

 CRYPTO

CRYPTO MAGAZINE

N° 1 | 2016

Sichere Kommunikation
für eine integrierte
Bodenluftabwehr





Geschätzte Leserin, geschätzter Leser

Beweglichkeit, Schnelligkeit und Flexibilität – Eigenschaften, die eine bodengestützte Luftverteidigung heute erfüllen muss. Die Systeme haben sich in den letzten Jahren enorm entwickelt und müssen nicht nur neuen Bedrohungsformen standhalten, sondern auch extrem effizient sein.

Auch gewinnt die internationale Zusammenarbeit immer mehr an Bedeutung, was aber die Komplexität der Systeme der Bodenluftabwehr erhöht. Deshalb ist die sichere Kommunikation innerhalb dieser Systeme essenziell, um vor Angriffen und Manipulation geschützt zu sein. Ziel ist es, die Integrität jederzeit sicherzustellen.

Ich wünsche Ihnen bei der Lektüre der neusten Ausgabe des CryptoMagazines viel Vergnügen.

Giuliano Otth
President and
Chief Executive Officer

Fokus

Vom Ballon zur Drohne – die rasante Entwicklung der Bedrohung aus der Luft

Seite 3

- 7 | Das AOC – die Schaltzentrale der Luftwaffe
- 12 | Neue Gefahren, neue Kooperationen: Wenn Armeen gemeinsam operieren
- 15 | Das Funkgerät bleibt still: Einsatz gegen ein unbenanntes Flugobjekt
- 18 | Unsichtbarer Schlagabtausch zwischen Boden und Luft
- 20 | Sensible Funkverbindungen im Grenzschutz

Impressum

Erscheint 2-mal jährlich | **Auflage** | 6'200 (Deutsch, Englisch, Französisch, Spanisch, Russisch, Arabisch)

Herausgeber | Crypto AG, Postfach 460, 6301 Zug, Schweiz, www.crypto.ch

Redaktionsleitung | Anita von Wyl, Crypto AG, T +41 41 749 77 22, F +41 41 741 22 72, anita.vonwyl@crypto.ch

Nachdruck | Honorarfrei mit Zustimmung der Redaktion, Belegexemplare erbeten, Copyright Crypto AG

Bildnachweis | Crypto AG: S. 2, 6, 23 | Jose Lledo / Shutterstock: S. 21 | Keystone: S. 15 | Schweizer Luftwaffe: S. 10, 11 | Shutterstock: Titelseite, S. 3, 5, 8, 16, 18, 20 | Stoyan Yotov / Shutterstock: S. 4



Drohnen sind ein wichtiger Bestandteil der taktischen Luftraumaufklärung

Vom Ballon zur Drohne – die rasante Entwicklung der Bedrohung aus der Luft

Von simplen Ballons hin zu hochkomplexen Drohnen – die Bedrohung aus der Luft hat sich seit ihren Anfängen stark verändert. Entsprechend musste sich auch die Verteidigung weiterentwickeln. Da die Systeme immer durchgängiger und integraler werden, ist eine Vernetzung untereinander und mit Partnern enorm wichtig. Die sichere Kommunikation unter den Systemen und der Schutz gegenüber von Manipulation sind der Schlüssel für die Zukunft in der Bodenluftverteidigung.

Ein mit Gas gefüllter Ballon schwebt zu Zeiten der Französischen Revolution als Aufklärer über eine Stadt – dies ist die erste bekannte militärische Nutzung des Luftraums. Der erste wirkliche Luftangriff wurde in der österreichischen Revolution mit Hilfe von Ballonbomben bei der Belagerung Venedigs 1848/49 durchgeführt. Die Gegner wehrten solche Angriffe mit auf Pferdekarren montierten Geschützen oder durch einfaches Gewehrfeuer ab. Später kamen Zeppeline und kleinere Kanonen als Abwehrmassnahmen zum Einsatz. Im Ersten Weltkrieg waren Flugzeugbomber die konkreteste Bedrohung aus der Luft. Dabei setzten die Verteidiger überwiegend eigene Flugzeuge zur Luftabwehr ein. Kanonen oder andere Geschütze waren zu ungenau, um den Feind wirkungsvoll auf Abstand zu halten.

Zwischen dem Ersten und Zweiten Weltkrieg realisierten die einzelnen Staaten, dass der Luftraum künftig ein wichtiger Teil des Schlachtfeldes sein würde und damit auch die Verteidigung des eigenen Gebiets gegen Angriffe aus der Luft einen höheren Stellenwert erlangen musste. Im Zweiten Weltkrieg kamen dafür weiterhin Fliegerstaffeln zum Einsatz. Zusätzlich verstärkten die Armeen ihre Verteidigung vom Boden aus und setzten dazu Flak-Geschütze (Flugabwehrkanonen) ein. Die Entwicklung von Bodenlufraketen nahm erst gegen Ende des Krieges konkrete Formen an, für einen Einsatz kamen die Projekte aber zu spät.

Kalter Krieg bringt neue Technologien

Einen richtig grossen Sprung machte die Bodenluftabwehr im Kalten Krieg. Hierzu trug neben der rasanten Entwicklung von Düsenflugzeugen, Raketentriebwerken oder Radartechniken vor allem die real gewordene Bedrohung durch die Atombombe bei. Hielt sich früher der von einzelnen Bombern angeordnete Schaden in gewissen Grenzen, musste nun mit allen Mitteln verhindert werden, dass auch nur ein einziges feindliches Flugzeug sein Ziel erreichte. Vor allem die Sowjets investierten stark in die Bodenluftabwehr, da die Flugzeugtechnologie der USA der ihrigen deutlich überlegen war. So folgten auf die Stealth-Technologie (Tarnkappentechnik, welche die Radarortung von Flugobjekten erschwert) der Amerikaner beispielsweise stärkere Radarsysteme, präzisionsgelenkte Munition und Lenkflugkörper.

Wichtig ist eine hohe Resistenz gegen Störungen der Kommunikation besonders im Hinblick auf die elektronische Kriegsführung.

Die wohl grösste und kostenintensivste Entwicklung im Kalten Krieg war NORAD – das North American Aerospace Defense Command. Dabei handelt es sich um eine gemeinsame Einrichtung der USA und Kanada zur Überwachung des Welt- raums, um vor Angriffen mit Interkontinentalraketen zu warnen.

Damit verschafften sich beide Staaten eine Vorwarnzeit vor Angriffen über dem Nordpol von etwa drei Stunden für alle grösseren Städte. Zusätzlich wurden zwei atomsichere Operationsbasen – eine davon steht in den Cheyenne Moun- tains – errichtet. Nach Ende des Kalten Krieges sollten die finanziellen Mittel gekürzt werden. Also musste sich NORAD neue Aufgaben suchen – und fand sie in der Überwachung von Anti-Drogen-Operationen. Mittlerweile operiert NORAD von einer Air-Force-Basis aus, die Tiefenbunker wurden in den sogenannten «warm standby»-Modus versetzt.

Kleines Budget – grosse Bedrohung

Heute zeigen sich ganz andere Bedrohungen. Nicht mehr teure Lenkraketen mit grösstmöglicher Reichweite oder Atom- bomben sind es, worauf sich die moderne Bodenluftabwehr einstellen muss. Kleinflugzeuge, Marschflugkörper und un- bemannte Drohnen, die bereits mit vergleichsweise kleinem Budget angeschafft werden können, sind zur vielfältigen Herausforderung für ein Abwehrsystem geworden. Diese Flugkörper bewegen sich meist unter dem Radar und können sogar ohne grosses Aufsehen innerhalb der eigenen Landes- grenzen gestartet werden. Solche Hightechprodukte können bereits für weniger als 10'000 US-Dollar hergestellt und beschafft werden. Dabei sind solche Flugobjekte in der Lage, beispielsweise zehn Kilogramm Nutzlast rund 800 Kilometer weit zu tragen und verfügen über einen Streukreisradius (Circular Error Probable, CEP) von zehn Metern oder weniger. Das heisst, ein Angreifer kann theoretisch von Zürich aus gezielt ein beliebiges Gebäude in halb Europa treffen – von London über Paris bis nach Berlin und Rom.



Die Kommandozentrale muss den höchsten technischen Anforderungen genügen



Die Parabolantenne ist Teil des Raketenabwehrsystems

Das schnelle Aufspüren solcher Objekte und die rasche Entscheidung über die nötigen Gegenmassnahmen sind von essenzieller Bedeutung. Hochauflösende Luftlagebilder ergänzen dabei gerade in topografisch anspruchsvollen Gebieten die Radarüberwachung. Wichtig ist auch, dass eine moderne Bodenluftverteidigung permanent, also ohne Unterbrechung, wirken kann. Denn Kampfflugzeuge als Abwehr- mittel bleiben zwar wichtig, können aber nicht unbegrenzte Zeit in der Luft bleiben. Auch sollte das System über eine Mehrfachzielbekämpfung verfügen, um entsprechend viele Angreifer gleichzeitig abzuwehren. Zudem ist eine hohe Resistenz gegen Störungen der Kommunikation besonders mit Blick auf die elektronische Kriegsführung wichtig.

Ein aktuelles System, das die Anforderungen an moderne Bedrohungsformen sowie klassische Angriffswaffen erfüllt, ist MANTIS (Modular, Automatic and Network capable Targeting and Interception System), ein stationäres Luft- Nahbereichs-Flugabwehrsystem. Es kann sowohl gegen Flug- zeuge und Hubschrauber als auch gegen kleine Ziele wie UAVs (unmanned aerial vehicle), besser bekannt als Drohnen, Lenk- waffen und sogenannte C-RAM-Ziele, also Counter-Rocket, Artillery and Mortar, eingesetzt werden. MANTIS besteht im Kern aus einer Bedien- und Feuerleitzentrale, zwei Radarsen- soren sowie bis zu acht angeschlossenen Geschützen. Ein weite- res System, das sich derzeit im Einsatz befindet, ist das Flugab- wehrraketensystem PATRIOT. Dieses besteht aus mehreren Einzelkomponenten, die auf Lastwagen montiert sind, um eine höhere Mobilität zu sichern. PATRIOT dient zur Abwehr von Flugzeugen, Marschflugkörpern und Mittelstreckenraketen. Zur Erfassung, Identifizierung und Bekämpfung der Luftziele verfügt das PATRIOT-System über ein Multifunktionsradar.

