Neue Zürcher Zeitung

Der Kampfjet ist Teil eines elektronischen Gesamtsystems – die totale Autonomie gibt es nicht

Bei der Beschaffung neuer Kampfflugzeuge steht die Frage nach der Datensicherheit im Zentrum. Was sind die Gefahren der Vernetzung? Wo wird die Schweiz abhängig vom Ausland?

Georg Häsler, Lukas Mäder

2 Kommentare →

12.05.2021, 05.30 Uhr

Verwundbar ist nicht der einzelne Jet, sondern das Gesamtsystem. Die Felskaverne für die Hardware reicht nicht mehr, um die Luftwaffe vor Angriffen zu schützen.

Eddy Risch / Keystone

Kann ein modernes Kampfflugzeug aus der Ferne ausgeschaltet werden? Wie viel Einfluss hat das Herstellerland

auf den Jet, den die Schweiz beschaffen will? Wie sicher sind die Schnittstellen eines solchen komplexen Systems?

Die Frage nach der Datensicherheit ist einer der grossen Streitpunkte der gegenwärtigen Debatte um neue Kampfflugzeuge für die Schweiz.

Ein Kampfjet ist eine multifunktionale Plattform, ausgerüstet mit Sensoren, um Gefahren zu sehen, und Waffen, um diese zu bekämpfen. Das Flugzeug ist aber auch Teil eines komplexen elektronischen Netzwerks.

Die wichtigsten Erkenntnisse: Die Jets haben im **Einsatz** keine stehenden Verbindungen zu den Herstellern und Herstellerländern. Sie können auch ohne die volle Vernetzung wirkungsvoll eingesetzt werden. Die Navigation, die Kommunikation und die Verwendung der Waffensysteme sind redundant ausgelegt. Die wirklichen Abhängigkeiten entstehen in den Bereichen **Logistik** und **Ausbildung**. Entscheidend für die Kontrolle über die Systeme sind auch die gesetzlichen Grundlagen der Herstellerländer.

Und generell gilt: Wo elektronische Systeme vernetzt sind und Daten übertragen werden, besteht auch die Gefahr von Cyberangriffen. Diese Gefahr müssen die Verantwortlichen ernst nehmen und Massnahmen ergreifen.

Inhaltsverzeichnis

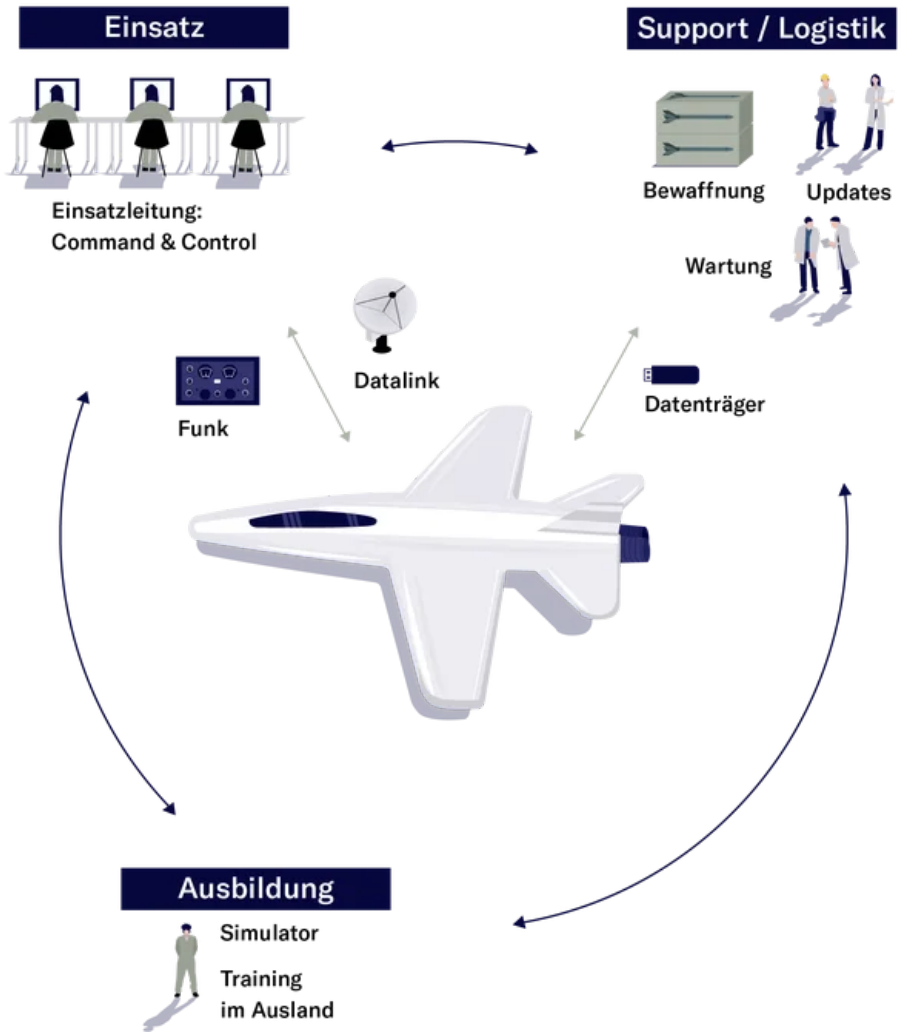
Wie sieht das System eines Kampfjets aus? ↑

