

Digitalisierung in der militärischen Luftfahrtindustrie

BDLI



Bundesverband der Deutschen
Luft- und Raumfahrtindustrie e.V.

VORWORT

**Generalleutnant
Dr. Ansgar Rieks**

Stellvertreter des Inspektors
der Luftwaffe



Bedeutung der Digitalisierung für die Luftwaffe im Kontext der Auftragserfüllung

” Als sich die Digitaltechnik erstmals in einem Kampfflugzeug der Luftwaffe bewährte und unsere Piloten einer neuartigen Flugsteuerung vertrauten, waren viele unserer jetzigen Angehörigen des fliegerischen Dienstes noch nicht geboren. Im Juni 1981 setzte das Kampfflugzeug Tornado einen Startpunkt der Digitalisierung, und auch heute stehen wir mit unseren Planungen für ein „Next Generation Weapon System“ und dem Projekt „Luftgestützte Wirkung im elektromagnetischen Spektrum“ an der Spitze der technologischen Entwicklung. Auch bei allen anderen Fähigkeitsentwicklungen unserer Luftwaffe spielt die Digitalisierung eine entscheidende Rolle.

Nach fast vier Jahrzehnten muss niemand mehr von der Bedeutung der Digitalisierung überzeugt werden, insbesondere da der Begriff in den letzten Jahren eine breite, öffentliche Resonanz gefunden hat und für nahezu alle Lebensbereiche diskutiert wird. Die technologische Entwicklung verläuft in immer größerer Geschwindigkeit. Wer aber heute von einer „digitalen Disruption“ spricht, hat wohl in der Vergangenheit die „digitale Evolution“ verschlafen.

Heute geht es daher nicht nur um Vision, sondern auch um die Tat! Denn wenn wir nicht auch weiterhin Digitalisierung prägen, dann prägt sie uns. Für Luftstreitkräfte gilt unverändert, auch zukünftig ihre Potenziale zu nutzen, die Änderungen, die sie bringt, proaktiv aufzugreifen und von Beginn an alle Aspekte der Digitalisierung einzubeziehen – vom digitalen Mindset bis hin zur Cyber-Resilienz von Waffensystemen und zur Nutzung der heutigen ersten Ansätze von Künstlicher Intelligenz.

Hierbei stehen wir im engen Dialog mit der Industrie und Forschung. Ähnlich wie die Wirtschaft, steht auch die Luftwaffe in einer fortwährenden digitalen Transformation. Wir haben hierzu eine Vielzahl digitaler Aktivitäten auf den Weg gebracht, die sich zunächst in der Ausbildung auswirken werden und auf moderne digitale Technik mit Virtualisierung und Augmented Reality zurückgreifen. Unter dem Leitsatz „move information – not people“ sollen für unsere Operationen unter anderem Entscheidungsprozesse beschleunigt werden. Digitalisierung bringt auch für die Luftwaffe immer stärker eine Orts- und Zeitunabhängigkeit. Maßgeblich bleibt dabei aber unverändert, die richtigen Mittel zum richtigen Zeitpunkt am richtigen Ort zu haben, um den militärischen Auftrag zu erfüllen.

Informationsüberlegenheit ist heutzutage mehr denn je die Grundlage, um in den Szenarien militärischer Auseinandersetzungen, die von einem hohen Anteil hybrider Bedrohungen und dem Einsatz extensiver digitaler Fähigkeiten geprägt sind, zu bestehen. Dies bedeutet für eigene Kräfte über die notwendigen Informationen zu verfügen und gleichzeitig einem Gegner den Zugang zu diesen Informationen zu verwehren. Angesichts von „Big Data“ kommt der Auswertung und Bewertung von Daten mehr denn je eine hohe Bedeutung zu. Nur damit können sich die „traditionellen“ Eigenschaften von Luftkriegsmitteln – Reichweite, Geschwindigkeit und Flexibilität – künftig effektiv entfalten. Die Beherrschung des elektromagnetischen Spektrums als bedeutendem Träger für diese Informationen ist Enabler für eine umfassende Projektion von Luftmacht. Aus diesem Grund hat die Luftwaffe u.a. das Rüstungsprojekt „Luftgestützte Wirkung im elektromagnetischen Spektrum“ im Fokus der eigenen digitalen Fähigkeitsentwicklung.

