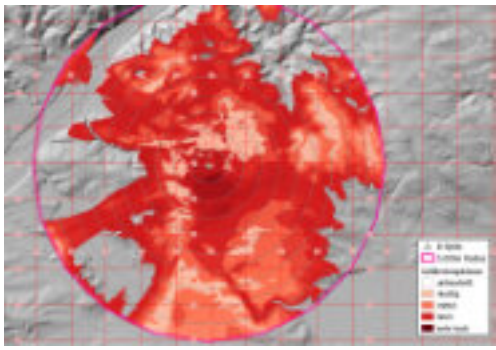
„Gefährliche Fauna":
Diese Forschungsprojektreihe des IMG und des Naturhistorischen Museums Wien, mit welcher das IMG im Rahmen des Forschungsmarkttages 2017 den Ersten Platz erringen konnte, macht auf tierische Gefahren aufmerksam. Dazu haben Expertinnen und Experten eine Datenbank für die im Einsatz befindlichen Soldatinnen und Soldaten erstellt. Dabei werden von Einzellern und parasitischen Würmern (u.a. Nematoda, Platyhelminthes), Insekten, Spinnentieren, bis hin zu Wirbeltieren wie Fischen, Reptilien, und Säugetieren unterschiedlichste Tierarten-oder -gruppen behandelt. Das Projekt konnte Ende 2020 für den Einsatzraum Nordafrika abgeschlossen werden, nun wird es auf Zentralafrika ausgeweitet. Wie relevant diese Informationen sind, werden an folgenden Beispielen sichtbar: Verletzungen und Vergiftungen durch Säugetiere und Reptilien, wie durch Giftschlangen, spielen in vielen Ländern Afrikas eine wichtige Rolle. Giftschlangenbisse können zu Lähmungen, Blutungen, Muskelspasmen oder -nekrosen, Gewebeschädigungen, Herzbeschwerden und infolgedessen auch zum Tod führen. Schätzungen der "World Health Organization" zufolge kommt es allein am afrikanischen Kontinent jährlich zu 435.000 bis 580.000 Schlangenbissen bei Menschen, wovon etwa 20.000 Fälle jährlich tödlich enden.
(Mehr dazu ab Seite 96)



FiBack:
Semiautomatic Methods for finding hidden Backdoors
FiBack zielt auf die (teil-)automatisierte Analyse kritischer IT Infrastruktur hinsichtlich vom Hersteller eingebauten Backdoors ab. Bisher war eine solche Analyse großteils manuell und daher sehr aufwendig. Ziel des Forschungsprojektes ist es, diese Analyse (teil-)automatisiert durchzuführen, um mehr Komponenten zu prüfen. Entwicklung von Techniken und Methoden, sowie neuer hybrider Ansätze, welche die automatisierten Analysen mit Expertenwissen durchführen sind Forschungsschwerpunkte, um tiefer gehende und versteckte Sicherheitslücken zu finden.



Geo-Analyse „Unter dem Radar":
In der letzten Novemberwoche 2021 fand das Vorhaben Joint Action 21 der LVAk an der TherMilAk statt. Im Zuge dieses Vorhabens wurde das mobile Geo-Element zur Deckung kurzfristiger Geo-Bedürfnisse der Teilnehmer eingesetzt. In der fachlichen Diskussion mit einem Teilnehmer des 22. Generalstabslehrgangs zum Thema Fliegerabwehr wurde eine geographische Analyse konzipiert und prototypisch umgesetzt. Dabei wird die Sichtbarkeitsanalyse, eine Standardfunktion des geographischen Informationssystems, soweit adaptiert, dass sich das Ergebnis nicht auf „Gelände wird von einem Standort aus (nicht) gesehen" beschränkt, sondern es wird jene Höhe über Grund ausgegeben, ab der ein fliegendes Objekt erkannt werden kann. In der Darstellung sind z.B. jene Bereiche orange ausgewiesen, in denen ein Objekt erst ab einer Flughöhe von 75m über Grund gesehen werden kann.



Die zweite Darstellung zeigt eine Bewertung dieser zuvor bestimmten „Unterfliegungshöhen" in Abhängigkeit der Entfernung zur Beobachtungsstelle. Dafür wird folgendes angenommen: Je näher zu einer B-Stelle sich ein Objekt unerkannt aufhalten kann, umso kritischer ist dieser dafür nutzbare Geländeteil zu bewerten. Das bedeutet z.B., dass Geländeteile mit hoher Unterfliegungshöhe, die sich jedoch weit entfernt von der B-Stelle befinden, ein geringes Gefährdungspotential für die eigene B-Stelle besitzen. In der Darstellung ist dieses Potential in vier Klassen unterteilt und je höher dieses beurteilt wird, umso rötlicher ausgewiesen.

Bundesministerium für Landesverteidigung

Bundesministerium für Landesverteidigung

Ausgewählte Vorhaben und Projekte

Bundesministerium für Landesverteidigung

IKT&CySihZ

Cyberkompetenz

connect-protect-inform

- Verteidigung im Cyberraum
- Sicherstellen der Führungsfähigkeit
- Betrieb aller IT-Services

WIR SCHÜTZEN ÖSTERREICH.

bundesheer.at

UNSER HEER

Bundesministerium für Landesverteidigung

FüAbt

Führungsabteilung

ObstdG Mag. Christof Tatschl

Mit 1. Februar 2021 habe ich die FüAbt des IKT&CySihZ übernommen und nach der ersten Beurteilung der Lage hat sich die völlig veraltete und inadäquate Struktur der FüAbt für die Auftragsfüllung zur Unterstützung eines modernen IKT und Cyber-Verbandes als größte Herausforderung herausgestellt. Die mangelnde personelle Ausstattung in faktisch allen Funktionsbereichen der FüAbt haben die Einnahme einer Truppeneinteilung notwendig gemacht. Durch diese Maßnahme konnte zumindest temporär verhindert werden, dass ganze Leistungsbereiche zeitweilig ausfallen mussten. Die weiter andauernden notwendigen Einschränkungen durch die Covid-19-Bedrohung haben die Auftragserfüllung weiter erschwert. Durch die drückende Auftragslage konnten die Mitarbeiter der FüAbt nicht in den Genuss der Schutzmaßnahme Home Office kommen, und es musste mit anderen Maßnahmen ein möglichst hoher Schutz der Bediensteten sichergestellt werden. Nur so konnte eine gesetzes- und erlasskonforme Verwaltung sowie die Auftragserfüllung des IKT&CySihZ weiter gewährleistet werden. Es ist den Mitarbeitern, die bereits unter normalen Verhältnissen oft an ihre Leistungsgrenzen gehen mussten, für ihre Leistungsbereitschaft unter den erschwerten Bedingungen der Corona-Schutzmaßnahmen hohe Anerkennung zu zollen.

Durch das Fehlen von Verwaltungselementen in den dem IKT&CySihZ untergeordneten Bereichen, sind diese nahezu vollständig von der Serviceleistung der FüAbt abhängig. Ein Ausfall der Leistung in der FüAbt hätte somit auch unmittelbar eine Einschränkung der Leistungsfähigkeit der Bereitstellungs- und Einsatzelemente zur Folge, da nun technische Spezialisten für Verwaltungsaufgaben eingeteilt werden müssten. Dieser negative Wirkzusammenhang wird vor allem im Personalbereich spürbar, der für die Aufgabenerfüllung des IKT&CySihZ die wertvollste Ressource zu verwalten hat. Obwohl das Ziel und der Weg für ein erfolgreiches Personalmanagement klar sind, konnte bisher aufgrund des strukturellen und personellen Mangels in der FüAbt, sowie einer Vielzahl an äußeren Abhängigkeiten, die von uns nicht beeinflusst werden können, der Weg nicht beschritten werden und die Personalentwicklungskurve zeigt damit im Bereich der Cyberkräfte weiter eine negative Tendenz.

Mit den am 1. Juli 2021 eingeleiteten Organisationsmaßnahmen der obersten militärischen Führung in eine Direktionsstruktur ergeben sich für die FüAbt weitere Herausforderungen. Durch das Fehlen von Bearbeitungskapazitäten auf der Direktionsebene, wird sie zumindest ein Mindestmaß an Führungsfähigkeit der Dion 6 IKT und Cyber über zwei Ebenen hinweg sicherstellen müssen. Zudem müssen, gemäß den derzeitigen Vorgaben, künftige Aufgabenbereiche InfoOps und opKomm, FüU und IWM für die GDLV wahrgenommen werden. Es wird ihr eine wesentliche Aufgabe in der Koordination des Wirkungskreises: Einsatz–Planung–Bereitstellung in der Dion 6 zukommen. Bereits unmittelbar nach der Anordnung der Überleitung musste die FüAbt wiederum die Truppeneinteilung ändern, um auch die Überleitung bestmöglich unterstützen zu können. Dabei musste das Personal wiederum äußerste Flexibilität und Anpassungsfähigkeit beweisen.

Die künftigen Aufgaben der FüAbt werden umfassend und weitreichend sein. Es gilt innovativ an die Aufgabenerfüllung heranzugehen und viel aufzubauen. Eine Herausforderung, auf die sich die FüAbt mit ihren Mitarbeitern bereits intensiv vorbereitet und der sie sehr positiv entgegensieht.

Künftige Aufgaben der FüAbt des IKT&CySihZ in der Direktion 6 IKT und Cyber: Führung und Verwaltung des IKT&CySihZ, Unterstützung der Führung der Dion 6 IKT und Cyber, gesetzes- und vorschriftenkonforme Verwaltung des IKT&CySihZ und Verwaltungsunterstützung für die Abt IKT Cyber Einsatz (IKTCyE) und IKT Cyber Planung (IKTCyPl), Einheitskommandant für die dem IKT&CySihZ zugeordneten Cyber-GWD, Planungs- und Steuerungsaufgaben für die technischen und einsatzorientierten Bereiche im IKT&CySihZ, IWM für die gesamte GDLV, einschließlich der RiLi-Kompetenz, Sicherstellen des „Services HKzl" an den vier Standorten (WALS, GRAZ, WIEN/Stift, WIEN/Hebu) zur Unterstützung der Dionen der GDLV, Sicherstellen der Basisleistungen für die Führungsunterstützung der GDLV, Leitbediener Unterstützung für die Dionen der GDLV, Planung und Steuerung der Ausbildung für das IKT&CySihZ, Verwalten der Milizexperten in der Dion 6 IKT und Cyber und Aufbau einer strukturierten Miliz im IKT&CySihZ, Aufgaben der Wirtschaftsverwaltung und Betriebsorganisation für das IKT&CySihZ inklusive Datenschutz, Controlling, Budget und Einkauf, Aufbau der neuen Fähigkeit opKomm für den operativen Einsatz der Kräfte des ÖBHs sowie der Beginn der Fähigkeitsentwicklung Bereich InfoOps, einschließlich der Führung der der Dion 6 IKT und Cyber zugeordneten Teile PsyOps.

Öffentlichkeitsarbeit

Aus Sicht der Öffentlichkeitsarbeit war das Jahr 2021 ein interessantes wenn auch ungewöhnliches Jahr.

Die klassische „Öffentlichkeitsarbeit" war durch Covid-19 auch 2021 wieder stark eingeschränkt. Dies betraf sowohl Veranstaltungen im Rahmen der ÖA, Personalwerbeveranstaltungen wie auch Firmeninformationstage.

Einige Highlights möchten wir in weiterer Folge anführen.

Matinée des Jahres 2021

Auch heuer ist es Mitarbeitern der Direktion 6 IKT und Cyber gelungen, in die engere Auswahl der herausragendsten Leistungen des Österreichischen Bundesheeres zu gelangen.

SMN.mobile - Gewinner des „Special-Awards"

Das Team „SMN.mobile", bestehend aus Experten der Direktion 6 IKT und Cyber entwickelte unter enormen Zeitdruck eine Software, die es Bediensteten des Bundesheeres erlaubt, Telearbeit mit einer gesicherten Anbindung zu verrichten. Eine Lösung, die noch dazu den militärischen Sicherheitsvorschriften entsprechen musste.

Übergabe des „Special-Awards" an das Team SMN.mobile

Nominierung als „Zivilbediensteter des Jahres 2021"

Hofrat MAS Dipl.-HTL-Ing. MSc MBA MSc Dr. Rupert Fritzenwallner war maßgeblich an der Modernisierung und Digitalisierung von Sondernetzen im Österreichischen Bundesheer beteiligt. Durch diese Leistungen platzierte er sich unter den ersten drei Nominierten der Kategorie „Zivilbediensteter des Jahres 2021".

Hofrat MAS Dipl.-HTL-Ing. MSc MBA MSc Dr. Rupert Fritzenwallner

Dienstaufsichten und Besuche

Generalstabschef beim Herzstück der Cyberkräfte

Der Chef des Generalstabes, General Robert Brieger, besuchte im Rahmen seiner Dienstaufsicht das IKT&Cybersicherheitszentrum in der Stift Kaserne in Wien.

Generalmajor Hermann Kaponig und seine Mitarbeiter gaben dem Generalstabchef ein umfassendes Lagebild über die Leistungsfähigkeit des Zentrums. Dabei standen die Leistungsbereiche mit Schwergewicht auf Anschaulichkeit, Praxisbezug und den besonderen und einzigartigen Nutzen für das ÖBH im Vordergrund.

Foto: HBF/LeonaBauer

Im Flakturm der Stift Kaserne wurde das aktuelle Thema Autarkie der Kasernen inklusive Trinkwasserversorgung und Ausfallsicherheit, aber vor allem der IKT – Struktur vorgestellt. General Robert Brieger zeigte sich „von der Bandbreite der Leistungen, dem Einsatz der Mitarbeiter und dem flexiblen Denken bei diesen komplexen Themen" beeindruckt.

Bundesministerin Tanner besucht Direktion 6 IKT und Cyber

Anlässlich des Besuches aller Dienststellen der Stift Kaserne besuchte Frau Bundesministerin Klaudia Tanner auch die neu geschaffene Direktion 6 IKT und Cyber. In aller Kürze präsentierte der Leiter der Direktion die Aufgaben und Fähigkeiten. Es folgte ein Rundgang durch die Räumlichkeiten im Bunker. Die Bundesministerin erhielt einen Überblick über die Verbindungen der IKT – Systeme des ÖBH. Das sehr präsente Thema Autarkie, wurde bei der Besichtigung eines Notstromaggregats ebenfalls ausgiebig erläutert.

Foto: HBF/Heinschink

Jung-Gamedesigner bei den Cyberkräften

Das Leben wird immer digitaler, und stellt besonders für die „Generation Z", die bereits von Geburt an mit digitalen Technologien und Medien lebt, eine Herausforderung dar. Oftmals fehlt in diesem Alter die unabdingbare Sensibilisierung auf die stets wachsenden Gefahren im Umgang mit der digitalen Kommunikation.

In einer Kooperation mit den Gamedesignern der vierten Klasse unseres Partners der HTL Spengergasse soll im Rahmen von Diplomprojekten und Diplomarbeiten das Thema Awareness durch spielerische Ausarbeitung nähergebracht werden. So sollen junge User von Beginn an im Umgang mit Kommunikationsmitteln, Sozialen Netzwerken und Datenschutz sensibilisiert werden.

Die Gamedesigner lernten bei der Kennenlern-Veranstaltung in der Heckenast-Burian Kaserne die Aufgaben der Direktion 6 IKT und Cyber genauer kennen. Großes Interesse weckten die Möglichkeiten einer Zusammenarbeit mit der Direktion 6 IKT und Cyber, die von Diplomprojekten über den Cybergrundwehrdienst bis hin zu einem dauerhaften Dienstverhältnis reichen.

Neben dem persönlichen Kennenlernen stand vor allem Ideenfindung für mögliche zukünftige Projekte im Vordergrund.

Im Rahmen der Maturaarbeiten werden im Schuljahr 2022-2023 Projekte ausgearbeitet. Ziel ist die Entwicklung von Mobile Games für alle Usergruppen, um den sicherheitsbewussten Umgang mit allen Herausforderungen der modernen Kommunikation aufzubauen.

Übungen

Die Cyber-Truppe übt im gesamtstaatlichen und internationalen Verbund

Nationale wie auch Internationale Cyber-Experten konnten sich in gesamtstaatlichen und länderübergreifenden Übungen im September und Oktober 2021 positionieren. Um für den Ernstfall gerüstet zu sein, nutzten unsere Experten der Direktion 6 IKT und Cyber die nationalen und internationalen Trainingsmöglichkeiten.

Innerstaatliches KSÖ-Cybersicherheits-Planspiel

Das Kuratorium Sicheres Österreich (KSÖ) veranstaltete in Zusammenarbeit mit dem Austrian Institute of Technology (AIT) ein länderübergreifendes Cybersicherheits-DACH-Planspiel vom 20. bis zum 21. September in Wien.

In einer IT-Simulationsumgebung der „AIT Cyber Range" kämpften acht Teams digital als technisch-operative Mitarbeiter oder strategische Spieler. Das Bedrohungsszenario war ein realistischer Cyber- Angriff auf einen fiktiven internationalen Pharmakonzern.
(Federführung MilCyZ)

Foto: Katharina Schiffl

Internationale operative Cyberverteidigungs-Übung CYBER PHALANX 2021 der EU

Das Military University Institute in Lissabon führte vom 27. September bis zum 01. Oktober die diesjährige CYBER PHALANX, eine Weiterbildung kombiniert aus Kurs und Übung, durch. 130 Teilnehmer aus der Europäischen Union und NATO wurden als Führungskräfte in operativen Planungsprozessen sensibilisiert. (Federführung IKTCyber Einsatz)

Foto: Instituto Universitário Militar

Multinationale technische Cyberverteidigungs-Übung (MLCD21) in Deutschland

Die Multi-Lateral Cyber Defense Exercise (MLCD2021) fand vom 04. bis zum 08. Oktober 2021 auf der Cyber Range des Forschungsinstituts CODE in München statt. Die Cyber-Teams wurden nicht nach Nationalitäten gebildet, sondern das Schwergewicht lag auf der Durchmischung der Gruppen nach individuellen Fertigkeiten.
(Details siehe MilCyZ S. 73-74)

Foto: CIR Bundeswehr

Common Roof 21: Übung der Cyber-Experten

Von 2. bis 19. November fand in der Schwarzenberg-Kaserne in Wals-Siezenheim die multinationale Übung "Common Roof 21" statt. Das Übungsszenario war ein Erdbeben im Rheintal in der Schweiz mit Auswirkungen auf Deutschland und Österreich.

Zur Unterstützung der zivilen Infrastruktur und zur Aufrechterhaltung des staatlichen Krisenmanagements wurde ein interoperables, militärisches Führungsnetz errichtet und gegen Cyberbedrohungen geschützt.
(Federführung APPL)

Events

LEVEL UP

Am 21. August 2021 fand im Messezentrum Salzburg zum ersten Mal das Event „LEVEL UP", eine Veranstaltung zu den Themen E-Sports und Computerspiele, statt. Aufgrund der aktuellen Covid-19 Lage, wurde das Event dieses Jahr in kompaktem Format gehalten, wobei der Veranstalter versicherte, die Ausstellungsfläche nächstes Jahr, entsprechend der Situation, zu erweitern. Bei dieser Messe standen die Interaktion und das Spielen im Vordergrund, sodass bei jedem Aussteller etwas Aktives geboten wurde.

Die Zielgruppe der TN lag zwischen 14-25 Jahren, wobei der Großteil der Besucher unter 18 Jahre alt war. Diese Altersgruppe fällt genau in die Zielgruppe des Cybergrundwehrdienstes. Die Begeisterung für Computerspiele und für einen Arbeitsplatz in der IT-Branche gehen oft Hand in Hand, somit ist der Cybergrundwehrdienst für angehende IT-Experten die Chance, deren Wissen sinnvoll einzubringen.

Auf Grund des Besuches fassen wir den Entschluss, dass eine zukünftige Kooperation und ein Auftritt bei dieser Veranstaltung großes Potenzial sowohl für die Rekrutierung für den Cybergrundwehrdienst als auch für Personalwerbung birgt.

Militärische Sicherheit

Im Kalenderjahr 2021 wurde durch den Großteil der Bediensteten die interne IKT-Sicherheitsbelehrung im Lernprogramm SITOS (Fernausbildung Bundesheer) durchgeführt. Die jährliche Belehrung der militärischen Sicherheit erfolgte – auch aufgrund der Covid-19-Situation – als Bereitstellung eines Handouts mit der nachweislichen Kenntnisnahme. Durch den stetigen Aufwuchs innerhalb der Dion 6 IKT und Cyber wurden ca. 30 Dauerpassierkartenanträge bearbeitet, administriert und in weiterer Folge den neuen Mitarbeitern ausgegeben.

Ein Schwergewicht der Tätigkeit im Referat ist die Bearbeitung von Verlässlichkeitsprüfungen. Im Kalenderjahr 2021 wurden ca. 300 Prüfungen eingeleitet und an die jeweils zuständigen Militärkommanden zur Durchführung übermittelt. Es wurden ca. 50 Security Clearances bei der zuständigen Fachabteilung beantragt sowie für 5 Firmen wurde eine Firmenprüfung vorbereitet.
Das Referat militärische Sicherheit unterstützte den Schlüsselverantwortlichen/ Schlüsselbearbeiter bei der Adaptierung der Schlüsselordnung. Erfreulicherweise gab es keine Beanstandungen bei 3 - mit Unterstützung durch die Militärpolizei - präventiv durchgeführten Suchtmittelüberprüfungen. Im Jahr 2021 erfolgte die Bearbeitung bzw. Genehmigung von ca. 250 Zutrittsanträgen mit gesamt ca. 6000 Buchungszeilen.

Es wurden 2 Sicherheitskontrollen im Bereich Wien durchgeführt. Ca. 250 Belehrungen bezüglich Verpflichtung zum Schutz klassifizierter

Informationen (Geheimschutzverpflichtung) erfolgte ebenso wie die Bearbeitung von in etwa 40 internen Vorfällen.

10 Grundregeln für die militärische Sicherheit

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

Die militärische Sicherheit ist kein Selbstzweck!

Betriebsorganisation und Wirtschaftsversorgung der Direktion 6 IKT und Cyber

Die Administration der Einkaufsagenden in den verschiedensten Spektren im IT-Bereich oder für die verschiedensten Versorgungsgüter wurde in insgesamt ca. 600 Vorgängen über Einkaufsakte, Beschaffungsanträge, Einleitungen zur Beschaffung, Kreditkarten oder BBG-Beschaffungen oder Beschaffungen von Versorgungs- und Wirtschaftsgütern aus dem zentralen und dezentralen Budget durchgeführt.

Gleichzeitig werden durch die Budgetstruktur ca. 350 gültige Service-, Bereitstellungs- oder Abrufverträge für die Sicherstellung des IT-Betriebes administriert, verrechnet und laufend aktualisiert, 750 Rechnungen, 70 Vertragsanpassungen, 900 Abrechnungen für die Leiharbeiter sind nur einige Zahlen und Fakten dazu.

Die Betriebsorganisation ist das Administrationselement für die Leiharbeiter im Zuständigkeitsbereich und musste ca. 75 externe Mitarbeitervorgänge erledigen [aufnehmen, kündigen oder verrechnen]. Die BetrOrg 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 2021, 13 Datenschutzanfragen erledigt. Dabei kam es zu keiner Überschreitung der gesetzlich vorgeschriebenen Frist von vier Wochen für die Beantwortung der Auskunft. Das Jahr 2021 war durch eine geringe Anzahl an Auskünften gekennzeichnet, der Durchschnitt der letzten zehn Jahre betrug 40 Auskünfte pro Jahr. Weiters wird auch der Aufgabenbereich Qualitätsmanagement von der Betriebsorganisation abgedeckt.

Qualitätsmanagement

Qualitärmanagement als Kernaufgabe erlaubt uns, alle organisatorischen Maßnahmen wie

- Planung, Steuerung und Optimierung von Prozessen anhand vorgegebener Anforderungen,
- die Prozessqualität, der Arbeitsqualität und damit der Produkt- und Dienstleistungsqualität

zu verbessern.

Qualitätsmanagement ist eine Kernaufgabe des Managements und eine kontinuierliche Maßnahme, die zur Verbesserung dient. Die DIN EN ISO 9000 ff. ist die international am weitesten verbreitete Norm, die Begriffe, Prinzipien und Standards für ein wirksames Qualitätsmanagementsystem (QMS oder QM-System) beschreibt und bestimmt.

Im QM wurde im heurigen Jahr begonnen, die Bereiche Personalwerbung, -ausschreibung, -einstellung und –verabschiedung darzustellen und mittels Prozessen abzubilden. In diesen vier Prozessgruppen sind derzeit 23 Prozesses definiert, die laufend ergänzt und adaptiert werden. Auch wurde die graphische Darstellung der laufenden Statistik „Telearbeit" umgesetzt und monatlich zur Information des Kommandanten fortgeschrieben.
Der Bedienstetenschutz für ca. 550 Mitarbeiterinnen und Mitarbeiter ist ein weiteres zentrales Aufgabengebiet der Betriebsorganisation und hatte dabei 70 Angelegenheiten des Bedienstetenschutzes zu erledigen [aZa mit Referat Wi].

Die Wirtschaftsverwaltung umfasst die Gebarung des dezentralen Budgets, welche die Bereiche allgemeiner Betrieb, Ausbildung, dezentrales WiGerät und Repräsentationsausgaben der Dion 6 IKT und Cyber abdeckt. Bei diesen Beschaffungsvorgängen sind die Tätigkeiten von der Angebotseinholung, Mittelbindung, Bestellung, Übernahme der Ware, Inbestandnahme und Übergabe an die Bedarfsträger durchzuführen. Hierbei handelt es sich z.B. vom einfachen Kugelschreiber, über Ersatzkomponenten IT, Ausbildungskosten, welche aus dem dezentralen Budget zu beschaffen sind, bis hin zu Wi-Gerät und Ausstattungen für die Covid-19 Schutzmaßnahmen.

Parallel dazu wurde die Teilinventur des Wi-Gerätes, für ca. 16.000 Wi-Güter in der Verwaltung der Direktion 6 IKT und Cyber [ca. 200 verschiedene Gerätetypen] durchgeführt und an die neue Organisationsstruktur angepasst.

Log&Infra

Neuorganisation Log&Infra/ FüAbt/Dion 6 IKT und Cyber

Die Umgruppierung zur Dion 6 IKT und Cyber verlangte einen breiten Blickwinkel über das IKT&CySihZ hinaus, wobei nicht nur Logistik, geteilt in Eigenversorgung (EV) und Fremdversorgung (FV), sondern auch Infrastruktur&Baumaßnahmen aller der Dion 6 IKT und Cyber nachgeordneten OEs zu beurteilen, voranzutreiben und zu begleiten sind. Diese zusätzliche Hauptaufgabe erzwang eine Umstrukturierung des Fachbereiches Log&Infra (FB Log&Infra).

Eine weitere Aufgabe des FB Log&Infra ergab sich in der neuen Organisation Dion 6 IKT und Cyber im Bereich der Fremdversorgung. Neben der Umsetzung von Maßnahmen in der Fremdversorgung und Konfigurationslogistik (FV&KonfigLog) wurde ein Teilbereich des Betreibenserlasses, Zuständigkeit für die FMSysRäume ÖBH, als Hausherr übernommen. In diesem Zusammenhang wurde die Verwaltung des Rechenzentrums ÖBH und die BÜZ der Fremdversorgung zugeordnet.

Eine weitere Maßnahme zur logistischen Konsolidierung der Dion 6 IKT und Cyber verlangte die Implementierung eines Fahrbetriebes im IKT&CySihZ. Die Nutzung, Betreuung und Verwaltung der HKf und Kfz wurde im Zuge der Fremdversorung vormals durch KdoSKB abgewickelt. Dieses breit gefächerte Aufgabenfeld, unter Beibehaltung einer äußerst schlanken Struktur, verlangte Innovation und Kreativität in der Erstellung der neuen OrgPl Struktur im Bereich Log&Infra/ Dion 6 IKT und Cyber.

Somit gilt es in Zukunft folgende Umsetzungsbereiche im Fachbereich Logistik&Infrastruktur abzudecken:

- Beratung des Direktors in Sachen Log&Infra aller Nachgeordneten.
- Eigenversorgung IKT&CySihZ
- Fremdversorgung IKTGer ÖBH
    - Konfigurationslogistik
    - Verwaltung ReZ ÖBH und BÜZ
    - Umsetzung Hausherr mit IKTBetr
- Umsetzung Infrastrukturmaßnahmen im klVbd und Nachgeordneten
- Leitung Fahrbetreib

Umsetzung Betreibenserlass in der Fremdversorgung

Der Betreibenserlass wurde 2018 von der IKTS erlassen und dem damaligen KdoFüU&CD als Hausherr zur Umsetzung zugeordnet. Nach verschiedenen ReOrg verblieb der Auftrag Hausherr in der Dion 6 IKT und Cyber und wurde in den FB Log&Infra/FV integriert. Die Zuständigkeit als Hausherr gem Betreibenserlass umfasst das Sicherstellen der ordnungsgemäßen Verwaltung von ca. 160 FMSysR (Fernmeldesystemräumen) im ÖBH die großteils in Kasernen disloziert sind. Die technische Funktionalität der FMSysR wird großteils der Dion4 /Dispo&BetrFü/Ref IKT(of) zugeordnet, die Überwachung dem IKTBetr und Verwaltung Fachbereich Log&Infra sowie Sicherheitsmaßnahmen der milSih. Seitens IKTBetr wurde eine Excel-Tabelle ausgearbeitet, die für alle MilKden zur Bearbeitung jeweils freigeschalten wurde, um den örtlichen Zustand der nachgeordneten terr Einrichtungen zu dokumentieren. Die Aufgabe als Hausherr umfasst diese Einträge mit dem örtlichen Zustand des FMSysR zu überprüfen und ggf Hilfestellung bei Problemen zu leisten. Die Umsetzung der Überprüfungen erfolgt einerseits mit der Zusammenstellung des Erhebungstrupps (ErhTrp) „Hausherr", der sich aus Fachorganen von IKTBetr, Log&Infra/FV, milSih der Dion 6 IKT und Cyber zusammensetzt und der mit StbAbt 2, 4, und 8 der zuständigen MilKden die Sachlage erörtern wird.

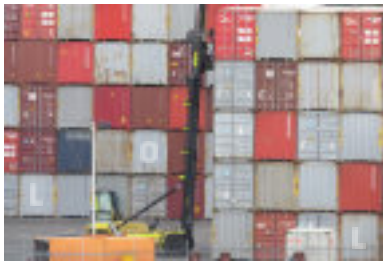
Die Leitung des ErhTrp/Dion 6 IKT und Cyber übernimmt der RefLtr FV bzw stv S4, der sich beim jeweiligen MilKdt anmelden und die Dion 6 IKT und Cyber entsprechend vertreten wird. Die Überprüfungsthemen liegen im Bereich Zutrittsberechtigung, Schlüsselordnung, bautechnischem und Sicherheitszustand, Reinlichkeit, Brandschutz, Lagerung und Prüfung Besitzbestand von Altgerät und technische Ausstattung sowie der Gesamteindruck des FMSysR.

Die Priorität der Überprüfung wird bei Störfällen in FMSysR, FMSysR der SiStufe A und den FMSysR der MilKden liegen, sowie allen FMSysR die eine essentielle Schlüsselfunktion bei einem Blackout-Szenario aufweisen.

Übernahme Rechenzentrum ÖBH und BÜZ in die FV/FB Log&Infra

Im Zuge der logistischen Konsolidierungsvorgänge seit 2016 und Adaptierungen der OrgPl Sachmittelteile der Bereiche IKT&CySihZ erging seitens IKTS die Aufforderung, die Serverbestände der 1. und 2. VE zu reduzieren. Nach Prüfung der Sachlage auf logistischer Ebene stellte sich heraus, dass es keinen Überhang an Servern gab, da die Serverbestände des Rechenzentrum ÖBH dem IKTBetr zugeordnet wurden und somit über dem Bestand des OrgPl SMTl lag. Weiters wurden die Bestände der Serverfarmen seit Beginn Aufstellung HDVA, aufgrund ständiger Veränderungen und Wechsel der Sys sowie Zugriff verschiedener Dienststellen, nie ordnungsgemäß erhoben.
Eine Inventur wurde nie durchzuführt. Der logische Schluss der VersFü war es, das ReZ ÖBH in die Verwaltung der FV zu übernehmen, entsprechende logistische Fachorgane über Jahre auszubilden, Bestandserhebungen laufend durchzuführen und 2022 mittels Inventur einem verantwortlichen IKT- und logistisch ausgebildeten Fachorgan zur Verwaltung zu übergeben.

Mit dieser erstmaligen Inventur erfolgt 2022 eine klare Trennung der Serverbestände IKTBetr und dem ReZ ÖBH sowie der BÜZ. An dem Vorhaben wurde seit 2019 geplant, ausgebildet, Gerätebereinigungen, Abgaben und Bestandsaufnahmen durchgeführt, mit dem Ziel 2022 die Inventur durchzuführen.



Infrastruktur

Der Aufgabenbereich Infrastruktur im FB Log&Infra teilt sich in Bedeckung von Infra-Maßnahmen im IKT&CySihZ sowie in der Dion 6 IKT und Cyber. Einerseits sind Bedarfe von KLBM (Kleinbaumaßnahmen) wie Aus-malen, Behebung defekter Jalousien oder SchließSys-Berichtigungen im klVbd abzuarbeiten, andererseits erstreckt sich der Wirkungsbereich über Großkasernen von WIEN bis LALE zum MilGeo Museum – alles im Bereich des IKT&CySihZ. Nach Einnahme der Organisation der Dion 6 IKT und Cyber erweiterte sich der Aufgabenbereich auf die Garnisonen der nachgeordneten Vbd und deren Baubedarfe.

Die aktuellen Projekte, die 2022 umgesetzt werden, umfassen im Bereich IKT&CySihZ die Fertigstellung der Adaptierung der Radarhalle HEBU, die MunKastenanlage im Bereich Obj6 STIFT Kas, der Bau einer Waffenkammer im Obj 5 und Ausbau des Führungstraktes der Dion 6 IKT und Cyber im Obj4 STIFT Kas.

Personal

Personalgewinnung und Personalentwicklung stellen im Bereich der Cyberexperten seit jeher eine große Herausvorderung dar. Es konnte im Jahr 2021 zwar ein leichter Anstieg des Personals erreicht werden (Aufnahmen 66, Abgänge 49), jedoch vorallem im Bereich der Cybersicherheit ist der Arbeitsmarkt heißer umkämpft denn je.

Die Vielfältigkeit der Dienstverhältnisse und Verträge und die große Personalfluktuation stellen extreme Herausforderungen dar, denen mit einem besonderen Maß an Personalbetreuung, optimalen Personalprozessen und intensiver Personalwerbung entgegengetreten werden muss. So wurde auf Eigeninitiative eine Riege an Cyber-Informationsoffizieren herangebildet, die besonders zu den einschlägigen Bildungseinrichtungen Kontakt halten.

Eine der Säulen der Personalgewinnung ist der Cybergrundwehrdienst. Im Jahr 2021 waren in 3 Einrückungsterminen gesamt 63 Cyber-Rekruten in den unterschiedlichsten Aufgabenbereichen des IKT&CySihZ im Einsatz.

Großer Wert wird auch auf die Ausbildung gelegt, so wurden zu IT-Ausbildungen im In- und Ausland 273 Teilnehmer entsendet, die sich insgesamt 443 Manntage in Ausbildung befanden.

Die Miliz wird in Zukunft eine immer wichtigere Rolle spielen. Es sind bereits hochkarätige Fachkräfte in militärischen Funktionen beordert, die verstärkt zur Auftragserfüllung herangezogen werden sollen. Hier ist vorallem Expertise bei Cyber-Vorfällen und eine personelle Verstärkung zur Erreichung einer längeren Durchhaltefähigkeit von großer Wichtigkeit.

Fachbereich Steuerung

Das IKT-Nutzungsmangement startete mit gleichem Umfang von 3 Personen ins Kalenderjahr 2021. Die Aufgaben wurden zunächst gemäß Vereinbarung bei der Teamarbeitsbesprechung vom 19.11.2020 auf alle 3 Bediensteten verteilt. Gemessen am Aufgabenumfang 2020, der bereits 2020 sehr intensiv beanspruchte, war 2021 im nachhinein betrachtet noch umfangreicher in den Aufgabenfeldern, was auf eine ständig steigende Kumulation der Aufgaben bis Jahresende zurückzuführen war.

Durch die unstabile Situation im Bereich der Leitungsebene war der Aufgabenumfang möglichst breit zu verteilen und die autonome Abwicklung vieler einzelner Schritte bei Vorhaben und vor allem Planungen zur Umsetzung zu unterstützen. Nachdem die Weiterführung der ursprünglich geplanten Struktur der Leitungsebene im IKT&CySihZ bereits mit Ende des III. Quartals 2020 durch die weiteren Planungsschritte zu „Unser Heer" ausgesetzt wurde, sollte im I. Quartal 2021 ein einsetzender Prozess zur Synergiegewinnung in der Führungsabteilung die Agenden der Führungsgrundgebiete verschmelzen.

Damit wurde das IKT&CyNuMngt in der Konfiguration als Fachbereich Steuerung mit dem bestehenden Referat Ausbildung gekoppelt, um die FGG 3,5 und 7 und die Umsetzung der Jahresplanung 2021 einigermaßen ausreichend bedecken zu können. Davon unbenommen wurden die weiterführenden Kernziele in der Konzeption im IT-Servicemanagement sowie Ver-besserungsmöglichkeiten des Vorhabenportfolios, wenn auch mit weniger Nachdruck als Ende 2020 geplant, verfolgt. Wesentliche Defizite mussten dafür in der vorläufigen Aufgabenum-

setzung für die Organisationsentwicklung in Kauf genommen werden, dieser Zustand sollte sich aber mit Ende des II. Quartals 2021 schlagartig ändern. Die danach einsetzende Periode bis Jahresende war im Wesentlichen von einer konstanten, maßgeblichen Begleitung der Überleitung in der Direktion 6 IKT und Cyber geprägt und verlangte eine besondere Konzentration auf die Aufgaben. Vor allem In der ersten Jahreshälfte wurden viele kleine konzeptive Arbeitsschritte mit Schwergewicht im I. Quartal in Wochenklausuren erledigt. Die erhoffte Reduzierung von Nebenaufgaben ist 2021 trotz vehementer Neuorientierung nicht eingetreten!

Insgesamt konnte das IKT&CyNuMngt dadurch seinen wichtigsten Aufgaben 2021 durch noch höhere Konzentration auf die Kernthemen und mit Inanspruchnahme wesentlicher Mitleistung vor allem der technischen Bereiche und des IMG zufriedenstellend bewerkstelligen.

Durch die geplante Umstrukturierung im Fachbereich Steuerung wird es zu einem wesentlichen Leistungsschub kommen.

Aufgaben und Leistungen

Digitales Handbuch

Vorhaben	Zeitraum 2021	Übungsraum	Stärke Max.	svKdo	Szenario/Zweck/ Fähigkeit	COI	Dienstaufsicht
Cyber Defence Exercises			50	KdoSKB	milLV - Abwehroperation im Cyber-Raum	DCOI	KdoSKB
CROSSED SWORDS	Jan/Feb tbd	LVA	3				
LOCKED SHIELDS	Apr tbd	EST	8		Führungsunterstützung (Computer Network Ops)		
CYBER EUROPE	1.HJ tbd	BEL	4				
CYBER PHALANX	05.04-09.04	PRT	15		Entsandt wird der Beitrag Übungsleitung, die Training Audience milCERT verbleibt in AUT		
MILCERT conference 2021 (MIC 2021)	19.01-21.01	FRA	8				
MULTILATERAL CYBER DEFENCE EX	Feb tbd	DEU	4				

Vorhaben zu Inlandsaufgaben im Ausland

Beispielhaft werden folgende Teilaufgaben angeführt:

Einsatzvorbereitung und Übungen

Ausgehend von den Bearbeitungen Ende 2020 wurden 2021 zunächst kontinuierlich die eigenen Aufträge der Jahresplanung in Anlehnung an den Vorhabensplan KdoSKB verfolgt.