Network Security Platform HC-8224 100M Rugged – für den taktischen und operativen Einsatz



Aufgrund der Reaktionsgeschwindigkeit von Bodenluftabwehr-Systemen sind sie ein Beispiel für die Vernetzung von Sensoren und Effektoren im militärischen Umfeld. Zahlreiche weitere Systeme für taktische und operative Einsätze kommunizieren ebenfalls mit dem Operation Centre über teilmobile Netze und gemeinsame Infrastruktur. Die transportierten Informationen sind ein attraktives Angriffsziel, um manipuliert oder abgehört zu werden.

Mit dem **HC-8224 100M Rugged** verfügt die Crypto AG über ein leistungsfähiges und hochsicheres Chiffriergerät für taktisch-operative Anwendungen. Das widerstandsfähige Gerät wurde speziell für raue Einsatzbedingungen entwickelt. Das kompakte Gehäuse erlaubt vielfältige Einbaumöglichkeiten in beweglichen Installationen, beispielsweise in Fahrzeugen oder mobilen Infrastrukturen. Durch die passive Kühlung sind weder Ventilator noch Luftlöcher vorhanden, und dank dem optionalen Interface-Adapter ist das Gerät komplett wasser- und staubdicht – ideal geeignet für den Feldeinsatz und somit auch für Outdoor-Anwendungen.

Vollvernetzung als Zukunftsvision

Neue Abwehrsysteme kommunizieren hierbei untereinander, stellen mittels einer Vernetzung auch anderen Truppen der Armee die Daten zur Verfügung und liefern dem menschlichen Entscheidungsträger alle nötigen Informationen – und das so abgesichert, dass der Gegner nicht mithört. Bei der integrierten Bodenluftverteidigung sollen sowohl die luft- und bodengestützten taktischen Daten als auch die der Sensoren (zumeist Radarsysteme) und Effektoren (insbesondere Kampfflugzeuge und Flugabwehr) alle miteinander vernetzt werden. Damit können die zur Verfügung stehenden Abwehrmittel im gleichen Raum zur gleichen Zeit eingesetzt werden. Die Effizienz des Verteidigungssystems wird dadurch deutlich erhöht und auch der Ausfall einzelner Komponenten fällt nicht mehr so stark ins Gewicht. In dieser Vernetzungsstufe könnte somit ein Ziel von einem luftgestützten Sensor erfasst werden, aber ein bodengestützter Effektor würde die Lenkwaffe starten.

Problematisch kann allerdings die Fülle der gesammelten Daten für die Person werden, die die Entscheidungen letztendlich treffen muss. Diese müssen so aufbereitet werden, dass der Mensch möglichst nicht selbst noch Rechenoperationen durchführen muss, um beispielsweise ein Flugzeug zweifelsfrei zu identifizieren. Heutzutage ist eine manuelle Bewältigung dieser Informationen nicht mehr möglich, Daten müssen deshalb so aufbereitet werden, dass sie als strategische Information dienen.

Alle diese gesammelten Informationen laufen im sogenannten Air Operations Centre (AOC) zusammen, der Einsatzzentrale der jeweiligen Luftwaffe. Hier werden Luftoperationen geplant, überwacht und die nötigen Kräfte geführt. Hierzu zählen sowohl Flugzeuge als auch bodengebundene Komponenten. Beispielsweise wird bei internationalen Konferenzen wie der OSZE-Tagung in Basel (Schweiz) in Zusammenarbeit mit Deutschland und Frankreich ein Luftschild eingerichtet, welcher ohne Bewilligung vom AOC nicht durchfliegen darf. Damit dieser Schild und die generelle Verteidigung gegen Bedrohungen aus der Luft notfalls mit Waffengewalt durchgesetzt werden kann, ist ein modernes Abwehrsystem nötig.

Das AOC – die Schaltzentrale der Luftwaffe

Im Air Operations Centre (AOC) laufen die Fäden der Luftwaffe zusammen. Die Aufgaben sind vielfältig. Sie reichen von der Luftraumüberwachung und Einsatzführung bis hin zum Ausarbeiten von detaillierten Dienstplänen für Piloten und Maschinen. Dabei sind Abläufe und Befehlsketten genau geregelt. Ein Blick ins AOC der Schweizer Luftwaffe zeigt, was in solchen Kontrollzentren passiert.

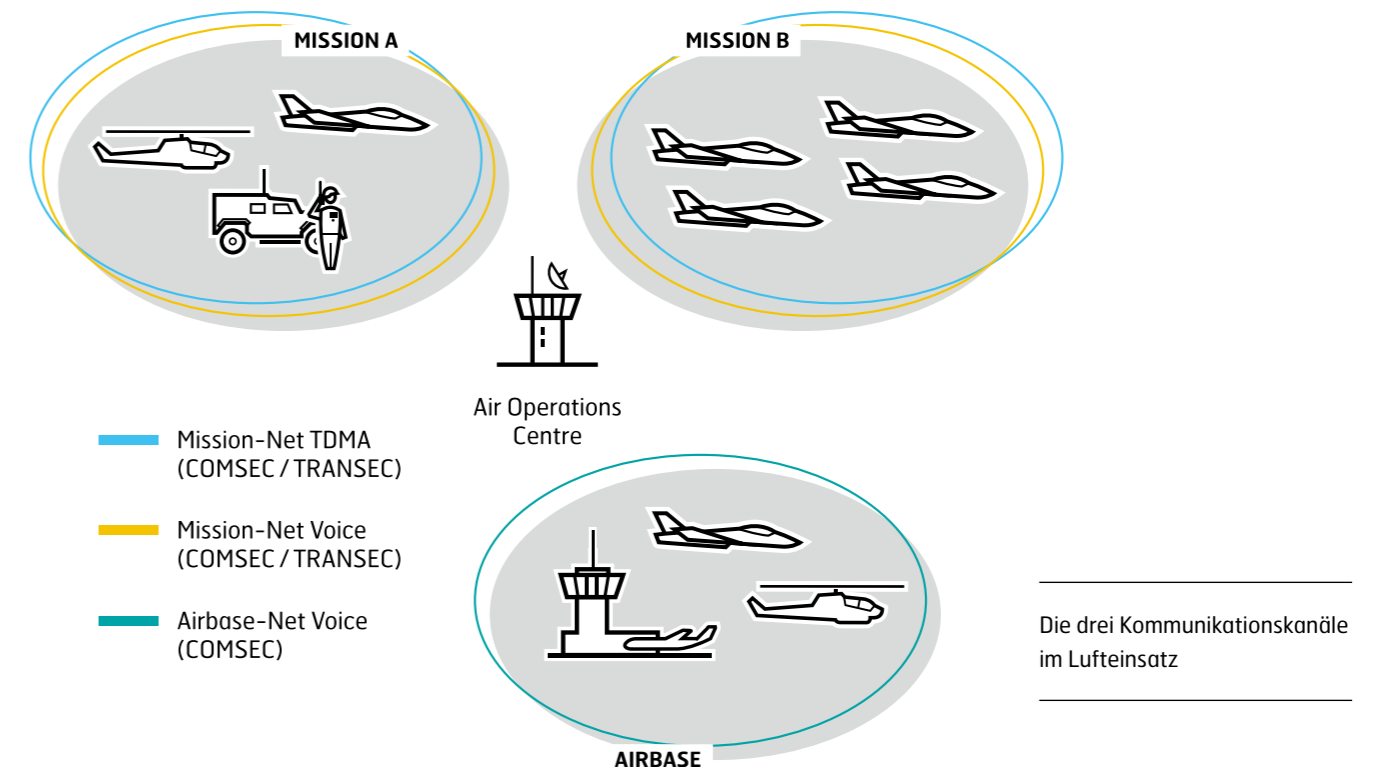
Das Herz der Schweizer Luftwaffe schlägt im zürcherischen Dübendorf. Vom Air Operations Centre (AOC) aus werden die Aktivitäten der Luftwaffe geplant, organisiert und angeordnet. Zu den wichtigsten Aufgaben des AOC zählen die permanente Luftraumüberwachung – 24 Stunden an sieben Tage die Woche – und im Ernstfall die Einsatzleitung der Luftverteidigung. Dafür ist ein Offizier rund um die Uhr auf Pikett.

Controller), welche vom AOC aus die Piloten in ihren Trainingsflügen und beim Luftpolizeidienst führen, kommt das Luftlagebild ebenfalls als wichtigstes Instrument zum Einsatz.

Die Verantwortlichen an den Bodenstellen und die Piloten kommunizieren in der Regel über drei Kommunikationskanäle miteinander: Mission-Net Voice, Mission-Net Data und Airbase-Net Voice. Ersterer ist ein Broadcast Push-to-Talk (PTT)-Sprachkanal für die Kommunikation zwischen Jägerleiter und Pilot sowie zwischen den Piloten untereinander. Der zweite Kanal ist ein Datenlink, der zur Übermittlung von taktischen Daten zwischen dem AOC und den Flugzeugen eingesetzt wird. Und Airbase-Net Voice wird der Sprachkanal genannt, über den die Kommunikation zwischen den Piloten und dem Flughafen-Tower zur Betreuung des Starts beziehungsweise des Anflugs sowie zur Einweisung am Boden (Taxiing) abläuft.

