



FORUM EINSTein

Zentrum für Wirtschaft,
Wissenschaft und Politik

info@forum-einstein.org

&

Marc Furrer, Senior Partner
Monti.Stampa.Furrer, Zürich

White Paper

zu den

Schlüsselkriterien für die Sicherstellung der digitalen Souveränität der Schweiz

am Praxis-Beispiel der

Ersatzbeschaffung des neuen mobilen
Kommunikationssystems der Armee
(Ersa mob Komm)

WHITE PAPER

SCHLÜSSELKRITERIEN FÜR DIE SICHERSTELLUNG
DER DIGITALEN SOUVERÄNITÄT DER SCHWEIZ

DIGITALE SOUVERÄNITÄT IM VERTEIDIGUNGSBEREICH LEBENSWICHTIG

Armasuisse evaluiert derzeit im Beschaffungsvorhaben Ersa mob Komm zwei Systeme, die für das künftige taktische Funk-Kommunikationssystem der Schweizer Armee in Frage kommen. Mit dem Ersatz der bestehenden analogen Geräte durch digitale Systeme mit moderner IP-Architektur werden die für die parallele Übermittlung von Sprachfunk, Daten und Multimedia erforderlichen, grösseren Bandbreiten erreicht. Die Beschaffung des neuen Systems wird die Schweiz insgesamt rund CHF 700 Mio kosten.

Angesichts der intensiver werdenden Cyber Angriffe auf schweizerische Behörden und Unternehmen ist die Behauptung der digitalen Souveränität zu einer zentralen Aufgabe geworden. Taktische Kommunikationssysteme müssen immer, aber besonders auch dann zuverlässig funktionieren, wenn die zivilen Kommunikationsmittel nicht mehr verfügbar oder nicht mehr sicher sind. Die digitale Souveränität und damit die Verhinderung des unkontrollierten Abflusses von Daten durch Back-doors ist in zivilen Kommunikationsinfrastrukturen wichtig, **im Verteidigungsbereich jedoch Missionskritisch**. Deshalb müssen bei der Auswahl der richtigen Lösung für die Schweizer Armee übergeordnet zu technischen Kriterien unbedingt die Schlüsselkriterien für die Sicherung digitaler Souveränität beachtet werden:

- Garantie der Datenhoheit, zuverlässig und robust.
- Möglichkeiten der Interoperabilität
- Starke Schweizer Industriebasis
- Autonome Instandhaltungsfähigkeiten in der Schweiz



DIGITALE SOUVERÄNITÄT ERFORDERT DATENHOHEIT UND KLARE ANFORDERUNGEN

Die heutigen Vorgaben für die Beschaffung werden der absoluten Notwendigkeit nach digitaler Souveränität und der damit verbundenen Dringlichkeit zu wenig gerecht. So warnt der **neuste MELANI-Bericht** (30.4.2019) davor, dass Hersteller zum Spielball der Interessen ihrer Herkunftsländer werden: *„Es ist nicht davon auszugehen, dass sich selbst im Extremfall irgendein privatwirtschaftliches Unternehmen gegen geltendes Recht in seinem Heimatstaat stellt“*, hält der Bericht fest (S. 7): *„Je nach Hard- und Software sowie Auswahl von Dienstleistern sollten angemessene Massnahmen ergriffen werden, mit denen unberechtigte Zugriffe auf Systeme und Daten möglichst verhindert, jedoch zumindest erkannt und gestoppt werden können“* (S. 8). Zudem bestehe das Risiko, dass die *„scheinbar kostengünstigste Offerte eines Anbieters infolge angezeigter flankierender Massnahmen zu internen Mehrkosten führt...“* (S. 8).

Die Beschaffungsbehörde soll deshalb verpflichtet werden, für die neuen Kommunikationssysteme im Verteidigungsbereich folgende Anforderungen zur Sicherstellung digitaler Souveränität zwingend vorauszusetzen:

- Offenlegung der Software (Sourcecode inkl. Firmware)
- Möglichkeit für nationale Kryptologie
- Zertifizierte Hardware
- Garantierte Freiheit von „Back-Doors“
- Unabhängigkeit der Hersteller von den Behörden im Herkunftsland

WAHL DES RICHTIGEN INDUSTRIEPARTNERS ENTSCHEIDEND FÜR INTEROPERABILITÄT

«Erfolgreiche Kooperation setzt stabile Beziehungen voraus. Solche sollen vor allem mit den Nachbarstaaten, weiteren Staaten und Organisationen im europäischen Raum sowie globalen Technologieführern gepflegt werden.» (Bundesrats-Bericht zu den Grundsätzen der Rüstungspolitik, S. 8)

Kommunikations- und Führungssysteme der Armee müssen auch bei grenzüberschreitenden Ereignissen wie Katastrophen und terroristischen Angriffen abhörsicher betrieben werden können. Dabei spielt die Interoperabilität mit Nachbarstaaten und je nach Bedrohungslage auch mit der NATO eine Rolle. Diese werden ihre Netze nur für Partner öffnen, deren Kommunikationssysteme sie als vertrauenswürdig und sicher beurteilen.

