CRYPTO

CRYPTO MAGAZINE

N° 1 | 2015

Taktische Kommunikation in der Luftwaffe

Geschätzte Leserin, geschätzter Leser

Die sichere Übermittlung von taktischen Informationen in der Luftwaffe ist von enormen technologischen Entwicklungsschritten geprägt worden, zu denen Unternehmen wie die Crypto AG massgeblich beigetragen haben. Unverändert geblieben ist die Tatsache, dass der zuverlässige Schutz der Kommunikation zwischen Einsatzführung und Kampfflugzeugen ein besonders kritischer Faktor für den Erfolg einer Mission ist.

Welchen Risiken die ausgetauschten Informationen dabei ausgesetzt sind und welche Schutzmassnahmen dagegen ergriffen werden können, lesen Sie unter anderem im Interview mit dem Kommandanten der Schweizer Luftwaffe.

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

Giuliano Otth

President and
Chief Executive Officer

Fokus

Information als matchentscheidender Erfolgsfaktor in der Luft

Seite 3

Impressum

Erscheint 3-mal jährlich | **Auflage** | 6'200 (Deutsch, Englisch, Französisch, Spanisch, Russisch, Arabisch)

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

Redaktionsleitung | Tanja Dahinden, Crypto AG, T +41 41 749 77 22, F +41 41 741 22 72, tanja.dahinden@crypto.ch

Konzept / Layout | illugraphic, Sonnhalde 3, 6332 Hagendorn, Schweiz

Übersetzung | Apostroph Luzern AG, Töpferstrasse 5, Postfach, 6000 Luzern 6, Schweiz

Druck | Druckerei Ennetsee AG, Bösch 35, 6331 Hünenberg, Schweiz

Bildnachweis | Bloomberg / Kontributor: S. 17 | Bundesarchiv: S. 9 | Crypto AG: S. 2, 20, 21, 23 | DCNS Group: S. 22 | Keystone / Photopress-Archiv / RIA / Str: S. 6 | R. Winzer: S. 7, 12, 13 | R. Winzer (Royal Jordanian Falcons): S. 3 | Schweizer Luftwaffe: S. 11 | Shutterstock: Titelseite, S. 15, 19

Information als matchentscheidender Erfolgsfaktor in der Luft

Bei den Luftstreitkräften entscheiden rasche und verlässliche Kommunikationswege zwischen den involvierten Partnern über Erfolg oder Misserfolg einer Mission. Aus der durch die verschiedenen Sensoren (Radare usw.) generierten Datenflut müssen die Piloten in kürzester Zeit die für ein konsolidiertes Lagebild erforderlichen Informationen erhalten und mit ihrem Einsatzleiter rasch und präzis die Befehle und Angaben für den anstehenden Auftrag austauschen können. Der Einsatz der hierzu erforderlichen Kommunikationsmittel ist mit ganz besonderen Herausforderungen verbunden.

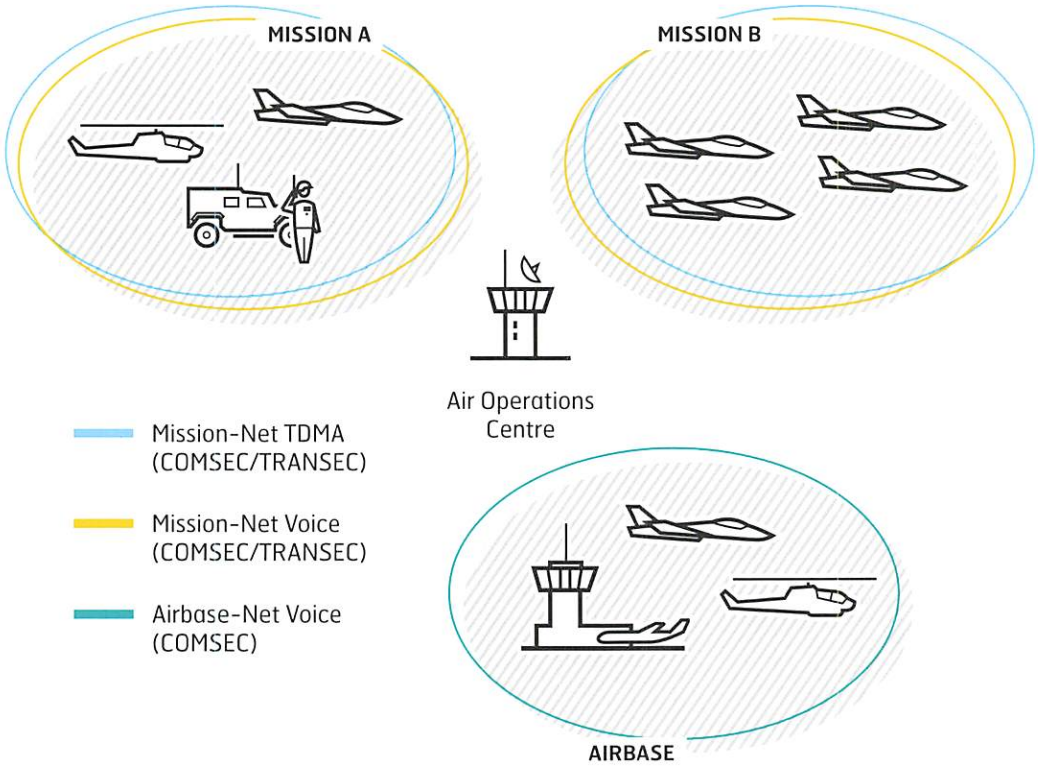
Ralf Winzer | Customer Segment Manager

Der erfolgreiche Einsatz der modernen Luftwaffe hängt längstens nicht mehr nur von leistungsfähigen Kampfflugzeugen und dem Geschick der Piloten ab. Zahlreiche Akteure und deren effiziente Kommunikation untereinander tragen eine mindestens ebenso grosse Mitverantwortung für die zielgerichtete Ausführung einer Mission in den Lüften.

Wie jedes Militärdispositiv setzt die Luftwaffe das perfekte Zusammenspiel zwischen Effektoren, Sensoren und Kommandostrukturen voraus. Zu den Effektoren zählen insbesondere die Kampfflugzeuge und Flugabwehr (Flab)-Einrichtungen.

Die Sensoren – bodenbasierte Radarsysteme mit fixen und mobilen Stationen, aber auch der Bordradar usw. – liefern die erforderlichen Daten, die im Tactical Operation Centre (TOC) zur Erstellung der ausgewerteten Luftlagebilder (Recognised Air Pictures [RAP]) verdichtet werden.

In der Einsatzstelle beziehungsweise dem Air Operations Centre (AOC) führen die Tactical Fighter Controller (TFC) anhand der Missionsziele und der vorliegenden RAP die ihnen jeweils zugewiesenen Piloten.



Die drei Kommunikationskanäle im Lufteinsatz

Die Kommunikation zwischen den Flugzeugen und den Bodenstellen erfolgt typischerweise über drei Kommunikationskanäle:

- **Mission-Net Voice:** Broadcast Push-to-Talk (PTT)-Sprachkanal zwischen dem Piloten und dem TFC beziehungsweise den Piloten untereinander
- **Mission-Net Data:** Ein Datenlink zur Übermittlung von taktischen Daten zwischen dem AOC und den Flugzeugen (und anderen Gefechtsteilnehmern). Die Übermittlung erfolgt typischerweise im TDMA (Time Division Multiplex Access)-Verfahren.
- **Airbase-Net Voice:** Sprachkanal zwischen dem Piloten und dem Flughafen-Tower zur Betreuung des Starts beziehungsweise Anflugs sowie zur Einweisung am Boden (Taxiing)

Bedrohungen und Schutzmassnahmen

Der Informationsaustausch zwischen den Fliegern und den Bodenstellen ist dabei unterschiedlichen Bedrohungen ausgesetzt:

- **Abhören (Interception):** Das Abhören der Übermittlungen gibt dem Gegner Aufschluss über die Absichten der Mission, über den Stand der vorhandenen Erkenntnisse sowie über die Einsatzdisposition und Position der Flugzeuge.
- **Orten:** Das Anpeilen der Funksignale ermöglicht es dem Gegner, die aktuelle Position und Flugrichtung der Gefechtsteilnehmer zu ermitteln.
- **Stören (Jamming):** Der Gegner unterbindet die Kommunikation durch das Aussenden von Störsignalen auf der gleichen Frequenz.
- **Täuschen:** Der Gegner verändert die Meldungen beziehungsweise speist Falschmeldungen in die Kommunikationskette ein.

Sowohl die übertragenen Informationen als auch die benutzten Kommunikationskanäle müssen durch adäquate Massnahmen gegen obige Bedrohungen wirksam geschützt werden.

TRANSEC und Frequency-Hopping

Die Sprach- und Datenkommunikation während des Gefechts sind überlebenswichtige Komponenten im Lufteinsatz. Aller automatisierten elektronischen Datenübermittlungs-, Feuerleit- und Steuerungssysteme zum Trotz bleibt die Sprachkommunikation «in der Hitze des Gefechts» die erste Wahl in der Kommunikation zwischen dem Piloten, seinen Mitstreitern und dem TFC.

Bei der Datenkommunikation, im Rahmen derer Sensordaten verschiedener Systeme an mehrere unterschiedliche Missionsteilnehmer übertragen werden müssen, gelangt wie erwähnt das TDMA-Verfahren zum Einsatz: Jedes teilnehmende System erhält im periodisch zu übertragenden Datenblock einen Zeit-Slot zugewiesen, in dem es seine Daten einfügt.

Verschiedene TRANSEC (Transmission Security)-Massnahmen ermöglichen es, die Kommunikation vor Jamming zu schützen und eine Ortung massgeblich zu erschweren. Besonders durchgesetzt hat sich bei der Sprach- und Datenübermittlung im Gefecht das Frequency-Hopping: Das Funkgerät sendet nicht auf einer konstanten Frequenz, sondern «springt» mehrmals pro Sekunde innerhalb des definierten Frequenzbands. Anpeilungen und Jamming auf einer bestimmten Frequenz werden hierdurch erheblich behindert. Eine situationsbedingte Anpassung der Sendeleistung optimiert zudem eine stabile Verbindung gegenüber der Detektierbarkeit.