Ohne Luftlagebild läuft nichts

Das Herzstück und zentrale Arbeitsinstrument im AOC ist das Luftlagebild. Verschiedene Sensoren wie militärische oder zivile Radare in den Bergen oder jene der F/A-18 liefern Daten, die von einem sogenannten Multiradartracker zu einem aktuellen Luftlagebild, dem sogenannten Recognised Air Picture (RAP), aufbereitet werden. Anhand dieses Bildes überwachen die Verantwortlichen im AOC den Luftraum und treffen im Ernstfall Entscheidungen. Für die Jägerleiter (Tactical Fighter





Das AOC ist rund um die Uhr an sieben Tagen pro Woche besetzt

Steigen von den sieben Schweizer Militärflugplätzen militärische Jets, Helikopter, Transport- oder Schulungsflugzeuge für Trainings- und Ausbildungsflüge oder für Einsätze in die Luft, plant und koordiniert dies das AOC. Im Detail heisst das: In Dübendorf wird im Vorfeld festgelegt, welcher Pilot wann welches Flugzeug fliegt, welchen Luftraum er benützen kann, wohin die Maschinen allenfalls verschoben werden oder ob sie für Unterhaltsarbeiten am Boden bleiben müssen. Sind die Flieger in der Luft, ist das AOC für die Einsatzleitung und die taktische Flugsicherung vom Boden aus verantwortlich und beruft die Piloten falls nötig für luftpolizeiliche Aufgaben ab. Im Alltag können die Staffeln ihre Begehren für Training und Ausbildung anmelden und das AOC koordiniert entsprechend. Für konkrete Einsätze hingegen gibt allein Dübendorf die Befehle aus.

Sondereinsatz während des WEF

Einer dieser Einsätze ist die jährlich wiederkehrende Sicherung und Überwachung des Luftraums während des World Economic Forums (WEF) in Davos. Zum Schutz der Tagungsteilnehmer – darunter viele Staatschefs und internationale Wirtschaftsführer – wird die Nutzung des Luftraums über Davos im Umkreis von 48 Kilometern eingeschränkt. Dies wird vom AOC aus streng kontrolliert und durchgesetzt. Ohne Bewilligung darf keine Maschine diesen Luftraum durchfliegen oder gar darin landen. Der Führungsrhythmus in diesen Tagen ist ungleich höher als im Alltag. Erteilt das AOC im Normalfall die Befehlsgebung wöchentlich, geschieht dies während des WEF

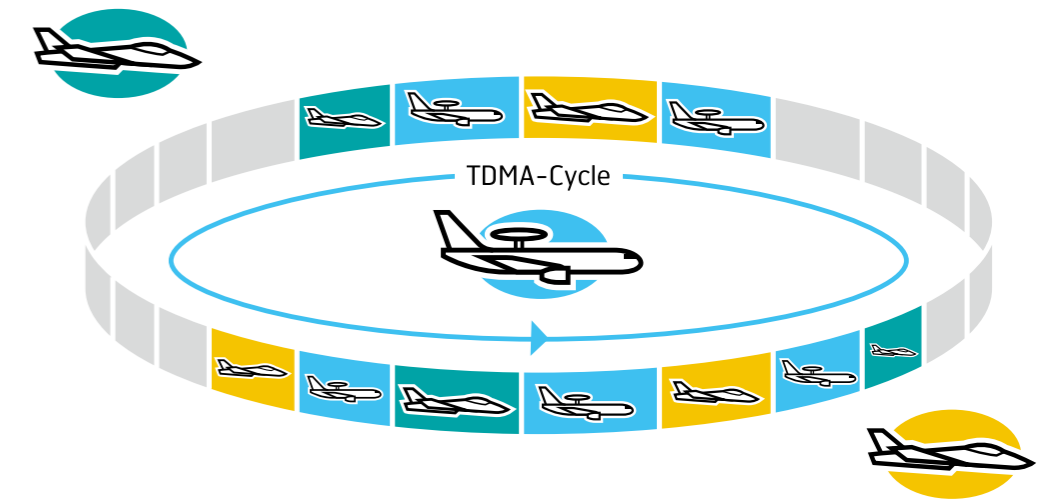
täglich. Dabei ist nicht nur der Kontakt zur vorgesetzten Stufe – spricht Verteidigungsminister und Kommandant der Luftwaffe – viel enger als üblich, auch die Lagebeurteilung mit den Polizeieinheiten vor Ort findet in regelmässigen Abständen statt.

Vielfältige Aufgaben

Zum Alltag der Luftwaffe gehören neben luftpolizeilichen Einsätzen auch nächtliche Such- und Rettungsaktionen mit dem Helikopter. Bis zu zwei Mal pro Woche steigt ein mit einer Wärmebildkamera ausgestatteter Super Puma oder Cougar dafür in die Luft auf. Muss noch während der Nacht nach einer Person gesucht werden, kontaktiert im Normalfall das entsprechende kantonale Polizeikorps den diensthabenden Offizier des AOC. Dieser bietet Pilot, Copilot, Bordmechaniker und den Operateur für das Nachtsichtgerät auf, beurteilt zusammen mit der Polizei die Lage und erteilt den Befehl zum Einsatz.

Ein weiterer Aufgabenbereich des AOC ist der Lufttransportdienst des Bundes. Das heisst, wenn Bundesräte mit dem Helikopter unterwegs sind, Flugzeugsatzteile auf dem Luftweg verschoben werden oder die Maschine von swisstopo, dem Geoinformationszentrum des Bundes, in der Luft ist, geschieht die Planung und Koordination dafür in Dübendorf.

An der Spitze steht der Chef des Operationszentrums der Luftwaffe, ein Oberst im Generalstab. Ihm direkt unterstellt sind der Chef Einsatzplanung, der Chef Einsatzführung (zuständig für den Einsatz der Jägerleiter, welche die Piloten



Time Division Multiplex Access (TDMA): Jeder Slot wird einer Station zum Senden zugeteilt, während die anderen Stationen empfangen. Dies ermöglicht den permanenten Datenaustausch zwischen allen Netzteilnehmern für Commands, Track Exchange, Common Operational Picture usw.

führen), der Chef Nutzung / Steuerung Flugzeuge (Einsatz- und Wartungsplanung der Maschinen) sowie der Kommandant des Lufttransportdienstes vom Bund und der Chef Einsatzunterstützung. Während eines Einsatzes wie während des WEF ist dem Chef des AOC zusätzlich eine Abteilung des Flugsicherungsunternehmens Skyguide unterstellt.

Dringt ein unangemeldetes Flugzeug in den eingeschränkt nutzbaren Luftraum ein, läuft ein standardisierter Prozess ab.

Im AOC arbeiten Berufsmilitärpiloten, Berufsoffiziere, aber auch Zivilangestellte. Manche von ihnen sind militärdienstpflichtig in der Schweizer Milizarmee, wieder andere haben nie militärischen Dienst geleistet oder ihre Dienstpflichten bereits erfüllt.

Keine Chance für unliebsame Zuhörer

Zur Bewältigung der Alltagsaufgaben sowie der Einsätze während des WEF kommen beim AOC verschiedene Kommunikationsmittel zum Einsatz, die anhand verschiedener Massnahmen geschützt werden (mehr dazu im Interview mit Oberst im Generalstab Peter Bruns auf Seite 10). Denn der Informati-

onsaustausch zwischen Fliegern und Bodenstellen ist unterschiedlichen Bedrohungen ausgesetzt. Durch Abhören von Übermittlungen könnten Gegner Details über die Missionen erfahren. Mittels Orten ist die Ermittlung von aktueller Position und Flugrichtung der Maschinen möglich. Durch das sogenannte Jamming versucht der Gegner die Kommunikation durch das Aussenden von Störsignalen auf der gleichen Frequenz zu unterbinden. Und anhand von Täuschungen will die Gegenseite Meldungen verändern oder speist Falschmeldungen in die Kommunikationskette ein.

Eine mögliche Schutzmassnahme bei der Datenkommunikation ist das Time Division Multiplex Access-Verfahren (TDMA). Müssen Sensordaten verschiedener Systeme an mehrere unterschiedliche Missionsteilnehmer übertragen werden, erhält jedes teilnehmende System einen Zeit-Slot, in dem es seine Daten einfügt. Zum Schutz vor Jamming wird häufig das Frequency-Hopping eingesetzt: Die Funkgeräte senden nicht auf einer konstanten Frequenz, sondern wechseln mehrmals pro Sekunde innerhalb des definierten Frequenzbandes.

Und um sich vor unberechtigten Mithörern zu schützen, kommen abhörsichere Verschlüsselungstechnologien zum Einsatz, welche die abgehörten Meldungen nicht interpretierbar und damit nutzlos machen.

«Wir würden am liebsten alles schützen»

Im AOC laufen teils hochsensible Daten zusammen und vertrauliche Informationen werden kommuniziert. Wie die Kanäle geschützt werden, welche Herausforderungen dabei entstehen und was in einem Störfall passiert, sagt der Chef des AOC, Oberst im Generalstab Peter Bruns.

Peter Bruns, wie schützt die Armee die Kommunikations- und Datenübermittlungswege im AOC?

Wo immer möglich, setzen wir auf eigene Netze und Infrastruktur, über die intern vertrauliche Telefongespräche und Videokonferenzen geführt werden können. Für die Kommunikation mit externen Partnern wie Polizei und Schweizerischer Rettungsflugwacht (Rega) werden im Normalfall zivile Netz- und Funkverbindungen genutzt. Ebenfalls sehr wichtig sind redundante Systeme. So können wir die für uns zentrale Autonomie gewährleisten.

Welche Rolle spielen Verschlüsselungstechnologien?

Verschlüsselungstechnologien kommen natürlich zum Einsatz. Beispielsweise an den Schnittstellen zwischen den eigenen und zivilen Netzen. Auch die Übertragungswege der Sensordaten für die Aufbereitung des Luftlagebildes sind durch Verschlüsselung geschützt.

Wo liegen für Sie die grundsätzlichen Herausforderungen?

Wir würden natürlich am liebsten alles schützen. Das ist aber nicht immer praktikabel. Wenn Informationen nicht rechtzeitig einem Entscheidungsträger zur Verfügung stehen, nützt der beste Schutz nichts.

Wie lösen Sie dieses Dilemma?

Indem wir anstatt komplexe Kommunikationsmittel lieber einfache, dafür sichere Wege wählen, zum Beispiel das Telefon. Wo nötig, können wir mittels Verschlüsselung sichere Leitungen herstellen.