Die Luftwaffe trägt digitale DNA seit jeher in sich. Um die Fülle der sich bietenden Chancen zu nutzen, bringen wir neben unserer Erfahrung und unserer operationellen Expertise, frische Ideen in den Dialog ein, denn: Digitalisierung ist der Schlüssel unseres gemeinsamen Erfolges!

Wir stehen bereit, alle technologischen, projektorientierten und ethischen Aspekte der Digitalisierung ebenso mit zu diskutieren, wie auch Fragen der Führung und der Ausbildung. Möglicherweise erweist sich anschließend die Digitalisierung vielleicht doch als Auslöser einer Disruption – jedoch mit einer überaus positiven Stoßrichtung!

INHALT

INDUSTRIEPOLITISCHE POSITIONIERUNG DES BDLI	4
DIGITALISIERUNG & EINSATZBEREITSCHAFT	5
DIGITALISIERUNG & AUSTRÜSTUNG	5
DIGITALISIERUNG & ZULASSUNG	5
DIGITALISIERUNG & FÜHRUNG IM EINSATZ	6
DIGITALISIERUNG & KÜNSTLICHE INTELLIGENZ	6
DIGITALISIERUNG & CYBERSICHERHEIT	7



DIGITALISIERUNG IN DER MILITÄRISCHEN LUFTFAHRTINDUSTRIE

INDUSTRIEPOLITISCHE POSITIONIERUNG DES BDLI

Die militärische Luftfahrt ist seit jeher durch sehr hohe Technologieansprüche geprägt und dementsprechend umfangreich gestalten sich die Potenziale durch die Digitalisierung. Wie auch die Industrie hat die Luftwaffe erkannt, dass Digitalisierung anzugehen, eine Führungsaufgabe ist. Mit dem stellvertretenden Inspekteur der Luftwaffe, Generalleutnant Dr. Rieks, hat die Luftwaffe einen „Chief Digitalisation Officer“ implementiert, der dieses querschnittliche Unterfangen in der Zukunft angehen wird. Mit dem Organisationsbereich CIR (Cyber- und Informationsraum) respektive einer eigenen Abteilung Cyber- und Informationstechnik (CIT) des BMVg, sowie Institutionen wie dem „Cyber Innovation Hub“ oder der „Agentur für Innovationen in der Cybersicherheit“ haben das Verteidigungsministerium und die Bundeswehr zahlreiche Multiplikatoren von relevantem Wissen geschaffen, dessen Anwendung vollumfänglich nutzbar gemacht werden soll.

DIGITALISIERUNG & EINSATZBEREITSCHAFT

Die personelle Einsatzbereitschaft kann durch digitale Werkzeuge wie Anwendungen der Künstlichen Intelligenz (KI) sowohl im Flugbetrieb als auch im Maintenance-Bereich effizienter erreicht und gesteigert werden. Immer komplexere Simulationen machen es in Kombination mit Virtual- und Augmented Reality möglich, Personal in der Ausbildung und im Training besser auf widrige Einsatzumstände vorzubereiten. Gleichzeitig steht dann freigeswordenes Gerät bzw. entsprechende materielle Kapazität dort zur Verfügung, wo sie wirklich gebraucht werden – nämlich in einer praxisbezogenen Ausbildung und im Einsatz.

Die Erhebung, Verarbeitung und Auswertung von Daten kann dabei helfen, bestehende Prozesse zur materiellen Einsatzbereitschaft (Materialbeschaffung und Wartung) in ihrer Komplexität noch besser zu durchdringen und sie so effizienter zu gestalten. Für die Luftwaffe und die Industrie bedeutet das gleichermaßen, Möglichkeiten zur Leistungssteigerung in allen Phasen des Produktlebenszyklus, von der Forschung und Entwicklung bis hin zur Betreuung in der Nutzungsphase ganzheitlich ausschöpfen zu können – auch bekannt als „End-to-End Product Lifecycle Management“.

Das gleiche gilt spiegelbildlich für die fliegenden Verbände und das Kommando Cyber- und Informationsraum (CIR) der Bundeswehr. Hier bieten sich im Bereich der Einsatzbereitschaft erhebliche Potenziale. Planungsprozesse, die sich auf eine breite und validierbare Datenbasis abstützen können, vermögen Ressourcenflüsse zu optimieren und Engpässe im Verbund mit smarten Supply-Chain-Lösungen der Industrie zeitnah zu überwinden oder gar nicht erst entstehen zu lassen. Ein Beispiel hierfür ist SmartForce, die Bereitstellung und Analyse von Daten des militärischen Transportflugzeugs A400M für den deutschen und französischen Kunden.