COMSEC und Chiffrierung

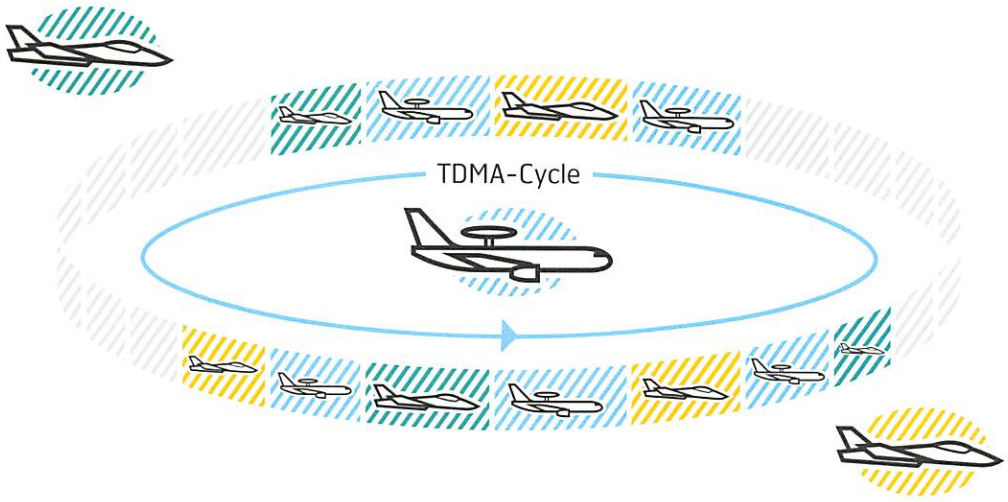
Die übermittelten Informationen beinhalten üblicherweise keine «Staatsgeheimnisse», ein Mithören durch den Feind kann aber dennoch empfindliche Auswirkungen auf das Geschehen haben. Weitaus gravierender sind die Konsequenzen, wenn der Gegner durch Verfälschen der Meldungen aktiv in die Kommunikation eingreift und hierdurch beispielsweise Flieger umleitet oder Schussbefehle manipuliert.

Eine abhörsichere Verschlüsselung von Sprache und Daten bietet hierbei wirksam Schutz für die Kommunikationssicherheit (Communication Security – COMSEC). Die abgehörten Meldungen sind für den Gegner nicht interpretierbar und somit nutzlos. Zudem kann er keine abgeänderten Meldungen in den verschlüsselten Kreislauf einspeisen.

Air Operations Centre:
Die Schaltzentrale der Lufteinsätze

Das Air Operations Centre (AOC) stellt das zentrale taktisch-operative Führungsinstrument einer Luftwaffe dar. Die Betriebsabläufe sind in der durch die NATO beeinflussten Welt weitgehend standardisiert. Das Kommando liegt beim Chef Einsatz des Führungsstabes Luftwaffe (FST LW), auch als Air Component Command (ACC) bezeichnet. Der Arbeitsrahmen wird durch die Air Operation Directive (AOD) – ein übergeordneter «Betriebsbefehl» für die Luftwaffe – sowie die Rules of Engagement (ROE) – die Bedingungen für den Waffen- beziehungsweise Kampfeinsatz – vorgegeben.

Das schweizerische AOC umfasst die drei Bereiche Einsatzplanung, Einsatzführung und Einsatzsupport. Aufgrund der Nähe des AOC zu den relevanten Einsatzzentralen kann der FST LW in Echtzeit in das Geschehen im Luftraum eingreifen. Die Arbeitsergebnisse des AOC beziehungsweise des ACC sind der Air Tasking Order (ATO), worin die einzelnen Flüge in einem Tageszeitrahmen detailliert geplant sind, sowie der Airspace Control Order (ACO) und die Special Instructions (SPINS), worin die Ziele für die Luftraumüberwachung sowie allfällige Anweisungen für Sondersituationen festgehalten sind. Eine Spezialsituation stellt beispielsweise die Gewährleistung der Sicherheit eines internationalen Anlasses mit Regierungsvertretern wie dem World Economic Forum (WEF) im schweizerischen Davos dar.



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.

100 Jahre Schweizer Luftwaffe: Das Militär erobert den Luftraum

Bei vielen Streitkräften weltweit geniesst die Luftwaffe ein hohes Prestige und übt auf die Beobachter eine besondere Faszination aus – sind die Flugzeuge und die weiteren Fluggeräte doch mit hoch entwickelter und komplexer Technologie ausgestattet. Die Ausbildung der Piloten, aber auch des Unterstützungspersonals, ist anspruchsvoll und langwierig. Die Schweizer Luftwaffe konnte im Juli 2014 ihr hundertjähriges Bestehen feiern. Für die Crypto AG ist dies ein Anlass, die spannende Geschichte der militärischen Luftfahrt in diesem Land und im Allgemeinen nachzuzeichnen.

Ralf Winzer | Customer Segment Manager

«Was geschieht hinter dem Hügel?» Diese Frage eines jeden Befehlshabers im Gefecht fand eine ganz neue Art der Beantwortung, als es für Menschen möglich wurde, in die Lüfte aufzusteigen.

Bereits im Jahr 1891 entdeckte die Schweizer Armee (gemeinsam mit einigen weiteren europäischen Armeen) den Luftraum als Einsatzgebiet. Der Generalstab beschloss die Beschaffung von Fesselballons zur Unterstützung der Aufklärung durch die Kavallerie. Mit viel Pioniergeist wurde die erste Luftschiffereinheit ausgebildet und ausgestattet. Die Kugel- und Drachenballons wurden mit feldmässig erzeugtem Wasserstoff befüllt, stiegen mit einem am Boden verankerten Seil auf und ermöglichten die erste Form von Luftaufklärung, deren Erkenntnisse beim Aufkommen des neuartigen Feldtelefons in Echtzeit an die Bodentruppen übermittelt werden konnten. Die Aufklärung bildete somit den ersten und auch heute noch wesentlichen Einsatzzweck der Luftstreitkräfte weltweit.

Drachenballon, im Volksmund auch «Bundeswurst» genannt (undatierte Aufnahme während des Ersten Weltkrieges 1914 – 1918)

Hawker im Duett: Schweizer Hunter T Mk 68 mit australischer Sea Fury im Show-Flug an der AIR14 in Payerne

Mit dem sich abzeichnenden Ersten Weltkrieg beschleunigten sich nicht nur die politischen Ereignisse, auch das Militär musste sich mit rasch verschiebenden Fronten und schnellen Truppenbewegungen auseinandersetzen. Der Nutzen von Fesselballons wurde daher in Frage gestellt. Gleichzeitig zeigten mehrere Flugpioniere in ganz Europa und den USA ihre ersten funktionsfähigen Flugzeuge, deren potenzieller Nutzen dem Militär nicht verborgen blieb. So beauftragte der Schweizerische Bundesrat am 31. Juli 1914 den Kavallerie-Hauptmann und leidenschaftlichen Piloten Theodor Real mit der Erschaffung einer Fliegertruppe. Eine unter der Bevölkerung durchgeführte Spendenaktion ermöglichte die Finanzierung dieses Vorhabens. Hauptmann Real konnte neun Flugpioniere motivieren, die ihre privaten Maschinen einbrachten. Mit dem Krieg sah sich die Schweiz gezwungen, eine eigene Luftfahrtindustrie aufzubauen, da die in Deutschland bestellten Maschinen nicht mehr ausgeliefert werden konnten. So entwickelte der Rüstungsbetrieb K+W in Thun im Kanton Bern mit dem DH-1 einen Doppeldecker mit Doppelrumpf für Aufklärungsaufgaben.

In der Zwischenkriegszeit wurde die wachsende Bedeutung der Luftkriegsführung erkannt, die Fliegertruppe avancierte zur vollwertigen Waffengattung und baute ihre Bestände an Flugmaterial sukzessive aus. Im durch die Weltkriege konfliktbehafteten Umfeld erweiterten sich die Aufgabenfelder der Luftstreitkräfte kontinuierlich: Neben der Aufklärung kamen kampfunterstützende Massnahmen wie die Sicherung des Luftraums, die Kontrolle von feindlichem Luftraum und die Bekämpfung von Erdzielen hinzu.

Seit 1935 entwickelte sich des Weiteren eine mit 20-mm-Kanonen ausgestattete wirksame Fliegerabwehr. Bei Ausbruch des Zweiten Weltkrieges war die Schweizer Luftwaffe bereits mit 86 Jagd- sowie 121 Beobachtungs- und Erdkampfflugzeugen ausgestattet, insbesondere Messerschmitt Me-109 und Morane D-3800. In diesem Zeitraum wurden zudem die Transportflugzeuge Junker Ju-52 beschafft, von denen vier Exemplare auch heute noch unter der liebevollen Bezeichnung «Tante Ju» für Rundflüge eingesetzt werden.

Die Schweizer Luftwaffe war ab diesem Zeitpunkt in der Lage, die drei Aufgaben wahrzunehmen, die sie auch heute noch hat: Nachrichtenbeschaffung, Schutz des Luftraums und Lufttransporte.

Im Rahmen der Verteidigung des schweizerischen Luftraums kam es wiederholt zu Kampfhandlungen zwischen schweizerischen und fremden Flugzeugen. Neben der eigentlichen Fliegertätigkeit mussten auch die erforderliche Logistik sowie ein geeignetes Führungsinstrumentarium für die Luftwaffe aufgebaut werden. So lieferten während der Mobilmachung ab dem Jahre 1939 221 bodenbasierte Beobachtungsposten

Angaben über den Luftraum und andere militärisch relevante Ereignisse und erstellten das Luftlagebild. Radartechniken waren zum damaligen Zeitpunkt noch weitgehend unbekannt. Die Flieger verständigten sich per Sprechfunk mittels eines ausgeklügelten Systems, dem «Bambini-Code». Zweck dieser «Kindersprache» war – im Gegensatz zur heutigen verschlüsselten Kommunikation – nicht das Verbergen der Meldungsinhalte, sondern eine möglichst gute Verständlichkeit in lärmiger Umgebung dank einfacher und eindeutiger Schlüsselwörter. So setzten sich die «Angeli» (eigene Flugzeuge) gegen die «Diaboli» (feindliche Flugzeuge) zur Wehr. Die Luftwaffe verfügte für ihre Missionen über «Bibis» (Jagdflugzeuge) und «Camions» (Transportflugzeuge). Ein Funkspruch an die «Bambini» richtete sich an alle; man flog in Richtung «Norwega» (Norden), «Atlanta» (Westen), «Sudan» (Süden) oder «Mekka» (Osten). Nach dem Einsatz begaben sich die Piloten mit «Ritorno Casino» zurück zu ihrer Basis, wo sie ihren Flugzeugen auf dem «Campo» (Flughafen) einen «Campari» gönnten (auftankten).