Moderne Kampfjets sind nicht einfach Flugzeuge. Sie sind Teil eines komplexen Informations- und Kommunikationssystems. Ein modernes Kampfflugzeug kann in Echtzeit Daten aus verschiedenen Quellen verarbeiten: Es tauscht mit anderen Flugzeugen Radardaten aus, gibt seine

Informationen für das Lagebild an die Einsatzleitung weiter und empfängt von den Bodentruppen die Koordinaten des Ziels.

Ein wichtiger Bestandteil dieser permanenten Kommunikation ist der Datenlink 16. Dabei handelt es sich um eine Datenverbindung der Nato, welche die Schweiz in den 2000er Jahren auf ihren F/A-18-Jets eingeführt hat. Dieser Link ist auch für das neue Kampfflugzeug vorgesehen.

Moderne Kampfjets sind Teil eines komplexen Informations- und Kommunikationssystems



NZZ

Daneben steht dem Piloten auch der Sprechfunk zur Verfügung, welcher ebenfalls zur Datenübermittlung mit Bodentruppen benutzt werden kann. Die Datenverbindungen sind standardmässig verschlüsselt, die Sprechfunkverbindung bei Bedarf.

Am Boden kommen weitere Informatiksysteme zum Einsatz: für die Planung und Auswertung der Einsätze sowie die Wartung der Flugzeuge, inklusive Updates für die Bordelektronik. Zu diesen Zwecken werden Daten mit den Jets ausgetauscht – unter grössten Sicherheitsvorkehrungen.

Dieser Datenaustausch geschieht weder über eine Wireless-Verbindung noch in Echtzeit, sondern mittels physischer Datenträger. Das ist sicherer. Die Speichermedien werden dem Flugzeug entnommen und in speziellen Geräten ausgelesen oder beschrieben. Die entsprechenden Systeme am Boden sind speziell geschützt.

Welche Cyberangriffe auf einen Kampfjet sind denkbar?

Kampfjets stecken voller Elektronik; ihre dazugehörigen IT-Systeme am Boden sind komplex und haben Schnittstellen nach aussen. Diese Abhängigkeit lässt neue Risiken entstehen: Cyberangriffe, Manipulation durch den Hersteller oder ein Ausfall der Systeme durch einen technischen oder menschlichen Fehler.

Trotz zahlreichen Vorkehrungen: Ausschliessen lassen sich solche Szenarien nicht. Mit der zunehmenden Komplexität der elektronischen Systeme erhöht sich diese Gefahr sogar

noch. Eine Luftwaffe muss damit rechnen, dass ihre gesamte Flotte ausser Gefecht gesetzt werden kann, ohne dass es zu einem einzigen Schusswechsel kommt.

