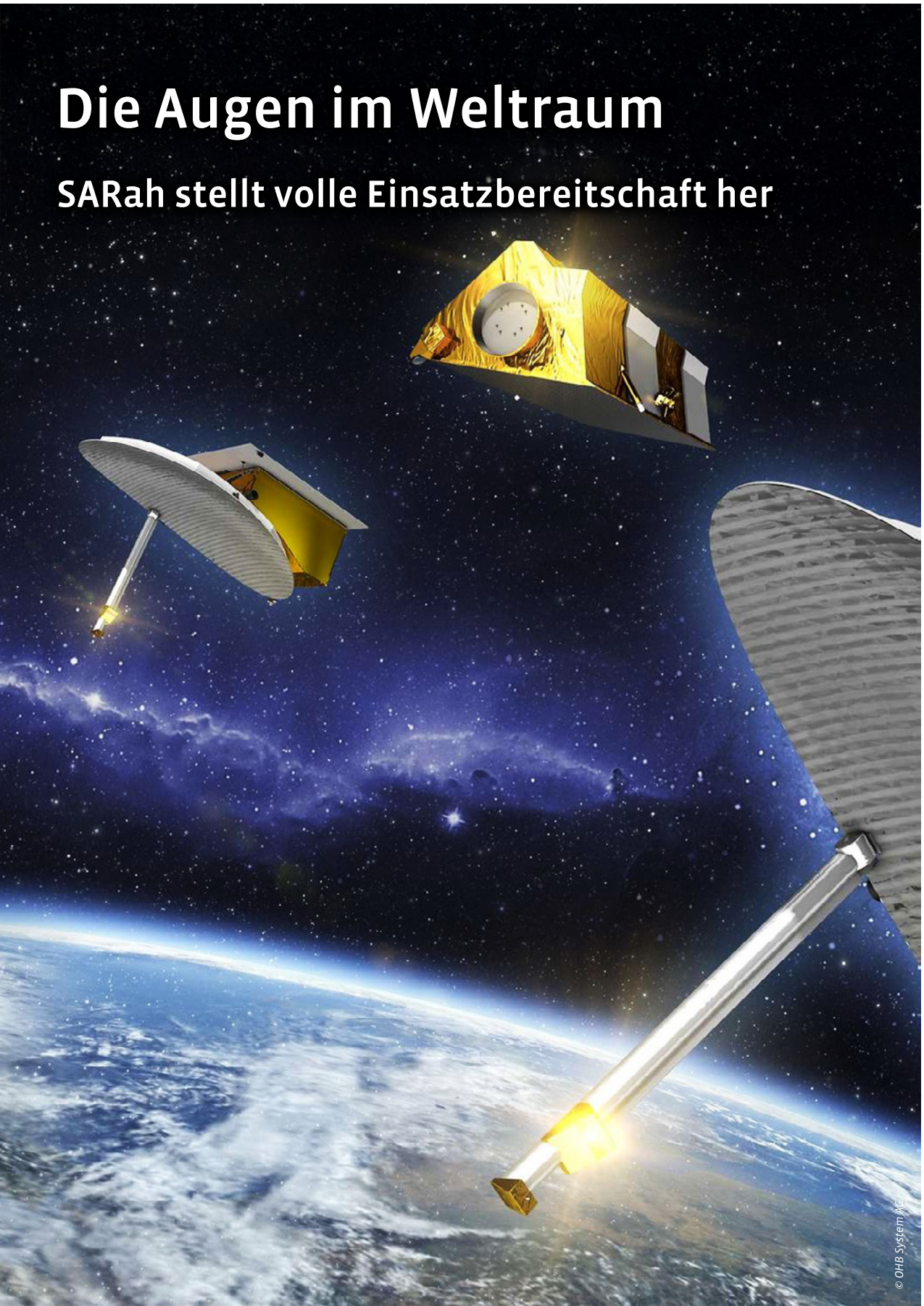
NEWSLETTER VERTEIDIGUNG

12. MAI 2026 I ISSN 2194-0088 I 19. JAHRGANG

AUSGABE 18

Die Augen im Weltraum

SARah stellt volle Einsatzbereitschaft her



© OHB System AG

Europas bröckelnde Sicherheit – Ergebnis schlechter Vorsorge?

Von Manfred Opel

Wo wir stehen

Offensichtlich hat Donald Trump, betrachtet man die Summe seiner öffentlichen Äußerungen, keinerlei bedeutendes historisches, geografisches oder auch politisches Wissen. Hinzu kommt, dass er sich mit seiner verarmten New Yorker Hinterhofsprache zu kaum einem einzigen politischen Thema differenziert auszudrücken versteht. Das erzeugt vermeidbare und ernste Risiken; nicht nur für die USA.

Trump will für sich selbst und wohl auch für die USA vorteilhafte „Deals“ (= geldwerte Geschäfte) machen; und zwar auch dort, wo es im politischen Bereich gar keine solchen Geschäfte zu machen gibt. Politik hat mit Werten, Verantwortung und Konfliktlösung, mit der Bewahrung des Friedens, mit allgemeinem Wohlstand sowie der Gesundheit zu tun und nichts mit exklusiven Vorteilen für bestimmte Gruppen und Möchtegern-Herrscher aller Art.

Er schwafelt praktisch immer nur oberflächliches Zeug daher, nahezu ohne jede fachliche oder historische Substanz. Wenn er zum Beispiel über die Einsätze der US-Streitkräfte berichtet, wird sofort klar, dass er weder von „seinem“ Militär, noch von militärischer Strategie auch nur den Hauch einer Ahnung hat. Und dennoch können sich heute weder das US-Militär noch die Chefs verbündeter Regierungen wirksam dagegen wehren. Sie müssen Aufmerksamkeit und sogar „Verehrung“ heucheln, weil der lob-süchtige „goldene Donald“ jederzeit sehr giftig werden kann, wenn er zu bemerken glaubt, dass ihn jemand nicht ernst nimmt. Das erlebte zum Beispiel der Kanadische Premier Mark Carney, den Trump auf internationaler Bühne lautstark abkanzelte, ohne je mit ihm persönlich über die dabei vorgebrachten Probleme ernsthaft gesprochen zu haben.

Sein simpler und mit sog. „Trumpismen“ aufgeladener Sprachstil ist unterdessen zu seinem Markenzeichen geworden. Wissenschaftliche Analysen, etwa solche der Universität Zürich, zeigen, dass sein Vokabular, im Vergleich zu dem anderer US-Präsidenten, deutlich schlichter ist. Donald Trump gibt sich zwar überlegen, doch intellektuelle Substanz besitzt er nicht.

Zu seiner aufgeblähten „Überflutungs-Rhetorik“ zählen insbesondere die Worte „great“ (großartig; er benutzt dieses Wort wohl am häufigsten), „deal“ (Übereinkunft), „tremendous“ (riesig), „incredible“ (unglaublich), „beautiful“ (wunderbar) oder „huge“ (gewaltig). Doch auch die Worte „nasty“ (gemein; Standardwort, um Kritiker, Journalisten oder politische Gegner abzuwerten), „strong“ (stark), „fake news“ (absichtliche Falsch-Nachricht), „woke“ (übertrieben; nur scheinbar politisch korrekt) oder „tariffs“ (Zölle) benutzt er sehr oft und wohl, um sich damit das Image des politisch „harten Hundes“ zu geben. Doch häufig ordnet er sogar diese wenigen Begriffe inhaltlich falsch zu.

Die meisten der von bestimmten Politikern häufig benutzten Begriffe und Bezeichnungen sollen, vor allem als Instrumente ihrer „Öffentlichen Politik“, dazu dienen, ihnen politische Ansehens- und Meinungs-Vorteile zu verschaffen. Sie sollen Wirkungen erzielen. Dabei kommt es nicht darauf an, was ein Politiker sagt, sondern auf das, was die Adressaten darunter verstehen und insbesondere, was sie in der Folge für wahr halten. Deshalb ist die „Sprache“ für Donald Trump ein willkommenes Identifizierungs-Instrument, das er jedoch nicht überzeugend und ausgewogen zu nutzen versteht. Allerdings kommt ihm dabei entgegen, dass nahezu die ganze „gebildete Welt“ die englische Sprache benutzt. Und durch die moderne Datentechnik nimmt dieser Trend in der Zukunft sogar noch kräftig zu. Das hilft ihm, auf die verschiedenste Art und Weise direkt mit den „politischen Menschen“ dieser Welt zu kommunizieren.

Der Zwang zur Kopie

Putin andererseits, Trumps historischer Gegenspieler, ist wohl einer der weltweit besten Polit-Profis, was die Kunst der Verdrehungen und falschen Behauptungen angeht. Doch die Wirkung seiner politischen Aktivitäten hat insbesondere in letzter Zeit deutlich gelitten. Das hat verschiedene Gründe.

Ein Sprichwort erinnert daran, dass die Lüge zur schärfsten Waffe gegen das Vertrauen werden kann. Getreu dem volkstümlichen Ausspruch „Wer einmal lügt, dem glaubt man nicht, auch wenn er dann die Wahrheit spricht“, wird dem einmal überführten Lügner, auch bei allen zukünftigen, ehrlichen Aussagen misstraut. Genau in dieser Situation befindet sich Wladimir Putin heute.

Die gesamte Welt befindet sich schon seit Jahrzehnten in einem gewaltigen Umbruch. Die Supermächte USA und Russland, aber auch China, haben heute ihr Grund-Versprechen, nämlich, den globalen Frieden zu bewahren und zu fördern, nicht erfüllt. Sie sind sogar zu aktiven Kriegs-Parteien mutiert. Damit ist die alte Weltordnung, wonach vor allem die ständigen Mitglieder des Sicherheitsrats der Vereinten Nationen in besonders verantwortungsvoller Art und Weise dem Weltfrieden verpflichtet sind, wohl für immer dahin.

Das bedeutet: Die Welt steht heute einerseits vor gänzlich neuen und komplexeren Aufgaben als noch zur Mitte des vergangenen Jahrhunderts. Andererseits hat es sich gezeigt, dass die sog. Friedensbewegung, die glaubte, man könne „Frieden schaffen ohne Waffen“, auf der ganzen Linie gescheitert ist.

Dieses war ein extrem teurer Ausflug in die Welt der Träume, der von Putin und anderen immer schon befeuert wurde, aber im Grunde nur eine freiwillige Selbst-Entwaffnung der jeweiligen potenziellen Gegner Russlands zum Ziel hatte.