> Die Schweizer Luftwaffe war in der Lage, die Aufgaben wahrzunehmen, die sie auch heute noch hat: Nachrichtenbeschaffung, Schutz des Luftraums und Lufttransporte.

Nach dem nahezu nahtlosen Übergang vom Zweiten Weltkrieg zum Kalten Krieg stiegen die Anforderungen an die militärische Luftfahrt. Höhere Geschwindigkeiten und Flughöhen wurden notwendig, um der immer leistungsfähigeren Flugabwehr entkommen und den Einsatzort zeitnahe erreichen zu können. Gleichzeitig mussten die Maschinen langsam und bodennah Beobachtungen und allenfalls Angriffe auf Bodenziele durchführen können. Ab den 1950er Jahren erlangte die militärische Fliegerei und deren Abwehr eine tragende Bedeutung in den Militärdoktrinen.

Entsprechend musste der Propeller dem Düsentriebwerk weichen. Wie andere Länder auch, rüstete die Schweizer Armee markant auf und stattete sich sukzessive mit einstrahligen Kampfflugzeugen englischer Herkunft aus. In diesem Kontext erwies sich insbesondere der Hawker Hunter als eines der fortschrittlichsten und wendigsten Jagdflugzeuge seiner Zeit. So erstaunt es nicht, dass die schweizerische Kunstflugstaffel, die Patrouille Suisse, die Wendigkeit des Hunters in kühnen Manövern bis heute immer wieder zur Schau stellt.

Die Technologie und die Luftfahrt entwickelten sich rasant weiter. In den 1960er Jahren stand bereits die nächste Erneuerungswelle an. Die Militärführung entschied sich für die französische Mirage III von Dassault, eine Maschine, die mit ihrer charakteristischen dreieckigen Tragfläche die doppelte Schallgeschwindigkeit erreichen und in spezialisierten Versionen sowohl für die Luftaufklärung als auch als Abfangjäger eingesetzt werden konnte. Im Zeitraum 1975 – 1985 wurde die fliegerische Kampfflotte mit circa 100 F5-Tiger-Jagdflugzeugen (Typ E und F) von Northrop aufgefrischt.

In den 1990er Jahren beschlossen die politischen Gremien nach kontroversen Diskussionen zwischen Armeegegnern und -befürwortern und einer Volksabstimmung, in der Letztere die Oberhand gewannen, die Beschaffung von 34 Kampfflugzeugen des Typs F/A-18 Hornet von McDonnell Douglas (unterdessen Boeing). Mit dem F/A-18 verfügt die Schweiz aktuell über ein polyvalentes Kampflugzeug der vierten Generation, dessen Bordelektronik über die im heutigen Kampfgeschehen erforderlichen Fähigkeiten verfügt (Radar, Feuerleitsystem, Früherkennung feindlicher Zielerfassung, Täuschung des gegnerischen Feuerleitsystems usw.). Der F/A-18 übernimmt hiermit als Nachfolger der Mirage IIIS die Verteidigung des schweizerischen Luftraums.

Die historische Entwicklung der Luftwaffe zeigt beispielhaft auf, welche Auswirkungen technologische Entwicklungen auf militärische Handlungsweisen im Allgemeinen, aber auch auf die Ausrüstung an Einsatzmitteln mit sich bringen. Im letzten Weltkrieg und in der darauf folgenden Ära des Kalten Krieges waren hunderte Maschinen in der Verteidigung des Luftraumes eines kleinen Landes wie der Schweiz im Einsatz. Angesichts der heutigen Radaranlagen, Luftabwehrdispositivs und Informationsbeschaffungs- und Auswertungssystemen kann die gleiche Aufgabe gegenwärtig durch wenige Dutzend Flugzeuge bewerkstelligt werden.

Die Geschichte der militärischen Luftfahrt zeigt beispielhaft, wie Menschen und Unternehmen dank technologischen Spitzenleistungen sowie grossem Enthusiasmus herausragende Leistungen in einem sich rasant weiterentwickelnden Umfeld hervorbringen können, sei dies in der eigentlichen Aviatik, in der Informationsbeschaffung und im Bereich der Kommunikationstechnologien. Die weitere technische Entwicklung im Umfeld der Landesverteidigung wird mit Sicherheit auch in Zukunft spannende Neuerungen mit sich bringen, zu denen es die Crypto AG weiterhin nicht unterlassen wird, ihren Beitrag zu leisten.

Taubenkorb für Radfahrer- und Gebirgstruppen (1917)

Eine andere Art der Übermittlung: Brieftauben im Militär

Die Taube wurde bereits in der Antike als Trägerin und Übermittlerin von Botschaften eingesetzt. Das kluge Tier ist in der Lage, den Weg zurück in seinen «Heimatschlag» zu finden, wenn es an einem entfernten Ort ausgesetzt wird. Die Taubentürme der damaligen Republik Genua oder die Verkündung des Sieges in Waterloo durch die Engländer im Jahr 1815 per «Luftpost» zeigen, dass sich auch das Militär die Fähigkeiten der gefiederten Tierchen für die Langstreckenübermittlung von taktischen Nachrichten geraume Zeit zunutze gemacht hat. Die Schweizer Armee gründete im Jahr 1917 einen Brieftaubendienst, der 1951 in die regulären Übermittlungstruppen integriert wurde. Die Vögel fanden autonom ihren Weg, waren flink und brauchten sich kaum vor der feindlichen «Luftabwehr» zu fürchten. Die Tauben erwiesen sich als ein derart effizientes Kommunikationsmittel, dass die letzten 30'000 schweizerischen gefiederten Angehörigen der Armee erst im Jahr 1996 aus dem Dienst entlassen und einer gemeinnützigen Stiftung übergeben wurden.

«Sicherheit ist ein Prozess stetiger Verbesserungen»

Interview mit Korpskommandant Aldo C. Schellenberg, Kommandant der Schweizer Luftwaffe

Das Interview führte Casha Frigo Schmidiger | Publizistin

Die Schweizer Luftwaffe hat eine breite Aufgabenpalette in der ordentlichen wie in der ausserordentlichen Lage. So nimmt sie nicht nur die Wahrung der Lufthoheit wahr (darin enthalten sind Luftpolizeidienst und Luftverteidigung), sondern verfolgt weitere vielfältige Aufgaben wie den Lufttransport sowie die Verbreitung von Informationen für politische und / oder militärische Instanzen. Welche Rolle spielt für Sie dabei ein funktionierendes Führungs- und Informationsnetz und welchen Stellenwert hat der Schutz der darauf verarbeiteten Informationen?

Der Einsatz der Schweizer Luftwaffe (LW) basiert auf einem Systemverbund bestehend aus Sensoren, Effektoren, Führungssystemen, Flugplätzen, Kommunikationsmitteln und Luftfahrzeugen. Die heute praktizierte Echtzeitführung verlangt nach einem funktionierenden Führungs- und Informationsnetz. Informationen werden in Applikationen verarbeitet, sodass sowohl die Applikationssysteme wie die Übertragungsnetze entsprechend der Klassifikation der Informationen geschützt werden müssen. Der Schutz der Informationen ist zwingend, damit weder in der Informationskette von den Sensoren zu den Effektoren noch in der Befehlskette von der Einsatzzentrale bis zum Kampfflugzeug Fehler passieren.

Welche Risiken bestehen, dass der Informationsaustausch zwischen Sensoren und Effektoren von aussen beeinflusst werden kann – und welche Folgen könnte das haben?

Da die Applikationssysteme wie auch die Übertragungsnetze von der Aussenwelt entkoppelt sind, neigt man dazu, die Risiken für die Beeinflussung von aussen als gering einzustufen. Für die Abschätzung des Risikos muss man verstehen, mit welchen Methoden ein entkoppeltes System angegriffen werden kann. Vermutlich die grösste Gefahr ergibt sich durch die unachtsame Verwendung von Speichermedien, mit denen Malware ins System eingeschleust werden kann. Aus Medienberichten weiss man, dass Angriffe auf «gegnerische» Systeme verübt wurden. Über solche – vermutlich von Geheimdiensten verübten – Aktionen sind kaum erhärtete Fakten bekannt. Der Schaden kann jedoch enorm sein, weil im Extremfall ganze Systeme lahmgelegt werden. Besonders gravierend scheint, dass man sich durch das einwandfreie Funktionieren der Systeme im täglichen Einsatz in trügerischer Sicherheit wähnt.

Auf vielen einzelnen Komponenten wie dem FLORAKO (einem Schweizer Radarsystem für die Luftraumüberwachung) basiert auch das Führungs- und Informationssystem der Luftwaffe (FIS LW). Welche operativen Möglichkeiten gibt es Ihren Kommandanten an die Hand und welche sollen in der nächsten Zukunft noch dazukommen?