Zur besseren Abwicklung der Geschäftsvorgänge für die Übungsvorhaben im Rahmen der Einsatzvorbereitungen wurde das bereits 2020 geplante digitale Handbuch erstellt. Das Handbuch war für die interne Bearbeitung im IKT&CySihZ gedacht und sollte dem jeweiligen Projektleiter die ökonomische Bearbeitung der aktenmäßigen Aufgaben im Rahmen der jährlichen Übungsplanung für die angeordneten Auslandsübungen erleichtern. Durch die Überleitung in die Direktion 6 IKT und Cyber wurden die Agenden der Einsatzvorbereitung im IKT&CySihZ schließlich im IV. Quartal 2021 offziell dokumentiert an IKTCyE zur Weiterführung übergeben.

Ausgangsbasis

Der Hauptaufwand 2021 konzentrierte sich auf meist sehr kurzfristige Umsetzungsbefehle und Erfahrungsberichte sowie Entsendeweisungen. Die Planungen dazu gestalteten sich wesentlich schwieriger als die Situation 2020, wo ab dem Ende des I. Quartals längere Zeit Stillstand vorherrschte und alle Bearbeitungen infolge der Absagen im 1. Halbjahr weitgehend finalisiert wurden.

Kernziele Leistungsportfolio und Steuerung

Die Beiträge zur Erfüllung der Leistungsaufträge Im Rahmen der Streitkräftebasis wurden über das IKT&CyNuMngt bis Mitte 2021 weitergeführt und in monatlicher Ausfertigung an KdoSKB im Detail übermittelt. Mit der einsetzenden Überleitung wurden die eigentlichen Bearbeitungen nicht mehr schlagend, waren aber als eine gut fundierte Grundlage für die weiteren Arbeitsgänge in der Festlegung der Aufgaben und Leistungsziele zum begleitenden Controlling verwendbar.

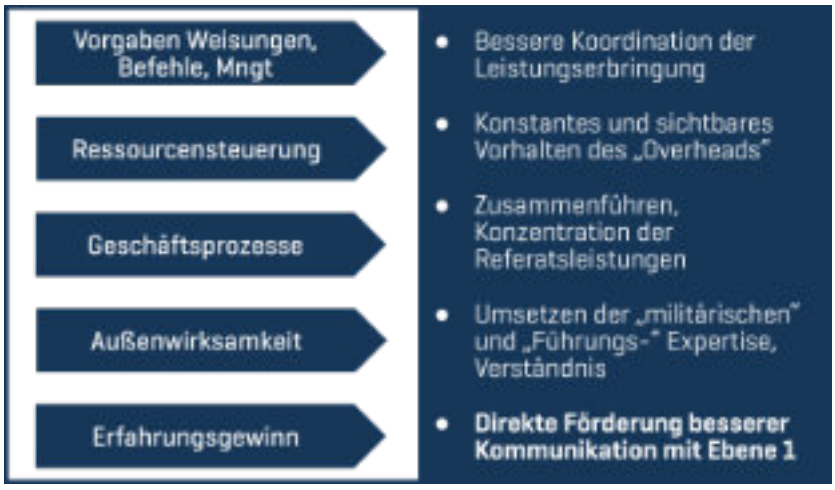
Der Hauptwirkungsbereich der Analysen, die sich immer stark auf die Dokumentation der Leistungsfähigkeit, sowohl in der Serviceentwicklung als auch im laufenden Betrieb stützten, bedurfte aufgrund der Entwicklungen auch 2021 ständiger Neubeurteilungen, die weit über die Wirkungssteuerung hinausgingen und auch im Gesamtblick ständig auf die ganze Organisationsentwicklung gerichtet waren.

Koordinierung Leistungsumfang; Steuerung aller Vorhaben, Ausbildung, Üb, EVb

Dabei wirkte immer die Problematik einer ausgewogenen Schichtung der Aufträge mit, um das ständige Ressourcenfehl im Personalbereich ausgleichen zu können. Die Zusammenlegung IKT&CyNuMngt und Referat Ausbildung zum Fachbereich Steuerung erzeugte zumindest für den Zeitraum eines Quartals eine äusserst kompakte Arbeitsbasis, die bestätigte, dass zwei funktionierende Elemente sofort miteinander sehr gut wirksam werden konnten.

Für die technischen Bereiche war auch das Jahr nach der Verfügung der neuen Struktur alles andere als ein Booster. Der Personalaufwuchs war sehr überschaubar und im Jahresvergleich angesichts der angepeilten Ressourcenziele schlichtweg mehr als bescheiden.

Daraus entwickelte sich ein Rückstau in der Serviceentwicklung, der in einen konstant steil ansteigenden Arbeitsaufwand mündete, die Unzulänglichkeiten durch verzögerte Lieferungen waren dazu nicht hilfreich, sondern eher dazu geeignet, diesen Umstand noch weiter zu verstärken.

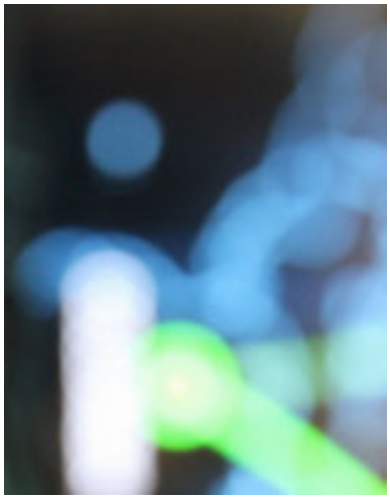


Für 2021 maßgebliche Arbeitsdokumente und Arbeitsfelder, die bearbeitet wurden:

- Wirkungscontrolling Jahresbericht 2020 für Detailbudget 524
- Fortführung Leistungsauftrag 2021 mit Kennzahlensteckbrief und Weiterentwicklung zu Leistungszielen in der Ebene 1 als zugewiesener Leistungsumfang je Bereich und IMG
- Beitrag zur Wirkungsorientierung im Ressort für den spezialisierten Personalaufwuchs Cyber
- Ressourcen-, Ziel- und Leistungsplan 2022 für Detailbudget 524 mit Kennzahlensteckbrief
- Einsatzvorbereitung Planung 2022 bis 2025 gemäß Übungsprogramm mit 7 Meldeformaten (technische Übungen mit Federführung IKT&CySihZ) und konzeptioneller Aussicht für die Übungsserie ASDEM
- Erhebung und Antrag zur Ausbildungsunterstützung 2022
- Meldesystematik der Einsatzbereitschaft Kernfähigkeit im IKT&CySihZ
- Anordnungen und Anlageevidenz der Morgenlage und Wochenmeldungen im IKT&CySihZ bis zum Juli 2021 zur Überleitung an IKT&Cyber-Einsatz
- Entsendeweisungen und Umsetzungsbefehle zu den

technischen Übungen im Ausland

- Anordnung der Beiträge zu EUBG 2020/2 und 2021/2
- Wehrpflichtigenkontingentierung Vorlage der Wehrpflichtigenbedarfserhebung 2022 bundesweit für Cyber-GWD und Anteile Funktions-GWD für IKT&CySihZ
- Beitrag zur Unterstützung des Masterplanungsprozesses 2021/2022
- Anordnungen zur Umsetzung Vorhabensplan Streitkräftebasis 2021 bis 2023 und zur Masterplanung IKT&CySihZ 2021 und 2022 bis 2025 inklusive Terminmanagement
- Ganzjährige Weiterführung des Vorhabenportfolios im IKT&CySihZ
- Beiträge und Konzeptionen zu Mitgliedschaften, nationalen Kooperationen und internationalen Kooperationen (PESCO, CARD, MCDC, SCC, EUMS, FNC, EDA, NATO/PfP/PARP Zyklus, C3B Beiträge, Initiativen, Assessments, Defense Talks, NATO-Konzepte), Akten zu internationalen und nationalen Abkommen und Vereinbarungen inklusive der erforderlichen Grundlagenerhebungen und Dokumentationen dazu
- Koordinierungen und Mitarbeit im Projekt CBRN SaaS im Zuge der Expertengruppe TQC
- Improvement – Vorgang zur Ablaufregelung in den Aufgabenfeldern „Steuerung von Vorhaben" und „Milizabläufe"
- Vorgabe einer Ausrichtung zum Servicekatalog und zur Weiterentwicklung Serviceportfolio
- Erhebung und Erstellung der halbjährlichen Zwischenberichte zu den Forschungsprojekten
- Mitwirkung an der Kommandantenklausur zur Erstellung Vision/Mission im Februar 2021 und an den Ergebnissen der Herbstklausur 2021 der Direktion 6 IKT und Cyber
- Mitwirkung am Beitrag zur Lehrveranstaltung „Militärstrategische Führung und Lagebild" im Rahmen des Fachhochschul-Masterstudiengangs 2020 (Generalstabsausbildung)
- Übernahme des Überleitungssekretariats für die Überleitung der Direktion 6 IKT und Cyber
- Bearbeitung der Aufgabenanalyse und Beiträge zur Geschäftseinteilung/BMLV und Dienstanweisung Generaldirektion Landesverteidigung
- Bearbeitung des begleitenden 1. bis 4. Controllings für die Überleitungsphase ab Juli 2021 und dazu notwendige laufende Abstimmungen
- Beginnende Erhebung und Ablaufkoordination zur Jahresplanung 2022
- Mitwirkung am Leistungsbericht 2021



„Weiterbildung und Wissensmanagement GROSSgeschrieben"

Für die externe Ausbildung 2021 wurden für die Bediensteten mehrere Module ausgewählt, die aber nicht alle angesprochen werden konnten. Im Bereich des Servicemanagements konnte der Referatsleiter in mehreren aufeinanderfolgenden Modulen die Ausbildung zum Professional Manager für ITIL 4 abschließen.

Diese wirklich sehr anschaulich vermittelten Kurse für ITIL 4 Foundation Bridge (Modul zum Umstieg auf ITIL 4), Create, Deliver & Support (CDS), Direct, Plan & Improve (DPI), Drive Stakeholder Value (DSV) und High Velocity IT (HVIT) vervollständigten eine umfassende Sichtweise auf die aktuellsten Inhalte und Trends im IT-Servicemanagement.

Foto: Bundesheer/HARALD MINICH

Durch die direkte und stärkere Befassung mit Aufgabenstellungen in den Modulen, zu teilweise selbst gewählten IT-Themen der Teilnehmer, wurde es ermöglicht, alle Phasen in einer durchdachten Logik zu durchwandern und in einem kompakten Rahmen alle notwendigen Schritte im Servicemanagment nachvollziehen zu können.

Als „flankierende Verstärkung" zu diesem Thema wirkte das Modul zur „TOGAF Foundation" mit theoretischer Schulung und praktischen Beispielen zum Framework der Unternehmensarchitektur und die Architekturentwicklungsmethode in den gesamten Phasen. Vor allem im Bereich der Interoperabilität und der fähigkeitsbasierenden Planung stellt dieses Instrument viele neue Aspekte zur Verfügung. Im Kontext zum Risikomanagement wird der bereits bekannte Ansatz aus ITIL 4 mit dem Hauptfokus betrachtet, diese Risiken zu identifizieren, zu klassifizieren und zu mindern.

Foto: Kommando Luftunterstützung

Diese Inhalte und ein weiteres Modul zu Vertragsgestaltung, Haftung und Servicebestimmungen im Bereich des IT-Outsourcings waren neben der Vermittlung der ITIL-Kenntnisse für die eigenen Bearbeitungen im ITSM und zum besseren Verständnis im IT-Betrieb unterjährig für eine weitergehende Betrachtung immens hilfreich.

Durch die weitreichende Vernetzung und die sichtbare Steigerung der Teilnahme an Forschungsprojekten und internationalen Kooperationen 2021 wurde die Koordinierung und Dokumentation dazu noch wichtiger und unvermindert weitgeführt. 2021 waren die Bereiche an 29 Forschungsprojekten maßgeblich beteiligt, davon konnten trotz Covid-19 bedingten Verzögerungen 10 Projekte abgeschlossen werden.

Um wirklich eine Wissens- und Forschungsbasis zu haben, die es erlaubt, redundante Beteiligungen vermeiden zu können oder zeitgemäß die richtigen Trends im Forschungsmanagement einzuschlagen, sind die Arbeitsplätze in der neuen Struktur der aktuellen Version 4 bei weitem nicht ausreichend.

Insofern war zumindest ein Synergieeffekt mit der Hereinnahme des Informations- und Wissensmanagement mittelbar und unmittelbar in die Führungsabteilung für die Bearbeitungen in der Organisationsentwicklung der Direktion 6 IKT und Cyber spürbar.

„Zusatzpakete" Services, Projekte, Organisationsentwicklung und operative Absteuerung

In noch mehr Teilgebieten als 2020 lieferte der Fachbereich Steuerung 2021 Leistungen für Dienstellen außerhalb des IKT&CySihZ:

Vorhabensverantwortung für Projekt „EU-Ops-WAN/Anbindung interne Infrastruktur (Phase I)" im IKT&CySihZ, begründet durch die deutliche Überschneidung der Ressourcenleistungen über mehrere Bereiche, wobei ein Großteil der Aufgabenstellung an Applikationen für dieses Vorhaben zeitweilig direkt an den Bereich Applikationen übertragen wurde, Ausübung der Serviceverant-

wortung für ASECOS I/Fähigkeitserhalt inklusive der Inbetriebnahme einer weiteren Zelle bei VPol (ASECOS 20), Abschluss der Umstellung auf Windows 10 für 2 weitere Zellen und die beginnende gerätemäßige Vorbereitung der Inbetriebnahme der Zelle im Jagdkommando für das I. Quartal/2022, ressortweite Druckerauswertung der jährlichen Zählerstände für alle Multifunktionsgeräte mit Klickvertrag; dazu wurde zusätzlich intern unterjährig der Auftrag zur Prüfung der Scripts für eine Ausweitung mit Schnittstelle zu DGMN erteilt, weil dadurch der zukünftige Aufgabenumfang mittels zusätzlicher Automatisierung deutlich reduziert werden könnte, die zeitweise erforderlichen koordinierenden Tätigkeiten im Rahmen der Expertengruppe CatB-Projekt „CBRN SaaS" (Expert Group Testing, Qualification and Certification; Technological Demonstrator for the Chemical, Biological, Radiological and Nuclear Surveillance as a Service) mit ab Mitte II.

Quartal wirksamer Inanspruchnahme der Vertretung des Vorsitzenden der Expertengruppe und Übernahme des Überleitungssekretariats für die Direktion 6 IKT und Cyberund gleichzeitig gemeinsame Überleitungsverantwortung mit dem CTO für das neue Organisationselement „IKT-Cyber-Bereitstellung", das im Laufe des Prozesses nach neuen Vorgaben des Steuerungsgremiums in der Planung auf den Kernbereich „Referat IKT-Cyber-Bereitstellung & Steuerung" und ein optionales Element „Referat Architekturmanagement" reduziert wurde.

„Wir haben unsere Lektion gelernt"

Für die gesamte konzeptionelle Arbeit und inhaltliche Neuorrientierung in der Direktion 6 IKT und Cyber wurde 2020 und 2021 weiterführend bereits sehr fundierte Grundlagenarbeit geleistet, die den Stellenwert für das Segment „IKT & Cyber Bereitstellung" mehr als ausreichend dokumentierte. Im gegenwärtigen Status bedarf es noch einer Loslösung von Nebenaufgaben (z.B. Projektverantwortlichkeiten, Serviceverantwortung, operative Absteuerungen), um die volle Arbeitsfähigkeit auf die Kernthemen zu richten, für die dieses Organisationselement eigentlich prädestiniert sein sollte.

Indirekt wird die Leistung auch dann merkbar steigen, wenn in der IKT- und Cybertruppe der technischen Bereiche die Unterstützung zum Personalaufwuchs durch die Ressortführung endgültig unterstrichen wird.

Die Verzögerungen im Personalaufwuchs führten zwangsläufig zu einer Verzögerung der Leistungerbringung und zu einem Rückstau in der Serviceentwicklung. Nach der Überleitungsphase und Konsolidierung wird das neu geschaffene Referat IKTCyBstg&Steuerung in der Lage sein, die proaktiven Bereiche des IKT&CySihZ in der Planung zu unterstützen und so auf diese Weise zur raschen Auftragserfüllung beitragen.

Wie in allen anderen maßgeblichen Elementen der Leitungsebene der Direktion 6 IKT und Cyber wurden auch im IKT&CyNuMngt Leistungen im 2. Halbjahr zwangsläufig zurückgeschraubt, um die erforderliche Arbeitsbereitschaft weiterhin verfügbar zu haben und bereits ausgewogene Arbeitsabläufe durch planbare „Schablonen" und „Blaupausen" zu unterstützen und notwendigenfalls mit Zuversicht delegieren zu können.

IKT&CySihZ

Cyberkräfte

wir kämpfen digital

- Verteidigung im Cyberraum
- Sicherstellen der Führungsfähigkeit
- Betrieb aller IT-Services

WIR SCHÜTZEN ÖSTERREICH.

bundesheer.at

UNSER HEER

Appl

Bereich Applikationen

Nach dem vom Covid-19 geprägten Jahr 2020 konnte sich der Bereich Applikationen im folgenden Jahr voll und ganz auf das Kerngeschäft konzentrieren. So konnte 2021 der Mitarbeiterstand ausgebaut und wesentliche innovative Vorhaben umgesetzt werden, welche ein hohes Potential für die Digitalisierung wesentlicher Geschäftsprozesse des Verteidigungsressorts aufweisen.
Ein Hauptaugenmerk lag in der Stabilisierung des Betriebes der einsatzwichtigen und unternehmenskritischen Applikationen durch die Umsetzung von Change Requests der Anwenderfachabteilungen und auf Anpassungen aufgrund von gesetzlichen Änderungen. Weiters wurden Technologieanpassungen in den Großanwendungen PERSIS und LOGIS durch das Redesign der graphischen Oberfläche vorgenommen und zahlreiche neue Funktionalitäten im BMLV-ELAK implementiert. Am Ende des Jahres konnte der in die Jahre gekommen PUMA durch das innovative Content Management System Liferay DXP zur Erstellung und kollaborativen Nutzung von ansprechenden und zeitgemäßen Intranet Inhalten abgelöst werden.

Besonders hervorzuheben sind wesentliche neue Anwendungen mit einem hohen Mehrwert für Entscheidungsträger und Bedarfsträger im Fachbereich. Mit dem PersMgmt-Dashboard können aktuelle, aussagekräftige Personalkennzahlen unter Einhaltung der erforderlichen Sicherheitsstandards generiert werden. Im Rahmen der logistischen Verfügbarkeitsmeldung kann der jeweilige Materialerhaltungszustand einsatzwichtiger Systeme und Geräte nach Organisationseinheit und Lokation zugeordnet und abgefragt werden. Mit der Implementierung des IKT-Servicekataloges ist es erstmal möglich, alle Services in einer Webanwendung zu erfassen, zu bearbeiten, abzufragen und die Abhängigkeiten automatisiert darzustellen. Ende des Jahres konnte das Combined Federated Battle

HR Dipl.Ing. Gerald Hofmeister

Laboratories Network im Rahmen eines internationalen Joining Events die Final Operational Capability erreichen. Damit ist die Teilnahme an Verifikations- und Validierungsvorhaben im Rahmen der Federated Mission Networking Initiative und anderen internationalen Testevents möglich.
Es wurden mehrere Digitalisierungsvorhaben eingeleitet, die richtungsweisend sind und eine neue Ära der Servicebereitstellung für einen erheblichen Kundenkreis einläuten. Durch die Digitalisierung der Behördenverfahren werden medienbruchfreie, durchgängige digitale Verfahren vom Bürger zur Militärbehörde geschaffen. In einem ersten Ansatz wird der Geschäftsprozess Familienunterhalt und Wohnkostenbeihilfe umgesetzt. Mit der bargeldlosen Verpflegsteilnehmerabrechnung, der „digitalen Küche" und dem Projekt „Smart Waste" werden Warenwirtschaftssysteme, Geräte und Abfallsysteme miteinander verknüpft und mittels KI Optimierungspotential identifiziert. Im Rahmen des Projektes „Industry Foundation Classes" Roundtrip wurden die Voraussetzungen geschaffen, digitale Gebäudemodelle zwischen unterschiedlichen Softwarelösungen auszutauschen und weiterzubearbeiten. Damit konnte die beherrschende Stellung des Marktführers gebrochen, und der Werterhalt für das Ressort sichergestellt werden.
Der Bereich Applikationen bedankt sich bei allen Dienststellen des Ressorts für die gute Zusammenarbeit im Jahr 2021.

Der Bereich Applikationen stellt den unterschiedlichsten Endanwendern Softwarelösungen zur kundenorientierten Bedarfsdeckung von Anwenderanforderungen mit hoher Verfügbarkeit und maximaler Integrität bereit. Das Leistungsportfolio umfasst Softwareprodukte für die Abdeckung im einsatzorientierten Aufgabenspektrum genauso wie für den täglichen Dienstbetrieb. Dabei kommen sowohl Standardprodukte als auch Eigenentwicklungen zum Einsatz. Diese werden in die bestehende IKT-Systemlandschaft integriert und in einem Change-Managementprozess den wechselnden Kundenanforderungen angepasst.
Der Bereich Applikationen ist der zentrale Datenhalter und Datenbereitsteller des Verteidigungsressorts mit der Applikationsverantwortung für ca. 17.000 User (SMN, DGMN). Die Informationsversorgung der Endanwender wird durch über 100 IT-Services in unterschiedlichen Informationsdomänen je nach Klassifizierungsstufe oder bedarfsspezifischer bzw. organisatorischer Zugehörigkeit sichergestellt.

Personalmanagement-Dashboard (PersMngt-Dashboard)

Das oberste Management des BMLV benötigt aktuelle, aussagekräftige Kennzahlen rund ums Personal, die Bereitstellung der Information soll in Web-Technologie unter Einhaltung höchster Sicherheitsstandards erfolgen. Bestehende schriftliche Berichte sollen durch das Dashboard ersetzt und somit vereinheitlicht werden.

In einer Durchlaufzeit von knapp drei Monaten konnten 10 wesentliche Kennzahlen (u.a. Altersschichtung, Beorderungen nach Bundesland, Stellungsergebnis nach Geburtsjahrgang) bereits in einem modernen Dashboard in Web-Technologie bereitgestellt werden.

PersMgmt-Dashboard - Hauptmaske

Zu jeder Kennzahl sind noch Detailstatistiken aufrufbar. Die Daten wurden zwecks Vergleichbarkeit und vor allem um Trends zu erkennen, in der Historie aufgebaut und können im Bedarfsfall für den berechtigen Anwender als Rohdaten bereitgestellt werden. Die Darstellungsform der Grafiken kann individuell angepasst werden. Die regelmäßige automatisierte Aktualisierung der Daten auf Basis der zentralen Personaldatenbank von PS-NT erfolgt nach Vorgabe der Anwenderfachabteilung AllgPersAng.

Die Erweiterung des Berechtigungssystems um hierarchie- und rollenbezogene Einschränkungen bei der Darstellung der Kennzahlen erfolgt 2022, um auch anderen Hierarchieebenen als der obersten Führung das PersMgmt-Dashboard verfügbar machen zu können.

Antrag auf Erholungsurlaub mittels PAAN-Ich-Rolle

Bedienstete des BMLV mit eigener SMN-Chipkarte sollen über die PAAN-Ich-Rolle einen Antrag auf Erholungsurlaub stellen und den Antragsstatus verfolgen können. Nach Genehmigung des Vorgesetzten sollen die Daten automatisiert in PERSIS übernommen werden.

Der Bedienstete mit eigener SMN-Chipkarte kann in PAAN einen Antrag auf Erholungsurlaub stellen. Der Bedienstete hat eine transparente Gesamtübersicht über alle Erholungsurlaube und deren Bearbeitungsstatus.

PAAN - Monatsnachweis/Erholungsurlaub

Der durch den Antrag automatisch angestoßene ressortspezifische Genehmigungsprozesse (u.a. Berücksichtigung eines Zwischenvorgesetzten) läuft bereits als erster Prozess in der Web-Version der geschäftsfallorientierten Bearbeitung (GOB 4.0). Die Nutzung der Funktionalität kann optional erfolgen. Die BMLV-weite Ausrollung erfolgt im 1. Quartal 2022, danach sind weitere Funktionalitätserweiterungen geplant (u.a. Zeitkarte, Sonderurlaub, Pflegefreistellung, Integration mit der Web-Standesliste).

ePAT – Integration in den Personalapplikationen und Einbindung Signaturpad

ePAT – elektronisches Patienteninformationssystem ist das zentrale Service zur IKT-Unterstützung der Sanitätsorganisation im BMLV und ersetzt den papiermäßigen Gesundheitsakt.

ePat - Einstiegsmaske

Auf Basis der Erkenntnisse des erfolgreichen Probebetriebs in der Sanitätsorganisation Oberösterreich wurden neue Anforderungen an ePAT gestellt, wie Schnittstellenanbindung an die zentralen Personalapplikationen, die Integration eines Signaturpads oder diverser Importfunktionalitäten.

Im Jahr 2021 wurde das Rollout von ePAT in der Sanitätsorganisation erfolgreich fortgesetzt, mittlerweile werden ca. 13.000 Patienten verwaltet. Ein handelsübliches Signaturpad wurde in ePAT zwecks effizienter Dokumentation von durchgeführten Belehrungen der Patienten integriert.

Zur effizienten Erfassung von durchgeführten Massenimpfungen (Covid-19) bzw. Patientenstammdaten bei Massenuntersuchungen wurde die Möglichkeit des Excel-Imports nach ePAT realisiert.

Im Jahr 2022 wird die Integration von ePAT mit PS-NT, den Personalapplikationen des BMLV zwecks Austausch von Ergebnisdaten und automatischer Aktualisierung von Patientenstammdaten im Bedarfsfall fortgesetzt.

Besoldungsreform

Mit der 2. Dienstrechts-Novelle 2019, BGBl. I Nr. 58/2019 wurden die Bestimmungen über die Vordienstzeitenanrechnung umfassend überarbeitet und für die Mehrheit der Bundesbediensteten eine amtswegige Prüfung und ggf. Neueinstufung angeordnet. PersAppl wurde mit der Bereitstellung der notwendigen Funktionalitäten zur Umsetzung der „Besoldungsreform 2019" in den Personalapplikationen des BMLV umgehend beauftragt.

Ziel ist die IKT-mäßige Unterstützung des Gesamtprozesses unter Nutzung bereits vorhandener Daten von PERSIS.

Alle angeforderten Funktionalitäten konnten bereitgestellt und das Vorhaben konnte im Jahr 2021 abgeschlossen werden. Es wurde eine Erstdatenübermittlung zur Bundesbesoldung in PM-Bund durchgeführt und ein entsprechender Geschäftsprozess in GOB inklusive Dokumentenmanagement (Infoschreiben, Bescheide) bereitgestellt. Die bestehenden Schnittstellen zu PM-Bund wurden adaptiert, die Ergebnisdaten werden rückverarbeitet. Ein Großteil der erforderlichen Korrekturen des Besoldungsdienstalters kann automatisiert durchgeführt werden. Die Anwender haben die Möglichkeit der vorherigen Simulation und Gegenüberstellung der Ergebnisse sowie einer Excel-Exportfunktionalität.

Einsatzbesoldung Neu

Aufgrund der Erfahrungswerte zur Bewältigung der ersten CORONA-Welle 2020 wurde die Einsatzbesoldung von Präsenzdienstleistenden mit der HGG-Novelle 2021 reformiert. Die gesetzliche Änderung ist in Abstimmung mit PM-Bund so rasch wie möglich in den bestehenden Personalapplikationen des BMLV umzusetzen.

Zur Umsetzung der neuen gesetzlichen Anforderungen wurden neue bzw. bestehende PVCs – Personalvorgangscodes in PERSIS bereitgestellt bzw. adaptiert. Die Heeresgebührengesetz(HGG)-Gesetzesnovelle ist vollinhaltlich bereits umgesetzt.

Elektronischer Personalakt für Auslandeinsatz-Vertragsbediensteter (AE-VB)

Zur Vermeidung hohen manuellen Manipulationsaufwandes wurde seitens AuslEBa für AE-VB die Umsetzung des elektronischen Personalaktes für die Personengruppe AE-VB bei der zuständigen Anwenderfachabteilung AllgPersAng angefordert.

In PERSIS wird eine strukturierte Ablageform von Dokumenten zu einer Person in bestehender Standardtechnologie bereitgestellt. Die Planung sieht eine Bereitstellung der Funktionalität mit 1. Quartal 2022 vor und kann um weitere Personengruppen ergänzt werden. Der datenschutzrechtlich konforme Zugriff auf den elektronischen Personalakt wird über das vorhandene Berechtigungssystem geregelt.

IMM – Informationsmodul Miliz

Eine rasche Kommunikation zu Milizangehörigen soll zeitgemäß sichergestellt werden. Die Information soll über SMS, eMail bzw. persönliches Anschreiben erfolgen.

In den zentralen Personalapplikationen wird die Speicherung von Kontaktdaten überarbeitet. Die Generierung von Massen-Emails über eine Schnittstelle zum MTM des BMLV wurde zur Verfügung gestellt. Die rasche Umsetzung für konkrete eMail-Benachrichtigungen ist damit sichergestellt und ist seit Mitte 2021 im Einsatz.

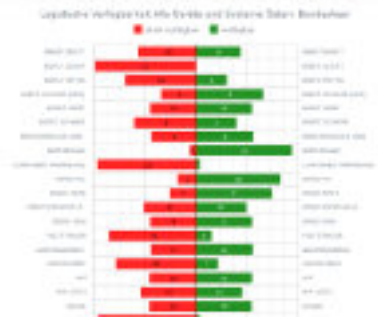
Digitalisierung der Behördenverfahren

Masken - Prototyp

Umsetzung eines bestehenden Geschäftsprozesses in PS-NT (FU/WKB – Familienunterhalt & Wohnkostenbeihilfe) zur Schaffung eines durchgängigen, digitalen Verfahrens (ohne Medienbruch, Device Unabhängigkeit) vom Bürger bis zur Militärbehörde. Der realisierte Musterprozess ist Basis für die Digitalisierung weiterer 100 Prozesse im eGovernment-Bereich.

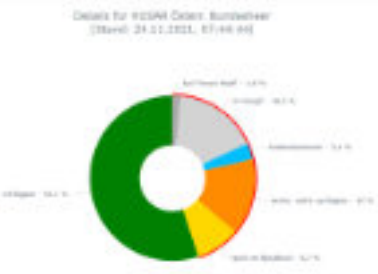
Anfang 2021 wurde das Projekt gestartet, die Ressourcenbereitstellung, das Aufstellen eines neuen Teams in der Abteilung Personalapplikationen, die Herstellung der Arbeitsfähigkeit und das Errichten eines Prototyps konnte bereits 2021 erreicht werden. Die Umsetzung erfolgt unter Nutzung von Standardtechnologien im eGovernment-Bereich (u.a. PVP – Portalverbund, eID, Handysignatur). Die Inbetriebnahme des künftigen Bürger-Portals mit Bereitstellung des Musterprozesses und Anbindung an die bestehenden Personalapplikationen ist für Mitte 2023 geplant.

Logistische Verfügbarkeitsmeldung (LogVerfM)



Von berechtigten Anwendern können Geräte/Systeme, welche sich im Nutzbestand der jeweiligen OrgEinheit befinden, zu einem Gerätetyp zugeordnet werden. Diese werden dann im ersten Schritt in der Gesamtübersicht nach verfügbar und nicht verfügbar angezeigt.

In Folge kann zu einem dieser Geräte/Systeme eine genauere Verfügbarkeit nach Gründen, Indexnummer, technischem Zustand oder nach Standort auf einer Übersichtskarte von Österreich abgerufen werden. Die Gründe für eine Nicht-Verfügbarkeit werden nach bestimmten Regeln gesetzt (z.B.: in der Materialerhaltung, Im Auslandseinsatz, im HLogZ,...). Die Auswertung wird aus dem operativen System von LOGIS erstellt und die Daten werden alle 10 Minuten aktualisiert



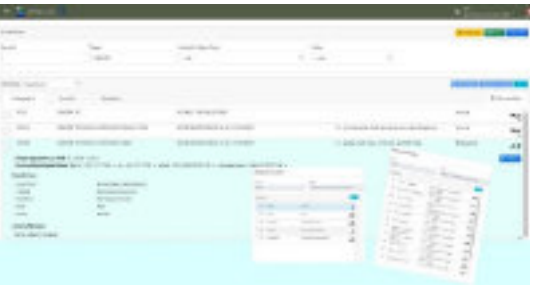
Beschaffung von VW ID.3 (Projekt „A03 – Ökologisierung des Bundesheeres")

Mit dem Ankauf der neuen VW ID.3 Modelle schlägt auch das ÖBH den Weg in Richtung E-Mobilität für nicht militärische Zwecke ein. Mit Anfang Juni wurden 30 Fahrzeuge in Bestand genommen. Damit stellt sich auch für die Logistik die Herausforderung, die Lagerung / Nutzung der benötigten AKKUS in bestmöglicher Art und Weise zu unterstützen.

Es ist notwendig die Anzahl und die Art der Ladezyklen (schnell bzw. langsam Ladung) zu dokumentieren und zu steuern. Ladestatus zu Beginn und Ende einer Fahrt müssen mit möglichst geringem Aufwand dokumentiert werden können.

Auch für die auf Lager liegenden Akkus muss abrufbar sein, wann diese ggf. geladen werden müssen. Das Laden der Akkus wird analog einer Betankung dokumentiert und mit Abschluss des Fahrbefehls im Fahrten- und Transportmanagement (FTM) an LOGIS übermittelt. Die Anzahl und die Art der Ladevorgänge werden in LOGIS über die Mechanismen der Geräteüberwachung gesteuert und diese Informationen stehen damit dem Nutzer jederzeit abrufbar zur Verfügung. Dazu war es notwendig, sowohl im FTM, in LOGIS und in der Schnittstelle der beiden Services die entsprechenden Funktionalitäten bereitzustellen, einzuführen und bei der Anwenderschulung zu unterstützen.

Umstellung LOGIS/ Firmenverwaltung auf Webtechnologie



Im Zuge der technischen Erneuerung von Software wurde das Teilservice LOGIS/ MatS/Firma auf den neuesten Stand der Softwaretechnologie gebracht. Sowohl Oberflächendesign des Teilservices Firmenverwaltung als auch Zugrifftechnologien vom Client zur Datenbank und die Installationsmechanismen am Client entsprachen nicht mehr den heutigen Anforderungen in den Bereichen Sicherheit und Benutzerfreundlichkeit. Bei der Umstellung waren zwei große Herausforderungen zu bewältigen:

Erstens die Akzeptanz der Anwender, da sich das Look & Feel in einem gänzlich neuen Bild präsentiert (bei gleicher Funktionalität) und zweitens die technische Umsetzung in Bezug auf das Gesamtservice LOGIS, da die bestehenden Schnittstellen zu anderen Teilservices möglichst unverändert bleiben sollten. Durch die frühe Einbindung der Anwenderfachabteilung wurde die Umstellung bestens angenommen und die Einführung beim Anwender gut unterstützt.

Transportunterstützung der Truppe in LOGIS

Einen weiteren Schritt Richtung Technologieerneuerung und gleichzeitig auch ein Stück neuer Funktionalität im Bereich LOGIS zur Unterstützung von Materialtransporten wurde mit der Produktivsetzung des Teilmoduls Transportunterstützung der Truppe geschaffen. Über Schnittstellen sowohl zu LOGIS als auch zur Munitionsverwaltung (Auftragsübersicht Lager) werden die zu transportierenden Versorgungsgüter auf Basis der Übergabe/Übernahme Geschäftsfälle aus den operativen Systemen an das Teilservice Transportunterstützung übermittelt und hier können dann nach unterschiedlichsten Kriterien Transportvorhaben zusammengestellt werden. Die Erstellung der entsprechenden Transportpapiere – vor allem bei Gefahrguttransporten - ist ein zentraler Punkt dieser Anwendung.

Die Routen können konfiguriert werden, Teil- Be- und Entladungen werden unterstützt. Bei entsprechender Qualität der Stammdaten werden für Gefahrguttransporte die Berechnungen für Zusammenlagerungen auf Grund der ADR Vorschriften durchgeführt und der Benutzer bei falschen Zusammenlagerungen bzw. Überlagerung entsprechend gewarnt.

SW-technische Unterstützung des Ausscheideprozesses

Eine noch offene Lücke in der softwaretechnischen Unterstützung der Logistik im ÖBH war der Ausscheideprozess. Nach langen Absprachen der Fachabteilungen wurde der Prozess festgelegt und konnte jetzt in LOGIS implementiert werden. Von der Auswahl der auszuscheidenden Versorgungsgüter unter Berücksichtigung der beim Artikel definierten Vorgehensweise über Vorbereitung der benötigten Unterlagen, dem

Erfassen der Zustandsfeststellung, der Zusammensetzung der Kommission (dort wo erforderlich), der notwendigen Bestandsbuchungen bis hin zu einem ebenfalls in LOGIS abgelegten Ausscheideprotokolls. Der gesamte Vorgang wird über einen LOGIS-Geschäftsfall („Ausscheidung") abgehandelt.

Die Auswahl der Versorgungsgüter erfolgt über LOGIS Standardmechanismen („Bestandsauswahl" oder Einlesen von gescannten Barcodes). Somit kann der gesamte Lebenslauf eines Versorgungsgutes von der Beschaffung bis zur Ausscheidung lückenlos dokumentiert und verfolgt werden.

Smart Waste

Digitalisierung in der Bewirtschaftung von Lebensmittelabfällen

Gemäß Vorgabe der EU müssen die Mitgliedstaaten den Lebensmittelabfall bis 2030 um 50% reduzieren. Der Beitrag des ÖBH dazu lautet „Trennen – Messen – Evaluieren – Optimieren – Vermeiden – Wiederverwerten".

Die Lebensmittelabfälle werden in unvermeidbare und vermeidbare Abfälle getrennt. Wir messen die Abfallmasse und den Füllstand der Abfalltonnen kontinuierlich mittels entsprechender Sensoren, die über „Long Range Wide Area Network" (LoRaWAN) in das Dynamische Gesicherte Militär Netz (DGMN) eingebunden sind. Wir werten die Daten mittels PowerBI aus und vergleichen die Kennzahlen miteinander. Wir optimieren das Abfallaufkommen und die Entsorgungslogistik. Wir führen Abfälle nach Möglichkeit einer Wiederverwertung zu.

Damit leisten wir einen wichtigen Beitrag zur Nachhaltigkeit und zur Erreichung der Ziele des Green Deal.

Checkpoint MaHü

Am 15.09.2021 wurde der „Checkpoint MaHü – unser Heer" von Verteidigungsministerin Klaudia TANNER feierlich eröffnet. Dieses Projekt soll es interessierten Personen möglich machen, sich über die vielseitigen beruflichen Möglichkeiten und Jobs beim Heer zu informieren sowie hochwertige Produkte im Bundesheer-Design zu erwerben.

Die IT-mäßige Planung und Realisierung erfolgte unter maßgeblicher Beteiligung der Abteilung Bauwesen-Applikationen. Die Ausstattung umfasst neben einem DGMN-Arbeitsplatz mit diesbezüglichen IT-Services auch moderne Visualisierungsmittel wie Virtual Reality und Digital Signage (Infoscreens).

Checkpoint MaHü - Foto: BMLV/Michael Bauer

Vorbereitung Windows11 Update

Microsoft veröffentlichte sein neues Betriebssystem „Microsoft Windows11" am 04.10.2021 als Nachfolger von Windows 10. Das neue Betriebssystem zeigt sich dem Benutzer mit einer geänderten Optik (z.B. neues Logo, abgerundete Fensterecken, neue Sounds). Eine wesentliche Neuerung besteht darin, dass Apps, die für das Betriebssystem Android entwickelt wurden, auf Windows11 direkt lauffähig sind.