Obwohl der US-Präsident nicht den blassesten Schimmer gehabt haben dürfte, was dieser Soldat tut, kann als sicher gelten, dass er ihm einen „incredible job“ attestierte.

© whitehouse.gov

Das eigentliche Ziel Putins war es schon zu seiner Zeit als russischer Geheimdienstler in der DDR, den russischen Machtbereich nach Westen, sogar bis zum Atlantik, zu verschieben. Nur dadurch, so ist er noch heute überzeugt, kann Russland seinen Supermacht-Status für immer und ungefährdet implementieren sowie absichern. Putin denkt auch im Nuklearzeitalter wie die Herrscher in der „konventionellen Vergangenheit". Eine Änderung ist bei ihm auf diesem Feld nicht in Sicht. Dabei ist wesentlich, dass er die zahlreichen unseligen Kriege, welche die heutigen Instabilitäten im eurasischen Raum verursachten, höchstpersönlich und in ihrem Kern beeinflusst hat. Putin kann sich hierbei auch nicht herausreden – die historischen Fakten sprechen klar und deutlich gegen ihn.

Kalaschnikow überall

Wladimir Putin war von 31. Dezember 1999 bis zum 7. Mai 2008 (zunächst kommissarisch) Präsident der Russischen Föderation. Zuvor, in den Jahren 1975 bis 1990, war er Mitarbeiter des KGB, des berüchtigten und gnadenlosen russischen Geheimdienstes. Zwischen Mai 2008 und 2012 war Putin formal Ministerpräsident Russlands. Seit dem 7. Mai 2012 (wiedergewählt 2018 und 2024) ist Putin erneut Präsident der Russischen Föderation. Seine fünfte Amtszeit als Präsident Russlands begann im Mai 2024. Seither hat sich Einiges verändert:
Er ist heute mit geradezu diktatorischen Vollmachten ausgestattet.

Doch unterdessen scheinen Alter und gesundheitliche Probleme auch bei ihm zunehmend zu immer deutlicheren Einschränkungen zu führen. Da Putin keiner ist, der delegiert oder die Macht der Führung freiwillig aus der Hand gibt, wird er sich derzeit wohl immer öfter mit dem Problem beschäftigen, wie er das, was er als „sein Erbe" ansieht, in zuverlässige Hände legen kann. Der „große Stalin", der am Ende des Zweiten Weltkrieges sogar die russischen Breitspurschienen eilends bis Berlin verlegen ließ – nur, um mit seinem geliebten Zug bequem und ungefährdet zur Potsdamer Konferenz fahren zu können –, würde sich über die Unentschlossenheit und die vielen Misserfolge Putins heute wohl mehr ärgern als wundern.

Aus Putins extrem langer Regierungszeit sind viele Ereignisse und Geschichten bekannt, die er, zuweilen sogar wiederholt, selbst erzählte und die ganz offenbar seinen Ruhm als „treuer Diener des russischen Vaterlandes" mehren sollten. Wir sind heute durch die rasante internationale politische Entwicklung in den vergangenen nahezu 40 Jahre etwas klüger geworden.
… aber eben nur etwas.

© kremlin.ru

Während sich in Moskau die Stimmung kontinuierlich verschlechtert, versichert sich der Kreml-Chef der Loyalität z.B. des belarussischen Diktators von Putins Gnaden, Alexander Lukaschenko.

Man muss derzeit ganz nüchtern festhalten: Die ganze, weitgehend von Moskau politisch gesteuerte sog. Friedensbewegung, die besonders in den frühen 1980er Jahren aktiv war, ist unterdessen klar als Propaganda-Offensive Moskaus zu erkennen. Putin war damals einer der „Erfinder" dieser Bewegung, die zum Ziel hatte, das gesamte westliche Europa von Atomwaffen frei zu halten und dessen militärische Stärke strukturell massiv abzubauen.

Das ist, wie man heute klar erkennen kann, Moskau bisher auch weitgehend gelungen. Ironischerweise brachte erst der Ukraine-Krieg in dieser Hinsicht die Wende, weil nunmehr die meisten Menschen begriffen haben, dass Putin alle seine friedlichen Aussagen nur dazu benutzt, um bei seinen zukünftigen Gegnern Abrüstung und militärische sowie politische Schwäche zu fördern.

Die Folgen sind im freiheitlichen Europa heute einerseits die hektischen und extrem teuren Bemühungen, das bestehende defensive Defizit gegenüber Russland wenigstens mittelfristig wieder einigermaßen ausgleichen zu können und andererseits die Notwendigkeit, auch die strategische nukleare Verteidigung Europas selbst organisieren und implementieren zu können.

Das wird ein sehr weiter und steiniger Weg werden. Denn Donald Trump hat in der ihm eigenen Offenheit entschieden angekündigt, er werde Europa nicht mit amerikanischen Nuklearwaffen schützen, weil das eine essenzielle nukleare Gefahr für die USA bedeuten würde.

In diesem Zusammenhang drängt sich einmal mehr die Frage auf, weshalb die Bundeswehr ausgerechnet die relativ leichte einmotorige amerikanische F-35 als Trägerflugzeug für die US-Nuklearwaffen beschaffen will, die zudem eine relativ geringe Reichweite hat. Nach dem Starfighter-Desaster schwor die Bundeswehr alle heiligen Eide, niemals mehr ein einmotoriges Kampfflugzeug zu beschaffen. Wo sollten denn die Ziele dieser Flugzeuge überhaupt liegen, wenn die Nuklear-Einsätze vom Fliegerhorst Büchel in der Eifel aus erfolgen sollen? Und wohin sollen diese Flugzeuge nach ihrem Nuklear-Einsatz zurückkehren – den ganzen Weg zurück nach Büchel? [Als Kasten ausführen]

Bei öffentlichen Auftritten – hier vor den Streitkräften in Fort Bragg – feiert Donald Trump sich ausgelassen selbst und schwärmt von sich in den höchsten Tönen, obwohl es für „seine" USA alles andere als gut läuft.

© whitehouse.gov

Der große Selbstbetrug

Doch für diese Wahrheit muss man Trump sogar sehr dankbar sein, denn das ist der große Selbstbetrug der NATO: Man hat bisher immer behauptet, die USA würden die Europäer auch nuklear schützen. Das aber kann allein deshalb nicht der Realität entsprechen, weil die USA niemals eine substanzielle nukleare Eigengefährdung eingehen würden, nur um den Versuch zu unternehmen, einen oder einige europäische Staaten mittels des Einsatzes von amerikanischen Nuklearwaffen zu schützen.

Trump hat das zwar bisher noch nicht mit letzter Klarheit so formuliert. Doch aus allen seinen offiziellen Äußerungen zu den grundsätzlichen Problemen des Nuklear-Einsatzes sowie aus der kürzlich neu formulierten US-Nuklearstrategie muss man ohne jeden Zweifel folgern, dass Trump nichts, rein gar nichts, militärisch tun wird, was das nukleare Risiko für die USA erhöhen könnte.

Doch einen gravierenden Schönheitsfehler hat diese Absicht des Donald Trump dennoch: Exakt zu dem Zeitpunkt, an dem Trump nicht mehr in der Lage sein wird, (z.B. auch mit Hilfe der Europäer) die beiden anderen nuklearen Supermächte zeitgleich militärisch erfolgreich – auch nuklear – bekämpfen zu können, wird insbesondere sein „goldenes“ Amerika selbst im Kern nuklear gefährdet sein.

Genau dann braucht er einen treuen und starken Gefährten. Und das können logischerweise nur die Europäer sein. Trump wäre sehr gut beraten, dieses entscheidende Faktum niemals zu vergessen.

Die langfristige politische Lage ist folglich für die USA wesentlich problematischer als für Europa. Russland und auch China brauchen Europa extrem dringend. Die USA ist dabei nur ein störender Konkurrent. Die Frage ist also, ob sich die militärische und vor allem die politische Führungs-Riege der USA über diesen grundlegenden Zusammenhang klar ist.

Verfolgt Trump weiter seine egozentrische Politik der Deals und des sinnlosen Zerbombens, wird er damit zwangsweise nur die Gegnerschaft – auch der Europäer gegenüber den USA – stärken, die ihm seinen „Verrat gegenüber der Ukraine“ und die indirekte Verantwortung für die Kostenexplosion bei allen Energieträgern ohnehin schwerlich verzeihen werden.

Dabei darf man niemals vergessen, dass die öffentlichen Beschimpfungen des derzeitigen Papstes durch Donald Trump letzterem wohl mit hoher Wahrscheinlichkeit die ewige Verdammnis bescheren wird.

Über den Autor: Brigadegeneral a.D., Dipl.-Ing. Manfred Opel, M.A., ehemalig MdB, war u.a. Referatsleiter für Strategische Planung im Internationalen Militärstab des NATO-Hauptquartiers in Brüssel sowie General für Luftwaffenangelegenheiten der Rüstung. Der Beitrag gibt seine persönlichen Einschätzungen und Ansichten wieder.