FIS LW unterstützt mit seinen vielseitigen und massgeschneiderten Werkzeugen sowohl die Stabsarbeit als auch die Einsatzplanung und Einsatzführung der Luftwaffenmittel. Zudem bietet es die Möglichkeit, Einsätze zu überwachen und auszuwerten. Mittels der Kommandoführung auf FIS LW werden Grund- und Einsatzbefehle erfasst, verwaltet und verteilt, egal ob der Empfänger in einer Führungsanlage, auf einem Flugplatz, teilmobil mit Richtstrahl erschlossen oder im Ausland über Satellit eingebunden ist. Die FIS-LW-Einsatzleitung steuert Fliegereinsätze von der Mittelbereitstellung über die Flugvorbereitung bis zum Start und nach der Landung über die Retablierung bis hin zu Auswertungen und Statistiken. Egal ob Jagdflugzeuge zum Luftpolizeidienst befohlen werden, eine Stinger-Batterie zum dynamischen Flab (Fliegerabwehr)-Schutz aufgeboten wird, Nachrichtenverbände zu Dutzenden von Beobachtungsposten geschickt werden oder Transporthelikopter abgeschnittene Dörfer versorgen sollen – immer ist FIS LW das System, über welches die Planung und Befehlsgebung erfolgt. Ob eine Air Operation Directive verfasst wird oder der Beginn einer Flugzeugbereitstellung signalisiert wird: Es ist immer das gleiche FIS LW mit flexibel konfigurierbaren Rollenberechtigungen. FIS LW läuft seit 2003 an 365 Tagen im Jahr während 24 Stunden – auch wenn die Luftwaffe ihre Aufträge Luftpolizeidienst und SAR (Search and Rescue) Tag für Tag wahrnimmt. Sollte sich die Lage einmal verschärfen, muss nichts geändert oder ausgetauscht werden – dasselbe FIS LW wird bis hin zum Verteidigungsfall eingesetzt.

Korpskommandant Aldo C. Schellenberg
(*1958) studierte Wirtschaftswissenschaften an der Universität Zürich und promovierte zum Dr. oec. publ. Er war Inhaber einer Unternehmungsberatungsfirma. Seit 2013 ist Schellenberg Kommandant der Schweizer Luftwaffe.

Wie rüstet sich die Luftwaffe bei Spezialeinsätzen wie dem jährlich in Davos (Schweiz) stattfindenden World Economic Forum (WEF)? Welche Rolle spielt hier die Wahrung der Informationshoheit?
Die Cyberbedrohung ist real. Schwerwiegende Auswirkungen können Cyberangriffe vor allem dort haben, wo sie Operationen und Infrastrukturen gefährden können. Deshalb werden bereits bei der Konzeption und Beschaffung von Systemen die notwendigen Sicherheitsmechanismen eingebaut, damit Cyberangriffe keinen Erfolg haben. Für die Einsatzführung der Luftfahrzeuge ist eine eindeutige, identifizierte Luftlage notwendig. Daher wird alles unternommen, um die Integrität wie auch die Übertragungssicherheit der Daten sicherzustellen. Da die gleichen Systeme für die Einsatzplanung und Einsatzführung im täglichen Betrieb wie auch für «Spezialeinsätze» verwendet werden, sind im Bereich der Informationssicherheit keine zusätzlichen technischen Massnahmen erforderlich.

Stichwort Cyberattacken: Was kann die Schweizer Armee Ihrer Meinung nach tun, um sich vor Cyberattacken zu schützen?
Die Armee muss permanent in der Lage sein, Cyberbedrohungen zu erkennen, sich davor zu schützen und diese abzuwehren. Dazu sind die folgenden Prozesse zu implementieren und zu beherrschen:

- Führung, um jederzeit und dauernd in der Lage zu sein, die Cyberabwehr, sowohl in der Grundbereitschaft wie auch in der Einsatzbereitschaft der Armee, sicherzustellen und zu steuern. Dafür sind die benötigten Partner und Leistungserbringer bestmöglich einzusetzen.
- Antizipation, um mögliche Cyberbedrohungen frühzeitig zu erkennen, damit die notwendigen Entscheidungen gefällt und entsprechende Massnahmen geplant werden können.
- Prävention, die es erlauben soll, in allen möglichen Bereichen (technisch, organisatorisch, menschlich usw.) die durch Cyberbedrohungen bedingten Risiken zu verringern und die Einsatzfähigkeit der Armee jederzeit sicherzustellen.
- Reaktion, die Auswirkungen sowohl im technischen als auch nicht technischen Bereich zu eruieren und die Einsatzfähigkeit der Armee wiederherzustellen.

Diese Prozesse müssen in allen Lagen umgesetzt werden können, selbst in einem stark gestörten Cyberraum.

Werden in der Armee strategische und taktische Informationen bezüglich der Sicherheit unterschiedlich behandelt?
Ja. Die Klassifizierung von strategischen und oder taktischen Informationen werden dem Informationsgehalt und ihren Bedeutungen in Bezug auf eine Operation entsprechend klassifiziert. Entsprechend der Klassifizierung ist die Handhabung unterschiedlich. Das hat wiederum Einfluss auf das Design der technischen Systeme.

Wie sicher ist unser Luftraum heute?
Die Schweiz liegt an verschiedenen Kreuzungspunkten internationaler Luftstrassen. Das hat einen der komplexesten und dichtesten Lufträume in Europa zur Folge. Über eine Million Instrumentenflüge führen jährlich durch den Schweizer Luftraum, ein Teil davon als Transit, aber über 450'000 Flüge gehen zu oder von einem Schweizer Flughafen. Der Instrumentenflugverkehr wird rund um die Uhr von zivilen und militärischen Radars überwacht und von Flugdienstleitern geführt.

Das strikte Einhalten der Luftfahrtvorschriften ist unerlässlich und muss permanent kontrolliert und wenn nötig durchgesetzt werden. Letzteres ist eine hoheitliche Aufgabe des Staates und aus diesem Grund ist die Luftwaffe per Gesetz mit der Wahrung der Lufthoheit betraut.

Wie die Polizei am Boden, führt die Luftwaffe im Luftraum präventive Kontrollen durch, greift bei technischen Problemen (z. B. Ausfall von Transpondern oder Kommunikationssystemen) helfend ein oder interveniert mit ihren Kampfflugzeugen bei gravierenden Verletzungen der Luftfahrtvorschriften und bei Grenzverletzungen durch staatliche Luftfahrzeuge. Präventive Kontrollen finden fast täglich statt, während sogenannte Hot Missions ein- bis zweimal pro Monat erfolgen. Unfälle lassen sich aber nie ganz ausschliessen – absolute Sicherheit gibt es nicht. Sicherheit ist denn auch kein statischer Zustand, sondern ein Prozess stetiger Verbesserungen. Jeder sicherheitsrelevante Vorfall muss genau analysiert werden und wenn nötig zu Massnahmen zur Verbesserung der Sicherheit führen. Die Luftwaffe leistet dazu einen wesentlichen Beitrag. Bis 2020 wird im Sinne einer Optimierung der «Luftpolizeidienst24» (LP24) – Bereitschaft während 24 Stunden an 365 Tagen – eingeführt.

Unbemannte Aufklärung aus der Luft

Luftfahrzeuge stellen ein privilegiertes Mittel der Aufklärung – der Beschaffung von relevanten Informationen ausserhalb des eigenen Einflussbereiches – dar. Ausserhalb des eigenen Einflussbereiches zu operieren setzt aber voraus, möglichst diskret, flexibel und rasch agieren zu können und eigene Mittel – insbesondere Menschen – keinen vermeidbaren Risiken auszusetzen. Unbemannte Flugobjekte beziehungsweise Drohnen bieten hierbei interessante Möglichkeiten.

Ralf Winzer | Customer Segment Manager

Kenntnisse über die Umgebung sind in einer Konfliktsituation von eminenter Bedeutung: Jeder Einsatzleiter, militärische Befehlshaber oder politische Unterhändler ist zur erfolgreichen Erfüllung seiner Aufgabe darauf angewiesen, in Erfahrung zu bringen, was beim Kontrahenten vorgeht, wie das Terrain beschaffen ist, kurz: zu wissen, was ihn «hinter dem Hügel» erwartet.

Mit dem Aufkommen der Luftfahrt hat sich auch die Luftaufklärung entwickelt, das heisst die Möglichkeit, Landbeschaffenheit und Truppenbewegungen von der Luft aus beobachten zu können, ohne zuerst bodenbezogene Hindernisse mühsam überwinden zu müssen. Doch die militärische Aviatik hat ihren Preis: Jagdflugzeuge, Militärhelikopter und ähnliche Fluggeräte sind äusserst komplex in der Entwicklung, kostspielig in der Anschaffung, benötigen eine umfangreiche Unterhaltslogistik und erfordern Flugplätze, deren Landebahnen von weitem erkennbare Zielscheiben für gegnerische Handlungen darstellen. Die grössten Bemühungen gelten jedoch der umfangreichen Ausbildung der Piloten, die in der Lage sein müssen, ihre überschallschnellen Maschinen jederzeit perfekt zu beherrschen und ihren jeweiligen Auftrag erfolgreich zu erfüllen.

Aufklärungs-Drohnen-System ADS 95 der Schweizer Armee*: Konsole der mobilen Bodenkontrollstation: Bedienung der Sensoren mit Auswerter-Arbeitsplatz (links), Navigation und Landkarten (Mitte), Fluginstrumente mit Piloten-Arbeitsplatz (rechts)

Was liegt näher als der Wunsch nach einem leichten Fluggerät, das sich vom Boden aus steuern lässt oder das in der Lage ist, autonom zu fliegen? Die Vorteile dieser Unmanned Aerial Vehicles (UAV) oder Remotely Piloted Aircrafts (RPA) sind offensichtlich:

- Ausschliesslich mit Aufklärungstechnologie ausgestattet, sind RPAs leicht und zudem günstig in der Anschaffung und im Betrieb.
- Die erforderliche Infrastruktur (Startrampe, Lenkungssystem) ist minimal.
- Die Fluggeräte sind sehr wendig und können gegnerische Radare im Konturenflug (sehr tief über dem Boden fliegend) «unterfliegen».
- Mit leisen Rotoren und Nachtsichtgeräten ausgestattet, sind RPAs äusserst diskret unterwegs.
- RPAs entsprechen aufgrund ihrer geringen Masse momentan (noch) nicht dem «Beuteschema» der üblichen Luftabwehr.
- Der Pilot befindet sich in sicherer Entfernung am Boden unmittelbar neben dem Auswerter, der die Sensoren bedient und die übermittelte Aufklärungsinformation analysiert und weiterleitet.

* Die in diesem Text dargestellten Einsatzszenarien beziehen sich weder auf das ADS 95 noch auf die Aufgaben der Schweizer Armee.