Die Abteilung Bauwesen-Applikationen hat alle erforderlichen Vorbereitungen getroffen, um Windows11 in das Dynamische

Gesicherte Militär Netz (DGMN) zu integrieren. Das Kabinett der Frau Bundesministerin (KBM) wird das erste Organisationselement des ÖBH sein, bei dem Windows 11 zum Produktiveinsatz kommt.

Digitaler Zwilling (BACtwin)

Digitalisierung in der Gebäudeautomation

Heizungssteuerung, Warmwasseraufbereitung, Klimatisierung, Strom- und Energiezähler sind zentrale Elemente zum Betrieb von Gebäuden. Im Digitalisierungszeitalter sind idealerweise alle Steuerungs- und Messkomponenten untereinander und mit einer „Kommandozentrale" vernetzt – Stichwort Internet of Things (IoT). Dabei kommt eine Vielzahl von Properties, Daten und Parametern zum Tragen.

BACtwin, der digitale Zwilling in der Gebäudeautomation (GA), stellt eine Bibliothek mit Standard-Aggregaten, GA-Funktionslisten sowie Automationsschemata und –beschreibungen zur Verfügung. Dadurch wird ein durchgängiger Prozess von den Bauherrnvorgaben über die Planung und das Engineering bis zum Betrieb geschaffen.

Das ermöglicht die Umsetzung des Green Deal und stellt sicher, dass nicht jede Pumpe und jeder Ventilator jeweils neu geplant, entwickelt, visualisiert und betrieben werden muss.

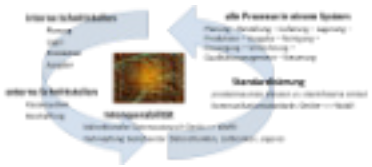
BACtwin wurde auf Initiative und unter maßgeblicher Beteiligung der Abteilung Bauwesen-Applikationen entwickelt und soll in die Standardisierte Leistungsbeschreibung Haustechnik (LB-HT) aufgenommen werden.

Digitale Verpflegsverwaltung

Bargeldlose Verpflegsteilnehmerabrechnung und „Digitale Küche"

Das IT-Service „Verpflegsteilnehmer-Erfassung und bargeldlose Abrechnung" (VTA) ist mittlerweile an acht Standorten im Produktionsbetrieb.

Auch im Bereich der Großküchengeräte spielen die Themen Vernetzung, Digitalisierung, Künstliche Intelligenz und Internet of Things eine immer größere Rolle. Warenwirtschaftssystem und Geräte müssen interoperabel miteinander kommunizieren können. Nur dadurch kann die Erfüllung diverser Vorgaben (gleichbleibende hohe Qualität in allen Verpflegseinrichtungen gemäß mikrobiologischer Untersuchungen etc.) dauerhaft gewährleistet werden.



Digitalisierung in der Verpflegsverwaltung

Auf Initiative der Abteilung Bauwesen-Applikationen fand im Jahr 2019 eine Tagung zum Thema „Digitale Küchengeräte" statt. Im Zuge der Planung und Errichtung der Regionalküche Salzburg, deren Betriebsaufnahme für Herbst 2022 vorgesehen ist, sollen die Ergebnisse der genannten Tagung, aber auch des „Proof of Concept Digitale Großküche" evaluiert und in die Tat umgesetzt werden.

Tankanlagenmanagement

Digitalisierung im Kraftfahrwesen

Die Tankanlagen des ÖBH versorgen die Heereskraftfahrzeuge mit Treibstoff und müssen autark agieren können. Die digitale Vernetzung mit einem zentralen Server ermöglicht den Verantwortlichen tagesgenaue Informationen über den Füllstand und den Verbrauch der Tankanlagen. Das IT-Service bietet unter anderem auch Übersichten über die einzelnen Tankvorgänge und ermöglicht die zentrale Verwaltung der ca. 8.000 Tankchips. Die zentral gesammelten Daten können anderen IT-Services des ÖBH (z.B. LOGIS) verfügbar gemacht werden, um die rasche, effiziente, wirtschaftliche und umweltfreundliche Versorgung der Tankanlagen mit Treibstoffen zu gewährleisten.

Das IT-Service läuft im Dynamischen Gesicherten Militär Netz (DGMN). Zum Stichtag 19.11.2021 waren 20 der insgesamt ca. 50 Tankanlagen auf das neue System umgestellt.

Tankanlage Salzburg Nord - Foto: BMLV/Helmut Steger

Computerassistiertes Testen

Digitalisierung in der Heerespsychologie

Im Ressortbereich des BMLV werden in den Prüfzentren des HPA und bei den Stellungskommissionen jährlich über 50.000 Personen auf ihre psychologische Eignung für verschiedene Funktionen getestet. Die dabei eingesetzten, teilweise gesetzlich determinierten Testverfahren, bedürfen einer IT-Unterstützung.

Das IT-Service „Computerassistiertes Testen" (CAT) läuft im Dynamischen Gesicherten Militär Netz (DGMN) und ermöglicht dem psychologischen Dienst, die Entwicklung, Bereitstellung, Validierung und Wartung der psychologischen Testverfahren in einem System umzusetzen. Die Untersuchungen selbst finden ebenfalls mit CAT statt und werden vom zuständigen Fachbereich durchgeführt.

Probandin bei der Testung - Foto: Kurier

Digital Asset Management

Digitalisierung und Modernisierung im ÖA-Bereich

Im Ressortbereich des BMLV existiert eine Vielzahl von Bildern, die in den letzten 60 Jahren erstellt und archiviert bzw. vereinzelt in der Bilddatenbank der Heeresbild- und Filmstelle (HBF) gespeichert wurden. Der Zugriff darauf war der HBF vorbehalten.

Seit Anfang 2021 ersetzt das Digital Asset Management (DAM) die bestehende Bilddatenbank. Neben der HBF können auch die Dion Komm, die RedTD, das HDruckZ und alle Militärkommanden die digitalen Assets wie Bilder, Grafiken, Video- und Audiodateien im DAM, das im Dynamischen Gesicherten Militär Netz (DGMN) betrieben wird, speichern.
Das System unterstützt die Benutzer unter anderem bei der Erfassung der Metadaten wie der Urheber- und Nutzungsrechte oder der Beschlagwortung. Es ist geplant, dass alle Mitarbeiter des ÖBH über Bitbox im SMN auf das DAM zugreifen und Bilder oder andere Assets suchen, finden und downloaden können.

Scharfschießen Panzerabwehrrohr 66/79 - Foto: BMLV/Daniel Trippolt

Sicherheitszone Medizin

Digitalisierung in der Militärmedizin

Der Sanitätsbereich des ÖBH (Sanitätszentren (SanZ), Feldambulanzen (FAmb), Stellungskommissionen (SteKo) arbeitet zurzeit, mangels eines gesamtheitlichen medizinischem Informationssystems mit Insellösungen. Die einzelnen Systeme (Röntgen, Computertomografie, Labor etc.) werden von den einzelnen Dienststellen betrieben und sind nicht miteinander vernetzt.

RIS/PACS-Arbeitsplatz - Foto: Stefan Hammerschmid

Durch die „Sicherheitszone Medizin" im Dynamischen Gesicherten Militär Netz (DGMN) wird eine auf die Anforderungen der Medizin ausgerichtete gemanagte Systemumgebung in ganz Österreich zur Verfügung gestellt. Die einzelnen medizinischen Geräte werden digital über standardisierte Schnittstellen mit den dazugehörigen Fachinformationssystemen verbunden. Ein Beispiel dafür ist „RIS/PACS": Das Radiologie-Informationssystem (RIS) beinhaltet Patientendaten und Metadaten von Bildern. Die Bilder selbst befinden sich im Picture Archiving and Communication System (PACS). Die Patientendaten und die Bilddaten werden über eine sichere Schnittstelle miteinander verknüpft.

In der „Sicherheitszone Medizin" werden auch Schnittstellen zu externen Stellen wie dem Epidemiologischen Meldesystem EMS (System zur Registrierung anzeigepflichtiger Krankheiten wie Covid-19) oder dem Epidemiologischen-Informations-System EPISys (Einmeldung von negativen Covid-19-Tests für die automatische Erstellung des Grünen Passes) zur Verfügung gestellt.

Neues Intranet mit dem Content Management System Liferay DXP

Innovative Software zur Erstellung und kollaborativen Nutzung von ansprechenden und zeitgemäßen Intranet-Inhalten

Seit 27.10.2021 steht das neue Content Management System (CMS) Liferay DXP für alle Anwender des SMN zur Verfügung.

Startportal – Termine, Frage der Woche

Sämtliche zur Bereitstellung dieses IKT-Service „CMS/Intranet" erforderlichen Tätigkeiten wie Installation, Integration, Konfiguration, Entwicklung von ressortspezifischen Anpassungen aber auch Unterstützung der Schlüsselanwender, Erstellung von Schulungsmaterialien und Einweisung der Trainer erfolgten durch die Abteilung Informationsmanagement&Büroautomation (Infomngt&BA) des Bereichs Applikationen der Direktion 6 IKT und Cyber. Zuständig für Design und Inhalte ist DionKomm.

Der Einstieg in das neue Intranet erfolgt über das Startportal in dem den Anwendern aktuelle News und Termine angezeigt werden. Außerdem stehen ein zentraler Übersichtskatalog und Links zu den wichtigsten Arbeitswerkzeugen zur Verfügung. Beispiele für die interaktive Funktionalität, die das neue CMS bietet, sind die „Frage der Woche" und der Feedbackbogen. Den Autoren von Intranet-Inhalten bietet das neue CMS eine intuitive Benutzeroberfläche mit Funktionalität am neuesten Stand der Technik.

So können Intranet-Inhalte erstellt werden, die den Nutzern des Intranet Informationen in einer zeitgemäßen, modernen Form präsentieren. Außerdem stehen Kollaborationsfunktionalitäten wie Wikis, Blogs, Diskussionsforen, Kommentare und vieles mehr zur Verfügung.

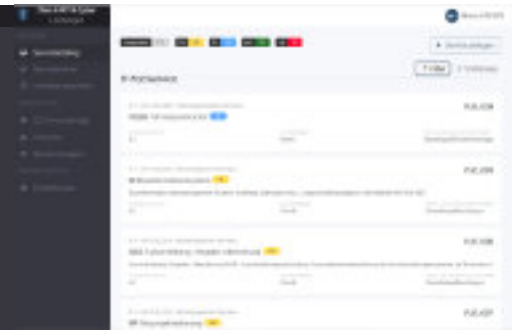
Bearbeitung von Intranet-Inhalten mit Liferay DXP

Servicekatalog

IKT-Services übersichtlich und transparent

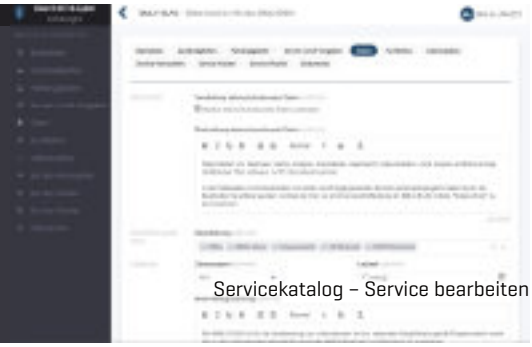
Die IKT-Dienstleister des BMLV/ÖBH stellen eine große Anzahl von IKT-Services bereit (IT-Infrastrukturservices, IT-Basisservices, IT-Fachservices, Kommunikationsservices sowie Cyber-Sicherheitsservices). Für das Management dieser Services ist es wichtig, einen zentralen Überblick über alle Services mit allen relevanten Informationen zu haben. Der hierfür relevante Prozess des IT-Servicemanagements ist das IT-Service-Catalogue-Management.
Seitens der Abteilung Infomngt&BA wurde eine Web-Applikation entwickelt, die diese Funktion erfüllt.

In der Web-Applikation Servicekatalog können sämtliche Services mit deren allgemeinen und BMLV/ÖBH-spezifischen Eigenschaften erfasst, bearbeitet und abgefragt werden.



Servicekatalog – Liste der Services

Neben allgemeinen Eigenschaften von Services wie Service-Beschreibung, Servicegruppe und Funktionalität beinhaltet der Servicekatalog auch die Zuständigkeiten (Service-Verantwortung, Anwenderfachabteilung, Support, etc.), die Service-Level-Vorgaben (Verfügbarkeit, Betriebs- und Supportzeiten, etc.), Angaben zu den verarbeiteten Daten (Datenschutzrelevanz, Klassifizierung) und zum Lebenszyklus (Inbetriebnahmezeitpunkt, Auftragsgrundlagen, Alleinstellungsmerkmale).



Servicekatalog – Service bearbeiten

Um eine möglichst umfassende Servicedokumentation zu bieten, können auch Daten betreffend Architektur, Betrieb, Zugriffsrechte, Integrationsgrad u.v.m. erfasst werden. Dies kann nicht nur mittels den vorgesehenen Eingabefeldern erfolgen, sondern es können auch beliebig viele Dokumente je Service hinzugefügt werden.

Ein ganz wichtiger Punkt ist die Möglichkeit Abhängigkeiten zwischen Services zu erfassen, außerdem können zu jedem Service beliebig viele Kennzahlen erfasst werden.

Die Web-Applikation für den Service-Katalog bietet somit einerseits eine wesentliche Unterstützung des Kerngeschäfts der IKT-Dienstleister und andererseits eine zentrale Übersicht der Leistungen der IKT-Dienstleister für die relevanten Führungsebenen des BMLV/ÖBH.
Auch beim Vergleich der Leistungsfähigkeit der IKT-Dienstleister des BMLV/ÖBH mit anderen Ressorts und Organisationen spielt der Service-Katalog eine entscheidende Rolle.

BMLV-ELAK 2021

Funktionalitätserweiterungen, betriebliche Maßnahmen, Abbildung Reorganisation 2021 und mehr

Auch im Jahr 2021 gab es betreffend den BMLV-ELAK wieder große eine Anzahl von funktionalen Erweiterungen und Ergänzungen auf Basis der Anwenderanforderungen.
Es fanden zwei Upgrades statt mit denen insgesamt 280 Punkte umgesetzt wurden.

Detailinformation zu Dokumenten im BMLV-ELAK

Besonders hervorzuheben sind dabei:

- Berücksichtigung des neuen eindeutigen Identifikationsmerkmals für Personen im BMLV/OBH, der LVID und Ablöse der SV-Nummer an allen relevanten Stellen im BMLV-ELAK (z.B. Geschäftsstück-Dialoge, Suchen, Platzhalterersetzung).
- Hervorhebung der bereits gelesenen und seit dem letzten Öffnen veränderten Dokumente in der Detailanzeige im Arbeitskorb
- Erledigungen in mehreren Akten auf einmal einzelgenehmigen
- Automatische Verweisanlage beim Abfertigen (konfigurierbar)
- Amtssignatur von Beilagen zu Erledigungen
- Bearbeitung von Geschäftsstücken aus dem Suchordner und den Verweisordnern heraus (sofern man damit belastet ist)

- Übersichtlichere und einheitliche Funktionsmenüs
- Funktion „alle Einsichtnahmen parallelisieren im Objektlauf"

Darüber hinaus werden laufend betriebliche Maßnahmen zur Erhöhung der Stabilität und Performance des BMLV-ELAK durchgeführt. Die Infrastruktur-Software wurde auf den neuesten Stand gebracht und eine neue Lösung für die zentrale PDF-Konvertierung bereitgestellt.

Die BMLV-ELAK-Informationsseite wurde auf das neue CMS Liferay DXP umgestellt.

Neue BMLV-ELAK-Infoseite im Intranet

Die Leistungsfähigkeit des BMLV-ELAK und des dahinterstehenden Teams der Abteilung Infomngt&BA konnte im Rahmen der Umsetzung der großen Reorganisation 2021 eindrucksvoll unter Beweis gestellt werden. So gelang es mit einer Vorbereitungszeit von nur zwei Wochen, die gesamte Reorganisation zum Stichtag des Inkrafttretens im BMLV-ELAK abzubilden, sodass alle Anwender im BMLV/ÖBH ihre Arbeit nahtlos fortsetzen konnten.

Core-Service Mailing und Chat 2021

Mailservices für immer mehr Einsatzbereiche

Aktuell gibt es vier physikalisch getrennte Mailservices im Verantwortungsbereich der Abteilung Infomngt&BA: Mailmanagement im SMN, Internet-Mailing (Webmail), Mailmanagement im AbwA und Mailmanagement im HNaA.

Im Aufbau begriffen ist ein Service Mailmanagement/GEHEIM das im Hochsicherheitsnetzwerk ASECOS laufen wird und eine Schnittstelle zum EU Operations WAN (Geheim-Netz der EU) haben wird.

Für Übungen und Einsätze werden laufend Mailsysteme bereitgestellt (zuletzt für die Common Roof 2021).

Im Jahr 2021 wurde darüber hinaus an der Bereitstellung für folgende weitere Einsatzbereiche gearbeitet:

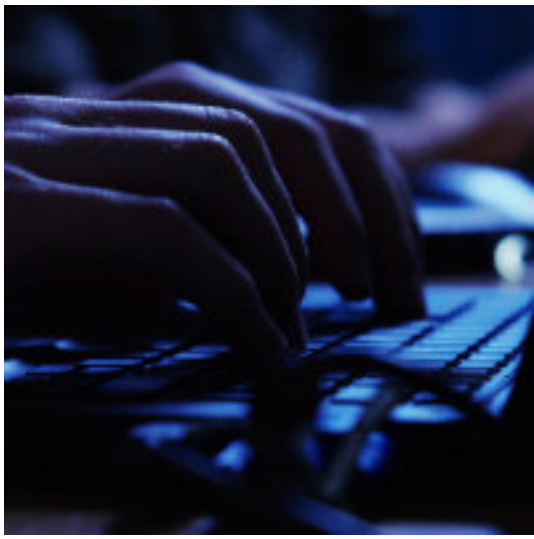
- Tactical Communication Network (TCN): Bereitstellung von autarken Mailsystemen für das verlegbare Einsatznetzwerk.
- Telekommunikationsverbund (TKV): Kommunikation mit der neuen Telefonanlage (insbesondere für Präsenzservices)
- Videokonferenz: Buchung von Online-Besprechungsräumen aus dem Mailsystem heraus (Ressourcenmanagement und Passwortvergabe für die Videokonferenzen)

Außerdem wurden 2021 für alle Mail- und Chatserver im Verantwortungsbereich der Abteilung Infomngt&BA im SMN und im Internet Major Release Upgrades durchgeführt, sodass diese nun auf dem neusten Stand der Produkte HCL Domino und HCL Sametime sind.

HCL Domino HCL Sametime

Für das Service Internet-Mailing ist es zur zusätzlichen sicherheitstechnischen Absicherung erforderlich, eine 2-Faktor Authentifizierung zu implementieren und bereitzustellen. Das bedeutet die Anwender bekommen im Rahmen der Anmeldung an das Service mittels SMS einen Code auf ihr Mobiltelefon geschickt, der zusätzlich zum Passwort eingegeben werden muss, damit die Anmeldung durchgeführt wird.

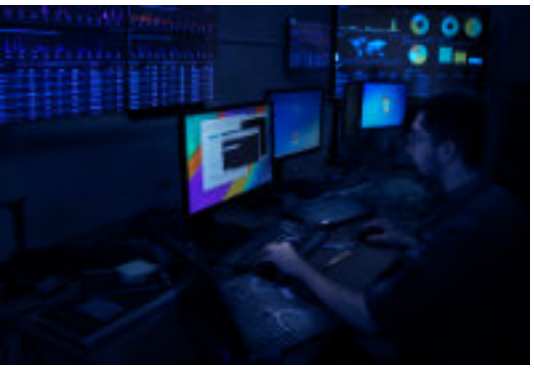
Für die 2-Faktor-Authentifizierung wurde 2021 ein erfolgreicher Proof of Concept durchgeführt, die erforderliche Software wurde beschafft.



Combined Federated Battle Laboratories Network - Final Operational Capability

Mit dem Anschluss an das Test- und Entwicklungsnetz CFBLNet verfügt das Bundesheer erstmals über die Möglichkeit ein eigenes "Battle Lab" für die internationale Testung und Zertifizierung von IKT-Services zu betreiben.

Das CFBLNet wird u. a. im internationalen Interoperabilitätsprogramm FMN (Federated Mission Networking) für die technische Verifikation genutzt. FMN gilt derzeit als relevantester Treiber für die Interoperabilität militärischer IKT-Services.



Vom 29. November bis 3. Dezember 2021 erfolgte nach Tests mit Finnland und Kroatien unter Beteiligung der NATO Communications and Information Agency das "Joining" in die FMN-Testumgebung. Zunächst wurden vier technische Basisdienste und das Service "Text-based Collaboration" (Chat) in Betrieb genommen und damit formell die "Final Operational Capability" des AUT Battle Labs am CFBLNet hergestellt. In der Folge soll dieses FMN-Referenzsystem sukzessive gem. dem österreichischen Ambitionsniveau erweitert bzw. an die jeweils aktuelle FMN-Spezifikation angepasst werden.

ABC-Informationssystem - Schnittstelle zum US-Wetterdienst NOAA

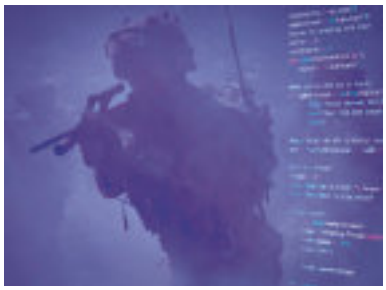
Das ABCIS benötigt für Gefährdungsprognosen nach einer Freisetzung radiologischer, chemischer oder biologischer Gefahrstoffe genaue und weiträumige Wetterdaten einschließlich Windfelder bis 30km Höhe.

Im Zuge des Forschungsprojektes Grib2METGM wurden Möglichkeiten untersucht, Berechnungsergebnisse globaler Wettermodelle für Gefährdungsprognosen zu nutzen.

Nach Abschluss des Forschungsprojekts wurde 2021 im Rahmen eines bestehenden Wartungsvertrags von Joanneum Research GmbH eine Schnittstelle zum US-Wetterdienst NOAA (National Oceanic and Atmospheric Administration) realisiert.

Vom Referat Einsatzorientierte Systemintegration in Zusammenarbeit mit Experten aus den Bereichen IKT-Technik und dem Militärischen Cyber-Sicherheitszentrum wurde diese in das IKT-System ÖBH implementiert.

Bevor eine solche Schnittstelle zwischen einem einsatzwichtigen IT-System des Bundesheeres und einer ausländischen Behörde für die operationelle Nutzung freigegeben werden kann, ist allerdings noch ein Sicherheitsaudit erforderlich, das im ersten Quartal 2022 geplant ist.



Datenfunksoftware - Anbindung Kurzwellenfunksystem Landstreitkräfte

Mit der erfolgreichen Erprobung bei der trilateralen Übung COMMON ROOF 2021 sind die technischen Voraussetzungen gegeben, dass die Applikation Datenfunksoftware 2 nunmehr auch mit dem neuen digitalen Kurzwellenfunksystem der Landstreitkräfte (KW LaSK) genutzt werden kann.

Foto: HBF/Daniel TRIPPOLT

Für eine formelle Freigabe der operationellen Nutzung ist noch ein Sicherheitsaudit durch das Militärische Cyber-Sicherheitszentrum erforderlich, welches im ersten Quartal 2022 durchgeführt wird. Die Datenfunksoftware ist eine in der Abteilung Einsatzorientierte Applikationen entwickelte Anwendung für die gesicherte und dokumentierte Datenübertragung über alle bei den Landstreitkräften eingeführten Funksysteme.

Die Applikation nutzt einen Verschlüsselungsmechanismus des Heeresnachrichtenamts und ist bis zur Klassifizierungsstufe VERTRAULICH bzw. GEHEIM (beim Jagdkommando) zugelassen. Bis zur Stufe EINGESCHRÄNKT kann auch das SMN in das Netzwerk einbezogen werden.

Digitalisierung des Aufklärungsverbunds - Forschungsprojekt PIONEER

Wie im vorjährigen Leistungsbericht bereits dargestellt - das Vorhaben wurde im Oktober 2020 begonnen - ist dieses Projekt, das im nationalen Verteidigungsforschungsprogramm FORTE gefördert wird, die Initialzündung für die Digitalisierung des Aufklärungsverbunds im Bundesheer.

Erste sehr erfolgversprechende Ergebnisse, nämlich ein spezielles Softwaresystem für Auswerter in einer "All Sources Intelligence Cell", wurde im Oktober 2021 bei einer großen Stabsübung an der Militärakademie in Wiener Neustadt erprobt.
Dieses System soll, funktional erweitert, nächstes Jahr in den Aufklärungslehrgang am Modell des großen Verbandes der LaSK und die entsprechende Stabsübung integriert werden.

IKT&CySihZ

Cyberforces

we are future

WIR SCHÜTZEN ÖSTERREICH.

bundesheer.at

UNSER HEER

IKTTe

Bereich IKT-Technik

Neben der Erhaltung und Weiterentwicklung der eingeführten Infrastruktur sowie der Einführung von neuen Systemen und Plattformen wurde, trotz Covid-19 Rahmenbedingungen, die Erarbeitung von Grundlagen für die Bereitstellung des IKT-System-Einsatz betrieben. Eine besondere Herausforderung für den Bereich ist die Verkürzung der Wartungs- bzw. Support-Zyklen bei der eingesetzten Infrastruktur Software (Betriebssysteme, Datenbankmanagement-systeme, Entwicklungsumgebungen, etc.). Dies bedingt einen höheren Aufwand (z.B. kürzere Zyklen für Batches, Versionen, verkürzter Zeitraum für den vom Hersteller garantierten Support von eingesetzten Versionen, laufende Bereitstellung von Security-Fixes und –Updates) im Rahmen der Bereitstellung der Infrastruktur. Bei gleichen oder stagnierenden Personalressourcen hat dies negative Auswirkung auf die Weiterentwicklung bzw. die Einführung von neuen IKT-Services.

Die Spezialistinnen und Spezialisten des Bereiches IKTTe haben durch massive Automatisierung von Abläufen in der Erhaltung und Weiterentwicklung auf die geänderten Rahmenbedingungen reagiert und das DevOps (DevelopmentOperations) Konzept, unter anderem im Hinblick auf rasche Auslieferung von qualitativ hochwertiger Software und kontinuierlicher Verbesserung der Infra-struktur-Software, umgesetzt.

Der Bereich IKTTe war im Jahr 2021 mit Problemen und Lieferverzögerungen beim Ankauf neuer Hardware konfrontiert, was zu erheblichen Zeitverzögerungen und hohem internen Aufwand geführt hat.

Mag. Wolfgang Hacker

Es bleibt die Hoffnung, dass sich die angespannte Situation am Hardware-Markt 2022 verbessern wird.

Zusätzlich zur Erhaltung und Weiterentwicklung der bestehenden Infrastruktur wird uns 2022 die Mitwirkung bei der Einführung und Erprobung von Systemen und Plattformen, die Erarbeitung von Grundlagen für die Bereitstellung des IKT-Systems-Einsatz, sowie die Personalrekrutie-rungen fordern.

Ich bedanke mich bei meinen Mitarbeiterinnen und Mitarbeitern für deren hervorragenden Einsatz und das hohe Maß an Leistungsbereit-schaft. Ferner bedanke ich mich bei meinen Vorgesetzten sowie allen Organisationselementen für die konstruktive Zusammenarbeit im vergan-genen Jahr.

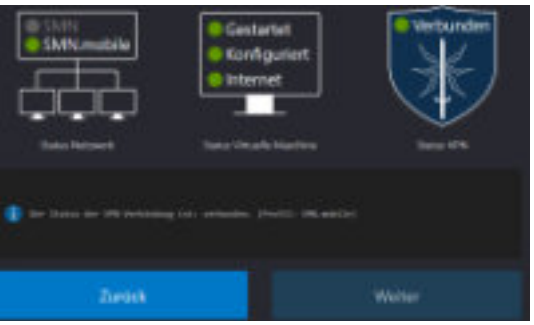
Als Teil des IKT & Cybersicherheitszentrums ist der Bereich IKT-Technik, unter besonderer Berück-sichtigung der Anforderungen im Hinblick auf Autarkie, Interoperabilität und IKT-Sicherheit, verantwortlich für die Konzeption und Bereitstellung der IKT-Infrastruktur für das BMLV/ÖBH.

Dazu zählen das Netzwerk zur Übertragung von Sprache und Daten, die Endgeräte für alle Anwenderinnen und Anwender des Ressorts, wie z.B. Desktops bzw. Notebooks, Smartphones, Server und zentrale Datenbanksysteme, aber auch Hardware für spezielle Anforderungen wie Radarsysteme und Funkgeräte im mil. Bereich.

Ferner wird die systemnahe Software für den Betrieb der IKT-Systeme und die Standardsoftware auf allen Endgeräten implementiert, um eine einheitliche Basisausstattung für die Bewältigung der Aufgaben im Rahmen der Einsatzvorbereitung und im Einsatz zur Verfügung zu stellen. Der Bereich IKT-Technik gliedert sich in die Abteilung Kommunikation, Hardware und Systemsoftware und Technische Querschnittsaufgaben.

SMN.mobile

Die Nutzung von SMN-Endgeräten außerhalb von militärischen Liegenschaften war bisher nur über die GovNet-Box und für einen sehr eingeschränkten Personenkreis möglich. Die Produktion dieser HW-Lösung wurde seitens des Herstellers eingestellt. IKT&CySihZ wurde nach Abschluss einer Variantenbeurteilung beauftragt, das Service SMN.mobile zu entwickeln, um insbesondere die gestiegenen Ausstattungsanforderungen im Zusammenhang mit "Home-Office" und "Telearbeit" zu decken.



Seit der Einführung von SMN.mobile im März 2021 haben über 2.500 Nutzer SMN.mobile verwendet, davon bis zu 711 gleichzeitig. Sobald 2022, mit vielen Monaten Covid-19 bedingter Verspätung, die neuen SMN-Notebooks ausgeliefert werden, werden die Nutzungsstatistiken sicherlich noch weiter steigen. Gem. der Planungsvorgabe werden bis zu 9.000 Nutzer und davon bis zu 3.000 gleichzeitig erwartet.

Die aktuelle Beschaffung von HP Notebooks wurde im 2020 gestartet. Ausgelöst durch die Covid-19 Pandemie wurden bisher problemlose Beschaffungs- und Lieferprozesse hinsichtlich Qualität und Dauer der Durchführung massiv verschlechtert.

Obwohl bis Dezember 2021 kein einziges der über 3.000 bestellten Notebooks geliefert wurde, mussten aufgrund von Komponentenmangel und anderwertigen Mängeln mehrmals neue Gerätetypen getestet und integriert werden (zuletzt im November 2021). Trotz größter Anstrengungen im Bereich Technik und Beschaffung konnten Lieferzeiten von voraussichtlich 6-12 Monaten nicht verhindert werden. Seitens der Hersteller wird erst 2022/2023 mit einer Entspannung der Liefersituationen gerechnet.

TCN

Zweck des Vorhabens TCN ist die Sicherstellung eines für NATIONALE und INTERNATIONALE Einsätze und Übungen geeigneten Vermittlungssystems für Sprache und Daten sowie des erforderlichen Verteilungs- und Einbindungssystems für Endteilnehmer an verlegbaren Führungseinrichtungen inklusive Lagerbetrieb.

Im Jahr 2021 haben einige konkrete Schritte im Vorhaben TCN (Tactical Communication Net) stattgefunden. An der FüUS wurde die Ausbildungsanlage (Containersystem) in Betrieb genommen (8 Ausbildungsplätze, 4 Taktische Router mit notwendigen Zusatzsystemen). Erstmals wurde dabei ÖBH Kryptomaterial eingespielt und die Funktion positiv getestet.

Dadurch erfüllt TCN die internen IKT-sicherheitstechnischen Vorgaben. Ferner wurden im IKT&CySihZ zwei Referenzsysteme aufgebaut, welche zukünftig für Entwicklertests im Rahmen der Erhaltung und Weiterentwicklung des Systems genutzt werden sollen.

Im September konnte die erste Schulung (techn. Systemeinweisung) durchgeführt werden. Die Schulung dauerte 4 Wochen und bot die Gelegenheit erstmals konkrete Netzwerkkonfigurationen zu testen. Dies bildete die Voraussetzung, um mit dem Erstellen der Betriebsvorgaben zu starten.

Im Oktober 2021 wurde die „Train the Trainer" Schulung durchgeführt und danach mit der Schulung der Operatoren an der FüUS begonnen.

Im Juli 2021 erfolgte die erste Teillieferung des Systems TCN. Mit November 2021 wurde mit der Güteprüfung begonnen. Gemeinsam mit dem Auftragnehmer werden die Systemkomponenten im Detail überprüft, allfällige Fehler werden dokumentiert und im Rahmen eines definierten Prozesses bearbeitet bzw. technische Lösungen vom Auftragnehmer bereitgestellt. Ein Systemtest ist Anfang 2022 an der FüUS geplant, um das System TCN möglichst einsatznah zu überprüfen.

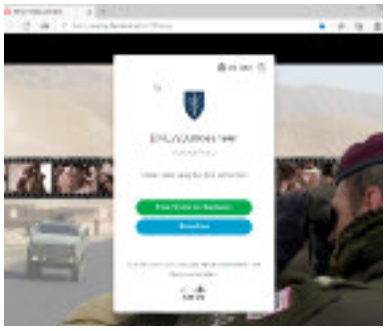
VKSng

Aus der Einhaltung von Covid-19 Maßnahmen haben sich im Ressort unter anderem Anforderungen für die Durchführung von virtuellen Besprechungen mit internen und externen Teilnehmern ergeben

bzw. ist die Anzahl an virtuellen Besprechungen schlagartig gestiegen, was das eingeführte System an seine Kapazitätsgrenzen geführt hat.

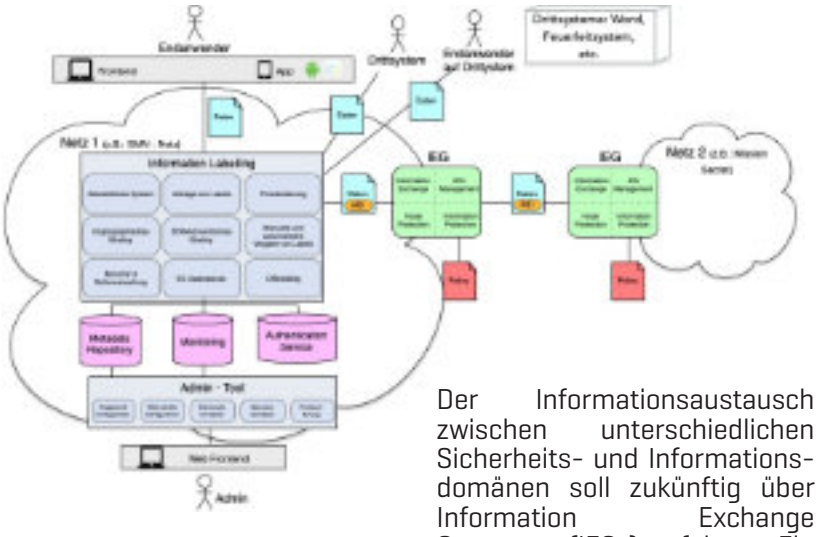
Das Videokonferenzsystem (VKS13) hat 2021 eine massive Erweiterung erfahren. Es wurde ein System eingeführt, bei dem vom jeweiligen Arbeitsplatz der Bediensteten aus (auch über SMN.mobile!) eine Videokonferenz mit allen virtuellen Konferenzräumen gemacht werden kann, die auf den Servern des BMLV/ÖBH gehostet werden.

Darüber hinaus wurden auch die zentralen Komponenten erneuert und verstärkt, um dem gesteigerten Bedarf Rechnung tragen zu können. In insgesamt 50 virtuellen Konferenzräumen können nun bis zu 2.000 Teilnehmer eine Videokonferenz abhalten.



Anfang 2022 wird diese Phase der Erweiterung mit der Einführung eines Passcode-Schutzes für die virtuellen Konferenzräume und die Möglichkeit, über Webbrowser von extern – so wie das von intern bereits möglich ist – an Videokonferenzen des BMLV teilzunehmen abgeschlossen. Damit entfällt für externe Teilnehmer die Notwendigkeit einer Installation der Webex Teams App.

Information Labelling



Gem. den Zielsetzungen in der IKT-Strategie sind bis 2025 IKT-Sicherheitsservices auf zentraler und dezentraler IKT-Infrastruktur bereitzustellen, die unter anderem dem gesicherten Informationsaustausch zwischen unterschiedlichen Informations- und Sicherheitsdomänen dienen und einen unzulässigen Datenabfluss verhindern.

Hierzu werden umfassende Fähigkeiten zum Thema „Information Labelling" im BMLV/ÖBH benötigt. „Information Labelling" beschreibt Zusatzinformationen, welche an jedes beliebige Datenformat angehängt oder integriert werden. Dieser Information Label enthält zum Beispiel Informationen in Bezug auf die Klassifizierung der Daten oder Regeln zur Weitergabe der Daten.

Der Informationsaustausch zwischen unterschiedlichen Sicherheits- und Informationsdomänen soll zukünftig über Information Exchange Gateways (IEGs) erfolgen. Ein IEG besteht aus den Modulen „Node Protection", „Information Protection", „Information Exchange" sowie dem „IEG Management". Im Modul „Information Protection" werden die ausgehenden Daten anhand der angehängten oder integrierten Label überprüft, ob diese in eine andere Sicherheitsdomäne übertragen werden dürfen. Im Jahr 2021 wurde die Anforderungsanalyse unter Berücksichtigung von nationalen und internationalen Standards und Normen gestartet.

TKV

Im Telekommunikationsverbund (TKV) steht Ende 2021 und Anfang 2022 ein wichtiger Meilenstein an. Nach dem Abschluss der Bewertung der eingegangenen Angebote wurde ein vorläufiger Bestbieter ermittelt, mit dem nun ein Test vor Zuschlag durchgeführt wird.

Ziel dieses Tests ist es, die Erfüllung der Muss-Forderungen der Leistungsbeschreibung zu überprüfen und

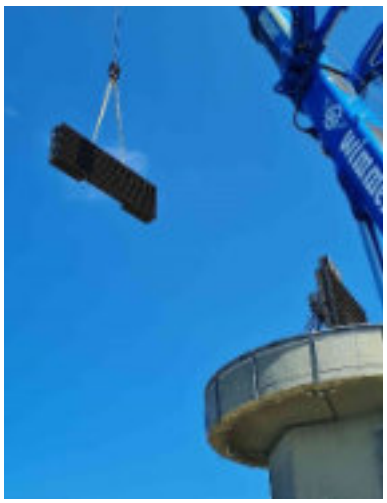
damit die Fähigkeit des angebotenen Systems, sich in die bestehende Infrastruktur des BMLV einzugliedern.

In der zweiten Jahreshälfte 2021 wurde damit begonnen, diesen Test vorzubereiten, indem ein umfangreiches Testbed aufgebaut und konfiguriert wurde. Besonders erfreulich war in diesem Projekt die reibungslose Zusammenarbeit der Bereiche Technik, Betrieb, Applikationen und Sicherheit.

Umbau KOL

Zur Einhaltung der elektrischen Sicherheit, festgelegt in der Norm IEC 60364 bzw. ÖVE/ÖNORM E 8001, musste LEONARDO S.p.A. die interne Stromversorgung der Radaranlage anpassen. Die Planung der erforderlichen Umbauten wurde in Zusammenarbeit mit ARWT/ET geprüft.

Nach den ersten Überprüfungen an der Radaranlage zeigte sich die Notwendigkeit, Nachbesserungen durchzuführen. Diese erforderlichen Korrekturen wurden mit LEONARDO S.p.A. vereinbart und geplant.



Im April und Mai 2021 erfolgten Nachbesserungen im Bereich Software und elektrische Sicherheit durch LEONARDO S.p.A.. Die Systemprüfungen im Juni, direkt am Radarsystem, wurden für die Teile Bedienung und militärischer Mode 5 in Zusammenarbeit mit KdoLRÜ und RadB durchgeführt.
Des Weiteren erfolgte die Qualitätsprüfung der Datenübertragung an EZ/B mit ADV/LRÜ.