Bildauswahl und -beschriftung: Daniel Kromberg

Aufklärungssatelliten

SARah – ein enormer Gewinn für die Aufklärung

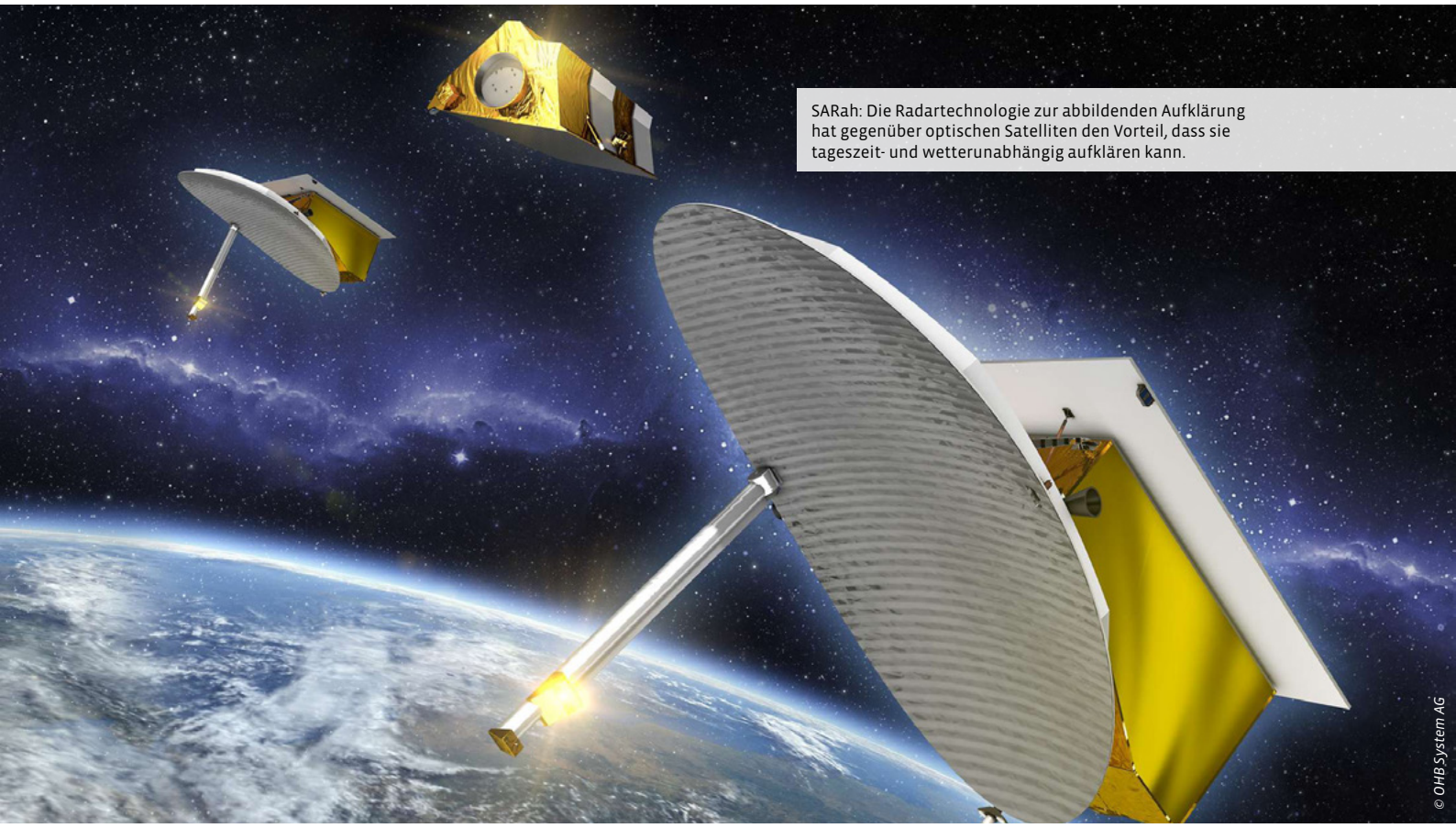
Satelliten spielen eine große Rolle für Deutschlands Sicherheit. Die Aufklärungssatelliten der Bundeswehr liefern als „Augen im Weltraum“ Bilder von der Erde – auch dann, wenn es draußen dunkel ist oder dichte Wolken den Himmel bedecken. Genau hier setzt das Aufklärungssystem SARah an, das nach und nach das ältere System SAR-Lupe ablöst.

Was bedeutet „SAR“?

SARah ist ein bildgebendes Radarsatellitensystem, das weltweit hochaufgelöste Bilddaten gewinnt. „SAR“ steht für Synthetic Aperture Radar (Radar mit synthetischer Apertur oder Öffnungsweite). Anders als bei einem optischen System benötigt diese Aufnahmetechnologie keine Lichtquelle wie die Sonne. Es sendet Radioimpulse aus, empfängt die Echos von der Erdoberfläche und berechnet daraus ein sogenanntes SAR-Bild. Der große Vorteil: Wolken, Rauch oder Dunkelheit über dem Zielgebiet spielen keine Rolle. Wo optische Satelliten nur bei wolkenfreiem Himmel und Tageslicht zuverlässige Bilder liefern, kann ein SAR-Satellit unabhängig von der Tageszeit und bei nahezu jeder Wetterlage über einem Interessensgebiet Bildinformationen gewinnen.

Die neue Generation: Was SARah besonders macht

Das System SARah besteht aus insgesamt drei Satelliten. Einer davon nutzt ein modernes Phased-Array-Radar. Vereinfacht gesagt handelt es sich um eine große, elektronische Antenne, deren Strahl sich in unterschiedliche Richtungen „ausrichten“ lässt, ganz ohne mechanische Drehbewegung. Dadurch kann der Satellit schnell von einem Zielgebiet zum nächsten wechseln. Die beiden anderen Satelliten verwenden eine Reflektortechnik, die auf den Erfahrungen mit dem bislang durch die Bundeswehr genutzten Satellitensystem SAR-Lupe aufbaut, aber leistungsfähiger geworden ist. Ergänzt werden die Satelliten durch weltweit verteilte Bodenstationen, die die Datenanbindung zu den Satelliten sicherstellen, sowie durch Rechenzentrenkapazitäten in Deutschland, in denen die Daten zu Bildern prozessiert, gespeichert und für die Auswertung aufbereitet werden.



SARah: Die Radartechnologie zur abbildenden Aufklärung hat gegenüber optischen Satelliten den Vorteil, dass sie tageszeit- und wetterunabhängig aufklären kann.

„Objekte am Boden können durch die Ablösung von SAR-Lupe durch SARah noch besser verifiziert und identifiziert werden. Darüber hinaus sind Bildinformationen deutlich schneller verfügbar. Damit besitzen wir ein hochmodernes System, das die Fähigkeit der ‚Weltweiten Abbildenden Aufklärung' in der SAR-Line weiter sicherstellt. Gleichzeitig wird die Führungsrolle Deutschlands in der SAR-Technologie im internationalen Vergleich weiter ausgebaut", erklärt Oberstleutnant F., der für das Projekt „Radarsatellitensystem zur Weltweiten Abbildenden Aufklärung SARah" verantwortlich ist.

Wofür nutzt die Bundeswehr SARah?

Ein Beispiel sind Krisenregionen, in denen sich die Lage schnell ändern kann. Satellitenaufnahmen helfen, Truppenbewegungen, neue Stellungen, Flugplätze oder Hafenanlagen im Blick zu behalten. Auch für eigene Einsätze im Ausland sind solche Informationen wichtig: Sie unterstützen die Planung von Marschrouten, die Beurteilung von Gefahren und die Absicherung von Standorten. Darüber hinaus können die Daten in bestimmten Situationen auch zivilen Zwecken dienen, etwa beim Überblick über Überschwemmungsgebiete oder großflächige Schäden nach Naturkatastrophen.

Aus Zahlen werden Bilder

Die Satelliten senden ihre Aufklärungsergebnisse über Bodenstationen an die in Deutschland verorteten Rechenzentren. Diese Rohdaten werden anschließend vor Ort aufbereitet. Aus reinen Zahlenkolonnen entstehen mittels systemeigener SAR-Prozessoren Rohbilder. Diese können durch Bundeswehrpersonal ausgewertet werden. Die Erkenntnisse fließen beispielsweise in das Lagebild „Militärisches Nachrichtenwesen" ein und werden durch weitere Aufklärungsergebnisse ergänzt. Das ist wichtig, denn das militärische Ziel, Wirkung zu entfalten und Informationsüberlegenheit zu gewinnen, ist nur mit Hilfe eines vollständigen und ständig aktuellen Lagebildes möglich. Die Nutzung des Weltraums für die Domänen Aufklärung und Führung ist somit eine wesentliche Voraussetzung für den gezielten Einsatz moderner Streitkräfte.

> ***„Nachdem bereits seit Ende 2023 der erste von insgesamt drei SARah-Satelliten höchst zuverlässig seinen Dienst versieht und hervorragende Ergebnisse liefert, wird das System SARah Ende 2026 durch die beiden weiteren SARah-Satelliten seine volle Leistungsfähigkeit entfalten."***
>
> *Generalmajor Armin Fleischmann, Beauftragter für den Weltraum der Teilstreitkraft CIR*

© Bundeswehr/Stefan Uj

Am Boden werden die Daten verarbeitet und ausgewertet.

© Bundeswehr/Kevin Schrief

Mehr Unabhängigkeit – und große Verantwortung

Mit SARah steigt die Unabhängigkeit Deutschlands in der strategischen Aufklärung. Zwar bleibt die Bundeswehr in der Praxis eng mit Partnern vernetzt, etwa in der NATO. Eigene, verlässliche Informationsquellen sind aber gerade in einer unberechenbaren Sicherheitslage umso wichtiger. Sie ermöglichen es der Bundesregierung, sich ein Bild von militärischen Entwicklungen in der Welt zu machen – im wahrsten Sinne des Wortes. Das Projekt SARah zeigt, wie sehr sich Weltraum und Sicherheitspolitik inzwischen durchdringen. Informationen, Geschwindigkeit und Verlässlichkeit sind heute mindestens so wichtig wie Panzer und Flugzeuge. Zum Alltag gehört heute, dass deutsche Soldatinnen und Soldaten sowie politische Entscheidungsträger sich auf Daten aus dem All verlassen können. Die „Augen im All" werden Deutschland dabei helfen, in dieser Welt den Überblick zu behalten.

Die Bundeswehr im Weltraum: Status quo und Ausblick

Die drei SARah-Satelliten ergänzen beziehungsweise ersetzen perspektivisch das Aufklärungssystem SAR-Lupe, das seit 2007 seinen Dienst im Weltall verrichtet. Genau wie bei SAR-Lupe sollen auch die drei SARah-Satelliten für mindestens zehn Jahre den operativen Betrieb sicherstellen.

02.08.2012	Startpunkt für die Beschaffung des Systems SARah war die Zeichnung der „Abschließenden funktionalen Forderung/Realisierungsgenehmigung" durch den damaligen Generalinspekteur der Bundeswehr.
18.06.2022	Der erste von insgesamt drei Satelliten aus dem SARah-Satelliten-Programm wurde von der Vandenberg Space Force Base in Kalifornien/USA ins Weltall befördert.
24.12.2023	Die letzten beiden von insgesamt drei SARah-Satelliten sind von der Vandenberg Space Force Base in Kalifornien/USA ins All gestartet. Diese beiden Reflektor-Satelliten vervollständigen das Aufklärungssystem SARah.
4. Quartal 2026	Volle Einsatzfähigkeit der SARah-Satelliten

Text: Martina Pump

Software Defined Defence – Softwareupdates als Teil der Gefechtsführung

Von Marc Simon

Softwareupdates können mittlerweile nicht nur bei PCs oder Fahrzeugen für neue Features und verbesserte Leistungsfähigkeit sorgen. Auch im militärischen Kontext werden sie immer mehr zum entscheidenden Faktor. Wer in der Lage ist, seine Systeme schneller auf neue Herausforderungen einzustellen als der Gegner, ist im Vorteil.