Was kann die Kommunikation stören und was tun Sie in diesen Fällen?

Fällt beispielsweise der Strom aus oder werden bei Bauarbeiten ungewollt Leitungen beschädigt, kommen redundante Systeme zum Einsatz. In den allermeisten Fällen spüren wir im AOC gar nichts davon, weil der Übergang automatisch und nahtlos verläuft.

Wie häufig finden gezielte Cyberangriffe statt?

Täglich. Aber auch das dringt nicht bis zu uns ins AOC vor. Einerseits, weil wir grossen Wert darauf legen, möglichst wenig Angriffsfläche zu bieten. Zudem wehren IT-Spezialisten der Armee diese Angriffe schon im Frühstadium ab.

Aussicht aus dem AOC der Schweizer Luftwaffe in Payerne



Peter Bruns ist Oberst im Generalstab und Chef der Operationszentrale in Dübendorf. Seine Karriere startete der promovierte Ökonom vor über 30 Jahren bei der Schweizer Luftwaffe. Als Berufsmilitärpilot flog er unter anderem die F/A-18 Hornet. 2015 schloss Bruns an der Eidgenössischen Technischen Hochschule (ETH) Zürich den Master «Sicherheitspolitik und Krisenmanagement» (MAS SPCM) ab.

Dank dem technologischen Fortschritt können in kurzer Zeit immer grössere Datenpakete übermittelt werden. Was für Vor- und Nachteile sind damit verbunden?

Aus operationeller Sicht bringt es uns nur Vorteile. Wichtige Daten sind immer schneller verfügbar. Durch den Einsatz vieler verschiedener Sensoren jedoch wird deren Handling immer komplexer.

Welche Rolle spielt die Mobilität in der Kommunikation?

Eine grosse. Für Einsätze wie während des WEF (World Economic Forum) sind die Entscheidungsträger immer unterwegs. Da ist es natürlich wünschenswert, aktuelle Lagebilder auch über mobile Kommunikationsmittel wie Tablets austauschen zu können.

Wo liegen die Probleme?

Dass wir dann nicht mehr auf unsere eigenen Netze zurückgreifen können, sondern zivile nutzen müssen. Und jede Brücke ins zivile Netz bedeutet eine zusätzliche Angriffsfläche. Natürlich können wir auch solche Kanäle sicher gestalten. Doch der damit verbundene technische Mehraufwand muss verhältnismässig bleiben.

Verschlüsselungstechnologien kommen an den Schnittstellen zwischen den eigenen und zivilen Netzen zum Einsatz.

Was heisst das genau?

Die Integration und Fusion dieser Daten ist ein wichtiges Thema. Die Menge an Informationen ist grösser als jene, die in der zur Verfügung stehenden Zeit verarbeitet werden kann. Ideal jedoch wäre, wenn die Daten aus den Sensoren in Echtzeit so aufbereitet werden könnten, dass sie für die Entscheidungsträger auch Sinn machen. Daran arbeiten wir.



Neue Gefahren, neue Kooperationen: Wenn Armeen gemeinsam operieren

Internationale Zusammenarbeit gewinnt im Bereich der Bodenluftabwehr an Bedeutung. Gründe dafür sind veränderte Bedrohungsszenarien und teils begrenzte finanzielle Mittel einzelner Staaten. Solche Kooperationen stellen die beteiligten Streitkräfte allerdings vor grosse Herausforderungen.

Noch vor wenigen Jahrzehnten suchten Soldaten den Himmel mit blossen Auge nach feindlichen Flugobjekten ab und lauschten auf entsprechende Geräusche. Über Funk meldeten sie an die Einsatzzentrale, wenn ein Flugzeug ins Blickfeld geriet oder der Turbinenlärm eines Düsenjets zu hören war.

Tempi passati. Mit den heutigen Bedrohungsszenarien kommt das menschliche Auge, Gehör und auch die menschliche Kommunikation nicht mehr mit. Viel zu hoch ist die Geschwindigkeit moderner Flugzeuge. Die Bodenluftabwehr richtet sich zudem längst nicht mehr nur gegen Militärjets. Die Palette der Bedrohungen reicht von ballistischen Raketen und Marschflugkörpern (Cruise Missiles) bis zu getarnten Drohnen.

Dies sei mit ein Grund, warum eine Arbeitsteilung über bilaterale und multilaterale Zusammenarbeit sinnvoll sein könne, meinen Militärstrategen. Die Vorstellung, dass jeder Staat autonom sein Territorium gegen die mannigfaltigen Bedrohungen aus der Luft schützt, sei langsam, aber sicher überholt.

Doch: Weit schwieriger als die Überwindung überholter Vorstellungen gestaltet sich die Koordination unter den Partnern. Etwa die Sicherstellung der Kompatibilität der militärischen Konstellationen oder die Interoperabilität. So müssen die einzelnen Streitkräfte strukturell fähig sein, als grosser Verband geschlossen oder in Teilen im Rahmen einer multinationalen Operation eingesetzt werden zu können. Des Weiteren gilt es die funktionelle Austauschbarkeit von Wehrmaterial und Personal sowie die Gleichartigkeit von Wehrmaterial und Ausbildung sicherzustellen.

Gefahren in allen Höhenbereichen

Im 21. Jahrhundert haben einerseits die subkonventionellen Gefährdungspotenziale wie zum Beispiel terroristische Bedrohungen stark zugenommen, andererseits drohen heute Gefahren aus grosser Distanz: Projektile werden aus weiter Ferne abgefeuert, Drohnen legen aus eigener Kraft lange Strecken zurück – zum Teil mehrere tausend Kilometer. Zudem sind sie oft derart gut getarnt, dass nicht nur das menschliche Auge und Ohr Mühe haben, sondern auch Radargeräte versagen und die eigentlichen Abwehrmittel an ihre Grenzen stossen.

Diese Gefahren bedrohen Land und Leute ausserdem nicht mehr nur aus einer Ebene des Luftraums, sondern von ganz nah bei der Erdoberfläche bis ganz hoch. So bewegen sich Marschflugkörper zum Teil nur wenige Meter über dem Boden, Mittelstreckenraketen hingegen fliegen im unteren Bereich der Erdatmosphäre. Eine effiziente Bodenluftabwehr muss somit in allen Höhenbereichen wirksam sein. Ausserdem zeichnen sich am Horizont bereits die nächsten Entwicklungsschritte ab, welche die Aufgaben in der Bodenluftabwehr noch komplexer machen dürften.

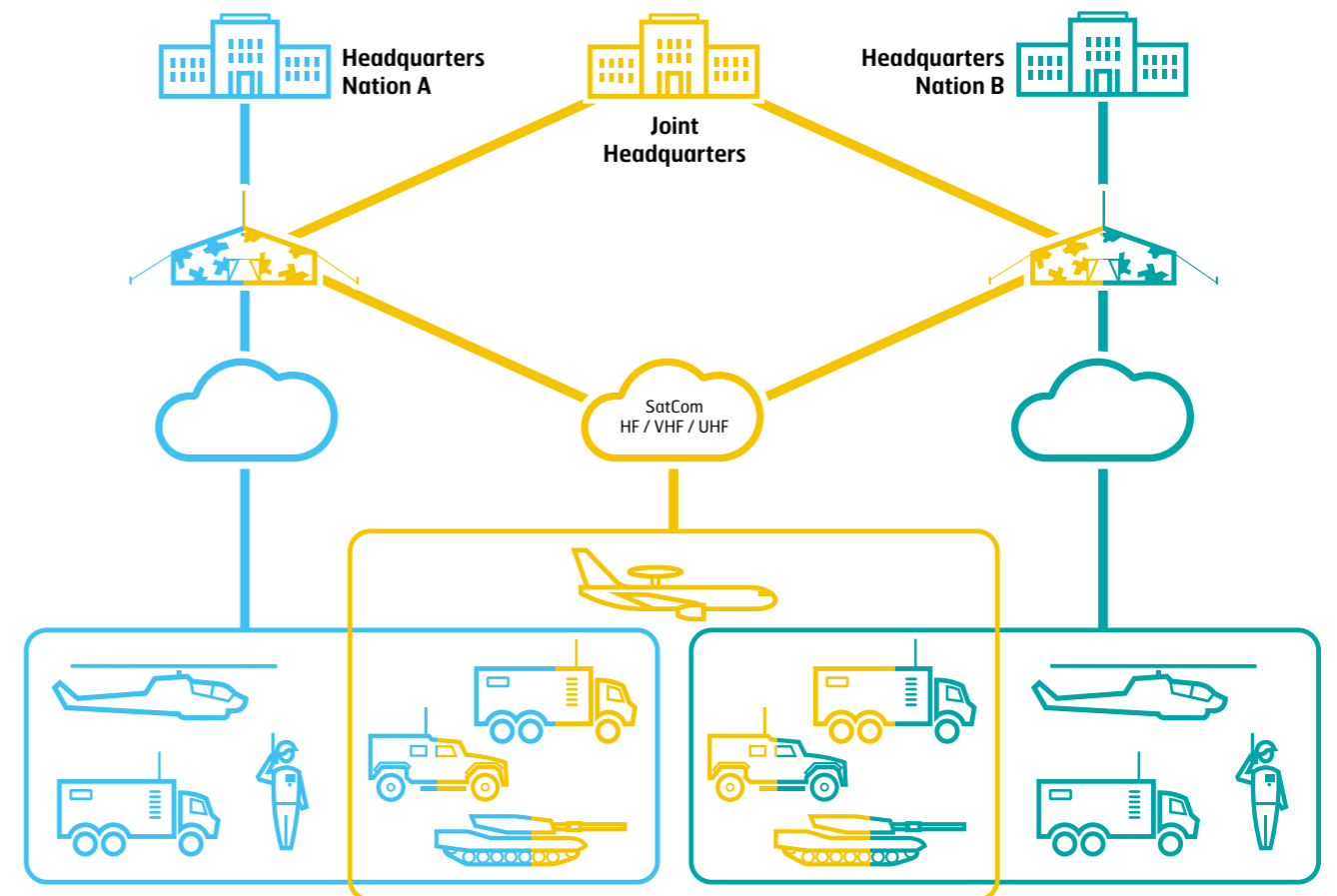
Geheimes bleibt geheim

«Das Bedrohungsspektrum hat sich deutlich verbreitert», bilanziert ein Experte. Das gelte umso mehr, weil die Bevölkerung davon ausgehe, dass sie von ihrer Bodenluftabwehr an 365 Tagen pro Jahr und 24 Stunden pro Tag geschützt werde.