Angreifer können versuchen, passiv Daten abzufangen. Das Ziel solcher Spionage können Angaben über geplante oder geflogene Einsätze sein, Informationen über die Konfiguration von Jets und Waffensystemen oder auch Befehle an die Piloten in der Luft in Echtzeit.

Angreifer können aber auch aktiv versuchen, die elektronischen Systeme zu manipulieren und den gesamten Einsatz zu stören. Eine solche Sabotage ist etwa denkbar, indem falsche Wartungsdaten oder eine Fehlkonfiguration physische Schäden am Flugzeug verursachen. Oder falsche Koordinaten führen den Piloten während eines Einsatzes in die Irre oder lassen ihn gar ein falsches Ziel angreifen.

Um solche Angriffe zu unterbinden, muss jegliche Verbindung des Kampfjet-Systems nach aussen streng kontrolliert werden. Idealerweise hat die Elektronik deshalb nur wenige Schnittstellen, was den Schutz vereinfacht. Besonders wichtig ist auch der physische Schutz der IT-Systeme: Rigorose Zutrittskontrollen müssen verhindern, dass Unbefugte Zugang zu Geräten oder Datenträgern erlangen können.

Kampfflugzeuge sind im Unterschied zu Verkehrsflugzeugen so konzipiert, dass sie weniger Angriffsfläche bieten. Sie bestehen aus einzelnen elektronischen Modulen, die jeweils für bestimmte Funktionen ausgelegt sind. Zwar kommunizieren diese Systeme miteinander, doch

idealerweise geschieht dies nur beschränkt und unter Aufsicht. So gibt es etwa Systeme, welche den Datenfluss innerhalb eines Jets auf Anomalien hin beobachten.

Wie kontrolliert die Schweiz die Elektronik der Kampfjets?

Weil es sich bei Kampfjets um komplexe Systeme handelt, lässt sich die eingebaute Hard- und Software von Aussenstehenden nur schwerlich vollständig kontrollieren. Immer wieder gibt es deshalb Spekulationen, die Flugzeughersteller würden Hintertüren oder sogenannte «kill switches» einbauen, mit denen sie Funktionen des Jets steuern oder ausschalten könnten. Die Hersteller weisen diese Spekulationen zurück.

Die Schweiz überprüft die Jets nicht komplett auf solche versteckten Funktionen hin. Die für die Beschaffung zuständige Armasuisse betreibt kein sogenanntes Reverse Engineering, mit welchem sich die Funktionen von Software analysieren lassen. Armasuisse hat von den Herstellern auch den Quellcode des gesamten Kampfjet-Systems nicht zur Überprüfung angefordert. Beide Methoden wären laut Armasuisse ineffizient und nicht zielführend.

Die Schweiz legt stattdessen Wert darauf, die Sicherheitsprozesse und Standards der Hersteller zu kennen. Armasuisse überprüft die Architektur der komplexen Systeme und deren Funktionsweise. Dafür mussten die Hersteller einen detaillierten Fragenkatalog zu technischen Aspekten beantworten.

Wichtig ist zudem die Sicherheit der gesamten Lieferkette: Wie läuft die Entwicklung von Hard- und Software ab? Wie prüft der Hersteller seine Zulieferer? Welche Schutzmechanismen gibt es auf dem Weg der Elektronik in die Schweiz? Diese Fragen sind entscheidend. Denn ein Angriff kann bereits lange vor der Übernahme des Jets oder seiner Komponenten durch die Schweizer Luftwaffe erfolgen.

Wie läuft ein Einsatz ab, und welche Risiken bestehen? ↑

Die Planung ↑

Für den Piloten beginnt ein Einsatz bereits bei der Planung. Dort steht ihm ein Computersystem zur Verfügung. Damit kann er Daten wie Karten oder Wegpunkte für seinen Flug vorbereiten. Weil diese Einsatzdaten heikel sind, klassifiziert sie die Schweizer Luftwaffe beim F/A-18 zum Beispiel als geheim.

Das IT-System zur Einsatzplanung befindet sich in einem speziell geschützten Raum mit Zugangskontrolle. Die Rechner haben keine direkte Verbindung zum Flugzeug. Der Pilot muss seine Einsatzplanung auf einem externen Speichermedium physisch zum Flugzeug bringen.