Egal ob im privaten Alltag, oder im Job – überall machen IT-Systeme die Prozesse schneller und sorgen für neue Funktionen. Auch im militärischen Umfeld kann kaum noch ein Waffensystem auf IT-Unterstützung verzichten. Es geht um Vernetzung, Erhebung und Auswertung von Daten und vieles mehr. Hier spricht man von Software Defined Defence (SDD), also einer Verteidigungsfähigkeit, die maßgeblich durch Software bestimmt wird.

Im Ukrainekrieg wird aktuell deutlich, wie gravierend die Auswirkungen dieser Entwicklung sind und in welchem Maß das Tempo der Softwareupdates sich direkt auf die Kampfkraft der eingesetzten Einheiten auswirkt. Am Beispiel der dort eingesetzten Drohnen lässt sich nachvollziehen, wie die Ukraine in kürzester Zeit ihre Systeme weiterentwickelte und durch Softwareupdates in der Lage war, schnell auf neue Herausforderungen zu reagieren. Wurden die Drohnen zu Beginn des Krieges noch ferngesteuert, finden sie mittlerweile autonom durch KI-Steuerung ihr Ziel. Und die Ukraine und Russland entwickeln ihre Drohnen mit maximalem Tempo weiter. Jede Errungenschaft des Gegners sorgt für Anpassungsbedarf bei den jeweils anderen Systemen. Je schneller diese Anpassungen gelingen, umso schneller lässt sich auch der Vorteil des Gegners negieren.

Am Beispiel der Fähigkeitsentwicklung zeigt sich die Bedeutung von Software Defined Defence.

© Bundeswehr/Schulze

Digitale Transformation für mehr Tempo

Damit solche Anpassungen schnell erfolgen können, ist es nötig, den gesamten Prozess von der Problemerkennung über die Weiterentwicklung der Software bis hin zum Aufspielen der neuen Version auf die Systeme zu optimieren. Spätestens jetzt wird klar: SDD ist kein einzelnes Projekt, sondern ein fundamentaler Paradigmenwechsel. Im Kern geht es um zwei zentrale Prinzipien. Zum einen die durchgängige, möglichst bruchfreie Vernetzung aller Sensoren und Effektoren auf dem Gefechtsfeld. Angedacht wurde diese bereits vor 20 Jahren, aber die Umsetzung ist erst durch heutige moderne Technologien wie Cloud, satellitengestützte Kommunikation oder Mesh-Netzwerke wirklich realisierbar.

Das zweite Prinzip ist die immer stärkere Verlagerung der eigentlichen Funktionen in austauschbare Software, also quasi die Verschiebung militärischer „Intelligenz“ von der Hardware in die Software. Diese wird getrieben durch die Notwendigkeit, sich schnell an neue Bedrohungen anzupassen und Resilienz durch Dezentralisierung zu erreichen.

Zudem findet eine Verschiebung von großen integrierten Plattformen wie beispielsweise Panzern hin zu dezentralen vernetzten Einheiten statt, die miteinander abgestimmt agieren. So können etwa Sensordrohnen Aufklärungsdaten bereitstellen, die von KI-Modellen ausgewertet und wiederum an davon getrennte Aktoren wie Kampfdrohnen oder Artillerie weitergegeben werden. Das bedeutet konkret: Nicht mehr das einzelne Waffensystem entscheidet über die Leistungsfähigkeit – sondern die Software, die es steuert, vernetzt und kontinuierlich weiterentwickelt. Diese Verschiebung eröffnet neue Möglichkeiten: Fähigkeiten lassen sich schneller anpassen, Bedrohungen dynamischer ausschalten. Gleichzeitig steigt aber auch die Komplexität erheblich.

Eine weitere Herausforderung wird deutlich, wenn man nicht Drohnen als Beispiel nimmt, sondern die „klassischen“ Waffensysteme. Hier wird schnell klar, dass wir uns in der Praxis eigentlich zwei unterschiedliche Geschwindigkeitswelten anschauen. Auf der einen Seite stehen herkömmliche Waffensysteme, die heute überwiegend als Legacy-Systeme bestehen und über Jahre oder sogar Jahrzehnte gewachsen sind. Aufgrund der häufig monolithischen Systemarchitektur sind schnelle Anpassungen nur begrenzt möglich. Dies wird sich absehbar auch nur teilweise ändern lassen, muss aber bei neuen Systemen von Anfang in einem alternativen Design berücksichtigt werden.

Auf der anderen Seite sehen wir bereits heute unbemannte Systeme an Land, zur See und in der Luft, die von den Herstellern im Grunde „SDD-native“ gedacht und entwickelt werden – und im Prinzip nur darauf warten, dass wir ihnen eine durchgängige, belastbare CI/CD-Pipeline bereitstellen, also die Möglichkeit einer kontinuierlichen Integration und Implementierung von Softwarekomponenten, bis ans „scharfe Ende“.

Marc Simon ist Leiter der Taskforce Software Defined Defence bei der BWI GmbH.

Bundeswehr setzt auf Software

Die Bedeutung, die SDD zukommt, sorgt auch bei der Bundeswehr für einen Fokus auf das Thema. Als primärem Digitalisierungspartner der Bundeswehr in Frieden, Krise und Krieg kommt der BWI GmbH hier eine Schlüsselrolle zu. Im Kontext von SDD baut sie die infrastrukturellen und organisatorischen Grundlagen auf, um sich selbst zur optimalen Unterstützung und Umsetzung von SDD zu befähigen und das Bundesministerium der Verteidigung (BMVg) bei der Konzeption und Umsetzung zu unterstützen. Zentral sind dabei drei Bausteine:

- **pCloudBw:** Die operative Wirksamkeit von Software Defined Defence hängt maßgeblich von einer intelligent verteilten Cloud-Architektur ab. Die private Cloud Bundeswehr (pCloudBw) mit den Anteilen Core, Fog und Edge bildet die Voraussetzung dafür, Daten, KI-Modelle und Softwarefunktionen sicher, resilient und latenzarm vom Rechenzentrum bis in den Einsatzraum bereitzustellen. Nur so lassen sich moderne Verteidigungssysteme dynamisch aktualisieren, domänenübergreifend vernetzen und in hochdynamischen Szenarien nahezu in Echtzeit steuern. Bereits heute stellt die BWI eine zugelassene Cloud-Infrastruktur im Core bereit, die ab 2026 schrittweise um Fog- und Edge-Komponenten sowie zusätzliche technologische Stacks erweitert wird.

- **Software Factory:** Die BWI bündelt ihre Softwareentwicklungsprozesse für die Bundeswehr bereits innerhalb einer eigenen Software Factory. Auf dieser IT-Plattform arbeiten heute schon Entwicklungsteams der BWI je nach Bedarf gemeinsam mit Industriepartnern aus über 50 verschiedenen IT-Unternehmen und im Rahmen eines Experiments auch aus der Bundeswehr. Damit Standards, Methoden und Best Practices, auf deren Basis Anwendungen für die Bundeswehr entwickelt werden, miteinander kompatibel sind und alles gut ineinandergreift, wurde ein „Software Engineering Framework“ definiert, das die BWI gemeinsam mit dem Zentrum Digitalisierung der Bundeswehr (ZDigBw) veröffentlicht und kontinuierlich weiterentwickelt.

- **Analytics and Simulation Advanced Platform (ASAP):** Die BWI etabliert derzeit gemeinsam mit der Bundeswehr eine Plattform, die Training, Verwalten und Life-Cycle-Management von Modellen im Kontext Machine Learning managt sowie das Ausbringen und Betreiben von KI-Modellen orchestriert. Diese baut auf der bereits seit Jahren bestehenden BWI-internen AI & Data Analytics Platform (AIDA) auf.

Roadmap für die nächsten Schritte

Bis Ende 2027 arbeitet die BWI GmbH an einer klaren Roadmap, um ihre Rolle als SDD-Enabler weiter zu schärfen. Dabei steht sie im engen Austausch mit dem BMVg und dem Kommando Cyber- und Informationsraum (KdoCIR). Außerdem stimmt sie sich mit verschiedenen Industrieverbänden ab, wie zum Beispiel dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV), dem Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V. (BDLI) und dem Bundesverband Informationswirtschaft, Telekommunikation und Kommunikation & organisatorische Medien e.V. (BITKOM). Ziel ist es, bestehende Vorhaben und Initiativen zu bündeln, neue Projekte gezielt zu orchestrieren und eine tragfähige Grundlage für die Streitkräfte der Zukunft zu schaffen.

Eine neue Evolutionsstufe resilienter Kommunikation

Blickt man auf die aktuellen Konflikte in Osteuropa oder im Nahen Osten, so rücken schnell Entwicklungen ins Blickfeld, die nicht nur die Art der Kriegsführung in atemberaubendem Tempo verändern. Sie stellen darüber hinaus langgehegte operationelle Einsatzgrundsätze in Frage und werfen neue Anforderungen an Ausrüstung und Fähigkeiten von Streitkräften auf.

Der sich abzeichnende tausendfache Einsatz von ferngesteuerten und mit Künstlicher Intelligenz (KI) sowie fortschrittlicher Sensorik ausgestatteten Waffensystemen, hergestellt und eingesetzt auf industriellem Niveau unter Ausnutzung marktwirtschaftlicher Gesichtspunkte, verändert die Einsatzstrategie nachhaltig: Auf einem „gläsernen" Gefechtsfeld, wo die sog. Kill Chain so kurz ist, dass die Zeitspanne zwischen Aufklärung und Bekämpfung keine Bewegung mehr zulässt, bilden sich „Todeszonen". Anderenorts übersättigen massengefertigte Low-Cost-Drohnen Luftverteidigungssysteme, um Städte und kritische Infrastruktur zu treffen.