Im Juli gingen die finalen Systemprüfungen im Bereich elektrische Sicherheit in Zusammenarbeit mit ARWT/ET sowie die finale Zertifizierung der Hebesysteme mit dem TÜV-Austria vonstatten. Danach erfolgte die positive Systemabnahme des Radarsystem ORS Kolomannsberg.

Wegen eines schwerwiegenden Hagelschadens am Radom der alten Radaranlage wurde der für 2022 vorgesehene Abbau in diesem August vorgezogen.

Im Anschluss konnte der Systemkurs für die Radaranlage am Kolomannsberg durch LEONARDO S.p.A gestartet werden.

LAN-Konsolidierung

Das Projekt LAN-Konsolidierung wurde mit 2019 gestartet, wobei die Umstellungsphase mit 2021 begonnen hat. Das Vorhaben wird sich über einen Zeitraum von mehreren Jahren erstrecken. Ziel ist es, mehrere ähnlich klassifizierte Netzwerke und deren Infrastruktur durch Einsatz von Virtualisierungstechnologie auf einer Infrastruktur abzubilden. Ein Nebenziel ist es, sogenannte „Insellösungen" zu integrieren und somit einer geordneten Erhaltung und Weiterentwicklung zu unterziehen. Im Rahmen des Projekts werden ca. 3.000 Switches berücksichtig. Die aus dem Projekt generierten Vorteile sind:

- Freispielen von Leitungen aufgrund HW-Konsolidierung
- Erhöhung der Netzwerkgeschwindigkeit durch Einsatz „State of the Art" Technologien
- Verschlüsselung der Leitungen innerhalb einer Liegenschaft
- Kostenreduktion durch
  - den Einsatz einer geringeren Anzahl von Switches,
  - optimale Ausnutzung von Anschlusskapazitäten,
  - einen geringeren Stromverbrauch der eingesetzten Hardware sowie durch
  - die Reduktion der Wartungskosten.

Mit Ende November 2021 wurden 25 Liegenschaften mit ca. 431 Switches und deren ausgewählten Netzen konsolidiert. Der Bereich IKTTe bedankt sich für die äußerst konstruktive Zusammenarbeit bei den Mitarbeiterinnen und Mitarbeitern der Organisationselemente IKT(of)/Dispo-&BetrFü/Dion4, Bereich IKT-Betrieb/Dion 6 IKT und Cyber sowie Abteilung BauWAppl/Appl/Dion 6 IKT und Cyber .

Soldatenfunkgerät

Durch die Ausrüstung der Soldaten mit Soldatenfunkgeräten und Headset mit integriertem Gehörschutz sowie der Möglichkeit der Positionsanzeige im Bedarfsfall, soll eine wesentliche Fähigkeitssteigerung im gefechtstechnischen Bereich (Ebene Zug-Gruppe-Soldat) erzielt werden.
Ziel des Vorhabens ist die Beschaffung und Einführung von 2.530 Stk. Soldatenfunkgeräten mit einem modularen Headset-System, in einer Standardausführung für den Betrieb mit dem Soldatenfunkgerät sowie auch in einer Kommandantenausführung für den Betrieb mit dem Soldaten- als auch dem eingeführten Truppenfunkgerät.

Das Headset-System umfasst einen integrierten Gehörschutz mit der Nutzung von In-Ear Headset oder alternativ, einem im BMLV eingeführten und als Option zu beschaffenden, Over-Ear Headset.
Das Soldatenfunkgerät und Headset mit integriertem Gehörschutz in einer gehärteten, militärischen Ausführung umfasst folgende grundlegenden Leistungsmerkmale und Fähigkeiten:

- Nahezu lautlose sichere Kommunikation innerhalb der Gruppe über Entfernungen bis zu 500 m (unter Nutzung der Relaisfähigkeit auch höhere Reichweiten)
- Erhöhung der taktischen Führungsfähigkeit innerhalb der Orgelemente
- Verbesserung der Eigensicherung und Reaktionsfähigkeit bei Krisen- und Notfallsituationen
- Hohe Verfügbarkeit
- Begrenzte Störfestigkeit und Abhörsicherheit (Transportation Security[TRANSEC]/ Communication Security [COMSEC]]
- Nutzerseitig volle gefechtsmäßige Handhabbarkeit für die Ebenen der untersten taktischen Führung und Einzelsoldaten zum Betreiben mobiler Funknetze für Sprache
- Möglichkeit der Positionsübertragung der Soldatenfunkgeräte und Darstellung am Gerät oder durch akustische Wiedergabe im Headset
- Integrierte Lösung der Sprachkommunikation (Headset) mit den Gehörschutzanforderungen

Das Ende der Angebotsfrist war mit 19. Jänner 2022 festgelegt. Die im Rahmen des Bewertungsverfahrens durchzuführenden praktischen Tests und Erprobungen sowie Labortests werden im 2. Quartal 2022 durchgeführt. Mit einem Abschluss des Bewertungsverfahrens und Ausschreibung eines Bestbieters ist im 3. Quartal 2022 zu rechnen.

Videoüberwachung an den Netzfunkstellen

Im Rahmen des militärischen Flugfunks werden ortsfeste Netzfunkstellen betrieben, welche für die sichere Abwicklung des militärischen Flugverkehrs erforderlich sind. Da sich die Netzfunkstellen auf unbemannten Höhenstationen befinden, ergibt sich die Notwendigkeit, die Stationen per Videoüberwachung von zentraler Stelle aus zu kontrollieren. Jede Netzfunkstelle ist mit Kameras und Scheinwerfern ausgestattet. Die Geräte sind mittels power over ethernet (POE) angebunden. Die Kameras senden unter anderem bei Eintritt (Pixelveränderung) Informationen an einen zentralen Sicherheitsserver. Die Technische Betriebs Überwachung (TBÜ) bei LRÜ hat durchgehend (7/24) die Möglichkeit, den Zustand der Netzfunkstellen zu überwachen.

Das System wurde im Jahr 2021 auf weiteren Netzfunkstellen installiert und in Betrieb genommen. Die zentrale Sicherheitssoftware wird im 1. Quartal 2022 im Zuge der Erneuerung in der entsprechenden Domäne auf virtuellen Servern aufgebracht bzw. in die für die Bereitstellung der Server implementierten Automatismen integriert.

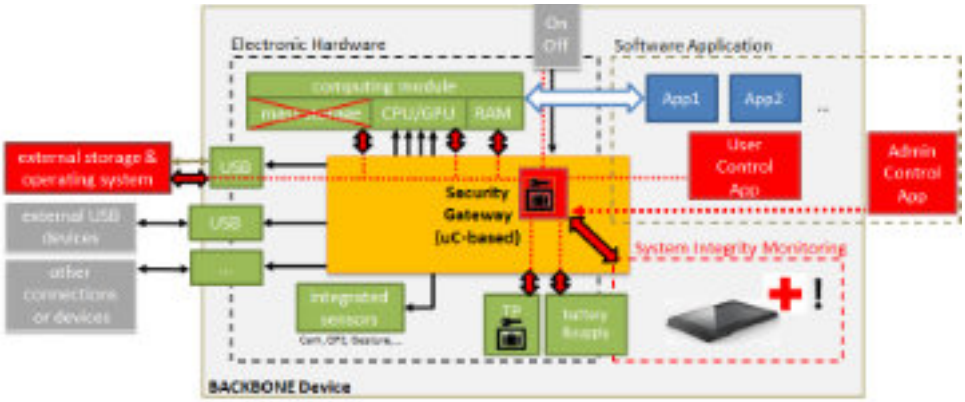
„SD4MSD – Single Device for Multiple Security Domains“

Militärische Einsätze im Feld stellen hohe Anforderungen an IKT-Geräte hinsichtlich Zuverlässigkeit und Sicherheit. Hierzu gehören zum einen die grundsätzliche Geräterobustheit, zum anderen aber vor allem auch die Absicherung gegenüber physischen Attacken und Cyber-Angriffen. Kompromittierungsversuche müssen jederzeit feststellbar sein und gegebenenfalls automatische Alarmierung, (Teil-)Deaktivierungen oder Notlöschung auslösen.

Derzeit am Markt erhältliche Endgeräte verfügen allerdings weder über die notwendige Geräterobustheit, noch unterstützen sie ein zuverlässiges Monitoring der Geräteintegrität. Außerdem lassen sie Maßnahmen vermissen, die es erlauben würden, dasselbe Gerät auf einfache Weise in unterschiedlichen Einsätzen, Sicherheitsdomänen und Klassifizierungsstufen verwenden zu können.

Das Unternehmen MUSE entwickelt eine eigenständige, cyber-physische Gesamtarchitektur für robuste Tablets, mit der Bezeichnung BACKBONE, mittels Implementierung einer allgegenwärtigen, hardwareseitigen Sicherheitsschicht in Form eines autonom agierenden „Security Gateways“, der als zusätzlicher Mikrocontroller realisiert wird (siehe Abbildung), und einer integrierten Überwachung des „Gesundheitszustands“ des IKT-Geräts. Um die Geräte in unterschiedlichen und sich ausschließenden Sicherheitsdomänen verwenden zu können, wird auf einen im Gerät integrierten permanenten Speicher für Betriebssystem und Nutzerdaten verzichtet.

Das Projekt SD4MSD setzt auf diese bisherigen Ergebnisse auf und hat sich zum Ziel gesetzt, ein integrales Gesamtkonzept auf physischer, Hardware- und Software-technischer Ebene für hochrobuste Endgeräte zu erstellen und mit der individuellen Konfigurierbarkeit für spezifische Einsatzzwecke zu kombinieren. Hierbei ist die Sicherstellung von Authentizität, Integrität und Vertraulichkeit über den gesamten Lebenszyklus des IKT-Geräts entscheidend.



Im ersten Forschungsjahr wurde dazu ein umfassender Anforderungskatalog in Form von Anwendungsfällen erstellt, die aus Sicht des BMLV zentral sind. Anschließend wurden Angreiferprofile (z.B. Innentäter) und Angriffsvektoren (z.B. Manipulieren des Endgeräts zum automatisierten „Leaken“) erstellt und nach ihrer Kritikalität und Eintrittswahrscheinlichkeit bewertet (Bedrohungsanalyse). Darauf aufbauend wurden geeignete Gegenmaßnahmen erarbeitet, die schließlich in Sicherheitsanforderungen und Mitigationsmaßnahmen für das Gerätekonzept mündeten. Mit diesem Anforderungsportfolio wird derzeit ein ideales und wissenschaftlich begründetes Gesamtkonzept für die Geräte-Hard- und -Software entwickelt, das parallel mit dem aktuellen Gerätestatus der Fa. MUSE verglichen wird (Abweichungsanalyse).

Im folgenden Forschungsjahr wird das Ziel verfolgt, die identifizierten Lücken möglichst zu schließen und die im Rahmen dieses Projekts umsetzbaren Entwicklungspunkte zur Validierung des Gesamtkonzepts in Form eines Demons-

trators zu realisieren. Neben der funktionalen Validierung des Demonstrators durch den Bedarfsträger werden auch Penetrationstests durchgeführt, um die Erfüllung der nicht-funktionalen Sicherheitsanforderungen sicherzustellen.

Magic Numbers

Dieses Jahr sind zwei Zahlen erreicht und überschritten worden, die sowohl etwas über die Komplexität, über die Größe, aber auch über die dahinterliegende Arbeit Auskunft geben:

6666-te kpm Merge

Logo: Gitlab

Am 09.01.2014 erfolgte der erste Merge im Versionsverwaltungssystem Gitlab zur Übernahme einer Software-Eigenentwicklung für das Projekt kpm (Kamino Puppet Module) in die Produktion.

Mit 10.06.2021 wurde der 6666-te Merge eines kpm-Modules durchgeführt. Der Tag ist an uns vorübergegangen wie jeder anderer. Es gab keine Ausfälle und wir haben danach auch nicht im Lotto gewonnen. Auch die partielle Sonnenfinsternis an diesen Tag zwischen 11:54 und 13:28 war nicht der Rede wert, da maximal 4% der Sonne vom Mond abgedunkelt waren.

Zwischenzeitlich haben wir mit Stand 29.11.2021 im Gitlab folgende Kennzahlen für das kpm Projekt:

- 7.122 merges (Übernahme in die Produktion)
- 310 Branches (Abzweigung von der Hauptlinie, wobei im Branch die Arbeit fortgesetzt wird und nach Fertigstellung des Arbeitspaketes im Branch dieser wieder in die Hauptlinie integriert wird)
- 22.965 Commits (Änderungen, die versioniert worden sind)

1001 VM

Am 23.08.2021 wurde die eintausendunderste Virtuelle Maschine (VM) in der zentralen VMware-Virtualisierungsumgebung im Objekt 6, in der STIFT Kaserne, in Betrieb genommen und die 1.000-er Grenze überschritten. Diese zentrale Virtualsierungsumgebung ist hochredundant nach dem Prinzip „no-single-point-of-failure“ quer über alle erforderlichen IKT-Infrastrukturkomponenten ausgelegt, um einen unterbrechungsfreien Betrieb zu ermöglichen.

Damit werden nicht nur über 1.000 Virtuelle Maschinen betrieben, sondern diese auch administriert, aktualisiert und überwacht. Bis auf ein paar wenige Virtuelle Maschinen handelt es sich bei diesen um virtuelle Server, die mit Kamino laufen.

Die virtuellen Server bzw. Virtuelle Maschinen werden auf physischen Servern betrieben, wobei diese Virtualisierungs-Hosts ihre Ressourcen als virtuelle CPUs und virtuellen Hauptspeicher den Virtuellen Maschinen zur Verfügung stellen. Dies lässt sich am einfachsten mit einer Getränkekiste vergleichen, wo der physische Server, der Virtualisierungs-Host, die Kiste ist und die Virtuellen Maschinen die Flaschen, welche in der Kiste transportiert werden.

Logo: VMware

TCNM/Liegenschaftsserver NEU

Im Rahmen des Vorhaben TCN (Tactical Communication Net) war auch das TCN-Managementsystem (TCNM) als Serverlösung bereitzustellen. Dies erforderte unsere Planungen für einen neuen Liegenschaftsserver diesem Vorhaben unterzuordnen. Jedoch bot es die Möglichkeit, unsere geplanten Konzepte und Neuerungen vorab anhand des TCNM-Servers zu implementieren und somit auch den TCNM-Server zeitgerecht betriebsbereit zu haben.

Die grundlegendste Änderung des Liegenschaftsservers NEU ist die Virtualisierung. Wobei nun das erste Mal nicht nur auf Servern der zentralen Infrastruktur, sondern auch auf Servern der dezentralen Infrastruktur, den Liegenschaftsservern, virtualisiert wird und es so möglich ist, mehrere virtuelle Server auf einem Liegenschaftsserver zu betreiben.

Dies bietet mehr Flexibilität in Bezug auf Zuständigkeiten, Services und Updatezyklen einzelner virtueller Server.

Am Beispiel des TCNM-Server stellt es sich wie folgt dar:

Am physischen Server Virtualisierungshost laufen die beiden virtuellen Server Liegenschafts-Server mit Kamino Release Dagobah und TCNM-Server für das TCN-Managementsystem mit Kamino Release Lonera. Bei Bedarf können noch weitere virtuelle Server wie z.B. MTM-Server oder andere Services, die als eigene virtuelle Server erforderlich sind, darauf betrieben werden.

Bis Ende 2022 wird die Ablöse der alten Liegenschaftsserver, sowohl Hardware als auch Software, durchgeführt werden. Die Basis für den neuen Liegenschaftsserver-Klon ist für den physischen Server bereits implementiert und anhand des TCNM-Servers auch erprobt. Der neue virtuelle Liegenschaftsserver mit Kamino Release Lonera ist in Entwicklung und die Integration der Liegenschaftsserver-Services ist in Arbeit. Die Beschaffung der neuen Server für die Hardware-Erneuerung ist in Vorbereitung und erfolgt im 1. Quartal 2022.

Logo: Kamino

KAMINO Releases

Wie bereits letztes Jahr im Beitrag „SMN-Wartung Kamino-Server" erläutert, wird die Serverinfrastruktur des ÖBH – sowohl zentral als auch dezentral – täglich auf den aktuellen SW-Stand gebracht. Denn nur aktuelle Systeme sind auch sichere Systeme.

Die Grundlage des Kamino-Serverklons, aber auch der gesamten Kamino-Umgebung mit seinen Entwicklungs-, Test- und Managementsystemen, bildet das Betriebssystem Red Hat Enterprise LINUX der Firma Red Hat. Daher richten sich die Kamino Releases auch nach dem Red Hat Release-Zyklus.
Für den davon abgeleiteten Kamino Release-Zyklus haben wir uns folgende Ziele gesetzt:

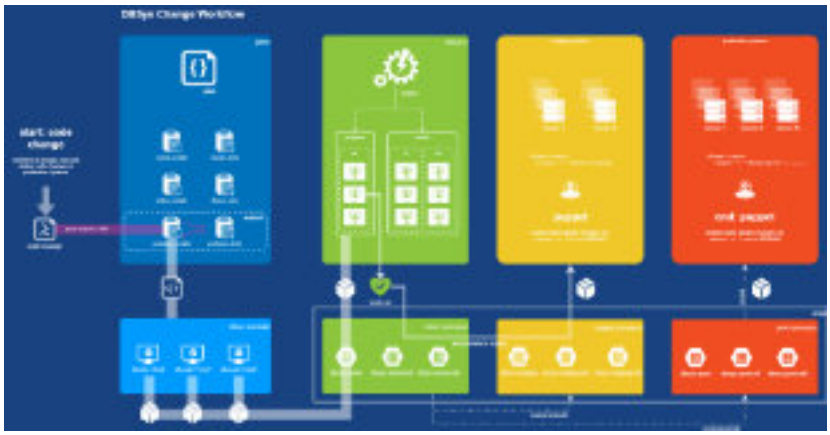
- Es wird kein Release ausgelassen
- 4 Wochen nach genereller Verfügbarkeit einer neuen RHEL-Version ist diese im BMLV im Einsatz (ab Kamino Release Kizan)
- Veraltete Releases werden deaktiviert (EOL-End of Life)

Aufgrund der Erfahrungen mit den Kamino Releases Fornax und Jakku konnte der Zeitraum für die Integration einer neuen Release, für die Bereitstellung der dafür erforderlichen SW-Pakete, für die Anpassung der Kamino-Umgebung und für das Testen auf 4 Wochen reduziert werden.
Der Kamino Release-Zyklus bis Mai 2024 stellt sich, basierend auf den RHEL 8 Planning Guide, wie folgt dar:

RHEL-Version	Kamino Releasename	Red Hat generelle Verfügbarkeit	Kamino generelle Verfügbarkeit	Status
RHEL8.2	Fornax	28.04.2020	20.07.2020	EOL 07.04.2021
RHEL8.3	Jakku	03.11.2020	22.01.2021	EOL 13.07.2021
RHEL8.4	Kizan	18.05.2021	28.05.2021	AKTIV
RHEL8.5	Lonera	09.11.2021	30.11.2021	AKTIV
RHEL8.6	Mandalore	Apr/Mai 2022	+ 4 Wochen	
RHEL8.7	Naboo	Okt/Nov 2022	+ 4 Wochen	
RHEL8.8	Ordo	Apr/Mai 2023	+ 4 Wochen	
RHEL8.9	Plexis	Okt/Nov 2023	+ 4 Wochen	
RHEL8.10	Quintil	Apr/Mai 2024	+ 4 Wochen	

CI/CD (Continious Integration/Continious Development)

Der im Referat DBSys implementierte CI/CD Workflow beschreibt die laufenden und sehr zeitnahen Releases von Code- und Konfigurationsänderungen. Die nachfolgende Visualisierung skizziert den vollautomatisierten Weg einer Codeänderung: installierbares Serverpaket (RPM; blau), Deploy am Testsystem, Integration Tests über mehrere Versionen/Architekturen hinweg (grün), und schließlich Release in ausgewählte „Staging" Systeme (gelb), sofern die Tests ok sind. Der Release auf die restlichen Produktionssysteme (rot) wird manuell durch einen DBA freigegeben.



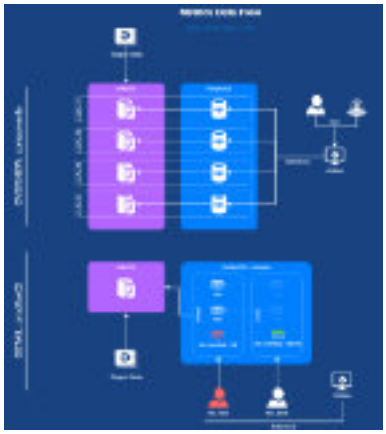
Die durchgehende Automatisierung dieser Prozesse und die damit einhergehende Geschwindigkeit und Qualitätssicherheit (Test Framework) ermöglicht viele kleine, überschaubare Releases und vermeidet Configuration Drift zwischen den unterschiedlichen Systemen und Umgebungen.

Durch den beschriebenen CI/CD Workflow und die automatisierte Testinfrastruktur im Referat Datenbanksysteme konnte die neue Oracle21c Release mit „Pluggable Database" Architektur in wenigen Tagen in die Automatismen integriert werden.

Oracle 21c wird vom Hersteller als sogenannte „Innovation Release" für Tests der neuen Architektur und Features bereitgestellt, wobei aber der Einsatz im Produktionsbetrieb nicht empfohlen wird. Eine massive Änderung ist der zwingende Einsatz von „Pluggable Databases" als Basisarchitektur und dadurch der Wegfall der Standalone DB Installation.
Durch die Bereitstellung der Oracle 21c Release konnten wesentliche Vorbereitungen für die nächste produktionstaugliche Version geschaffen werden, welche auf die neue Basisarchitektur („Pluggable Database") aufsetzen wird.

Monitoring/Metrics Collection

Eine der Herausforderungen in der Administration einer hochkomplexen IT-Infrastruktur im Umfang von tausenden Elementen ist es, den Überblick zu behalten und den aktuellen Status sowie Fehlentwicklungen erkennen zu können.



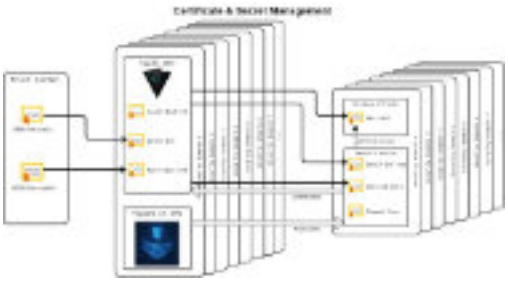
Die zugrundeliegende Monitoring und Metrics Collection Infrastruktur wurde um PostgreSQL Instanzen erweitert (blau), welche direkten Zugriff auf die Rohdaten in der InfluxDB Timeseries Databases (lila) haben.

Die PostgreSQL Instanzen ermöglichen einerseits die Aufbereitung, Aggregierung und Zusammenführung der Rohdaten, andererseits ein feingranulares Berechtigungsmanagement für Zugriffe auf sensible Daten und Messwerte.

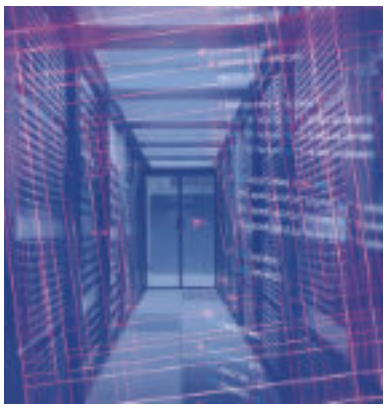
Die gesammelten und aufbereiteten Daten sind für den End-User in Grafana (Opensource Analytics & Monitoring Solution) via verschiedenste Dashboards und Panels visualisierbar.

Certificate & Secret Management für Kamino/ SMN

Um die Sicherheit aller Systeme und Services zu erhöhen, sind SSL/TLS Certificates notwendig. Durch die steigende Anzahl und die Forderung nach geringerer Lebensdauer der Certificates wird der administrative Aufwand des Certificate Management enorm und zwingt zur Automatisierung. Der komplette Certificate Lifecycle soll automatisiert erfolgen.



Da die Trust Center CAs ausschließlich im SMN erreichbar sind, und die Automatismen in jeder Umgebung (SMN, ICMD, IKTSysE, etc.) benötigt werden, ist es erforderlich, ein zentrales Infrastruktur Service für das Certificate Management in jeder Umgebung zur Verfügung zu stellen.



Automatisierung von Infrastruktursoftware – ein Beispiel

Die LOGIS-Infrastruktur besteht aus unterschiedlichsten Applicationserver-, Webserver- und Loadbalancer-Komponenten, wobei es zwischen diesen Systemen zahlreiche Abhängigkeiten gibt. Es wäre zum Beispiel möglich, dass das Deployment einer Applikation im Application Layer ordnungsgemäß funktioniert, der Anwender diese aber nicht verwenden kann, weil es ein Problem im Identity Management Layer gibt und daher Single-Sign-On nicht funktioniert.

Die Release-Zyklen der Hersteller sowohl beim Betriebssystem als auch bei den Services werden immer kürzer. Security Patches und Aktualisierungen für Softwarefehler müssen bei Bedarf installiert und auch getestet werden – manuell würde das auf Dauer im Chaos enden.

In der Continuous Integration (CI) LOGIS Infrastruktur wird mit dem Opensource Produkt Jenkins die gesamte CI-Pipeline auf Knopfdruck ausgeführt. Dabei werden die virtuellen Server neu installiert und alle Layer der LOGIS Infrastruktur mit der entsprechenden Software voll automatisch provisioniert.
Der nicht unerhebliche Aufwand für die Realisierung dieses Automatisationsprozesses resultiert auf der Gegenseite in einer Einsparung beim Testaufwand. Er bietet den Komfort, bei einer kleinen Änderung einer Komponente das Gesamtsystem mit allen seinen Abhängigkeiten testen zu können.

Die entwickelten Automatismen konnten vom Referat

Integrations-Software, bei der Umstellung der Entwicklungs-, Test- und Produktionsumgebungen für das Logistische Informationssystem des Österreichischen Bundesheeres auf das neue Server Betriebssystem Red Hat Enterprise Linux 8 (RHEL8) erfolgreich zum Einsatz gebracht werden.

Es werden JAVA Applikationen sowie Oracle Forms Anwendungen auf Applikationsservern eingesetzt und im Produktivsystem sind rund 2.000 Anwender gleichzeitig aktiv. Lastverteilung sowie Konzepte für Ausfallsicherheit durch den Einsatz von Clustertechnologien sind fixer Bestandteil bei der Planung der Infrastruktur.

Mit der Umsetzung eines mehrstufigen Sicherheitskonzeptes sowie dem Einsatz von Verschlüsselungstechnologien zwischen den Systemen bzw. den funktionellen Schichten werden die hohen internen IKT-Sicherheitsanforderungen erfüllt.

RHEL7 Umstellung der ZEDVA

Die Server der ZEDVA sind die Basis für die Bereitstellung der zentralen Funktionen des Personalinformationssystems PSNT (PERSIS, ERGIS, UNIS, etc.), der Anwendungen ORGIS, MILIS und EPEP sowie aller Teilanwendungen des Zentralen Berechtigungssystems (Chipkartenverwaltung, Zugriffsrechteverwaltung, etc.). Im Oktober 2021 fand die Umstellung dieser Server, nach einer Vorbereitungszeit von einem Jahr, auf die Betriebssystemversion RHEL 7 statt. RHEL 7 wird bis mindestens 2024 mit aktuellen Updates versorgt und bringt neben erhöhter Sicherheit (Firewall, SELinux) eine Modernisierung aller Softwarekomponenten und damit bessere Funktionalität, Performance und Stabilität.

Die Übersichtskizze zeigt das Entwicklungssystem der ZEDVA. Zusätzlich zum Entwicklungssystem wurde das Testsystem (6 Server) und das Produktionssystem (8 Server) umgestellt. Die Umstellung des Produktionssystems konnte trotz komplettem Austausch aller Server mit einer minimalen Betriebseinschränkung von nur 3 Stunden durchgeführt werden.

JIRA Umstellung auf Version 8

Das ITSM-Werkzeug JIRA wird sowohl im Bereich der Softwareentwicklung für Fehlerverwaltung, Problembehandlung und operatives Projektmanagement als auch als Ticketing-System für den IT-Support eingesetzt. JIRA kann durch seine Funktion zur Ablauforganisation auch für Aufgabenmanagement und Anforderungsmanagement verwendet werden.

Alle sich im Einsatz befindlichen Systemumgebungen des ITSM Werkzeugs JIRA wurden im März 2021 auf RHEL 7.9 migriert. Diese Umstellung war nötig, weil das End of Life (EoL) der Vorgängerversion im August dieses Jahres erreicht worden wäre. Der Support der aktuellen Version wird von der Firma Red Hat bis Juni 2024 zur Verfügung gestellt. Somit werden wichtige Bug Fixes und sicherheitsrelevante Updates weiterhin unterstützt.

Die Firma Atlassian beendet den Support für die JIRA-Server-Produkte mit Februar 2024, somit sollte eine weitere Umstellung der RHEL-Umgebung und der damit verbundene Aufwand nicht nötig sein. Die dadurch gewonnene Zeit kann für die Produktsuche und Einführung des Nachfolgeproduktes verwendet werden.
Das letzte große Update des ITSM-Werkzeugs JIRA wird planmäßig im Dezember 2021 auf der Produktions-Umgebung durchgeführt. Die Entwicklungs- und Testumgebung wurden bereits auf die Version 8.17.0 migriert. Die neue Version bringt Verbesserungen im Bereich Performance und Stabilität. Des Weiteren werden weitere Funktionen zur Verfügung gestellt, die es beispielsweise den Benutzern erlauben eine genauere Suche nach Tickets durchzuführen.

Für die Umstellung wurden die internen Erweiterungen angepasst und teilweise verbessert. So wird beispielsweise ein besseres Controlling des Lizenzsystems von JIRA unterstützt.

IKT&CySihZ

24/7

Militärische Cybersicherheit

WIR SCHÜTZEN ÖSTERREICH.

bundesheer.at

UNSER HEER

MilCyZ

Bereich Militärisches Cyberzentrum

Im zweiten Jahr des Bestehens des Militärischen Cyber-Zentrums wurde der Weg fortgesetzt, dieses Element als zentrales Kompetenzzentrum mit Spezialisten der Cyber-Sicherheit und Cyber-Defence aufzubauen (SCU - Special Cyber Unit) (vgl. S76). Auch 2022 müssen die Cyber-Defence-Systeme des Ressorts laufend an geänderte Angriffsmethoden angepasst und erweitert werden um gegen neue Angriffe bestehen zu können. Zentrale Fähigkeiten der CIS-Defence sind auch der Monitoring-, Alarmierung-, und Defence-Operationsprozess der Cybersicherheit. Auch der Aufbau dieser Fähigkeiten im MilCERT (militärische Computer Emergency Readiness Team) wurde fortgeführt und die Integration von Log-, SIEM- und Vulnerability-Managementsystemen in die IKT-Services aller Teilstreitkräfte aufgebaut. Dies ist auch die Basis des 2020 gestarteten Projektes zur Darstellung des ebenengerechten militärischen Cyberlagebildes zur Eigenlage des Ressorts in der Cyber-Domäne.

Um als militärische Organisation auf die permanent steigenden Bedrohungen aus dem Cyber-Raum effektiv und effizient reagieren zu können, sind die Sicherheitsaufgaben im IKT-, Cyber- und EloKa-Bereich in diesem Element konzentriert und in permanenter Optimierung. So wurde 2021 mit dem Aufbau von Rapid Response Teams (RRTs) gestartet, welche anlassbezogen und vorfallspezifisch in Form einer Truppeneinteilung aus dem MilCyZ herausgezogen und zielorientiert eingesetzt werden. Diese Struktur wird durch die Etablierung einer militärischen Cyber-Range/Cyber-Tüpl für den speziellen Fähigkeitsbereich der Cyber-Defence erweitert, um so auch entwickelte Cyber-Verteidigungswaffen auf Wirkung zu prüfen und Cyber-Defender in deren Einsatz zu schulen.

Die aktuell umgesetzte Quantität befähigt das MilCyZ den Aufgabenbereich der Basissicherheit und CIS-Defence (Cyber Information Systems) der IKT-Landschaft und der Bereitstellung einer Einsatz-EloKa-Datenbank zum Schutz mil. Truppen grundlegend wahrzunehmen. Aufgrund der - auch im mil. Umfeld - immer stärker wachsenden Vernetzung und Integration atypischer Komponenten (Steuersysteme, Waffensysteme, Sensoren, Effektoren, Software-Defined-Systems) ist der Spagat zwischen Funktionalität und Sicherheit immer

Dipl.-HTL-Ing. Lambert Scharwitzl, MA, MSc

schwieriger festzulegen. Daher kommt der IKT-Sicherheit im konzeptionellen Umfeld immer größere Bedeutung zu und Sicherheit ist von der „ersten Idee" bis zum laufenden Betrieb ein permanenter Faktor in der IKT-Landschaft.

Dass dieser Grat zwischen Sicherheit, Vernetzung und „Shared Funktionalität" sehr schmal ist, wurde der Republik auch 2021 mehrfach aufgezeigt. Cyber-Sicherheit bedeutet natürlich auch den teilweisen Verzicht moderner Features der zivilen Welt und Remote-Anbindung immer und überall (auch von nicht-militärischen Komponenten) wird auch nicht immer möglich sein. Schließlich muss das ÖBH noch funktionieren (Führungs- und Einsatzfähigkeit), wenn der Rest der IT-Welt der Republik nicht mehr kann, oder massive Cyber-Probleme hat.

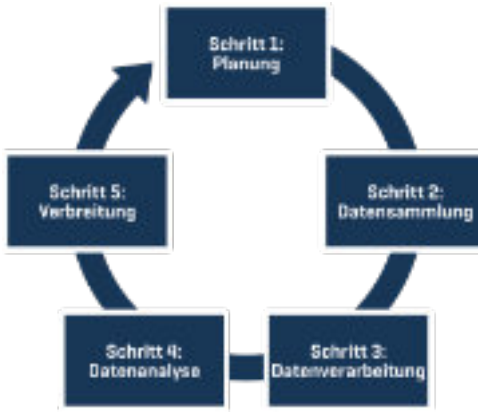
2021 wurden massive Angriffe auf die Infrastruktur des BMLV/ÖBH (SMN, DGMN, Goldhaube, Einsatzumgebungen...) erkannt, konnten jedoch durch die Cyber-Verteidigungssysteme des MilCyZ bisher erfolgreich abgewehrt werden. Der quantitative Umfang, aber auch die Qualität der Angriffe auf das Ressort sind 2021 massiv gestiegen und die aktuellen Ressourcen (speziell personelle) an deren Grenzen gestoßen. Dies ist bereits auf einen Level gestiegen, dass Spezialisten der Cyber-Sicherheit aus Projekten abgezogen werden müssen, um die Sicherheit von IKT-Systemen und –Services aufrecht erhalten zu können.

Auch im dritten Aufgabenspektrum des MilCyZ/UZEloKa, wurde massiv in den Aufbau einer RCIED-Datenbank (Radio Controlled Improvised Explosive Devices) investiert und erste Funktionalitäten geschaffen, um technische Einsatz-Datenbanken für den Schutz der eigenen Truppen im Einsatz bereitstellen zu können.

Das MilCyZ wird bei der Abwehr von Bedrohungen und Angriffen aus dem Cyberraum wirksam. Um diesen Schutz durchzuführen, ist die durchgängige, konsequente Abdeckung aller Aspekte der IKT- und Cybersicherheit nötig. Das MilCyZ plant und implementiert die Sicherheitssysteme für Eigenschutz und Verteidigung des ÖBH im Cyberraum.

Im Fall erkannter Cyberangriffe sind Kräfte zur Erkennung, Eindämmung und Abwehr verfügbar. Unverzichtbar ist die Erfassung & Darstellung der aktuellen Cyberlage auf Basis eigener Daten und Informationen von Partnern. MilCERT koordiniert Maßnahmen bei IT-Sicherheitsvorfällen, warnt vor Sicherheitslücken und stellt zukünftig Rapid-Response-Teams.

Erweiterung der Fähigkeit technischer Cyber Threat Intelligence



Skizze: MilCyZ/SihOpZ

Das IKT-Gesamtsystem des BMLV ist im Cyberraum ständigen Bedrohungen ausgesetzt. Zu diesen Bedrohungen zählen u.a. technische Schwachstellen in eingesetzten IKT-Produkten oder Konfigurationsfehler. Darüber hinaus ist aber auch die sich ständig ändernde Gefährdungslage, etwa durch neue Angriffstechniken oder Taktiken der Angreifer, sowie laufend angepasster Schadsoftware („Malware"), eine stete Herausforderung. Für das BMLV als Verteidiger gilt es, zu 100% „richtig" zu liegen und alle möglichen Bedrohungen zu identifizieren sowie Gegenmaßnahmen umzusetzen, BEVOR diese ausgenutzt werden.

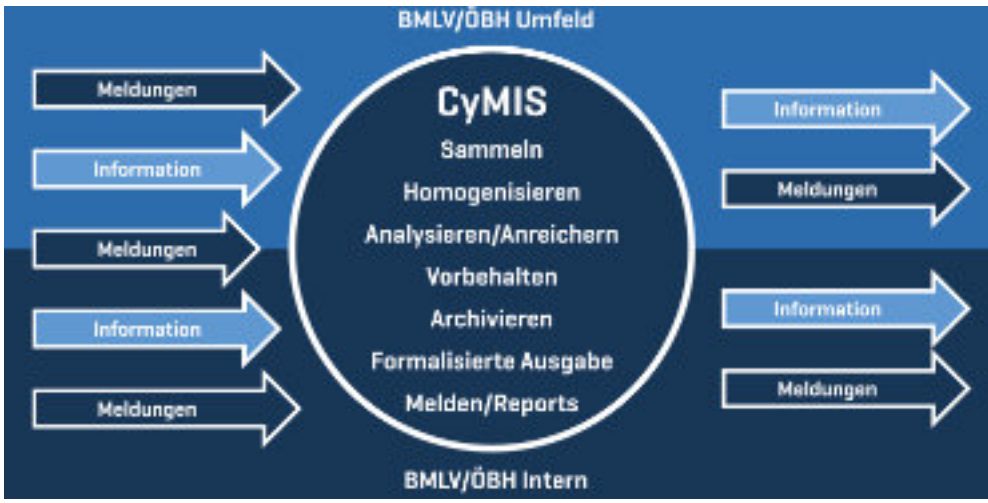
Im Gegensatz dazu muss ein Angreifer nur einmal eine Lücke finden um diese erfolgreich ausnutzen zu können. Zwar können nicht alle Angriffe im Voraus verhindert werden, dafür stehen weitere, detektive und reaktive Fähigkeiten zur Verfügung. Dennoch kann ein Großteil der Versuche, in das IKT-System des BMLV einzudringen, durch geeignete Mittel verhindert werden.

In diesem Hinblick ist das Militärische Cyberzentrum laufend dabei, das Wissen um aktuelle Bedrohungen auf aktuellem Stand zu halten und so zeitgerecht auf neue Trends reagieren zu können. Dazu ist die Sammlung, Verarbeitung, Analyse und Verbreitung an relevante Stellen innerhalb sowie an Partner des BMLV von Informationen über ebendiese Bedrohungen essenziell. Um dies zu erreichen, wurde 2021 der Grundstein für ein koordiniertes Cyber Threat Intelligence Programm gelegt. Die Prozesse sowie die Architektur des Programmes wurden, in Anlehnung an den „Intelligence Cycle" (siehe Abbildung), neu geplant und mit der konkreten Umsetzung begonnen. Künftig wird es möglich sein, technische Information aus dem Bereich der „Threat Intelligence" so zu verarbeiten, dass Techniker in ihrem Bereich die erforderlichen Informationen zur Verfügung haben. Dies dient der Umsetzung gezielter und zeitnaher Gegenmaßnahmen im gesamten IKT-System des BMLV zur Minimierung des Risikos. Damit wird ein essenzieller Beitrag zur Erhöhung der gesamten IKT-Sicherheit des BMLV geleistet.