DIGITALISIERUNG & AUSTRÜSTUNG

Bestehende Systeme (Legacy-Systeme) müssen für das Zusammenwirken in einem vernetzten Gefechtsverbund (Future Combat Environment) fit gemacht werden, insbesondere im Hinblick auf Kommunikation und Führungsfähigkeit. Zu einem späteren Zeitpunkt müssen diese Systeme auch weitere Sensorik und Assistenzsysteme zur Informationsverwaltung einbinden können. Vorausschauende Wartungsprozesse (Predictive Maintenance) in Legacy-Systemen gehören für die Aufrechterhaltung der Einsatzbereitschaft der Systeme und Plattformen so weit als notwendig eingebunden. Da alte Systeme nur bedingt technologisch aufwuchsfähig sind, müssen neue skalierbare Systemarchitekturen geschaffen werden. Auch deswegen nimmt das Future Combat Air System (FCAS) und das damit verbundene Next Generation Weapon System (NGWS) eine immens wichtige Rolle für die Zukunftsfähigkeit der deutschen militärischen Luftfahrt ein.

DIGITALISIERUNG & ZULASSUNG

Die Schaffung neuer Architekturen einhergehend mit der steigenden Komplexität erfordert ein Umdenken bei der Zulassung in der militärischen Luftfahrt. Hierbei ist der Schulterschluss von Industrie und Sicherheitsbehörden unumgänglich. Neuentwicklungen und Änderungen solcher Systeme riskieren wirtschaftliche Untragbarkeit, Nicht-Zulassung und inakzeptable Verzögerungen bis zum Zeitpunkt der Markteinführung, wenn die dafür nötige Infrastruktur (Regelwerk, Methodik, Personal) nicht konsequent an diese neuen Herausforderungen angepasst wird.

DIGITALISIERUNG & FÜHRUNG IM EINSATZ

Informationen können den Menschen zwar durch schiere Masse überfordern, bleiben aber unerlässlich, um in allen Situationen bestmöglich agieren zu können. Dies gilt insbesondere für Aspekte von Ausbildung und Unterstützung bis hin zum Umfeld bewaffneter Konflikte. Für alle Anwendungsszenarien muss es ein primäres Ziel sein, Daten zu erheben, in ihrer Masse beherrschbar zu machen sowie akteursübergreifend kommunizieren und verwerten zu können. Die Nutzung der durch die gesamte Flotte erfolgten Daten erlaubt die deutliche Verbesserung der zugrundeliegenden Algorithmen. Dabei ist den Datenschnittstellen besondere Aufmerksamkeit zu widmen. Nur wenn Daten und damit Informationen reibungslos zwischen Handelnden ausgetauscht werden können, kann das volle Potenzial digital gestützter Lösungen realisiert werden. Dies gilt insbesondere angesichts der komplexen Herausforderungen hybrider Szenarien, denen nur mit vernetzten Operationen begegnet werden kann. Mit Hilfe einer sogenannten „Secure Cloud Solution“ kann dies erreicht werden.

Gerade im Einsatz wird die effiziente Verarbeitung von Daten immer wichtiger. Schon jetzt sieht sich die militärische Leitungsebene mit einer immensen potenziellen Datenflut konfrontiert. Diese in Zukunft vorteilbringend zu nutzen und zu schützen, wird essenziell für den Erfolg in künftigen Konflikten sein. Dabei kann die Industrie Big Data-Analysen aus dem Betrieb der Flotte auch bei internationalen Partnern beisteuern, um so Massendaten in Informationsüberlegenheit zu übersetzen und eine bessere Koordination zwischen den Partnern sicherzustellen.

Automation, Robotik und Digitalisierung haben elementaren Einfluss auf den Charakter moderner militärischer Konflikte. Durch die Omnipräsenz leistungsstarker Sensoren und einen steigenden Vernetzungsgrad der Systeme untereinander entsteht ein „digitales Gefechtsfeld“. Dieses wird immer mehr vom Ringen um Informationsüberlegenheit, also die Kenntnis über Lage, Stärke und Absicht des Gegners, dominiert. Das „Gefecht 4.0“ ist auch gekennzeichnet durch ein „contested information environment“, d.h. eine hohe Ausfallwahrscheinlichkeit satellitengestützter Fähigkeiten und die Störbarkeit zellbasierter Kommunikationssysteme. Hier wird es darauf ankommen, die Kernführungsfähigkeit auch unter Störbedingungen durch geeignete Übertragungsverfahren mit geringer Bandbreite aufrechtzuerhalten. Neue plattformübergreifende Konzepte (Systemverbund) werden nötig sein, um auch in der Zukunft erfolgreich operieren zu können.