Wie weitreichend diese Entwicklung bereits ist, zeigt ein Beispiel aus dem Sommer 2025: Im Rahmen der ukrainischen Operation „Spinnennetz" wurden russische Militärflughäfen tief im Landesinneren angegriffen – auf Distanzen, bei denen eine konventionelle Fernsteuerung der Drohnen nicht mehr möglich war. Stattdessen übernahm Künstliche Intelligenz die hochpräzise Steuerung und Zielerfassung. Dieses Szenario verdeutlicht, dass resiliente Konnektivität jenseits der Sichtlinie in Kombination mit KI-gestützter Autonomie längst kein Zukunftsszenario mehr ist, sondern zur operationellen Realität geworden ist.

Nicht die Masse, sondern die Präzision entscheidet

Diese Bedrohungen erfordern neue, ganzheitliche Abwehrmöglichkeiten. Dabei erkennen immer mehr strategische Vordenker und operationelle Einsatzplaner, dass es nicht nur um den Umfang der vielzitierten „Drohnenwälle" geht, sondern auch um die Fähigkeit, diese schnell, gezielt und präzise zum Einsatz zu bringen. Denn – so lernt es jeder Infanterist bereits in der Grundausbildung – wer besser zielt und schneller schießt, gewinnt den Feuerkampf.

Das Zielen und Schießen indes sind Attribute der Kill Chain, also der vernetzten und hoch-agilen Operationsführung, die den Ausschlag über den Missionserfolg gibt. Ein zentrales Element dieser Art der Operationsführung sind moderne Führungsnetzwerke, die sich auf sichere, resiliente und weitreichende Kommunikation abstützen können.

Dass diese Erkenntnis auch in Deutschland angekommen ist, zeigt ein wegweisendes Experiment der Bundeswehr: Im Dezember 2025 erprobte sie erstmals einen vollständigen Aufklärungs- und Wirkverbund im Gefechtsübungszentrum des Heeres, bei dem ausschließlich unbemannte Systeme – Drohnen und Loitering Munition – eingesetzt wurden. Die dabei genutzte Software Command & Control Unmanned Management System (C2-UMS Bw) vernetzt unterschiedliche unbemannte Plattformen zu einem integrierten Gefechtsverbund. Generalinspekteur Breuer machte das strategische Ziel dabei unmissverständlich klar: „Was wir hier im Gefechtsübungszentrum ausprobiert haben, geht 2026 in die Umsetzung, sodass es 2027 der Brigade Litauen zur Verfügung steht." Die belastbare Kommunikation innerhalb dieses Verbunds ist die technische Grundvoraussetzung für seinen Erfolg.

„Kommunikation ist ein Schlüsselelement, das in seiner neuen Dimension noch nicht vollständig verstanden wurde", erläutert Tobias Willuhn, Business Director für Deutschland/EU und NATO des israelischen Deep-Tech-Startups Elsight. „Denn sichere, resiliente und zuverlässige Kommunikation ist auf den Gefechtsfeldern der Gegenwart und der Zukunft die Grundvoraussetzung für jeden Erfolg. Dabei geht es nicht länger nur um Sprachübertragung per Funk; Kommunikation umfasst heute vor allem den hochfrequenten Austausch von Daten – von Mensch zu Mensch, von Mensch zu Maschine und mit schnell wachsender Bedeutung auch zwischen Maschinen – millionenfach", so Willuhn.

Was muss die militärische Kommunikation der Zukunft können?

Aktuelle Einsatzszenarien stellen drei Kernfähigkeiten in den Mittelpunkt zukünftiger Kommunikationslösungen:

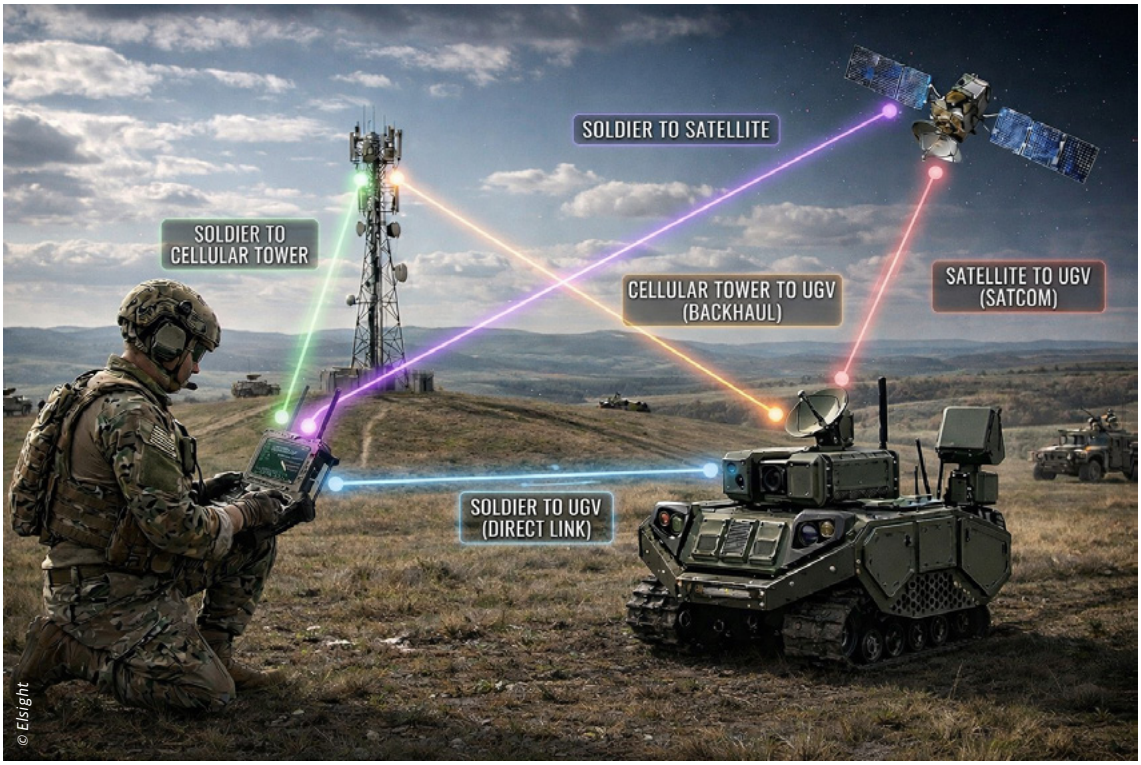
1. **Elektromagnetische Resilienz und aktiver Signalschutz**

   In „Peer-to-Peer"-Szenarien mit einem Gegner, der technologisch auf Augenhöhe agiert, sind die Maßnahmen des Elektromagnetischen Kampfs (EK) allgegenwärtig. Kommunikationsverbindungen müssen nicht nur robust und resilient gegen Störmaßnahmen (Jamming) feindlicher EK-Trupps sein, sie müssen zunehmend auch der Identifikation und Lokalisation durch feindliche Aufklärungskräfte (COMINT/SIGINT) entgegenwirken. Die Dimension dieser Bedrohung ist konkret: Russische EK-Systeme wie das Borisoglebsk-2 können Berichten zufolge Signale in einem Umkreis von bis zu 300 km stören – eine Reichweite, die die gesamte Tiefe einer Gefechtszone erfassen kann.

   Dass Elektromagnetischer Kampf längst keine abstrakte Bedrohung mehr ist, zeigt auch der Übungsbetrieb der Bundeswehr selbst: Bei der Übung Summer Jamm 2025 in Münster trainierten Kräfte der Teilstreitkraft Cyber- und Informationsraum (CIR) gemeinsam mit Polizei und NATO-Partnern gezielt das Jamming gegnerischer Drohnen. Was im Übungsbetrieb als Werkzeug eingesetzt wird, ist auf dem echten Gefechtsfeld die permanente Bedrohung für die eigene Kommunikation. Belastbare Kommunikationslösungen müssen daher nicht nur jammingresistent sein – sie müssen auch die eigene Signatur aktiv verschleiern, um Aufklärung und gezielte Bekämpfung des Sendestandorts zu verhindern.

2. **Weitreichende BVLOS-Konnektivität in industriellem Maßstab**

   Durch den großflächigen und weitreichenden Einsatz bewaffneter UAV – von FPV-Drohnen bis hin zu autonomen Langstreckenplattformen – müssen immer größere Distanzen zuverlässig überbrückt werden. Konventionelle Sichtlinien-Kommunikation (LOS) scheidet dabei strukturell aus: Kommunikationsnetzwerke (C2/Comms) müssen konsequent außerhalb des direkten Sichthorizontes (BVLOS) betrieben werden können.



HALO nutzt eine intelligente Bonding-Technologie, die Daten in mit AES-256-CBC verschlüsselte Pakete aufteilt und diese gleichzeitig über alle verfügbaren Netzwerke überträgt. Der Datenverkehr wird dabei automatisch basierend auf der Echtzeit-Leistungsfähigkeit der Verbindungen geroutet, wodurch nahtlose Übergänge zwischen Netzwerken ohne Verbindungsabbrüche möglich sind.

Die Dimension dieser Anforderung wird durch aktuelle Bundeswehr-Beschaffungen greifbar: Im Februar 2026 genehmigte der Haushaltsausschuss des Bundestages die Beschaffung von rund 4.300 Loitering Weapons HX-2 und rund 2.200 Virtus-Systemen für insgesamt circa 540 Millionen Euro – gedacht als Wirkungselement eines Aufklärungs- und Wirkverbunds, der eine Fläche von 100 × 100 Kilometern abdecken soll. Auf einer Fläche dieser Größenordnung ist Sichtlinien-Kommunikation schlicht ausgeschlossen. BVLOS-Konnektivität ist somit keine Option, sondern die einzige realistische Lösung. Verliert man auf dieser Fläche die Verbindung, verliert man die Drohnen – und gefährdet damit unter Umständen die gesamte Mission.

3. Echtzeit-Datenfusion und Multi-Domain-Interoperabilität

Der massenhafter Einsatz autonomer Systeme und die stetige Verkürzung der Kill Chain stellt ungeahnte Anforderungen an Bandbreite, Latenz und Datendurchsatz. Entscheidend ist dabei nicht nur die schiere Übertragungskapazität, sondern die Fähigkeit, Datenströme aus heterogenen Quellen – Drohnen, Radaren, Kameras, Satelliten, akustischer und seismischer Sensorik – nahezu in Echtzeit zu einem einheitlichen, KI-bewerteten Lagebild zu fusionieren.