Die Verbindungen während des Fluges ↑

Rollt der Kampfjet auf die Startbahn, findet die Kommunikation zwischen Pilot und Einsatzleitung über zwei Kanäle statt: über Sprechfunk sowie über den Datalink. Beide

Kanäle sind verschlüsselt; der Sprechfunk lässt sich aber auch unverschlüsselt betreiben.

Der Datalink ist ein sehr mächtiges Instrument. Damit kann das Kontrollzentrum am Boden militärische Lagedaten sowie gewisse schriftliche Kommandos an den Jet übermitteln, die dem Piloten angezeigt werden. Eine direkte Steuerung des Flugzeuges ist nicht möglich.

Der Kampfjet kann über den Datalink auch mit anderen Systemen kommunizieren. Das kann zum Beispiel ein anderes Flugzeug sein, mit dem die Radardaten ausgetauscht werden, oder eine Artillerieeinheit, die vom Jet die Zielkoordinaten für einen Beschuss erhält. Der Pilot kann selbst bestimmen, mit wem der Jet eine Datalink-Verbindung aufbaut und welche Daten er aussendet.

Die Schlüssel für die Kommunikation

Weil der Link 16 wichtig ist, um Informationen auszutauschen oder den Einsatz zu steuern, hat seine Sicherheit höchste Priorität. Die Schweizer Luftwaffe verwendet konkret den Link 16 der Nato. Die Schlüssel dafür erhält die Schweiz von den USA – egal welcher Kampfjet am Schluss tatsächlich beschafft wird.

Deshalb ist die Schweiz bei der Verschlüsselung vom westlichen Verteidigungsbündnis und konkret von den USA abhängig. Daran ändert sich auch nichts, wenn sich der Bundesrat schliesslich für die Beschaffung eines europäischen Flugzeugs entscheiden sollte.

Diese Abhängigkeit ist politisch gewollt und Teil der Anforderungen für die Neubeschaffung: Damit wird die Interoperabilität mit Nachbarländern oder während Übungen im Rahmen der Partnership for Peace (PfP) ermöglicht. Technisch wäre es zwar möglich, ein eigenes, schweizerisches System zur Verschlüsselung der Datenverbindung einzubauen. Doch das würde den Kauf verteuern, und die gewünschte Interoperabilität wäre damit nicht möglich.

Die Verschlüsselung der Kommunikation über den Datalink ist entscheidend für die Sicherheit während des Einsatzes. Die Schlüssel dürfen keinesfalls Dritten in die Hände fallen. Deswegen gelten für ihre Anlieferung aus den USA höchste Sicherheitsanforderungen.

Warum sind die Systeme für die Wartung so wichtig?

Das IT-System als zentrales Element

Die Wartung mag auf den ersten Blick als zweitrangig für die Einsatzsicherheit erscheinen. Doch das ist falsch. Der gesamte Unterhalt der Jets ist heute von Computersystemen abhängig. Deshalb kann eine Manipulation dieser Daten zu Störungen führen. Ein Ausfall des Informatiksystems könnte die Flotte zwingen, am Boden zu bleiben.

In der Luft sammeln Kampfjets permanent Betriebsdaten ihrer Untersysteme wie der Triebwerke. Die Datenträger mit diesen Informationen können Techniker nach der Landung entnehmen und auf einem Computersystem auswerten.

Schafft es ein Angreifer, diese Wartungsdaten zu manipulieren, kann das technische Folgen für das Flugzeug haben: Ein Ersatzteil wird nicht rechtzeitig nachbestellt oder ersetzt, weil das System falsche Angaben liefert – was die Einsatztauglichkeit einschränkt.

Dieses Wartungssystem weist Schnittstellen nach aussen auf. In der Schweiz etwa zum bundesnahen Betrieb Ruag, der für den Unterhalt zuständig ist. Teilweise gehen die Daten auch an die Herstellerfirma. Diese Vernetzung ist ein zusätzliches Risiko für Cyberangriffe.