RPAs können Luftaufklärung im sichtbaren Bereich, aber auch im Infrarotspektrum oder in anderen Messbereichen liefern. Des Weiteren können schwere Geräte durchaus auch mit Waffen und Feuerleitsystemen bestückt werden.

Airborne Surveillance wird sowohl für militärische als auch für Polizei- und Grenzschutzzwecke eingesetzt. Vor allem letztere zwei Aufgaben erfolgen zunehmend durch den Einsatz von Drohnen. Diese funktionieren ähnlich wie ein Modellflugzeug. Der wesentliche Unterschied liegt darin, dass das Spielgerät nur in Sichtweite dirigiert werden kann, während eine Drohne via mobile oder fixe Bodenkontrollstation gesteuert wird. Die Bedienungskonsole der Bodenstation umfasst typischerweise drei Bereiche. Der Surveillance-Bereich zeigt die von den Sensoren empfangenen Aufklärungsinformationen (insbesondere die Bilder der Kameras) und erlaubt dem Auswerter, die Sensoren zu steuern beziehungsweise Kameras auszurichten und relevante Details heranzuzoomen. Der Steuerungsbereich – ähnlich ausgestattet wie ein Flugzeugcockpit mit Kompass, Höhen- und Geschwindigkeitsmesser usw. – erlaubt es dem Piloten, die Drohne zu dirigieren. Die Pilotenarbeit erfordert bei den heutigen RPAs hauptsächlich die Eingabe von Flugrichtung und -höhe (vergleichbar mit dem Autopiloten eines Flugzeugs). Die Stabilisierung in der Luft erfolgt automatisch. Der Start erfolgt zuweilen über eine Art Katapult; die Landung geschieht durch ein – dem zivilen ILS (Instrument Landing System) ähnlichen – Funkleitsystem weitgehend selbstständig. Der dritte Konsolenbereich bietet dem Piloten und dem Auswerter verschiedene Navigationshilfen und Landkarten.

Die durch die Sensoren der Drohne gewonnenen Daten werden typischerweise in Echtzeit an die Einsatzleitung beziehungsweise das Operations Centre übermittelt, wo diese Informationen analysiert werden und in das Lagebild (Common Relevant Operational Picture – CROP) einfliessen.

Aufklärungs-Drohnen-System ADS 95 der Schweizer Armee*: Ranger-Drohne mit Startrampe

Drohnen haben in den vergangenen Jahren an militärischer Bedeutung gewonnen. Manche Analysten sehen in ihnen das Symbol für einen Wandel in der Kriegsführung. Einige gehen in ihrer Annahme sogar so weit, dass Drohnen eines Tages die Kampf- und Logistikfunktionen bemannter Luftfahrzeuge weitgehend übernehmen werden.

> Die Datenübermittlung zwischen Drohne und Bodenkontrollstation sowie zwischen Bodenkontrollstation und Operations Centre ist das Rückgrat eines jeden Drohnensystems.

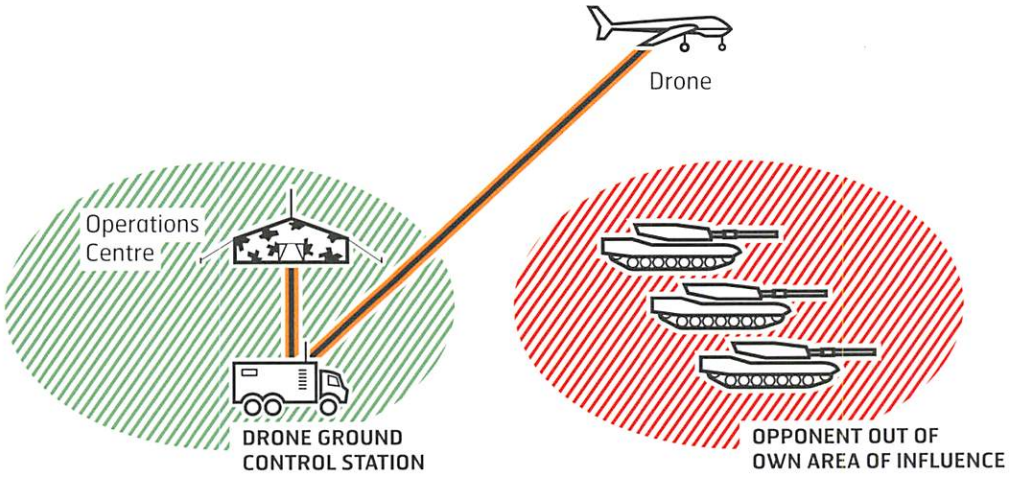
Drohnen lassen sich in drei Kategorien unterteilen: Strategische Drohnen werden für die weiträumige Aufklärung über feindlichem Gebiet eingesetzt. Dazu gehören Systeme wie der RQ-4 Global Hawk von Northrop Grumman, der auf einer maximalen Flughöhe von 20'000 Metern bis zu 40 Stunden operiert und eine Reichweite von 3'000 Seemeilen hat. Zu den operativen Drohnen gehören die MQ-1 Predator und MQ-9 Reaper von General Atomics. Sie werden in militärischen Einsatzgebieten verwendet und können sowohl zur Aufklärung als auch zu Angriffszwecken genutzt werden. Taktische Drohnen schliesslich bewegen sich in geringer Flughöhe auf kurzen Strecken. Ihre Hauptfunktion besteht darin, Befehlshabern vor Ort die Überwachung feindlicher Aktivitäten zu ermöglichen, ohne dabei eigene Soldaten zu gefährden. Ein Beispiel hierfür ist der RQ-14 Dragon Eye von MCWL. Im Gegensatz zu strategischen und operativen Drohnen, die entweder ferngesteuert oder für den autonomen Flug vorprogrammiert werden können, werden taktische Drohnen stets über Operateure in der Bodenkontrollstation gesteuert. Sie werden auch häufig von Polizeikräften zur Kontrolle von Menschenmassen und zur Grenzüberwachung eingesetzt.[1]

Drohnen liefern sowohl in der Landesverteidigung, bei der Terrorbekämpfung, der Polizeiarbeit (beispielsweise bei Demonstrationen und Unruhen) sowie beim Grenzschutz wertvolle Arbeit. Diskret und zeitnah gelangen sie an den Ort des Geschehens. Wesentlich relevanter ist jedoch die Tatsache, dass sich bei einem solchen Einsatz kein Mensch einer unmittelbaren Gefahr aussetzen muss.

Die Datenübermittlung zwischen Drohne und Bodenkontrollstation sowie zwischen Bodenkontrollstation und Operations Centre ist das Rückgrat eines jeden Drohnensystems. Dieses muss möglichst unanfällig gegen Störungen und unerlaubtes Abhören sein. Ein potenzieller Gegner soll die Drohne weder manövrierunfähig machen, deren Steuerung übernehmen noch die von ihr erfassten Daten abfangen können.

Während der Schutz vor Störungen beziehungsweise vor Jamming durch Frequency-Hopping und ähnliche Verfahren gewährleistet wird, bedingt der Schutz vor unerwünschtem Abhören eine wirksame Verschlüsselung, welche die Übermittlungsrate des Datentransfers in keinster Weise beeinträchtigt. Drohnen zeigen in dieser Hinsicht anschaulich die Bedeutung einer hochsicheren Datenübermittlung.

Quelle:
[1] ETH Zürich, CS, 2010: Analysen zur Sicherheitspolitik



Die Drohne liefert – gesteuert über ihre Bodenkontrollstation – Informationen über gegnerische Truppenbewegungen. Die Bodenkontrollstation übermittelt die gewonnenen Informationen an das Operations Centre.

Personenschutz an Konferenzen: Sichere mobile Kommunikation ist unabdingbar

Eine Konferenz mit Spitzenpolitikern und weiteren Entscheidungsträgern bedeutet unvermeidlich ein Grossaufgebot an Sicherheitskräften. Der Aufwand, die persönliche Sicherheit der nationalen und internationalen Gäste und ihrer Delegationen garantieren zu können, ist beträchtlich. Das anvisierte Ziel muss «absolute Sicherheit» von der Anreise bis zur Abreise sein. Ein wesentlicher Erfolgsfaktor ist ein sicherer mobiler Kommunikationsverbund von Personenschützern mit engem Kontakt zum Mission Operation Centre und anderen komplementären Leistungserbringern.

Urs Kürzi | Customer Segment Manager

Der geladene Spitzenpolitiker landet mit seinem Jet auf einem privaten Flughafen ausserhalb der Wirtschaftsmetropole. Die Anreise des hochrangigen Gastes und seiner Delegation an die Konferenz ist bequem gestaltet: Die Gäste werden nach der Landung direkt an der Flugzeugtreppe mit einer Limousine abgeholt und unverzüglich in das extra für die Konferenz aufgebaute Zollbüro gefahren, um die Einreiseformalitäten, Personenkontrollen und die Zollabfertigung zu erledigen.

Der Personenschützer begrüsst die Gäste gleich nach der Einreise am Zollbüro und händigt seinem Pendant, dem Sicherheitsagenten des Spitzenpolitikers, ein sicheres Mobiltelefon aus. Der Personenschützer und der Sicherheitsagent des Konferenzteilnehmers sind dabei in derselben Kommunikationsgruppe. Das zivile Kommunikationsmittel, ein Mobiltelefon mit integriertem Chiffriermodul, fällt nicht weiter auf, beinhaltet in einem verschlüsselten Adressbuch jedoch alle Telefonnummern der Sicherheitskräfte und diverse Notfallnummern. Die Telefonnummern und die Namen der Sicherheitsfunktionäre sind dank der hardwarebasierten Verschlüsselung auf dem Smartphone gegen alle Attacken aus dem Mobilnetz geschützt, selbst bei Verlust des Gerätes. Die Handhabung des sicheren Mobiltelefons bedarf keiner Instruktion, weil es sich kaum von einem handelsüblichen Smartphone unterscheidet. Einmal in die sichere Applikation eingeloggt, ist die Bedienung intuitiv.