Mit anderen Worten: Armeen brauchen heute hochkomplexe und damit auch teure Systeme, um die Sicherheit im Bereich Bodenluftabwehr zu gewährleisten. Ganz abgesehen von den technologischen Herausforderungen und der Verfügbarkeit von Systemen, ist dies insbesondere für Staaten kleinerer und mittlerer Grösse – angesichts der beschränkten finanziellen Mittel – alles andere als eine einfache Sache.

Die Vorstellung, dass jeder Staat autonom sein Territorium gegen die mannigfaltigen Bedrohungen aus der Luft schützt, ist langsam, aber sicher überholt.

Doch eine solche Zusammenarbeit unter Armeen ist naturgemäss äusserst komplex – insbesondere ausserhalb bestehender fester Bündnisse wie der Nato, zum Beispiel in sogenannten Ad-hoc-Arrangements. Es besteht ein klassisches Dilemma: Welche Informationen werden mit den Partnern geteilt und welche nicht? Denn moderne Konflikte haben gezeigt, dass man die Lage nur kontrollieren kann, wenn man den Informationsraum beherrscht.



Die sichere Kommunikation zwischen den Staaten wird gewährleistet, ohne dabei die eigene Autonomie aufzugeben

Doch das Dilemma sei lösbar, meinen Experten: «Klassifizierte Daten bleiben bei einer solchen Kooperation klassifiziert», wird betont. Dies sei dank klar definierter Prozesse und Strukturen mit klar definierten Aufgaben, Verantwortlichkeiten und Kompetenzen möglich. In modernen Kommunikationslösungen könnten zum Beispiel Schalter «umgelegt» werden. Vereinfacht gesagt: Wird der Schalter auf Position A gestellt, wird mit dem Partner gesprochen, auf Position B nur intern. Bei derartigen Mehr-Kanal-Chiffrierlösungen kommen je nach Kommunikationspartner oder Mission nationale oder nationenübergreifende Algorithmen zum Einsatz. Durch die flexible Wahl der Kommunikationsverbindung bleibt die Souveränität der Partner jederzeit gewahrt.

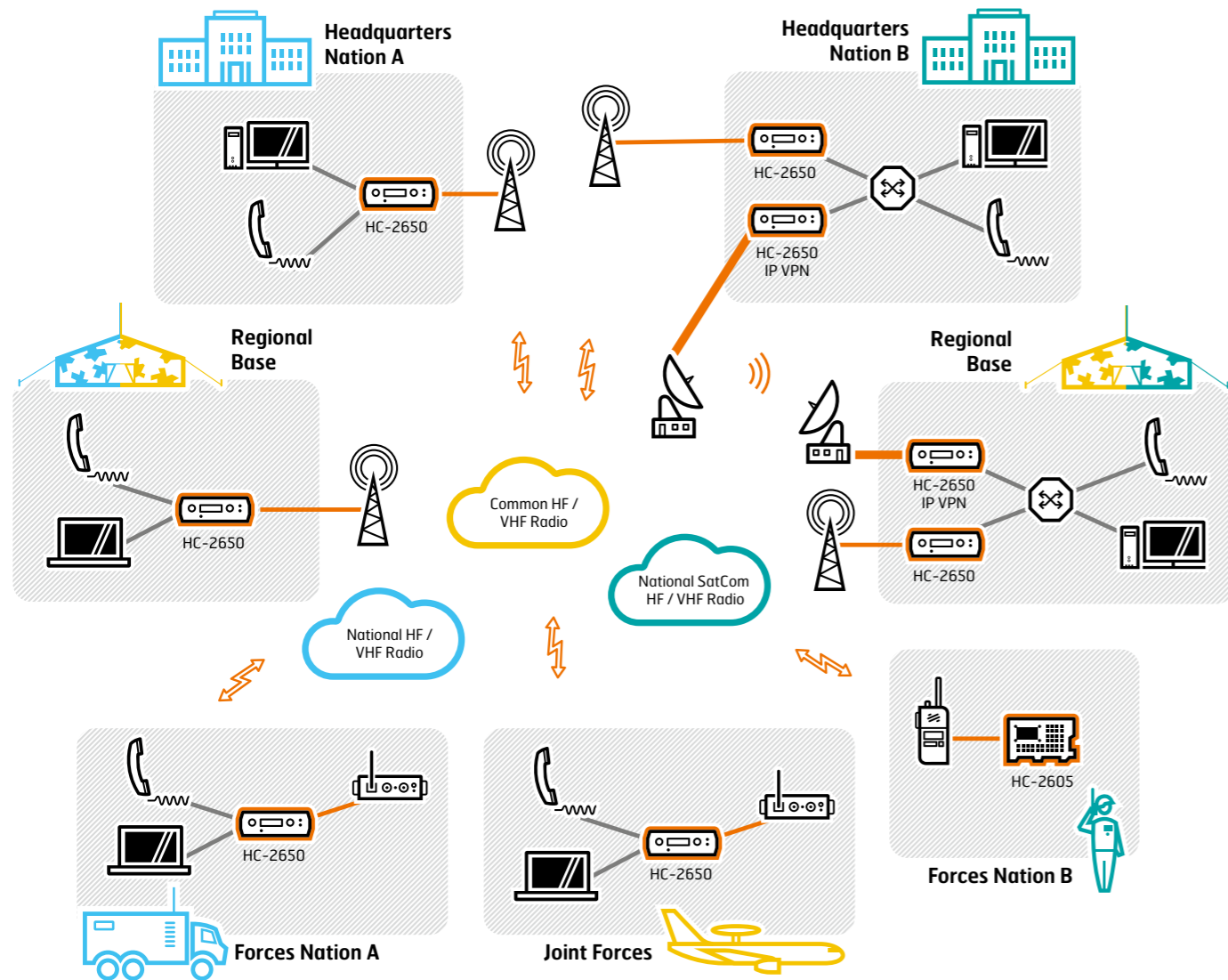
Praxistest erforderlich

Ausserhalb klassischer Militärbündnisse braucht es gemäss Experten für eine erfolgreiche internationale Zusammenarbeit im Bodenluftbereich eine bestimmte Anzahl funktionierender Schnittstellen. Das Stichwort dazu heisst Interoperabilität. Fachleute unterscheiden dabei zwischen mentaler, struktureller und materieller Interoperabilität:

- Zur mentalen Interoperabilität zählen gemäss dieser Unterscheidung Sprache, Terminologie und Abläufe
- Zur strukturellen Interoperabilität gehört zum Beispiel die Kommandostruktur
- Zur materiellen Interoperabilität zählt etwa das Vorhandensein konkreter Kommunikationssysteme

Laut Experten lässt sich diese Interoperabilität nicht von oben verordnen. Es handle sich vielmehr um einen Vorgang, der Schritt für Schritt vorangetrieben werden müsse. Er sei als Lernprozess zu verstehen, der in der Führung und im Ausbildungsverhalten konkrete Veränderungen erfordere – bis hin zur Anschaffung von neuen Geräten.

Priorität habe allerdings die mentale Interoperabilität, sind sich die Experten einig. Konkret müssten Fremdsprachenkenntnisse verbessert und Standards vereinheitlicht werden, zum Beispiel die Kartensymbolik. Am einfachsten und schnellsten werde mentale Interoperabilität erreicht, wenn gegenseitig Führungskräfte zu den Partnertruppen entsandt werden – und das Gelernte dann im eigenen Verband



Das Funkgerät bleibt still: Einsatz gegen ein unbenanntes Flugobjekt

umgesetzt wird. «Kooperation und Interoperabilität kann nicht theoretisch erlernt werden, sondern muss vor Ort erlebt werden», heisst es in Offizierskreisen. «Konzepte auf Papier sind schön und gut, aber man muss es üben.»

Im Bereich der Bodenluftabwehr ist allerdings auch materielle Interoperabilität immer wichtiger. Ein konkretes Beispiel dafür sind die Systeme zur Abwehr von ballistischen Raketen. Solche bestehen aus einem Frühwarnsystem, das aufgrund der grossen Reichweiten der Raketen idealerweise ganze Kontinente abdeckt.

Führen und Kommunizieren im multinationalen Umfeld

Funk hat sich dank Digitalisierung zum integrationsfähigen Medium mit allen üblichen Betriebsarten entwickelt. Modernste IP VPN-basierte Sprach-, E-Mail-, Chat- oder Daten-Link-Applikationen werden darüber abgewickelt. Mit MultiCom Radio Encryption bietet die Crypto AG ein System, das umfassende Informationssicherheit in Funknetzen jeder Dimension und ebenso als integralen Bestandteil von C4I-Systemen gewährleisten kann. Es deckt strategische und taktisch-operative Einsatzprofile ab. Dank Multi-Algorithmus-Fähigkeit sind multinationale Joint Network Operations möglich.

Das MultiCom-System mit seinem Herzstück, dem Radio Encryption HC-2650 / HC-2605 Ensemble, ermöglicht durchgängige, sichere Funkkommunikation über alle Hierarchien hinweg. Es stellt dies mit einer gemeinsamen Algorithmus-Basis, unabhängig von den Funkgeräten und Betriebsparametern wie Frequenzbereich, Applikation, Waveform oder Modus, sicher.

Das Risiko einer Bedrohung aus der Luft wächst – nicht zuletzt durch den vermehrten Einsatz von Drohnen. Moderne Flugabwehrsysteme müssen heute flexibel und schnell sein. Der Schlüssel eines effektiven Abwehrsystems ist aber die sichere und verschlüsselte Kommunikation. Dabei stellen sich unterschiedliche Herausforderungen.