Eine Besonderheit diesbezüglich stellt das System des F-35 dar. Der Hersteller Lockheed Martin bietet ein Netzwerk an, das dem Austausch von Betriebsdaten zwischen allen Ländern mit F-35 dient. Eine Luftwaffe mit wenigen Dutzend Jets erhalte so dieselben betrieblichen Erfahrungswerte, wie wenn sie Hunderte von F-35 im Einsatz hätte, wirbt das Unternehmen. Laut Lockheed lassen sich so die Betriebskosten tiefer halten.

Dieses System namens «Odin» soll dereinst vom amerikanischen Verteidigungsministerium betrieben werden. Die teilnehmenden Staaten können dabei definieren, welche Daten sie an «Odin» weitergeben wollen. Dies soll die Datenhoheit gewährleisten.

Lockheed Martin offeriert zudem als Offset-Produkt mit dem Jet ein «Cyber Center of Excellence», das Vertrauen schaffen soll. Gemeinsam mit der Tessiner Firma Nozomi und einem weiteren Schweizer Anbieter will der Hersteller des F-35 Cybergefahren erkennen und Gegenmassnahmen entwickeln.

Die Idee entstand in Japan, um das F-35-System der japanischen Luftwaffe vor chinesischen Angriffen zu schützen.

Im Kern geht es Lockheed zwar um die Sicherheit des eigenen Systems. Der US-Konzern kann aber als Nebenprodukt der Schweiz bei den Zu- und Abflüssen von Daten entgegenkommen.

Kampfjets sind zunehmend softwarebasiert und erhalten deshalb regelmässig Updates. Beim F/A-18 geschieht dies heute etwa alle zwei bis drei Jahre. Bei moderneren Jets dürften die Software-Aktualisierungen häufiger ausfallen. Diese Updates werden ausgiebig getestet, weil ein Fehler weitreichende Folgen haben könnte. Die zentrale Komponente der Flugsteuerung wurde bisher beim F/A-18 in über 20 Jahren gerade ein Mal aktualisiert.

Die System-Updates stellen aus Sicht der Cybersicherheit ein Risiko dar. Gelingt es einem Angreifer, die Software-Aktualisierungen zu manipulieren, verändert dies das System im Kern: Er kann die Funktionsweise des Kampfjets sabotieren.

Zur Sicherheit gehört deshalb auch, den Transfer der Software vom Herstellerland in die Schweiz zu überwachen. Doch die Kompromittierung der Software-Aktualisierungen kann bereits früher geschehen: beim Hersteller oder gar bei einem Zulieferer. Die Sicherheit der Lieferkette muss deshalb höchste Priorität haben.

Grundsätzlich könnte die Schweiz ihre Jets auch weniger oft oder gar nicht aktualisieren. Doch die Vorgabe ist klar: Die Flugzeuge sollen in derselben Konfiguration wie im Herstellerland fliegen. Das hat grosse Kostenvorteile, es verhindert aber auch Sicherheitslücken im System und ermöglicht neue Funktionen.

Welche Risiken bestehen in der Ausbildung?

Zum Gesamtsystem Kampfflugzeug gehört die Zusammenarbeit mit den Herstellerländern in der Ausbildung. Hier stehen nicht in erster Linie die Daten im Vordergrund, sondern die direkten Kontakte mit anderen Armeen und Luftwaffen.

Bis vor wenigen Jahren trainierten Piloten der Schweizer Luftwaffe in den USA auf F/A-18 der Navy. Höhepunkt des Pilotenaustauschs war jeweils eine Landung auf einem US-Flugzeugträger. Über diese Kontakte kennen Schweizer und Amerikaner die Einsatzverfahren und die Kultur voneinander – und bauten über die Jahre ein Vertrauensverhältnis auf.

Auch mit europäischen Staaten pflegt die Schweiz eine freundschaftliche Zusammenarbeit in der Ausbildung. Schweizer F/A-18 trainieren etwa über dem französischen Jura oder üben die Betankung in der Luft mit dem Tankflugzeug der französischen Luftwaffe. In Schottland und Norwegen finden regelmässig Nachtflugkampagnen statt. Dafür verschiebt die Luftwaffe nicht nur die Jets ins Ausland, sondern auch Teile der Logistik und der Einsatzleitstelle.