Für die Zukunft gewappnet mit dem Militärischen „Cyber Melde und Informationsservice" (CyMIS)

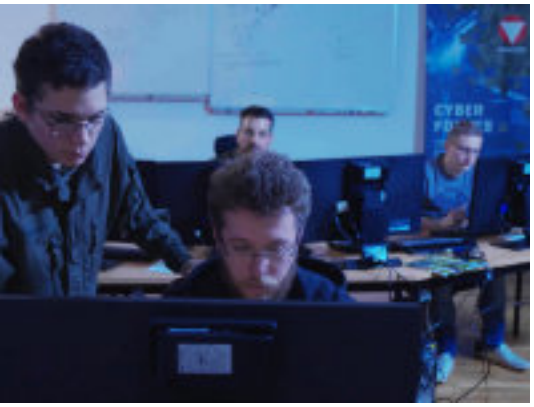
Die Vision des Mil-Cyber-LZ lautet: „Das Militärische Cyberlagezentrum liefert alle für das taktische, operative und strategische militärische Entscheiden notwendigen, cybersicherheitsrelevanten Informationen, zu jeder Zeit, in der benötigten Form, an jeden beliebigen Ort."

Um diese Vision wahr werden zu lassen, arbeitet das Mil-Cyber-LZ bereits seit einigen Jahren an einem entsprechenden Konzept und dessen Umsetzung. Teilaspekte werden mithilfe von BMLV/OEBH internen und externen Partnern erarbeitet.
Forschungsprojekte, welche aktuell mit internen Bedarfsträgern und externen Forschungspartnern betrieben werden, stellen dafür eine fundierte wissenschaftliche Basis sicher. Dies mündet in einem Vorhaben (Projekt), welches den Lagebilderstellungsprozess, soweit sinnvoll möglich, digitalisiert. Die Zielsetzung ist es, ein Service zu entwickeln, welches es, grob gesprochen, erlaubt Informa-



Grafik: MilCyZ/SihOpZ

tionen (z.B. auch in Form von Meldungen), dort wo sinnvoll, automatisiert zu sammeln, zu speichern, zu homogenisieren, zu analysieren, mit Zusatzinformationen anzureichern, mit bekannten Daten zu korrelieren und entsprechende Reports (auch in Form von „Echtzeit"-Dashboards) zu erstellen und Ebenen gerecht zur Verfügung zu stellen. Damit werden die Fähigkeiten des Militärischen Cyberlagezentrums entsprechend dem Auftrag hergestellt bzw. gesichert, weiter ausgebaut und zukunftssicher gemacht.



Mit Hilfe des Militärischen „Cyber-Melde und Informationsservice" kurz „CyMIS" werden also gesammelte Informationen primär zur Erfassung der aktuellen und historischen Cyberlage des BMLV/OEBH verwendet. Dies ist die Basis, um u.a. periodische und anlassbezogene Cyberlagebilder erstellen zu können. Des Weiteren wird es aufgrund der zentral vorliegenden Informationen auch möglich, besser Trends und weitere Zusammenhänge erkennen bzw. ableiten zu können. In Zukunft werden, mit Hilfe des Systems, spezifischere Informationen (Produkte/Lagebilder) rascher für unterschiedliche Bedarfsträger entwickelt und laufend zur Verfügung gestellt.

milCERT Interoperability Exercise 2021 (MIC21)

Das milCERT des BMLV (militärisches Computer Emergency Readiness Team) hat bei der heuer erstmalig stattfindenden Übung MIC21, organisiert durch die Europan Defence Agency (EDA), erfolgreich teilgenommen und dabei den dritten Platz in der Gesamtwertung erreicht. Darüber hinaus wurde die Spezialwertung "Situation Reports" durch das österreichische Team gewonnen.

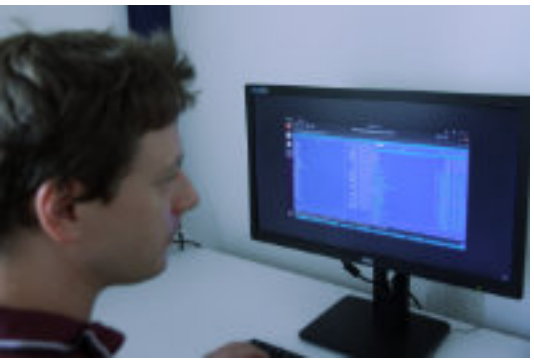
Zusammenarbeit und Informationsaustausch sind ein Schlüsselfaktor bei der Bekämpfung von Bedrohungen im Cyberraum. Daher setzte die EDA bei der neuen Übungsserie (eine Fortsetzung für 2022 wird bereits geplant) den Fokus auf eben diese Themen. Die teilnehmenden Teams mussten in einer virtuellen Umgebung live stattfindende Angriffe auf typische militärische IT-Umgebungen (z.B. Büroumgebung, Befehls-Infrastruktur/„C2", Kommunikationssysteme, kritische Infrastruktur sowie Sensor- und Waffensysteme) erkennen, diese analysieren und relevante Bedrohungen aufzeigen. Darüber hinaus mussten regelmäßig Berichte, so genannte „Situation Reports" (kurz SITREP) erstellt werden, welche ebenfalls bewertet wurden. Diese SITREPS sind insofern relevant, als dass sie die Auswirkungen der erkannten Angriffe (z.B. „Denial of Service" (DoS), Kompromittierung mit Schadsoftware oder vollständige Übernahme) gegenüber der militärischen Führung darstellen. Diese muss anhand der Informationen im Ernstfall ggf. über mögliche weitere Maßnahmen oder Alternativen entscheiden.

Neben der Qualität der Berichte wurde auch der Zeitfaktor, wie schnell Angriffe erkannt und gemeldet werden, sowie die Genauigkeit gewertet.

Ziel der Übung war es, milCERTs innerhalb der EU näher zusammenzubringen um die Zusammenarbeit sowie den Informationsaustausch zu stärken. Darüber hinaus sollten auch gemeinsam Cyber-Sicherheitsvorfälle erkannt und gelöst werden. Daher war es genauso wichtig, neben der „eigenen Infrastruktur" (das virtuelle Übungsnetzwerk) auch die Partner im Hinterkopf zu behalten. Typische Erkennungsmerkmale für Angriffe, so genannte „Indicators of Compromise" (IoC), mussten den anderen milCERTs zur Verfügung gestellt werden. Diese können somit im Anschluss in den eigenen Umgebungen danach suchen und so eventuell übersehene Angriffe retrospektiv erkennen und geeignete Gegenmaßnahmen einleiten.

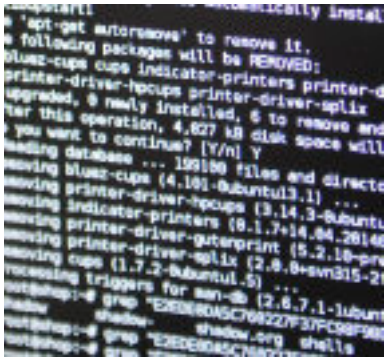
Wie der Estnische Verteidigungsminister, Kalle Laanet, als virtueller Gastgeber in seiner Rede bemerkte, „haben die zivilen CERTs innerhalb der EU bereits sehr gute Kontakte aufgebaut und kontinuierlich verbessert. Im Gegensatz dazu ist dies bei militärischen CERTs noch nicht der Fall. Dies ist, u.a. aufgrund ihrer sensiblen Umgebung, zwar verständlich, dennoch ist es wichtig, Möglichkeiten zur Vertrauensbildung zu schaffen, um den Informationsaustausch zu verbessern. Diese Live-Fire Übung sorgt genau dafür."

Das österreichische milCERT ist bestrebt, auch weiterhin an dieser Übungsserie teilzunehmen, und den Informationsaustausch über Cyber-Angriffe mit Partnern auf EU-Ebene zu verbessern. Denn nur gemeinsam wird es künftig möglich sein, den Herausforderungen im Cyberraum effektiv begegnen zu können.



Sicherheitsaudit und Pen-Testing

Im Rahmen von IKT-Sicherheitsaudits werden neben Eigenentwicklungen auch immer wieder Produkte überprüft, welche auch außerhalb des BMLV zum Einsatz kommen. 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.



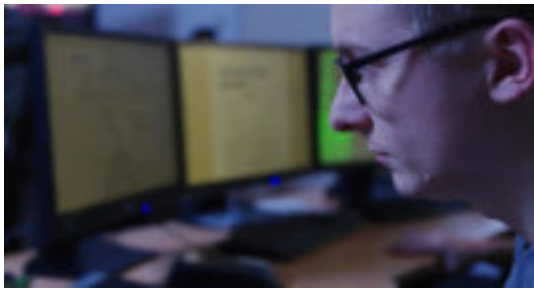
Im vergangenen Jahr wurden für folgende Lösungen Schwachstellen gemeldet:

- In der Firmware für Meinberg-LANTIME-Zeitserver konnten mehrere Schwachstellen gefunden werden, welche es einem Benutzer der Weboberfläche erlaubten, Dateien am Betriebssystem auszulesen und zu manipulieren. Der Hersteller hat unter www.meinberg.de ein Security Advisory veröffentlicht, in dem er die Schwachstellen beschreibt und das MilCert als Finder würdigt.

- In Software zur Verwaltung von Radiologiedaten, welche in vielen österreichischen Krankenhäusern, aber auch international im Einsatz sein soll, wurden gravierende Schwachstellen gefunden, unter anderem in Bezug auf die Authentifizierung der Benutzer und die Vertraulichkeit der Daten. Der Hersteller wurde informiert und hat versprochen, die Schwachstellen mit dem nächsten Update für alle seine Kunden zu schließen.

- In einem Content Management System (CMS) und dessen Plugins wurden zahlreiche Schwachstellen gefunden, die in Kombination im schlimmsten Fall zu einer Übernahme des betreffenden Servers durch einen Angreifer führen können. Der Vertriebspartner wurde informiert und befindet sich für die Bewertung und Behebung der Schwachstellen in Abstimmung mit dem Hersteller.

- In der Firmware eines Druckers konnten veraltete Softwarepakete gefunden werden. Außerdem wurde festgestellt, dass die Webapplikation des Druckers nicht angemessen gehärtet ist. Die Funde wurden den Hersteller übermittelt. Dieser brachte daraufhin eine neue Firmwareversion heraus.



Geschäftsordnung MilCyZ und Cyber-Notfallmanagement

Das Militärische Cyber Zentrum (MilCyZ) wird bei der Abwehr von Bedrohungen und Angriffen aus dem Cyberraum wirksam. Um diesen Schutz

durchzuführen, ist die durchgängige und konsequente Abdeckung aller Aspekte der IKT- und Cybersicherheit im gesamten Lebenszyklus von Systemen und Services in der IKT-Landschaft des BMLV/ÖBH nötig. Es plant und implementiert die Sicherheitssysteme für Eigenschutz und Verteidigung des ÖBH. Im Fall erkannter Cyberangriffe sind Kräfte zur Erkennung, Eindämmung und Abwehr verfügbar.

Unverzichtbar für die aktuelle Aufgabenzuordnung, sowie den Dienstbetrieb in diesem „jungen OrgElement" war somit eine Geschäftsordnung und die Formalisierung des Cyber-Notfallmanagements (Richtlinie), welche in diesem Jahr erfolgreich implementiert wurde.

Forte: Explore AI

In den letzten Jahren haben sich die Möglichkeiten der Artificial Intelligence (AI) drastisch erweitert. Dies liegt zum einen an neuen Techniken und Methoden, speziell im Bereich der neuronalen Netze und des Machine Learnings, aber zum anderen auch an der Verfügbarkeit günstigerer und leistungsfähiger Hardware, die es ermöglicht, schon lange existierende Technologien effizient umzusetzen.

Grafik: www.forte-bmlrt.at

Im Bereich des Militärwesens hat das Thema „Machine Learning" sowie andere AI-Techniken schon länger eine Rolle gespielt. Allerdings war dies bisher hauptsächlich reduziert auf die Auswertung von Informationen: Open-Source-Intelligence (OSITN), aber auch die allgemeine Unterstützung der Lageerkennung sind Paradebeispiele für Bereiche, in denen durch den Einsatz neuer Techniken bedeutende Ergebnisse erzielt wurden. Wichtig war in den letzten Dekaden die automatisierte und intelligente Auswertung von Offline-Daten, bspw. die Erkennung von Militärgeräten auf Bildern und in Videos.

Im Rahmen der akademischen Forschung wurden allerdings in den letzten Jahren einige Fortschritte erzielt, die speziell für die militärische Anwendung wichtig sind. Beispielsweise haben im Bereich der automatisierten Erkennung von sog. Targeted Attacks, d.h. Malware-Angriffe, welche für das Ziel maßgeschneidert und oftmals mit hohen Ressourcen entwickelt werden, wesentliche Fortschritte gemacht.
Diese sind freilich noch weit von einer tatsächlichen Nutzbarkeit entfernt. Das gilt auch für das Pendant – die Nutzung intelligenter und selbstlernender Malware für den zielgerichteten Angriff auf (militärische) Ziele. Dennoch illustrieren diese Beispiele gut den Einfluss dieser neuen Technologien auf das Militärwesen im Cyber-Bereich, der fünften militärischen Dimension.

Das Ziel dieser Studie war die Analyse der Ziele, Möglichkeiten und Bedürfnisse des österreichischen Bundesheeres in Hinblick auf die möglichst effiziente Verortung der finanziellen Mittel in diesem Bereich. Dabei wurde nicht nur auf die derzeitige Situation eingegangen, da dies in einem sich derartig schnell entwickelnden Bereich rasch zu veralteten und damit unzutreffenden Ergebnissen führen würde. Vielmehr wurden basierend auf dem derzeitigen Stand der Technik mithilfe der explorativen Szenarienanalyse mögliche Technologieentwicklungen und Cyber-Defense Use-Cases systematisch aufbereitet, um abzuschätzen, in welche Richtungen sich Technologien und Anwendungen entwickeln können. Zudem wurden gemeinsam mit dem BMLV entsprechende strategische Maßnahmen zu deren Begegnung entworfen.

exploreAI

Grafik: FH-St. PÖLTEN für die Studie

Cyber Bedrohungen

Multi-Lateral Cyber Defense Exercise

Im Oktober fand erneut die Multi Lateral Cyber Defense Exercise unter Beteiligung verschiedener Nationen statt.

Während der Übung wurden verschiedene Fähigkeiten gefordert, die bei defensiven Operationen im Cyber-Raum benötigt werden. Dazu wurden den Teams verschiedene Aufgaben gegeben. Zu Beginn der Übung sind diese auf einem relativ einfachen Niveau, um den Teams Gelegenheit zu geben sich untereinander kennenzulernen, aber auch um sich mit der Arbeitsumgebung vertraut zu machen. Im Laufe der Übung stieg der Schwierigkeitsgrad dann kontinuierlich an. Am Ende eines Übungstages erfolgte dann ein Debriefing. Teilnehmende Teams waren:

Foto: www.unibw.de/code/news/mlcd-2021

Österreich, Niederlande, Jordanien, Polen, Frankreich, Großbritannien und Deutschland. Luxemburg war als Beobachter anwesend. Ein interessanter Aspekt der Zusammenarbeit im Rahmen der MLCD Excercise war das Mischen der Teams. Die Teams wurden also unabhängig ihrer Nationalität, nach ihren Fähigkeiten und Erfahrungen im Rahmen der Veranstaltung zusammengewürfelt. Im Rahmen der unterschiedlichen, wechselnden Szenarien erhielt jedes Teammitglied die Gelegenheit, einmal in die Rolle des Teamleiters zu schlüpfen und diese Erfahrung zu machen.

Künstliche Intelligenz in der Multi Anti Virus Engine

MAVE (Multi Anti Virus Engine) ist eine Eigenentwicklung des MilCyZ zur Prüfung des Datenverkehrs auf Schadsoftware. Dabei handelt es sich im einen Cluster von mehreren vernetzen Systemen, welcher Dateien analysiert und mithilfe von verschiedenen Antivirenprogrammen sowie Scannern bösartigen Inhalt erkennen kann. Dadurch ist ein kontrollierter Download von Dateien aus dem Internet sowie der Empfang von E-Mails in klassifizierten Netzen mit eingeschränktem Datenaustausch möglich.

Aufgrund der modularen Systemarchitektur können sowohl kommerzielle Antivirensoftware als auch selbst entwickelte Programme zur Schadcode Analyse oder Dateivalidierung eingebunden werden. Insbesondere die Implementierung eigener, bedarfsorientierter Analysetools ermöglicht es, rasch auf neue Bedrohungen zu reagieren und Dateien in einem Umfang zu analysieren, welche mit proprietären Tools nicht realisierbar wäre.

Mit der Version 4.0 wurden, unter anderem, erstmalig Technologien zur Anomalie-Erkennung via AI & Machine Learning eingesetzt. Dies ermöglicht es MAVE auch mit den aktuellsten Analysemethoden auf dem Gebiet der Malware-Analyse auszustatten. Darüber hinaus integriert MAVE einen SMTP-Gateway, um Dateianhänge in E-Mails zu filtern und mittels einfacher Schnittstellen können auch Anwendungen des BMLV Daten vor der Verarbeitung automatisiert auf Schadcode überprüfen.

MAVE führt drei Millionen Scans pro Monat durch und etwa 3% der dabei geprüften Dateien werden als nicht zulässig abgewiesen.

Diese stellen aufgrund ihrer Inhalte eine potentielle Gefahr für die klassifizierten Netze des BMLV dar und durch eine restriktive und lückenlose Überprüfung gewährleistet MAVE, dass Malware und Schadsoftware nicht in die IKT-Systeme des BMLV gelangen.

Kompetenzsteigerung Forensik Mobilgeräte

Wie bereits medial berichtet worden ist, richten Cyberangreife ihren Fokus verstärkt auf die Kompromittierung mobiler Endgeräte.

Ein Beispiel dafür ist die Verbreitung von Malware durch gefälschte E-Mails, die in Verbindung mit Paketzulieferern steht.

Foto: hxxps[:]//de[.]securelist[.]com/mobile-malware-evolution-2016/72443/

Aufgrund der Beschaffenheit mobiler Endgeräte, sowie deren Betriebssysteme, unterscheidet sich derartige Malware stark von jener für herkömmliche Computer. Das bedeutet gleichzeitig, dass auch neue Methoden, Software und Hardware benötigt werden, um derartige Malware analysieren zu können.

Smartphones und mobile Endgeräte sind aus unserem heutigen Alltag nicht mehr wegzudenken. Auch im Berufsleben haben diese bereits Einzug gehalten und unterstützen den User bei ihren Tätigkeiten. Dabei steht schon lange nicht mehr die ursprüngliche Idee des Telefonierens im Vordergrund. Smartphones sind kleine, leistungsstarke Computer auf denen zusätzlich Apps installiert werden können, um z.B. E-Mails zu verfassen oder Onlinebanking zu tätigen. Durch die eingebaute Kamera ist es auch möglich, schnell und einfach Bilder von seiner Umgebung zu machen. Dies führt zwangsläufig auch dazu, dass immer mehr sensible und schützenswerte Daten darauf abgespeichert werden. Aufgrund dieser Tatsache, richten auch immer mehr Cyberkriminelle und staatliche Angreifer ihren Fokus auf die Kompromittierung dieser Endgeräte. Dies umfasst u.a. das Ausspähen von Kontakten und Login-Daten, wie z.B. Onlinebanking und E-Mail Accounts.

Da davon ausgegangen werden kann, dass diese Entwicklung weiterhin anhält, ist es von Nöten, die Kompetenz in diesem Bereich zu steigern, um die Angriffsmethoden von staatlichen Angreifern oder Cyberkriminellen zu identifizieren und im besten Fall verhindern zu können.

Echtzeitdatenimport in hochklassifizierte Netze

Bei Schnittstellen zwischen niedrig- und hochklassifizierten Netzen (z.B. VERTRAULICH, GEHEIM) ist der Abfluss von sensiblen Daten technisch zu unterbinden.

Bei strategischen Systemen kann der Import über Datenträger (unter Einhaltung spezieller technischer und organisatorischer Sicherheitsmaßnahmen) bewerkstelligt werden. Anders ist die Situation bei Informationen, die hohe Echtzeitanforderungen haben, wie z.B. Radardaten.

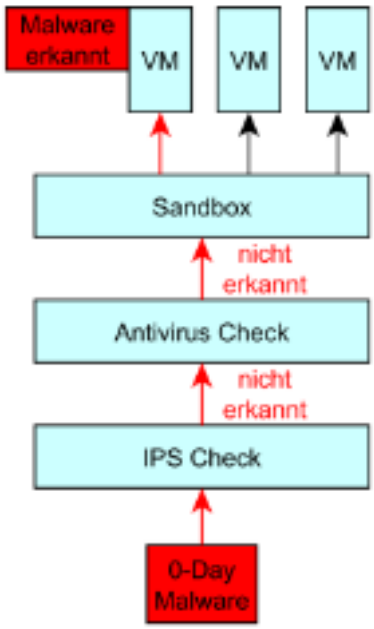
Datendioden sind ein probates Mittel, um unidirektionale Datenverbindungen technisch nahezu vollständig sicher zu realisieren. In Zusammenarbeit mit Dion2/LRÜ konnten die Übertragung von Radardaten in Echtzeit über eine Datendiode technisch erfolgreich demonstriert werden.

Damit konnte ein wesentlicher Grundstein für die Verarbeitung von höheren Klassifizierungsstufen in einsatzrelevanten Anteilen des IKT-Systems ÖBH geschaffen werden.

Ausbau der Angriffssensorik

Die Erkennung von schadhaften Dateien nur mittels AV-Signaturen ist schon seit längerem nicht mehr zeitgemäß. Aus diesem Grund hat das ÖBH seit geraumer Zeit zusätzliche Sicherheitssysteme im Einsatz. Der Markt und auch die Möglichkeiten dieser Systeme ändert sich laufend und es gibt immer mehr neue interessante Produkte, welche unser aktuelles Portfolio erweitern könnten.

So wurde eine weitere Sandbox beschafft, welche sich mit hohen Synergieeffekten in unsere Infrastruktur einfügen lässt. Solche Sandboxen dienen dazu, noch unbekannte Schadsoftware und Angriffsvektoren in einem abgeschotteten Umfeld auszuführen und zu erkennen. Somit ist auch das detektieren dieser noch nicht öffentlich bekannten Angriffe möglich. Da aber keines von diesen Sandbox-



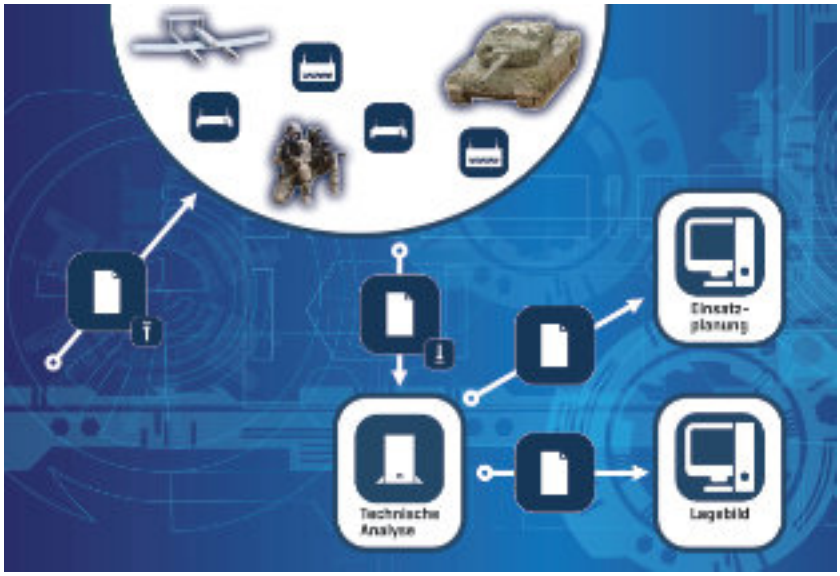
Systemen perfekt ist, ist es von Vorteil auf mehrere verschiedene Anbieter zurückzugreifen, die sich zusammen ergänzen können.

Um einen besseren Überblick über das eigene Netzwerk zu haben und um festzustellen, ob hier unter Umständen jemand darin Angriffsversuche ausübt, gibt es die Möglichkeit der Überwachung von ausgewählten Netzwerksegmenten mit speziellen Clients bzw. Servern. Diese erkennen solche Angriffe und ziehen idealerweise den Angreifer auf Systeme, wo diese keinen relevanten Schaden anrichten können. Das Einrichten solcher Systeme ist aber ziemlich ressourcenintensiv, da diese nahtlos an die eigene IT-Infrastruktur angepasst werden müssen.

Um einen reibungslosen Betrieb im Produktivsystem zu gewähren, wurde nach der initialen Evaluierung der Systeme auf einen Testbetrieb in ausgewählten Versuchsnetzen umgestellt. Diese erweiterte Teststellung über einen längeren Zeitraum ist nötig, um potentielle Fehler zu erkennen und um die Funktionalität der Systeme zu optimieren.

EMS EyeBots

Der vermehrte Einsatz von neuen Technologien in der Kommunikations- und Übertragungstechnik vervielfacht die Möglichkeiten der Informationsübertragung für alle Beteiligten auf dem Gefechtsfeld. Diese werden aber dadurch auch vulnerabel gegenüber gezielten bzw. auch unbeabsichtigten Störungen auf nahezu allen Frequenzbändern.



Das Fehlen von Kommunikationskanälen oder die fremdgesteuerte Nutzung des elektromagnetischen Spektrums (EMS) 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 dieses Forschungsprojektes 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. Im Vergleich zu herkömmlichen Sensoren kann man eine wesentlich höhere Anzahl von Sensoren einsetzen, da sie kostengünstig sind. Dies hat den Vorteil, dass bei einem Ausfall von einzelnen Komponenten die Einsatzfähigkeit des gesamten Systemverbundes nur gering beeinträchtigt wird. Die Komponenten können vergleichsweise schnell und einfach beschafft werden, da es sich um sogenannte Commercial Of The Shelf (COTS) Produkte handelt und man damit technologisch am Puls der Zeit bleibt.
Langfristig gesehen könnten Sensoren in Zukunft in vielfacher Ausführung in einem Sensornetz zur mobilen Erfassung des EMS mitgeführt werden und zur eigenen Informationsverdichtung auf dem Gefechtsfeld beitragen.

Ausbau der Fähigkeiten der Elektronischen Kampfführung

Die Elektronische Kampfführung (EloKa) bewegt sich mit ihren Maßnahmen – den Elektronischen Unterstützungsmaßnahmen, den Elektronischen Gegenmaßnahmen und den Elektronischen Schutzmaßnahmen – im Elektromagnetischen Spektrum. Die Abteilung Unterstützungszentrum Elektronische Kampfführung (UZEloKa) im Militärischen Cyberzentrum (MilCyZ) leistet im Schwergewicht durch Wissensmana-

gement und Einsatzvorbereitung die notwendige Unterstützung im Bereich der Elektronischen Kampfführung.

Folgende Fähigkeiten wurden im Jahr 2021 im MilCyZ weiter ausgebaut:

Bedrohungssimulation:
Im Themenfeld der Gegenmaßnahmen bei Radio Controlled Improvised Explosive Devices (RCIED) spielt die Kenntnis der aktuell vorherrschenden Bedrohungen eine wesentliche Rolle. Im Jahr 2021 wurden durch die Abteilung UZEloKa weitere Bedrohungen analysiert und der Aufbau von Simulationen von Bedrohungen weiterverfolgt. Die Simulationen dieser RCIED-Bedrohungen ermöglichen in weiterer Folge ein Testen der nationalen Selbstschutzausrüstungen auf deren Wirksamkeit und deren Effektivität. Die Simulationen müssen im elektromagnetischen Spektrum realen Bedrohungen soweit wie möglich entsprechen. Gleichzeitig besteht jedoch dabei die Forderung, alle technischen Parameter der eingesetzten Funkmodule ansprechen zu können, damit die Wirkung der Selbstschutzausrüstungen des ÖBH auf die Übertragungswege zukünftiger Bedrohungen frühzeitig getestet werden kann.
Dies ermöglicht dann eine rechtzeitige Bereitstellung der benötigten Informationen, um eine umfassende Einsatzvorbereitung dieser Systeme durchführen zu können.

Informationsbereitstellung:
Die Verfügbarkeit von benötigten Informationen stellt grundsätzlich eine essentielle Basis für ein erfolgreiches Arbeiten dar. Im Fachbereich der EloKa ist ein Element die zentrale Informationsbereitstellung der geplanten Electronic Warfare Database. Im Jahr 2021 wurden nun weitere Schritte für eine Eigenentwicklung getätigt, in dem unter anderem die Grundlagen, die Bedarfsträger und die Inhalte ermittelt werden. Ein direktes Ergebnis ist die Grundlage für eine Neuentwicklung einer nationalen Datenbank im Themenfeld der RCIEDs, um die Informationsbereitstellung und Bedrohungsanalysen für die nationalen Bedarfsträger sicherstellen zu können.

Cyber-Framework

2021 wurde damit begonnen, die einzelnen Cyber-Sicherheitssysteme im Ressort zu einem durchgängigen Cyber-Framework zu strukturieren, um so zukünftig einen durchgängigen Prozess der Cyber-Verteidigung von IKT-Systemen und –Services im Ressorts gegen Vorfälle und Angriffe aus dem Cyberraum bewältigen zu können.

In Kombination mit dem Aufbau der SCU (Special Cyber Unit) wird die Robustheit und Einsatztauglichkeit im gesamten Lebenszyklus der IKT-Landschaft im Ressort massiv erhöht was sich auch direkt auf die gesamtstaatliche Einsatzfähigkeit des ÖBH in der Cyber-Domäne (laufende Amtshilfe, Cyber-Assistenz udgl.) auswirkt.

Die SCU bildet im Gesamtfeld der Cyber-Truppe die fachliche Eliteeinheit, zum Einsatz bei schwerwiegenden Vorfällen und Angriffen aus dem Cyber-Raum des ÖHB und deckt dabei den gesamten Cyber-Framework ab. Die SCU wird anlassspezifisch durch Truppeneinteilung gebildet. Dabei zählen zu den Fähigkeiten des MilCERTs: (Cyber-Raum-Überwachung und Setzen von Sofortmaßnahmen zur Aufrechterhaltung der Funktionsfähigkeit der IKT-Landschaft inkl. Erstellung eines Cyber-Lagebildes), der RRTs (Rapid Response Teams; zusammengezogenes Einsatzteam zur Analyse und Behandlung von einzelnen Cyber-Vorfällen) den Cyber-Waffentechniker (technische Anpassung bestehender und Entwicklung neuer Defence-Systeme gegen aktuelle Angriffstechnologien und -abläufe), sowie den Cyber-Sicherheitsmanagern zur Sicherheits- und Auswirkungsbeurteilung von Cyber-Vorfällen auf die gesamte IKT-Servicelandschaft des BMLV/ÖBH in Form des Informationssicherheitsmanagements.


IKT&CySihZ
Verteidigung
Cyber
Internet
Modern
Serverraum
Smart
Funk
Email
Arbeitsplatz
Strom
Sicherhei
Netzwerk
Kommunikatio
Daten
WIR SCHÜTZEN ÖSTERREICH.
bundesheer.at
UNSER HEER
Bundesministerium für Landesverteidigung

IKTBetr

Bereich IKT-Betrieb

Beschäftigte uns im Jahr 2020 durch das erstmalige Auftreten von Covid-19 der Schutz der Bediensteten in Verbindung mit der Sicherstellung der Aufgabenerfüllung, so konnten wir im Jahr 2021 in diesem Bereich schon auf umfangreiche Erfahrungen bei der Planung der Dienstbetriebes zurückgreifen. Mit der Auslieferung der Eigenentwicklung SMN.mobile als Ersatz für die GovNet-Boxen, konnte Homeoffice als Schutzmaßnahme breitflächig eingesetzt werden. SMN.mobile ermöglicht den Zugriff auf die IKT-Services im sicheren militärischen Netz (SMN) unter Nutzung eines Internetzuganges.

Zur Kommunikation mit nicht an der Dienststelle anwesenden Bediensteten wurde ein neues Videokonferenzservice eingeführt. Telearbeit und Homeoffice sind wesentliche Treiber der Digitalisierung der täglichen Arbeit im Ressort.

Die Covid-19 Pandemie und Witterungseinflüsse machten eine Neuplanung im Projekt Midlife Upgrade ofRVN (ortsfestes Richtverbindungsnetz) erforderlich. Ähnliches gibt es auch zum Thema IKT-Services für Übungen und Einsätze zu berichten. So musste u.a. das Weltwirtschaftsforum verlegt oder ein Scharfschießen mit den Luftraumüberwachungsflugzeugen Covid-19 bedingt abgebrochen werden.

Zur Führung seiner Kräfte stützt sich das Ressort auf verfügbare IKT-Services, die abgesehen von einigen Ausnahmen im 24/7 Modus betrieben werden. Bei aufrechter Stromversorgung können diese im In- und Ausland genutzt werden. Kommt es jedoch zu einem Blackout, fallen Systeme, welche nur durch externe Netzbetreiber versorgt werden, aus. Eine autarke Stromversorgung des

HR Ing. Harald Steindl, MSc

Fernmeldesystems ÖBH (FMSys ÖBH) und des zentralen Rechenzentrums stellt daher eine Grundvoraussetzung dar, um die Aufrechterhaltung der Führungsfähigkeit des ÖBH und des BMLV in den wichtigsten Lokationen zu gewährleisten. Umfangreiche Tests im Jahr 2021 zeigten, dass im Anlassfall das zentrale Rechenzentrum und die zentrale Netzwerksteuerung mit Strom aus eigener Produktion versorgt werden können.

Ein anderes Bild bietet der Bereich der ortsfesten Übertragungseinrichtungen. Ein Blackout kann zu Einschränkungen oder Ausfällen im Servicebetrieb führen. Maßnahmen zur Steigerung der Autarkie sind daher zu planen und umzusetzen.

Im Jahr 2021 zeigte sich, dass sich die Bediensteten des IKT&CySihZ bzw. der Dion 6 IKT und Cyber den Herausforderungen stellten und diese in hervorragender Weise gemeinsam mit Engagement bewältigten.

Ich bedanke mich bei den Bediensteten des Bereiches IKT-Betrieb, der Bereiche und Abteilungen des IKT&CySihZ bzw. Dion 6 IKT und Cyber und bei allen Dienststellen und Kommanden für die hervorragende Zusammenarbeit im abgelaufenen Jahr.

Der Bereich IKTBetr als Teil des IKT&CySihZ ist zuständig für den Betrieb der IKT-Services und die Unterstützung der IKT-Anwender. Bereitgestellt werden IKT-Infrastrukturservices zur Übertragung von Sprache und Daten, IKT-Services zum Schutz der eigenen Netze sowie zur zentralen Speicherung der Daten und zentrale Applikationsservices für unterschiedliche Nutzungszwecke.
Eine wesentliche Aufgabe des Bereiches ist die Betriebsführung für die Infrastruktur „Objekt 6". Dieser militärische Sonderbau beherbergt neben dem zentralen Rechenzentrum, der Einrichtung für die Netzwerkbetriebsführung auch geschützte Aufnahmemöglichkeiten für die Bundesregierung, die oberste militärische Führung und den ORF.

Die Aufgaben im Bereich des Frequenzmanagements, des Krypto-Managements im Rahmen der NDA/MoD und des Berechtigungsmanagements runden das breite Aufgabengebiet des Bereiches ab.

IKT-Unterstützung für Übungen und Einsätze

Auch das Jahr 2021 stand, wie bereits das Vorjahr, im Zeichen von Covid-19. Nach vielen erfolgreichen Jahren wurde die „Luftraumsicherungsoperation (LRSiOp) DAEDALUS 2021" nicht durchgeführt, denn das Weltwirtschaftsforum (WEF) in DAVOS fand diesmal im virtuellen Raum statt. Somit fiel auch für die Systemsteuerung/ IKT&CySihZ das bedeutendste Vorhaben des Jahres aus, wo im Rahmen der IKT-Unterstützung durch die Systemsteuerung elementare Abläufe und Automatismen der Betriebsführung in einem Einsatzszenario alljährlich trainiert wurden. Im Jänner 2021 konnte noch eine Einweisung mit verlegbaren Satelitenterminals und die Übung „HANGOVER IV" in der SCHWARZENBERG-Kaserne und am GAISBERG unterstützt werden.

Die Substitution der ortsfesten Radarstation STEINMANDL unter Einsatz des „deployable air defence radar" (DADR) musste auf einen späteren Termin verschoben werden. Das Luft-Luftschießen „Waffensystem EFT AAG21" in SCHLESWIG/DEU im Frühjahr musste aufgrund Covid-19 abgebrochen werden. Es fand stattdessen im September die Übung „Waffensystem EUROFIGHTER Squadron Exchange CZE" statt. Vom Abbruch der „AAG21" waren auch Bedienstete des Bereiches, die vor Ort unterstützt hatten, betroffen. Durch ein sehr gutes Risikomanagement und eine gut geplante Rückholung kamen letztendlich die Bediensteten des Bereiches gesund nach Hause. Auch die Übung „BLACK SWAN 21" in UNGARN und die FüU-Übung bzw. Erprobung GefStd-Modul der 4.PzGrenBrig wurden pandemiebedingt kurzfristig abgesagt.

Nach 2 Monaten Pause konnte Ende April 2021 wieder mit dem Vorhaben „Zusammenziehung EUBG" in der KROBATIN-Kaserne gestartet werden. Im Frühjahr 2021 wurden noch die beiden Auslandsvorhaben „ADRIATIC STRIKE 2021" in CERKLJE/SLO und „HOT BLADE 2021" in BEJA/PRT erfolgreich unterstützt.

Der Sommer 2021 wurde durch 3 Vorhaben geprägt. Im Raum VORARLBERG fand die Flugfunkübung „DEEP VISION 21" statt, zeitgleich am TÜPl LIZUM/WALCHEN die „SLÜ MilAK 21" und kurz darauf die „CONSTRUCTOR 21" im Raum ALLENTSTEIG. Alle Vorhaben konnten ohne Probleme durchgeführt werden.

Durch die Austragung der 5. Weltkonferenz der ParlamentspräsidentInnen im September in WIEN wurde KdoLRÜ recht kurzfristig mit der Durchführung der „LRSiOp WIEN 2021" beauftragt, die durch die Systemsteuerung unter Einbindung der Bereiche Appl, IKTTe, MilCySihZ und IKTBetr optimal serviciert werden konnte.

Von September 2021 bis ins Frühjahr 2022 wird das Mid Life Upgrade (MLU) auf der ortsfesten Radarstation STEINMANDL durchgeführt. Dazu wurde das DADR bis zum Frühjahr 2022 auf die Radarstellung (RadStlg) ZEILERBERG verlegt und stellt die entsprechende Radarbedeckung während der Abschaltungen der ortsfesten Radarstation STEINMANDL (ORS ST) sicher.

Im September fanden auch die „Beorderten Waffenübung StbKp/StbB7" in SCHWABEGG und das „Teilstreitkräfteübergreifende Scharfschießen LOFER" mit IKT Unterstützung erfolgreich statt.

Foto: EDA

Auch der Helicopter Tactics Instructor Course "HTIC 21" konnte in UNGARN mittels VSAT (verlegbares Satellitenterminal) positiv absolviert werden.
Ebenfalls im Oktober fand die FlA-Übung „CAVEMAN ALLEGORY" in ZELTWEG und die internationale Evaluierungsübung „Verbandsübung

7.JgBrig & NEL 2 InfBn" in ALLENTSTEIG statt. Ein Routerfehler führte unter anderem auch zu einem Ausfall des Übungsnetzwerkes. Dieser konnte in Zusammenarbeit mit den Netzwerkspezialisten des Bereiches IKTTe jedoch in kurzer Zeit behoben werden. Zeitgleich ging ebenfalls in ALLENTSTEIG die Jamming-Übung „CROWS WEEK 21" über die Bühne.

