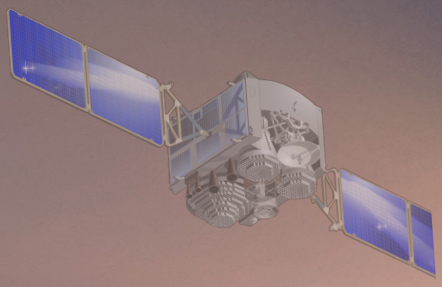
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
**armasuisse**
Science and Technology S+T



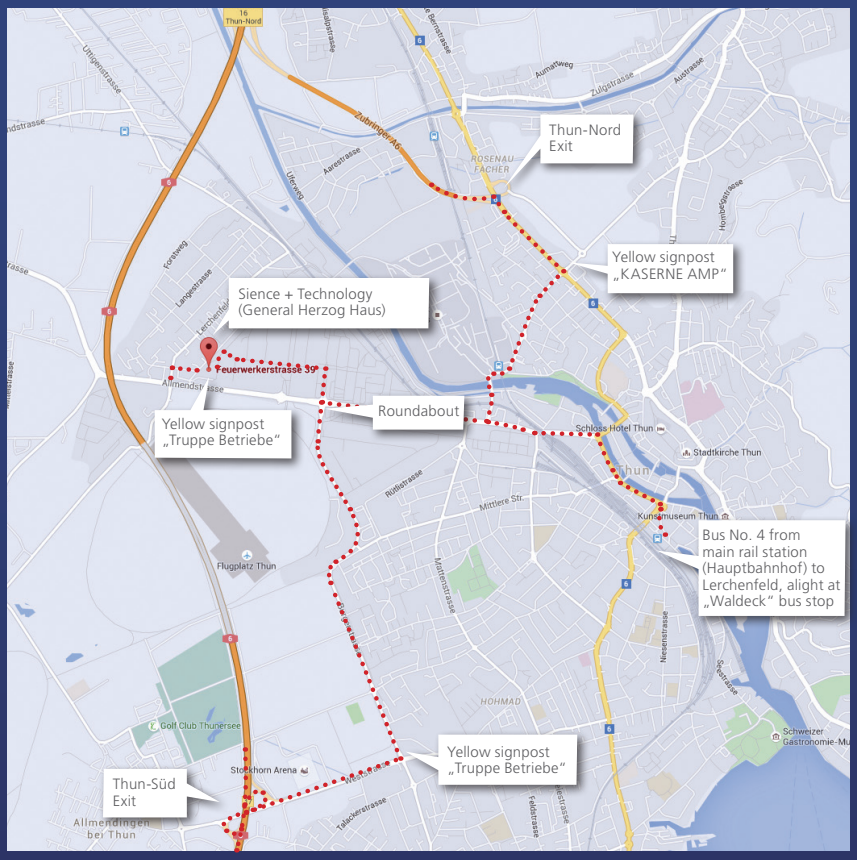
# Defence Future Technologies

## What we see on the horizon

Under the supervision of Dr. Quentin Ladetto

**November 2017**

# Contents/Publishing details




**Contact**
Research Program Manager
Dr. Quentin Ladetto; Tel. +41 58 468 28 09
quentin.ladetto@armasuisse.ch

**www.sicherheitsforschung.ch**

Issued by: armasuisse, Science and Technology, Feuerwerkerstrasse 39, CH-3602 Thun
Edited by: Research Management and Operations Research, tel. +41 58 468 29 11, www.armasuisse.ch/wt


ISBN: 978-3-9524890-0-0

# Editorial

„If a man takes no thought about what is distant, he will find sorrow near at hand."

Confucius (551 B.C. – 479 B.C)

**Dear Reader,**

**If technology is not the only driver in the evolution of warfare, it can be considered for sure as an enabler, not to say the trigger, of most of the changes that occur at the turning point between generations.**

**We, at armasuisse S+T, test and evaluate the operational readiness, functionality and effectiveness as well as the security requirements of current and future systems of the Swiss Armed Forces. We do our best to enable our customers to take conscious technology decisions, minimize investment risks, and keep informed on future technologies.**

**For a country like Switzerland, anticipation is therefore paramount to identify the opportunities and threats a technology can represent for the different military capabilities building our national armed forces. This anticipation is performed concretely by the following research programs:**

- **Reconnaissance and surveillance**
- **Communications cyberspace and information**
- **Impact, protection and safety**
- **Unmanned mobile systems**
- **Technology foresight**

**These research activities not only help gathering experience and knowledge, but they also allow the participation in national and international networks of competences. Different actors have accepted to contribute to this publication and we hope, thanks to them, to provide you with an interesting and instructive reading.**

**Dr. Thomas Rothacher**
Director Science and Technology

# Introduction

"The future is not some place we are going, but one we are creating. The paths are not to be found, but made. And the activity of making them changes both the maker and the destination."

John H. Schaar

**Dear Reader,**

**There are a lot of different ways to anticipate the future, ranging from the basic question if it is worth the challenge to the more proactive attitude of building it. One thing however that is absolutely sure is that if you don't try, you will always have to react rather than to take advantage of a possible opportunity. This is something that you cannot afford if you are considering the defense and security of a country.**

**The armasuisse Science and Technology Foresight research program has the mission to get the necessary understanding of the emerging technologies which might have implications for the military in general, and for the Swiss armed forces in particular. After centralizing the relevant information on emerging technologies on a collaborative platform, the next most important step is to make sense of it, and then, not to be underestimated, to disseminate that information within the armed forces.**

**In parallel to futuristic scenarios, simulations and war-games which allow to better grasp the potential of a technology (translated into the improvement of a system or the creation of a new capability), we believe it is important to get an understanding, or sometimes more a feeling, of the enabling technologies: their potentials, strengths and weaknesses.**

**Building on the report "Defence Future Technologies: Emerging Technology Trends 2015", the present publication offers, via short contributions, an overview of the technological areas that will for sure impact the future of warfare. It is by default not exhaustive, but it emphasizes the competences built by armasuisse Science and Technologies as well as the importance of establishing national and international cooperations. The challenges are many and the ever increasing speed of convergence of the various technological areas makes Technology Foresight a necessary and fascinating activity.**

**I would like to specially thank all the authors for their contribution, and hope that the reader will find in each article some new elements, which would lead hopefully to new contacts and fruitful exchanges.**

**I wish you an inspiring reading.**

**Dr. Quentin Ladetto**
Research Program Manager - Technology Foresight

# Table of Contents

# Antizipation der Technologieentwicklung für die Sicherheit eines kleinen Staates

**Der Staat ist mit seinen Sicherheitsinstrumenten verantwortlich die Lebensgrundlage seiner Bürger vor Bedrohungen und Gefahren zu schützen. Dies tut er vermehrt in einer Welt, die wirtschaftlich stark vernetzt ist und in der eine beschleunigte Entwicklung und eine breite Verfügbarkeit von Technologien eine wichtige Rolle spielt. Dies hat grundlegende Konsequenzen auf die Austragung von Konflikten. Sicherheitskräfte sind gezwungen sich auf kommende Technologieentwicklungen einstellen. Ein kleiner Staat wie die Schweiz tut dies mit Hilfe eines Prozesses zur Technologiefrüherkennung, welcher helfen soll blinde Flecken zu vermeiden und selektiv ausgewählten weitergehenden Abklärungen, mit dem Ziel eine hinreichende Beurteilungsfähigkeit in Technologien mit Relevanz für Sicherheitskräfte zu erlangen.**

**Keywords: Technologie, Monitoring, Disruption, Fähigkeit**

**Autor:** **Dr. Hansruedi Bircher**, armasuisse W+T

## Einleitung

Wie werden militärische Konflikte in 20 Jahren ausgetragen? Diese Schlüsselfrage steht nicht nur im Mittelpunkt der Veranstaltung DefTech 2017, sondern auch bei all jenen, welche an der Weiterentwicklung und der Planung von Sicherheitskräften beteiligt sind. Eine genaue Prognose zu stellen dürfte schwierig sein, denn zu viele verschiedene Faktoren, wie beispielsweise ökonomische, gesellschaftliche oder politische Entwicklungen in verschiedensten geografischen Dimensionen und Ausprägungen erhöhen die Komplexität eines solchen Unterfangens. Beschränkt man sich aber auf die Betrachtung der technologischen Dimension, lassen sich doch ein paar Tendenzen erkennen, welche hinsichtlich der Sicherheit von Staat und Gesellschaft und damit auch hinsichtlich der Austragung von Konflikten, einen wesentliche Einfluss haben werden.

## Sicherheitspolitisches Umfeld

Sicherheit gehört zu den Grundbedürfnissen des Menschen. Die Schweizerische Sicherheitspolitik hat zum Ziel die Handlungsfähigkeit, Selbstbestimmung und Integrität der Schweiz und ihrer Lebensgrundlage gegen Bedrohung und Gefahren zu schützen und einen Beitrag zu Stabilität und Frieden jenseits ihrer Grenzen zu leisten. Um Sicherheit zu gewährleisten werden Sicherheitsinstrumente eingesetzt, zu denen auch die Armee gehört. Diese müssen flexibel und aufeinander abgestimmt den Herausforderungen einer multipolaren Weltordnung genügen, welche sich durch eine zunehmende Globalisierung der Wirtschaft, einer breiten Verfügbarkeit von Informationen und Technologien, sowie einer Ausweitung des Einflussbereichs nichtstaatlicher Akteure auszeichnet. Gerade die breite Verfügbarkeit von Informations und Kommunikationstechnologien bergen das Potenzial der Unterminierung staatlicher Souveränität durch Cyberangriffe oder der gesellschaftlichen Ordnung durch Informations-Operationen, welche in ihren Auswirkungen einem militärischen Vorstoss ebenwürdig sein können.

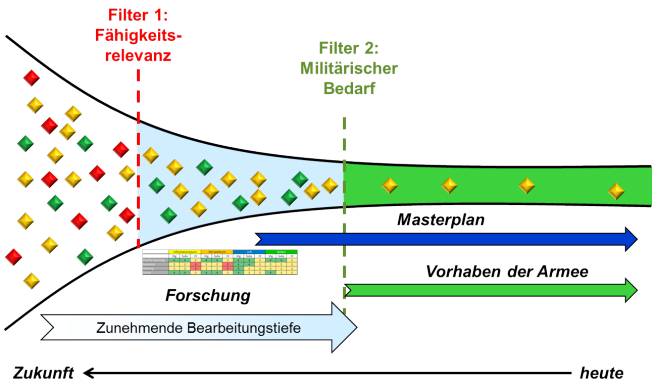



*Abbildung 1: Selektion von Themenfeldern von der Antizipation (langfristig) zur selektiven Vertiefung aufgrund der Fähigkeitsrelevanz bis hin zum Kompetenzaufbau für die Planung und Vorhaben der Armee. Die Themenbreite nimmt ab und die Bearbeitungstiefe ist zunehmend je konkreter Technologien für die Armeeplanung relevant werden. Der Kompetenzaufbau ist auf Beurteilungsfähigkeit ausgerichtet.*

## Abhängigkeit kleiner Staaten

Gerade kleine Länder wie die Schweiz weisen meistens eine grosse wirtschaftliche Abhängigkeit von ausländischen Staaten auf. Sie sind auf eine florierende Exportwirtschaft und freie Marktzugänge angewiesen, weil ihre Binnenmärkte für Produktionsvolumen, welche sich rentabel herstellen lassen, oftmals nicht ausreichen. Dies gilt im Besonderen auch für Unternehmen, welche über Technologien verfügen, die für Sicherheitskräfte und Armee relevant sind. Hinzu kommt, dass viele Staaten in diesem Gebiet ihre Märkte schützen und ihre Industrie aktiv mit Technologieprojekten fördern. Dies bedeutet für einen kleinen und liberalen Staat wie die Schweiz, dass eine flächendeckende Industrie zur Versorgung von Armee und Sicherheitskräften mit entsprechender Ausrüstung ausser Reichweite liegt und dass sie in Bezug auf Rüstungsgüter und Technologietransfer auf Kooperationen mit anderen Nationen angewiesen ist. Diese Abhängigkeit und die fehlende Technologie- und Industriebasis in vielen sicherheitsrelevanten Bereichen ist bei der Ausgestaltung der Mittel zur Antizipation der Technologieentwicklung und deren Konsequenzen auf die Aufgabenerfüllung von Armee und Sicherheitskräften zu berücksichtigen.

## Technologieentwicklung: Kulmination und Disruption

Technologische Innovation ist ein Schlüsselfaktor für die erfolgreiche Platzierung von neuen Produkten auf dem Markt. Auch Armeen und vermehrt auch nicht-staatliche Akteure nutzen neue Technologien. Damit beabsichtigt man gegenüber einem potenziellen oder realen Gegner einen operativen Vorteil zu erlangen. Treiber der technologischen Entwicklung sind die Potenziale, welche Technologiefirmen in oftmals globalen Märkten identifiziert haben. Viele dieser Technologien haben Dual-use Charakter, sind also durchaus auch für Armee- und Sicherheitskreise von Belang. Das Streben nach Marktanteilen liess in den letzten zehn Jahren enorme Mittel in die Lancierung neuer Produkte fliessen, was zu einer massiven Beschleunigung der Technologieentwicklung führte. Dabei muss zwischen inkrementellen Verbesserungen bestehender Technologien, welche meistens mit viel Marketing-Aufwand als „neu“

angepriesen werden, und radikalen Technologiefortschritten unterschieden werden. Radikale Technologiefortschritte führen meistens zu neuen Konstruktionskonzepten und damit zu Inkompatibilität mit Produkten der vorhergehenden Generation. Nach einer Phase der Co-Existenz werden bestehende Technologien dann grösstenteils abgelöst. Für Armeen mit sehr langen Wiederbeschaffungszyklen werden radikale Technologieablösungen vermehrt zum Problem und auch zur Kostenfalle. Sehr oft kündigen sich radikale Technologieentwicklungen relativ lange im Voraus an. Schwieriger ist hingegen die Bestimmung des genauen Zeitpunkts der Verfügbarkeit. Sehr oft ist der Durchbruch abhängig von der Reife peripherer Technologien,

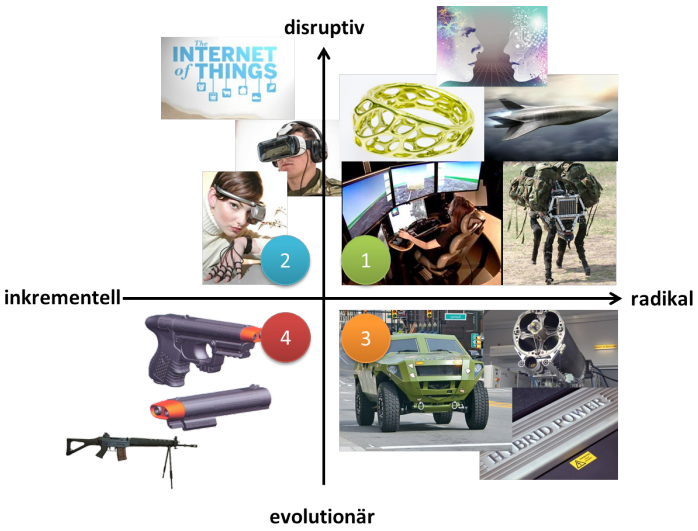



*Abbildung 2: Priorität von Themen der Antizipation (langfristig) in Abhängigkeit radikal neuer Technologiekonzepte und ihres disruptiven Potenzials.*

welche die Ausschöpfung des vollen Potenzials radikaler Technologieinnovationen erst zulassen. So sind beispielsweise leistungsfähige Batterien mit hoher Kapazität und kurzen Ladezeiten eine wichtige Voraussetzung für den Durchbruch der Elektromobilität. Erlangen verschiedene Technologien gleichzeitig die notwendige Reife spricht man von der Kulmination technologischer Entwicklungen. Diese ist die Basis für radikale Ablösungs- und Substitutionsprozesse. Betrachtet man heute beispielsweise die Entwicklung der Technologien um Big Data, künstlicher Intelligenz, Breitbandkommunikation und Digitalisierung der Sensorik, lassen sich einige Technologiecluster ausmachen, welche kulminativen Charakter haben und deshalb einiges an radikalem Entwicklungspotenzial aufweisen. Das Beispiel lässt sich fast beliebig erweitern, wenn wir an die Fortschritte in der Biotechnologie, an digitale Produktion oder an Automation und Roboterisierung denken. Daher steht uns in der kommenden Dekade wohl eine Zeit mit radikalen technologischen Änderungen an.

Die zentrale Frage, welche sich Angesichts dieser Ausgangslage stellt, fokussiert auf die Auswirkungen des technologischen Fortschritts auf Staat, Wirtschaft und Gesellschaft. Ändern sich Formen der sozialen Interaktion, des Verhaltens von Einzelpersonen und von Gruppen oder etablieren sich neue Geschäftsmodelle während dem alte verschwinden, spricht man von Disruption. Für Armeen und Sicherheitskräfte bedeutet Disruption die Auseinandersetzung mit Szenarien und Umständen, für welche bisherige Einsatzmittel und Vorgehensweisen ungeeignet oder unzureichend sind. Solche Szenarien können durch den Einsatz disruptiv wirkender Technologien aktiv zum eigenen Vorteil genutzt oder als Grundlage für eine geeignete Reaktion auf eine neu entstehende Bedrohung analysiert werden. Sicherheitskräfte werden sich wohl darauf einstellen müssen, dass Technologien, welche früher staatlichen Institutionen vorbehalten waren, breit zugänglich werden und dadurch asymmetrisch agierenden Gruppen neue Möglichkeiten eröffnen. Wie am Beispiel von Mikrodrohnen gezeigt werden kann, kommen diesbezügliche Regulierungen oftmals zu spät. Auch die Diskussionen über Informationsverwertung und Wahrung der Privatsphäre oder über Ethik beim Einsatz von autonomen Robotiksystemen zeigen einerseits den disruptiven Charakter laufender Technologieentwicklungen auf und weisen andererseits darauf hin, dass technisch Machbares nicht unbedingt dem gesellschaftlich Akzeptierten entsprechen muss, wobei der Kulturkreis und der zeitliche Wandel von gesellschaftlichen Werten und Normen eine wesentliche Rolle spielen. Deshalb ist die grundsätzliche Diskussion über die Anwendung disruptiver Technologien auf breiter Ebene zu führen, will man nicht Gefahr laufen, dass Ängste, Unsicherheiten und Widerstände von Beteiligten und Betroffenen eine vernünftige Verwendung solcher Technologien verunmöglichen oder sich sogar breiter gesellschaftlicher Widerstand gegen deren Einsatz formiert.

## Handlungsspielraum und Möglichkeiten kleiner Staaten

Wie kann nun ein kleiner Staat, wie die Schweiz, dessen Wirtschaft international stark vernetzt ist und dessen Industrie- und Kompetenzbasis in Technologien mit Relevanz für die nationale Sicherheit bestenfalls Nischen besetzt, die Kulmination und Disruption technologischer Entwicklungen beurteilen und daraus die notwendigen Konsequenzen ziehen? Diese Aufgabe ist komplex und kann sicher durch verschiedene methodische Ansätze gelöst werden.

Beschränkung und Fokussierung: Ein möglicher Weg ist die Fokussierung der Mittel auf die Beurteilungsfähigkeit von Technologien. Dabei sollen Technologien und deren Entwicklung vorerst möglichst breit erfasst und dann beurteilt werden. Dies kann mit Hilfe eines Technologiefrüherkennungs-Prozesses realisiert werden, welcher technologische Megatrends aufnimmt, deren Relevanz für die operationellen Fähigkeiten von Einsatzkräften abschätzt und schliesslich eine Beurteilung der künftigen Verfügbarkeit bzw. der technologischen Reife vornimmt. Weist eine Technologie disruptives Potenzial für Einsatzkräfte auf und ist absehbar, dass diese in den kommenden fünf bis zehn Jahren zur Produktreife entwickelt werden kann, sind in vielen Fällen weitergehende Abklärungen sinnvoll. Dies können vorab Studien zur Erarbeitung von technisch-wissenschaftlichen Grundlagen und zur Identifikation von Experten und Institutionen sein, die massgeblich an der Entwicklung solcher Technologien beteiligt sind. Diese Vorgehensweise erlaubt es in der Beobachtung von technologischen Entwicklungen blinde Flecken zu vermeiden und Hypes von effektiver Technologieinnovation zu unterscheiden. Experimentelle Untersuchungen und der Aufbau von Demonstratoren bilden ein Gefäss um erste Erfahrungen im Umgang mit neuen Technologien zu sammeln, deren Grenzen aufzuzeigen und Verantwortlichen von Sicherheitskräften das mitunter disruptive Potenzial in möglichen Einsätzen aufzuzeigen. Die Abstimmung der Erkenntnisse aus der Technologiefrüherkennung mit dem Fähigkeitsbedarf der Armeeplanung ist die Basis für das gezielte Steuern der Bearbeitungstiefe und das bewusste Eingehen von Kompetenzlücken in der Antizipation von Technologieentwicklungen. Nur die stete Abwägung von Breite in der Erkennung von technologischen Entwicklungen und vertieften Abklärungen in gezielt ausgewählten Bereichen erlaubt einen Ressourceneinsatz, der auch für einen kleinen Staat tragbar ist.

Kooperationen: Wie bereits angetönt verfügen kleine Staaten nur sehr selten über eine flächendeckende und tiefgehende Kompetenzbasis im Bereich von sicherheitsrelevanten Technologien, weil oftmals weder die notwendige Industriebasis noch einschlägige Ausbildungsinstitutionen vorhanden sind. Die Hochschullandschaft der Schweiz ist rein zivil geprägt. Die Kooperation mit Universitäten und Fachhochschulen erlaubt zwar den Zugriff auf die wissenschaftliche Exzellenz

renommierter Forschungsinstitute. Diese ist jedoch hinsichtlich relevanter Schwerpunkte für die nationale Sicherheit stark fragmentiert und weitgehend auf Dual-use Technologien beschränkt.