Für die Ausbildung liefern die Hersteller auch Simulatoren. Im Fall des F-35 kann ein solcher über das «Odin»-Netzwerk auch mit dem Hersteller korrespondieren. Armasuisse ist bezüglich einer vernetzten Ausbildung zurückhaltend. Die Beschaffungsbehörde sieht «Odin» als Logistiksystem. Es würden darüber keine operationellen Daten mit den USA ausgetauscht.

Auch hier wird das Dilemma sichtbar: Die Schweiz könnte von den Erfahrungen der anderen Luftwaffen profitieren, verliert dabei aber ein Stück Eigenständigkeit.

Welche Kontrolle haben die Anbieterstaaten?

In ihren Kampagnen werben die europäischen Kampfjet-Anbieter explizit mit der Datenhoheit ihrer Systeme. Dassault Aviation aus Frankreich, der Hersteller der Rafale, argumentiert in einer Präsentation für die «Allgemeine Schweizerische Militärzeitschrift» («ASMZ»), der eigene Jet könne dank eigenständigen Navigations- und Kommunikationssystemen seine Missionen «völlig autonom ausführen». Dies trifft aber grundsätzlich auch auf die amerikanischen Systeme zu, die ebenfalls mit der sogenannten Trägheitsnavigation ausgerüstet sind.

Der wirkliche Unterschied zwischen den USA und Europa betrifft die Gesetzgebung.

Alle Anbieterstaaten wollen verhindern, dass ihre Waffen in falsche Hände geraten – nicht zuletzt auch, um das Wissen der eigenen Industrie zu schützen. Letztlich soll damit aber

vor allem die ungewollte Proliferation von Waffensystemen verhindert werden, ein Ziel, das auch die Schweiz unterstützt. Die USA verfügen über die klarsten Regularien in diesem Bereich, beruhend auf der United States Arms Export Control Act (AECA).

«Die US-Regierung erklärt sich bereit, für unsere Partnernation die Artikel nach dem gleichen Beschaffungsprozess zu beschaffen, den sie für ihren eigenen Bedarf verwendet», so erklärt die US-Botschaft in Bern das Vorgehen. Alle Exporte müssen ausserdem durch den Kongress genehmigt werden.

Dies bedeutet, dass die US-Gesetze auch nach der Auslieferung eine gewisse Wirkung entfalten.

Im Rahmen der AECA unterliegen alle amerikanischen Verteidigungsartikel dem End Use Monitoring (EUM), also einer Endverbrauchsüberwachung. Sogenannte Security Cooperation Officers überprüfen regelmässig, ob das Waffensystem so geschützt wird wie ursprünglich abgemacht. Bei besonders heiklen Komponenten, wie etwa Ausrüstung für die Kommunikationssicherheit, findet diese Kontrolle jährlich statt.

Bereits heute überprüfen US-Beamte die F/A-18 oder auch die leichte Flugabwehrlenkwaffe Stinger. Es geht dabei laut der amerikanischen Botschaft auch darum, die technologischen Sicherheitsvorkehrungen zu überprüfen.

Die Europäer verlangen wesentlich weniger Einblick. Der Eurofighter-Anbieter Deutschland setzt bei

«ausfuhrgenehmigungspflichtigen Gütern» auf Verträge und Vertrauen. Eine Sprecherin des Bundesministeriums für Verteidigung schreibt der NZZ, der «Endverwender» müsse vor dem Export eine «Endverbleibserklärung» abgeben: «Diese besagt, dass vor der Weitergabe der Kriegswaffe an einen anderen Endverwender die Zustimmung der Bundesregierung erforderlich und einzuholen ist.» Kontrollen gibt es keine.

Auch Frankreich übe keine nachträglichen Kontrollen aus, schreibt die französische Botschaft in Bern: «Französische Waffensysteme, insbesondere die im Rahmen des Air-2030-Wettbewerbs vorgeschlagenen, werden als Instrumente von Souveränität und Unabhängigkeit konzipiert und entwickelt, und so werden sie auch der Schweiz angeboten.» Allerdings gilt auch für die europäischen Kampfflugzeuge, dass zum Beispiel amerikanische Waffen entsprechend den US-Regularien überprüft würden.