Zum Abschluss des Jahres fand in den KW 46-48 eine Fallback-Übung statt. Einer Testwoche zur Überprüfung der technischen Verfügbarkeit folgte eine weitere Testwoche für betriebliche Verfügbarkeit, um auch in diesem Bereich die Abläufe mit einer Teststellung zur Nachbereitung der Übung „CAVEMAN ALLEGORY 21" zu evaluieren. Den Abschluss bildete eine Woche Betrieb des Fallbacksystem Goldhaube. Ziel des Vorhabens war eine realitätsnahe Übergabe/Übernahme des diensthabenden Systems LRÜ im Falle einer Evakuierung der EZ/B und die Überprüfung der taktischen, betrieblichen und zeitlichen Vorgaben im Falle einer Evakuierung der EZ/B.

Insgesamt wurden im Jahr 2021 durch die Systemsteuerung/IKT&CySihZ 39 Vorhaben unterschiedlicher Ausprägung betreut.

Benutzerbetreuung für European Training Mission (EUTM) MALI

Für die zweite österreichische Kommando-Führung bei der European Union Training Mission Mali (EUTM Mali) von Dezember 2021 bis Juni 2022 lag erneut die koordinierende Verantwortung für den erfolgreichen Aufbau der IKT-Infrastruktur im Einsatzraum in den Händen der Mitarbeiter des Referates Benutzerbetreuung IT WEST (BenBe IT West).

Wie bereits 2019, während der ersten österreichischen Kommando-Führung in MALI, bestand der Auftrag darin, wieder eine Anbindung an das sichere militärische Netz (SMN) nach Österreich herzustellen. Für die Ausstattung der Arbeitsplätze und des Netzwerkes wird SMN-Gerät im Einsatzraum verwendet. Diese spezielle Art der Einbindung in das SMN wurde während der europäischen Flüchtlingskrise im ÖBH entwickelt, um eine rasche SMN-Anbindung für Verbindungsoffiziere weltweit bei externen Organisationen herstellen zu können. Dabei wird über einen SMN-Router/Switch und einen Server die verschlüsselte Sprach- & Datenverbindung ins SMN hergestellt. Schon im Jahr 2019 wurde während der ersten Kommando-Führung EUTM MALI eine Adaptierung der Anbindung mittels „Virtual Private Network (VPN)-Schlüsselbox" über das Internet durchgeführt und erfolgreich eingesetzt.

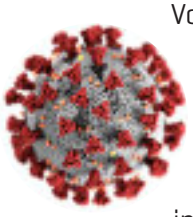
Für die zweite Kommandoführung 2021 erfolgte im Juni 2021 eine fachspezifische Erkundung vor Ort zur Planung und Festlegung der missionsspezifischen IKT-Ausstattung. Diese wurde, wie schon in den Jahren davor - 2019 und auch 2020 bei „resolute support misson (RSM)" Afghanistan – durch einen Mitarbeiter des Referates BenBe IT WEST im Einsatzraum installiert.

Im Oktober 2021 wurde das IKT-Gerät im Zuge der fachlichen Einsatzvorbereitung in der SCHWARZENBERG Kaserne in Wals vorkonfiguriert, die Funktionalität getestet, das Gerät für den Cargo Flug zusammengestellt und schlussendlich verpackt. Anfang Dezember 2021 verlegte das Team des IKT-Sonderbautrupps, bestehend aus 6 zivilen und militärischen Bediensteten, unter der Führung BenBe IT WEST nach MALI, um die vorbereiteten IKT-Systeme und IKT-Geräte im Hauptquartier (MHQ) „european union training misson (EUTM) MALI" in BAMAKO aufzubauen, zu testen, letzte Einstellungen vorzunehmen und die eingesetzten Truppenkräfte einzuweisen.

Ebenso wird eine Erkundung der Anbindung und Erhebung des Materialbedarfs, zur Herstellung der Weiterverwendung des Systems im Trainings Center der malischen Armee in KOULIKORO ab Juni 2022, durchgeführt werden.

Foto: Bundesheer/Pusch

Die Benutzerunterstützung im 2. Jahr der Pandemie



Hat sich der Unterstützungsbedarf der IKT-Anwender im Ressort im 2. Jahr der Pandemie gegenüber zum Vorjahr verändert? Kam es, wie voriges Jahr, auch heuer während des 3. und 4. Lockdown im Jahr 2021 zu einer merkbaren bedarfsgetriebenen Veränderung im Bereich der Unterstützungsleistungen?

Vor der Beantwortung der Fragen ist es wesentlich, einen Blick auf ausgelieferte neue Produkte und zusätzliche Leistungen im IKT-Support zu werfen.

Zu Beginn des Jahres 2021 waren die Covid-19 Teststraßen, die mit ressorteigenen IKT-Geräten gegen Ende des Jahres 2020 ausgestattet wurden, noch im Vollbetrieb und die GovNet-Boxen waren die einzige Möglichkeit, sich über das Internet mit dem SMN zu verbinden, um unabhängig von der Infrastruktur in den militärischen Liegenschaften an einem beliebigen Ort die IKT-Services im SMN zu nutzen.

Im Herbst 2020 wurde das IKT&CySihZ mit der Entwicklung einer eigenen Software zur sicheren Anbindung von SMN-Notebooks über das Internet an das SMN beauftragt. Mit den steigenden Infektionszahlen während der Covid-19 Pandemie wurde die Auslieferung der Software von sehr vielen IKT-Anwendern im Ressort dringend erwartet, um auch außerhalb der Dienststelle, z.B. im Home-Office, die IKT-Services im SMN zu nutzen.

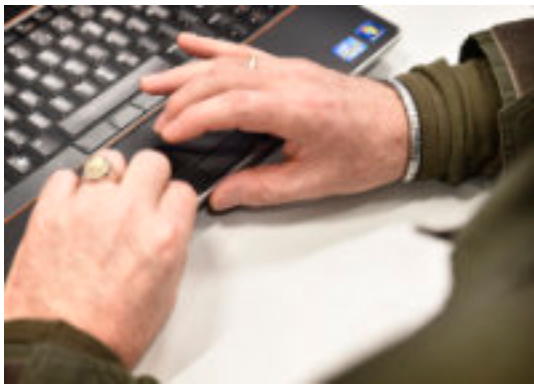
Foto: HBF/Pusch

Im Frühjahr 2021 war es endlich soweit. SMN.mobile wurde ausgeliefert und zur Nutzung auf Notebooks, die die entsprechenden Leistungsparameter aufwiesen, im SMN freigegeben.

Mit SMN.mobile war es ab dann einer großen Anzahl von Anwendern möglich, alle IKT-Services wie ELAK, MTM, ETB, PERSIS, ERGIS etc. zu nutzen und auf die Datenbestände auf den SMN-Servern zuzugreifen. Für die Entwickler, Systemspezialisten und Benutzerbetreuer des IKT&CySihZ bietet SMN.mobile die Möglichkeit, von fast jedem Ort aus und zu jeder Tageszeit auf die Werkzeuge und Managementsysteme, die bislang nur an den IKT-Arbeitsplätzen an der Dienststelle genutzt werden konnten, zuzugreifen, um entweder im Wege der Telearbeit ihre Arbeitsleistung zu erbringen oder bei Eintreten von Störungen beim Betrieb der IKT-Services rasch - ohne an der Dienstelle anwesend zu sein - an der Behebung der Störung zu arbeiten. Zeitgleich erfolgte die Ausrollung weiterer gemanagter Smartphones und die Umstellung der Military Domain PC (MD-PC) auf eine aktuelle Version des Universalklons.

Mit diesen Produkten konnte die Digitalisierung im Ressort um einen bedeutenden Schritt vorangetrieben werden, ohne auf die etablierten Absicherungssysteme gegen Cyber-Angriffe zu verzichten oder diese in ihrer Funktionalität zu beschneiden.

Aber nicht nur die Anwender im SMN profitierten davon, es wurde auch die Truppe im Assistenzeinsatz an der Staatsgrenze mit gemanagten Smartphones zur Kontrolle der Covid-Tests von Einreisenden ausgestattet. Parallel wurde Silentel - eine Software-Lösung zum Führen verschlüsselter Sprachkommunikation über Smartphones auch an Anwender in anderen Ressorts ausgeliefert. Im Gegensatz zum ersten Lockdown im Jahr 2020, wo durch die Bediensteten des IKT&CySihZ massiv auf die Stabilität der eingesetzten Software geachtet wurde, und Hardware-Erneuerungen nur dann durchgeführt werden, wenn Gefahr für die Aufrechterhaltung der Verfügbarkeit der IKT-Services bestand, gab es im Jahr 2021 diesbezüglich keine Einschränkungen.



Alle Updates und Erneuerungen der zentralen IKT-Infrastruktur und bei den zentralen Applikationsservices wurden durch das IKT&CySihZ plangemäß durchgeführt.

Um nun zu den eingangs gestellten Fragen zurück zu kommen, sind die Daten aus dem Leistungsbereich der IKT-Benutzerbetreuung zu betrachten.

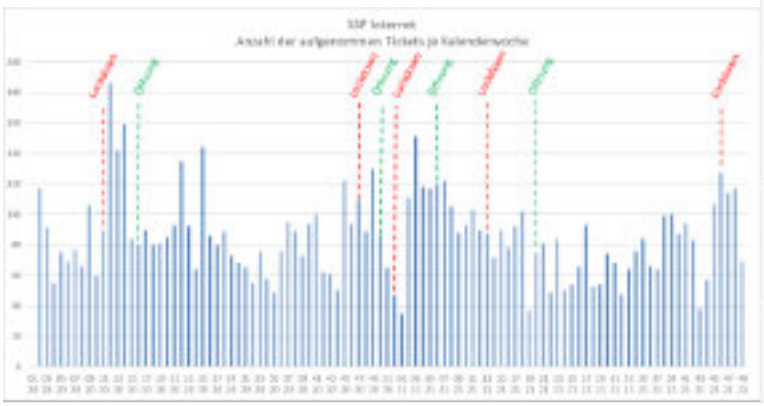
- Hat sich der Unterstützungsbedarf der IKT-Anwender im Ressort im 2. Jahr der Pandemie gegenüber zum Vorjahr verändert?

- Kam es, wie voriges Jahr auch, heuer während des 3. und 4. Lockdown zu einer merkbaren bedarfsgetriebenen Veränderung im Bereich der erbrachten Unterstützungsleistungen?

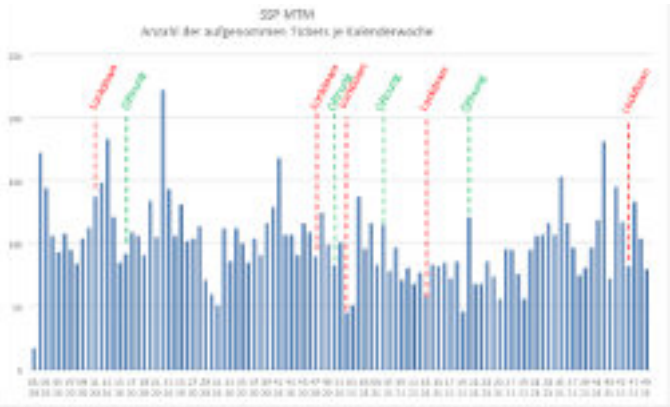
Beginnend mit der Auswertung des für Internet-Services zuständigen Serviceschwerpunktes SSP-Internet zeigt das untenstehende Diagramm Details dazu.
Im Diagramm fällt eine Spitze zu Beginn des Jahres 2021 in der 3. Kalenderwoche auf. Diese hohe Anzahl an aufgenommenen Anfragen der IKT-Anwender fällt in die Zeit eines Lockdown und begründet sich in Unterstützungsleistungen für die Covid-19 Teststraßen und in der vermehrten Nutzung der zusätzlich ausgelieferten gemanagten Smartphones. Im Vergleich zum 1. Lockdown des Jahres 2020 tritt diese Spitze nur in einer Woche auf, um bis zum Ende des Lockdown in der 6. Kalenderwoche 2021 auf einem erhöhten Niveau zu bleiben.

Dieses erhöhte Niveau an Unterstützungsleistungen in den Kalenderwochen 4 bis 7 basiert auf vermehrten Anfragen, die im Zusammenhang mit der Nutzung der Internet-Services und zur Handhabung der mobilen Endgeräte im Homeoffice stehen. Mit der Rückkehr der Bediensteten aus dem Homeoffice schwingt sich die Support-Leistung beim SSP-Internet wieder auf ein normales Niveau mit saisonbedingten Schwankungen, wie z.B. die Urlaubszeit eine solche auslöst, ein. Erst mit dem Lockdown zum Ende des Jahres 2021 zeigt sich wieder ein erhöhter Leistungsumfang beim SSP-Internet, ausgelöst durch die Arbeit der IKT-Anwender im Homeoffice. In weiterer Folge wird ein Blick auf die Support-Leistungen beim Serviceschwerpunkt Mail- und Terminmanagement (SSP MTM) in den Jahren 2020 und 2021 gelegt. In die Zuständigkeit des SSP MTM fallen Unterstützungsleistungen zum IKT-Service Mail- und Terminmanagement sowie zu den applikationsspezifischen Teilen der gemanagten Smartphones.

Einzelne Spitzen in den Wochen des Jahres 2021 lassen sich vermehrt auf die Anwenderunterstützung bei der Durchführung der Betriebsystem-Updates auf den gemanagten Smartphones zurückführen. Mit Einführung des Quarantänemodus für gemanagte Smartphones, können viele Funktionen des Gerätes aus Sicherheitsgründen nicht mehr genutzt werden, wenn ein Anwender das Update nicht bis zu einem bestimmten Zeitpunkt eingespielt hat.



Anzahl aufgenommene Tickets im SSP Internet in den Jahren 2020 und 2021



Anzahl aufgenommene Tickets im SSP MTM in den Jahren 2020 und 2021

Damit wird erreicht, dass die Anwender freigegebene Betriebsystem-Updates rechtzeitig vor dem Beginn des Quarantänemodus einspielen. Erfolgt dies nicht, können aus Sicherheitsgründen mit Wechsel in den Quarantänemodus viele Funktionen auf den gemanagten Smartphones nicht mehr genutzt werden. Für die Rückkehr in den normalen Modus werden die Anwender durch SSP MTM unterstützt.

Ein weiterer häufig angefragter Punkt ist die Unterstützung bei der Installation von Apps oder der Zugriff auf die Chat-Funktion im SMN. Diese Funktion von Sametime wird von vielen Anwendern erstmalig bei Telearbeit/Homeoffice während eines Lockdown genutzt. Viele Anfragen um Unterstützung wurden auch zu den Themen Einrichtung/Nutzung von Organisationspostfächern und zum Web-Client des Mail-Systems im SMN gestellt. So gesehen, lernen viele Anwender erst durch das Arbeiten außerhalb der Dienststelle viele IKT-Services und damit die Möglichkeiten und Vorteile der Digitalisierung ihrer Arbeitswelt kennen und nutzen.

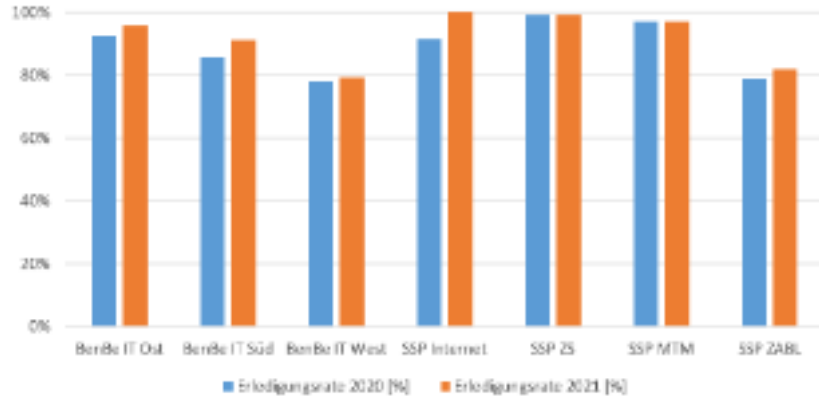
Zum Abschluss wird noch ein Vergleich der Lösungsraten anhand des untenstehenden Diagramms gezeigt.

Wie die Jahresvergleiche bei den Lösungsraten der Serviceschwerpunkte zentrale Services (SSP ZS, zuständig für ElAk und Stammportal) und SSP MTM zeigen, wird die Lösungsrate durch die Bediensteten in diesen SSP weiterhin erfolgreich stabil hochgehalten.

Eine wichtige Aufgabe für den SSP ZS bestand im Jahr 2021 darin, gemeinsam mit dem Bereich Applikationen die Direktionsstruktur mit Stichtag 1. Juli 2021 im IKT-Service ElAk umzusetzen.

Beim SSP Internet zeigt sich im Vergleich der Jahressäulen eine merkbare Steigerung, die auf einen höheren Wissenstand in Verbindung mit der Routine der Bediensteten im 1st Level Support im Umgang mit den neuen digitalisierten Funktionen zurückzuführen ist.

Bemerkenswert ist die Steigerung beim SSP ZABL (zuständig für das zentrale IKT-Service LOGIS). Erscheint sie auch auf den ersten Blick gering, inhaltlich ist in diesem SSP den Bediensteten bei der Bearbeitung der oftmals komplexen Anwenderanfragen jedoch eine merkbare Steigerung gelungen.



Erledigungsraten der Supportstellen imVergleich der Jahre 2020 und 2021

Deutlicher wird dies unter dem Gesichtspunkt, dass der SSP ZABL Anfragen von LOGIS Power-Usern zu bearbeiten hat, die thematisch von funktionalen bis zu applikationstechnischen Anfragen reichen. Im SSP ZABL erfolgt entweder die direkte Bearbeitung oder die Filterung, ob eine Anfrage zur weiteren Bearbeitung an die Anwenderfachabteilung (funktional) oder an den 2nd Level Support des Entwicklerteams im IKT&CySihZ (applikationstechnisch) weiterzuleiten ist. Eine spannende Aufgabe, die viel Erfahrung und Wissen bei der Bearbeitung erfordert.

Erwähnenswert sind auch die Steigerungen im Bereich der Benutzerbetreuungen (BenBe IT Ost, Süd und West - erkennbar im linken Teil des Diagramms), denn in diesen Bereich fällt im Schwergewicht die Lösung von Anfragen der Leitbediener rund um die Themen SMN-Server mit dem Kamino-Klon und der LAN-Infrastruktur. Beides betrifft Themen, die für die Verfügbarkeit aller IKT-Services für die Anwender im SMN von essentieller Bedeutung sind. Die geringeren Lösungsraten in den Jahren 2020 und 2021 bei BenBe IT West sind auf mehrere projektbezogene Dokumentationstickets zu neuen IKT-Systemen für die

Truppe oder diverse Unterstützungsleistungen für Übungen und Einsätze zurückzuführen. Diese Tickets bleiben naturgemäß über einen längeren Zeitraum für die Arbeitsdokumentation offen und werden erst nach Abschluss der projektbezogenen Arbeiten geschlossen.

Etwas mehr Sorgen bereitet dem Referat Berechtigungsmanagement und den Bediensteten im 2nd Level Support die erhöhte Ausfallsrate bei den Chip-Karten der sogenannten 600.000er Serie. Diese Kartengeneration wurde ab Jahresende 2019 an die Bediensteten im Ressort als Ersatz für die bisherige Kartengeneration ausgeliefert.

Als mögliche Ursache für den Ausfall wurde eine Sicherheitsfunktion auf dem implementierten Chip der Karte identifiziert, die zum Auslösen der Kartensperre führen kann, ohne dass eine solche bei den Notebooks und Desktops im SMN systemisch zu diesem Zeitpunkt erforderlich wäre. Die Situation zeigte sich in der Analyse äußerst komplex. Gegenwärtig wird an einer Lösung durch das IKT&CySihZ im Zusammenwirken mit weiteren Stellen im Ressort gearbeitet, um dieses die Arbeit der Anwender störende Problem umfassend zu beheben.

Die Bediensteten im Referat Berechtigungsmanagement werden durch dieses Problem stark gefordert und sind bemüht, im Anlassfall so rasch wie möglich eine Ersatzchipkarte auszustellen und zum Versand zu bringen oder zur Abholung bereitzustellen.

Das ortsfeste Richtverbindungsnetz - ofRVN

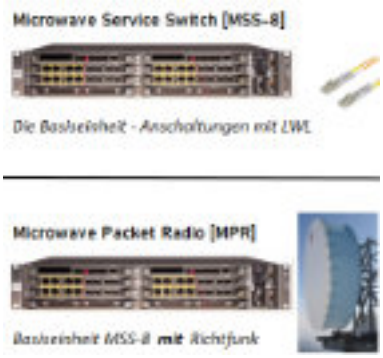
Under construction – Wir bauen weiter um

Under Construction so lautet auch das diesjährige Motto für das ortsfeste Richtverbindungsnetz (ofRVN). Das ofRVN wurde beginnend mit 2003 errichtet. Der Bedarf an Übertragungsbandbreite konnte damit, für die darauffolgenden 15 Jahre abgedeckt werden. Eineinhalb Jahrzehnte später, im Jahr 2018 hatten die Komponenten des Trägernetzes das „end of life" erreicht und seitdem wird das System einem Midlife-Upgrade (MLU) unterzogen, wobei wesentliche Hardware-Komponenten zu tauschen sind.

Seit annähernd vier Jahren wird das Trägersystem ofRVN abschnittsweise umgebaut. Ein Abschnitt bezeichnet dabei zwei benachbarte Stationen und den physikalischen Verbindungsweg, wobei im urbanen Bereich überwiegend Glasfaserleitungen und auf der Fernebene Richtfunkstrecken zur Anwendung kommen. Bei den Umbautätigkeiten im Jahr 2021 wurden, an 10 Standorten im Bereich WIEN, TIROL, SALZBURG, sowie in ZELTWEG nachfolgende Geräte bzw. Verbindungswege in Betrieb genommen.

- 6 Microwave Service Switch (MSS-8)
- 9 Microwave Packet Radio (MPR)
- 7 Funkstrecken
- 11 Glasfaserverbindungen
- 3 Taktgeber MEINBERG

Die sogenannte Südspange des Backbone Ringes, die von WIEN über GRAZ bis in die EZ/B führt, ist damit im Wesentlichen fertig gestellt. Ebenso auch die Westspange, die bis nach INNSBRUCK reicht. Vereinfacht kann man sagen, das etwa 50 % des Netzes umgebaut sind.



Neue Basiseinheit MMS- 8

Mit der steigenden Anzahl an neuen Geräten und den dazu gehörenden Funkstrecken haben sich aber auch Fehler eingeschlichen, die behoben werden mussten bzw. die noch eine Instandsetzung erfordern. Diese reichen von Störungen in der Sendeanlage bis hin zum systemweiten Fehler, der zum Ausfall von Speicherkarten führen kann. Die zum Teil aufwendige Fehlersuche sowie die anschließenden Instandsetzungen fordern das eigene Personal und die Angestellten des Auftragnehmers.

Dazu sind bei allen Geräten, die bis zum 1.Quartal 2021 verbaut wurden, präventiv die Speicherkarten zu tauschen und mit einer neuen Version des Betriebssystems auszustatten. Die Speicherkarten, angepasst auf jedes einzelne Netzelement, werden im Labor vorbereitet. Der Austausch der im Labor vorbe-

reiteten Geräte erfolgt vor Ort an der Sende-, Empfangsanlage nach einem zuvor geregelten Ablauf. Mit diesem Vorgang ist immer eine Unterbrechung in der Dauer von etwa 45 Minuten pro Gerät verbunden. Das Zeitfenster für die Unterbrechung wird vorab mit den Bedarfsträgern abgestimmt, um die Beeinträchtigung des Servicebetriebes möglichst gering zu halten. Mit Jahreswechsel 2021/2022 sollte der Tausch der Speicher-Karten bei 30 der derzeit verbauten 59 Geräte vollzogen sein.

Es gibt aber auch andere Widrigkeiten, die dazu geführt haben, dass die Frist bis zur Erledigung des MLU auf Ende 2024 verlängert werden musste. Die Folgen der Covid-19 Pandemie, wie Lockdown oder darauffolgende Lieferschwierigkeiten haben die Umbaumaßnahmen für mehrere Wochen zum Erliegen gebracht. Damit einhergegangen ist auch eine neuerliche Planung der Schulungen für unsere Bediensteten.

Das Netz in den Bergen

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

RV-Station im Hochgebirge

Etwa ein Drittel der Geräte steht auf Höhenstationen, die sich zum Teil im subalpinen, aber auch im hochalpinen Gelände befinden (17 Stationen über 1000 m, davon sechs auf über 2000 m).

Während Geräte mit LWL-Verbindungen innerhalb von ein bis zwei Tagen umgebaut werden können, besteht ein Mehraufwand bei Richtfunkstrecken. Die Arbeiten in diesem Bereich beanspruchen ein Zeitfenster von drei bis vier Tagen bei entsprechend passender Wetterlage. In beiden Fällen werden aber auch Adaptierungen an der Stromversorgung durchgeführt bzw. sind auch Umschaltungen der Benutzerverbindungen erforderlich. Bei Funkstandorten muss zuerst die bestehende Sende-/Empfangsanlage abgebaut werden, um Platz für das neue Gerät zu schaffen. Das Einrichten der Antennen und erforderliche Abnahmemessungen für die Sende-/Empangsanlage sind ebenso zeitlich bei der Umbauplanung zu berücksichtigen wie der Aufbau der neuen Geräte.

Die Antennen im Einfluss von extremen Wetterbedingungen

Im Winter werden vorrangig Umbautätigkeiten auf niedrig gelegenen Standorten, die über Glasfaserkabel verbunden sind und keine Außenaktivitäten erfordern, durchgeführt. Die Saison für Umbauten in den Bergen beginnt im April und endet zumeist im November, wenn der erste Schnee fällt.
Die Abdeckung auf der Vorderseite der Antenne, das Flatterradom, bewegt sich im Wind und verhindert damit das Anlegen von Schnee und Eis. Die Antenne selbst kann Stürme bis 200 km/h Stand halten.

Antennenanlagen bei Wetterextremen

Im Jahr 2022 wird der Weiterbau von der EZ/B nach SALZBURG Stadt erfolgen. Bis zum Ende des ersten Quartals sollte auch der Tausch der Speicherkarten abgeschlossen sein.

Schaden bei Sichtkontrolle im Frühjahr – Die Funktionalität war nicht beeinträchtigt

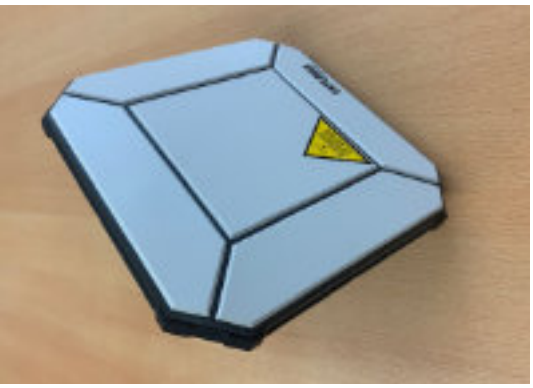
Die Hälfte des Netzes ist umgebaut – wir bauen weiter!

Alles wird gut – wenn nichts mehr geht kommt Hilfe vom technisch logistischem Zentrum der Luftraumüberwachung (TLZ)

Providerleistungen und Neuerungen in der Satelliten-Kommunikation

Der Großteil der national und international angemieteten Telekommunikationsdienstleistungen im BMLV wird durch Services von einem Provider über Rahmenverträge der Bundesbeschaffungsgesellschaft (BBG) bereitgestellt. Diese Dienstleistungen umfassen das Kommunikationsspektrum von mobiler Kommunikation über Internationale Datenverbindungen, bis hin zu Internetservices via Satellit.

National werden Datennetze, abseits des ortfesten Richtverbindungsnetzes, auf Basis Ethernet-Services in unterschiedlichen Bandbreiten an militärischen Liegenschaften angeschaltet. Diese „Point to Multipoint" (PtMP) Dienstleistungen werden sowohl im SMN als auch im „Tactical Communication Network" (TCN) zur Vermaschung der Systeme und Liegenschaften errichtet.



mobiles SAT-Terminal EXPLORER 510

Internet-Services werden im Besonderen im Projekt „selektives WLAN für Rekruten" (selWLAN Rekr) in Kombination mit WLAN-Installationen in mehr als 60 Liegenschaften zur Verfügung gestellt.

Dieses Service ermöglicht speziell den Rekruten die Nutzung des Internets mit deren privaten Endgeräten in militärischen Liegenschaften.

mobiles SAT-Terminal EXPLORER 710

Ebenfalls forciert wird mit Unterstützung durch das Ressort die Verbesserung der Mobilfunkanbindung der militärischen Liegenschaften. In der OSTARRICHI-Kaserne, Amstetten, konnte innerhalb weniger Monate die Mobilfunkanbindung in der Liegenschaft massiv verbessert werden. Im Rahmen dieses Vorhabens wurde eine LWL-Anbindung in Zusammenarbeit mit Pionierkräften zum Kommandogebäude in der OSTARRICHI-Kaserne hergestellt. Die Mobilfunksendeeinrichtung wurde auf dem bestehenden Mastsystem (Kurwellen-Funkanlage) montiert und in Betrieb genommen.

In Verbindung mit der fortschreitenden Digitalisierung stellt die Breitbandanbindung der militärischen Liegenschaften an die zivile Provider-Infrastruktur im Rahmen der Sicherheitsinseln neben der Anbindung an das ofRVN eine wesentliche Grundlage für die zukunftssichere Kommunikation im BMLV dar. Im Jahr 2021 wurden Grundlagen und Konzepte für die Dimensionierung der LWL-Anbindungen definiert und mit den Maßnahmen zur Umsetzung in den nächsten Jahren begonnen.

Neben den terrestrischen Services nehmen die Satelliten gestützten Kommunikationsmittel im Rahmen der militärischen Kommunikation einen hohen Stellenwert ein. Als primäre Satellitensysteme werden INMARSAT und IRIDIUM im Bereich der Sprachkommunikation und der schmal-bandigen Datenkommunikation bis 128 kbps verwendet. Die Endgeräte sind entweder im klassischen „Mobiltelefon-Design" mit großer Satellitenstabantenne (z.B.: IRIDIUM 9575 oder ISATPhone PRO) oder in Form eines tragbaren Satellitenterminals in Notebookgröße (z.B. COMHAM Explorer 710) ausgeführt.

mobiles SAT-Terminal IRIDIUM GO

Die neueren Satellitenterminals (z.B.: COMHAM Explorer 510 und IRIDIUM GO!) benötigen bereits ein Smartphone, ein Tablet oder ein Notebook, um das Terminal einzurichten und um die Sprachkommunikation zu betreiben.

Als Verbindungsschicht zwischen Terminal und Endgerät werden WLAN-Protokolle verwendet. Die Sprachkommunikation erfolgt mit dem Protokoll SIP.

mobiles SAT-Terminal IRIDIUM PTT

Eine besondere Form der Sprachkommunikation wurde mittels IRIDIUM „Push to Talk" (PTT) realisiert. Bei IRIDIUM PTT ist es möglich, die Sprachkommunikation via Satellit in Sprechgruppen („Talkgroups") analog eines herkömmlichen Funksprechgerätes zu betreiben. Die Ausleuchtungszonen („Spots") für IRIDIUM PTT können weltweit für definierte Zonen positioniert werden. In diesen Zonen kann ein Funkgespräch zwischen den Geräten für 40 Sekunden geführt werden. Zusätzlich können „Talksgroups" mit anderen IRIDIUM PTT Organisationen geteilt werden.

Eine Gemeinsamkeit der Satellitenkommunikationsanwendungen ist die GPS-Funktionalität. Die zuvor angeführten Terminals verfügen alle über GPS-Antennen zur Positionsbestimmung, welche für den Betrieb der Terminals erforderlich sind. Die Position der Satellitenterminals kann nach entsprechender Konfiguration an ein Verortungssystem („Blue Force Tracking") zyklisch übertragen und anher visualisiert werden.

Die Sprachkommunikation über mobile Endgeräte im Zusammenhang mit dem sicherheitspolizeilichen Assistenzeinsatz (SihPolAssE) und den Assistenzleistungen des Bundesheeres wird zum größten Teil mittels TETRA-Endgeräten durchgeführt.

Die Systemorganisation BOS (Landfunkdienst für Behörden und Organisationen mit Sicherheitsaufgaben) im BMLV wurde in den letzten Monaten stark gefordert, da mehr als 800 Endgeräte nachgekauft, verschlüsselt, programmiert und logistisch bearbeitet wurden.

Ein wesentlicher Bonuspunkt im täglichen Dienstbetrieb für das Ressort ist die Programmierung der BOS-Endgeräte durch eigene Kräfte des Bereiches IKT-Betrieb. Wodurch flexibel und zeitnah auf den Bedarf der Anwender im Ressort reagiert werden kann.

mobiles SAT-Terminal IRIDIUM PTT

Die mobile Datenkommunikation erlangte für viele Bediensteten des Ressorts ab März 2021 mit der Ausrollung des IKT-Service SMN.mobile im SMN eine besondere Bedeutung. Für dieses Service können die Smartphones (z.B.: iPhone ab der Generation XR) als privater WLAN-Hotspot

BOS - Verwendung in einem Fahrzeug

genutzt werden. Ebenso wurden mobile LTE-Router verstärkt in allen Organisationen zur Aufstellung gebracht.

Eine besondere Herausforderung im Jahr 2021 war ab Juni die Implementierung der neuen Organisationsstruktur im ETB-BMLV.

BOS - Programmierstation und verschiedene BOS-Funkgeräte

Durch die Erhöhung des Datenvolumens für ressorteigene Smartphones (10GB) und die Einführung eines unlimitierten Datenvolumens für LTE-Router wurde für die geforderten Services (SMN-Mobile, Videokonferenzen, ...) - ohne nennenswerte Erhöhung der Grundkosten - ein wesentlicher Beitrag zur Digitalisierung - besonders für die Nutzung der IKT-Services im SMN im pandemiebedingten Homeoffice - erbracht.

Durch die Pandemie getriggert, wurde Telearbeit und Homeoffice gefördert und angeordnet. Um die Erreichbarkeit der Mitarbeiter während der Telearbeit und im Homeoffice zu gewährleisten, wurden vermehrt Anrufumleitungen von den Nebenstellen sowohl auf dienstliche- als auch private Mobiletelefone parametriert. Mit dieser Maßnahme bleiben die Bediensteten durch Wählen der jeweiligen Nebenstelle an jedem Ort erreichbar.

Die Einzigartigkeit dabei ist die manuelle Implementierung der Organisationsbezeichnungen - sowohl in der Lang- als auch in der Kurzbezeichnung - aller neuen Ebenen.

Die intensivste Arbeit bestand in der Duplizierung der einzelnen Einträge für die Überleitungsverantwortlichen und die neuen Strukturen. Durch die Zusammenarbeit mit der Abteilung Informationsmanagement und Büroautomation Applikationen des Bereiches Applikationen im IKT&CySihZ konnte die Masse der Organisationselemente mit den dazugehörigen Mitarbeitern und Strukturen termingerecht bis zum Datum der Einnahme der Organisation umgestellt werden.

Ebenfalls im Juli 2021 wurde mit den Arbeiten zur Einführung des Telekommunikationsverbundes (TKV) als Nachfolge für den Nebenstellenverbund Österreich (NVÖ) im Rahmen der Erarbeitung des TKV - Tests vor Zuschlag (TKV TvZ) begonnen.

Der Testaufbau umfasst alle zentralen Komponenten (Server, Session Border Controller, Router, Switches...), alle Varianten von Endgeräten (IP-Phones, TDM-Telefone, analoge Telefone und Softphones und die Integration der Komponenten in das SMN. Bereits diese große Teststellung des TKV fordert alle Bereiche des IKT&CySihZ, weil ein Zusammenwirken aller Services für eine erfolgreiche Überprüfung der geforderten Funktionalitäten erforderlich ist.

Kompetenz im Frequenz-Schlüsselwesen für das Ressort

Der folgende Abschnitt steht unter dem Motto - Kompetenz im Frequenz- und Schlüsselwesen für das Ressort - mit dem Ziel einen Einblick in die Aufgaben des Referates Frequenz- und Schlüsselwesen (Frq&SchlW) und der National Distribution Auhority Ministry of Defence Austria (NDA/Mod AUT) zu geben. Es geht um Aufträge und Aufgaben, welche in einem bestimmten zeitlichen Rhythmus oder auf Anforderung

wahrgenommen werden, deren termin- und fristgerechte Erledigung einen wesentlichen Beitrag zur Aufrechterhaltung der Führungsfähigkeit im ÖBH darstellen.

Der Aufgabenbereich des Referats Frq&SchlW gliedert sich in drei voneinander unabhängige Teile. Die Tätigkeiten beschränken sich nicht nur auf nationale Maßnahmen, sondern spielen sich in erheblichem Maße auch im internationale Umfeld ab. Die internationale Komponente ist im Wesentlichen für den Bereich Frequenzmanagement und die Tätigkeit der NDA/Mod AUT von Bedeutung.

Der Tätigkeitsbereich im traditionellen Schlüsselwesen ist hingegen rein auf nationale Aufgaben ausgelegt. Hier werden sämtliche Schlüsselunterlagen für die in Österreich und bei Auslandseinsätzen verwendeten Systeme gemäß den gültigen Vorgaben und Richtlinien (Schlüsselbereiche, Gültigkeit und Anzahl der Schlüssel) erstellt und an die Bedarfsträger verteilt.

Die Verteilung der Schlüsselunterlagen ist für jedes System verschieden und ist in den jeweiligen betrieblichen Richtlinien festgelegt. In den Richtlinien ist die genaue Bezeichnung der Schlüsselbereiche, die Bezeichnung (Monats-, Jahres-, Primär-, Secundär-, Frequenzsprungsschlüssel, Operator-, Structurekeys, Passwörter, die Gültigkeitsdauer, die Anzahl der zu erstellenden Schlüssel, die Klassifizierungsstufe und die Unterscheidung der Verwendung, (Inlands-, Auslands-, Reserve-, oder Wartungsschlüssel) und die jeweiligen Bedarfsträger festgelegt.

Die Erstellung der Schlüsselunterlagen erfolgt jedoch nur für jene Systeme/Geräte, für die die Schlüssel vom Sachbearbeiter SchlW selbst erzeugt werden.

Datenträger für digitale Schlüssel

Für folgende Systeme/Geräte erfolgt die Schlüsselerzeugung durch das Ref Frq&SchlW:

- BFF-32-0
- CONRAD
- Datenfunksoftware
- GISI
- MEC-9-0
- PRC-2200/A
- TFF-41-0

Lochstreifen Datenträger eines Schlüssels

Beim Frequenzmanagement handelt es sich um einen Teilprozess des Spektrum-Managements, um koordinierte Frequenzzuweisungen und -zuteilungen für militärische Nutzer bereitzustellen und um Störungen im Betrieb zu vermeiden bzw. zu beheben.

Militärisches Frequenzmanagement umfasst primär den Bereich Frequenzverwaltung sowie die Frequenzverteilung und -zuteilung aus dem militärisch nutzbaren Frequenzspektrum an konkrete Funksysteme und Funkstellen.

Die Durchführung erfolgt auf operativer Ebene. Die Umsetzung auf taktischer Ebene wird im Rahmen der Befehlsgebung geregelt.

Der Abteilung IKTCyPl in der Dion 6 IKT und Cyber(vormals Informations- und Kommunikationstechnologieplanung - IKTPl) obliegt die grundsätzliche Funkfrequenzplanung und -koordinierung für das BMLV sowie die Zuständigkeit über die Erteilung von Betriebsgenehmigungen und Frequenzverfügbarkeiten.

Die zentrale militärische Funkfrequenzverwaltung und

Frequenzzuteilung wird im IKT&CySihZ im Referat Frequenz- und Schlüsselwesen (Frq&SchlW) wahrgenommen. Die Zuteilung und Verteilung von Frequenzen erfolgt nicht nur für ressortinterne Bedarfsträger, sondern auch für ziv. Firmen im Rahmen von Erprobungen, auf Anfrage der Fernmeldebehörde und auch für ausländische Truppenteile.