Oft fehlt es auch an Hintergrundwissen im militärtechnischen Bereich. Dieses kann zwar teilweise durch Schweizer Industrie und KMUs abgedeckt werden. Sehr oft ist dieses jedoch auf Technologien fokussiert, welche zur Herstellung und Weiterentwicklung ihrer Produktepalette verwendet werden können. Die Kompetenzen der schweizerischen Industriebasis sind für die Beurteilung von technologischen Entwicklungen freilich sehr wertvoll. Es bleiben aber Lücken, welche nur mit Hilfe ausländischer Kooperationspartner geschlossen werden können. Dabei ist der Aufbau und die Pflege von Beziehungen zu ausländischen Regierungsstellen als auch die aktive Teilnahme in multilateralen Organisationen im Rahmen der neutralitätspolitischen Vorgaben zentral. Beide Vorgehensweisen eröffnen Kooperationsmöglichkeiten mit einschlägigen Forschungsinstituten und damit den effizienten Zugang zu Experten und Wissen. Der Einblick in Forschungspläne anderer Länder oder Organisationen im Bereich von Militär- und Sicherheitstechnologien ermöglicht eine Bewertung der eigenen Aktivitäten und damit auch die Antizipation von relevanten technologischen Entwicklungen. Zudem multipliziert eine aktive Teilnahme in internationalen Expertengruppen sehr oft den Ertrag der eingesetzten Mittel und ist zugleich auch ein Gradmesser für die Qualität national erbrachter Leistungen.

Übersichtliche Strukturen: Kleine Staaten verfügen oft über schlanke Organisations- und Verwaltungsstrukturen. Dies erhöht die Übersicht hinsichtlich Funktionen und Zuständigkeiten. Direkte persönliche Kontaktnahmen über Organisationsgrenzen und Hierarchien hinweg sind eher möglich. Dadurch können formalisierte Koordinationsabläufe eingedämmt und die Zusammenarbeit verschiedener Disziplinen vereinfacht werden. Auch zur Antizipation technologischer Entwicklungen wird dieser Vorteil genutzt, indem Plattformen für den Austausch und die Diskussion von Erkenntnissen geschaffen wurden, wo sich Vertreter aus verschiedenen wissenschaftlichen Disziplinen (Ingenieur- und Naturwissenschaften, Militärwissenschaften, Medizin, Ökonomie, Ethik, Recht, etc…) und sicherheitsrelevanten Aufgabenbereichen regelmässig persönlich treffen können. Dieser multidisziplinäre Ansatz ermöglicht eine umfassende Bewertung des technologischen Fortschritts. Übersichtliche Strukturen und kurze Wege fördern den Abgleich von diesbezüglichen Erkenntnissen mit Bedarfsträgern im Umfeld der nationalen Sicherheit.

## Zehn Aussagen zur technologischen Entwicklung im Jahr 2037

1. Die Einsatzsysteme zu Land und zur Luft werden zunehmend mit „intelligenten" Funktionalitäten ausgerüstet, welche deren Autonomie erhöhen. Mensch und Maschine arbeiten aufgrund ihrer jeweiligen Stärken als Team zusammen. Die Entwicklung läuft jedoch von „Man in the Loop" zu „Man on the Loop", wobei nach wie vor der Mensch die Verantwortung für das Resultat des Handelns trägt.
2. Dank der weitgehenden Digitalisierung von Sensoren und der Anwendung von künstlicher Intelligenz können Sensorinformationen direkt klassifiziert und ausgewertet werden. Dies erlaubt die Flut von Sensorinformationen auf diejenigen Aspekte zu reduzieren, welche für den Menschen interessant sind. Zudem kann der Einsatz von Sensoren an die Umgebung angepasst und damit optimiert werden. In diesem Zusammenhang spricht man von „intelligenten Sensoren".
3. Die Nutzung von Big Data Technologien und künstlicher Intelligenz eröffnen prädiktive Analysemöglichkeiten. Öffentlich zugängliche Quellen in Form von Texten, Bildern oder Sprache können in Echtzeit semantisch erfasst, mit eigenen Sensordaten und Informationen fusioniert und mit Hilfe von hinterlegten Modellen und neuronalen Netzwerken prädiktiv ausgewertet werden. So können beispielsweise präventiv Massnahmen zur Eindämmung von Netzwerkattacken, zur Vermeidung von Fehlfunktionen komplexer Systeme oder zur Optimierung von Prozessen im Rahmen des Flottenmanagements eingesetzter Systeme vorgeschlagen, bzw. automatisiert eingeleitet werden.
4. Kameras lassen eine effiziente Abbildung der Realität in virtuelle dreidimensionale Umgebungen zu. Diese können durch künstlich erzeugte Elemente ergänzt oder ersetzt werden. Hinzu kommen nach Bedarf die Simulation der akustischen, der haptischen und der Geruchsreize. Virtuelle Realitäten werden nicht nur in Simulatoren von Trainingssystemen eingesetzt, sondern auch in ferngesteuerten Einsatzsystemen zur realitätsgetreuen Nachbildung der Arbeitsumgebung eines Operateurs. In bemannten Systemen dienen virtuelle Realitäten zur Verbesserung des Situationsbewusstseins.
5. Digitale Produktionstechniken, wie 3D-Printing erlaubt es Konstruktion und Herstellung von Objekten örtlich zu trennen. Dadurch können verschiedenste Ersatzteile dort hergestellt werden, wo sie benötigt werden, was die logistischen Abläufe stark verändern wird. Zudem können neue Konstruktionsprinzipien erschlossen werden, welche sich gewichtssparend oder leistungssteigernd auswirken.
6. Die Einsatzkraft der Zukunft agiert vernetzt und verfügt über ein Heath-Monitoring-System, mit welchem seine Einsatzfähigkeit überwacht werden kann. Seine Position, wie auch diejenige seiner Kameraden kann ausserhalb und innerhalb von Gebäuden ermittelt werden. Je nach Bedarf wird er durch ein Exoskelett, Nachtsichtgeräte oder durch die Versorgung mit Zusatzinformationen durch augmentierte Realität unterstützt. Die Energieversorgung wird möglichst autark ausgelegt sein. Die gesellschaftliche Akzeptanz wird massgeblich definieren, wie weit Technologie und Mensch zu einem Gesamtsystem integriert werden.
7. Die weitgehende digitale Vernetzung von Systemen und die Abhängigkeit der Verfügbarkeit von umfangreicher technischer Unterstützung zur Erlangung eines Vorteils gegenüber einer Gegenpartei stellt gleichzeitig eine Verwundbarkeit dar und damit ein potenzieller Angriffsvektor. Deshalb wird der Robustheit und Resilienz von Systemen eine besondere Bedeutung zugemessen. Für den Fall einer degenerierten Systemumgebung sind alternative Vorgehensweisen erarbeitet und eingeübt.
8. Zur Steigerung der Robustheit werden Navigationssysteme redundant ausgelegt. Damit beabsichtigt man die Abhängigkeit zu globalen Satellitennavigationssystemen (GNSS) zu reduzieren. Methoden der bildbasierten Navigation werden stark an Bedeutung gewinnen.
9. Neue Materialien, wie beispielsweise Graphen, lassen den Bau von Superkondensatoren und damit leistungsfähigen Energiespeichersystemen zu. Diese bilden die Voraussetzung für Elektromobilität und genügende Einsatzdauer mobiler elektronischer Systeme.
10. Aktive drahtlose Kommunikations- und Sensorsysteme nutzen das elektromagnetische Spektrum aufgrund hinterlegter künstlicher Intelligenz, je nach Belegung, Umgebungsbedingungen und Bedarf, agil. Die Gesamtleistung kann durch intelligente Optimierung von Sende-, Empfangs- und Datenverarbeitungsparametern gesteigert, die Störbarkeit vermindert werden. Kommunikationssysteme werden vermehrt auch als Sensoren genutzt. Die Vernetzung von elektromagnetischen Sensoren lässt je nach Situation auch rein passive oder ein Gemisch von aktiven und passiven Komponenten zu, was verbesserte Detektion-, Lokalisierungs- und Nachverfolgungsmöglichkeiten erschliesst.

## Ausblick

Sicherheitskräfte müssen sich auf die kommenden technologischen Entwicklungen einstellen. Auch wenn sie nicht beabsichtigen diese zeitnah zu implementieren, wird man sich mit den daraus entstehenden Bedrohungsformen und Verwundbarkeiten auseinander setzen müssen. Beschaffungsorganisationen wie die armasuisse und die Nutzer werden mit einer zunehmenden Technologiekomplexität konfrontiert. Dies heisst nicht, wie unser Alltag im zivilen Leben zeigt, dass damit die Bedienbarkeit schwieriger wird.

Es bedeutet aber, dass die Integration von neuen Technologien in eine Umgebung umfangreiche Kompetenzen erfordert, wenn man dem Anspruch genügen will, die Technologien und damit die Systemumgebung der Armee aktiv steuern und mit den zur Verfügung stehenden Mitteln optimal ausgestalten zu wollen. Dabei wird man wohl um die Implementierung eines Technologiemanagementsystems nicht herumkommen. Ferner ist absehbar, dass linear aufgesetzte Beschaffungs- und Nutzungsprozesse in Projekten mit hoher Technologiekomplexität an ihre Grenzen stossen.

Es braucht neue, wahrscheinlich iterative Ansätze, wie der Betrieb von permanenten Test- und Simulationsumgebungen, in welchen man Stand radikaler technologischer Entwicklungen und deren Auswirkungen auf die Systemumgebung ermitteln kann. Das Disruptionspotenzial müsste mit Ansätzen, wie „Concept, Development and Experimentation“ (CD&E) ermittelt werden. Diese Grundlagen liefern Antworten, wann eine Technologie reif ist und wann es sich aus Sicht der Einsatzkräfte lohnt einen technologischen Generationenwechsel vorzunehmen.


### Dr. Hansruedi Bircher

arbeitet seit 1992 bei armasuisse Wissenschaft und Technologie“ (W+T). Er ist Leiter des Kompetenzbereichs „Forschungsmanagement und Operations Research“ und Mitglied der Geschäftsleitung. Neben einer naturwissenschaftliche Ausbildung als Chemiker mit abgeschlossenem Doktorat verfügt er über eine MBA-Zusatzausbildung in „general Management“ der Universität St. Gallen. Er ist verantwortlich für das Technologie- und Forschungsmanagement in armasuisse. In dieser Funktion ist er im Rahmen des PfP-Programms auch Schweizer Vertreter am „Science and Technology Board“ (STB) der NATO.

# Anticipating the technological challenges of the battlefield of tomorrow

**In a world in which technologies become the catalyst of numerous changes, and in which major innovations come no longer from the military, but from the civil industry, it is paramount to understand how these latter can impact the future of warfare. Translated into systems or into capabilities, technological disruptions will materialize as opportunities as well as threats. To anticipate them, a 360° horizon scanning is performed, covering the trends in Information & Communication, Energy, Nanotechnology & Materials, Life Sciences, Sensors, Robots and Autonomous Systems.**

**Keywords:** **Technology, foresight, disruption, convergence, horizon scanning, futur, trend**

**Author:** **Dr. Quentin Ladetto**, armasuisse S+T

## Introduction

It is almost impossible nowadays not to notice an acceleration in the development of technologies and in the different generations of products coming to market. If we look a little bit closer, we realize that technology is not only accelerating, but that areas are converging, interacting together to generate an exponential growth in terms of use and potential. But how will it continue? Is the adoption of all these new capabilities something natural, or as humans tend to evolve linearly, this convergence will result in a divergence, or rupture, between different groups of the population? Is an abrupt end possible as most of the technologies require energy, rare materials (uranium, lithium, gold, silver, etc.) and petrol, and these are not available in unlimited quantities?

With all these changes taking part in the society, and presented as the 4th industrial revolution, it is obvious that its impacts also reach the battlefields; would it be in the new processes, capabilities, devices, opportunities and threats it creates [1].

What is really new in this revolution is the accessibility to the technologies (not limited to state actors) and their increasing dual-use nature. This dual-use has a direct impact in the researchers working on these technologies, as a career might appear less appealing in the defence sector than in other industries. If we consider Artificial Intelligence, the large disparity in commercial versus military R&D spending could have a cascading effect on the types and quality of autonomy that are incorporated into military systems [2]. Will civilian products be more efficient than their analogue military ones? This might be the case, and it opens at the same time the question of availability as they might be acquired by non-state actors, terrorists or not.

With the pressure to be the first on the market and the high dynamic of the different research ecosystems, the challenge is therefore to assess WHEN and not IF a technology will become available.

## Military challenges

All these new technologies and their combinations generate numerous military challenges alimenting the dream (or fear) of potential disruption mastered by one actor only.

The unpredictability of the threat is one of them; new devices can be created and they can be mission specific or they can be created for one specific occasion only, meaning that it is a unique element not produced in series, and therefore not offered as such by the defence industry.

Connected with the unpredictability is the growing asymmetry in conflicts: old systems vs new systems; state and non-state actors; respect or not respect of the different conventions. You have to plan and understand the potentials and threats these technologies are representing even if you are not using them.

Used in old systems, these technologies might expand their life-cycle and offer new capabilities. This would mean that there might be many more generations of a same product on the battlefield than it is the case today. Modularity will be a necessity. A different generation can be obtained by update of some hardware, but also and most frequently by the update of some software/firmware. In the last case, the reliability of the source as well as the guarantee of the update itself are paramount. All the different systems will also generate an important amount of data to document any action and mission. This data will become of strategic importance as it will enable a learning process for every system to be smarter on day 2 of a conflict that it was on day 1.

Interoperability will be of growing importance as each system will have to be able to act as individual, but also to cooperate within a swarm with elements of different type and different generations.

As the digital and the use of algorithms are rising also on the battlefield, there might be the temptation to focus on the software rather than the hardware, and to spend efforts to master the technologies created by the civil industry, rather than to invest in the long process of developing new military ones.

As a consequence of these new paradigms, it might become of interest to consider an additional phase within the OODA (Observe-Orient-Decide-Act) loop with respect to innovation, as going quicker through the loop alone might soon be not sufficient anymore.

## Technology Trends

Considered from a megatrend point of view, there is a feedback loop between the technologies and the capabilities they serve on the battlefield. Would a new technology enable a capacity, or the need for a capacity motivate the creation of a new technology? It might depend on the situation, but the improvements in technology are for sure supporting the main military objectives megatrends.

**Awareness**: Awareness about multiple elements such as location, physical indicators, situation, is available anywhere at anytime thanks to communication and connected sensors.

**Distance**: Distance is not an issue anymore as systems can be operated remotely from the theatre of operations.

**Precision**: From observation to action, sensors and processing power are enabling stochastic model to guide ammunitions better or to validate decisions.

**Speed**: Speed is increasing and it is facilitated by developments in different areas ranging from mobility to computing.

Materializing these trends, the following elements are considered potentially disruptive if reaching maturity [3][4]. Like the nuclear bomb, it is to expect that some of them will play a dissuasive more than an active role on the battlefield. However, countries will need to master them to maintain their military power.

- Swarms
  The necessity of fighting simultaneous an important numbers of (potentially low-cost) systems might require new capabilities as the existing platforms could be completely overwhelmed.
- Human-Machine Teaming
  The presence on the battlefield of both human and machines, autonomous or not, will require interactions between them, which might induce new tactical aspects. As machines will improve, it might also become more difficult to understand and anticipate their behavior decided by artificial intelligence (AI).
- Hypersonic vs low velocity weapons
  Speed, if connected with some type of guidance, might render obsolete the present anti-missile systems. They enable a nuclear attack everywhere on Earth almost instantaneously. In contrast, drones are capable to carry explosives almost at no speed and at really low altitude above ground.
- Militarization of Space
  Space represents a strategic asset with a force multiplayer effect for every country willing to develop a politic of power. The space dependence of the world economy makes any military action in space a high risk.
- 3D Printing
  If 3D printing offers new logistic opportunities for the armed forces, it also creates new threats for the manufacturing by non-state actors of weapons or other elements prohibited by treaties.
- Synthetic biology
  The use of synthetic biology to modify natural biological systems is used in various areas ranging from health to agriculture. The possibility to directly edit the DNA can enable the creation of new bio-agents presenting new threats potentially coming from non-state actors.
- Neurosciences
  With the goal of understanding how the brain and the nervous system work, neuroscience is the basis for the augmented soldier and advanced man-machine interfaces.
- Quantum encryption/computing
  If the quantum computing becomes reality, all the encryption technologies and security protocols used until now would become obsolete.

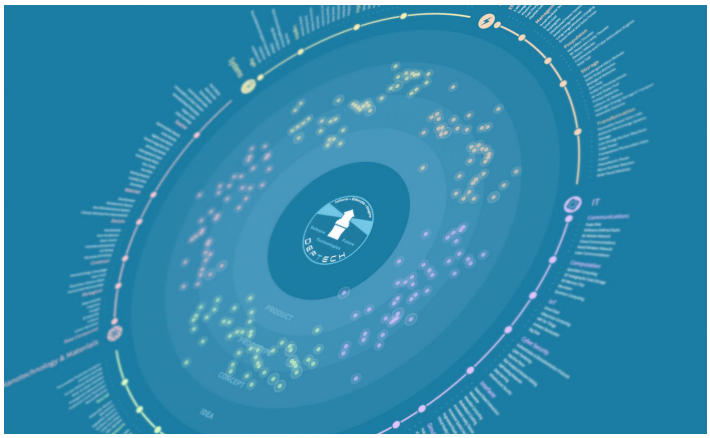


*Figure 1: Collaborative technology platform supporting and regrouping the expert-sourcing information approach.*

In order to cover the 360° horizon of the technologies and get a structured basis for analysis and anticipation, a collaborative platform focusing on technologies was created in 2015 (Figure 1) [5][6]. The goal of the technology platform is first to have an open place where technologies and new concepts can be discussed and assessed. Second, it offers the possibility to dynamically visualize the information considering different points of view (doctrine, system, readiness, scenarios, etc), as well as visualize the connection and interactions between the different technologies. The horizon is divided into 6 main, debatable, categories [7]. Each category is then organized into clusters, composed by the single technologies.

## Information & Communication

Being at the center of what is called sometimes called "The fourth industrial revolution" the technological developments in data transmission, storage, analysis and security have been the main actors of this revolution. Together, they gave birth to new areas of interest such as such as Big Data, Data Mining, Cyber-Warfare and Artificial Intelligence which impacts on the society are still to be understood.

The technology trends pursue the following goals:

Increase and improve computing power, storage and security: Quantum -computers, -sensors, -encryption, - communication, when operational, will disrupt the ICT ecosystem.

Make better and quicker decision: Artificial Intelligence opens new possibilities and their discovery has just started. You can take advantage of other people experience and accelerate any learning curve.

Be connected everywhere: new constellations of small satellites and high altitude long endurance platform together with laser communication.

Understand and explore a real or simulated environment: artificial and virtual reality help providing direct information to the user superposed with the object in real or simulated environments.

## Energy

The ability to acquire energy is becoming more and more compact as alternative methods in the energy fields open the way to renewable sources such as sun, the wind, biofuels. Progress in storage, charging/generation, and weight are some of the key enablers for autonomous and remote pilot systems.

The technology trends pursue the following goals:

Optimize power sources to become smaller, lighter, safer, cheaper, charge faster and last longer: new batteries using alternative chemistries and materials are being developed; supercapacitors and fuel cells.

Generate energy using different approaches and sources: use movement, pressure, heat to harvest or scavenge energy.

Optimize solar energy with cells that are more efficient, smaller and flexible: use new options for power generation and deployments on fixed and flexible supports.

Charge your devices remotely: wireless charge electronic equipments, implanted devices and electric vehicles.

## Nanotechnology & Materials

The field of materials and manufacturing is vast with emerging research in materials with new properties allowing new applications and manufacturing processes.

The technology trends pursue the following goals:

Produce spare parts or new parts "on demand": Additive manufacturing (3D Printing) is opening the way to new approaches for faster, cheaper and more complex fabrication.

Novel materials with enhanced and multifunctional properties: from stretchable nanofibers tougher than Kevlar to self-healing material, transparent resin and biodegradable electronics, innovation is intense to make materials tailored to specific uses

being generally more resistant, lighter and cheaper to produce.

Produce drinkable water everywhere: different research to easily clean and treat water, from saltwater to treat water from air-conditioning units.

## Life Science

Life sciences and enabling technologies (such as ICT) are making major progresses as they are driven by the changes in the social domain. Societal pressures of aging, access to food, freshwater or energy, increasing global interconnectivity and commercial imperatives are expected to result in the swiftest advances to these technologies.

The technology trends pursue the following goals:

Edit and modify the genome: Advances in genetic engineering – CRISPR-Cas9 open the way to personalized medicine.

Predict human behavior and social interactions: Biometric algorithms allowing language, behavior and physiological pattern recognition.

Augment the human capabilities and improve the human-machines interface: Artificial implants offering additional sensory abilities to people (from the repaired to the augmented soldier); drugs that improve memory, intelligence, endurance and overall physical performance. Brain-machine interface as a long-term goal in parallel to voice, gesture recognition and optical sensing to communicate with computing and autonomous systems.

Create new material with increased properties: Synthetic biology is used to create new materials, also inspire by nature (biomimicry), as well as new energy sources.

Produce organs so that you don't rely on donors: Use additive manufacturing to bio-print the organs, or let them grow on some genetically modified animals.

## Sensors

Enabling the digitalization of more and more elements of the society, sensors are becoming ubiquitous as they are integrated in all aspects of our everyday life. Connect objects, also known as The Internet of Things, benefit from all improvements in micro-electromechanical systems (MEMS), communication and data sciences. They will affect all the different sectors of the society, from transportation to energy, to agriculture.