Das Bundeswehr-Projekt Uranos KI, dessen Beschaffung der Bundestag im Dezember 2025 bewilligte, illustriert diese Herausforderung exemplarisch: Das System fusioniert Aufklärungsdaten aller Sensorplattformen eines Kampfbataillons nahezu in Echtzeit und leitet daraus Zielzuweisungen für Soldaten, Technik und Artillerie ab. Zwei Bataillone der Brigade Litauen sollen diese Fähigkeit spätestens ab Mitte 2027 erhalten. Die Kommunikationsinfrastruktur, die diese Datenströme trägt, ist dabei die strategisch verwundbarste Komponente des gesamten Verbunds – und gleichzeitig diejenige, auf die bislang am wenigsten Augenmerk gelegt wurde.

Hinzu kommt die Anforderung der nahtlosen Multi-Domain-Interoperabilität: Moderne Streitkräfte operieren gleichzeitig über Land, Luft, See, Weltraum und Cyberspace. Satellitenkommunikation, taktische Funknetze, 5G-Mobilfunk und MANET-Strukturen müssen dabei nicht als getrennte Silos, sondern als integriertes, ausfallsicheres Kommunikationsnetz funktionieren. NATO-Partner müssen über standardisierte Schnittstellen und Wellenformen wie ESSOR gemeinsam operieren können. Streitkräfte, die auf nur eine Übertragungsmodalität setzen, schaffen sich eine strukturelle Verwundbarkeit – die ein moderner Gegner mit Sicherheit gezielt ausnutzen wird.

Hier setzt die Lösung von Elsight an, die ihre Geschäftstätigkeit im Bereich Resilient Communication derzeit weltweit ausdehnen, um auch auf den europäischen Märkten präsent zu sein. Bei Elsight hat man sich angesichts der beschriebenen Herausforderungen zunächst eine zentrale Frage gestellt:

Wie kann man robuste Kommunikationsverbindungen jenseits der Sichtlinie gewährleisten, die gleichzeitig zuverlässig, resilient sowie hoch leistungsfähig und damit für den militärischen Einsatz in aktuellen und zukünftigen Szenarien geeignet sind?

Die Antwort: Man nutzt das gesamte Spektrum der zur Verfügung stehenden Signalquellen aus – Direktfunk (P2P/LOS SDR), Cellular/Mobilfunk (LTE/5G) und LEO Satellite (z. B. Starlink, OneWeb etc.). Unter Nutzung eines hoch performanten Algorithmus und KI-Unterstützung gelingt es, sowohl die Auswahl der Quellen als auch die Lenkung des Datenflusses in Echtzeit und entsprechend der Vorgaben des jeweiligen Missionsprofils optimal zu gestalten.

Von der Herausforderung zum Produkt

Entlang dieser Zielführung entstand das sogenannte HALO, das in Form einer kaum 100 Gramm leichten Platine sämtliche verfügbaren Netzwerke nutzbar macht, um Informationspakete zu übertragen.

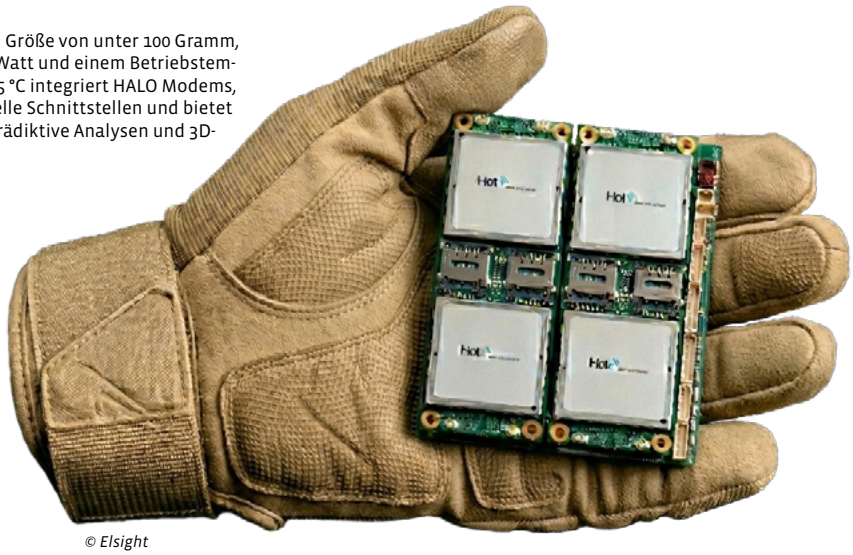
„Unser HALO unterstützt nicht nur die militärisch weit verbreiteten P2P- und MANET-Standards, sondern auch vielfache Mobilfunk-Verbindungen mittels vier 5G/LTE-SIM-Karten sowie alle gängigen LEO-SatCom-Verbindungen. Die KI wählt autonom das Routing für den optimalen Datentransfer aus, indem sie die jeweils schnellsten bzw. stabilsten verfügbaren Datenlinks nutzt. Dabei ist es unerheblich, ob es sich um klassische Audio-Kommunikation mit vorgeschobenen infanteristischen Einheiten oder verdeckt agierenden Spezialkräften, die weitreichende Steuerung von UAVs, USVs und UGVs oder den Datenaustausch mit autonomen Aufklärungs- und Wirksystemen weit hinter den feindlichen Linien handelt“, führt Tobias Willuhn weiter aus.

„Der Sweetspot der Lösung ist dabei ganz klar die robuste Konnektivität jenseits der Sichtlinie, selbst in ‘contested’ – also besonders schwierigen – elektromagnetischen Szenarien, wie wir sie in aktuellen Kriegsgebieten vorfinden. Dabei ist nicht nur die Resilienz gegen Störmaßnahmen ein entscheidender Vorteil, sondern auch die Möglichkeit, die eigene Kommunikation innerhalb des herkömmlichen Funkverbindungsspektrums zu maskieren. So reduzieren wir erheblich die Gefahr der Aufklärung des Sendestandorts und die mögliche Gefährdung durch weitreichende Waffensysteme. Die operationellen Erfahrungen und direkten Rückmeldungen aus den weltweiten Einsatzgebieten geben uns wiederum die notwendigen Impulse, um unsere Lösungen fortlaufend agil weiterzuentwickeln. Unsere Fähigkeit zu schnellen Iterations- und Optimierungszyklen ist etwas, auf das wir zu Recht stolz sind. Sie bildet auch die Grundlage, um mit OEMs, Technologie- und Plattformanbietern in Deutschland, der EU und den NATO-Staaten langfristige Kooperationen und Partnerschaften einzugehen und gemeinsam den Streitkräften unserer demokratischen Länder die Mittel für eine glaubhafte und erfolgreiche Abschreckung an die Hand zu geben.“

Europäischer Rückenwind: AGILE, EUDIS und die neue Verteidigungsarchitektur

Der strategische Rahmen für Lösungen wie den HALO wird derzeit auf europäischer Ebene aktiv gestaltet. Im März 2026 hat die Europäische Kommission das Programm „AGILE“ vorgeschlagen – ein Schnellfinanzierungsinstrument, das Verteidigungstechnologien innerhalb von ein bis drei Jahren vom Prototyp in den Feldeinsatz bringen soll. Förderschwerpunkte sind ausdrücklich KI-Systeme für militärische Lagebilder, autonome Systeme sowie Drohnentechnologien. Flankiert wird AGILE durch das Europäische Innovationsprogramm für den Verteidigungssektor (EUDIS) mit einem Budget von 1,5 Milliarden Euro für den Zeitraum 2025 bis 2027, das insbesondere kleinere Unternehmen und Startups auf dem Weg in den Verteidigungsmarkt unterstützt.

Als Deep-Tech-Startup mit nachgewiesener Fähigkeit zu schnellen Iterationszyklen mit unmittelbaren Einsatzerfahrungen ist Elsight exakt das Profil, das diese Programme adressieren – und das europäischen Streitkräften den entscheidenden Zeitvorteil gegenüber potenziellen Gegnern verschaffen kann.



Mit einer kompakten, tragbaren Größe von unter 100 Gramm, einem Stromverbrauch von 6,5 Watt und einem Betriebstemperaturbereich von -40 °C bis +85 °C integriert HALO Modems, GPS, WiFi/Bluetooth sowie serielle Schnittstellen und bietet zudem Remote-Management, prädiktive Analysen und 3D-Netzabdeckungstools.

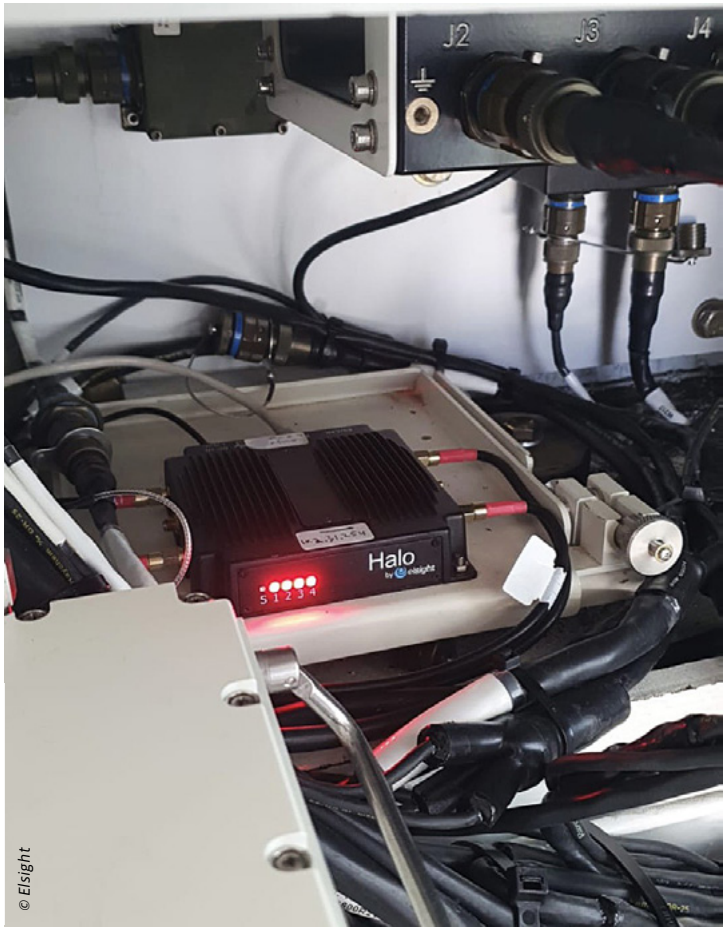
© Elsight

Erste HALO-Boards für Deutschland

So ist es nur konsequent, dass Elsight die Produktion der ersten HALO-Boards „Made in Germany“ bereits angestoßen hat und die Etablierung einer eigenständigen Repräsentanz in der Bundesrepublik mit schnellen Schritten vorantreibt. Diese soll voraussichtlich in Süddeutschland aufgebaut und noch im Laufe des Jahres 2026 eröffnet werden, sodass der heimischen Nachfrage nach marktverfügbaren Systemen auf der Basis resilienter Lieferketten entsprochen werden kann.