Die Anforderung von Frequenzen für österreichische Truppenteile für Übungen oder Einsätze im Ausland erfolgt durch das Referat Frq&SchlW in der Funktion der NARFA[1] AUT (National Radio Frequency Agency Austria) bei der jeweiligen NARFA im Ausland oder bei gemeinsam koordinierten Frequenzen mit der NATO.

Die Frequenzanträge ausländischer Übungsteilnehmer für Übungen und Ausbildungsvorhaben in Österreich erfolgen ebenfalls über einen genormten Frequenzantrag von der jeweiligen NARFA an die NARFA AUT.

Diese genormten Frequenzanträge erfolgen über ein Online Programm der NATO mit der Bezeichnung SMIROnLine (Spectrum Management Information Repository – SMIR) mit festgelegten Formaten und Abläufen.

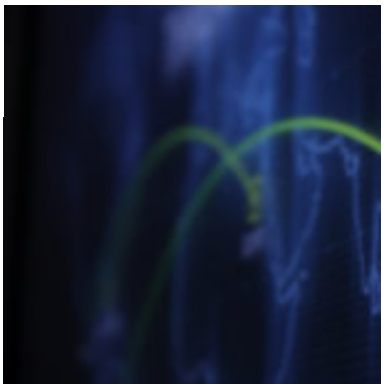
Die Koordinierung, Anforderung bzw. Zuteilung von Frequenzen ist die primäre Tätigkeit, jedoch werden durch das Referat Frq&SchlW auch Anträge für fernmeldebehördliche Bewilligungen für die Verwendung von drahtlosen Mikrofonübertragungssystemen, Steuerungs- und Überwachungssystemen, Funksystemen für die Sturm-Flachwasserboote, Arbeitsboote und Pionierboote für das Ressort bei der Fernmeldebehörde beantragt.

Die erhaltenen Bescheide werden an die Bedarfsträger übermittelt. Alle zugehörigen Daten der Anmeldung und der erhaltenen Bescheide werden durch das Referat Frq&SchlW evident gehalten.

Die Teilnahme an Arbeitsgruppen im Rahmen von Beschaffungsvorgängen, die Erstellung von Fachbeiträgen zu Projektplanungen, Dienstvorschriften, Fernmelde-Planungsdokumenten und betrieblichen Richtlinien, sowie das Mitwirken bei der Systembetreuung, Software-Erprobung und Systemtests für die verschiedensten Systeme (CONRAD, FNMS, KUWEL, Datenfunksoftware runden das Tätigkeitsfeld ab.

Eine enge Zusammenarbeit besteht auch mit der Fernmeldebehörde des BMLRT (Bundesministerium für Landwirtschaft, Regionen und Tourismus), welche dem BMLV Frequenzen und Frequenzbereichen aus den verschiedensten Frequenzbereichen in der sogenannten „Liste staatlicher Funk" (LSF), zur Verfügung stellt.

Die LSF ist das Verzeichnis aller dem BMLV zur dauerhaften Nutzung zugewiesenen Frequenzen und Frequenzbereiche auf Grundlage des Art. 48 des Internationalen Fernmeldevertrages (Funkanlagen für die nationale Verteidigung) und des § 2 Abs. 1 TKG (dem BMLV zugewiesenen Frequenzen und Frequenzbereiche zum Zwecke der Landesverteidigung). Sie gliedert sich in 10 Abschnitte und beinhaltet allgemeine Bestimmungen der Frequenznutzung sowie Angaben über Nutzungsbeschränkungen auf Grund von Bestimmungen der VO Funk (Vollzugsordnung für den Funkdienst) oder in-/ausländischer Frequenzzuteilungen.



[1] Auf internationaler Ebene wird die Bezeichnung NARFA für eine militärische Fernmeldebehörde verwendet. Beim BMLV übernimmt das Referat Frq&SchlW in der Dion 6 IKT und Cyber im Zuge von internationalen Frequenzkoordinierungen die Funktion einer nationalen NARFA, bezeichnet wird sie als NARFA AUT.

Abschnitte der Liste Staatlicher Funk:

- Abschnitt I 9-29700kHz
- Abschnitt II 29,7-47,0MHz
- Abschnitt III 47-68MHz
- Abschnitt IV 68,0-87,5MHz
- Abschnitt V 118-144MHz
- Abschnitt VI 146-174MHz
- Abschnitt VII 230-410MHz
- Abschnitt VIII 410-570MHz
- Abschnitt IX 960-10.000MHz
- Abschnitt X > 10GHz

Im Rahmen der internen Nutzungsvorgaben sind Frequenzen und Frequenzbereiche im BMLV zu eigenen Frequenzgruppen zusammengefasst und im Zuge einer Zuteilung auch als solche anzusprechen.

Analog den Abschnitten der LSF beruht die Einteilung auf den klassischen militärischen Funk- und Radarfrequenzbereichen. Im Gegensatz zur LSF erfolgt eine Unterteilung lediglich in sieben Frequenzgruppen. Der VHF-Truppenfunk sowie der Frequenzbereich über 1 GHz sind jeweils zu einer Frequenzgruppe zusammengefasst.

Einteilung der Frequenzgruppen im BMLV:

- Frequenzgruppe A (HF): Frequenzbereich 9,0 kHz bis 29700,0 kHz (29,7 MHz)
- Frequenzgruppe B (VHF): Frequenzbereich 29,700 MHz bis 87,500 MHz
- Frequenzgruppe C (VHF): Frequenzbereich 118 MHz bis 144 MHz
- Frequenzgruppe D (2m-Band): Frequenzbereich 146 MHz bis 174 MHz
- Frequenzgruppe E (UHF): Frequenzbereich 230 MHz bis 410 MHz
- Frequenzgruppe F: Frequenzbereich 410 MHz bis 570 MHz
- Frequenzgruppe G: Frequenzbereich 1 GHz bis 10 GHz

Die LSF, die für das BMLV getroffene Einteilung in Frequenzgruppen, sowie die Grundsatzweisung „Funkfrequenzspektrummanagement" (Management- und Nutzungsvorgaben für das Funkfrequenzspektrum im BMLV und ÖBH), sind die Arbeitsgrundlagen für das Frequenzmanagement im Referat Frq&SchlW für alle Bedarfsträger und Funksystemen im BMLV und ÖBH.

Die Wahrnehmung der Agenden der NDA/MoD AUT stellt ebenfalls einen Aufgabenbereich des Referats dar.

Im Jahr 2006 erging der Auftrag zur Errichtung einer NDA und seit 2008 wird Kryptomaterial von NATO Mitgliedsstaaten übernommen, registriert und an die Bedarfsträger im ÖBH verteilt. Die NDA/MoD AUT ist verantwortlich für die Verwaltung von Kryptomaterial der NATO innerhalb des ÖBH, die Aufgaben werden durch die Crypto Custodian (Kryptoverwalter) wahrgenommen.

Die Ausbildung zum Crypto Custodian der NDA/MoD AUT erfolgt durch die NSA (National Security Agency) der Vereinigten Staaten von Amerika. Die Arbeitssprache der Crypto Custodian ist auf Grund der internationalen Zusammenarbeit und des englischsprachigen Basismaterials, vorrangig Englisch. Durch die NDA/MoD AUT wird Kryptomaterial in zwei NATO COMSEC Accounts und einem nationalen COMSEC Account verwaltet.

Weiters wurden durch die NDA/MoD AUT vier Sub COMSEC Accounts für Bedarfsträger innerhalb der Organisation des ÖBH errichtet. Kryptogeräte der NATO werden als CCI (Controlled Cryptographic Item) bezeichnet.

Diese Kryptogeräte unterliegen einer besonderen Behandlung im Rahmen der Verteilung, Lagerung und im Betrieb bei den jeweiligen COMSEC Usern (Nutzer von Kryptomaterial). Die NDA/MoD AUT ist Teil des NATO Kryptoverwaltungssystems, welches durch DACAN (Military Committee Distribution & Accounting Agency, NATO) geleitet, koordiniert und kontrolliert wird.

Schlüsselladegerät

Die Nutzung von NATO Kryptomaterial in Österreich ist durch bi- und multilaterale Verträge vereinbart und setzt eine hohe Verantwortung durch die Crypto Custodian in der Umsetzung der damit verbundenen Aufgaben voraus. Vor Unterzeichnung eines Memorandum of Understanding (MoU) und eines Technical Agreement (TA) wird die NDA/MoD AUT zur Prüfung der Verträge auf Durchführbarkeit eingebunden. Auch die Vorgaben zur Einhaltung von technischen Sicherheitsbestimmungen erfolgen durch die NATO. Die Umsetzung erfolgt durch die NDA/MoD AUT in Zusammenarbeit mit den zuständigen Stellen im Resort.

Zur Umsetzung der NATO Vorschriften bei der Nutzung von NATO Kryptomaterial durch Nicht NATO Mitgliedsstaaten (NNN), wurde durch die NDA/MoD AUT die „Regelung zum Umgang mit NATO Kryptomaterial im ÖBH" erstellt und durch IKT&CySihZ verlautbart. Damit wurde die schriftliche Grundlage zur sicheren Handhabung von NATO Kryptomaterial für alle österreichischen COMSEC User geschaffen.

Die Übernahme sowie Übergabe von Kryptomaterial erfolgt durch die Crypto Custodian oder Kuriere der NDA/MoD AUT bei internationalen militärischen Dienststellen, Regierungsstellen sowie Firmen.

Kam zu Beginn der Tätigkeit die NDA/MoD AUT hauptsächlich beim System Eurofighter NATO Kryptomaterial zum Einsatz, so folgten mit der Zeit viele weitere Systeme und Kryptogeräte. Die Kryptoschlüssel können in den verschiedensten Formen (Lochstreifen, Datenträger) übergeben oder/und auf Datenladegeräten geladen werden.

Schlüsselladegerät

Jährlich werden durch die Crypto Custodian oder Kuriere der NDA/MoD AUT, über 6000 km an Straßenkilometern im Rahmen von Kryptotransporten zurückgelegt.

Mit 2020 beginnend und 2021 weiterführend, werden sämtliche bei der FlWft2 befindlichen Kryptogeräte zum Blockupgrade zu einer Firma in Deutschland transportiert und nach Fertigstellung wieder nach Österreich gebracht. Der Transport von Kryptomaterial erfolgt mit speziell umgebauten Fahr- und Flugzeugen.

Foto: Bundesheer/Horst Gorup

Der militärische und zivile Einsatz von Kryptomaterial durch die COMSEC User (Nutzer von Kryptomaterial) erstreckt sich im Rahmen von Übung oder Einsatz, internationaler Dienstverwendung, Teilnahme an Arbeitsgruppen/Projekten über eine Vielzahl von Ländern in Europa, Amerika, Asien bis hin nach Afrika.

Eine Nebenaufgabe der NDA/MoD AUT ist unter anderem die Aufbringung des Signaturzertifikates der Firma A-Trust auf den Dienstausweis, sowie die enge Zusammenarbeit mit der Informationssicherheitskommission des Bundeskanzleramtes bei der Verteilung von EU Kryptomaterial.

IKT&CySihZ

Cyberforces
wir sind cyber

WIR SCHÜTZEN ÖSTERREICH.

bundesheer.at

UNSER HEER

IMG

Institut für Militärisches Geowesen

Auch das Jahr 2021 war für das IMG primär durch die dienstlichen Auswirkungen der Covid-19 Pandemie gezeichnet. Wie im Vorjahr konnte trotz der Corona-Einschränkungen der Dienstbetrieb, die Produktionsleistung sowie die anstehenden Weiterentwicklungen, insbesondere auf Grund der Initiative und Flexibilität der Mitarbeiter, fast ungebremst durchgeführt werden.

Dies inkludierte u.a. die ersten Überlegungen zur Einsatzgeologie, Bereitstellung eines mobilen MilGeo Teams als Force Provider, technologische Weiterentwicklungen im Bereich 3D, Satellitenbildanalyse und Virtual-Reality (VR), Standardisierung des Aktualisierungszyklus der TÜPL-Karten, Optimierungen im Bereich GeoDaten-Visualisierung und Digitalisierung sowie die erfolgreichen nationalen und internationalen Testungen zu Navigation Warfare.

Im Nov 2020 wurde der weit über 10 Jahre alte Organisationsplan des IMG mit dem neuen Referat „Navigation und Galileo" als eigenständiges OrgElement und Truppennummer auf Ebene Einheit übergeführt und 2021 die notwendigen personellen Maßnahmen dazu durchgeführt. Dies inkludierte u.a. auch die Aufnahme einer Reihe von jungen, qualifizierten und motivierten Mitarbeitern in den permanenten Dienststand des ÖBH, um die langfristige personelle Entwicklung des IMG sicherzustellen.

Neben dem hosting einer Reihe von internationalen high level Fachmeetings (PESCO GeoMETOC, MN GSG, EU Geospatial Capability Board) ist insbesondere die gleichzeitige Gestellung zweier Fachfunktionen im Auslandseinsatz aus dem IMG

Bgdr Mag. Dr. Friedrich Teichmann, MAS, MSc

heraus besonders hervorzuheben: den „Chief Geo" bei KFOR und den „Force Cartographer" bei UNFICYP. Sowohl die internationale Reputation als auch der Erfahrungsgewinn der Mitarbeiter bei einem Auslandseinsatz in der Fachfunktion kann nicht hoch genug bewertet werden.

Die anlaufende ReOrg sollte die Möglichkeit bieten, das IMG als kritischer Beitragsleister für „Information Superiority" auf allen Ebenen bestmöglich zu platzieren und die Weiterentwicklung im Bereich Weltraum (Satelliten-Navigation, Erdbeobachtung und Space Situational Awareness) zum Nutzen im Ressort voranzutreiben.

Dem Grundauftrag zur Beitragsleistung zur „Information Superiority" folgend, stellte das IMG auch 2021 mehrfach wöchentlich spezielle Covid-19-Ausbreitungskarten (Österreich, EU, Welt) für die sicherheitspolitische und strategische Führung zur Verfügung.

Das IMG ist der zentrale Dienstleister des BMLV für Geo und Space bzw. Anwendung von Weltraumtechnologien, in der alle Prozessschritte erfolgen: Grundlagenarbeit inklusive wissenschaftlicher GeoFaktoren-Analyse und Innovationsentwicklung, GeoDaten-Beschaffung sowie strukturierte GeoDaten-Haltung, Erstellung von sämtlichen kartographischen Produkten, Anfertigung von einsatzrelevanten Geo-Informationen, spezielle Themenkarten inklusive Satellitenbildanalysen, Bereitstellung der digitalen GeoDaten für alle Waffen-, Einsatz-, Führungs- und Simulationssysteme des Bundesheeres und Spezialprojekte mit Raumbezug, 3D-Modellierungen, Verteilung und Bereitstellung dieser Produkte und die notwendige Fachausbildung auf allen Ebenen. Die Produkte und Dienste des IMG werden Joint, also für Land- und Luftstreitkräfte angeboten, sind international kompatibel im Sinne der Interoperabilität für multinationale Einsätze konzipiert und für alle Führungsebenen und die Gefechtstechnik, erstellt. Derzeit erfolgt der Fähigkeitsaufbau einerseits im Bereich Navigation Warfare in Kombination mit der gesamtstaatlichen Aufgabe für den operativen Anteil der Galileo PRS-Behörde, sowie eines mobiles MilGeo-Elementes mit 3D-Modellierung und Virtuelle Realität.

Binationale Kooperation im Bereich „Gefährliche Fauna“

Die Datenbank „Gefährliche Fauna“ enthält neben der Beschreibung der Tierarten auch die geographischen Aspekte und Details zu den entsprechenden Lebensräumen und Verhaltensweisen der Tiere, die für Menschen potenziell gefährlich sind.

Aber auch Erste Hilfe bzw. Therapieoptionen beim Menschen für den Bedarfsträger sind abrufbar. Möglich wird dies durch die interdisziplinäre Expertise des Teams vom Kdo SanDstBw VI 2. Hier findet das Wissen aus verschiedenen Fachbereichen, beispielsweise der Entomologie, Biologie, Tropenmedizin, Tiermedizin oder Toxikologie,

Pressekonferenz FBM im AG Rossau - Foto: HBF/Pusch

Im Kommando Sanitätsdienst der Bundeswehr VI 2 (Kdo SanDstBw VI 2) wird diese Datenbank weiterentwickelt und mit medizinischen Informationen zu den Gifttieren ergänzt. Bereits auf einer Pressekonferenz des Naturhistorischen Museums (NHM) und des Bundesministeriums für Landesverteidigung (BMLV) am 17. März 2021 sprachen sich die Beteiligten auf österreichischer Seite für eine internationale Zusammenarbeit aus.

Die Weiterentwicklung der Datenbank beim deutschen Partner ermöglicht den Nutzern zukünftig, schnell auf Informationen hinsichtlich der Giftwirkungen von Tieren und Insekten zurückzugreifen.

den Weg in Ausbildung, Einsatzplanung und -vorbereitung sowie direkt in die Einsatzgebiete. Ein großer Schritt und Beitrag zur Force Health Protection des eingesetzten Personals.

Siehe auch unter: https://www.bundesheer.at/cms/artikel.php?ID=10805

MilGeo-Analyse Bergkarabach (fWÜ Experten IMG + LVAk)

Auf Grundlage der von IMG erstellten Satellitenbildkarte für den Einsatzraum Bergkarabach, einer kurzen MilGeo-Information über den Einsatzraum sowie eines Briefings durch den Projektleiter des Institutes für Friedenssicherung und Konfliktmanagement bzw. Institutes für Höhere Militärische Führung an der Landesverteidigungsakademie wurde eine spezielle Vorgehensweise der Durchführung gewählt.

An Hand einer exemplarischen Analyse hochauflösender Satelliten- und Geländedaten wurden militärische Folgerungen hinsichtlich einer Geofaktoranalyse gezogen, die als möglicher taktischer Mehrwert für die Einsatzführung dienen sollen.

Aus militärgeografischer Sicht hat das Gelände und die Verkehrsinfrastruktur das taktische Handeln für alle Konfliktparteien maßgeblich eingeschränkt. Ebenso wurde offenbar nicht zufällig der Zeitraum ab September 2020 für die militärische Operation ausgewählt.

Daher stellt sich die Frage, mit welchen Umfeldbedingungen resp. Möglichkeiten und Einschränkungen für eine defensive und offensive Einsatzführung zu rechnen war.

Unterstützungsleistung: Einsatzgeologie

Auch das Jahr 2021 zeigt die Notwendigkeit der Fähigkeitenentwicklung im Bereich Einsatzgeologie sowohl am Institut für Militärisches Geowesen, als auch im gesamten Österreichischen Bundesheer. Die Vorbereitungen auf die Bewältigung von Naturgefahren wie z.B. das schwere Erdbeben auf der Karibikinsel Haiti am 14. August oder der Vulkanausbruch auf der kanarischen Insel La Palma im Herbst, aber auch Aufgaben des täglichen militärischen Dienstbetriebes wie z.B. geotechnische Baugrunduntersuchungen oder Geländeanalysen, waren demnach Schwergewichte dieses Jahres.

Insbesondere die Unterstützung der HTS/InstPi/LAbt-PiBauD bei der Bodenklassifikation und Tragfähigkeitsbestimmung für den Ausbau der Ortskampfanlage Steinbach in Allentsteig zwischen 27. und 29. Juli war ein Höhepunkt des Jahres. Hier wurde der Untergrund mit einfachem Gerät vor Ort untersucht sowie Bodenproben für eine Laboranalyse entnommen.

Führungssimulator in Weitra, Einsatz VR-Brille, Besuch FBM Tanner

Am 18. Mai 2021 besuchte Verteidigungsministerin Klaudia Tanner die 3. Jägerbrigade in Weitra und nahm an einer digitalen Übung des Bundesheers teils, wo rund 150 Soldatinnen und Soldaten das Vorgehen und die Maßnahmen im Krisenfall trainierten. Fokus der virtuellen Übung waren dabei öffentliche Sicherheit und Ordnung – wie diese rasch wiederhergestellt und auch aufrechterhalten werden können.

FBM Tanner mit der VR-Brille des IMG

Gemeinsam mit dem langjährigeren Entwicklungspartner des IMG, der Firma VRVis, wurde in zwei Projekten eine Anwendung entwickelt, die mithilfe von Virtual Reality-Technologie kooperative, militärgeografische Stabsplanung ermöglicht und somit die virtuelle Einsatzplanung erleichtert. Bundesministerin Klaudia Tanner testete bei ihrem Besuch unter anderem diese Anwendung.

Zusätzlich zur Verwendung von Computern kann mit der „Virtual Reality"-Brille das Einsatzgebiet vorab virtuell besucht werden. Somit können die Soldatinnen und Soldaten bereits in der Einsatzvorbereitung eine weltweite Erkundung des vorherrschenden Geländes durchführen. Durch diese Möglichkeiten sind erste taktische Ableitungen frühzeitig möglich.

AFDRU Übung Tritolwerk

Die "Austrian Forces Disaster Relief Unit" (AFDRU) ist einerseits als Milizeinheit des ABC-Abwehrzentrums strukturell abgebildet und wird andererseits als "Plattform" für den internationalen humanitären und Katastropheneinsatz des Bundesheeres genutzt. AFDRU ist eine speziell für den internationalen humanitären und Katastropheneinsatz trainierte Einheit die sowohl im In- als auch im Ausland eingesetzt werden kann. Dazu werden im Anlassfall, innerhalb weniger Stunden verfügbare Berufs- und Milizsoldaten und erforderliche Spezialisten von zivilen Einsatzorganisationen zu einem hoch qualifizierten Einsatzkontingent formiert.

Das ABCAbwZ führte die AFDRU BWÜ 21 im Zeitraum von 12. Juli 2021 bis 17. Juli 2021 am ABC- & KatHiÜPl Tritolwerk bei Wr. Neustadt durch. Die AFDRU BWÜ 21 wurde unter Federführung ABCAbwZ und Unterstützung durch das IMG

geplant und durch IMG mit einem Team in der Übungsleitung unterstützt. Als Szenario lag ein komplexes Großschadensereignis (diesmal ein "Man Made Disaster"), ausgelöst durch eine Explosion im Hafen von Beirut im Libanon (LBN), zugrunde.

An der AFDRU BWÜ 21 nahmen neben militärischen auch zivile Kräfte ausgewählter Feuerwehren und des Bergrettungsdienstes NÖ teil. Die KW 28 stellte am ABCAbwZ eine Schwergewichtswoche dar. Um Synergien maximal zu nutzen, übte der AFDRU-Basislehrgang, die AFDRU-BWÜ und die Lehrabteilung zur gleichen Zeit am ABC- & KatHiÜPL TRITOLWERK.
Zusätzlich wurde am 15. Juli 2021 das zentrale Partnerschaftsseminar (ZPS) des ÖBH und die Partnerschaftsbeurkundung des ABCAbwZ durchgeführt.

GeoOps Allgemein

Das mobile MilGeoElement (mMilGeoEt) deckt vor Ort auf Ebene einer Brigade alle Bereiche, wie Entscheidungsträgerberatung, Analyse von Geofaktoren, Geodaten- und Kartenproduktion sowie die Geodatenaufnahme im Gelände mit modernsten Mittel, ab.

Generalstabschef Gen Brieger am Stand des IMG: „GIS mit Biss!"

In der Entscheidungsträger- bzw. Kommandantenberatung des Einsatzraumes werden auch Modelle der virtuellen Realität (VR) und Pseudo-3D Modelle verwendet; im Bereich der Geodatenanalyse werden Verfahren der Geostatistik, Multispektralanalyse, Satellitenbildauswertung, 3D-Analyse und andere GIS-Verfahren angewandt.

Die Produktion von digitalen Geoprodukten zur Führungsunterstützung und analogen Einsatzkarten zählt zu den wesentlichen Aufgaben des mMilGeoEt vor Ort.

Neben den klassischen Elementen der Vermessung werden bei der Geodatenaufnahme im Gelände auch innovative Remote Sensing-Verfahren eingesetzt, wie terrestrisches Scanning, Lidar- und Multispektralsensoren auf UAV sowie die Aufnahmetechniken des Systems IKE.

Forschungsmarkttag TherMilAk

Das IMG war am diesjährigen Forschungsmarkttag an der TherMilAk mit zwei laufenden Forschungprojekten vertreten. Nachdem wir 2017 bei der jeweiligen Prämierung mit „GIS mit Biss" den ersten und 2019 mit „milGeoCoopSandbox" den zweiten Platz erreichen konnten, gingen wir dieses Mal erwartungsgemäß leer aus.

Stand 8 „GIS mit BISS" oder „Force Health Protection und Health Promotion für den militärischen Einsatzraum Afrika" demonstrierte im dafür gestalteten Venom Escape Room multimodale Info-Versorgung über die Verbreitung potentiell gefährlicher Tierarten und davon ausgehende einsatzrelevante Beeinträchtigungen.

Im Rahmen der Fortsetzung, Erweiterung und Weiterent-

wicklung der Projektreihe „Gefährliche Fauna“ wird - in Zusammenarbeit sowohl mit dem Naturhistorischen Museum Wien als auch mit dem Sanitätsdienst der Deutschen Bundeswehr - das Ziel verfolgt, Soldatinnen u. Soldaten bestmöglich über potentielle Gefahren durch die Tierwelt in internationalen Einsatzgebieten, notwendige präventive Maßnahmen und Verhaltensweisen zu informieren und mittels Datenbank zur Verfügung zu stellen.

Stand 9 „milGeoCoopSandbox“ oder „Nutzung von Extended-Reality Technologien als Beitrag zur umfassenden Lagebilddarstellung“ präsentierte einen virtuellen „Sandkasten“ (Battle Table) zur kooperativen Nutzung in der milGeoVA (Visual Analytics) für die Beurteilung des militärgeographischen Umfeldes im Rahmen der Stabsarbeit.

Die Erstellung und Akquise von 3D-Daten auf Basis terrestrischer, luftfahrzeuggebundener und satellitenbasierter Sensorik und daraus abgeleiteter 3D-Geo-Produkte sind aktuelle Herausforderungen. Auf Grund der operationell zur Verfügung stehenden Technologie sind Anwendungen aus dem Bereich VA für den Konsum der 3D-Geo-Produkte überaus zweckmäßig.

Marktstandleiter

Das Portfolio an Geo-Produkten des IMG entwickelt sich parallel zu den zur Verfügung stehenden Geo-Basisdaten weiter.

In diesem Kontext ist der Konsum der 3D-Geo-Produkte durch den Bedarfsträger von zentraler Bedeutung: Damit geht ein Technologiesprung einher, der den Konsum von einer Papierkarte in das passende Medium überleitet. Auf Grund der operationell zur Verfügung stehenden Technologie sind Anwendungen aus dem Bereich Visual Analytics (VA) für den Konsum der 3D-Geo-Produkte als überaus zweckmäßig zu beurteilen; die Art der Datenpräsentation innerhalb der VA und eine nachhaltige Nutzung im Anschluss an die VA-Geländeerkundung ist herausfordernd und Inhalt dieses Forschungsvorhabens.

Mitwirkung beim Generalstabslehrgang (Planspiele Horn von Afrika, Donauraum)

Etwa alle drei Jahre wird IMG seitens Landesverteidigungsakademie/IHMF ersucht, die operative Ausbildung im jeweiligen Generalstabslehrgang im Rahmen des „Joint Wargame Horn of Africa“ (in englischer Sprache) mit den relevanten Milgeo-Informationen zu unterstützen, dies war auch im laufenden Kalenderjahr der Fall.

Landing Zones Identified

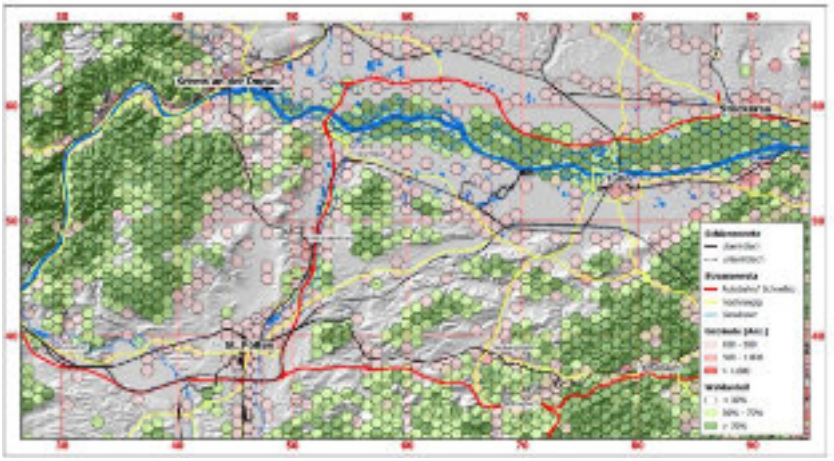
Die Besonderheit 2021 lag allerdings darin, dass erstmals auch - auf den Ergebnissen der operativen Planungen - intensiv auf die Taktik-Ebene eingegangen und ausgeplant wurde.

NÖ Donaurraum - Übersicht physisch

Dabei konnten seitens IMG wertvolle Erkenntnisse hinsichtlich sowohl der Bedarfslage als auch der wechselseitigen kommunikativen Erfordernisse gewonnen werden. Auch der Donauraum wurde intensiv beübt, und hier war ein Geo-Fachmann ebenfalls gefragt (übrigens immer derselbe...):

Geostatistische Analyse des Einsatzraumes – Hexagon-Karte

Die militärgeographische Aufbereitung des Geländes im Einsatzraum stellt eine Kernaufgabe des militärischen Geodienstes dar. Um diese Aufbereitung rasch und in wiederholbarer Qualität durchzuführen, wurde erstmals im Rahmen des Lehrplanspiels 21 der LVAk eine automatisierte geostatistische Auswertung konzipiert und umgesetzt.



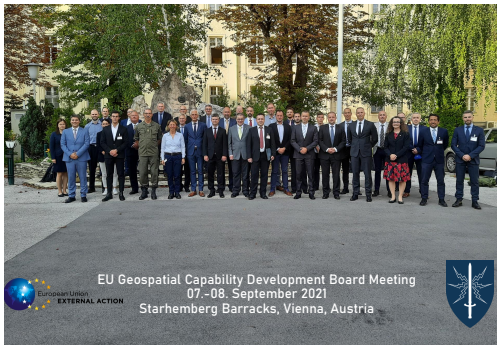
Geostatische Auswertung Rm St.Pölten - Krems/D. - Tulln

Basisdaten der geostatistischen Auswertung sind österreich- und weltweit verfügbare Geodaten, wie Geländehöhenmodell, Landbedeckung oder Siedlungsstrukturen. Als statistische Befundgröße wurde das Hexagon gewählt, das auf Grund seiner topologisch/geometrischen Eigenschaft eine gleichartige Nachbarbeziehung zu allen angrenzenden Hexagonen besitzt.

Das Hexagon kann bei der statistischen Auswertung als Container für sämtliche Ergebnisse verstanden werden; Quantitäten in absoluten Zahlen oder flächenmäßige Anteile an der Gesamtgröße des Hexagons sind Beispiele statistischer Kennwerte des jeweiligen Hexagons. Welche Kennwerte in der militärgeographischen Aufbereitung des Einsatzraums relevant sind, ist im Dialog zwischen Bedarfsträger und dem militärischen Geodienst zu bestimmen.

Für das Lehrplanspiel 21 und der anschließenden Joint Action 21 wurden Bewaldung, Bebauung, und Steilheit des Geländes automatisiert den Gewässern, Verkehrs-, Energieversorgungsnetzen gegenübergestellt, und dienten danach als Datengrundlage für spezifische Geo-Produktanfragen der einzelnen Stabszellen. Diese automatisierte geostatistische Auswertung ist als konsequente Fortführung der bestehenden Geofaktorenmatrix zu verstehen, kann auf einen beliebigen Einsatzraum angewendet werden und liefert wiederholbare und nachvollziehbare Resultate. Die Bereitstellung dieser Geoproduktart im Rahmen der Joint Action 21 und dem damit verbundenen intensiven Gedankenaustausch mit dem Bedarfsträger dient als Orientierung zur Weiterentwicklung dieser militärgeographischen Fähigkeit.

Hosting Internationaler Treffen im Fachbereich



EU Geospatial Capability Board in Wien

Multi National Geo Support Group in Salzburg

6th Geo Meteorological and Oceanographic Support Coordination Element in Wien

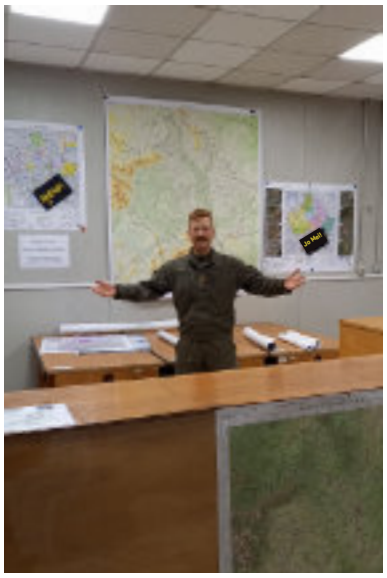
Attachés am TÜPl Seetaler Alpe

MilGeo-Fachpersonal im Auslandseinsatz: Kosovo (KFOR), Zypern (UNFICYP)

KFOR

Seit August 2020 besetzt Österreich durch Angehörige des IMG (bisher Oberst M. Göttlich, Oberst Heissl, Hauptmann Thur und Major Köstinger) den Posten des KFOR „Chief Geo". In seiner Funktion als Kommandant der Geosektion, die Teil der J2-Branch im KFOR-Hauptquartier ist, steuert er den gesamten Geosupport bei KFOR, der auch zwei nachgeordnete Geozellen bei Regionalkommanden umfasst. Die Arbeit erfolgt im 500m² großen Map Depot im Camp Film City (Pristina) in dem rund 100.000 Karten gelagert werden.

Unter Abstützung auf den von den USA gestellten Geoanalysten werden pro Monat etwa 500 Geoprodukte ausgegeben, Karten aktuell gehalten und gedruckt, Anfragen nach Spezialkarten erfüllt sowie digitale Führungssysteme gewartet.



Hauptmann Thur im Map Depot KFOR

Der KFOR Chief Geo kann außerdem auf die Unterstützung durch die NATO Communications and Information Agency (NCIA) zählen. Diese beauftragt er bei längerfristigen Vorhaben, wie momentan der Erstellung eines aktualisierten Datensatzes für Straßen und darauf aufbauend eines Straßenatlas.

UNFICYP

Multinat. Geländebesprechung über ein Bauvorhaben innerhalb der Pufferzone mit Teilnehmer aus DE, RO, AR, CY, AT, GB, CN

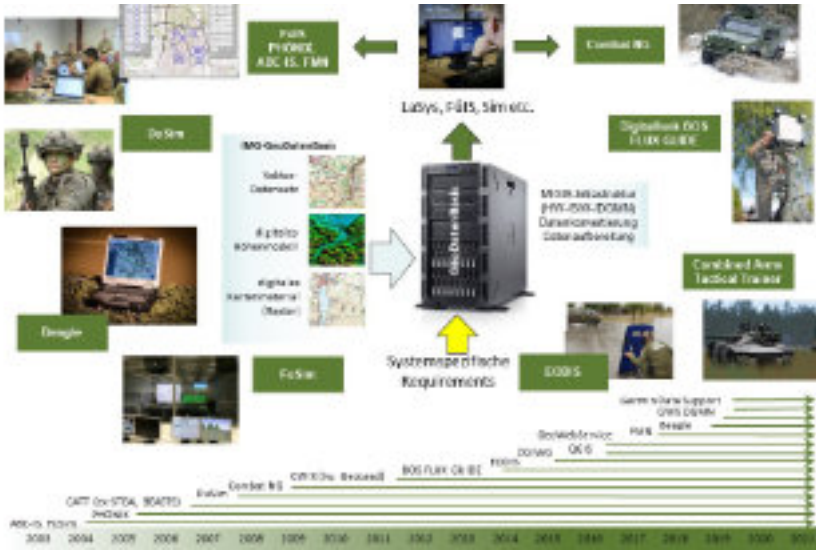
Von Juli 2020 bis Juli 2021 verantwortete R Dr. STRAUß (Ref MilGeo am IMG) als SO3-CARTOG die Kartographie der gesamten UN-Mission auf Zypern (UNFICYP). Dabei wurden neben der Produktion klassischer Karten und Geo-Softwareschulung auch geographische Analysen und Satellitenbildauswertungen durchgeführt, deren Ergebnisse u.a. durch die Missionsleiterin auch dem Sicherheitsrat der Vereinten Nationen präsentiert wurden.

Auf Grundlage der österreichischen Geo-Expertise wurde erstmals eine umfassende Analyse der Geo-Datenqualität durchgeführt, wobei Geometrie, Koordinate und Semantik der Realität gegenübergestellt wurde. Die Erkenntnisse aus dieser Analyse bildeten den Ausgangspunkt einer tiefgreifenden Daten-Hygienemaßnahme entlang der gesamten Pufferzone. Zusätzlich zu den Aufgaben des SO3-CARTOG wurden die Agenden des NUO, WiUO und KzlUO für das österreichische Kontingent übernommen sowie erstmals eine Alarmierungskette für alle militärischen Stabsmitglieder des Hauptquartiers aufgebaut und geleitet.

Das Jahr 2021 im Referat Daten & Systeme

Einen Überblick über die meisten durch das Referat Daten & Systeme im Jahr 2021 mit Geodaten versorgten und betreuten Plattformen aus den Bereichen Land, Luft und Simulation sind den beiden folgenden Abbildungen zu entnehmen. Auffallend ist dabei beispielsweise, dass sämtliche Luftfahrzeugtypen des ÖBH - von dem A-25 "Tracker" über den S-70 "Blackhawk" bis zum Eurofighter Typhoon als Bedarfsträger des Referates Daten & Systeme vom IMG mit Geodaten versorgt werden.

2021 starteten außerdem die Vorarbeiten zum Geosupport für das Cockpit/MissionPlanningSystem des Leonardo AW169M.
Gleichsam "hinter den Kulissen" war das Jahr 2021 nicht zuletzt geprägt durch die intensiven Arbeiten an der Erstellung eines GeoWebService für das ÖBH. Eine besondere Rolle spielte dabei die intensive Zusammenarbeit mit der Abteilung Einsatzorientierte Applikationen (EinsAppl) der Dion 6 IKT und Cyber, die für die reibungslose IT-technische Umsetzung des GeoWebService verantwortlich zeichnet.



Portfolio RefDaten 2021 - Land, Grafik: Dion 6 IKT und Cyber/IMG

Mit Abschluss der letzten Performancetests Ende des Jahres und der Durchführung eines finalen Sicherheitsaudits Anfang 2021 wurde das GeoWebService des ÖBH mit 1. Quartal 2021 in den Regelbetrieb übergeführt werden und somit einem breiten Nutzerkreis im ÖBH künftig eine Vielzahl an digitalen Geodaten anbieten können.

Geowebservice – Ein neues IT-Service im ÖBH geht online

Das im abgelaufenen Jahr 2021 als neues Service in den Regelbetrieb übernommene GeoWebService des Bundesheeres (GWS/ÖBH) bietet dem Nutzer verschiedenste Geodaten, etwa topographische oder thematische Karten aller Maßstabsbereiche sowie Luft- und Satellitenbilder, die über einen Webservice zur Verfügung gestellt werden. Programme, die über die standardisierte OGC-Schnittstelle Web Map Service (WMS), Web Map Tile Service (WMTS) oder Web Feature Service (WFS) verfügen, können auf diesem Weg auf aktuelle Geodaten zugreifen ohne diese lokal gespeichert zu haben. Eine SMN-Netzwerkverbindung ist allerdings Voraussetzung für die Nutzung des GWS/ÖBH.

Gemeinsam mit der Abteilung Einsatzorientierte Applikationen (EinsAppl) der Dion 6 IKT und Cyber konnte die Entwicklung des GWS/ÖBH 2021 entscheidend vorangetrieben werden. Durch die Nutzungsvorgabe von IKTPl konnte der Probebetrieb beendet und GWS im Sommer 2021 in ein reguläres IT-Service übergeführt werden.