Auf den ersten Blick wirken die Regularien der USA streng. Kontrollen können aber auch als Teil einer Partnerschaft verstanden werden. Die Schweiz wird beim Schutz der eigenen Systeme unterstützt, aber sie lehnt sich im Fall der USA vordergründig stärker an das Herstellerland an als im Fall der europäischen Anbieter, allerdings auf der Basis glasklarer gesetzlicher Grundlagen.

Ein weiteres Thema betrifft die Datensicherheit der Firmen. Könnten sie allenfalls im Fall erhöhter Spannungen gezwungen sein, ihre Server dem Zugriff der eigenen Regierung zu öffnen? Kritisch beobachtet werden auch in diesem Fall besonders die USA, die seit 9/11 über die sogenannte Patriot Act verfügen. «Sobald das Eigentum an

der Plattform auf den Partner übergegangen ist, hat die US-Regierung nicht die Möglichkeit, ohne Zustimmung auf das System zuzugreifen», schreibt die US-Botschaft der NZZ auf eine entsprechende Frage.

Die Kontrolle über Daten und Informationen ist heute ebenso so wichtig wie die Luftüberlegenheit. Das System Kampfjet schafft die Verbindung zwischen diesen beiden Operationssphären. Cyber- und Luftraum sind übergreifend zu verstehen – und bedingen ein konsequentes Multidomain-Denken. Dass die zunehmende Vernetzung auch Auswirkungen auf die autonome Landesverteidigung hat, scheint offensichtlich zu sein.

Ein Schreiben aus dem Bestand der diplomatischen Dokumente (Dodis) des Bundesarchivs zeigt, dass diese Erkenntnis die militärische Führung der Schweiz schon vor vierzig Jahren umgetrieben hat.

Analyse: Die Schweiz führt eine Scheindebatte

«Es ist offensichtlich, dass sich in einem Ernstfall sofort gewisse Probleme mit benachbarten Luftwaffen ergeben würden.» Diese Aussage stammt aus dem Jahr 1978, geäussert vom damaligen Kommandanten der Flieger- und Fliegerabwehrtruppen, Korpskommandant Kurt Bolliger. In einem geheim klassifizierten Papier an den Generalstabschef wies er darauf hin, dass der Zusammenarbeit mit einem möglichen Verbündeten («Grün») ein besonderer Stellenwert zukäme, «weil es heutzutage wegen der technischen Entwicklung nicht mehr denkbar ist, solche Dinge in letzter Minute zu improvisieren».

Bolliger nimmt eine realistische Lagebeurteilung vor: Bereits tief im Kalten Krieg war an eine absolut autonome Luftverteidigung nicht mehr zu denken. Eine Zusammenarbeit mit den Nachbarn ist unabdingbar. Schon damals ging es nicht nur um die räumliche Dimension, sondern auch um die Vernetzung und die Kommunikation.

Die zentrale Anforderung an ein neues Kampfflugzeug und auch an die bodengestützte Luftverteidigung wäre deshalb die Interoperabilität. Also die Fähigkeit, möglichst eng zusammenzuarbeiten. In der Evaluation wurde dieser Faktor vertieft geprüft. Trotzdem konzentriert sich die öffentliche Debatte in der Schweiz zu stark auf den Aspekt der Autonomie, die – unter Berücksichtigung aller Fakten – präziser als Scheinautonomie bezeichnet werden sollte.

Verwundbar ist nicht der einzelne Jet, sondern das Gesamtsystem. Die Felskaverne für die Hardware reicht nicht mehr, um die Luftwaffe vor Angriffen zu schützen. Der Einsatz ist abhängig vom Funktionieren der elektronischen Systeme. Diese müssen deshalb wirksam vor Angriffen und vor Ausfällen geschützt sein.

Die Cyberbedrohung lässt Räume verschmelzen. Die Landesverteidigung hält sich nicht mehr an die Landesgrenze. Der Schutz der Systeme erfolgt deshalb im Verbund effektiver als im Alleingang.