The technology trends pursue the following goals:

Long distance biometric identification: improved biometric to facilitate identification and reduce identity theft.

Improve situational awareness for autonomous vehicles: development of low-cost new lasers-on-a-chip that would be able to scan in every direction at 100'000 Hertz.

CBRN detection with no human casualty: hyperspectral, terahertz and biochemical sensors integrated in unmanned systems.

Navigation and positioning without satellite system: atom-based inertial technologies to become independent of GPS.

Monitoring goods to certify quality control: sensors monitoring temperature, humidity, shocks, vibrations, etc providing the history of a good to decide if it is safe to use of consume.

Augmented human with restored or enhanced capabilities: from exoskeletons to advanced prosthetics, robotized components are enabling or improving new natural and hybrid capabilities.

## Robots and Autonomous Systems

The number of unmanned and automated systems is increasing. Starting with a man IN the loop (like remotely piloted drones), the trend is to have systems, and swarms of systems, able to perform missions without a human operator and manage extensive tasks in complicated environments for extended periods of time (man OUT of the loop).

The technology trends pursue the following goals:

Increase in intelligence and autonomy: at the crossroad of numerous technologies, systems are becoming more and more intelligent and are able to interact with humans, taking over certain repetitive or programmable tasks.

Minimize human casualties using disposable assets: everywhere possible, robots and unmanned systems will be used to perform missions and tasks which might endanger human lives.

Improve human capabilities (towards transhumanism): various types of exoskeletons and advanced prosthetics allow to restore and/or enhance human capabilities and senses.

Remotely monitor health, diagnose and operate: Use sensors, data mining and new human-machine interfaces to provide remote health diagnoses capabilities up to robotic surgery.

## Conclusions

The sustained high pace of development in technologies and the convergence of various domains, facilitated by our connected and globalized society, open the way to new opportunities or threats, and this at system (Figure 2) as well as at capability level.

It is however not always clear if and how a new technological improvement will make its way onto the battlefield considering the numerous challenges it must overcome (cost, acceptance, ethics, etc). Emphasized by the asymmetry between opponents, expensive and complex new systems might offer limited superiority in time and in effectiveness, which will challenge their procurement [8]: The more the soldier is equipped, specialized and trained, the more „facilitated" the combat is, the more the resistance manages to adapt by actions out of the fight, and the more, at the end, the results disappear.

The diversity of threats made possible and available to state and non state actors thanks to technologies is in itself a real challenge. To counter them, innovation, flexibility and adaptability will be key, and to be successful, it is necessary to find a way so that new ideas can make their way already before the old ones are out.

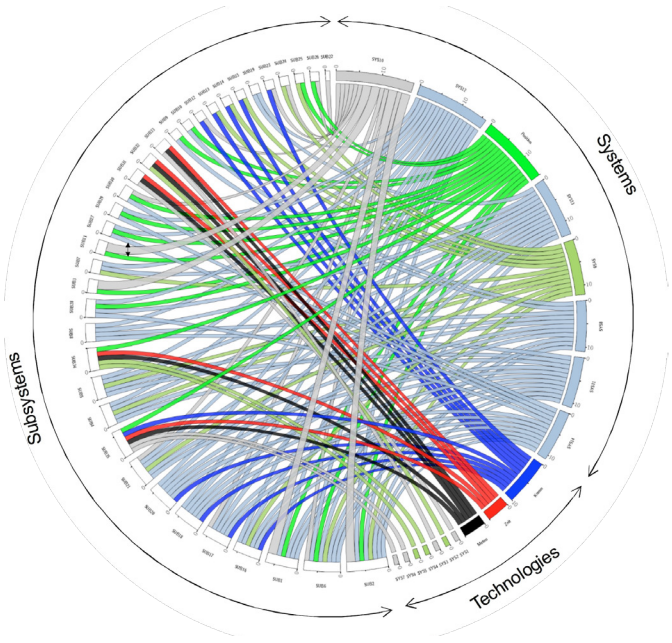



*Figure 2: Representation on a same graph of the connexions between the technologies, the subsystems and the systems. Such image allows to visualize the importance of each element and how they interact. This is important to better understand synergies and where modularity might help to reduce logistic efforts, improve commonality and therefore reduce cost.*

## Acknowledgement

Special thanks to Dr. Michael Rüegsegger for his support in the discussion and the generation of the illustration combining technologies, subsystems and systems.

**Dr. Quentin Ladetto**
is research director at armasuisse Science and Technology. He leads the Technology Foresights program which goal is to anticipate and get the necessary understanding of the emerging technologies which might have their implications for the military in general and the Swiss armed forces in particular.
Quentin owns a PhD in Geomatics from the Swiss Institute of Technology in Lausanne (EPFL) and an Executive MBA in management and corporate finance from HEC Lausanne.

He can be reached at
quentin.ladetto@armasuisse.ch

## References

[1] M-A. Ryter (2017), La quatrième révolution industrielle et son impact sur les forces armées, Military Power Review, Nr. 1/2017

[2] K. Schwab (2016), The Fourth Industrial Revolution, World Economic Forum

[3] M. L. Cummings (2017), Artificial Intelligence and the Future of Warfare, Research Paper, Chatham House.

[4] Chocs Futurs (2017), Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN)

[5] Q. Ladetto (2015), Defence Future Technologies – Emerging Technology Trends, armasuisse Science and Technology.

[6] http://envisioning.io/deftech & http://tdb.envisioning.io

[7] Ksenia Ivanova and Guy Edward Gallasch (2016), Analysis of Emerging Technologies and Trends for ADF Combat Service Support 2016, Australian DoD, Science and Technology

[8] Patrick Clervoy (2016), Le paradoxe de la reine rouge, DSI hors-série N°45 – Le Soldat Augmenté, janvier 2016

# Die Zukunft der Robotik und ihre Auswirkungen auf Sicherheit und militärische Operationen

**Der Beitrag befasst sich mit der Zukunft der Robotik für Anwendungen im militärischen Bereich. Da sich die Zukunft nicht exakt prognostizieren lässt, wurden zur Beschreibung Szenarien, also hypothetischen Zukunftsbilder, entwickelt. Die Entwicklung und Interpretation der Szenarien basierte dabei auf einer schlüssigen Kombination denkbarer Entwicklungsannahmen. Eine anschliessende, erste Beurteilung der Szenarien durch ein Expertenteam deckte auf, dass die erwartete Entwicklung stark von der gewünschten Zukunft abweicht.**

**Keywords:** **Szenarioentwicklung, Zukunftsbilder, Systembild, Robotik, Unbemannte Systeme, Killerroboter, Sicherheit, Militärische Operationen, Schlüsselfaktoren**

**Autoren:** **Dr. Mark Höpflinger**, armasuisse W+T; **Dr. Alexander Fink**, ScMI Scenario Management International AG

## Einleitung

Obwohl vorwiegend noch in den Kinderschuhen, erregt das Thema ‚Mobile Robotik' zurzeit grosse Aufmerksamkeit und Roboter beginnen langsam aber stetig, Einzug ins zivile und militärische Leben zu halten. Heutige mobile Roboter funktionieren vergleichsweise einfach und können noch kaum mit vielfältigen Aufgaben in komplizierter Umgebung umgehen. Aktuelle Forschungsresultate, u.a. getrieben durch den Fortschritt im Bereich der Datenverarbeitung (Sichtwort ‚Künstliche Intelligenz'), der Elektronik und Mechanik lassen aber erahnen, welches zukünftige Potential entfesselt werden könnte. Es wird kaum angezweifelt, dass die militärische Verbreitung und die Bedeutung von Robotern weiter zunimmt. Wie die Situation in Zukunft, beispielsweise nach 2037 aussieht, lässt sich natürlich nicht exakt voraussagen. Es können jedoch Entwicklungsmöglichkeiten in Form von Szenarien, also Zukunftsbildern, aufgezeigt werden. Dies erlaubt, über die Zukunft nachdenken zu können, ohne sie exakt vorhersagen zu wollen und erlaubt die Ableitung von Handlungspfaden.

## 1. Szenarioentwicklung

Eine möglichst ‚treffende' Einschätzung der Zukunft ist essentiell für deren Antizipierung.

Die Wahl des optimalen Instruments zur Einschätzung der Zukunft, also ‚Prognosen', ‚Trends' und ‚Szenarien' hängt davon ab, wie weit die einzuschätzende Zukunft von der Gegenwart entfernt ist [FS11]:

Zur kurzfristigen Betrachtung der Zukunft werden üblicherweise Prognosen mit quantitativen, auf Extrapolationen basierenden Aussagen verwendet. Dies dient einer Unternehmung beispielsweise zur Beurteilung und zur Fällung von operativen Entscheiden. Für mittelfristigere Betrachtungen werden Prognosen verwendet, welche auf der Analyse von aktuellen oder absehbaren Trends basieren und das richtige Entscheiden auf taktischer Ebene erlauben sollen. Für längerfristige Betrachtungen sind Prognosen eher ungeeignet – eine quantitative Einschätzung mittels Extrapolation der Vergangenheit ist langfristig ungenau und fehlerbehaftet und Trends können zu falschen Annahmen führen. Szenarien hingegen dienen der qualitativen Beschreibung einer längerfristigen Zukunft (> 10 Jahre) und als Instrument für strategische Entscheidungen, beispielsweise zur Anpassung einer Unternehmensstrategie.

Unter Szenario wird hier eines von mehreren, potentiell möglichen Zukunftsbilder verstanden, das auf einer schlüssigen Kombination denkbarer Annahmen bezüglich der Entwicklung beruht [FS16]. Zur Beschreibung der möglichen Zukunft werden verschiedene Zukunftsbilder generiert, welche dominante Merkmale der Entwicklung abbilden. Die Verknüpfung der Szenarioentwicklung mit der Analyse der strategischen Nutzung kann als übergreifendes Rahmenkonzept, Szenario-Management' bezeichnet werden.

Die Szenarioentwicklung erfolgte in den drei Schritten (1) Szenariofeld-Analyse und Auswahl von Schlüsselfaktoren, (2) Entwicklung von alternativen Zukunftsprojektionen und (3) Bildung und Analyse der Szenarien. Danach lagen mehrere Szenarien vor, die in einer ‚Landkarte der Zukunft' visualisiert wurden. Dem schloss sich die Szenario-Interpretation an, die wiederum drei teilweise parallele Teilprozesse beinhaltet: (4A) die zielgruppengerechte Kommunikation der Szenarien, (4B) die Bewertung der Szenarien und (4C) die Konsequenzanalyse, bei der die Auswirkungen der Zukunftsbilder auf die eigene Organisation abgeschätzt werden.

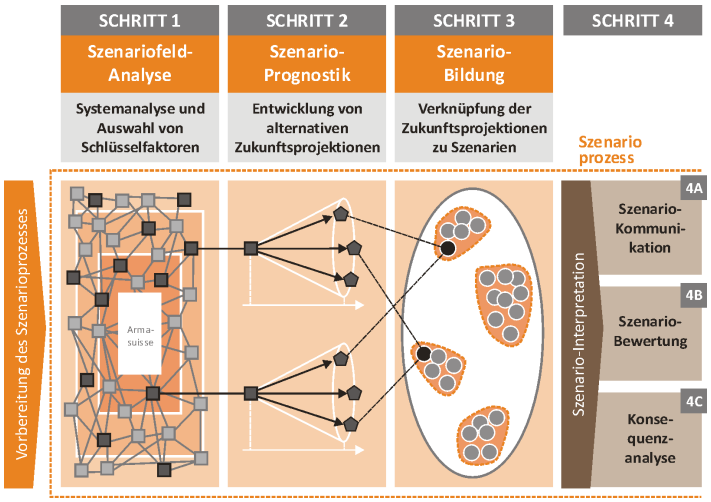



*Bild 1: Phasen der Szenarioentwicklung und Szenario-Interpretation*

### 1.1 Szenariofeld-Analyse: Systembild, Einflussfaktoren und Schlüsselfaktoren

Das Szenariofeld ist der Bereich, für den in den Szenarien alternative Entwicklungen beschrieben werden. Da es hier um die Beschreibung grundlegender Entwicklungen ging, war die armasuisse selbst nicht Gegenstand der Betrachtung. So entstanden Umfeldszenarien, für die das Szenariofeld folgendermassen definiert wurde: „Die Szenarien beschreiben mögliche Entwicklungen von robotischen Systemen– insbesondere der unbemannter Systeme – sowie der damit verbundenen Technologien und deren Auswirkungen auf Sicherheit und militärische Operationen."

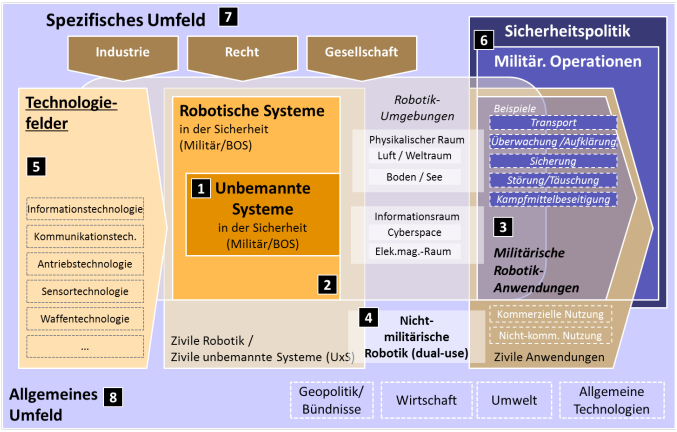



*Bild 2: Systembild mit acht Einflussfeldern*

Bild 2. zeigt das Systembild, welches für die Szenarioentwicklung verwendet wurde. Im Mittelpunkt des Systembildes stehen die „unbemannten Systeme“ für Anwendungen im Bereich der Sicherheit (1). Ein unbemanntes System beinhaltet eines oder mehrere unbemannte Vehikel sowie die nötige Infrastruktur (Kommunikationsmittel, Kontrollstationen, Immobilien etc. zum Betrieb. Die Vehikel können am Boden, in der Luft, unter/auf Wasser oder im Weltraum agieren. Übergeordnet befinden sich die „Robotischen Systeme“ (2), welche auch stationär, beispielsweise als fix montierte Roboterarme in Produktionsstätten, oder zur Ergänzung des Körpers des Menschen eingesetzt werden können. Robotische Systeme werden bereits heute zahlreich und in verschiedenen militärischen Aufgabengebieten (3) eingesetzt. Die meisten aktuellen Anwendungen finden unbewaffnet statt, beispielsweise im Bereich der Aufklärung und Überwachung. Die Verbreitung von bewaffneten Systemen nimmt aber zu.

Das grösste, wirtschaftliche Potential von mobilen Robotern wird im Zivilen erwartet (4) (Ref). Die kommerzielle Nutzung von stationären Industrierobotern ist seit Jahrzenten weit verbreitet und auch mobile Systeme werden heute, üblicherweise in ‚einfacher‘, kontrollierter Umgebung, produktiv eingesetzt, beispielsweise im Bereich der Lagerbewirtschaftung. Kompliziertere Anwendungen werden angedacht und medienwirksam demonstriert, sind aber kaum implementiert. Die nicht-kommerzielle Nutzung beschränkt sich heutzutage auf die Verwendung von einfachen Servicerobotern (z.Bsp. als Staubsauger, Dachrinnen- oder Poolreiniger) und Systemen im Freizeitbereich.

Die Entwicklung der ‚unbemannten Systeme‘ der Robotik wird durch verschiedene Technologiefelder beeinflusst (5), beispielsweise dem Feld der Informationstechnologie mit den Schlagwörtern ‚Big Data‘, ‚Cloud Computing‘ und ‚Künstliche Intelligenz‘ (KI). In Bezug auf KI zeichnet sich ab, dass Roboter für den Einsatz in alltäglichen, unkontrollierbaren Umgebungen mit unvorhersehbaren Ereignissen nicht mehr klassisch programmiert werden können sondern in der Lage sein müssen, sich anzupassen/zu lernen. Zum Datenaustausch mit Datenbanken, mit Rechenzentren, aber auch untereinander oder mit den Operateuren spielt Kommunikationstechnologie eine entscheidende Rolle. Neben den erwähnten Technologiefeldern gibt es diverse weitere, welche einen starken Einfluss auf die Entwicklung der Robotik ausüben können sowie das spezifische Umfeld in Bezug auf Industrie, Recht und Gesellschaft (7) und das allgemeine Umfeld mit Geopolitik, Wirtschaft, Umwelt und allgemeinen Technologien (8).

Basierend auf dem Systembild und dessen Einflussfelder wurden insgesamt 80 Einflussfaktoren identifiziert, welche die acht Felder beschreiben. Die grosse Anzahl der Faktoren erlaubt eine breite Erfassung des Szenariofeldes, ist aber für die weitere Szenarioentwicklung kaum sinnvoll und schlecht handhabbar. In einem nächsten Schritt wurde das Set von Einflussfaktoren reduziert auf die wesentlichen Faktoren, sogenannte Schlüsselfaktoren. Dazu wurde das Instrument der Vernetzungsanalyse verwendet: Für jeden Faktor wurde seine Aktivität, ein Mass für die Wirkung des Faktors auf andere, und seine Passivität, ein Mass für die Beeinflussung des Faktors durch andere Faktoren, bestimmt.

Bei der Auswahl der Schlüsselfaktoren wurden folgende drei Kriterien besonders beachtet:

- Vernetzung: Schlüsselfaktoren sollen eng miteinander vernetzt sein um wesentliche Zusammenhänge zu repräsentieren und prägnante Szenarien zu ermöglichen.
- Relevanz: Schlüsselfaktoren sollen einen grossen Einfluss auf den relevanten Kern des Szenariofeldes haben.
- Hebelkraft: Faktoren, welche trotz geringer Vernetzung einen grossen Einfluss auf das Szenario haben, wurden auch als Schlüsselfaktoren berücksichtigt.

Aufgrund der Analyse und subjektiven Gruppendiskussionen wurden die folgenden 18 Schlüsselfaktoren bestimmt.

1. Militärische Auseinandersetzungen
2. Cyber-Konflikte im Sicherheitsumfeld
3. Militärische Streitkräfte
4. Internationale Regulierung / Zulassung von Waffen (-technologien)
5. Rechtliche Grundlagen und Rechtsfähigkeit robotischer Systeme
6. Robotische Systeme in den Streitkräften / in den Kommandostrukturen
7. Bedrohungen / Gefahren und Abwehrbarkeit von robotischen Systemen
8. UxS/Roboter als kritische Infrastruktur / Abhängigkeit der Robotik von Infrastrukturen
9. Künstliche Intelligenz
10. Roboterisierung des Menschen / Humanisierung von robotischen Systemen
11. Beziehung zwischen Mensch und UxS (allgemein und militärisch)
12. Autonomie und Vernetzung robotischer Systeme
13. Steuerung und Kontrolle militärischer UxS
14. Verfügbarkeit UxS im Militär / BOS
15. Rolle / Bedeutung von UxS im Militär
16. Einsatz von UxS/Robotik zur Kriegsführung (Waffeneinsatz)
17. Aggressoren mit UxS-Einsatz
18. Militärischer unbewaffneter Einsatz von UxS/Robotik

## 1.2 Entwicklung von alternativen Zukunfts-projektionen

Für jeden der 18 Schlüsselfaktoren wurden mindestens zwei Dimensionen festgelegt, welche die relevanten Entwicklungsmöglichkeiten des Faktors möglichst gut abbilden sollen. Dadurch wurden zukünftige Zustände bestimmt, sogenannte Zukunftsprojektionen, welche später, durch die Berücksichtigung von Projektionen anderer Schlüsselfaktoren zu komplexen Zukunftsbildern verknüpft wurden.
Beispielsweise entstanden für den Schlüsselfaktor 8, „Roboter

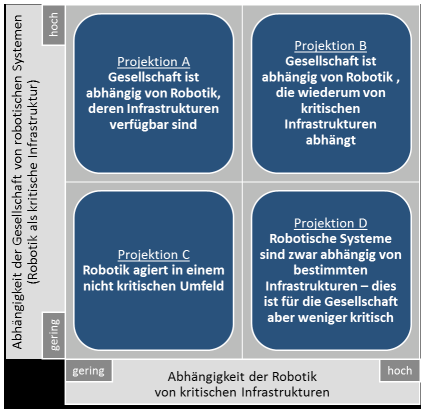



*Bild 3: Bsp. von Zukunftsprojektionen zum Schlüsselfaktor 8*

als kritische Infrastruktur / Abhängigkeit der Robotik von Infrastrukturen“ vier Projektionen, welche den unterschiedlichen Grad der gegenseitigen Abhängigkeit beinhalten (Bild 3).