Auf der rund zwei Stunden dauernden Reise zum Austragungsort der Ministerkonferenz informiert der Personenschützer den Security Manager im Mission Operation Centre per verschlüsselte Textnachrichten über den Status des Konvois. Auf spontane Wünsche der Gäste kann unterwegs eingegangen werden, denn Abweichungen vom Tagesprogramm gehören für Personenschützer zum Alltag. Sie sind sich an spontanes Reagieren gewöhnt und verstehen es, Entscheide kurzfristig zu fassen. Die Fahrrouten werden den aktuellen Verkehrs- und Wetterbedingungen angepasst und dem Mission Operation Centre entsprechend kommuniziert. Die Checkpoints zum Konferenzort, welche unter der Verantwortung der Polizei geführt werden, lassen sich dank der vorgängigen Anvisierung speditiv passieren.

Die Personenschützer, in einer Spezialeinheit der Armee geführt, garantieren die Sicherheit der völkerrechtlich geschützten Personen und bewachen deren Unterkünfte. Das Konferenzgebäude hingegen wird vom Objektschutz der Armee gesichert. Diese Arbeit besteht im Wesentlichen aus der Identitätskontrolle der Personen sowie der Kontrolle der Ware, die in das und aus dem Konferenzgebäude geführt wird. Die Kontrollen und das Inspizieren des Materials bedeuten für die Mitarbeiter des Objektschutzes einen grossen Aufwand.

Einfache und pragmatische Vorbereitung grenzt Bedrohungen ein

Der erfolgreiche Schutz einer Konferenz beginnt bereits Monate vorher mit einer gründlichen Planung. Der staatliche Sicherheitsdienst erstellt eine genaue Liste über die anreisenden Spitzenpolitiker mit genauen Angaben über An- und Abreisezeiten, Flugnummern und einer detaillierten Meetings- und Referatsplanung. Auch das Gefährdungspotenzial und die geeigneten Schutzmassnahmen der jeweiligen Gäste werden vorgängig eruiert und mit ihren Sicherheitsagenten abgesprochen. Dieses Wissen minimiert ihre Gefährdung an der Konferenz massgeblich. In der Folge wird die Missionsinfrastruktur vorbereitet und die Alternativpläne werden mit den Sicherheitsdispositiven erfasst und in Einsatzpläne überführt.

Die Personenschützer nutzen aus Diskretionsgründen üblicherweise Smartphones, da diese den Anschein handelsüblicher Mobiltelefone machen. Ein zentraler Vorzug einer mobilen Voice-Lösung besteht darin, unvorhergesehenen Ereignissen zu folgen. Gerade dann sind die Sicherheitskräfte auf eine schnelle und sichere Sprachkommunikation angewiesen. Auf Wunsch können selbst die Konferenzteilnehmer mit verschlüsselten Smartphones ausgerüstet werden, sodass sie untereinander verschlüsselt sprechen und Textmeldungen austauschen können.

Ein weiterer wichtiger Sicherheitsaspekt ist die Geheimhaltung des Aufenthaltsorts der zu schützenden Konferenzbesucher sowie ihrer Personenschützer, die alle auch ihr eigenes Secure Smartphone mitbringen. Um zu vermeiden, dass diese Personen geortet werden können, empfiehlt es sich, temporär eine lokale Mobilnummer beziehungsweise SIM-Karte zu verwenden. Dies schliesst auch die Möglichkeit nicht aus, Anrufe nach Hause oder an eine beliebige Nummer im Herkunftsland zu tätigen – und zwar ohne Bekanntgabe des Aufenthaltsorts. Hierfür terminiert ein Gateway im Ministerium im Herkunftsland die verschlüsselten Anrufe und vermittelt diese weiter ins nationale Telefonnetzwerk.

Security Management Centre

Ein zentrales Kommunikationsmanagement ist unverzichtbar, da es speziell auf schnell ändernde Situationen ausgelegt ist. Möglich macht dies die Crypto Management Suite CMS-1200. Mithilfe derer werden die Kommunikationshierarchie definiert, Adressbücher erstellt, Teilnehmer in kryptografisch getrennte Gruppen (Crypto Domains) abgegrenzt, die dann in die Sicherheitsmodule der Smartphones übertragen werden. Das Handling beim Verlust von Geräten oder der Einbezug von Ad-hoc-Einheiten in ausserordentlichen Situationen werden von der Crypto Management Suite vollumfänglich unterstützt, sodass die Sicherheits-Policy unter allen Umständen durchgesetzt werden kann. Das Security Management bietet auch noch eine weitere Spezialität: Nur gemäss der definierten Kommunikationshierarchie autorisierte Personen beziehungsweise Vertreter einer definierten Benutzergruppe können mit den hochrangigen Konferenzteilnehmern in Verbindung treten.

> Die Sicherheitskräfte sind auf eine schnelle und sichere Sprachkommunikation angewiesen.

Wache im Luftraum

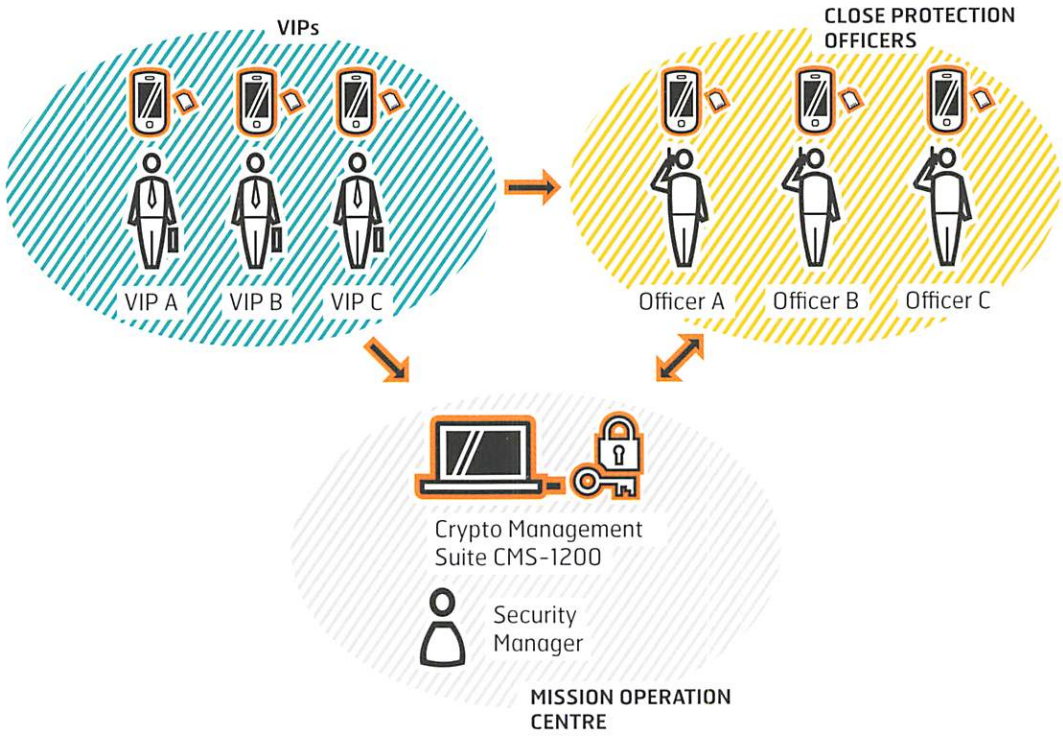
So viel zum Szenario auf dem Boden und zum direkten Schutz der Gäste. Für die Wahrung der Lufthoheit ist selbstredend die Luftwaffe zuständig. Während der Konferenz ist der Luftraum für sämtliche zivilen Flugzeuge gesperrt. Jede Regelverletzung im eingeschränkten Luftraum kann unverzüglich aufgeklärt werden. Hierfür starten vom nächsten Militärflugplatz Kampfjets der Armee für Patrouillenflüge, um die Luftraumüberwachung der Schutzzone durchzusetzen. Im Falle einer Verletzung des gesperrten Luftraumes (beispielsweise aufgrund Nichtwissens wegen mangelnder Flugvorbereitung der Piloten) sind die Kampfjets in wenigen Minuten in der Luft, identifizieren das Flugzeug, lassen vom Air Operation Centre die Identifikation mit dem zivilen Flugplan checken, nehmen mit dem Piloten Kontakt auf und eskortieren das Flugzeug aus der Sperrzone hinaus. Luftraumverletzungen dieser Art können eine Busse im fünfstelligen Dollarbereich nach sich ziehen. Zum Schutz von Konferenzen, an denen die hochrangigsten Entscheidungsträger aus Politik und Wirtschaft teilnehmen, muss die Luftwaffe aber auch für Abschüsse vorbereitet sein, wenn zweifellos Gefahr droht. Während der Konferenz begleitet den Verteidigungsminister stets ein Luftwaffenpilot als Verbindungsmann zum Air Operation Centre. Ignoriert der Pilot eines in den gesperrten Luftraum eingedrungenen Flugzeugs jeglichen Versuch, mit den Kampfjets Kontakt aufzunehmen, die mit Flügelschaukeln oder dem Abfeuern von Magnesium-Leuchtmunition klar machen, ihnen zu folgen, kann der Verteidigungsminister grundsätzlich einen Abschuss anordnen.

Die Luftwaffe stellt darüber hinaus nicht nur Helikopter für Geländesicherungsflüge, um die im Radarschatten liegenden Täler zu überwachen, sondern fliegt auch Personen- und Materialtransporte in die benachbarten Städte. Einzelne Helikopter sind für sogenannte SAR (Search and Rescue)-Einsätze ausgerüstet, um bei Unfällen die Rettung oder die medizinische Versorgung sicherzustellen. Für alle Eventualitäten stehen auch Helikopter mit Bordschützen zur Verfügung, um für eine Intervention gegen langsam fliegende Objekte bereit zu sein.