Der Standort in Süddeutschland ist dabei kein Zufall: Im Februar 2026 eröffnete die Bundeswehr in Erding ihr erstes militärisches Innovationszentrum, in dem Truppe und Industrie gemeinsam Drohnen, Drohnenabwehr und autonome Systeme erproben. Diese Infrastruktur bildet einen idealen Rahmen für die enge Zusammenarbeit mit Technologiepartnern wie Elsight, die praxisnahe und schnell integrierbare Kommunikationslösungen für den unbemannten Gefechtsverbund bereitstellen. Parallel hat die Bundeswehr Ende 2025 die „Birds Group“ am Kommando Heer aufgestellt – eine dedizierte Organisationseinheit, die Standards für den Drohneneinsatz entwickelt und Industriepartner koordiniert. Auch hier öffnet sich ein direkter Anknüpfungspunkt für Elsights Aktivitäten in Deutschland.

Dabei adressiert Elsight nicht nur Kunden aus den Bereichen Einsatzkräfte, Militär und Krisenreaktion, sondern auch andere Branchen, in denen z. B. für Inspektions- und Wartungsarbeiten oder zur Überwachung von Standorten auf Drohnen zurückgegriffen wird, die jenseits der Sichtlinie in schwierigen Umgebungen funktionieren müssen. Die resiliente Lieferkette auf Basis heimischer Produktion bildet dabei die Grundlage, um der wachsenden Nachfrage aus Deutschland, der EU und dem NATO-Verbund verlässlich zu entsprechen. (DK)



© Elsight

Einbau einer HALO-Einheit zu Test- und Evaluationszwecken in eine bodengebundene autonome Plattform: Integration in bestehende oder zu entwickelnde Systeme und Plattformen sind aufgrund der kompakten und robusten Auslegung ohne Verzögerungen möglich und können so auch in einer frühen Entwicklungsphase einen erheblichen Mehrwert für die Erreichung der Produktzertifizierung bedeuten. ▶

Unternehmenskooperation plant Entwicklung eines Drohnen-Schutzschilds

Das Unternehmen Rheinmetall und die Telekom AG wollen gemeinsam einen Abwehrschirm gegen Drohnen und Sabotage entwickeln, um Städte und kritische Infrastrukturen in Deutschland schützen. Darauf verständigten sich die Unternehmen im Vorfeld der bevorstehenden AFCEA Fachausstellung in Bonn.
Durch die aktuelle geopolitische Lage rückt der Schutz kritischer Infrastrukturen (KRITIS) in den Fokus, während hybride Bedrohungen durch Sabotage oder Drohnenflüge kontinuierlich zunehmen. In diesem Kontext bündeln die Unternehmen ihre Kompetenzen.

Das Ziel der Partner ist es, Fähigkeiten und Technologien gegen vielfältige Angriffsmöglichkeiten auf KRITIS-Standorte zu entwickeln – ein sogenannter Multi-Threat-Protection-Ansatz. Es umfasst Technologien für die Cybersicherheit sowie den physischen Schutz etwa von Liegenschaften – auch als Perimeter-Sicherheit bezeichnet. Details der Zusammenarbeit wollen die Unternehmen zu einem späteren Zeitpunkt bekanntgeben.
Armin Papperger, Vorsitzender des Vorstands der Rheinmetall AG, erklärte: „Die Bedrohung durch Drohnen ist hochgradig digital. Deshalb braucht ihre Abwehr die Verbindung aus Sensorik, Effektoren und sicheren Kommunikationsnetzen. Rheinmetall und die Deutsche Telekom bündeln genau diese Fähigkeiten."
Tim Höttges, Vorstandsvorsitzender der Deutschen Telekom AG, ergänzte: „Souveränität entsteht nicht nur durch Diskussionen, sondern durch Taten. Die Telekom übernimmt hier Verantwortung: Mit unserer Kompetenz bei Konnektivität, Cloud und Datenanalyse bringen wir Drohnenabwehr auf ein neues Level."

Drohnendetektion und -abwehr sind technisch komplex. Je nach Ort und Gelände sind Sensoren unterschiedlich geeignet. Der Telekom-Konzern hatte in Deutschland daher an internationalen wie auch an kleinen Regional-Flughäfen, wie Tannheim in Baden-Württemberg, seit 2017 verschiedene Sensoren internationaler Hersteller erprobt und in sein Angebot aufgenommen. So entwickelt die Telekom ihre technischen Fähigkeiten zur Drohnenabwehr und ihren Sensoren-Mix kontinuierlich weiter: Zum Einsatz kommen bei Kundenprojekten heute Video-, Audio-, Radiofrequenz (RF-) und Remote-ID-Sensoren sowie Drohnenradar.

Passive Sensoren zum Aufspüren potenziell gefährlicher Drohnen können an Funkmasten der Telekom installiert werden.

RF-Detektion bewährt in Kunden-Projekten

Ein Großteil der Drohnen im Markt fliegt, weil sie ein Pilot mit einer Funk-Fernsteuerung in Sichtweite bedient. Drohnen und Fernsteuerung kommunizieren miteinander auf einer Funk-Frequenz, englisch Radio Frequency (RF). Diese Funksignale und damit ihre Position lassen sich von RF-Sensoren ermitteln. RF gilt als sehr verbreitete Methode in der Drohnenerkennung und die entsprechenden Sensoren machen derzeit mehr als 90% aller Drohnen im unteren Luftraum sichtbar. Die von der Telekom eingesetzten RF-Sensoren arbeiten dabei passiv und senden kein aktives Suchsignal aus. Daher lassen sie sich problemlos an Funkmasten installieren, da sie andere sensible Mobilfunktechnik nicht beim Funken stören. Hoch an Funkmasten angebrachte RF-Sensoren haben sich nach Kunden-Erfahrungen der Telekom gerade in Stadtgebieten mit dichter Bebauung bewährt.

Spezialist in der Drohnenabwehr und der Drohnenproduktion

Rheinmetall zählt zu den weltweit führenden Systemhäusern bei der Flugabwehr – auch im Nah- und Nächstbereich. Effektoren des Düsseldorfer Technologiekonzerns befinden sich aktuell sowohl in der Ukraine als auch im Nahen- und Mittleren Osten im Einsatz. Zudem ist Rheinmetall selbst Spezialist für autonome Systeme in allen Domänen, zu Lande, zu Wasser und in der Luft.

Im Dezember 2025 erst haben Rheinmetall, die Polizei Hamburg und die Hamburg Port Authority (HPA) eine strategische Partnerschaft zur Weiterentwicklung von Drohnendetektions- und Abwehrkonzepten im Hamburger Hafen vereinbart. Im Fokus steht die konzeptionelle Entwicklung zukunftsweisender Technologien zum Schutz maritimer, ziviler und kritischer Infrastruktur. Aus technischer Sicht gilt der Hamburger Hafen als besonders herausforderndes Umfeld: Die unterschiedlichen Funkquellen, die maritimen Bedingungen und die dichte Infrastruktur stellen hohe Anforderungen an Detektionssysteme. Als Industriepartner bringt Rheinmetall bei dieser Allianz seine Expertise ein, um maßgeschneiderte Lösungen für komplexe Bedrohungsszenarien zu erarbeiten, wobei die Kooperation Teil einer überregionalen Sicherheitsstrategie ist.

Immer mehr Drohnen fliegen über Mobilfunk

Eine neue Herausforderung sind Drohnen, die über Mobilfunknetze gesteuert werden. Während die Masse der Piloten Drohnen über eine Funkfrequenz per Fernbedienung steuert, nimmt die Zahl der Piloten zu, die den Mobilfunk zum Steuern von Drohnen nutzen. Wie sich diese Drohnen finden lassen, erforscht die Telekom gemeinsam mit der Universität der Bundeswehr Hamburg (Uni-Bw H).

Hier wird das Mobilfunknetz künftig selbst zum Sensor und zu einer Art Riesenradar, indem es Veränderungen und Auffälligkeiten im Datenverkehr erfasst, die auf die Steuerung oder Kommunikation von Drohnen hinweisen, um diese etwa in temporären Flugbeschränkungsgebieten für Einsatzkräfte sichtbar zu machen. Die Basis hierfür ist das von der Telekom auf dem Campus der Uni-Bw installierte 5G-Standalone Hochleistungs-Netzwerk, das auf der Technik von Ericsson basiert.

Die meisten Drohnen werden heute noch mittels Funktechnologie gesteuert, aber gerade im militärischen Bereich nimmt die Nutzung von Mobilfunknetzen stetig zu.

Drohnenverstöße sind schwere Eingriffe in den Flugverkehr

Das Steuern von Drohnen per Mobilfunk ist bislang in Deutschland wenig verbreitet. Piloten müssen laut Gesetz die Drohne stets im Blick haben (line of sight). Wer außerhalb seiner Sichtweite eine Drohne steuert, hat oft kommerzielle Absichten – etwa beim Abfliegen von Stromtrassen oder Pipelines bei Beschädigungen. Diese Piloten müssen ihren Flug bei den Behörden beantragen. Wer nicht beantragt aber trotzdem über Mobilfunk steuert, begeht eine Straftat.
Drohnenflüge in Sperrgebieten erfüllen den Straftatbestand eines gefährlichen Eingriffs in den Flugverkehr. Systeme der Telekom haben im Kundenauftrag bereits in großem Umfang verbotene Drohnenflüge punktgenau lokalisiert, sodass Einsatzkräfte die Piloten schnell finden konnten.

Text: Rheinmetall; DK

IT Security, made in Germany

Die genua GmbH, ein Unternehmen der Bundesdruckerei-Gruppe und Lieferant der Bundeswehr, präsentiert auf der 39. AFCEA Fachausstellung wegweisende Lösungen für das Absichern einsatzkritischer und hochsensibler digitaler Infrastrukturen.