## 1.3 Bildung und Analyse der Szenarien

Aus dem Projektionsportfolio erfolgte anschliessend in sechs Schritten die Szenariobildung. Mittels einer Konsistenzbewertung wurden Widersprüche zwischen den Zukunftsprojektionen identifiziert. Eine automatische Konsistenzanalyse (SCMI Szenario Software) wurde durchgeführt um alle denkbaren Gesamtkombinationen (sog. Projektionsbündel) zu überprüfen. Anhand einer Clusteranalyse wurden Gruppen von Projektionsbündeln (auch als Rohszenarien bezeichnet) identifiziert. Dabei ist das Ziel, dass die einzelnen Rohszenarien möglichst verschieden zueinander sind, aber Projektionsbündel enthalten, welche möglichst ähnlich sind. Einerseits erlaubt die Verwendung einer grossen Anzahl Rohszenarien eine detailliertere Beschreibung

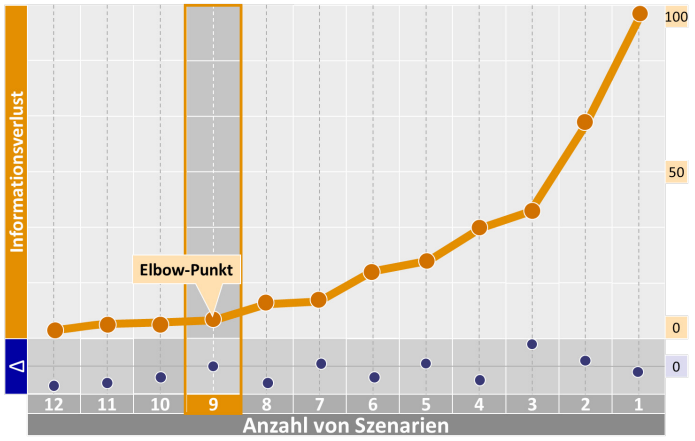



*Bild 4: Darstellung des Informationsgewinns in Abhängigkeit der Anzahl Szenarien*

der möglichen Zukunft, andererseits wird dadurch der Aufwand zur Beurteilung der Szenarien und zur Kommunikation erhöht. Zur Bestimmung der ‚optimalen‘ Anzahl der Szenarien wurde u.a. eine Auswertung bezüglich Informationsverlust verwendet [Bild 4] und die Anzahl damit auf neun festgelegt.

Zur Visualisierung des Zukunftsraumes wurden die Projektionsbündel/Rohszenarien so angeordnet, dass eine ‚Landkarte der Zukunft‘ entsteht [Bild 5], welche die charakteristischen Merkmale (prägnante Projektionen) der Szenarien hervorhebt. Die Einteilung der Szenarien innerhalb der Landkarte basiert auf einer Multidimensionalen Skalierung, wobei Szenarien mit ähnlichen Elementen dicht

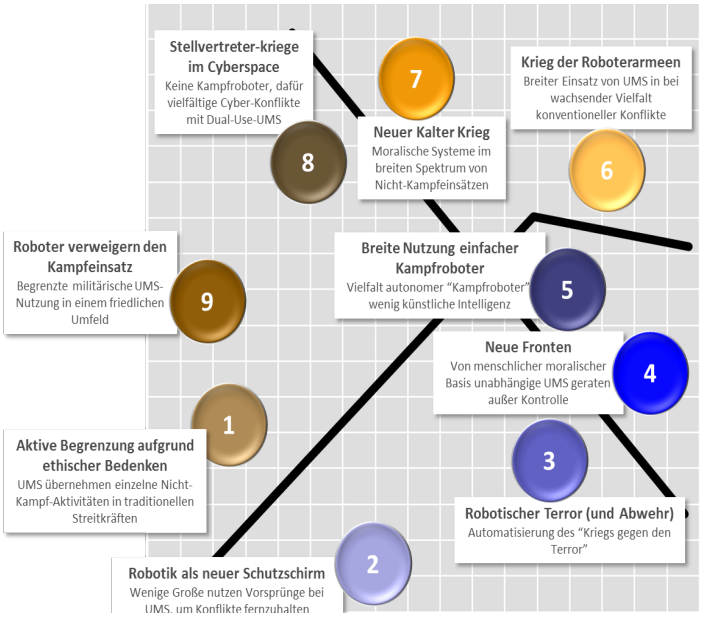



*Bild 5: Neun Szenarien in der Landkarte der Zukunft*

beieinander angeordnet werden. Durch eine grafische Analyse der Landkarte ist es nun möglich, die zentralen Kernfragen zu identifizieren. So zeigt Bild 5 exemplarisch vier Bereiche der Landkarte: So weisen die drei Szenarien im Sektor A insgesamt einen eher geringen Umfang militärischer Auseinandersetzungen auf. Bei den Szenarien im Sektor B erfolgen militärische Auseinandersetzungen primär in Form asymmetrischer Konflikte. Auf der anderen Seite der Landkarte – im Sektor D – findet man zwei Szenarien, in denen militärische Auseinandersetzungen primär in Form zwischenstaatlicher Konflikte erfolgen. Die beiden Szenarien im Sektor C zeigen ein breites Feld unterschiedlicher militärischer Konflikte – zwischenstaatlich und asymmetrisch.

Eine solche Analyse der Kerndimensionen vermittelt einen Eindruck von der Komplexität des betrachteten Themenfeldes. Gleichzeitig ließ sich die Komplexität wieder reduzieren, in dem drei zentrale Fragestellungen identifiziert wurden:

1. Wie könnte das zukünftige Sicherheitsumfeld aussehen; welche Bedrohungen ergeben sich durch UxS?
2. Wie könnten sich unbemannte Systeme insgesamt entwickeln?
3. Wie könnte die Nutzung von unbemannten Systemen in den Streitkräften/BOS zukünftig aussehen?

Für diese drei übergeordneten Fragestellungen lassen sich wiederum sechs spezifische Perspektiven einnehmen, die in Bild 6 dargestellt sind. Innerhalb dieser Perspektiven können auf der Landkarte jeweils spezifische Bereiche mit ähnlichen Entwicklungen identifiziert werden.

„Roboterisierung“ des Militärs/BOS (Perspektive 1, links oben):

Sektor A: Szenarien im Sektor A beschreiben eine Zukunft mit einem geringen Nutzung von Robotern durch Streitkräfte.

Sektor B: Die Szenarien beschreiben eine Zukunft mit einem hohen Grad der ‚Robotisierung‘ der staatlichen Streitrkäfte.

Sektor C: Die Szenarien beschreiben eine Zukunft mit einem hohen Grad der ‚Robotisierung‘ der staatlichen Streitrkäfte sowie der „Schurkenstaaten“/ Terrorgruppen.

Einsatz und Bedrohungen durch Roboter (Persp. 2, links unten):

Sektor A: Wenige große Streitkräfte dominieren den UxS-Einsatz. Die Bedrohung durch den UxS-Einsatz ist gering.

Sektor B: UxS sind zwar prinzipiell eine Bedrohung, lassen sich aber von den wenigen, großen Streitkräften abwehren.

Sektor C: UxS werden neben wenigen großen Streitkräften auch von „Schurkenstaaten“/Terrorgruppen eingesetzt. Die Bedrohung ist vorhanden, aber abwehrbar.

Sektor D: Breiteste Verfügbarkeit der UxS für verschiedene Streitkräfte sowie „Schurkenstaaten“/Terrorgruppen und umfangreiche Bedrohung durch UxS.

Sektor E: UxS-Einsatz bleibt auf verschiedene staatliche Akteure begrenzt, können aber schlecht abgewehrt werden und stellen so eine Bedrohung dar.

Sektor F: UxS-Einsatz bleibt auf verschiedene staatliche Akteure begrenzt, die Bedrohung ist insgesamt aber gering.

Künstliche Intelligenz (Perspektive 3, Mitte oben):

Sektor A: Die ‚künstlichen Intelligenz‘ der unbemannten Systeme wird aufgrund moralisch/ethischer/ rechtlicher Aspekte aktiv begrenzt.

Sektor B: Die künstliche Intelligenz bleibt aufgrund der technischen Rahmenbedingungen ein Randthema.

Sektor C: Unbemannte Systeme verfügen über eine, grosse künstliche Intelligenz‘, jedoch ohne moralische Basis.

Sektor D: Unbemannte Systeme verfügen über eine, grosse künstliche Intelligenz‘ mit ausgeprägter moralischer Basis [Menschenrecht/Völkerrecht wird eingehalten].

Roboterisierung des Menschen (Perspektive 4, Mitte unten):

Sektor A: Menschen und robotische Systeme bleiben zwei weitgehend voneinander getrennte Sphären.
Sektor B: Technische Effizienz dominiert: Menschen folgen dem Ideal des effizienten Verhaltens.
Sektor C: Der Übergang zwischen Mensch und Maschine wird immer fließender.
Sektor D: Menschlichkeit dominiert: Robotische Systeme folgen dem Ideal des humanen Verhaltens.

Nutzung von bewaffneten Robotern/ Autonomen Waffensystmen (Perspektive 5, rechts oben):

Sektor A: Insgesamt geringer Einsatz von bewaffneten Robotern.
Sektor B: Hohe Bedeutung von bewaffneten Robotern im Militär, offensiv und auch für einen Ersteinsatz.
Sektor C: Hohe Bedeutung von bewaffneten Robotern im Militär, jedoch primär defensiv.

Nutzung von unbewaffneten Robotern sowie deren nachträgliche Bewaffnung (Perspektive 6, rechts unten):

Sektor A: Insgesamt geringer militärischer Einsatz von bewaffneten Robotern, aber teilweise ausgeprägter Einsatz von unbewaffneten Robotern.
Sektor B: Insgesamt umfangreicher Einsatz von bewaffneten Robotern, auch mit nachträglicher Bewaffnung.
Sektor C: Insgesamt geringer Einsatz von bewaffneten und unbewaffneten Robotern.

## 2. Kurzbeschreibung der Szenarien

Aufgrund der Ausprägungen wurden die neun Szenarien folgendermassen benannt und beschrieben:

- **Aktive Begrenzung aufgrund ethischer Bedenken** (Sz. 1): Der bewaffnete Einsatz von Robotern wird international stark reguliert und kontrolliert (aufgrund ethischer/moralischer Bedenken sowie der Rechtslage). Die Streitkräfte sind traditionell aufgestellt und verwenden Roboter vorwiegend für spezifische Teilaktivitäten im Verbund mit Menschen. Insgesamt resultiert eine geringe Bedrohung durch feindliche Roboter.
- **Robotik als neuer Schutzschirm** (Sz. 2):
  Konflikte sind in erster Linie asymmetrisch (hybrid) und wenige grosse Staaten dominieren den Einsatz von Robotik. Bewaffnete Roboter werden eingesetzt, um den Konflikt geographisch vom eigenen Land fernzuhalten, auch mit präventiven Erstschlägen. Roboter werden hauptsächlich im Team mit Menschen benutzt, und sind ein wertvolles Asset der Armeen, es besteht jedoch eine geringe Abhängigkeit und die Streitkräfte können ihre Basisaufgabe auch ohne Roboter erfüllen. Die Bedrohung durch feindliche Roboter ist vorhanden, aber abwehrbar.
- **Robotischer Terror und Terrorbekämpfung** (Sz. 3):
  Konflikte sind in erster Linie asymmetrisch (hybrid). Neben den klassischen Streitkräften nutzen auch Terror-Organisationen/Schurkenstaaten Roboter, d.h. die Zivilbevölkerung wird von Terroristen durch bewaffnete Roboter bedroht, deren Einsatz völkerrechtswidrig erfolgen kann. Die militärische Bedeutung von Robotern bei staatlichen Streitkräften ist gross, der „Krieg gegen den Terror ist weitgehend automatisiert". Die Bedrohung durch feindliche Roboter ist vorhanden, jedoch punktuell.
- **Neue Fronten** (Sz. 4):
  Breites Feld unterschiedlicher militärischer Konflikte mit vielfältigem Einsatz von gut verfügbaren, weit entwickelten und stark vernetzten Robotern. Die Roboter agieren oft unvorhersehbar und eigenständig, auch im Kollektiv. Die militärischen, feindlichen Roboter, teilweise autark, können schlecht abgewehrt werden und stellen eine wachsende Bedrohung dar. Die Gesellschaft ist stark abhängig von ziviler und militärischer Robotik und toleriert somit ein gewisses Mass an Kollateralschäden. Die Abhängigkeit der Roboter vom Menschen und dessen Infrastruktur ist gering.
- **Breite Nutzung einfacher Kampfroboter** (Sz. 5):
  Breites Feld unterschiedlicher militärischer Konflikte mit vielfältigem Einsatz von einfachen, kaum vernetzten, aber autonomen Kamprobotern durch Staaten und terroristische Vereinigungen. Die Roboter stehen als eigenständige Einheiten unter der Überwachung (Not-Stopp verfügbar) und Verantwortung des Kommandanten. Aufgrund der beschränkten Intelligenz der Roboter werden sie vorwiegend für spezifische, gut bekannte Anwendungen eingesetzt. Dennoch ist die Bedrohung durch feindliche Roboter gross. Die Gesellschaft ist abhängig von der eigenen Robotik, im Zivilen wie auch im Militärischen.
- **Krieg der Roboterarmeen – Technische Effizienz dominiert** (Sz. 6): Wachsende Vielfalt zwischenstaatlicher Konflikte mit breitem Einsatz von bewaffneten und unbewaffneten Robotern in einem wenig regulierten Umfeld. Der menschliche Soldat wird im Feld nach und nach abgelöst. Die Roboter sind untereinander gut vernetzt, handeln weitgehend ohne menschliche Unterstützung und ohne eigene moralische Basis, werden aber von den Kommandanten überwacht. Militär und Gesellschaft ist abhängig von der Robotik. Kommandanten akzeptieren oft hohe Kollateralschäden durch die eigenen Roboter. Feindliche Roboter können durch eine traditionelle/ konventionelle Armee kaum abgewehrt werden und stellen eine grosse Bedrohung dar.
- **Neuer Kalter Krieg** (Sz.7):
  Aufrüstung, aber im Rahmen internationaler Konventionen. Gleichgewicht von Supermächten führt vereinzelt zu Stellvertreterkriegen, in denen intelligente Roboter umfangreich und gut vernetzt, jedoch vorwiegend unbewaffnet und zur Unterstützung der Soldaten eingesetzt werden. Die Furcht vor einer Eskalation mit ungeahnten Folgen durch den breiten Einsatz von hochentwickelten, autonomen Kampfrobotern führt zu einer Art ‚robotischer Abschreckung' und zum weitgehenden Verzicht auf deren Einsatz. Zur Ausbildung und im Training werden die Kampfroboter strikt unter der Kontrolle der Kommandanten gehalten. Die unmittelbare Bedrohung durch feindliche Roboter ist daher relativ gering. Im Allgemeinen ist die Gesellschaft jedoch stark von der eigenen Robotik abhängig.
- **Stellvertreterkriege im Cyberspace** (Sz. 8):
  Stark reguliertes und kontrolliertes Robotik-Umfeld. Wenige grosse Streitkräfte dominieren den Einsatz von Robotern, welche kaum bewaffnet sind und zahlreich und breit für unbewaffnete Anwendungen vorgesehen sind. Die Systeme werden zur direkten Unterstützung resp. in enger Bindung an die Soldaten (weitgehend eigenständig, ‚human on the loop') eingesetzt. Insgesamt geringer Umfang physischer Auseinandersetzungen, jedoch viele militärische Aktivitäten im Cyberspace. Die Bedrohung durch feindliche Roboter ist daher gering.
- **Roboter verweigern den Kampfeinsatz** (Sz. 9):
  Allgemein ein friedliches, stark kontrolliertes Umfeld mit insgesamt geringem Einsatz von Robotern für militärische Aktivitäten. Die Roboter verfügen über eine grosse moralische Basis, lehnen Gewalt gegen Menschen ab und folgen dem Ideal humanen Verhaltens. Im Gegensatz zu der Zivilgesellschaft sind Streitkräfte nicht angewiesen auf Roboter. Feindliche Systeme stellen kaum eine Bedrohung dar.

Neben den hier beschriebenen neun Szenarien gibt es selbstverständlich noch eine Vielzahl weiterer Möglichkeiten, wie sich das Umfeld robotischer Systeme entwickeln könnte. Dazu zählen auch sogenannte „Wild Cards" – also extreme Entwicklungen, die zwar grundsätzlich denkbar sind, deren Wahrscheinlichkeit oder strategische Relevanz aber so gering ist, dass sie nicht als Projektionen betrachtet werden und daher auch nicht zu eigenständigen Szenarien führen

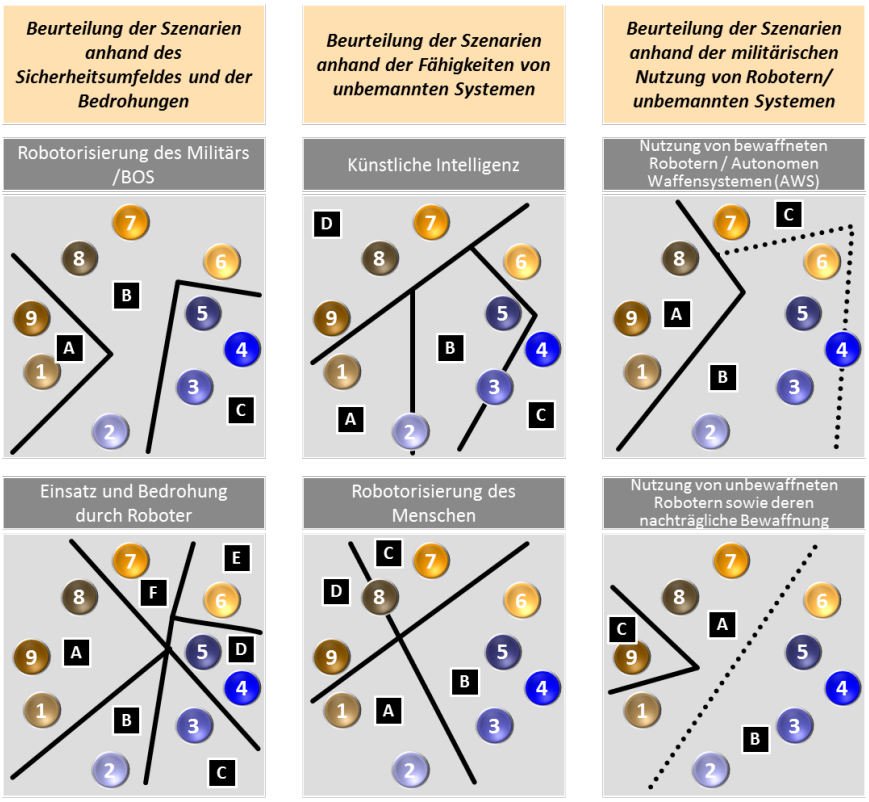



*Bild 6: Sechs weitere Perspektiven auf die Landkarte der Zukunft*

können [SS04]. Eine solche Wild Card ist beispielsweise ein Rückschritt ins Mittelalter oder die Versklavung des Menschen. Diskutiert wurde hier, dass aufgrund gewisser Umstände wie einer längeren Unterbrechung der Energieversorgung dem Menschen technischen Geräte nicht mehr im heutigen Umfang zur Verfügung stehen.

## 3. Szenario Bewertung

Zur Bewertung der Szenarien wurde vom Szenarioteam sowie weiteren, externen Experten eine Einschätzung vorgenommen, welche Szenarien am ehesten erwartet oder gewünscht werden und welche bereits als Gegenwart erkannt werden. Die Einschätzung erfolgte auf der Ebene der Projektionen (Bild 3) und wurde anschliessend auf die neun Szenarien hochgerechnet. Die Beurteilung durch die Experten ist in der folgenden Tabelle der ‚Top 3 Szenarien' zusammengefasst:

- In der Beurteilung zeigte sich die Gegenwart hauptsächlich im Szenario ‚Robotik als neuer Schutzschirm'. In diesem Szenario dominieren einige grosse Staaten den militärischen Einsatz von Robotern, welche hauptsächlich asymmetrisch verwendet werden um Konflikte vom eigenen Land fernzuhalten.
- Die gewünschte Zukunft wurde am besten erfasst durch Szenarien, welche keinen oder nur einen kontrollierten, begrenzten Einsatz von moralischen Kampfrobotern enthalten.
- Am wenigsten gewünscht, aber am ehesten erwartet wurden Szenarien, welche einen umfangreichen Einsatz von Kampfrobotern beinhalten und in denen technische Effizienz dominiert.

Die gewünschte sowie die erwartete Entwicklung geht somit in verschiedene Richtungen, was sich in der Landkarte der Zukunft klar wiederspiegelt (Bild 7).

| **Am ehesten erkannt als Gegenwart** | **Am ehesten gewünscht für die Zukunft** | **Am ehesten erwartet in Zukunft** |
|---|---|---|
| 1. Robotik als neuer Schutzschirm<br>2. Robotischer Terror und –abwehr<br>3. Breite Nutzung einfacher Kampfroboter | 1. Stellvertreterkrieg im Cyberspace<br>2. Aktive Begrenzung<br>3. Roboter verweigern den Kampfeinsatz / Neuer Kalter Krieg | 1. Neue Fronten/Krieg der Roboterarmeen<br>2. Neuer Kalter Krieg<br>3. Robotischer Terror |
| **Am wenigsten erkannt als Gegenwart** | **Am wenigsten gewünscht für die Zukunft** | **Am wenigsten erwartet in Zukunft** |
| 1. Roboter verweigern den Kampfeinsatz<br>2. Neuer Kalter Krieg<br>3. Neue Fronten | 1. Neue Fronten<br>2. Breite Nutzung einfacher Kampfroboter<br>3. Krieg der Roboterarmeen / Robotischer Terror | 1. Roboter verweigern den Kampfeinsatz<br>2. Aktive Begrenzung<br>3. Stellvertreterkriege im Cyberspace |

*Tabelle: Die Beurteilung der Experten der ‚Top 3 Szenarien' zusammengefasst.*

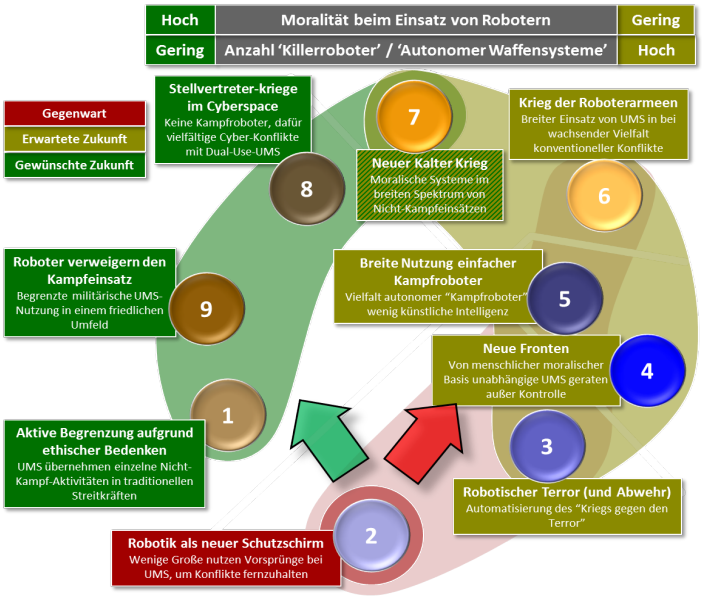



*Bild 7: Landkarte der Zukunft' mit visualisiertem Erwartungs- und Wunschraum*

## Fazit

Während die Auswertung keinen Aufschluss über die Eintrittswahrscheinlichkeit der Szenarien gibt, lässt sich feststellen, welche Entwicklung das Expertenteam erwartet. Die Experten gehen davon aus, dass die Nutzung von bewaffneten Robotern zunehmen und dass die Bedrohung durch feindliche und teilweise eigene Roboter ansteigen wird. Im Gegensatz dazu wünschen sich die Experten eher, dass die Aufrüstung mit bewaffneten Robotern stark kontrolliert und beschränkt wird und dass die Roboter über eine moralische Basis verfügen um im Sinne der Menschlichkeit zu handeln.