Dringt ein Flugobjekt in ein Hoheitsgebiet ein und kommuniziert nicht, stellt das eine Bedrohung dar. Das Spektrum solcher Objekte ist heutzutage breit gefächert: Marschflugkörper, ballistische Flugkörper oder Drohnen, um nur einige zu nennen. Dabei verändern sich die Bedrohungsarten in der heutigen Zeit schnell und in ständigem Wechsel. So haben beispielsweise Drohnen eine immer länger werdende Reichweite und können von kriminellen Organisationen oder Terrorzellen bedient werden. Das wichtigste Arbeitsinstrument in der Luftüberwachung, um solche Flugobjekte erkennen und einschätzen zu können, ist ein gesichertes und genaues Luftlagebild.

Zur Überwachung des Luftraums kommen sowohl zivile als auch militärische Einrichtungen der Bodenluftabwehr zum Einsatz. Solche Luftverteidigungssysteme haben sich im 21. Jahrhundert stark gewandelt. Systeme mit starren Strukturen, die einen hohen Aufwand für Verlegungen verursachen,

sind kein adäquates Mittel gegen die zu erwartenden Bedrohungen. Das Gebot der Stunde ist Beweglichkeit, Schnelligkeit und Flexibilität, um auf Lage- und Auftragsänderungen angemessen reagieren zu können. Damit steigen aber auch die Anforderungen an die Kommunikation.

Dank Sensortechnik zu genauen Bildern

Früher galt die Annahme: Ein «unnamed aerial vehicle» bewegt sich im oberen Luftraum in grenznahen Gebieten. Heute können derartige Bedrohungen auch im unteren Luftraum mitten im Hoheitsgebiet entstehen. Um ein möglichst vollständiges Luftlagebild zu erhalten, kommen verschiedene Komponenten zum Einsatz, die diese unterschiedlichen Aspekte berücksichtigen. Dabei gibt es beim Einsatz einzelner Komponenten kaum Abweichungen. Überall in der Welt werden Lufträume mit aktiver und passiver Sensorik überwacht. Für die sichere Verkehrsführung im Luftraum sind Flugver-



Durch das längsseitige Auftauchen wird ein unbenanntes Flugobjekt auf Verfahrensfehler hingewiesen

kehrskontrollstellen (FVK) verantwortlich. Der militärische Luftraumschutz hingegen ist je nach Staat oder Bündniszugehörigkeit unterschiedlich geregelt. Prinzipiell aber erfassen und projizieren überall ortsfeste zivile wie militärische Installationen die Bewegungen von Luftfahrzeugen im überwachten Luftraum in Echtzeit, sodass diese verfolgt, identifiziert, bewertet und nach Bedarf Informationen darüber ausgetauscht werden können. Für derartige Verfahrensschritte kommen verschiedene aufeinander abgestimmte Sensoren und Effektoren zum Einsatz. Sensoren sind bodenbasierte Radarsysteme mit fixen und mobilen Stationen, aber auch das Bordradar. Diese Sensoren liefern die erforderlichen Daten zur Erstellung von Luftlagebildern (Recognised Air Pictures, RAP). Zu den Effektoren zählen insbesondere Kampfflugzeuge und Flugabwehreinrichtungen.

Beispiel: Es findet ein Grossanlass mit mehreren tausend Zuschauern statt, der vor Bedrohungen geschützt werden soll. Dazu wird eine militärische Sperrzone errichtet. Um innerhalb dieser Sperrzone eine lückenlose Luftüberwachung sicherzustellen, müssen folgende Massnahmen ergriffen werden: Erstens müssen für die Überwachung innerhalb dieser Sperrzone Daten verschiedener Sensoren zum sogenannten «Recognised Air Picture», der erkannten Luftlage, zusammengeführt werden.

Als Sensoren dienen primär die militärischen Höhenradare. Diese erfassen aber keine Talkessel. Um die lokale Luftlage lückenlos zu generieren, müssen zweitens die Höhenradare

durch die Radare der Kampffjets, die sich in der Luft befinden, die Radardaten der zivilen Luftraumüberwachung sowie die elektronische Signalaufklärung ergänzt werden. Es entsteht ein «Local Air Picture». Nur so werden auch Flugobjekte mit sehr kleinen Radarquerschnitten, wie etwa Modellflugzeuge oder Drohnen, erfasst. Das heisst: Die Operationsführung ist stark vernetzt. Wobei die lokal generierte Luftlage über das militärische Breitbandkommunikationssystem in die Einsatzzentrale der Luftwaffe übermittelt wird.

Wenn das Funkgerät still bleibt

Handelt es sich beim gesichteten Flugobjekt um ein Luftfahrzeug, so besteht meist permanenter Funkkontakt. Über diesen werden zum Beispiel Vorgaben der FVK für Kurs und Flughöhe übermittelt. Bei einem Verstoss gegen die Luftverkehrsregeln wird zuerst versucht, über Funk mit dem fehlbaren Piloten Kontakt aufzunehmen. Wenn nun ein Flugobjekt nicht eindeutig identifiziert werden kann oder der notwendige Funkkontakt der FVK zu einem Luftfahrzeug abreiss und trotz aller Versuche nicht wieder hergestellt werden kann, entsteht Handlungsbedarf.

Dann kommen situationsabhängig auf Entscheidung eines zentralen Gefechtsstandes oder aber des Nationalen Lage- und Führungszentrums für Sicherheit im Luftraum weitere Komponenten zum Einsatz. Das kann zum Beispiel eine aus zwei Kampfflugzeugen bestehende Alarmrotte sein, die dann zur Position des betroffenen Luftfahrzeuges beordert wird, um die Situation aufzuklären. Die Alarmrotte wartet am Boden in ständiger Bereitschaft auf solche Einsätze. Während ihres Einsatzauftrages wird die Alarmrotte von einer militärischen Kontrollstelle per Flugfunk geführt.

Mit anderen Worten: Die Einsatzzentrale Luftverteidigung hat die Möglichkeit, bei Bedarf Kampffjets zu befehlen. Diese können ein fehlbares Luftfahrzeug identifizieren und es allenfalls auf eine andere Route leiten oder gar zur Landung zwingen. Die Interventionsfähigkeit dieses Luftpolizeidienstes besteht rund um die Uhr. Der Einsatz ist allerdings auf hoch fliegende und schnelle Flugobjekte beschränkt. Für langsame Flugobjekte im unteren Luftraum kommen Helikopter zum Einsatz.

In aller Regel wird die Besatzung eines in diesem Rahmen abgefangenen Flugzeuges mit dem längsseitigen Auftauchen der Alarmrotte auf Verfahrensfehler oder Fehlfunktionen aufmerksam gemacht. Die Piloten können dabei durch international standardisierte visuelle Zeichen Verbindung zueinander aufnehmen.

Sichere und schnelle Kommunikationskanäle

Stellt hingegen das abgefangene Luftfahrzeug eine militärische Bedrohung dar, müssen weitere Entscheide gefällt werden. Grundsätzlich trifft der Gefechtsstand entsprechend eines vorgegebenen Massnahmenkataloges diese Entscheidungen. Die Kommunikation über die jeweilige Situation, deren Entwicklung und einzuleitende Massnahmen findet,

ziviler- wie militärischerseits, zwischen den Luftfahrzeugen und Bodenkontrollstellen sowie Bodenkontrollstellen und vorgesetzten Führungszentren statt. Dabei liegen militärische Bedrohungen meist in der Verantwortung von Militärbündnissen – was die Kommunikation zusätzlich schwieriger gestaltet – und terroristische Bedrohungen aus der Luft in nationaler Verantwortung.

Sichere Kommunikation ist der Schlüssel für eine effektive Verteidigung.

Diese Entscheidungsbäume machen klar, dass die Effektivität der Verteidigung von der Kommunikation zwischen Entscheidungsträgern und den auszuführenden Einheiten abhängt. Sie muss schnell und sicher sein. Kommunikation gehört deshalb zur Schlüsseltechnologie. Im Ernstfall müssen sichere Kommunikationswege den Befehl zum Abschuss des «unnamed aerial vehicle» übertragen können. Sind die Kommunikationswege zwischen den Entscheidungsträgern gestört, nützt auch ein teures Luftverteidigungssystem wenig.

Kryptologischer Schutz für Befehle

Präzisionsarbeit am Himmel muss elektronisch sicher geführt werden. Entscheidend dabei ist die maximale Abstimmung zwischen dem «unnamed aerial vehicle» am Himmel, den Sensoren sowie der Einsatzführung. Die resultierende Datenflut können nur spezielle Übermittlungsprotokolle in Echtzeit übermitteln und zu einem Datenbild verdichten. Der Daten- und Funkverkehr bedarf des höchsten kryptologischen Schutzes, da bei solchen Luftoperationen über Leben oder Tod der Besatzung einer unkooperativen Maschine entschieden werden muss.

Es wäre fatal, wenn für Dritte die Möglichkeit bestünde, den Kampfpiloten am Geschützknopf falsche Anweisungen einzuspeisen und etwa den Abschussbefehl für ein verirrtes Flugzeug vorzutäuschen. Ebenso gefährlich wäre, wenn sich der Flugfunk zwischen den Piloten und den Bodenkontrollstellen oder Führungszentren beeinflussen oder auch nur abhören liesse. Der Informationsaustausch muss gegen jegliche Versuche der elektronischen Kriegsführung gewappnet sein. Das ist das A und O eines jeden Einsatzes gegen ein «unnamed aerial vehicle».



Unsichtbarer Schlagabtausch zwischen Boden und Luft

Finden, erkennen, zielen, treffen: Bei der Verteidigung gegen Angriffe aus der Luft sind **Schnelligkeit und technische Überlegenheit entscheidend. Gekämpft wird auch im elektromagnetischen Raum, wo Systeme der Bodenluftverteidigung Informationen sammeln und versuchen, die Kampf- und Kommunikationsfähigkeit des Gegners einzuschränken.**

Ein Angriff aus der Luft ist stets mit dem Einsatz von Spitzentechnologie verbunden. Moderne Angriffssysteme – Kampffjets und Kampfhelikopter, Transportflugzeuge und Bomber, Lenk Waffen und Drohnen – greifen auf eine breite Palette an ausgefeilten Methoden zurück, um Ziele effektiv auszumachen und zu zerstören.