An drei Ständen zeigt der BSI-qualifizierte Hersteller, wie Akteure im Verteidigungssektor und in der geheimschutzbetreuten Industrie die Sicherheit und Resilienz ihrer IT entscheidend steigern und so ihre digitale Souveränität sicherstellen können – mit sowohl Hardware-basierten als auch virtualisierten und konsequent nach dem Security-by-Design-Paradigma entwickelten IT-Sicherheitslösungen. Diese sind in der Regel mindestens BSI-zugelassen für VS-NfD, NATO RESTRICTED und EU RESTRICTED.

Digitale Souveränität: Sicher vernetzt für den Ernstfall

Darüber hinaus gewährt genua Einblicke in die Entwicklung zukunftsweisender IT-Sicherheitstechnologien wie die Absicherung von Cloud-Umgebungen auf Basis zugelassener virtualisierter Firewalls und Gateways. Für den mobilen Umgang mit VS-NfD-eingestuften Informationen hat genua mehrere BSI-zugelassene und NATO-konforme Lösungen im Portfolio – vom hochsicheren VPN-Software-Client genuconnect über die Software-Bundle-Lösung genusecure Suite, die genuconnect mit Festplattenverschlüsselung und Smartcard-Middleware zu einem VS-NfD-konformen mobilen Arbeitsplatz verbindet, bis zur Komplettlösung HP Sure Station, die die genusecure Suite mit einem Laptop und HP-eigenen Schutzfunktionen kombiniert.

Zuverlässige Netzsegmentierung

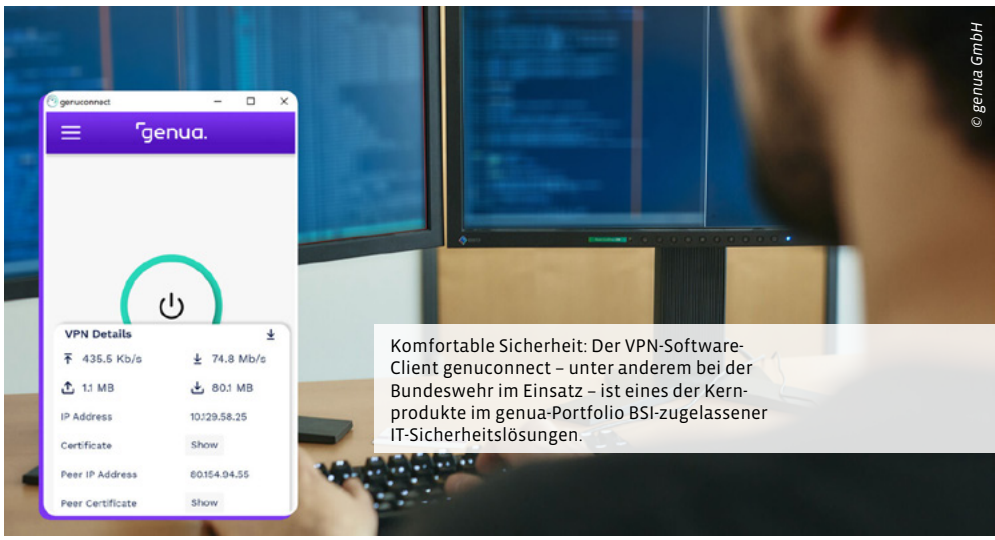
Die einzige vom BSI als „highly resistant“ eingestufte Firewall genugate integriert Application Level Gateway und Paketfilter. genugate Virtual ist die virtualisierte, schnell skalierbare Variante für dynamische Einsatzszenarien – die einzige virtualisierte Firewall mit VS-NfD-Zulassung.

Die hochskalierbare und Backdoor-freie Firewall & VPN-Appliance genuscreen erzeugt quantenresistent verschlüsselte Virtual Private Networks (VPN) für die VS-NfD-konforme Datenkommunikation über öffentliche Netze.

Am genua-Stand sind zudem zwei weitere Unternehmen der Bundesdruckerei-Gruppe vertreten: D-Trust zeigt, wie VS-NfD-konformes Filesharing mit Bdrive funktioniert, während xecuro hochsichere Kommunikationslösungen für den digitalen Austausch von sensiblen Informationen präsentiert, die auch die strengen Anforderungen des Bundes für Verschlusssachen-Kommunikation erfüllen. Darüber hinaus stellt der langjährige genua-Partner ECOS seinen Secure Boot Stick vor.

Experten-Vortrag: So stärken hybride Clouds Resilienz und Autonomie

genua-Experte Arnold Krille wird in seinem Vortrag „Trau Schau Wem: Hybride Clouds für Resilienz und strategische Autonomie“ im Rahmen der AFCEA Fachausstellung aufzeigen, wie man mit geschickter Wahl der Technologien und des Systemdesigns Risiken minimiert und auch unter schwierigen Bedingungen und in außergewöhnlichen Lagen arbeits- und einsatzfähig bleibt.



© genua GmbH

Komfortable Sicherheit: Der VPN-Software-Client genuconnect – unter anderem bei der Bundeswehr im Einsatz – ist eines der Kernprodukte im genua-Portfolio BSI-zugelassener IT-Sicherheitslösungen.

Text: genua; DK

Unternehmen stärken gemeinsam Sicherheit und Resilienz am Edge

Am 11.05.2026 haben die Unternehmen Red Hat und Panasonic Connect eine globale Zusammenarbeit angekündigt, um die Möglichkeiten zuverlässigen Edge Computings neu zu definieren.

Mit vorinstalliertem Red Hat Device Edge auf Panasonic TOUGHBOOK Geräten stellt Panasonic eine integrierte Plattform für sofort einsatzbereite Echtzeit-Datenverarbeitung bereit, die Prozesse in der industriellen Automatisierung, der intelligenten Fertigung, der Verteidigung sowie bei kritischen Infrastrukturen unterstützt.

Kombiniert mit Red Hat Device Edge sind die robusten Panasonic TOUGHBOOK Laptops und Tablets für EdgeComputing optimiert und werden den hohen Sicherheits und ComplianceAnforderungen von Behörden, Verteidigung sowie Telekommunikations- und Versorgungsunternehmen gerecht. Red Hat Device Edge vereint eine enterprise-taugliche Distribution des Open-Source-Community-Projekts MicroShift (eine schlanke von Red Hat OpenShift abgeleitete Kubernetes-Variante) mit Red Hat Enterprise Linux und der Red Hat Ansible Automation Platform. Organisationen haben die Flexibilität, den Umfang des Red Hat Device Edge Supports entsprechend ihren spezifischen betrieblichen Anforderungen zu wählen. Red Hat Device Edge wird in den kommenden Wochen auf Panasonic TOUGHBOOK Geräten erhältlich sein.

Kelly Switt, Senior Director, Industrial Business bei Red Hat, kommentiert: „Mit dieser Zusammenarbeit unterstützt Red Hat Panasonic Connect dabei, sich über klassische robuste Endgeräte hinaus zu intelligenten, autonomen Edge-Knoten weiterzuentwickeln, die selbst in anspruchsvollsten und entlegenen Umgebungen zuverlässig arbeiten. Unterstützt von Red Hat Device Edge bieten Panasonic TOUGHBOOK Endgeräte eine hochsichere und robuste Plattform für mobile Einsatzleitung, taktische Kommunikation, Drohnensteuerung und sichere Echtzeit-Datenverarbeitung – zuverlässig selbst unter härtesten Bedingungen, dort, wo die Ergebnisse zählen."

Masaki Takeda, Direktor der Mobile Solutions Business Division in Europa, ergänzte: „Durch die Partnerschaft mit Red Hat gewinnt TOUGHBOOK einen entscheidenden Mehrwert – dank erweiterter Sicherheit, durchgängiger Cloudto-Edge-Integration und langfristigem Support. Ohne umfassenden Schutz können Investitionen, insbesondere in der Verteidigung und in kritischen Infrastrukturen, schnell an Wirkung verlieren. Durch die Zusammenarbeit mit Red Hat bietet TOUGHBOOK ein integriertes Gesamtsystem, das Effizienz und Produktivität für Anwender steigert."

Text: Panasonic Connect Europe GmbH; DK

Die Zusammenarbeit zwischen Red Hat und Panasonic bietet Vorteile für die Unternehmen und die Anwender gleichermaßen.

© Panasonic

IMPRESSUM

Newsletter Verteidigung veröffentlicht in deutscher Sprache aktuelle Aufsätze, Berichte und Analysen sowie im Nachrichtenteil Kurzbeiträge zu den Themen Rüstungstechnologie, Ausrüstungsbedarf und Ausrüstungsplanung, Rüstungsinvestitionen, Materialerhaltung, Forschung, Entwicklung und Erprobung sowie Aus- und Weiterbildung. Newsletter Verteidigung hat eine europäische, aber dennoch vorrangig nationale Dimension. Aus der Analysearbeit von Newsletter Verteidigung werden regelmäßig hoch priorisierte Themenfelder aufgegriffen, welche interdisziplinär einen Bogen spannen von der auftragsgerechten Ausstattung der Bundeswehr mit Wehrmaterial, der Realisierungsproblematik von militärischen Beschaffungsvorhaben, der Weiterentwicklung der Streitkräfte, den technologischen Trends und Entwicklungstendenzen bei Wehrmaterial, der Weiterentwicklung der heimischen wehrtechnischen Industriebasis und der Rüstungs- und Sicherheitspolitik bis hin zur Rüstungszusammenarbeit mit Partnerländern und gemeinsamen Beschaffung von Wehrmaterial.

Newsletter Verteidigung erscheint auf elektronischem Wege (PDF-Format) mit 50 Ausgaben im Jahr. Eine Weiterverbreitung von Inhalten des Newsletter Verteidigung darf nur im Wege einer Gruppenlizenz erfolgen. Das Abonnement verlängert sich automatisch um ein weiteres Jahr, wenn es nicht drei Monate vor Ablauf mit Einschreiben gekündigt wird.

Verlagsanschrift:
VDS Verlag Deutsche
Spezialmedien GmbH

Ketzerbach 25-28
35037 Marburg, Germany

Tel. +49 6421 1832-899
Fax +49 6421 18329-05

E-Mail:
verlag@deutsche-spezialmedien.de

Gerichtsstand:
AG Marburg an der Lahn

Verantwortlicher im Sinne des Presserechts:
Daniel Kromberg (DK),
Chefredakteur

E-Mail:
redaktion@newsletter-verteidigung.de