Es bleibt abschliessend zu erwähnen, dass weitere Befragungen notwendig sein werden um ein breiteres Bild der Wünsche und Erwartungen zu erhalten.


### Dr. Mark Höpflinger

leitet das Forschungsprogramm 'Unbemannte Systeme/Robotik' bei armasuisse Wisssenschaft und Technologie, dem Technologiezentrum des Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS). Das Forschungsprogramm dient der Unterstützung des VBS bei der Identifikation von Chancen und Risiken von unbemannten Systemen für den Einsatz im Bereich der Sicherheit.

Er ist erreichbar unter
markus.hoepflinger@armasuisse.ch



### Dr. Alexander Fink

ist Gründungsinitiator und Mitglied des Vorstands von ScMI Scenario Management International AG. Alexander Fink verfügt über langjährige Erfahrung bei der strategischen Beratung von Industrie- und Dienstleistungsunternehmen. Er ist Autor bzw. Mitautor mehrerer Bücher, schreibt für zahlreiche deutsche und internationale Magazine und Fachzeitschriften. Alexander Fink studierte Wirtschaftsingenieurwesen an der Universität Paderborn und promovierte zum Thema szenariogestützte Unternehmensführung am Heinz Nixdorf Institut. Er engagiert sich an mehreren Hochschulen und hält gerne national wie international Vorträge zum Szenario-Management™.

Er ist erreichbar unter
fink@scmi.de


## Referenzen


[FS11] Fink, Alexander / Siebe, Andreas: Handbuch Zukunftsmanagement. Werkzeuge der strategischen Planung und Früherkennung. 2., aktualisierte und erweiterte Auflage. Campus, Frankfurt am Main, 2011

[FS16] Fink, Alexander / Siebe, Andreas: Szenario-Management. Von strategischem Vorausdenken zu zukunftsrobusten Entscheidungen. Campus, Frankfurt am Main, 2016

[SS04] Steinmüller, Angela / Steinmüller, Karlheinz: Wild Cards. Wann das Unwahrscheinliche eintritt. 2., veränderte und ergänzte Auflage. Murmann, Hamburg, 2004

# ICT Plattformen in Fahrzeugen – Minimierung der Risiken dank offenen Standards und Architekturvorgaben

**Die Beschaffung und Einführung von modernen Kommunikations- und Führungssystemen stellt Armeen auf der ganzen Welt vor grossen Herausforderungen. Die Zeiten, in denen ein reines Sprachfunk die Anforderungen abdecken konnten, sind unwiderruflich vorbei. Mit dem Fortschreiten der Entwicklungen rund um C4ISTAR Systeme steigen auch bei den Fahrzeugen die Anforderungen an Datenübertragung, Rechen- und Speicherleistung, sowie Bediengeräte. Einschränkungen hinsichtlich Platz, Energie und Gewicht stellen dabei harte Anforderungen, welche das Risiko des Scheiterns erhöhen. Das Verteidigungsministerium von Grossbritannien hat sich intensiv mit der Problematik beschäftigt und einen vielversprechenden Lösungsansatz entwickelt, welcher auch von der NATO übernommen wurde.**

**Keywords:** **Beschaffung, komplexe ICT Systeme, Trägerplattformen, Kommunikation, GVA, NGVA, C4ISTAR, STANAG, Architekturen, Standards**

**Autor:** **Dr. Marc Danzeisen**, Rayzon Technologies AG

Die Integrationsdichte in militärischen Fahrzeugen (alias Trägerplattformen) hat über die letzten Jahrzehnte stark zugenommen, wobei nicht nur C4ISTAR [a] Systeme integriert und vernetzt werden müssen. Moderne Fahrzeuge haben bereits eine Vielzahl von fahrzeuginternen Systemen welche immer umfangreicher, komplexer und vernetzter werden. So werden beispielsweise bei grösseren Fahrzeugen diverse Kameras verbaut um dem Fahrer eine ausreichende Rundumsicht zu ermöglichen. Sind dann noch moderne Sensor- und Waffensysteme auf dem Fahrzeug montiert, benötigen diese wiederum Datenverbindungen, Rechner-, Speicher- und Bedienelemente. Mit zunehmender Anzahl zu integrierenden Systeme wird auch die Stromversorgung zum Problem. Mit steigendem Energiebedarf nimmt die Autonomie der mobilen Systeme in den Fahrzeugen stetig ab, was einen direkten Einfluss auf den Einsatz und die Logistik hat.

Fehlende Standardisierung hat dazu geführt, dass im Rahmen von bisherigen Projekten geschlossene Systeme beschafft wurden. Dies hat zu einer Vielzahl von „Silo" Systemen geführt, was einerseits höhere Integrations- und Unterhaltskosten und andererseits höheren Gewicht-, Platz- und Energieverbrauch mit sich brachte. Die fehlende Harmonisierung der Systeme auch hinsichtlich deren Bedienkonzepte fordert gesonderte und systemspezifische Schulungen für Benutzer und Betreiber.

*Abb1: Integration von „Silo" Systemen in Fahrzeuge [1]*

Geschlossene Silo-Systeme erschweren deren Integration. Die Entwicklung der benötigten Übergänge (Gateways) sind aufwendig und teuer, da sie kundenspezifisch entwickelt werden müssen.
Die Beschaffung von grossen, geschlossenen Systemen bringt aber nicht nur technische Probleme mit sich. Die kommerzielle Abhängigkeit von den grossen Systemanbietern zählt hierbei wohl zu den folgeschwersten Nachteilen. Eine solche Abhängigkeit erfolgt dann, wenn Grossprojekte an einzelne Anbieter vergeben werden. Das sogenannte Lock-in, also die Bindung an den Lieferanten über den ganzen Lebensweg des Systems hinweg, hat auch Einfluss auf die Innovation. Kleine, innovative Anbieter können bei grossen Ausschreibungen für monolithische Systeme nicht, oder nur als Sublieferanten anbieten. Bei monolithischen Systemen beschränkt sich jegliche Innovation auf einen einzigen Lieferanten. Eine Studie [2] des UK MOD hat gezeigt, dass Ausschreibungen von Grossprojekten eine wesentliche Ursache für ungenügende oder gar fehlende Innovation bei der Weiterentwicklung von beschafften und eingeführten Systeme darstellt. Bei grossen und komplexen Systemen mit langjährigen Wartungsverträgen sind die Anbieter interessiert die Kosten für Unterhalt und Weiterentwicklungen tief zu halten, da wegen dem Preisdruck bei öffentlichen Ausschreibungen ein wesentlicher Teil der Erträge auf eben diesen Wartungsarbeiten kalkuliert wird.

## Herausforderungen

In Anbetracht dieser Sachlage erscheinen die Herausforderungen [b], welchen sich moderne Armeen gegenübergestellt sehen, kaum handhabbar:

- Armeen benötigen die Möglichkeit Einsatzkräfte agil und adaptiv für spezifische Einsätze auszurüsten
- Bedürfnisse und Technologie entwickeln sich schneller als Projekte liefern können
- Immer mehr Sensoren, mehr Sub-Systeme, mehr Displays und Konsolen (HMI - Human Machine Interface)
- Immer mehr Systeme müssen zusammen funktionieren - Systemverbund (SoS - System-of-Systems)
- Subsysteme haben unterschiedlich kurze Lebenszyklen
- Dringende operationelle Anforderungen (UOR)
- Gesamtlebenskosten müssen gesenkt werden

Die Technologien entwickeln sich auch im militärischen Umfeld immer schneller, wobei sich die Lebenszyklen zum Teil sehr stark unterscheiden. Sensorsysteme entwickeln sich beispielsweise rasant, sodass beschaffte Systeme in wenigen Jahren veraltet sind. Dem wirkt der Einzug von softwarebasierten Systemen (e.g. Software-Defined-Radio) etwas entgegen, sodass kleinere Aktualisierungen durch reine Software Updates realisiert

werden können. Jedoch erfordern grössere Neuerungen oft auch eine Aktualisierung der Systemhardware, oder Teile davon. Diese kurzen Lebenszyklen beissen sich mit den langwierigen Beschaffungsverfahren. Neue Technologien sind bis zu deren Einführung bereits veraltet, der erhoffte Mehrwert für die Truppe entsprechend reduziert und die Investition im schlimmsten Fall nicht mehr gerechtfertigt.

Projekte müssen kleiner werden, sodass sie rascher abgewickelt werden können. Die Komplexität der einzelnen Projekte ist zu verringern, damit sich auch die Anzahl der Risiken reduziert und die noch verbleibenden Risiken wieder beherrschbar werden. Damit die steigende Anzahl von (kleineren) Projekten nicht zu neuen Problemen führt, muss sichergestellt werden, dass die Prozesse auch für kleinere Beschaffungen handhabbar und verhältnismässig sind. Damit die kleineren Einzelprojekte aufeinander abgestimmt bleiben, muss eine übergeordnete Koordination sichergestellt werden. Wurde bei bisherigen Grossprojekten ein wesentlicher Teil der Verantwortung an die Generalunternehmer ausgelagert, muss bei einer Aufteilung der Beschaffungsvorhaben in kleineren Beschaffungsschritten die Gesamtverantwortung von den Armeen wahrgenommen werden.

Des Weiteren müssen die beschafften Mengen überdacht werden. Vollbeschaffungen erscheinen unter diesen Umständen nicht mehr sinnvoll und wirtschaftlich. Wird auf die vollumfängliche Ausrüstung aller betroffenen Fahrzeuge verzichtet, werden flexible Montagevorrichtungen unumgänglich. Sind die Systeme modular aufgebaut, können die Einsatzkräfte wiederum jeweils missionsspezifisch ausgerüstet werden, wobei sich die Modularität nicht nur auf die Montage- und Anschlussmöglichkeiten beschränken darf, sondern bis ins systeminnere weitergezogen werden muss. Im Idealfall können beispielsweise Aufklärungssysteme je nach Bedarf mit unterschiedlichen Sensortypen bestückt werden. Vielleicht sogar mit Sensoren von unterschiedlichen Anbietern und aus unterschiedlichen Technologiegenerationen.

Die Aufteilung von Systemen in Subsysteme hat auch einen positiven Einfluss auf die Systemkosten. Modularität, zusammen mit offenen und standardisierten Schnittstellen, ermöglicht die Reduktion von Integrations-, Test- und Unterhaltskosten. Subsysteme mit entsprechenden Schnittstellen können von mehreren Systemen benutzt werden. Die Aufteilung in Teilsysteme, mit gleichzeitiger Verringerung der Abhängigkeiten zwischen diesen, erhöht zudem die Stabilität des Gesamtsystems. Beim (vorübergehenden) Ausfall eines Teilsystems können die Funktionen der anderen Teilsysteme weiterhin genutzt werden.

## Konsequenzen des UK MOD

Das UK MOD (United Kingdom Military of Defence) hat von den schmerzhaften Erfahrungen bei früheren Projekte gelernt und entsprechende Konsequenzen gezogen [3]:

- Einführung von Systems Engineering
- Nutzen von Open System Architecture
- Vorgabe von Architekturen, welche SoS zulassen, bzw. fordern
- Das MOD übernimmt die Verantwortung für Definition und Unterhalt von Architekturen, Schnittstellen und Datenmodellen
- Beschaffung von kleineren Sub-Systemen statt monolithischer Lösungen

Mit der Einführung von Systems Engineering hat das UK MOD ein klares Statement zu den als relevant erachteten Fähigkeiten und Aufgaben der eigenen Leute abgegeben. Mit Hilfe des Systems Engineering sollen standardisierte Methodik und Werkzeuge für das Requirements Engineering, Systemdesign und die Integration bereitgestellt und das eigene Personal mit dem entsprechenden Wissen ausgerüstet werden. In Zusammenarbeit mit der Cransfield University bietet das UK MOD Kurse und Zertifizierungen für Systems Engineering Aus- und Weiterbildungen [4][5] an, welche die Besonderheiten von Beschaffungen für die Verteidigung berücksichtigt.

Die Arbeiten rund um die Land Open Systems Architectures (LOSA) bilden die Grundlage für die Beschaffung und Einführung von modularen und interoperablen (Teil-)Systemen für das Heer. Durch konsequente Architekturvorgaben wird sichergestellt, dass beschaffte (Teil-) Systeme in die Gesamtarchitektur passen. Das UK MOD übernimmt hierbei die Verantwortung für die Definition und den Unterhalt von Systemarchitekturen, Schnittstellen und Datenmodellen.

Das vom UK MOD entwickelte LOSA beinhaltet Architekturvorgaben für Systeme in Fahrzeuge, Soldatensysteme und Systeme für Militärbasen.

## Generic Vehicle Architecture

Der vorliegende Artikel beschränkt sich auf die fahrzeugrelevanten Architekturvorgaben der LOSA, welche unter dem Begriff Generic Vehicle Architecture (GVA) zusammengefasst sind.

Die wesentlichen Neuerungen der GVA lassen sich wie folgt zusammenfassen:

- Standardisierte, multifunktionale Bedieneinheit (HMI - Human Maschine Interface)
- Ethernet LAN (Real-Time Ethernet) als Datentransport Technologie
- Standardisierte Stromverteilung
- Standardisierte Videoverteilung
- Standardisierte Strom- und Datenstecker
- Nutzung von DDS / DDSi (Data Distribution Service - Interoperability)
- Nutzung des GVA Daten Models

Die multifunktionale Bedieneinheit wird als universelle Benutzerschnittstelle für die unterschiedlichen Anwendungen im Fahrzeug eingesetzt. Vorgegeben und demnach für alle Anwendungen gleich, sind übergreifende Tastenfunktionen. Die anderen Tasten können den anwendungsspezifischen Funktionen zugeordnet werden.

Die anwendungsübergreifende Mehrfachnutzung der Bedieneinheit reduziert die Anzahl der eingebauten Geräte und somit den Bedarf an Platz und Energie. Zudem führt


*Abb2: The 10.4-inch SD7310 smart display from General Dynamics Canada is used in vetronics applications.*
*Quelle: http://www.gd-ms.ca/*

die Vereinheitlichung der Benutzerschnittstelle (Hard- und Software) zu Einsparungen bei der Ausbildung, Unterhalt und Wartung der Systeme.

Der Einsatz von Ethernet als Technologie für den Datentransport erlaubt die Nutzung von entsprechend einfach verfügbaren und gleichzeitig erprobten Komponenten aus der Industrie.

Der GVA Standard beinhaltet auch bezüglich der Stromverteilung Vorgaben, wobei ein intelligentes Powermanagement gefordert wird, mit dem sich Teilsysteme gezielt ausschalten lassen können, wenn diese nicht benötigt werden. Die Digitalisierung und Vernetzung der Stromverteilung mit den Anwendungen ist zwingend, um die heute geforderte Autonomie von mobilen Systemen zu ermöglichen.

Die Vorgaben im Bereich der Videoverteilung stellen die nahtlose Einbindung von Videokameras in die GVA sicher. Die Nutzung des GVA Datenbusses für die Anbindung von Fahrzeugkameras vereinfacht einerseits die Verkabelung und ermöglicht andererseits allen Besatzungsmitgliedern den einfachen Zugriff auf die Kameras mit Hilfe der GVA Bedieneinheit. Dank der Standardisierung der Videoverteilung können aber auch teure Videosensoren wie Wärmebildkameras von mehreren Anwendungen gleichzeitig genutzt werden.

Damit die GVA kompatiblen Systeme auch ohne Adapter und Konverter zusammen funktionieren können, sieht GVA auch standardisierte Strom- und Datenstecker vor.

Die nachfolgende Grafik visualisiert die Grundarchitektur der UK MOD GVA mit seinen wichtigsten Bestandteilen.

Die GVA ist im UK MOD Def Stan 23-09 beschrieben. Nebst der Architektur, der Stromverteilung und der Bedieneinheit erhält auch die HUMS (Health and Usage Monitoring Systems) einen eigenen Bereich. Die Bedeutung der Systemüberwachung (Monitoring) nimmt auch im militärischen Umfeld stetig zu. Im Einsatzfall müssen die Einsatzkräfte die immer komplexer werdenden Systeme selbstständig betreiben und bei Bedarf auch Fehler beheben können. Die Modularität der GVA erleichtert Fehlerdiagnose, Wartung und Unterhalt. Standardisierte Schnittstellen zwischen den Teilsystemen, zusammen mit dem Ethernet-basierten Datenbus ermöglichen eine vereinfachte Überwachung der Zustände der einzelnen Teilsysteme und der ausgetauschten Daten.

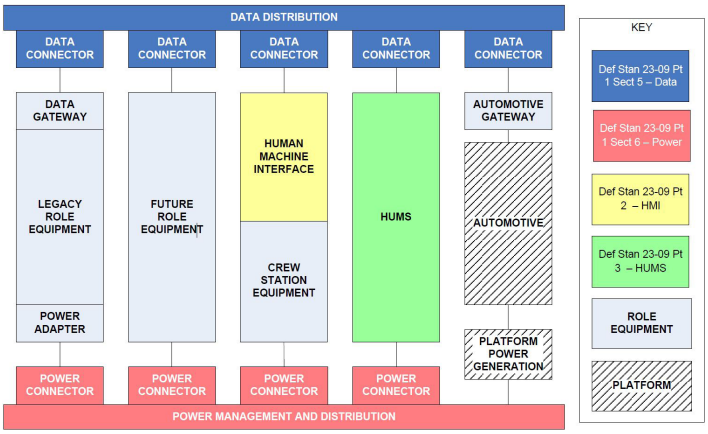



*Abb3: Grundarchitektur der UK MOD Generic Vehicle Architecture - GVA [6][7][8]*

Die wohl gravierendste Neuerung der GVA betrifft die Art und Weise, wie die Teilsysteme miteinander Daten austauschen. Die GVA fordert einen Paradigmenwechsel von prozess-/ anwendungsorientierter Kommunikation hin zu Datenorientiertheit.

Bei herkömmlichen Ansätzen verwaltet jede Anwendung (oder System) seinen eigenen Datenspeicher. Sollen Daten zwischen Anwendungen ausgetauscht werden, erfolgt dies mittels Meldungen zwischen den jeweiligen Anwendungen. Die Struktur und Inhalte der Meldungen werden mittels Protokoll- und Schnittstellenspezifikationen definiert. Eine Kompatibilität zwischen den verwendeten Datenstrukturen ist nicht erforderlich.

Im Gegensatz dazu nutzt die datenorientierte Kommunikation zwischen Anwendungen den sogenannten Publish/Subscribe Mechanismus. Hierbei erfolgt der Datenaustausch nicht zwischen zwei vordefinierten Anwendungen, sondern über ein geteiltes Medium. Hat eine Anwendung Informationen bekannt zu geben, publiziert sie diese über das Medium. Anwendungen, welche sich für diese Informationen interessieren, abonnieren die Publikationen. Damit nicht jede Anwendung sämtliche Informationen empfangen und verarbeiten muss, werden die Daten nach Themen strukturiert. So wird jede Publikation einem Thema zugeordnet, was den Anwendungen erlaubt nur Informationen zu bestimmten Themen zu abonnieren. Dieser Publish/Subscribe Mechanismus entkoppelt die Anwendungen voneinander. Die Anwendungen kommunizieren nicht mehr direkt miteinander. Dafür muss eine Drittinstanz die Verwaltung des Mediums, der Publikationen und Abonnementen sicherstellen. Diese Drittinstanz, in Form einer Middleware, stellt sicher, dass die Anwendungen die Publikationen zu den abonnierten Themen erhalten, auch wenn die Anwendungen vorübergehend keine Verbindung zum Medium/Middleware haben.

Der von GVA eingesetzte Standard für die Publish/Subscribe Kommunikation kommt aus der IoT (Internet of Things) Welt, wird von der Object Management Group (OMG) definiert und nennt sich DDS (Data Distribution Service) [9][10]. DDS nutzt das Internet Protokoll (IP) und kann somit verteilte Systeme über das Internet mit einander verbinden. Der DDS Standard ist öffentlich und wird seit seinem Erscheinen im Jahre 2004 stets weiterentwickelt. Seine Verbreitung in der Industrie hat in den letzten Jahren rasant zugenommen. Diverse Branchen haben die Vorteile des Publish/Subscribe Mechanismus entdeckt und nutzen das DDS für den Datenaustausch zwischen Subsystemen wie Sensoren, Anwendungen und Aktoren. So wird in modernen und intelligenten Produktionsanlagen das DDS eingesetzt, um modulare und dynamisch ausbaubare Fertigungsstrassen realisieren zu können. In grossen Gewächshäusern wird DDS eingesetzt, um die Daten von tausenden von Sensoren den unterschiedlichen Anwendungen zur Verfügung zu stellen, welche wiederum tausende von Aktoren mittels DDS Meldungen steuern. In der Landwirtschaft erlaubt die mit DDS erzielte Entkopplung der Subsysteme den Bauern das dynamische Wechseln von Gerätschaften an den Fahrzeugen, ohne dass die Systeme neu konfiguriert werden müssen. Während einem Raketenstart im Kennedy Space Center senden Sensoren 400'000 DDS Meldungen pro Sekunde und in der Robotik Industrie wird DDS als Kernkomponente des Robot Operating System (ROS) eingesetzt.