Koordination über Einsatzzentrale

Während der Konferenz herrscht in der Einsatzzentrale – oder Mission Operation Centre (MOC) – rund um die Uhr ein reger Betrieb – es kann treffend als «Nervenzentrum» der ganzen Operation bezeichnet werden. Das Telefon im MOC klingelt bedeutend häufiger, als es in einer regulären Einsatzzentrale der Fall ist. Der permanente Informationsaustausch und ein korrekter Meldefluss zu den Mitarbeitern im Mission Operation Centre sind entscheidend für den Erfolg und damit wesentlich für die Sicherheit der Konferenzteilnehmer. Darüber hinaus haben die Security Manager beste Kenntnisse über die lokale Beschaffenheit des Einsatzraumes. Dies ist unerlässlich, denn alle Meldungen, Gespräche, Lagebilder, Wettermeldungen, Luftüberwachungsbilder, Flug- und Einsatzpläne, Objektschutz, Transportaufträge, Verkehrsmeldungen bis zum VIP-Personenschutz werden in einem gemeinsamen Lagebild zusammengefasst und können von den Security Managern entsprechend interpretiert und mit der lokalen Beschaffenheit in Kontext gesetzt werden.

Beim privaten Flughafen ausserhalb der Metropole übernehmen die Personenschützer die Verantwortung für die Sicherheit, indem sie ihre Gäste im Auto begleiten oder den Konvoi aus der Luft überwachen.



Konfigurationsbeispiel einer bewährten Kommunikationshierarchie: Das Security Management Centre (Crypto Management Suite CMS-1200) unterstützt die Vorbereitung der Missionsinfrastruktur mit Secure Smartphones für die Personenschützer oder die flexible Reaktion auf sich schnell ändernde Situationen während einer «hot mission». Einfach und bequem lassen sich mittels PC-Applikation neue Kommunikationshierarchien definieren, zusätzliche Geräte ins Netzwerk aufnehmen, die Chiffrierschlüssel wechseln, verlorene Geräte ausschliessen, oder auf einem gestohlenen Gerät ein «Factory Reset» durchführen.

Eine sichere Sprach- und Messaging-Kommunikation vom Mission Operation Centre mittels Secure Smartphones zu den Personenschützern ist unerlässlich. Das Mission Operation Centre kommuniziert mit den Aussenposten der Armee, namentlich dem Objektschutz, den Checkpoints, den mobilen Radarposten, dem Logistikzentrum, dem Patrouillendienst und der zivilen Verkehrsleitzentrale der Polizei via sicheren Sprachfunk. Das Mission Operation Centre der Konferenz steht nicht zuletzt auch über den sicheren Flugfunk der Luftwaffe in permanentem Kontakt mit den Kampfjets und dem Air Control Centre. In einem Kommunikationsverbund zum Schutz einer Konferenz erfüllen verschiedenste gesicherte Kommunikationslösungen ihren Dienst, abhängig davon, welches System sich für die Einsatztruppe punkto Mobilität, Funkausbreitung und Bewegungsgeschwindigkeit besonders eignet. Im Falle der Personenschützer kommen noch Faktoren wie die Diskretion und das Bestimmen der Kommunikationshierarchie hinzu.

Ende gut – alles gut

Eine Konferenz dieser Art ist nicht nur politisch von Bedeutung, sondern bietet dem Austragungsort auch Gelegenheit, den Spitzenvertretern aus Politik und Wirtschaft ein positives Bild des Landes zu vermitteln. Sowohl Gäste als auch die lokale Bevölkerung sollten sich nicht wie auf einer Festung fühlen, sondern sich stets durch diskrete Massnahmen beschützt wissen. Sichere Kommunikation mittels Smartphones vermag gerade im Personenschutz eine verlässliche Sicherheit zu bieten. Am Ende zählt, dass die Sicherheit rund um die Uhr gewährleistet werden kann.

Quellen:

- «Tages-Anzeiger», Online-Ausgabe, 7.5.2014: So funktioniert das Air Operations Center
- «CUMINAIVEL», 22.1.2013: Spontanes und flexibles Handeln im Personenschutz

IDEX in Abu Dhabi: Sicherheit im Fokus

Alle zwei Jahre treffen sich die wichtigsten Anbieter von Rüstungsgütern an der International Defence Exhibition & Conference (IDEX) in Abu Dhabi. Im Februar 2015 war es wieder so weit: Unter dem Patronat Seiner Hoheit Sheikh Khalifa Bin Zayed Al Nahyan, Präsident der Vereinigten Arabischen Emirate und Oberbefehlshaber der nationalen Streitkräfte, fand die zwölfte Ausgabe der weltgrössten Verteidigungsmesse statt. Auch die Crypto AG war wieder mit einem Stand präsent.

Markus Baumeler | Head of Bid Management

Die IDEX ist dank ihrer enormen Grösse, der internationalen Ausrichtung und des vielseitigen Rahmenprogramms eine ideale Gelegenheit, mit Entscheidungsträgern aus dem Regierungsumfeld und ranghohen Vertretern von Verteidigungsorganisationen nachhaltige Kontakte zu knüpfen und sich fachlich auszutauschen.

Eröffnet wurde die Fachmesse mit einer spektakulären Inszenierung eines terroristischen Überfalls, welche das Publikum auf der Tribüne täglich von Neuem fesselte. Der realitätsgetreu nachgebaute Containerhafen wurde von einer Gruppe Terroristen eingenommen, wobei die fiktive militärische Intervention unter Federführung der Streitkräfte der

Szenario eines terroristischen Überfalls auf einen Containerhafen

Das portable Handterminal des MultiCom-Funksystems der Crypto AG ist auch mit arabischer Tastatur verfügbar

Vereinigten Arabischen Emirate nicht lange auf sich warten liess: Im Rahmen eines Grosseinsatzes mit Helikoptern, Panzern und Bodentruppen konnten die Terroristen bekämpft, die Geiseln befreit und die Hoheit über das Gebiet unter simulierten Bombardements zurückerlangt werden.

Die IDEX ist bekannt für solche actionreichen und aufwendig inszenierten Shows – aber auch für ihren Ruf als eine der wichtigsten Verteidigungsmessen, welche auch die führenden Unternehmen der Branche zu ihren Ausstellern zählen kann.

Anhaltendes Wachstum

Auf rund 140'000 Quadratmetern präsentierten über 180 lokale und 1'100 internationale Anbieter aus 55 Ländern ihre Produktneuheiten für Einsätze zu Wasser, zu Land und in der Luft, wobei die grössten Aussteller Unternehmen aus den USA, Deutschland, der Türkei, China, Italien und Frankreich waren. Über 80'000 Besucher, vornehmlich aus dem arabischen Raum, haben die Messestände im sehr grosszügig bemessenen Innen- und Aussenbereich frequentiert – so viele wie noch nie in der Geschichte der IDEX.

> Die IDEX ist eine ideale Gelegenheit, mit Entscheidungsträgern aus dem Regierungsumfeld nachhaltige Kontakte zu knüpfen und sich fachlich auszutauschen.

Erstmals vollständig in das Messegelände integriert war in diesem Jahr die Unmanned Exhibition (UMEX). Letztes Jahr war diese noch Teil der Naval Defence and Maritime Security Exhibition (NAVDEX), welche nun zum dritten Mal in Folge im Rahmen der IDEX stattgefunden hat. Dies unterstreicht die steigende Bedeutung unbemannter Systeme, deren Einsatzmöglichkeiten praktisch unbeschränkt sind und die in modernen Armeen immer mehr Verbreitung finden (siehe hierzu auch den Beitrag «Unbemannte Aufklärung aus der Luft», Seiten 12 – 14). Zahlreiche Live-Demonstrationen führten den Besuchern die ausgeklügelten technischen Funktionalitäten unbemannter Systeme vor Augen.

Ist «Star Wars» bald Realität? Werden sich die aus den gleichnamigen Filmen bekannten Kämpfe mit Laserwaffen in Zukunft nicht mehr nur in einer «weit, weit entfernten Galaxie» (Zitat aus den Filmen) abspielen? Dies dürften sich viele Besucher angesichts der an der IDEX präsentierten Laserkanonen – bestimmt für den Einsatz in der Flugabwehr – gefragt haben.

Eröffnung des Swiss Pavilions durch Korpskommandant André Blattmann, Chef der Schweizer Armee, Martin Sonderegger, Rüstungschef der Schweizer Armee, sowie die Schweizer Botschafterin Andrea Reichlin (v.l.n.r.)

Reges Interesse an den Lösungen der Crypto AG
Die Schweiz war dieses Jahr wieder mit über 30 Unternehmen an der IDEX vertreten. Eines davon war die Crypto AG, die zusammen mit den meisten anderen Schweizer Unternehmen unter dem Dach des Swiss Pavilion aufgetreten ist. Letzterer übte als attraktive Plattform wieder eine hohe Anziehungskraft auf die Messebesucher aus. Dies kann als Zeichen für die ausgezeichnete, auf langjährigem Vertrauen basierende Zusammenarbeit der Golfstaaten mit der neutralen, politisch stabilen Schweiz und ihren unabhängigen Unternehmen gewertet werden.

Dass Informationssicherheit und hohe Qualität im arabischen Raum grossgeschrieben werden, zeigten auch die zahlreichen Besuche am Stand der Crypto AG. Die Besucher informierten sich über die hochsicheren Lösungen und nahmen die Gelegenheit wahr, über die gegenwärtigen und zukünftigen Herausforderungen modernster vernetzter Verteidigungsorganisationen zu diskutieren. Auf reges Interesse stiess dabei unter anderem das MultiCom-Funksystem: Neben dem Sprechfunk bietet diese die Möglichkeit der zeitnahen Übermittlung von Textnachrichten, was im taktischen Einsatz stetig an Bedeutung zunimmt. Über die Tastatur des mobilen Handterminals (HC-2605) oder über einen am stationären Gerät (HC-2650) angeschlossenen Computer können Textnachrichten rasch, einfach und zuverlässig geschützt übermittelt und empfangen werden. So können beispielsweise durch einen hohen Umgebungslärmpegel bedingte Missverständnisse und Fehlinterpretationen vermieden werden.

Grosses Interesse zeigten die Besucher auch an den sicheren Lösungen aus den Bereichen End-user und Network Security. So staunten sie über die kleinste Chiffrierplattform der Welt, welche die Mobiltelefonie zuverlässig auf höchstem Niveau schützt, oder die hoch performanten Netzwerklösungen – beispielsweise die für die Integration in ein Flugzeug ausgelegte, robuste HC-8224 Airborne Version zum Schutz von IP/VPN-basierten Verbindungen.