Dasselbe gilt für die Bodenluftverteidigung. Anders als Ziele auf dem Boden bewegen sich fliegende Objekte meist mit rasendem Tempo: Kampffjets erreichen Spitzentempi von über 3'500 Kilometer pro Stunde, in Bodennähe sind es immer noch rund 1'500 Kilometer pro Stunde. Das Orten, Erkennen, Anvisieren bis hin zum Beschuss eines solchen Zieles stellt an Verteidigungssysteme am Boden speziell hohe technische Ansprüche.

Der Krieg im Äther

Einen wichtigen Teil der modernen Bodenluftverteidigung nimmt die elektronische Kriegsführung ein. Der elektronische Krieg besteht einerseits in der Signalaufklärung (Sensorik) und andererseits aus dem Kampf um die Hoheit im elektromagnetischen Raum (Effektorik, Electronic Warfare). Gekämpft wird dabei in jenem Teil des elektromagnetischen Spektrums, der für das menschliche Auge nicht sichtbar ist – die Radiowellen und der Infrarot- oder Ultraviolettbereich – und der deshalb von Funkern liebevoll als «Äther» bezeichnet wird. Dazu später mehr.

Die Signalaufklärung spielt eine zentrale Rolle bei der Nachrichtenbeschaffung der Luftwaffe; sie verrät, was das Auge nicht sieht und das Ohr nicht hört. So versucht die Funkauf-

klärung, Funksignale eines gegnerischen Flugobjekts mitzuhören und so Kommunikationsinhalte in Form von Sprache, Texten, Bildern und Daten abzufangen.

Ein schweres Unterfangen, denn Daten werden durch sichere Informations- und Kommunikationstechnologien (IKT) zwischen Flugobjekt und der Einsatzzentrale am Boden übermittelt. Zudem wechselt der Sender scheinbar zufällig, doch nach einem mit dem Empfänger synchronisierten Muster, die Frequenz. Will ein starker Sender die Verbindung stören, muss er seine Energie auf die ganze Bandbreite der möglichen Frequenzen verteilen – was wiederum die Effizienz des Störsenders (Jammer) verringert.

Die Sensorik dient auch der zeitnahen Identifikation von Luftfahrzeugen und somit der Beurteilung der Luftlage. Es geht darum, mit vielschichtigen Mess- und Analysemethoden elektromagnetische Signale zu erfassen und auszuwerten. Diese Daten geben schliesslich Auskunft darüber: Was fliegt wo und mit welcher Absicht?

Informationen über einen angreifenden Kampffjet liefern beispielsweise Funkwellen. Ein Radar (Radio Detection and Ranging) kann ein Flugobjekt nicht nur orten, sondern es anhand der Signatur des Echos auch identifizieren – oder zumindest erkennen, um welche Art von Objekt es sich wahrscheinlich handeln dürfte. Die Bodenluftverteidigung greift dabei auf ein Netzwerk von Radargeräten zurück, mit der Absicht, möglichst lückenlos den Luftraum zu erfassen und möglichst präzise Daten zu liefern.

Versteckspiel im Luftraum

Kampffjets, Helikopter oder Kampfdrohnen in der Luft sind dem Radar am Boden jedoch nicht chancenlos ausgeliefert. Durch Tarnkappentechnik können sie ihr Funk-Echo minimieren, was ihre Ortung und Erkennung erschwert oder gar verunmöglicht. Das Signal, das ausgefeilte Modelle einem Radargerät zurückstrahlen, kann so stark verkleinert werden, dass es der Fläche einer Münze entspricht. Die Tarnung funktioniert passiv, wobei die Form und die Materialbeschaffenheit eine wesentliche Rolle für die Tarnfähigkeit spielen.

Daneben existieren aber auch aktive Gegenmassnahmen: Sogenannte Düppel (Chaffs) beispielsweise werden vom Kampffjet abgeschossen und erzeugen eine Wolke, welche von den Funkwellen reflektiert wird. Ein gegnerisches Radar kann diese Wolke als falsches Ziel erkennen und den Einsatz von Bodenluftwaffen mitunter stark erschweren.

Die Systeme der Bodenluftverteidigung müssen immer höheren technischen Anforderungen genügen

Auch ein Jet- oder Raketenantrieb ist verräterisch, denn starke Hitzequellen sind im Infrarotbereich eindeutig erkennbar, auf grosse Entfernung und selbst durch Wolken. Dies machen sich Infrarotsensoren von Lenkraketen der Bodenluftverteidigung zunutze, die dadurch die genaue Position eines Flugobjekts eruieren können. Kampffjets können wiederum zur Ablenkung pyrotechnische Massen abwerfen, die heisser sind als ihr Antrieb, und bestenfalls der Lenkrakete ein falsches Ziel vorgaukeln.

«Lauter» als der Gegner

Während die Sensorik in erster Linie der Informationsbeschaffung dient, versucht die Bodenluftverteidigung im elektronischen Kampf den elektromagnetischen Raum zu ihren Gunsten und zu Ungunsten des Angreifers zu manipulieren. Hauptziel ist es, die funkbasierte Kommunikation und Fernlenkung sowie das Radar fliegender Objekte zu behindern oder zu verunmöglichen. Ebenso soll deren Tarnung und Täuschung im elektromagnetischen Spektrum aufgedeckt werden.

In der elektronischen Kriegsführung gilt es, Informationen über den Gegner abzufangen und den Kampf um die Hoheit im elektromagnetischen Raum zu gewinnen.

In der Praxis heisst dies: elektromagnetisch «lauter» zu sein als der Gegner. Denn beim elektrischen Stören geht es darum, durch Feldstärkenüberlegenheit die Verwendung bestimmter Wellenfrequenzen zu verhindern. Dabei die eigene Kommunikation nicht zu stören, ist eine nicht zu unterschätzende Herausforderung.

Die Effektorik versucht ebenfalls, die eigene Kommunikation und die eigenen Radarsysteme vor fremden elektromagnetischen Einflüssen zu schützen. Im Vordergrund steht das Durchsetzen eigener funkbasierter Telekommunikation und das Freihalten unabdingbarer Funkfrequenzen.

Der elektronische Kampf ist nebst Taktik, Einsatzdistanz und Treffsicherheit der Lenk Waffen ein wichtiger Faktor, wenn es darum geht, wer aus dem Duell zwischen Bodenabwehr und Flugobjekt als Sieger hervorgeht. Die technische Entwicklung der Angriffs- und Verteidigungssysteme wird hier auf die Spitze getrieben. Es ist ein hochtechnisierter Kampf der Massnahmen und Gegenmassnahmen, die oft automatisch laufen und ausgelöst werden.



Sensible Funkverbindungen im Grenzschutz

Die Aufgaben des Grenzschutzes werden immer komplexer. Mit der zunehmenden Mobilität der Menschen wird nicht nur der Tourismus oder der grenzüberschreitende Handel begünstigt – vielmehr finden auch kriminelle Organisationen oder Akteure mit terroristischen Absichten neue, über Landesgrenzen hinweg reichende Handlungsfelder. Entsprechend muss sich der Grenzschutz in vielen Ländern dieser neuen Situation anpassen und die notwendigen Vorkehrungen treffen, um weiterhin effizient und wirksam agieren sowie die innere Sicherheit wahren zu können.

Praktisch jeder souveräne Staat definiert sich unter anderem über ein geografisches Gebiet und die entsprechenden Landesgrenzen. Die Kontrolle von Personen- und Warenflüssen an diesen Aussengrenzen stellt eine hoheitliche Kernaufgabe des Staates dar. In der heutigen Zeit finden Grenzübertritte rechtlich gesehen nicht nur an den Aussengrenzen, sondern zum Beispiel auch an Flughäfen, in Frachtversandzentren, Zollfreilagern oder beim Einschiffen auf einem Hochseeschiff statt.

Entsprechend fallen dem Grenzschutz vielfältige Aufgaben zu, wie zum Beispiel:

- Personen- und Warenkontrollen an den Grenzposten an den Landesgrenzen, Häfen und Flughäfen
- Umsetzung der Zoll-, Einfuhr- und Ausfuhrbestimmungen an den oben aufgeführten Grenzübergängen
- Abfangen von gesuchten Kriminellen und Terroristen an den Grenzübergängen, in Zusammenarbeit mit Polizei- und Fahndungsbehörden
- Abfangen von Schmuggelwaren, Betäubungsmitteln, Waffen und anderen unerlaubten Gütern an den Grenzen

- Überwachung der Grenzen beziehungsweise der Grenzabschnitte abseits der definierten Übergänge
- Überwachung der Küsten und hoheitlichen Gewässer, in Zusammenarbeit mit der Küstenwache
- Umgang mit Flüchtlingen und illegalen Einwanderern
- Erkennung von Grenzverletzungen in der Luft, zu Lande und zu Wasser, in Zusammenarbeit mit der Armee

Anhand der aufgeführten Aufgaben wird deutlich, dass die Grenzschutzdienststellen darauf angewiesen sind, untereinander und mit anderen Organisationen einen weitreichenden Kommunikationsaustausch zu pflegen.

Interorganisationaler Austausch von Informationen

Die Führungs- und Einsatzleitstellen des Grenzschutzes müssen sich jederzeit mit den Aussenstellen – den Grenzposten, der Grenzpolizei an den Flughäfen, den Immigrationsbehörden an Häfen usw. – austauschen können. Die einzelnen Grenzposten beziehungsweise die dort tätigen Grenzbeamten benötigen dabei Zugriff auf die Fahndungssysteme der Polizei und der

Strafverfolgungsbehörden, um verdächtige Personen überprüfen zu können. Des Weiteren kooperieren die Grenzschutzbehörden in gemeinsamen Missionen mit weiteren für die Sicherheit des Landes und dessen Grenzen zuständigen Organisationen wie der Küstenwache oder der Armee.

mit weitaus umfangreicheren Mitteln konfrontiert, wie grossen kriminellen Organisationen im Umfeld des Rauschgift-, Waffen- oder Menschenhandels, international tätigen terroristischen Gruppierungen, aber auch mit gegnerischen militärischen oder paramilitärischen Einheiten.