Dank der guten Verbreitung von DDS in den unterschiedlichen Industriebereichen sind auch entsprechend viele DDS Middleware Implementierungen verfügbar. Mit den von der OMG standardisierten Erweiterungen rund um DDSi (DDS Interoperability) [11] wird zudem sichergestellt, dass die Implementierungen von unterschiedlichen Anbietern zusammen funktionieren. Die Wahl DDS/DDSi auch in der GVA einzusetzen hat Anbieter motiviert, Lösungen für die Nutzung von DDS über militärischen Kommunikationssystemen zu entwickeln.

Damit Subsysteme mit Hilfe von DDS/DDSi miteinander Daten austauschen können, muss ein gemeinsames Datenmodell definiert werden. Das Datenmodell stellt sicher, dass die Inhalte der DDS Meldungen von den Abonnenten verstanden werden. So ist das Datenmodell bis zu einem gewissen Mass branchenspezifisch, wobei einfachere Datenobjekte wie beispielsweise eine Temperatur-, oder Feuchtigkeitsmeldung nicht unterscheiden. Solch atomare Datenobjekte lassen sich folglich auch in einem generischen, für alle DDS basierten Systeme Datenmodell definieren. Bei komplexeren Datenobjekten hingegen werden spezifische Datenmodelle benötigt. So definiert das UK MOD für GVA ein Datenmodell für Landsysteme – das Land Data Model (LDM). Das gemeinsam genutzte LDM ist Voraussetzung, damit Subsysteme unterschiedlicher Hersteller DDS Datenobjekte ohne Anpassungen korrekt einlesen können.

Die nachfolgende Abbildung zeigt schematisch die resultierende Architektur in Fahrzeugen.

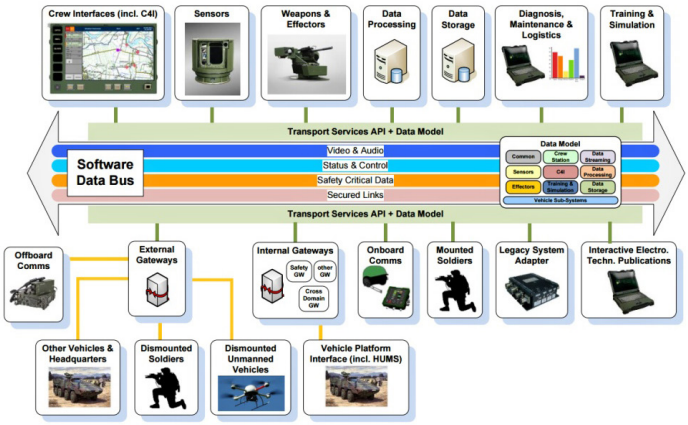



*Abb4: Datenbusorientierte Architektur für Fahrzeugsysteme*

Wie in Abbildung 4 ersichtlich, sind Ressourcen für Datenverarbeitung und –Speicherung anwendungsübergreifend bereitzustellen. Dieser Anforderung kommt der Einzug von software-basierten Systemen entgegen. Um Entwicklungs- und Unterhaltskosten von Hardware zu reduzieren, wird nach Möglichkeit auf systemspezifische Hardware verzichtet. Die Nutzung von generischer Hardware (e.g. MiniPC, EmbeddedPC) führt einerseits zu deutlich höheren Stückzahlen und der damit ermöglichten Reduktion der Stückkosten. Andererseits erlaubt dies die Vereinheitlichung von Entwicklungsumgebungen. Dank Virtualisierung können unterschiedliche Systeme auf ein und er selben Hardware betrieben werden. Die daraus folgende Reduktion der Anzahl von zu verbauenden Gerätschaften ermöglicht direkt Ersparnisse hinsichtlich Gewicht, Grösse und Stromverbrauch. Die folgende Abbildung zeigt ein Muster GVA Fahrzeug des UK MOD.

Die NATO hat den GVA Ansatz des UK MOD übernommen, erweitert und als STANAG 4754 – NGVA publiziert. Die

Erweiterungen betreffen insbesondere die Integration von des STANAG 4697 – PLEVID, welches Vorgaben für Video- und Audioverteilung in Fahrzeugen macht.

## Chancen und Risiken

Die Chancen und Risiken von (N)GVA lassen sich wie folgt zusammenfassen.

Technische Chancen:

- Vereinfachte Integration von Sub-Systemen (Standardisierte Schnittstellen für Strom, Daten und Vorgaben für "Mensch-Maschine" Schnittstelle)
- Inhärente Modularität und Skalierbarkeit (DDS/DDSi Middleware, GVA Daten Model und offene Spezifikation von Schnittstellen)
- Rechner- und Speicherkapazitäten können zwischen Systemen geteilt werden
- Sensoren können von mehreren (Sub-)Systemen genutzt werden
- Reduzierte Last für Benutzer (Systeme haben ähnliche Bedienschnittstellen, gleiches „Look & Feel")
- Einfachere Integration in zukünftige Ausbildungs- und Simulationsanlagen
- Einfache Realisation von automatisierten Monitoring-, Diagnose-, Wartungs- und Support Tools (SoS mit DDS/DDSi)
- Effizienteres Powermanagement (integriert und vernetzt)
- Mehr Flexibilität bei der einsatzspezifischen Bereitstellung der Fz (modulare Sub-Systeme)
- Vereinheitlichung der Fahrzeuge (Sub-Systeme sind unabhängig vom Fahrzeugtyp)
- Vereinfachung Verkabelung
- Geringerer Platzbedarf für Systeme (Komponenten werden geteilt)

Technische Risiken:

- Keine nahtlose Integration von Teilsystemen, wenn der Standard oder die Beschaffungsbehörde die Schnittstellen und Datenmodelle ungenügend spezifiziert
- Proprietäre Erweiterungen können zu erneuten Abhängigkeiten führen und/oder Integration von Drittsystemen erschweren
- Fehlende Weiterentwicklung des NGVA Standards (zu viele Teilnehmer mit divergierenden Interessen)

Kommerzielle Chancen:

- Reduzierte Integrationszeit, -risiken und -kosten (durch „Open Systems Approach")
- Vereinfachung der Durchsetzung von Verfügbarkeitsverträgen (basierend auf HUMS Daten)
- Reduzierte Unterhaltskosten, da Unterhalt und Wartung abhängig von Systemzuständen gemacht werden können (basierend auf HUMS Daten)
- Reduzierte Kosten, da Lock-in Situationen vermieden
- Bessere Handhabung von Obsoleszenz (mehr potentielle Anbieter von Ersatzteilen oder Sub-Systemen)
- Verringert Hürden für kleine Unternehmen Sub-Systeme anzubieten
- Mehr Wettbewerb, da mehr potentielle Anbieter
- Tiefere Ausbildungskosten bei den Truppen - insb. weniger Zeitaufwand (einheitliche HMI)

Kommerzielle Risiken:

- Lock-in, wenn zu wenig Hersteller (N)GVA konforme Produkte anbieten
- Hohe Kosten, um bestehende Fahrzeuge (N)GVA konform zu machen
- Wollen die Armeen die Kontrolle über komplexe ICT Beschaffungsprojekte wieder zurückerlangen, müssen die entsprechenden Kompetenzen aufgebaut und erhalten werden
- Die Armeen müssen die Gesamtverantwortung für die Systeme übernehmen

*Abb5: GVA kompatible Fahrzeugintegration*

## Zusammenfassung

Heutige militärische Kommunikationssysteme sind ICT Systeme. Die Systeme sind zum grossen Teil „software defined“, was die Systeme flexibel und erweiterbar macht, aber auch die Komplexität und Anfälligkeit für Fehlkonfigurationen erhöht. Beschaffung, Integration, Betrieb und Unterhalt von militärischen Kommunikationssystemen bergen folglich dieselben Risiken wie komplexe IT Projekte.

Die starken Einschränkungen hinsichtlich Platz, Strom und Gewicht machen die Integration von ICT Systemen in Fahrzeugen zur besonderen Herausforderung.

Offene System Architekturen und Standards reduzieren Integrationsrisiken und fördern den Wettbewerb. Modulare Architekturen (System of Systems) und standardisierte Schnittstellenvorgaben verbessern die Messbarkeit von Subsystemen und ermöglichen einen besseren Umgang mit den unterschiedlich kurzen Lebenszyklen der Teilsysteme.

Die Industrie zeigt sich gegenüber (N)GVA positiv eingestellt. Diverse bekannte Firmen beteiligen sich aktiv in den entsprechenden Arbeitsgruppen und bewerben ihre Produkte als (N)GVA konform.

Die Beschaffungsbehörde muss zum Smart Client werden. Sie muss Gesamtarchitekturen definieren, Architekturvorgaben für die einzelnen Teilsysteme ableiten, einzuhaltende Standards und Architekturen verstehen und wo nötig präzisieren oder anpassen, damit die beschafften Teilsysteme in die Gesamtarchitektur passen. Die (N)GVA definiert nur so viel wie nötig um Interoperabilität zwischen den konformen Teilsystemen sicher zu stellen. GVA sowie NGVA lassen noch sehr viel undefiniert, um den Projekten die benötigte Flexibilität zu lassen. Die Vorgabe (N)GVA konform zu sein alleine genügt nicht, um erfolgreich (Teil-) Systeme zu beschaffen und einzuführen. Der (N)GVA Ansatz geht davon aus, dass die Armee die Gesamtverantwortung übernimmt und massgeblich zum Erfolg beiträgt.

Gelingt dies, bestehen gute Chancen die Komplexität von heutigen Beschaffungsprojekten im Bereich der mobilen Kommunikation und Fahrzeugintegration zu meistern und den Truppen die benötigten Fähigkeiten zu ermöglichen.

**Dr. Marc Danzeisen**
ist seit 1999 im Telekommunikationsumfeld tätig. Er ist seit 2008 selbstständig und berät Behörden und Organisationen aus dem Sicherheitsbereich bei ICT Projekten. Aufträge beinhalten Tätigkeiten aus den Bereichen Forschungsmanagements, Exploration, Evaluation, Testing/Erprobung und Expertise. Seine Firma, Rayzon Technologies AG, entwickelt ICT Systeme für Live Tracking und Analyse, verteilte und mobile Plattformen für Video- und Messsysteme, sowie kundenspezifische Lösungen. Entsprechend der Kundenbedürfnisse liefert die Rayzon Technologies Konzepte, Funktionsmuster, Prototypen, Vorserien oder schlüsselfertige Lösungen.

## Erklärungen

[a] Command and Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition and Reconnaissance

[b] Die erläuterten Anforderungen entsprechen den am häufigsten zitierten Anforderungen in den referenzierten Dokumenten

## Referenzen

[1] UK MOD Land Equipment, Land Equipment DE&S, GVA Office, Keith Smith & Mark Ollerton, Land Systems, QinetiQ

[2] UK MOD: National Security through technology:
https://www.gov.uk/government/publications/national-security-through-technology-technology-equipment-and-support-for-uk-defence-and-security-cm-8278--2

[3] UK MOD – Defence Industrial Strategy - Whitepaper 2005

[4] Systems Engineering for Defence, https://www.cranfield.ac.uk/courses/taught/systems-engineering-for-defence-capability

[5] Defence Academy of the United Kingdom: Systems Engineering for Defence Capability MSc - SEDCMSC: http://www.da.mod.uk/Courses/Course-Details/Course/404

[6] Base Architecture GVA, UK MOD Def Stan, https://www.dstan.mod.uk/StanMIS/indexes/DefenceStandardDownload/4925?seriesId=20

[7] „The UK MOD Generic Vehicle Architecture - A Compelling Case for Interoperable Open Architecture“, Real-Time Innovations (www.rti.com)

[8] UK MOD: Defence Standard 23-009 Part 0, Issue 4 Date: 03 October 2016 - Generic Vehicle Architecture (GVA) Part: 0 : GVA Approach

[9] OMG DDS, http://portals.omg.org/dds/what-is-dds-3/

[10] DDS: OMG. Data Distribution Service (DDS), Version 1.4. Object Management Group, 2015. url: http://www.omg.org/spec/DDS/1.4

[11] DDSI: OMG. The Real-time Publish-Subscribe Protocol (RTPS) DDS Interoperability Wire Protocol Specification, Version 2.2. Object Management Group, 2014

# Technologische Trends in der Radartechnik

**Radarsysteme sind für heutige moderne Armeen unverzichtbar. Nur mit Radargeräten lassen sich weitentfernte Flugzeuge, Marschflugkörper oder Artilleriegeschosse zeitgerecht bei Tag und Nacht bei jedem Wetter erfassen. Die Bedeutung steigt stetig an, da markante Technologiefortschritte Verbesserungen und neue Möglichkeiten erlauben. Rotierende Antennen gehören schon bald der Vergangenheit an und werden durch Antennen mit elektronisch gesteuerter Strahlschwenkung ersetzt. Multifunktionssysteme werden mehrere Aufgaben gleichzeitig erfüllen können. Satellitensignale lassen sich künftig nutzen, um unauffällig die Umgebung nach Bedrohungen abzusuchen. Intelligente Kleinsysteme werden auf Minidrohnen und Fahrzeugen eingesetzt. Dieser Artikel thematisiert die Technolgiefortschritte und stellt die neuen Möglichkeiten vor.**

**Keywords:** **Radararchitektur, Gallium-Nitrid-Halbleitertechnologie, Multifunktionssystem, Drohnendetektion, kognitive Prinzipien, Passives Radarsystem, holographisches Verfahren, wetterunabhängige Bildaufklärung**

**Autor:** **Dr. Peter Wellig**, armasuisse W+T

Das Radarprinzip, d.h. die Ortung eines Ziels basierend auf elektromagnetischen Wellen, stösst sowohl in zivilen wie auch militärischen Anwendungen auf grosses Interesse. Im zivilen Umfeld hat in den letzten Jahren die Automobilindustrie einen Technologieschub zu modernen radarbasierten Abstandssensoren ausgelöst. Aufgrund des grossen Bedarfs und der Massenproduktion sind heutzutage sehr günstige Komponenten erhältlich.

Wichtige Kenngrössen militärischer Systeme sind grosse Reichweite, Genauigkeit und Resistenz gegenüber Störungen. Gewollte Störungen des Gegners, z.B. von elektromagnetischen Störsignalen oder Täuschmitteln (z.B. Düppel) gilt es zu unterdrücken, damit die eigentlichen Ziele trotzdem fehlerfrei erfasst werden. Eine weitere Fähigkeit ist die korrekte Klassifizierung, d.h. das Radargerät sollte erkennen, ob es sich um ein Flugzeug, einen Helikopter, eine Drohne oder ein Fahrzeug des Gegners handelt oder nicht.

Die bekannteste militärische Anwendung betrifft die Detektion von nicht-kooperativen Flugzielen mit Flugüberwachungsradarsystemen. Gefechtsfeldradargeräte erfassen die Aktivitäten am Boden, d.h. Bewegungen von Fahrzeugen und Personen und ermöglichen somit eine Übersicht der Bodenaktivitäten innerhalb eines vordefinierten Perimeters. Abbildende Systeme dienen zur Fernerkundung oder Bildaufklärung aus der Luft oder dem Weltraum. Durch Wolken hindurch lassen sich hochpräzise Abbildungen der Erdoberfläche erzeugen.

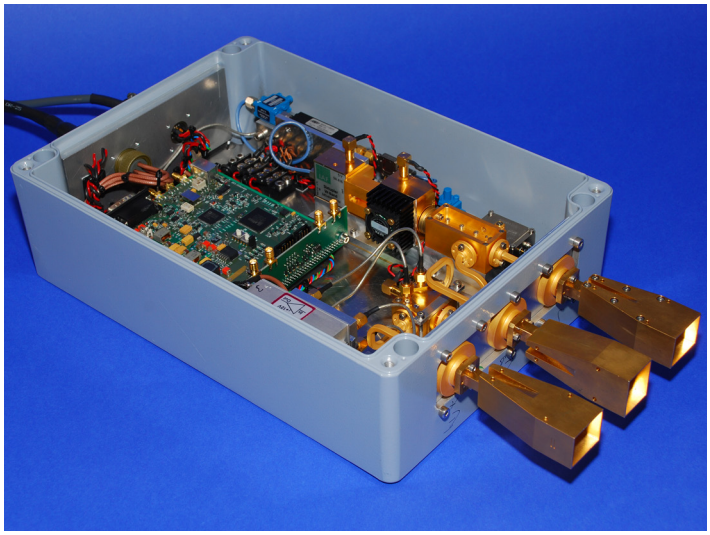


***Abbildung 1:*** *Ein frequenzmoduliertes Dauerstrich-Radar-System des Fraunhofer-Instituts für Hochfrequenzphysik und Radartechnik. Die Betriebsfrequenz liegt bei 94 GHz. Die Hochfrequenzkomponenten sind kompakt integriert.*

## Technologiefortschritte der Schlüsselkomponenten

Zur Generierung und Verarbeitung der hochfrequenten Signale bedarf es diverser Schlüsselkomponenten. Solche Komponenten sind beispielsweise schnell anzusteuernde Signalfilter und rauscharme Signalverstärker. Die Signalfilter dienen zur Filterung der Nutzsignale und zur Verbesserung der Signalqualität und die rauscharmen Verstärker zur Weiterverarbeitung sehr schwacher, weit zurückgestreuter Radarwellen. Diese und weitere Hochfrequenzbauteile auch aus dem Bereich der Telekommunikation erreichen aufgrund besserer Halbleitermaterialien (z.B. Gallium-Nitrid-Technologie [1]) zunehmend bessere Kennwerte, was letztlich die Reichweite und die operative Leistungsfähigkeit verbessert.

Von Vorteil ist es, die Signale digital zu erzeugen und zu verarbeiten. Ultraschnelle Analog-Digital- und Digital-Analog-Signalwandler werden stetig hinsichtlich Geschwindigkeit und Auflösung verbessert. Dies erlaubt eine Digital-Analog- und Analog-Digital-Wandlung des Radarsignals direkt bei der Antenne, wodurch die Vorteile der Digitalisierung optimal genutzt und die Funktionalitäten *software defined* werden [2, 3].

Schnelle Speichermedien mit grossen Speicherkapazitäten und leistungsstarke digitale Signalprozessoren entsprechen weiteren Schlüsselkomponenten. Das zukünftige Radargerät besitzt ein Gedächtnis und eine Intelligenz, d.h. Informationen der Umgebung und der Ziele werden über eine lange Beobachtungszeit ausgewertet und gespeichert [4]. Hinzu kommt, dass die volle Digitalisierung, die hochkomplexen Algorithmen, die grosse Anzahl von anzusteuernden Komponenten wie auch die geforderte Multifunktionalität massive Rechenleistungen beanspruchen werden. Der allgemeine Technologietrend zu besseren Speichermedien und schnelleren Signalprozessoren bewirkt deshalb auch bei Radarsystemen einen Technologieschub.

## Antennen: Intelligent und komplex

Rotierende Antennen werden bereits heute durch aktive Phased-Array-Antennen (*Active Electronically Scanned Array* AESA) ersetzt, bei denen die Strahlschwenkung elektronisch durchgeführt wird. Die Basis bilden sehr viele kleine Sende-Empfangseinheiten, die durch eine Kontrolleinheit angesteuert werden. Mit der sogenannten digitalen Keulenformung (*digital beamforming*) lassen sich gleichzeitig mehrere Strahlen und Strahlrichtungen realisieren. Dies ermöglicht die gleichzeitige Ortung von vielen kleinen oder weit entfernten Zielen. Die simultane Überwachung von Luft- und Bodenzielen inkl. Artillerieaufklärung, die Erfassung des Wetters und in Zukunft vermutlich auch die neu integrierte Datenkommunikation beschreiben nur einige Aspekte der neuen Multifunktionalität zukünftiger AESA-Systeme. In

der Literatur [5, 6] werden die Multifunktionssysteme als *Radio Frequency*-Systeme bezeichnet und der Begriff Radar entfällt.

Eine andere vielversprechende Antennentechnologie stammt ursprünglich aus der Datenkommunikation. Systeme mit sogenannten MIMO (*Multiple Input Multiple Output*) Antennen strahlen gleichzeitig verschiedene Sendesignale aus, was eine gute räumliche Auflösung über einen grossen Abdeckungsbereich ermöglicht. MIMO-Radarsysteme zeigen zudem eine robuste Unterdrückung der Störsignale auf [7].