Ein Beispiel hierfür findet sich im erwähnten FCAS. Zentraler Aspekt des bisher größten europäischen Verteidigungsvorhabens ist die Inkorporation verschiedenster Technologiesprünge. So soll das System beispielsweise erstmals das Zusammenwirken von bemannten und unbemannten Systemen (Manned-Unmanned-Teaming) ermöglichen. Dabei vergibt der Pilot Aufgaben wie Überwachung und Aufklärung an ihm unterstellte „Remote Carrier“, die ihre Aufträge anschließend selbstständig ausführen können. Somit wird FCAS nicht zuletzt in die Lage versetzt, das Konzept des „Swarmings“ für die Luftwaffe nutzbar zu machen.

DIGITALISIERUNG & KÜNSTLICHE INTELLIGENZ

Durch gesellschaftliche Randbedingungen, wie den demografischen Wandel, werden westliche Streitkräfte wie die Bundeswehr vermehrt darauf angewiesen sein, ihre vorhandenen personellen Ressourcen durch verschiedene Assistenzsysteme zu verstärken. Dabei bedarf es leistungsstarker und sicherer Systemarchitekturen, um die Vielzahl verschiedener Ressourcen zu akkumulieren und ihre Fähigkeiten dem Menschen bestmöglich zur Verfügung zu stellen. Die in diesem Zusammenhang anfallenden Datenmengen sind durch den Menschen allein nicht mehr verarbeitbar. Dementsprechend fällt der KI eine Rolle als militärische Schlüsseltechnologie zu. Dabei geht es in erster Linie darum, Systeme zu entwickeln, die die wachsenden Datenmengen schnell und transparent verarbeiten können, um dem Menschen Entscheidungshilfen zu bieten. Die Position des BDLI bezüglich der Einbindung des Menschen in die Autonomie von Künstlicher Intelligenz (human IN the loop vs. human ON the loop) lehnt sich dabei an die Positionierung des Bundesverbandes der Deutschen Industrie an, wonach KI den Menschen nicht ersetzen, sondern unterstützen soll.

Nichtsdestoweniger ist eine breite Debatte zwischen Politik, Gesellschaft, Wissenschaft und Industrie vonnöten, um eine Zielvorgabe zu erarbeiten, an der sich alle Akteure strategisch ausrichten können. Moderne hochperformante Systeme, die KI-Anwendungen bereitstellen können, sind zudem deutlich komplexer als heutige Systeme für sicherheitskritische Anwendungen in der Luftfahrt.

DIGITALISIERUNG & CYBERSICHERHEIT

Ohne Zweifel bestehen viele der aufgeführten Potenziale und Fragestellungen der Digitalisierung ebenfalls in der zivilen Luftfahrt sowie in anderen Industriezweigen. Was die militärische Luftfahrt hierbei jedoch deutlich unterscheidet, ist das enorm gesteigerte Sicherheitsbedürfnis – in der Entwicklung, Produktion und Wartung sowie im Einsatz. Digitalisierte Logistik, Führung oder sogar das „Gefecht 4.0“ sind immens abhängig davon, dass Gegner keinen Zugang zur eigenen Kommunikation erhalten. Hier verwundbar zu sein eröffnet potenziellen Aggressoren Möglichkeiten zur Industriespionage sowie zur Störung oder gar Vernichtung der eigenen Ressourcen – von der Infrastruktur bis hin zum fliegenden System. An dieser neuralgischen Schnittstelle Sicherheit herzustellen und eine stringente „Data Governance“ einzuführen sowie aufrecht zu erhalten, muss ein sicherheits- und industriepolitisches Grundinteresse der Bundesrepublik sein.