Informationssicherheit im Dialog
Auch in diesem Jahr durfte die Crypto AG nebst Gästen aus dem arabischen Raum den Chef der Schweizer Armee, Korpskommandant André Blattmann, den Rüstungschef der Schweizer Armee, Martin Sonderegger, weitere hochrangige Offiziere sowie die Schweizer Botschafterin Andrea Reichlin in den Vereinigten Arabischen Emiraten an ihrem Stand begrüssen. In diesem Rahmen wurden im direkten Dialog die neusten Trends, Herausforderungen in der Informationssicherheit, aber auch lokale Begebenheiten und Entwicklungen ausgiebig diskutiert.

Integrales Funksystem für vielseitige Einsätze

Ob von der Küstenwache zur Wahrung der Hoheit über die staatlichen Küstengebiete oder von vereinten Seestreitkräften im Kampf gegen Piraterie eingesetzt, aber auch in Fahrzeugen des Grenzschutzes oder der Landstreitkräfte oder in Auslandsvertretungen: Das portable, aber dennoch komplette Funksystem «Secure HF Radio Communication System» kann äusserst vielfältig verwendet werden und gewährleistet in jeder Situation eine hochsichere Messaging- und Sprachkommunikation.

Tanja Dahinden | PR & Corporate Communications Manager

Vor vielen Küsten weltweit, beispielsweise am Horn von Afrika, aber auch in Teilen Südostasiens, operieren meist als Banden organisierte Piraten. Diese teilweise schwer bewaffneten Milizen attackieren und entern (Fracht-)Schiffe auf offener See, was die internationalen Schiffsrouten bedroht und die Sicherheit der weltweiten Handelswege massiv gefährdet.

Um effektiv gegen Piraterie vorgehen zu können, schliessen sich die Seestreitkräfte verschiedener Staaten in vielen Fällen zu vereinten Streitkräften zusammen und unterstützen so gemeinsam die betroffenen Küstenstaaten. Solche multinationalen Einsätze werden von einer sich an Land befindlichen Militärbasis in der betroffenen Region oder einer Einsatzzentrale auf einem Schiff aus koordiniert.

Von dieser Zentrale aus werden Einsatzbefehle erteilt sowie Lageberichte und weitere höchst sensitive Informationen kommuniziert. Auch die an den Anti-Piraterie-Einsätzen beteiligten Schiffe und Aufklärungsflugzeuge selber stehen untereinander ständig in Funkkontakt.

Die (vereinten) Seestreitkräfte sind im Rahmen solcher Missionen zwingend auf eine hochsichere Übertragung von strategischen und taktisch-operativen Informationen angewiesen, um die Hoheit über das Einsatzgebiet jederzeit wahren zu können und die Sicherheit der eigenen Streitkräfte nicht zu gefährden. Unverschlüsselte Informationen könnten von den Kontrahenten abgefangen und manipuliert werden. Zur Verschlüsselung der hoch klassifizierten Informationen,

die innerhalb eines Staatenbunds ausgetauscht werden, wird üblicherweise ein länderübergreifender Algorithmus eingesetzt – so wahren die einzelnen Staaten kompromisslos ihre Souveränität.

> Die Hoheit über das Einsatzgebiet soll jederzeit gewahrt werden können.

Das portable, sichere Funksystem* der Crypto AG zur hochsicheren Kommunikation der Schiffe untereinander oder mit der Einsatzzentrale an Land lässt sich auf den sich jeweils in der Einsatzzone befindlichen Schiffen – Fregatten, Offshore Patrol Vessels usw. – als semipermanente Infrastruktur rasch und einfach installieren beziehungsweise deinstallieren. Die Systemkomponenten – vom Notebook über die Chiffrierlösung bis hin zum Funkgerät, der Antenne und weiterem Zubehör – sind in einem widerstandsfähigen Gehäuse verbaut.

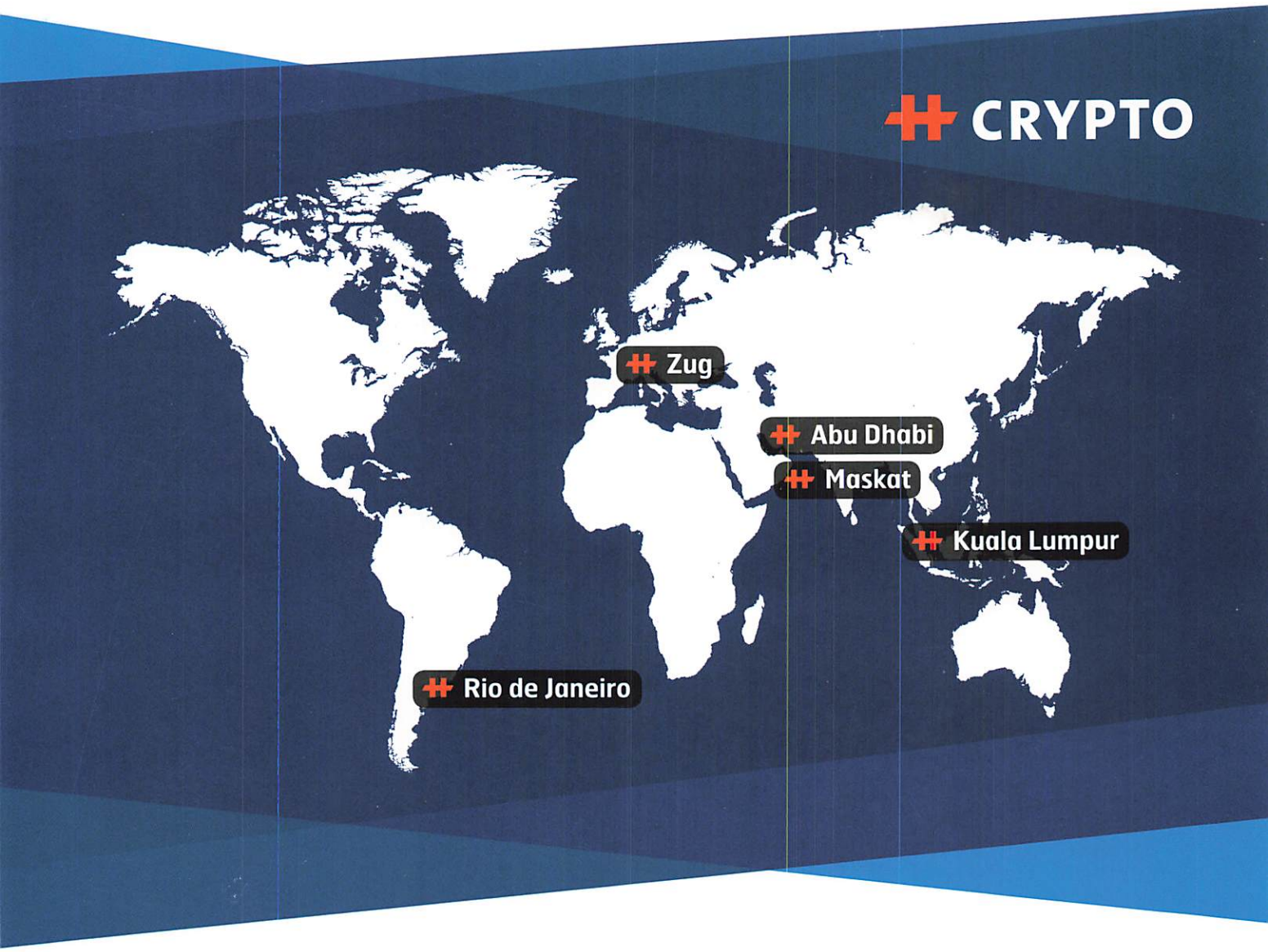
Das integrale System ermöglicht über eine chiffrierte Funkverbindung sowohl Sprachkommunikation als auch Message-Transfer, womit es verschiedenen Kommunikationsbedürfnissen entspricht: Müssen die Meldungen innert kürzester Zeit übermittelt werden, oder sind sie zwar von grosser Wichtigkeit, die Übermittlung aber nicht zeitkritisch? Ist eine sofortige Antwort beziehungsweise Quittierung erforderlich? Müssen bestimmte Vorkommnisse zwingend schriftlich dokumentiert werden?

Szenenwechsel. In einer ohnehin schon infrastrukturschwachen Region ist – hervorgerufen durch eine Naturkatastrophe, einen terroristischen Akt oder einen grösseren bewaffneten Konflikt – keine Kommunikation über das Internet, die Festnetztelefonie oder den Mobilfunk mehr möglich. Davon betroffen sind auch die sich in der Krisenregion befindenden Auslandsvertretungen, die dringend auf den Kontakt mit dem Hauptquartier des Aussenministeriums im Entsendeland angewiesen sind. Auch in einem solchen Fall gewährleistet das portable, konfigurierte und sofort einsatzbereite Secure HF Radio Communication System der Crypto AG eine komplett von einer zentralen Infrastruktur unabhängige und hochsichere Funkkommunikation.

Selbstverständlich ist diese Funklösung nicht nur für den Katastrophenfall bestimmt – sie lässt sich äusserst vielseitig und nicht auf bestimmte Szenarien beschränkt einsetzen. Unabhängig vom Einsatz und den jeweils vorliegenden Rahmenbedingungen sind in jedem Fall höchste Sicherheit und die Zuverlässigkeit des Gesamtsystems, ein störungsfreier Betrieb sowie ein umfassender Know-how-Transfer gewährleistet, da die Crypto AG alle Systemkomponenten aus einer Hand liefert.

* Das Funksystem unterstützt die HF-, VHF- und UHF-Frequenzbänder.

Das integrale Funksystem gewährleistet in jeder Situation einen hochsicheren Informationsaustausch, sowohl im militärischen als auch im zivilen Umfeld.



Hauptsitz

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

Regionale Büros

Brasilien, Rio de Janeiro
Malaysia, Kuala Lumpur
Sultanat Oman, Maskat
Vereinigte Arabische Emirate, Abu Dhabi

Seminare

Information Security Specialists
28. September bis 2. Oktober 2015

Technical Vulnerability Testing
5. bis 9. Oktober 2015

Contemporary Cryptography
12. bis 16. Oktober 2015

Die Seminare finden in den Räumlichkeiten der Crypto AG in Steinhausen, Schweiz, statt.

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