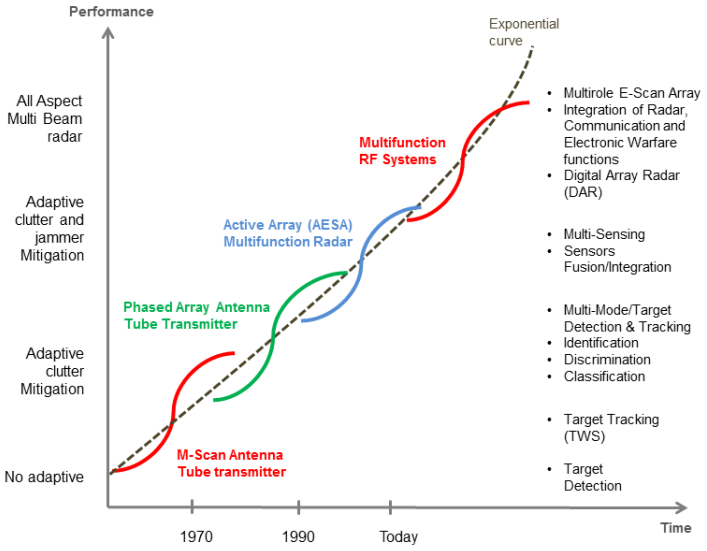



***Abbildung 2:*** *Die Weiterentwicklung der Radartechnologie in Form als S-Kurven dargestellt [5].*

## Frequenzbenutzung im Zusammenspiel mit mobiler Datenkommunikation

Der Bedarf der mobilen Datenkommunikation an grösseren Datenkapazitäten steigert das Interesse an Frequenzbändern, welche auch von Radarsystemen benutzt werden können. Das stellt eine grosse Herausforderung dar, da die verschiedenen Systeme sich nicht stören sollten. Ein umstrittener Frequenzbereich befindet sich beispielsweise zwischen 2 – 6 GHz. Die Forschung visiert eine Koexistenz an, d.h. die Benutzung des gleichen Frequenzbandes durch Radarsysteme und mobile Datenkommunikation ohne gegenseitige Störung [8]. Aktuell lassen sich Forschungsanstrengungen in diesem sogenannten RADCOM (Radar und Kommunikation) Bereich erkennen. Der MIMO-Ansatz entspricht hierbei der einen Forschungsrichtung. Ein anderer Forschungstrend betrifft das sogenannte kognitive Radarsystem, welches verstärkt die Umweltbedingungen und das elektromagnetische Spektrum analysiert und fortlaufend eine optimierte Anpassung der Parameter (z.B. Wellenformen) durchführt, auch zur Vermeidung gegenseitiger Störungen.

***Abbildung 3:*** *Rotierende Radarantennen werden künftig durch Antennen mit elektronisch gesteuerter Strahlschwenkung ersetzt (Bild TAFLIR-Radar der Schweizer Armee, © VBS/DDPS).*

## Das unsichtbare Radargerät

Radarsysteme lassen sich relativ einfach orten, da die ausgesendeten elektromagnetischen Wellen auch vom Gegner erfasst werden. Das ist ein Grund, warum das Interesse an passiven Systemen stetig steigt. Ein Passivradarsystem entspricht einer hoch modernen und sensiblen Empfangseinheit, welche die bereits vorhandenen Rundfunksignale (z.B. FM, DAB, DVB-T) zur Detektion bzw. zur Beleuchtung von Flugzielen verwendet. Man spricht auch vom bistatischen Fall, da Sender und Empfänger örtlich getrennt sind. Eine Ortung des Passivradarempfängers basierend auf elektromagnetischer Strahlung ist somit praktisch unmöglich.

Das Potenzial heutiger Passivradarsysteme wurde in den letzten Jahren erfolgreich demonstriert. Die Systeme weisen eine hohe Technologiereife auf; einem operationellen Einsatz bzw. einer Kommerzialisierung steht prinzipiell nichts im Wege [9, 10]. Beispielsweise zeigt das Passivradargerät im Gegensatz zu aktiven Systemen gute Eigenschaften zur Detektion von tieffliegenden Flugzielen [11] oder für die Überwachung von Tälern auf; es kann aber auch generell dort eingesetzt werden, wo Emissionsgrenzen den Einsatz aktiver Systeme verbieten.

Die Erweiterung des bistatischen Prinzips auf mehrere Sender und mehrere getrennte Empfänger lässt sich in der Forschung beobachten und betrifft auch eher traditionellere Radarfrequenzen. Man spricht von multistatischen (aktiven) Systemen [12]. Damit könnten Luftziele aus verschiedenen Richtungen erfasst werden, was eine bessere Ortung erlaubt. Herausforderungen widerspiegeln sich in der hochgenauen Synchronisation der verschiedenen Sende- und Empfangseinheiten sowie in der Datenverarbeitung in diesem Netzwerk.

## Drohnendetektion - eine grosse Herausforderung

Drohnen, insbesondere Kleindrohnen, werden zunehmend zu einer ernsthaften Bedrohung und deren Anzahl wird in den nächsten Jahren durch verstärkte Flugautonomie und Massenproduktion weiter zunehmen. Infolge kostengünstiger Miniaturisierung der Hochfrequenzkomponenten, z.B. durch Silizium-Germanium-Halbleitertechnologie, werden zukünftige Kleindrohnen mit sehr kleinen Radargeräten ausgestattet werden, was autonome Flüge im urbanen Gelände oder Schwarmmissionen erlauben wird.

Auf der anderen Seite ist die Detektion und Bekämpfung von kleinen Drohnen (<30 kg) äusserst schwierig. Aufgrund der kleinen Grösse der Flugobjekte, des tiefen Fluges über dem Boden und der grossen Anzahl möglicher Falschziele wie Vögel stossen heutige Radarsysteme für die Boden-Luft-Aufklärung an ihre Grenzen. In der Forschung sind zahlreiche Ansätze sichtbar um trotzdem eine automatische Ortung und eine robuste Zielzuweisung zu erreichen.

Ein vielversprechender Ansatz nützt die Messung der typischen Flugbewegungen aus. So ermöglicht die gemessene Verschiebung der Mikrodopplerfrequenz [13] zwischen dem ausgesandten und empfangenen Signals die Unterscheidung einer Drohne von einem Vogel aufgrund der Rotorbewegung bzw. des Flügelschlages. Ein anderer Ansatz basiert auf der Weiterentwicklung von kognitiven Prinzipien und digitaler Keulenformung zum sogenannten holographischen Radargerät. Eine lange Beobachtungszeit und eine intelligente Verteilung der Strahlrichtungen erlauben eine vertiefte Analyse von Dopplerfrequenzen und somit eine verbesserte Detektion und Klassifikation von Kleindrohnen. Im Nahbereich (<2 km) verspricht ein Multisensoransatz, d.h. eine Kombination aus günstigem Radarsensor mit anderen Sensoren (z.B. Wärmebildkameras, Mikrofone oder Detektoren für Funkaufklärung) die besten Chancen für einen erfolgreichen Einsatz.

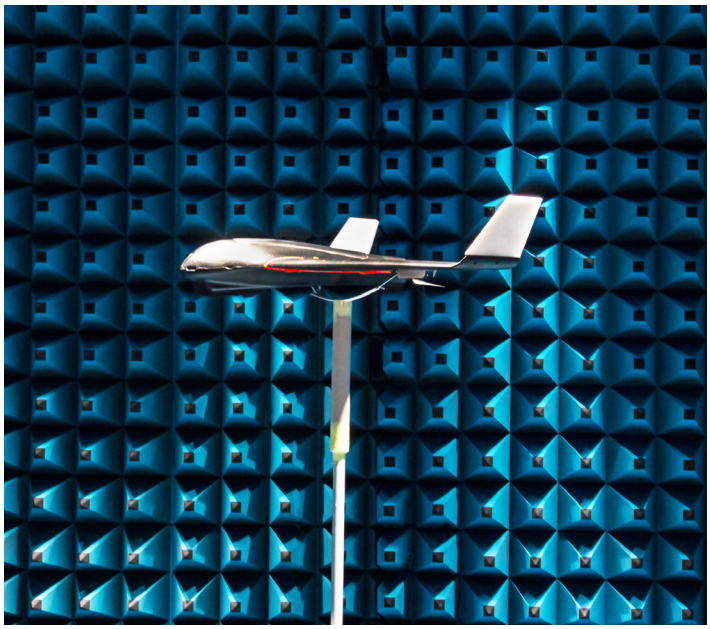


*Abbildung 4: Messung des Radarrückstreuquerschnittes der Drohne Skywalker X-8 FPV in der echofreien Messkammer von armasuisse / Wissenschaft und Technologie © VBS/DDPS.*

## Abbildende Radarsysteme werden wie Videokameras eingesetzt, jedoch tageslichtunabhängig auch bei Regen und Wolken sowie aus einer sagenhaft grossen Distanz

Einen markanten technologischen Fortschritt erwartet man auch für abbildende Systeme (*Synthetic Aperture Radar* SAR). SAR-Systeme werden auf Drohnen, Flugzeugen und Satelliten eingesetzt. Sie sind für die Bildaufklärung (*Imagery Intelligence* IMINT) von grossem Interesse, da die Bilder der Erdoberfläche zu jeder Tageszeit (Tag/Nacht) auch bei Wolken, Nebel und Regen erstellt werden können. Im Gegensatz zu visuellen Bildern hängt die geometrische Auflösung der SAR-Bilder nicht von der Abbildungsdistanz ab. Je nach Wahl des Schrägsichtwinkels, Flughöhe, Sendeleistung und Frequenzbereiches können sehr grosse Abbildungsdistanzen mit sehr guter Bildqualität erreicht werden.

Prinzipiell sind zahlreiche Zusatzinformationen für den Bildauswerter durch Antennen- und Softwareerweiterungen erhältlich. Beispielsweise ergeben sich 3D-Informationen zum Gelände und zu Gebäuden mittels Interferometrie (cross-track Interferometrie). Erkenntnisse zu kleinsten Veränderungen, z.B. der Bodenoberfläche bei Tunnelgrabungen, leiten sich durch differentielle Interferometrie ab. Die Zusatzoption „Bewegtziel-Detektion" (*Ground Moving Target Indication* GMTI) stellt eine Übersicht aller fahrenden Fahrzeuge innerhalb des ausgeleuchteten Gebietes dar [14]. Der klassische Ansatz dazu ist die along-track Interferometrie.

Die Generierung von scharf fokussierten Bildern aus den erfassten Radarechos ist äusserst rechenintensiv. Heutige SAR-Systeme zeigen bereits Echtzeiteigenschaften auf, jedoch nicht für höchste Bildauflösungen und nicht im georeferenzierten Bildformat. Durch gesteigerte Rechenkapazitäten auf Drohnen und Flugzeugen wird die Forderung nach höchster Auflösung und Echtzeitfokussierung (Stichwort *video-like* SAR) zunehmend besser erfüllt.

Die Auswertung der SAR-Bilder ist sehr aufwändig, da sie sich nicht wie visuelle Aufklärungsaufnahmen interpretieren lassen; SAR-Bilder wiederspiegeln vielmehr das Rückstreuverhalten der Erdoberfläche in Bezug auf die ausgesendeten elektromagnetischen Wellen. Voraussetzungen für eine erfolgreiche Bildauswertung sind eine gute Bildauflösung, eine scharfe Bildfokussierung, eine gute radiometrische Qualität, d.h. wenig Bildrauschen, Referenzbilder bzw. Referenzdaten und ein geübter Auswerter. Die Bildauflösung hat einen direkten Zusammenhang mit der Frequenzbandbreite der Sendesignale und der Genauigkeit der Fluglagedaten. Infolge von Fortschritten bei Hochfrequenzkomponenten, Antennentechnologie, Algorithmen und Signalprozessoren sind markante Verbesserungen der Bildauflösung bis in den Millimeterbereich zu erwarten [15].

Die Auswertung wird zusätzlich verbessert, bzw. Ziele werden besser erkannt, indem zukünftig Zusatzinformationen in hoher Qualität und in Echtzeit zur Verfügung stehen werden. Dies sind beispielsweise 3D-Informationen, geschätzte Geschwindigkeitswerte von Fahrzeugen oder die Charakterisierung einer Bodenstruktur auf Basis der Auswertung von Strahlungs- und Streueigenschaften der Oberflächen (polarimetrische Messgrösse). Die technische Realisierung sieht mehrere Antennen und eine massiv parallele Datenverarbeitung vor [16].

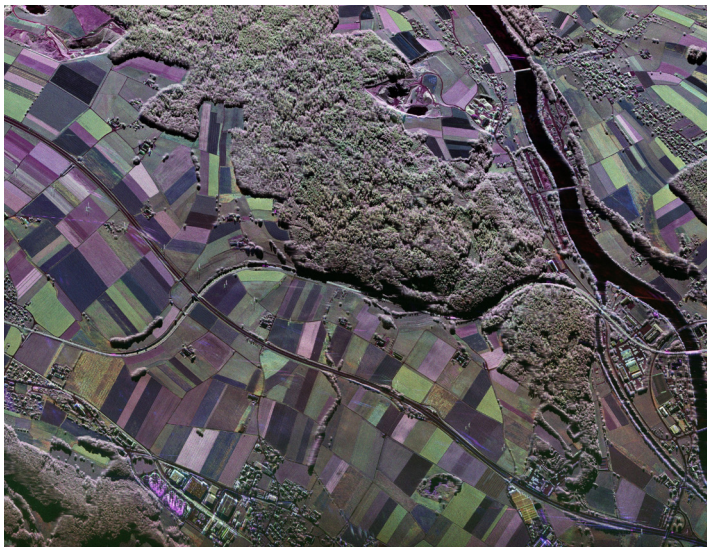


*Abbildung 5: SAR-Bild des Gebietes Wangen an der Aare (© VBS/DDPS). Die Farbwahl basiert auf polarimetrischen Radareigenschaften. Das SAR-Bild wurde durch den F-SAR-Sensor des Deutschen Zentrums für Luft- und Raumfahrt (DLR) erfasst.*

Die Verbesserung der Daten- bzw. Informationsqualität ermöglicht in Zukunft nicht nur die Verfolgung von Fahrzeugen aus einer grossen Distanz, sondern auch von menschlichen Aktivitäten. Der sogenannte DMTI (*Dismount Moving Target Indication*) Modus wird äusserst leistungsschwache Signale weiterverarbeiten und somit sehr langsame Bewegungen wie die eines Menschen erfassen können. Man spricht in diesem Zusammenhang von einem Paradigmawechsel [17].

Neben den erwähnten Fortschritten in Auflösung, Echtzeitfähigkeit und Multikanalinformation gilt es die Bildfokussierung bei Kurven- und Kreisflügen zu erwähnen. Die Fluggeometrie bei SAR-Aufnahmen ist grundsätzlich eingeschränkt, um ein scharf fokussiertes Bild über eine gewisse Integrationszeit zu generieren. Antennenanpassungen und moderne Fokussierungsalgorithmen werden in Zukunft beliebige Flugwege bei SAR-Aufnahmen erlauben. Diese Fortschritte ermöglichen letztendlich den Einsatz von SAR-Systemen auf Drohnen und Flugzeugen nicht nur für die Aufklärung sondern auch für taktische Überwachungsaufgaben.

Bi- und multistatische Ansätze sind auch bei SAR-Systemen von Interesse. So wurden in der Forschung bereits erfolgreich Empfänger auf Flugzeugen eingesetzt, welche vom Boden rückgestreute Radarwellen eines zweiten SAR-Flugzeuges oder eines SAR-Satelliten erfassen konnten. In Zukunft sind auch kleine intelligente Empfänger auf Minidrohnen denkbar. Zu nennen sind auch die Forschungsanstrengungen zur Verwendung von nicht-SAR Satellitensignalen (z.B. GPS) oder von Rundfunksignalen (DVB-T) für die Bildgenerierung, allerdings nur bei geringer Bildauflösung.

## Weitere Radarthemen

Abschliessend gilt zu erwähnen, dass auch zu den nicht genannten Themen wie zu Boden- und Wanddurchdringungsradar, *Low Probability of Intercept Radar* wie Rauschradar, Quantumradar, Mikrowellen-Photonik, Compressed Sensing oder radarabsorbierenden Materialien wie auch den zahlreichen elektromagnetischen Gegenmassnahmen (Tarnung, Störung, Täuschung) mit erheblichen Verbesserungen zu rechnen ist.


## Verdankung

Der Autor dankt herzlichst den Herren Dr. Hans Pratisto, Dr. Christof Schüpbach und Dr. Hansruedi Bircher von armasuisse Wissenschaft und Technologie sowie Herrn Dr. Alexander Hommes von dem Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik für die wertvollen Beiträge und Diskussionen zu diesem Artikel.



**Dr. Peter Wellig**

ist Forschungsprogrammleiter bei armasuisse Wissenschaft und Technologie. Er ist Elektroingenieur ETH und hat Nachdiplomstudiengänge in Informationstechnologie, Projektmanagement und Forschungsmanagement absolviert. In dem von ihm geführten Forschungsprogramm "Aufklärung und Überwachung" werden Technologien zu Radar- und weiterer Aufklärungssensorik in einem nationalen und internationalen Forschungsnetzwerk bearbeitet. Dr. Wellig ist Programmkomiteemitglied der internationalen SPIE Konferenz Target and Background Signatures. Seit 2004 ist er in diversen Funktionen der Forschungsorganisation der NATO/PfP tätig.

Seine Kontaktadresse ist
peter.wellig@armasuisse.ch.


## Referenzen


[1] B. Manz, How Far Can We Take GaN Technology?, The Journal of Electronic Defense, März 2015.

[2] D. Richardson, AESA Radar Technology, armada international, 3/2015.

[3] S. H. Talisa, Benefits of digital phased Array Radars, Proceedings ot the IEEE, Vol. 104, No. 3, März 2016.

[4] A. White, NATO faces up to radar challenges, IHS Jane's International Defence Review, Oktober 2015.

[5] A. Farina et al., AESA Radar – pan-domain multi-function capabilities for future systems, IEEE International Symposium on Phased Array Systems & Technology, Boston MA, Oktober 2013.

[6] H. Griffiths, Vectors in Radar Technology, IEEE AES Magazine, August 2016.

[7] P. Quaranta, Radar Technology for 2020, MILTECH, 9/2016.

[8] Spectrum Sharing Access for Radar and Communication (SSPARC) Program, DARPA, http://www.darpa.mil/program/shared-spectrum-access-for-radar-and-communications

[9] https://www.hensoldt.net/solutions/land/radar/passive-radar/

[10] https://www.thalesgroup.com/en/worldwide/homeland-alerter-100

[11] Ch. Schuepbach et al., Micro-UAV Detection using DAB-based Passive Radar, Konferenz IEEE Radar, Mai 2017.

[12] U. Boeniger et al., WYSIWYG or the more you see the better you get – towards a multistatic C-band radar system, NATO Expertenworkshop SET-231 Multi-Band Multi-Mode Radar, Oktober 2016.

[13] A. Schroeder et al., Numerical RCS and Micro-Doppler Investigations of a Consumer UAV, SPIE Konferenz Security and Defence, September 2016.

[14] S.L. Pendergast, Recent Advances in Radar Technology, Aerospace and Defense Channel, Microwave Journal, September 2015.

[15] M. Frioud et al., Implementation of a fast time-domain processor for FMCW Synthetic Aperture Radar data, SPIE Konferenz Remote Sensing, September 2015.

[16] Del Castillo et al., L-Band Digital Array Radar Demonstrator for Next Generation Multichannel SAR Systems, IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, Juni 2015.

[17] General Atomics, Lynx Multi-mode Radar, http://www.ga-asi.com/lynx-multi-mode-radar

# Les lasers militaires de haute puissance

**Les lasers de haute puissance sont à la veille d'atteindre un développement qui permettra leur intégration dans des systèmes militaires mobiles terrestres. Cet article tente de fournir quelques points de repère concernant les puissances laser requises pour neutraliser ou combattre diverses catégories de cibles (telles que capteurs optoélectroniques, drones, engins explosifs improvisés, obus de mortier ou roquettes). Après un aperçu des difficultés techniques devant encore être résolues pour permettre un usage militaire des lasers de puissance, les principaux avantages et inconvénients de ce nouveau type d'arme sont brièvement esquissés.**

**Mots-clés:** **Laser, puissance, densité de puissance, portée, temps d'illumination, C-RAM, drone, conditions météorologiques**

**Auteur:** **Dr. André Koch**, Dynamic Phenomena Sàrl

Initiée en 1983 par le président américain Ronald Reagan, l'Initiative de Défense Stratégique avait pour but l'interception de fusées intercontinentales, notamment à l'aide de systèmes laser de haute puissance. Trop ambitieux, le projet fut abandonné en 1993, à la fin de la guerre froide. Il a pourtant stimulé le développement d'armes laser de forte puissance; dès l'an 2000, des avions de type Boeing 747 ont été modifiés pour embarquer des lasers 2 MW: d'une masse de 40 tonnes, ces derniers devaient permettre la destruction de missiles à 400 km de distance, mais n'ont, semble-il, jamais été efficaces au-delà de 150 km; là encore, le projet fut interrompu en 2012. Depuis cette date, la technologie des sources laser a fortement progressé, atteignant presque les objectifs de puissance, d'encombrement et de poids qui permettront de les rendre opérationnelles dans des systèmes mobiles terrestres.

Ci-dessous, nous présenterons brièvement les principales caractéristiques d'un laser, puis donnerons un aperçu des possibilités qu'offrent les armes laser en fonction de leur puissance. On conclura par une estimation des avantages et inconvénients de ces systèmes relativement à un armement conventionnel.

## Caractéristiques d'un laser

Dans l'usage militaire, les lasers de haute puissance sont prévus pour concentrer de grandes quantités d'énergie sur une cible en vue d'en éblouir les capteurs optoélectroniques ou d'en affaiblir thermiquement la structure. Deux caractéristiques du laser sont déterminantes.

1. La puissance (en kW) de la source laser représente l'énergie lumineuse rayonnée par unité de temps.
2. La densité de puissance (en W/mm$^2$) correspond à la puissance par unité de surface. Cette grandeur est cruciale pour estimer l'impact du rayonnement sur la cible: plus la densité de puissance est élevée et plus rapidement la cible sera endommagée thermiquement.