Daraus ergeben sich für die militärische Luft- und Raumfahrtindustrie Forderungen an die Öffentlichkeit und den Gesetzgeber: (siehe Seite 8)

1. Die öffentliche Hand ist gezwungen im selben Maße wie die deutsche Industrie die digitale Transformation als Chance zur grundlegenden Veränderung und als Schlüsselement zum Erhalt bzw. Ausbau der Wettbewerbsposition – auch im internationalen Ländervergleich – wahrzunehmen. Das bedeutet, dass beispielsweise Beschaffungs- und Vergabeprozesse sowie Kommunikationswege einem digitalisierten industriellen Umfeld anzupassen sind. Hierzu gehört auch die verstärkte Ausbildung von qualifiziertem Personal, um den zukunftsentscheidenden Themen der Digitalisierung in Deutschland aus personeller Sicht gewachsen zu sein.
2. Die öffentlichen Mittel zur Förderung von Technologien zur Digitalisierung im spezifisch militärischen Luftfahrtkontext müssen verstärkt werden. Die zusätzlich bereitgestellten öffentlichen Mittel helfen dabei, die Schlüsselfähigkeiten der deutschen militärischen Luftfahrtindustrie vor dem Hintergrund der Digitalisierung im internationalen Wettbewerb zu erhalten bzw. auszubauen und damit die operativen Einsatzfähigkeiten der Luftwaffe von morgen zu garantieren.
3. Gesamtgesellschaftlich ist eine Diskussion anzuregen, welcher Grad der maschinellen Automatisierung bzw. menschlichen Einbindung für die verschiedenen Anwendungsfelder der Künstlichen Intelligenz jeweils erwünscht ist. Dabei muss neben der moralischen Kategorie auch der potentiell offensivere Umgang beim Einsatz von KI durch feindliche Streitkräfte berücksichtigt werden.
4. Die KI-Strategie der Bundesregierung erwähnt die Streitkräfte lediglich in zwei Sätzen. Auf Basis der gesellschaftlichen Diskussion ist das Bundesministerium der Verteidigung gefordert, die Forschung und Entwicklung relevanter Technologien voranzutreiben. Eine enge Verzahnung mit der Agentur für Innovation in der Cybersicherheit sowie dem Cyber Innovation Hub der Bundeswehr ist erstrebenswert.
5. Der 5G-Netzausbau ist zügig voranzutreiben. Dabei ist es in nationalem Interesse, die Netzwerktechnologie in deutsche oder zumindest europäische Verantwortung zu geben, um unberechtigte politische Einflussnahme durch Drittstaaten und technologische Verwundbarkeiten zu verhindern. Neben einer Überprüfung der Hardwarekomponenten wäre für die Stärkung des Vertrauens in Netzanbieter eine Einsichtnahme in Quellcodes und Entwicklungsprozesse durch Behördenvertreter sinnvoll.
6. Im Rahmen des von den Unternehmen immer stärker genutzten Cloud Computing rückt die Kontrolle von technischen Daten und Technologien stärker in den Fokus. Die in der Regel transnationale Zusammenarbeit in der LRI erfordert es, dass einheitliche europäische ausfuhrrechtliche Rahmenbedingungen für die Datenverlagerung auf Server in Drittländern und für die Erteilung von Zugriffsrechten aus Drittländern geschaffen werden.
7. Eine klare und rechtzeitige Positionierung der deutschen Politik innerhalb der EU ermöglicht eine deutlich bessere Ausgangssituation für die Industrie, sich bei europäischen (Förder-)Projekten zu platzieren, um Fähigkeitslücken zu schließen, damit Deutschland seiner Verantwortung und seinen Verpflichtungen gegenüber seinen Partnern weiterhin nachkommen kann.
8. Um der Herausforderung im Spannungsfeld zwischen stark steigender Komplexität und Zulassbarkeit in der militärischen Luftfahrt angemessen zu begegnen, ist eine zügige und konsequente Anpassung der Infrastruktur (Regelwerk, Methodik, Personal) im Schulterschluss von Industrie und Sicherheitsbehörden unumgänglich. Anstrengungen auf europäischer Ebene zur Vereinheitlichung und Weiterentwicklung der militärischen Zulassung, angelehnt an das in der zivilen Luftfahrt etablierte Modell (EASA, FAA), sind in diesem Zuge ausdrücklich zu begrüßen.
9. Um truppen- und systemübergreifende Interoperabilität sicherzustellen, sollte durch den Bedarfsträger ein sinnvoller Standardisierungsprozess moderiert werden, um bzgl. der entwickelten Lösungen für alle Beteiligten Zukunftssicherheit zu gewährleisten.

IHR ANSPRECHPARTNER IM BDLI



Robert Friebe
Referent Digitalisierung, Cybersicherheit und UAV

**Bundesverband der Deutschen Luft- und
Raumfahrtindustrie e.V. (BDLI)**
Tel.: +49 (0)30 206140-0
kontakt@bdli.de
www.bdli.de
März 2019