INDUSTRIEBASIS MIT LOKALEN FÄHIGKEITEN AUSSCHLAGGEBEND

Neben der Cyber-Souveränität ist eine leistungsfähige sicherheitsrelevante Technologie- und Industriebasis (STIB) zentral, nämlich Forschungseinrichtungen und Unternehmen in der Schweiz mit Kompetenzen, Fähigkeiten und Kapazitäten im sicherheits- und wehrtechnischen Bereich: «Da unser Land nicht die Fähigkeit besitzt, die gesamte Wertschöpfung auf dem eigenen Territorium zu garantieren, ist die Schweiz für den Aufbau digital souveräner Systeme auf glaubwürdige und bewährte ausländische Industriepartner angewiesen. Diese müssen jedoch den Erhalt und allenfalls Ausbau von lokalen Kernfähigkeiten unterstützen, weil in Krisensituationen ohne Verzug auf nahegelegenes technologisches Know-how zurückgegriffen werden muss.» (Damian Müller, Ständerat)

Robuste Funknetze und zuverlässige Vermittlung innerhalb dieser Netze und über die Schnittstellen zu den zivilen Netzen der Blaulichtorganisationen sind für die Führung in Krisensituationen essenziell. Dank (noch) vorhandener Fähigkeiten in der Vermittlungstechnik ist die Schweizer Industrie sehr wohl in der Lage, dafür geeignete Lösungen anzubieten.

Der Bundesrat beurteilt die leistungsfähige sicherheitsrelevante Technologie- und Industriebasis (STIB) als wichtige Komponente seiner Rüstungspolitik. So hat er im Rahmen der Entflechtung der RUAG beschlossen, die für die Landesverteidigung essenziellen Fähigkeiten in der «MRO Schweiz» zu bündeln, die inskünftig dem VBS nahesteht. Dazu gehört auch jener Bereich, in welchem die für Ersa mob Komm angebotenen „Tactical Routers“ entwickelt und hergestellt werden. Es handelt sich um eine in der Schweiz einzigartige Fähigkeit, deren längerfristiger Erhalt gefährdet sein dürfte, falls sich die Behörde für eine ausländische Lösung entscheiden sollte. Umgekehrt erhöht der Einsatz einer Schweizer Lösung bei der für ihre hohen Anforderung bekannten Schweizer Armee deren Chancen in den Exportmärkten.

INSTANDHALTUNG DURCH BEWÄHRTE PARTNER IN DER SCHWEIZ

Die umfassende Instandhaltungsfähigkeit der Missions-kritischen technischen Komponenten und Systeme der Armee ist entscheidend für deren nachhaltig autonomen Betrieb in Krisenzeiten und damit lebenswichtig für eine unabhängige und robuste Verteidigungsfähigkeit der Schweiz. Bei solchen Systemen, deren Originalhersteller nicht in der Schweiz domiziliert sind, muss zwingend durchgesetzt werden, dass die entsprechenden Fähigkeiten und Kapazitäten glaubwürdig und nachhaltig in der Schweiz etabliert sind.

RÜSTUNGSPOLITISCHE CHECKLISTE FÜR DIE BEURTEILUNG DER KONFORMITÄT MIT DEN SCHLÜSSELKRITERIEN FÜR DIE DIGITALE SOUVERÄNITÄT

Rüstungspolitische Anforderungen, die der Anbieter erfüllen soll:	NEIN	JA
Gewährleistung Cyber Souveränität und Datenhoheit (zB Sourcecode offenlegen; nationale Kryptologie möglich)		
Interoperabilität		
Lokale Wertschöpfung und industrielle Fähigkeiten im Bereich Tactical Routing (RUAG MRO)		
Echtes Materialkompetenzzentrum mit umfassenden lokalen Instandhaltungsfähigkeiten		
TOTAL	Kein NEIN akzeptabel	4x JA zwingend

Weitere Auskünfte: info@forum-einstein.org