Je nach den Bedürfnissen und den Anforderungen, die durch die Bedarfsträger an das IMG herangetragen werden, ist es möglich, den GWS/ÖBH laufend in seinen Funktionalitäten und seinem Datenumfang zu erweitern.

„Wir für euch!" – Der Basislehrgang Geoinformationssysteme

Das seit 2020 verfügte Curriculum „Basislehrgang Geoinformationssysteme (GIS)" stößt bei einer Vielzahl von mit Geoinhalten befassten Dienststellen des BMLV bzw. ÖBH auf reges Interesse.

Die Kurse gemäß diesem Curriculum fanden 2021 in der 14., 20., 24. und 40. KW in Bruckneudorf, Felixdorf, Allentsteig bzw. Salzburg mit insgesamt 28 interessierten und motivierten Teilnehmern u.a. aus den Bereichen ARWT, HLogS, HMunA, HTS/InstPi, MilKden PzGrenB35 und der Miliz (OSZE) statt.

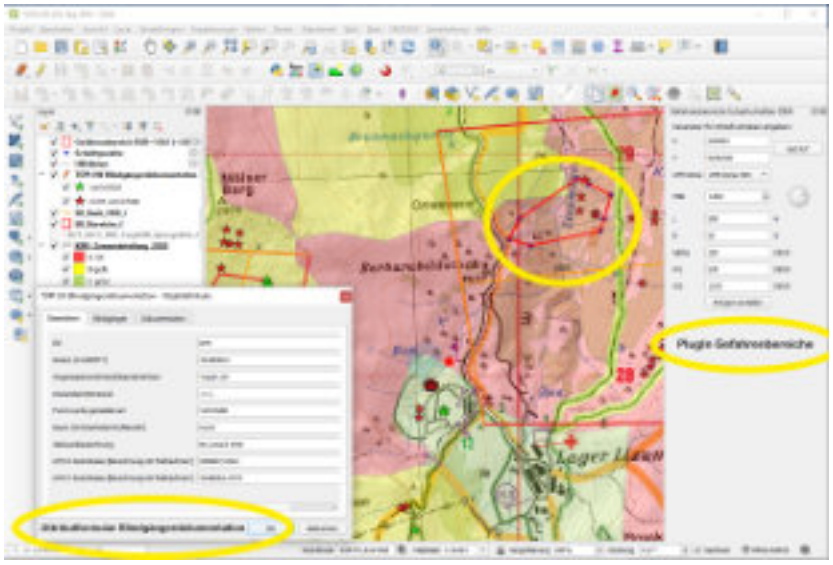
Internationale Standardisierung von Geodaten – DGIWG und JGSWG

Die Defence Geospatial Information Working Group (DGIWG) ist eine Arbeitsgruppe mit dem Ziel die weitest gehende Interoperabilität von Geoinformation im militärischen Kontext zu ermöglichen. Das BMLV ist seit 2017 eines ihrer 25 Mitglieder, die sich mehrmals pro Jahr zu verschiedenen Meetings treffen und 2021 teilweise mehrmals pro Monat über Telecons konferierten.

Die DGIWG arbeitet eng mit der NATO Joint Geospatial Standards Working Group (JGSWG) zusammen, die in vielen Fällen als „Auftraggeber" seitens NATO fungiert. Die JGSWG ist für die Ausarbeitung und Pflege aller georelevanten STANAGs zuständig.

Das IMG/Referat Daten & Systeme war 2021 Mitglied in zwei Custodial Support Teams (CST) der JGSWG (NATO Geospatial Information Framework „NGIF" und Defence Geospatial Web Service „DGWS").

GIS für „Jedermann" – Der Einsatz von QGIS im ÖBH



QGIS-Oberfläche mit PlugIn Gefahrenbereiche und Eingabeformular „Blindgängerdokumentation" (Grafik: Dion 6 IKT und Cyber/IMG)

Das Referat Daten & Systeme des IMG unterstützt mit seiner Geokompetenz im Bereich GIS-Projekte sämtliche Dienststellen des BMLV/ÖBH von der Projektkonzeption, über die umfangreiche Einweisung der Mitarbeiter mittels Basislehrgang-GIS (s. unten) und individuell aufbereiteten Workshops bis hin zur Aufbereitung von Geodaten in den verschiedensten Raster- und Vektorformaten.

Im November wurde die Version 3.10.4 von QGIS durch die aktuelle Longterm-Release 3.16.10 ersetzt.

Geodaten des IMG für die Hochgebirgslandelehrgänge Winter und Sommer 2021

Die Hochgebirgslandelehrgänge (HGLLG) im Februar und August 2021 dienten einmal mehr sowohl der Erlangung der Einsatzpilotenqualifikation der in Ausbildung befindlichen Piloten als auch der Fort- und Weiterbildung der Einsatzpiloten der Österreichischen Luftstreitkräfte.

Dabei werden die HGLLG unter der Leitung der Flieger- und Fliegerabwehrtruppenschule, wegen der unterschiedlichen Witterungsverhältnisse einmal im Winter (Februar) und einmal im Sommer (August) in hochalpinen Räumen Österreichs – etwa in den Hohen und Niederen Tauern oder rund ums Hochkönig-Massiv – durchgeführt.

Durch IMG Referat Daten & Systeme wird dabei aktuelles topographisches Kartenmaterial mit den, für die Dauer des Übungsvorhabens wesentlichen Geodatensätzen angepasst, in verschiedenen Maßstäben aufbereitet und sowohl als gedruckte Kartenwerke als auch in digitaler Form für den Einsatz in den Cockpits aufbereitet.

Der internationale Geodatenbestand über die Luftraumstruktur

Bis vor wenigen Jahren reichte es aus, die österreichischen Militärpiloten mit Kartenmaterial von Österreich auszustatten, mittlerweile sind die Luftstreitkräfte (LuSK) bei diversen Auslandseinsätzen nicht mehr wegzudenken und so änderten sich auch die Bedarfe der Luftstreitkräfte, die nun regelmäßig Unterlagen zur Luftraumstruktur ausländischer Einsatz- und Übungsräume bei IMG abrufen.

Neben diesen internationalen Einsätzen kommen noch internationale Übungen oder auch die Teilnahme an Airshows hinzu. Die Piloten brauchen daher ein dementsprechendes Kartenmaterial mit der aktuellen Darstellung der Luftraumstruktur dieser Nationen.
An diese speziellen Daten heranzukommen ist jedoch kein Leichtes oder mit erheblichen Kosten verbunden. Natürlich gibt es namhafte Anbieter, welche weltweit und tagesaktuell Luftfahrtkarten in unterschiedlichen Maßstäben bereitstellen. Diese werden auch in digitaler als auch in gedruckter Form von Dion 6 IKT und Cyber/IMG beschafft, aufbereitet und bereitgestellt.

ÖH-58 bei der Übung „Cold Response" über einem norwegischen Fjord

Jedoch damit findet man nicht immer das Auslangen. Die Probleme beginnen manchmal schon bei der Einspielung in die Flight Management Systeme (FMS) der jeweiligen Luftfahrzeuge.
Nicht alle dieser FMS sind in der, Lage die gleichen Datenformate zu verarbeiten. Es kommt noch hinzu, dass die Einspielung stets mit einer Datenkonvertierung einhergeht und damit in der Regel immer mit Qualitätsverlusten behaftet ist. Last but not least stellen die meisten dieser Karten nur die zivilen Luftraumstrukturen dar. Bei gemeinsamen Übungen oder Einsätzen ist es jedoch erforderlich, auch über militärische Lufträume Bescheid zu wissen.

Aus diesen Gründen ist es nach wie vor unabdingbar, einen eigenen Geodatenbestand über die Luftraumstruktur in unserem Umfeld zur Verfügung zu haben um diesen den Militärpiloten bei Bedarf bereitstellen zu können.

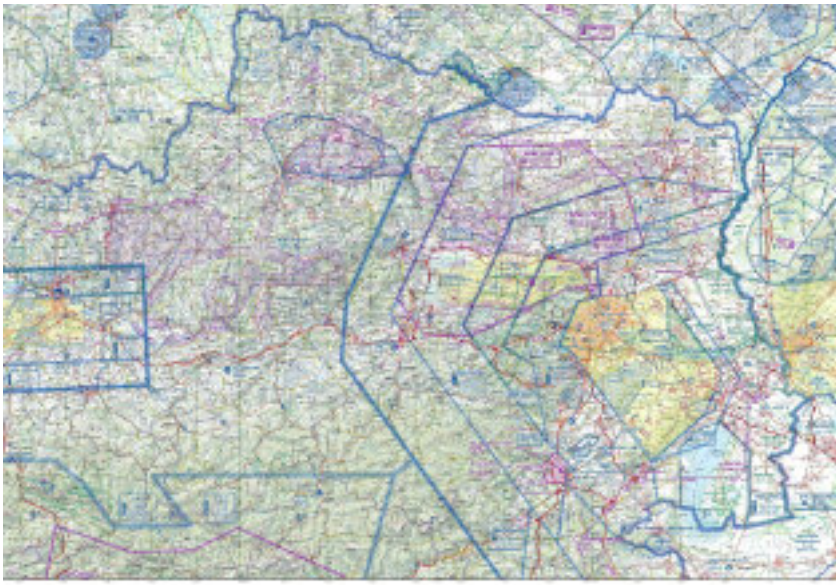
Einer der Hauptabnehmer dieser digitalen, selbst erstellen Kartenwerke ist das WaSys Eurofighter. Die speziellen Anforderungen des Eurofighters hinsichtlich der Einspielung von Geodaten oder Karten in das Flight Management System erforderten diesen Aufwand. Auch hier begann es im Kleinen mit der Luftraumstruktur von Österreich, es folgte kurz danach die Aufbereitung des Schweizer Luftraumes für die jährlich stattfindende Luftraumsicherungsoperation zum Schutz des Weltwirtschaftsgipfels (WEF) in Davos. Eine Ausbildungskooperation mit Deutschland folgte, vorerst begnügte man sich mit Kartenmaterial, welches die Luftraumstruktur Deutschlands bis Neuburg an der Donau darstellt. Gemeinsame Schießvorhaben mit den Eurofightern der Deutschen Luftwaffe über der Ostsee fordern nun auch die Aufbereitung der Luftraumstruktur bis zur Nord- und Ostsee, sogar über den deutschen Luftraum hinaus, denn ein Ausweichflugplatz bei diesen Vorhaben liegt auf dänischem Staatsgebiet.

ÖMK500 – Ausführung Flieger, Ausgabe 2021

Bevor aber der ausländische Luftraum bearbeitet wird, muss jährlich eine Österreichische Militärkarte – Ausführung Flieger in den Maßstäben 1:500.000 und 1:250.000 erstellt werden. Das Inkrafttreten dieser Fliegerkarten ist an das Erscheinen der zivilen Luftfahrtkarten der Austro Control gebunden und erfolgt üblicherweise im Frühjahr. Schon im Vorfeld ist es erforderlich, hier die Geodaten zu beschaffen, zu vergleichen, gegebenenfalls zu korrigieren und einzuarbeiten.

Das durch IMG ausgearbeitete Kartenmaterial wird vor Drucklegung einer Überprüfung durch Dion 2 unterzogen, um eine dementsprechende Qualitätssicherung gewährleisten zu können. Nach Drucklegung erfolgt die logistische Verteilung der Karten an die Bedarfsträger. Die ÖMK500Fl wird als ein Kartenblatt mit Vorder- und Rückseite, die ÖMK250Air ebenfalls als beidseitige, fünfblättrige Kartenserie herausgegeben. Das erstellte Kartenmaterial dient jedoch nicht nur der Navigation im Fluge, sondern wird auch für Planungen, Ausbildung und Flugvorbereitung herangezogen.

Hier endet jedoch noch nicht die Arbeit des IMG, die digitalen Vorlagen werden an die Flugmanagementsysteme (digitalen Cockpits) der einzelnen Luftfahrzeuge hinsichtlich Dateigröße, Farbgebung, Ein- bzw. Ausblendung einzelner Ebenen usw. angepasst, exportiert, konvertiert und danach über die Fliegerwerften in die einzelnen Luftfahrzeugtypen eingespielt.



Detail der ÖMK500 Ausführung Flieger (ÖMK500Fl) - (Grafik: Dion 6 IKT und Cyber/IMG)

A Never Ending Story – Die Aktualisierung der Tiefflugstreckenkarten

Für die Österreichischen Luftstreitkräfte ist der Tiefflug ein wesentliches Ausbildungs- und Übungskriterium. Hierbei geht es um Flugbewegungen unterhalb der gesetzlich vorgeschriebenen Mindestflughöhe von 150 m. Zu diesem Zweck wurden in Österreich Tiefflugstrecken- und gebiete festgelegt. Innerhalb dieser Gebiete gilt für Hubschrauber eine Mindestflughöhe von 5 m, für Flächenflugzeuge gelten 25 m und für Jets ist der Tiefflug derzeit untersagt. Das Fliegen in diesen niedrigen Höhen erfordert aber ein dementsprechend fundiertes Wissen über die Topographie und auch über etwaige Hindernisse in diesen Gebieten. Das IMG stellt zu diesem Zweck Kartenmaterial im Maßstab 1:50.000 mit Einzeichnung der lateralen Abmessungen sowie der Hindernisse dar.

Die neuen Schlechtwetterflugweg karten

Seit Bestehen der LuSK existieren Schlechtwetterflugwege. Dies sind definierte Wege, welche markante Wegpunkte aufweisen und Flugplätze miteinander verbinden. Sie dienen, wie der Name schon sagt, der Navigation bei schlechten Sichtverhältnissen.
Ursprünglich existierten ganze Listen mit Schlechtwetterflugwegen im Flugbetriebshandbuch, die alle Flugschüler auswendig lernen mussten. Jedoch auch hier verändert die Zeit einiges. Eine Überarbeitung dieser Schlechtwetterflugwege erfolgte jedoch nie durch die LuSK. Der Wunsch, diese jedoch für die Flugplanung als auch im Cockpit zur Verfügung zu haben, bestellt jedoch schon.

Nach Antrag des Institut Flieger /Flieger- und Fliegerabwehr Truppenschule (FIFIATS) erfolgte eine Ausarbeitung des zwar veralteten aber immerhin vorhandenen Basismaterials. Die ersten Ausarbeitungen wurden an die FIFIATS/Inst FI und Inst HS übergeben, welche die geänderten bzw. durch IMG neu erstellten Flugwege erkundeten und auf deren Flugtauglichkeit überprüften. Nach Rückmeldung durch die Militärfluglehrer wurden die Geodaten nochmals überarbeitet und bereitgestellt. Das Ergebnis dieser Bearbeitung sind nun Schlechtwetterflugwege, welche an die heutigen Gegebenheiten angepasst wurden, denn in den letzten dreißig bis vierzig Jahren wurde einiges an Infrastruktur in Österreich errichtet. Neue Autobahnen oder Eisenbahnlinien entstanden. Die Orts- oder Industriegebiete vergrößerten oder änderten sich.

Cockpit-Update des S70 "Black Hawk" – Bearbeitungen und Herausforderungen 2021

Seit dem Jahr 2020 läuft bereits das Cockpit-Upgrade des S70 „Black Hawk". Die Avionik des „Black Hawk" war nach 20 Jahren nicht mehr State of the art und muss an die Erfordernisse der Zeit angepasst werden. Gleichzeitig mit dem Avionik-Upgrade beschloss die Bundesregierung im Jahr 2015 die Flotte von neun Stück auf zwölf Stück zu erweitern. Im Bereich von Cockpit-Umrüstungen konnte das Österreichische Bundesheer und so auch das IMG auf die Erfahrungen beim Upgrade des AB212 zurückgreifen.

Gut verpackt trifft der erste modifizierte S-70 wieder auf seiner Homebase, dem FIH Brumowsky, ein

Die LuSK entschieden sich für den Ankauf von Kartenmaterial und Geodaten des namhaften Herstellers Jeppesen. Zusätzlich muss es aber möglich sein, eigene militärische Karten und Geodaten in die Avionik einzuspielen. Mittlerweile sind drei Maschinen auf die neue Avionik umgerüstet.
Diese Umrüstung erfolgt bei AVALEX in Florida/USA. Gleichzeitig wurde auch eine Mission Planning Station (MPS) beschafft, bei deren Überprüfung jedoch gravierende Fehler und Unzulänglichkeiten auffielen.

Geodaten für den AW169M „Leonardo" – Erste Schritte

Viele Erfahrungen des Cockpit-Upgrades des „Blackhawk" (s.o.) können für die Geodatenaufbereitung bei Einführung des IMzHS AW169M verwendet werden. Auch hier wurde IMG bereits im Vorfeld in die Planungen und Erstellung des Pflichtenheftes eingebunden.

Der AW169M verfügt über ein topmodernes digitales Cockpit für dessen Moving Map System IMG sämtliche Geodaten aufbereitet (Grafik: Leonardo)

Es gibt bereits seitens der LuSK eine mit Leonardo akkordierte Zeitleiste für die Testung der Avionik und der Mission Planning Station (MPS) samt dessen Geodaten.

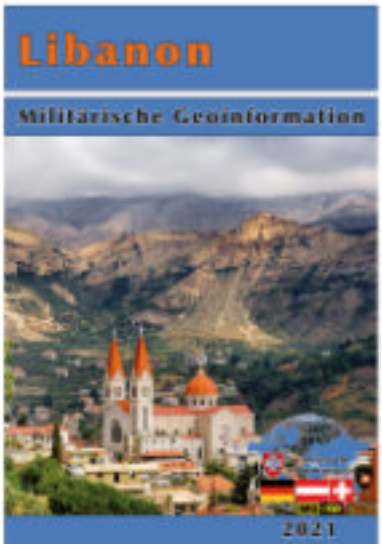
So wurden im 2. Halbjahr 2021 die ersten Geodaten an Leonardo zum Import in die MPS übergeben: ÖMK500Fl, ÖMK250Air, ÖMK50, Ortho- und Sat-Bilder usw. Danach erfolgt die Prüfung der Auflösung und der Qualität in der MPS.

Militärische Geoinformationen 2021

Für ausgewählte Krisengebiete der Erde und (potenzielle) Einsatzräume des ÖBH erstellt Dion 6 IKT und Cyber/IMG Militärgeographische Landesbeschreibungen (MLB) und Militärische Geoinformationen (MGI).

Diese landeskundlichen Informationen stellen einen allgemeinen Überblick über das jeweilige Land zu verschiedenen Themengebieten dar (Inhalte siehe untenstehende Abbildung). Sie dienen militärischen Planern als Bearbeitungs- und Beurteilungsunterlage sowie 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.



Coverbild der MGI Libanon 2021

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").

Dion 6 IKT und 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. Koordinierung, Kartographie, Lektorat und Layoutierung werden dabei federführend von Dion 6 IKT und Cyber/IMG wahrgenommen.

Inhalte MLB/MGI

Sämtliche MLB/MGI sind im Intranet auf der Seite des Militärischen Geowesens in der Rubrik „Länderinformationen" unter folgendem Link abrufbar: http://www.iktcysihz.intra.bmlv.at/geo/index.html

2021 wurden folgende MLB/MGI erstellt bzw. aktualisiert:

- MGI LIBANON (Neubearbeitung)
- MGI ÄTHIOPIEN (Aktualisierung der Ausgabe 2015)
- MLB ZYPERN (Neubearbeitung)

Karten für den TÜPl Lizum/ Walchen

Mit der Neuauflage der „Österreichischen Militärkarte 1 : 25 000 Truppenübungsplatz Lizum/Walchen" wurden die Veränderungen, die sich seit 2015 am TÜPl-Gelände zugetragen haben, kartographisch aktualisiert.

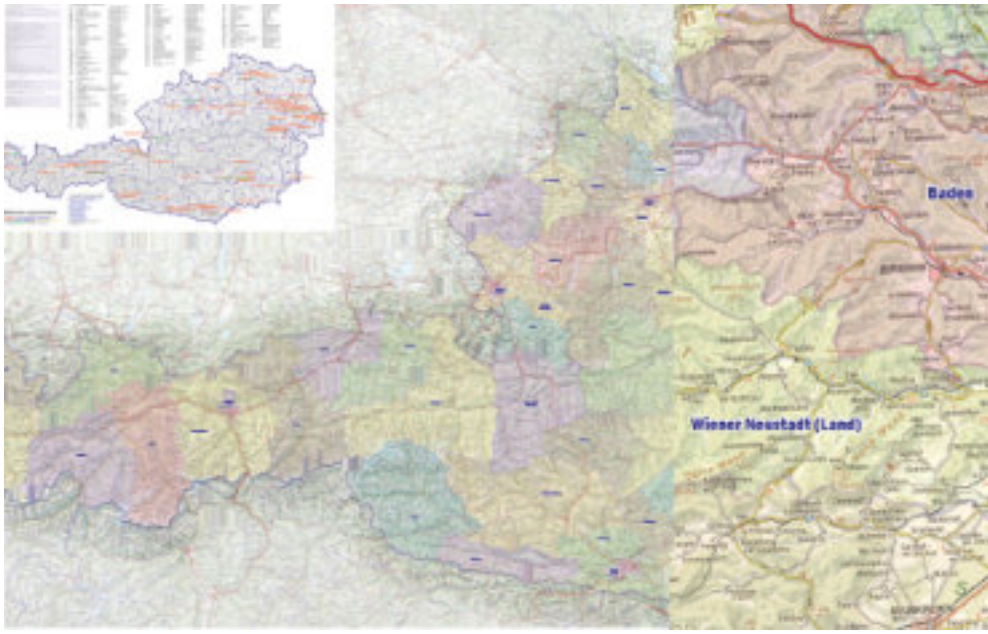
In enger Absprache mit dem TÜPl-Kommando konnten alle notwendigen Korrekturen eingearbeitet und die Karte inhaltlich somit auf den neuesten Stand gebracht werden. Gleichzeitig wurden die Kartenrandgestaltung sowie die Rückseite vollständig graphisch überarbeitet und den aktuellen Designvorgaben angepasst.

Zusätzlich wurden für die beiden Lagerbereiche neue, orthophotobasierte Lagerkarten im Format A3 maßgeschneidert angefertigt und dem Bedarfsträger zur Verfügung gestellt.

Ausschnitt aus der Lagerkarte Lizum

Österreichische Militärkarte 1 : 300.000 mit Politischen Bezirken

Diese Sonderkarte im Format 200 x 100 cm beinhaltet auf Basis des maßstäblich etwas verkleinerte Kartenwerkes „Österreichische Karte 1 : 250 000" (das standardmäßig aus 12 Einzelblättern besteht) eine Übersicht über die Politischen Bezirke Österreichs inklusive deren Bezeichnungen auf einem Blatt.



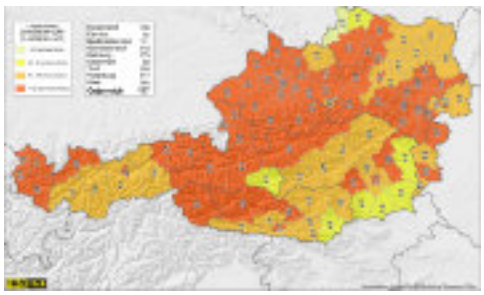
Sonderkarte 1:300 000

Dazu sind die Bezirke als Farbflächen semitransparent der Grundkarte überlagert worden. Zusätzlich informiert sie mittels einer Einsatzkarte im Maßstab 1 : 1 100 000 über die Standorte von Militärischen Liegenschaften nach Nutzungskategorien (z.B. Kaserne, Fliegerhorst, TÜPl, Kommandogebäude).

Sie dient den Planungs-, Übungs- und Einsatzeinheiten zur Unterstützung beispielsweise bei Assistenzleistungen, unter anderem in Zusammengang mit Covid-19, sowohl als geographische Übersicht als auch zur Verdeutlichung von zivilbehördlich territorialen Zuständigkeiten.

Covid-19 Kartenproduktion

Auch im Jahr 2021 war die Covid-19 Pandemie eines der bestimmenden Themen bei den Tätigkeiten des IMG. Im Jahresverlauf wurden gut 350 Karten zu der Entwicklung der Covid-19-Situation in Österreich und Europa, sowie zu der jeweils aktuellen Covid-19-Ampelschaltung erstellt.
Zunächst wurde die bereits im Jahr 2020 etablierte Karte mit den aktiven Covid-19 Fällen in Österreich fortgeführt, im März erfolgte eine Umstellung des Karteninhalts auf die 7-Tages-Inzidenz pro 100.000 Einwohner.



Covid-19 7-Tages-Inzidenz für Österreich

Auch die Karte zur Situation in Europa wurde auf diesen Karteninhalt umgestellt, hier erfolgte der Wechsel im Oktober des Jahres. Für beide Karten wurde im Juni die Frequenz der Erstellung reduziert.

Aktuell wurden zwei Mal, am Wochenbeginn sowie Mitte der Woche, Karten mit den aktuellen Inzidenzzahlen und jeweils am Ende der Woche eine aktualisierte Version der Corona-Ampel-Karte veröffentlicht.

MilGeo-Logistik allgemein

Die Hauptaufgabe des Referates Militärische Geoproduktbereitstellung am IMG ist es, das Österreichische Bundesheer, sprich alle Truppennummern, mit den aktuellen systematisierten Kartenwerken (TOP050, 250 und 500 sowie Fliegerkarten im Maßstab 250 u. 500), welche vom IMG in Kooperation mit dem Bundesamt für Eich- und Vermessungswesen (BEV) produziert werden, zu verteilen. Somit kann im Ernstfall jederzeit auf das neueste Kartenmaterial zurückgegriffen werden. Diese analogen Karten sind in Zeiten von Blackout Goldes wert. Somit ist der Soldat im Einsatz oder bei einer Übung mit diesen Kartenwerken bestens ausgerüstet.

Jährlich werden dadurch ca. 500.000 Blattbereiche der TOP050 bewegt. Weiters verfügt dieses Referat über ein analoges Kartenarchiv, hauptsächlich Karten des zivilen Marktes für die sofortige Verwendung, z.B. für Auslandseinsätze (Straßenkarten, topographische Karten, Stadtpläne, Wanderkarten; ca. 600 Stück weltweit) und ca. 120 Stück Fliegerkarten.

Navigation Warfare allgemein und am TÜPl Seetaler Alpe, „Seetaler Festspiele"

Navigation Warfare (NavWar) ist eine allgemeine militärische Aufgabe im Einsatz, bei der durch die Gesamtheit aller Maßnahmen die gegnerische Nutzung von Positions-, Navigations- und Zeitinformationen (PNT-Services) verhindert oder eingeschränkt und die wirksame Nutzung durch eigene Kräfte sichergestellt wird. Durch die Fähigkeit Navigation Warfare wird im ÖBH durch gesicherte PNT-Services (Position-Navigation-Timing) ein entscheidender Beitrag zum Schutz der Soldaten, Waffeneinsatzsysteme, Plattformen und von Infrastrukturen geleistet. Geprüfte PNT-Services sind integraler Bestandteil zur Generierung eines korrekten COP (Common Operational Picture) für die Einsatzführung.

Das Kompetenzzentrum für GNSS (Global Navigation Satellite System) im ÖBH setzt als Teil der nationalen GALILEO PRS Behörde die Rahmenbedingungen zur Nutzung von GALILEO PRS in ÖSTERREICH um und stellt Experten im Bereich PNT-Services auf nationaler und internationaler Ebene. Die Inanspruchnahme von Galileo PRS-Diensten durch österreichische Behörden bzw. durch Betreiber kritischer Infrastruktur stellt die staatliche Handlungsfähigkeit durch die systemimmanente Sicherheit der GALILEO PRS-Technologie sicher. Von 13. bis 17. September 2021 führte das Referat Navigation & GALILEO am Truppenübungsplatz Seetaler Alpe (TÜPl S) eine Testreihe im Zuge von Projekten zu Navigation Warfare mit den Forschungspartnern des IMG, Miliz-Experten sowie einer Delegation aus unterschiedlichen nationalen und internationalen zivilen und militärischen Forschungspartnern durch.

Das Schwergewicht des Übungsvorhanbens seitens des Referat Navigation&GALILEO war in Anwesenheit bzw. Kooperation mit der Deutschen Bundeswehr, NATO-NCIA (NATO Communications and Information Agency), EUSPA (European Union Agency for the Space Program), Fraunhofer Institut und Diehl Defence hochkomplexe Versuchsreihen zu GNSS Jamming/Spoofing durchzuführen.

Aufgrund der kontinuierlichen Adaptierung des TÜPl S zu einem Navigation Warfare (NavWar) TÜPl hatten unsere nationalen und internationalen Partner ebenso die Möglichkeit, auf dem weiträumigen Gelände eigenständige Testungen durchzuführen, was den Wissenstransfer zum ÖBH und ins Referat zusätzlich unterstützt. Die praktischen Erprobungen von PNT-Spoofing- und -Jamming-Angriffen wurden unter Einhaltung aller Sicherheitsbestimmungen in den Übungsräumen am Sportplatz TÜPl Seetaler Alpe durchgeführt. Zusammenfassend kann gesagt werden, dass durch die unter der Federführung des Referats Navigation&GALILEO zweimal jährlich stattfindenden

Testreihen am TÜPl S unverzichtbare Ergebnisse im Bereich der Grundlagenforschung liefert, damit die Fähigkeit Navigation Warfare im ÖBH durch gesicherte PNT-Services einen entscheidenden Beitrag zum Schutz der Soldaten, Waffeneinsatzsysteme, Plattformen und von Infrastrukturen leisten kann.

RUANDA: Unterwegs mit der TU und dem Roten Kreuz

Mit dem ASAP Projekt „UniNav" wird die Disziplin der Geodäsie mit der Materie Navigation – speziell der Satellitennavigation mittels GNSS (Global Navigation Satellite System)–verknüpft. Es wird anhand von automatisierter Klassifizierung von Landbedeckung und Gelände sowie einer persönlichen Bewertung eine Kostenmatrix für ein gewünschtes Gebiet erzeugt. Im Gegensatz zu herkömmlichen Navigationslösungen, die rein aufgrund des gelernten Straßennetzes Routen von A über B nach C vorschlagen, ist es mit der im Projekt anvisierten Lösung möglich auch im Gelände zu navigieren.

Hierzu werden zunächst für den Endanwender geeignete Profile erstellt. Diese können z.B. „sportlicher Fußgänger", „stark geländegängiges Kfz" oder „LKW" sein. Das Ziel dieser unterschiedlichen Profile ist, dass das Terrain unterschiedlich genutzt werden kann. Ein Endanwender kann ein passendes Profil wählen und die Navigationslösung schlägt eine hierfür passende Route vor. Hierzu muss jedoch zuvor das Gelände – genauer die konkrete Oberfläche sowie die konkrete Steigung und Festigkeit des Untergrunds – für das jeweilige Profil bewertet werden.

Ein typischer Anwendungsfall wäre ein Hochwasser-Katastrophen-Einsatz. Helfer können, sollte beispielsweise ein Straßenabschnitt überschwemmt sein, eine alternative Route unter Ausnutzung des Geländes automatisiert finden und so das Hindernis umfahren bzw. umgehen. Um diese Anwendungen zu verfeinern, wurde ebenso ein „Obstacle Layer" implementiert. Dies ist für dynamische Zusatzinformationen gedacht, um z.B. ein Vogelschutzgebiet, dass nicht befahren werden darf, in die Navigationslösung mit einfließen lassen zu können.

Der gedachte Regelkreis ist, dass ein ortskundiger Experte die „Area of Interest" trainiert, ein Einsatzleiter gewünschte Profile erstellt und das Gelände entsprechend bewertet und die Einsatzkraft vor Ort mit den aktuellsten Daten eine Applikation – z.B. am Smartphone – zur Navigation im Einsatzgebiet nutzt. Für dieses Projekt hat sich ein Konsortium, bestehend aus der TU Graz, dem Roten Kreuz Österreich, dem Disaster Competence Network Austria, der Fa. Pentamap und dem BMLV gebildet.

Da das Rote Kreuz eng mit deren Schwesterorganisation in Ruanda zusammenarbeitet, wurde Ruanda als Gebiet zur Verifikation der Lösung gewählt. Somit konnte auch praktisch erprobt werden, wie weit Fernerkundung ohne entspreche Ortskenntnis funktioniert. Die Ergebnisse waren teilweise überraschend gut, im Detail jedoch sind für die angedachte Anwendung kleinere Details zu bedenken. So ist beispielsweise ein tiefes Rinsal am Straßenrand bergeseitig, welches zwar eine Überflutung der Straße mindert, jedoch für handelsübliche PKW nicht zu überwinden. Ein Detail, das mittels Fernerkundung nicht erkannt wird. Ebenso reagieren die teilweise steilen Waldwege stark auf Regen, wie bei der Vorort-Erkundung schmerzhaft erkannt werden musste.

Derartige Details müssen von ortskundigen Quellen, die darüber hinaus den, an das Expertensystem gestellten Informationsgehalt verstehen, geliefert werden. Ebenso konnte im Zuge der Besprechungen zu Einsatzzwecken klar erkannt werden, dass der „Obstacle Layer" per Hand und unabhängig von weiteren Geländebeurteilungen eingezogen werden muss.

Zu Ende des Projekts werden die Projektpartner mit einem brauchbaren Demonstrator erste praktische Erkenntnisse gewinnen können und das Konsortium ist einstimmig der Meinung, in einem Folgeprojekt auf weitere entscheidende Aspekte im Bereich Erdbeobachtung und GNSS eingehen zu können, den nötigen Regelkreislauf für die Verwendung im Einsatz zu perfektionieren und danach einen generellen „Proof-of-Concept" zu erhalten, um danach in entsprechen Entwicklungsprojekten durch die Fa. Pentamap eine maßgeschneiderte Lösung für „Off Road Navigation" zu erhalten.

Bundesministerium für Landesverteidigung

Zahlen und Daten

Bundesministerium für Landesverteidigung

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
- 2021 wurden ca. 27.500 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 IKT&CySihZ

- Besetzungsgrad: 75,4%
- Personalverfahren: ca. 2.600
- Altersstruktur: 18J - 30J = 35% | 30J - 50J = 45% | > 50J = 20%
- Frauenanteil: 13%
- ca. 90 neue Cyberrekruten im Jahr
  Kontinuierlich ca. 30 Cyberrekruten im Einsatz

Logistik

- Materialbewegegungen auf VersNr Ebene: 3,4 Mio.

Bundesministerium für Landesverteidigung

Stichwortverzeichnis

Bundesministerium für Landesverteidigung

Dieses 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.

1-9

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

A

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

B

Backbone	Rückgrat (Hauptleitungen) von Netzwerken
Backnang	Ort in Deutschland
BACnet	Building, Automation and Control Networks (Netzwerkprotokoll für Gebäudeautomation
BACtwin	Building, Automation and Control Twin (Digitaler Zwilling)
BandlibrarySystem	Bandbibliothek zur Datenspeicherung auf Magnetbändern
BatchFenster	Konsolenfenster des Betriebssystems
BBG	Bundesbeschaffungsgesellschaft
BenBe	Benutzer-Betreuung
Big Data	Große komplexe Datenmengen
bilateral	Zwei Seiten, Parteien betreffend
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
Davos	Ort in der Schweiz
DBMS	Datenbank Management System
DDoS	Distributed Denial of Service
DGIWG	Defence Geospatial Information Working Group
DGMN	Dynamisches gesichertes Militärnetz
DhFMO	Diensthabender Fernmeldeoffizier
DhSys	Diensthabendes System
Dienstenetz	Logische Segmentierung des Trägernetzes (Leitung, Router) Netzwerkverkehr wird für unterschiedliche Kunden über ein und dieselbe Netzinfrastruktur logisch von einander getrennt und geroutet. Für jeden Kunden wird das Netz spezifisch abgesichert und verschlüsselt. Es werden somit mehrere Kundenentze zur Verfügung gestellt.
Digitaler Zwilling	Digitale Repräsentanz eines materiellen oder immateriellen Objekts/Prozesses aus der realen Welt in der digitalen Welt
Digitalisierung	Umwandlung von analogen Werten in informationstechnisch verarbeitbare Daten
dpi	Dots per inch (Drucktechnische Auflösung)
DSB	Datenschutzbeauftragter

E

E-Mail	Electronic Mail (Digitale Post)
early life support	Lösung von operativen Problemen während der Anlaufphase
EDA	European Defence Agency
EDRS	Endpoint Detection Response System
EFA	Europäisches Forum Alpbach
Ego-Perspektive	Ansicht, als wäre man die jeweilige Person
Einsatz	Tätigwerden des ÖBH zur Erfüllung seiner verfassungsgesetzlich verankerten Aufgaben lt. §2 Abs.1 Wehrgesetz
ELAK	Elektronischer Akt (unterscheide BMLV-ELAK und ELAK im Bund)
EloKa	Elektronische Kampfführung
EloKa-Truppe	Elektronische Kampfführungs-Truppe
Emotet	Computer Schadsoftware
EOW	EU Operations WAN (Europaweites gesichertes Netzwerk)
ePAT	Elektronisches Patienten Informations System
EPR	Eignungsprüfung
ERGIS	Ergänzungsinformationssystem
ESS	Employee Self Service
ETB	Elektronisches Telefonbuch
Ethernet	Kommunikationsstandard für Software und Hardware in einem kabelgebundenen Netzwerk
EU Battle Groups	European Union Battle Groups
EUBG	European Union Battle Groups 2020
EUCH	European Challenge 2020 (Cyber-Übung)
Eurofighter Typhoon	Abfangjäger des österreichischen Bundesheeres
EUTM	European Training Mission
Explore AI	Forschungsprojekt über den Einfluss von künstlicher Intelligenz auf das Militärwesen im österreichischen Kontext
Extranet	Erweiterung des Intranets, welches nur für eine festgelegte Gruppe an Nutzern zugänglich ist

F

Fauna	Tierwelt
FEG	Forterhaltungsgebühr
Fertigungsklausel	Festlegung von Unterschriftsberechtigungen und Formulierungen
FFT Proxy	Friendly Force Tracking Proxy
FGP	Abteilung für Fahrzeuge, Geräte und persönliche Ausrüstung
Fibre	Glasfaser

Firewall	Netzwerksicherheitskomponente
First-Line-of-Defence	Erste Verteidigungslinie
FM-Planung	Fernmelde-Planung
FMN	Federated Mission Networking
FMSysÖBH	Fernmeldesystem ÖBH
FNMS	Funknetzmanagementsystem (Software)
Force Provider	IKT-Fähigkeiten des ÖBH, die Bedarfsträgern nicht zur Verfügung stehen, sind zentral beim IKT&CySihZ bereitzuhalten
FORTE	Österreichisches Verteidigungsforschungsprogramm
FORTE CADSP	Forschungsprojekt Cyber Attack Decision and Support Platform
FOSSGIS	Free & Open Source Software for GeoInformationSystems
Frq&SchlW	Frequenz- und Schlüsselwesen
Führungsmittel	Systeme, Geräte und technische Verfahren mit denen die zur Führung erforderlichen 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/FIFIATS	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 (Echtzeit-analyse 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“

Telefon	Kommunikationsmittel zur Übermittelung von Tönen und speziell Sprache mittels elektrischer Signale
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

Abbildungsverzeichnis

Bundesministerium für Landesverteidigung

Abbildungsverzeichnis

Abbildungsverzeichnis

IMPRESSUM:

Amtliche Publikation der Republik Österreich
Bundesministerin für Landesverteidigung
Medieninhaber, Herausgeber und Hersteller:
Republik Österreich, Bundesministerin
für Landesverteidigung BMLV,
Roßauer Lände 1, 1090 Wien

Inhalt und Redaktion: IKT&CySihZ
Idee, Konzeption und Gestaltung: Roland Pachler
Layout: Michael Kriehebauer, Nicolas Stocker, Roland Pachler
Satz: Michael Kriehebauer
Fotos: Bundesheer, IKT&CySihZ, soweit nicht ausdrücklich anders
gekennzeichnet
Druck: ReproZ Wien, 1070 Wien

Bundesministerium für Landesverteidigung