Hochsichere Kommunikationslösungen für den Grenzschutz

Um erfolgreich gegen derartige Gegner vorgehen zu können, müssen der Grenzschutz sowie die mit ihm zusammenarbeitenden Stellen über sichere Kommunikationsmittel verfügen, die kompromisslos und jederzeit vor Störungen oder unerwünschtem Abhören geschützt sind. Neben der Verschlüsselung der Backbone-Netzwerkverbindungen kommt hierbei der Chiffrierung der typischerweise auf Funktechnik basierenden taktischen Kommunikationsmittel eine zentrale Bedeutung zu. Neben den Lösungen der Crypto AG zur Netzwerkchiffrierung nimmt hierbei das Crypto MultiCom Radio Encryption System eine besondere Stellung ein. MultiCom Radio Encryption umfasst mit dem HC-2650 und dem HC-2605 zwei Funkverschlüsselungsplattformen, die ein breites Spektrum an Bedürfnissen und Anforderungen von mobilen Anwendern abdecken – wie insbesondere im Einsatz an den Landesgrenzen.

Der Grenzschutz muss über sichere Kommunikationsmittel verfügen, die kompromisslos und jederzeit vor Störungen oder unerwünschtem Abhören geschützt sind.

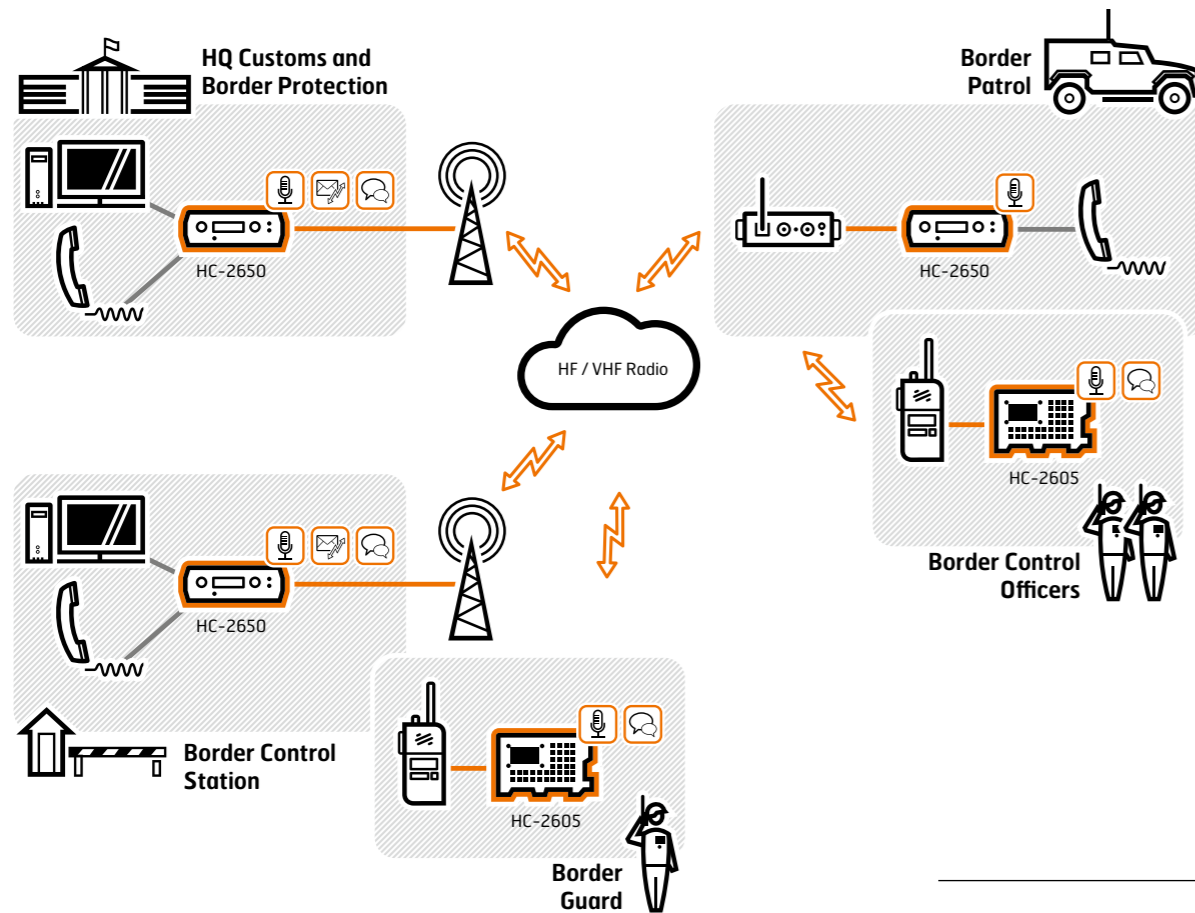
Der Grenzschutz sieht sich neben den vielen kleineren potenziellen Konfliktsituationen, wenn beispielsweise Personen mit unerlaubten beziehungsweise nicht deklarierten Waren oder ohne gültiges Visum aufgegriffen werden, auch Gegnern

Auch mit dem Handfunkgerät wird sicher kommuniziert



Grenzschutz-Patrouillenboot im Einsatz





Abhörsichere Funkverbindungen sind im Grenzschutz essenziell



Das HC-2605 verschlüsselt sowohl Sprache als auch Textnachrichten für die Übermittlung per Funk

Sowohl das HC-2650 als auch das HC-2605 sind Verschlüsselungsplattformen, die einer breiten Vielfalt an Funksystemen vorgeschaltet werden können. Die beiden Funkverschlüsselungslösungen unterstützen sowohl Sprechfunk als auch unterschiedliche Datenübertragungsarten (siehe Tabelle unten).

Während das HC-2650 für den stationären Einsatz oder den Einbau in Fahrzeugen konzipiert ist, stellt das HC-2605 ein portables Handset beziehungsweise Terminal dar, das zusammen mit einem Handfunkgerät jederzeit auf Mann mitgeführt werden kann.

Die Verschlüsselung des Sprechfunks sowie der Datenübertragung kann im Rahmen einer Vielzahl an Frequenzbändern eingesetzt werden, etwa in High Frequency (HF) für grössere Entfernungen (Beyond Line of Sight, BLOS) oder in Very High Frequency (VHF) und Ultra High Frequency (UHF) für den taktischen Einsatz oder beispielsweise bei Verbindungen zwischen fixen Grenzstationen und Patrouillen.

Sicherstellung der Kommunikation auch bei schlechten Rahmenbedingungen

Die Unterstützung der Übermittlung von Textnachrichten (MultiCom Chat) von einem mobilen Gerät aus stellt im Grenzschutzeinsatz einige wesentliche Vorzüge dar:

- Personen- und Fahrzeugdaten können unmittelbar erfasst und zur Überprüfung übertragen werden.
- Mittels eines integrierten GPS werden Textnachrichten optional mit den geografischen Standortkoordinaten versehen.

- Ein Informationsaustausch ist auch bei hohem Umgebungslärmpegel möglich oder wenn ein unmittelbares Beantworten der Nachricht über Sprechfunk nicht möglich ist.
- Während die elektrische Speisung des HC-2605 im Normalfall durch das Funkgerät sichergestellt wird, können Textnachrichten dank den integrierten Batterien auch bei ausgeschaltetem Funkgerät erfasst oder gelesen werden.
- Vordefinierte Textformulare (Ereignis-, Bestandes-, Notfallmeldungen) erlauben eine rasche und effiziente Kommunikation.
- Textmeldungen können aufgrund ihres geringen Bedarfs an Bandbreite auch bei schlechten Funkbedingungen erfolgreich übertragen werden, bei denen kein verständlicher Sprechfunk mehr möglich ist.

Applikationen in der Zukunft. Die Funkverschlüsselungslösungen der Crypto AG ermöglichen sowohl im Grenzschutz als auch bei anderen sicherheitskritischen Organisationen hochsichere Kommunikation – und dies durchgängig von der strategischen bis auf die taktische Ebene.

Oftmals stehen bei Grenzschutz, Küstenwache, Polizei und Armee die unterschiedlichsten Funksysteme im Einsatz. Dank den Funkchiffrierlösungen der Crypto AG können diese heterogenen Netze zu einem sicheren homogenen Funknetz zusammengeführt werden.

Beide Geräte, die mit nahezu sämtlichen gängigen Funksystemen betrieben werden können, verfügen über einen ausgeprägten Schutz gegen Schmutz, Wasser und elektromagnetische Abstrahlung. Ein kundenspezifischer Verschlüsselungsalgorithmus, der durch den Kunden zusätzlich angepasst werden kann, bietet bestmöglichen Schutz vor unerwünschtem Abhören durch den Gegner. Das Messaging-System basiert auf dem NATO-Standard STANAG 5066 für Datenübertragung über Funkwellennetze und ermöglicht somit die Integration weiterer

Übertragungsarten HC-2650 und HC-2605

	HC-2650	HC-2605
Secure Voice	✓	✓
Secure Data	✓	–
MultiCom Messenger (Secure E-Mail)	✓*	–
MultiCom Chat (Textnachrichten)	✓*	✓
IP VPN	✓	–

* bei Anschluss eines PCs beziehungsweise Notebooks



Crypto AG
Postfach 460
6301 Zug
Schweiz
T +41 41 749 77 22
F +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

CRYPTO cSEMINARS

cSeminar Information Security Specialists
3. bis 7. Oktober 2016

cSeminar Technical Vulnerability Testing
10. bis 14. Oktober 2016

cSeminar Contemporary Cryptography
17. bis 21. Oktober 2016

Die Seminare finden in der Crypto Academy
in Zug/Steinhausen statt.

Kontakt und weitere Informationen unter
www.crypto.ch/de/produkte-und-dienstleistungen#seminare