Im Zentrum stehen also nicht Legenden über «kill switches», sondern eine saubere vertragliche Absicherung der Zusammenarbeit und eine ehrliche politische Debatte.

Die Snowden-Affäre und die Abhöraktionen von US-Nachrichtendiensten auch bei befreundeten Regierungen – unter anderem auch bei der deutschen Bundeskanzlerin Angela Merkel – haben das Vertrauen unter den westlichen Staaten gestört. In der zugespitzten Diskussion geht allerdings oft vergessen, dass börsenkotierte Unternehmen kein Interesse an Hintertüren und Lecks haben.

Es fehlen in der aktuellen Beschaffung politische Kriterien für eine nähere Zusammenarbeit mit einem Hersteller und einem Herstellerland. So führt die Schweiz eine Scheindebatte über die Autonomie eines vernetzten Systems, statt über die Vorteile der Zusammenarbeit zu diskutieren.

«Air 2030»

geo. Die Schweiz erneuert mit dem Programm Air 2030 ihre Luftverteidigung. Dazu gehören unter anderem ein bodengestütztes System (Bodluv) und neue Kampfflugzeuge (NKF) für insgesamt 8 Milliarden. Im vergangenen September hat eine knappe Mehrheit von 50,1 Prozent einem Kredit von 6 Milliarden für die Jets zugestimmt. Zur Auswahl stehen die beiden amerikanischen Typen F-35 und F/A-18 Super Hornet, die französische Rafale sowie das europäische Gemeinschaftsprodukt Eurofighter.

Haltung der NZZ
Soeben wurde die Evaluation abgeschlossen, vor den Sommerferien trifft der Bundesrat den Typenentscheid. Das letzte Wort hat das Parlament. Die Beschaffung wird im Rahmen des Rüstungsprogramms 22 vorgelegt. Linke Kreise drohen für den Fall, dass ein amerikanischer Jet gewählt wird, mit einer Initiative.

Die NZZ befürwortet die Erneuerung der schweizerischen Luftverteidigung – und ist für die Beschaffung eines neuen Kampfflugzeugs. Alle vier evaluierten Typen wären für die Schweiz grundsätzlich geeignet. Denkverbote bezüglich eines amerikanischen Systems werden abgelehnt.

---

2 Kommentare

Werner Moser vor 5 Tagen

Irrelevant ob der Kampfjet eine Eigenproduktion ist, oder nicht (was er bekanntlich nicht sein wird!): es gibt die totale Autonomie nicht! Ob es sich dabei um eine operative-, elektronische-, logistische-, konstruktive- und daten-vernetze Abhängigkeit handelt, ist im einzelnen- u/o mit Blick auf alles zusammen derart komplex "interconnected", dass es nicht um die Beantwortung der Frage nach bestehenden Abhängigkeiten geht, sondern wie man mit diesen komplexen Zusammenhänge aller dieser Abhängigkeit umgeht. Um diese im besten Interesse der Schweiz auch gesichert zu wissen. Deshalb wird es u.a matchentscheidend sein, wie stark die Schweiz sich bei der Auswahl, Kauf, Unterhalt, operativ-/ militär- und / oder verteidigungsstrategisch einbringen kann. Und vice-versa, was den Kampfjet-Lieferant (Firma/Land) anbetrifft. Denn die Schweiz wird pro Saldo total vom Ausland abhängig sein. Dies anders sehen- u/o beurteilen zu wollen käme einer Selbsttäuschung gleich. Mit Blick auf die vorgesehenen Lieferanten (exUSA, exD, exF, ex SW, exEuro-Fighter) hätte man es mit zumindest plausiblen Abhängigkeiten zu tun. Lassen wir uns also überraschen!

2 Empfehlungen

H. H. vor 5 Tagen

Einfach eine Frage: Der Datenverkehr wird über einen von der Nato gestellten Algoritmus verschlüsselt, damit die Verschlüsselung mit mit den Nachbarländern kompatibel ist. Wieso sind nicht zwei verschiedene Verschlüsselungsalhoritmen möglich, unter denen die benutzer auswählen können?

Alle Kommentare anzeigen

Mehr zum Thema

Schweizer Armee Kampfjets