Pour éviter d'abîmer l'optique de sortie du laser de puissance (échauffement des miroirs et lentilles par absorption d'une partie de l'énergie lumineuse émise), le faisceau laser produit a un diamètre initial relativement grand (quelques décimètres) et l'on fait converger ce faisceau sur la cible à l'aide d'un télescope. Par exemple, en focalisant un faisceau laser de 10 kW ayant un diamètre initial de 25 cm sur une tache de 5 cm, on passe de 0,2 W/mm$^2$ dans le télescope de sortie, à 5 W/mm$^2$ sur la cible. Dans cet exemple, on n'a pas tenu compte de la perte de puissance du laser lors de sa propagation dans l'atmosphère : dans les faits, la qualité d'un faisceau laser se dégrade, son énergie lumineuse diminue en fonction de la distance parcourue. Les principales causes de ces altérations sont les suivantes.

- Absorption et diffusion de la lumière réduisent l'énergie d'un faisceau lumineux. Cette atténuation du faisceau dépend des conditions atmosphériques (temps clair, brume, brouillard, pluie, neige, etc.)
- Les variations de l'indice de réfraction dues aux fluctuations de température et à la turbulence de l'air induisent la réfraction des rayons lumineux.

Ces effets perturbateurs limitent la portée utile des lasers. La Figure 1 illustre la variation de la densité de puissance d'un faisceau laser en fonction de la distance parcourue dans l'air. Jusqu'au point de convergence du faisceau, la densité de puissance augmente parce que le télescope du laser focalise le faisceau sur la cible; au-delà de la cible, l'intensité lumineuse diminue en raison de la divergence du faisceau et par atténuation dans l'atmosphère.

De nos jours, la plupart des lasers militaires de haute puissance travaillent dans l'infrarouge, à la longueur d'onde de 1064 nm.

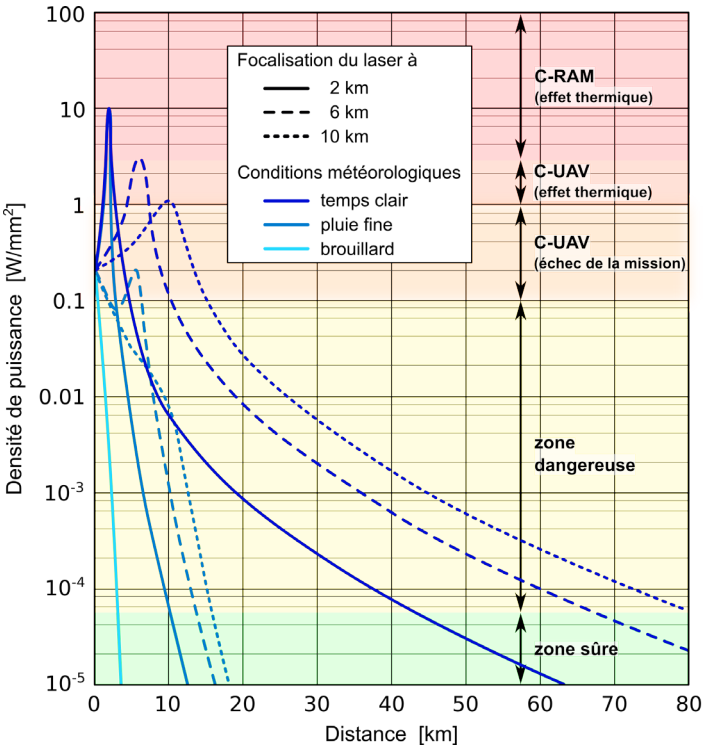



*Figure 1: Densité de puissance d'un faisceau laser en fonction de la distance, pour divers éloignement de la cible (2, 6 et 10 km) et selon les conditions météorologiques (temps clair, pluie fine ou brouillard). Dans cet exemple, la puissance du laser est de 30 kW (3 sources de 10 kW) avec une densité de puissance de 0.2 W/mm$^2$ sur les miroirs du télescope de sortie [2]; jusqu'au point de convergence, la densité de puissance augmente en raison de la focalisation du faisceau laser (le diamètre du faisceau diminue); au-delà de ce point, la densité de puissance décroît par suite de l'atténuation due à l'atmosphère et parce que le faisceau laser diverge derrière la cible.*

## Puissance requise pour un laser militaire

En fonction de l'effet recherché sur la cible, la puissance laser requise variera de quelques kW à plusieurs centaines de kW.

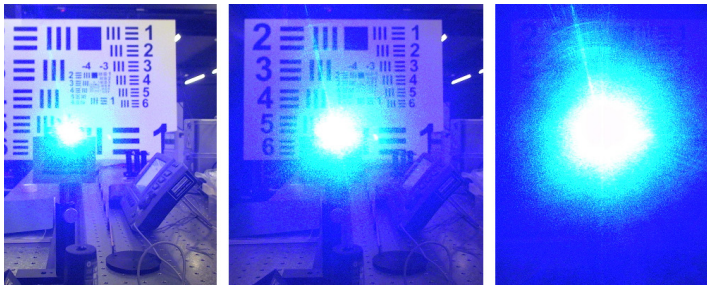


***Figure 2:*** *Effet d'un faisceau laser illuminant une caméra vidéo. La puissance du faisceau laser est respectivement de 0,06 mW (image de gauche), 0,36 mW (au centre) et 6 mW (à droite). Lorsque l'illumination laser cesse, la caméra vidéo présente un temps de latence d'environ une seconde avant de fournir à nouveau une image claire. Dans cet essai, la situation est idéale, avec le faisceau laser parallèle à l'axe optique de la lentille.*

Pour perturber un senseur optique (par exemple, une caméra vidéo comme dans la Figure 2), il suffira d'une dizaine de milliwatts sur le capteur; en tenant compte de l'atténuation atmosphérique, de la divergence du faisceau et de son angle d'incidence sur la cible, il faudra pourtant disposer de quelques kilowatts à la source pour être en mesure de perturber les senseurs optiques en toutes situations (distance à la cible de plusieurs kilomètres, angle d'incidence défavorable du faisceau sur la cible, conditions météorologiques désavantageuses).

La destruction d'engins explosifs, tels que munitions non explosées ou engins explosifs improvisés, pourra se faire à l'aide d'un laser d'une puissance de 1 à 5 kW, à condition que l'objet à détruire ne soit pas enterré (une couche de quelques centimètres de sable humide ou de terre suffit à dissiper la chaleur déposée par le laser): en illuminant l'objet à plusieurs centaines de mètres avec le faisceau laser, on l'échauffe jusqu'à destruction de la charge (figure 3).

Pour endommager la structure d'un micro- ou un mini-drone (masse inférieure à 20 kg) à une distance d'un kilomètre, la puissance laser devra atteindre 10 à 50 kilowatts. La difficulté est ici d'illuminer durant 5 à 10 secondes un point donné du drone pour l'affaiblir thermiquement ou l'enflammer (Figure 3).

Dans la lutte contre les obus d'artillerie ou de mortier (C-RAM, Counter Rocket, Artillery and Mortar), les lasers ont démontré leurs performances. Pour être utilisable, le laser devra idéalement délivrer 100 kW ou plus. Des essais C-RAM ont été effectués avec des lasers de 30 à 50 kW, mais avec des durées d'illumination assez longues (5 à 10 secondes), des distances à la cible relativement faibles (environ 1 km), des angles d'illumination favorables et de bonnes conditions météorologiques.

***Figure 3:*** *Résultat de l'illumination de cibles diverses par un faisceau laser de haute puissance [2].*

***A gauche****: poutrelle d'acier, illuminée durant 250 secondes environ par une source laser de 35 kW, distante de 1 km.*

***Au milieu****: obus de mortier de 8,1 cm, illuminé durant 10 secondes environ par une source de 50 kW, distante de 1 km.*

***A droite****: mini-drone, illuminé durant 10 secondes environ par une source de 30 kW, distante de 1 km.*

Ces valeurs sont résumées dans les deux tables suivantes qui fournissent, pour divers types d'engagement, une estimation de la puissance requise [1] et de la portée du laser [2].

| | Puissance du laser | | | |
|---|---|---|---|---|
| | ≈ 10 kW | ≈ 100 kW | 100 – 900 kW | > 1 MW |
| Objet combattu avec le laser | Micro- et mini-drones à faible distance | Micro- et mini-drones à grande distance<br>Structures au sol (mats, antennes, etc.)<br>Véhicule non-blindé | Obus d'artillerie et de mortier (C-RAM) à 5-10 km<br>Défense sol-air à 0-5 km | Tous types d'objets volants (p.ex. missiles de croisière) à 5-20 km |

***Table 1:*** *Puissance laser requise en fonction de l'objet combattu.*

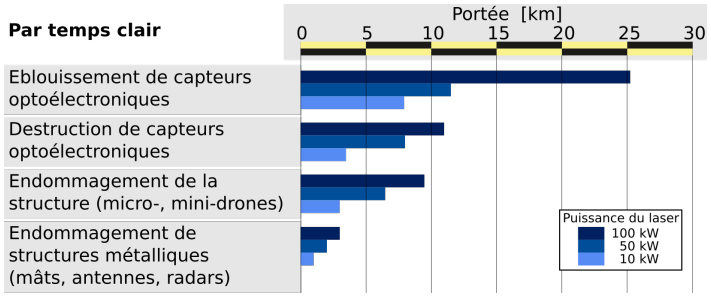



***Table 2:*** *Portée du laser en fonction de sa puissance.*

## Les difficultés techniques à surmonter

A moins de se limiter à des engins explosifs statiques ou à des micro- et mini-drones, le laser doit idéalement délivrer un faisceau de 100 kW ou plus. Intégrer des lasers aussi puissants dans un environnement militaire exige de résoudre un certain nombre de difficultés techniques, ce qui demandera encore 5 à 10 ans d'efforts [2, 3, 4].

- Les lasers de puissance sont encore trop lourds et volumineux pour des systèmes mobiles terrestres. Pour un laser de 10kW, il faut compter avec un poids de 2t et un encombrement de 4 m³, comme présenté sur la Figure 4.
- Le rendement des systèmes lasers est faible ; il ne dépasse guère 30%: un système laser de 100 kW requiert une source capable de délivrer plus de 300 kW : 200 kW sont dissipés en chaleur!


***Figure 4****: Démonstrateur du système laser mobile de 20 kW de Rheinmetall. On notera, sur le toit du véhicule, la tourelle avec télescopes pour deux lasers de 10 kW.*

- La propagation du faisceau laser dans l'atmosphère entraîne l'atténuation, la dispersion et la décohérence du faisceau. Ces pertes peuvent être partiellement compensées par la technologie du miroir adaptatif: la surface du miroir du télescope est déformée en temps réel pour compenser les turbulences atmosphériques sur le parcourt du rayon laser. Cette technologie, mise au point pour l'astronomie, est en cours d'adaptation aux lasers de puissance.
- Les lasers militaires sont mis en œuvre à ciel ouvert: ceci requiert des systèmes de contrôle du laser afin d'éviter tout dommage collatéral que pourrait engendrer le faisceau laser en cas, par exemple, de réflexion sur la cible ou lorsque celle-ci a été manquée. Un laser focalisé sur une cible située à 6 km reste potentiellement dangereux jusqu'à 70 km (voir Figure 1).

## Avantages des lasers de puissance sur les systèmes conventionnels

Par rapport à l'armement tactique conventionnel, les lasers de puissance présentent une série d'avantages.

- Le laser de puissance est un système versatile : l'énergie émise est adaptable à la cible et à l'effet recherché; on peut passer en une fraction de seconde d'une action non-létale à un effet létal.
- Les risques collatéraux sont minimes en comparaisons d'une munition classique. Le système étant silencieux et le rayon laser invisible (infrarouge), son utilisation est envisageable pour protéger de grands événements publics; l'usage du système laser est discret, réduisant le risque de provoquer une panique dans la foule.
- En raison de la vitesse de propagation du faisceau laser (la vitesse de la lumière), il n'y a pas lieu d'effectuer de calculs balistiques pour tenir compte du vent ou du retard sur la cible. Ceci est particulièrement avantageux lorsque cette dernière est petite et agile. Par contre, la cible doit rester visible durant le temps d'illumination.
- Si l'on ne tient pas compte de l'amortissement de l'appareillage, le prix d'un tir laser est bon marché (< CHF 1.-) comparé au coût de la munition classique. Les coûts d'exploitation d'un système laser sont inférieurs à ceux d'un système conventionnel : les composants mécaniques n'étant pas soumis à fortes sollicitations, l'usure de l'appareillage reste faible.
- La logistique est restreinte (pas de stockage ni de transport de munition, pas de surveillance de la munition).

## Inconvénients des lasers de puissance

Face à ces atouts, quelques défauts ou limitations des lasers de puissance doivent être mentionnés.

- Puissance encore trop limitée et encombrement excessif: pour être utilisable dans le contexte de la défense anti-aérienne, et si l'on ne veut pas se limiter à combattre des micro- et mini-drones, la puissance minimale d'un laser devrait atteindre 100 kW. Ces puissances ne sont pas encore disponibles sur des systèmes mobiles terrestres.
- Des conditions météorologiques défavorables (pluie, neige, brouillard) limitent l'usage du laser de puissance qui doit donc être combiné avec des systèmes classiques.
- Le prix d'un système laser de haute puissance reste, à ce jour, rédhibitoire: une estimation grossière donne des coûts de l'ordre de 0,5-1 Mio CHF par kW. Les énormes coûts de développement liés au «durcissement militaire», l'aspect encore expérimental des lasers de haute puissance dans le domaine de la défense sont causes de ces prix élevés.

## Conclusions

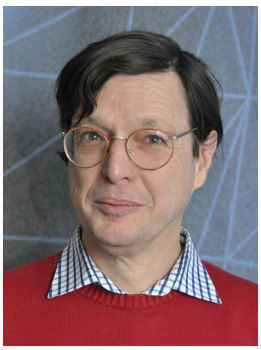
Les systèmes laser de haute puissance ont fait des progrès considérables dans les vingt dernières années; dans un environnement industriel, des lasers capables de délivrer 100kW en puissance continue sont déjà opérationnels; pour être utilisables dans un contexte militaire, ces systèmes doivent être «durcis» pour résister aux contraintes environnementales usuelles (température, vibration, humidité, poussière et sable, etc.)

En dépit des difficultés technologiques, il est hautement probable que les progrès techniques permettront, d'ici 2025, l'intégration de lasers délivrant 100 kW ou davantage dans des systèmes terrestres mobiles. Les limitations évoquées ci-dessus entraîneront que les armes laser seront couplées avec des armements classiques.

Les avantages tactiques et opérationnels (versatilité, simplicité d'utilisation et faibles coûts d'exploitation) favoriseront l'usage des lasers de puissance. Leur développement technologique doit donc être suivi avec attention.


## Remerciements

L'auteur remercie MM. G. Rubin et B. Ott pour leurs commentaires critiques sur le premier jet de ce texte. Cet aperçu des lasers se base largement sur [2].


## Dr. André Koch

Après des études de physique à l'université de Lausanne, André Koch s'est intéressé à l'étude de la morphogénèse lors d'un séjour post-doctoral au Max-Planck-Institut für Entwicklungsbiologie de Tübingen. Plus tard, de 1997 à 2000, il a travaillé pour l'entreprise suisse SM (Schweizerische Munitionsunternehmung) dans le domaine des charges creuses. De 2000 à 2010, il s'est intéressé à la détonique pour le compte d'armasuisse Sciences et Technologies. Enfin, depuis 2011, il est responsable, pour armasuisse, du programme de recherche concernant l'efficacité des munitions et la protection contre leurs effets ; c'est dans ce cadre qu'a été effectué le travail condensé dans le présent article.


## Littérature


[1] Analysis of High Energy Laser Weapon Employment from a Navy Ship. C. M. Ang, Thesis, Naval Postgraduate School, Monterey, 2012.

[2] Aktueller Stand der militärischen Lasersysteme. Rapport pour armasuisse W+T, Rheinmetall Air Defence, Zürich, 2015.

[3] Special Section Guest Editorial: High-Energy Laser Systems and Components. J.R. Albertine, Optical Engineering, 52 (2), 2012.

[4] Is this the time for a high-energy laser weapon program? D. H. Kiel, Optical Engineering 52 (2), 2012.

# Cyber (In)security in Air Traffic Management

**Many wireless communication and surveillance technologies in the aviation domain lack state-of-the-art security controls as cryptographic solutions prove difficult to deploy. With the rapid increase of cyber threats, serious concerns have been raised about the trustworthiness and safety of the next-generation air traffic management system. We argue for the need of a global intrusion detection system and propose a design based on crowdsourcing.**

**Keywords:** **Aviation security, cyber risks, crowdsourcing, digital avionics, air traffic management**

**Authors:** **Dr. Vincent Lenders**, armasuisse S+T; **Dr. Martin Strohmeier**, University of Oxford; **Matthew Smith**, University of Oxford
**Matthias Schäfer**, TU Kaiserslautern; **Prof. Ivan Martinovic**, University of Oxford

## Introduction

Air traffic management (ATM) is the backbone of what is arguably the key means of personal transport in the modern world. As the traffic load continues to grow dramatically, ATM has to manage ever more aircraft. Large European airports, such as Frankfurt, experience spikes of more than 1,500 daily take-offs and landings, and forecasts predict that world-wide flight movements will double by 2030. Additionally, with the growing adoption of unmanned aerial vehicle (UAV) technology for civil applications, we can expect a further boost in air traffic in the coming years.

To enable safe coexistence in such a dense air space, pilots flying according to instrument flight rules (IFR) have to rely on a plethora of digital communication and navigation technologies. Figure 1 gives an overview of some of the wireless technologies used in ATM between ground stations, aircraft and satellites. Depending on the location and the different flight phases, aircraft may rely on a subset of these technologies at any point in time.

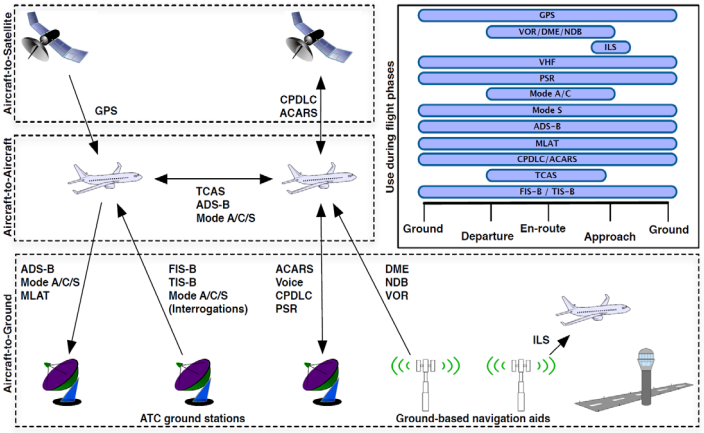



*Figure 1: An overview of the wireless technologies used in air traffic communication, between ground stations, aircraft and satellites.*

Historically, these ATM technologies are rooted in the military domain. However unlike in the military domain where the communication is protected by means of encryption and anti-jamming technologies, their adoption in the civil domain are based on unprotected signals without any sorts of authenticity, confidentiality, or jamming resistance. This approach may seem naïve and irresponsible today, but the design of these technologies dates back to a few decades ago in an era where cyber risks where not considered a major threat. When these technologies were originally designed, the benefits of having an open and interoperable ATM architecture among countries worldwide outweighed the need for protecting aviation systems against cyber attacks. Today, in the cyber era, with the widespread availability of tools such as low-cost software-defined radios (SDR) and open source software, the aviation community lost it is technical advantage in protecting insecure communication from potential attackers.

## Insecurity of Air Traffic Management Technologies

ATM technologies can be categorized in three applications: air traffic control, information services, and navigational aids. Table 1 shows the most important technologies in each application. In all three, there is a general trend to move away from conventional voice (VHF) and independent technologies (primary and secondary radar) towards automated and dependent technologies. For example, the Single European Sky ATM Research (SESAR) and Next Generation Air Transportation System (NextGen) programs have mandated the use of ADS-B and GPS by 2020 for commercial aircraft in the European and US airspaces respectively. These two technologies do not provide any kind of signal authenticity or confidentiality. armasuisse has, for example, demonstrated that ADS-B signals could be spoofed with little effort from the ground, to create confusion by injecting ghost aircraft in the recognized air picture (Schäfer, Lenders, & Martinovic, 2013). It is also well-known that GPS signals are vulnerable to spoofing attacks in which small portable spoofing devices can simply simulate the satellite signals from the ground to deceive aircraft or UAVs with wrong positions (Kerns, Shepard, Bhatti, & Humphreys, 2014).

More critical ATM technologies such as those being used for collision avoidance (e.g., TCAS) suffer from the same problems. Since the underlying data link used to sense and avoid collisions is based on unprotected plain-text messages sent over the wireless channel, man-in-the-middle attacks are thus impossible

| | |
|---|---|
| **Air Traffic Control** | |
| VHF | Voice (Very High Frequency) |
| PSR | Primary Surveillance Radar |
| SSR | Secondary Surveillance Radar (Mode A/C/S) |
| ADS-B | Automatic Dependent Surveillance-Broadcast |
| CPDLC | Controller–Pilot Data Link Communications |
| MLAT | Multilateration |
| **Information Services** | |
| ACARS | Aircraft Communications Addressing and Reporting System |
| TCAS | Traffic Alert and Collision Avoidance System |
| FIS-B | Flight Information System-Broadcast |
| TIS-B | Traffic Information System-Broadcast |
| **Navigational Aids** | |
| GPS | Global Positioning System |
| VOR | VHF Omnidirectional Radio Range |
| ILS | Instrument Landing System |
| NDB | Non-directional Beacon |

*Table 1: Wireless aviation technologies used for traffic management.*

to prevent. Even independent localization techniques such as multilateration (MLAT) are susceptible to attacks when they rely on unprotected signals. In previous research, we have demonstrated the feasibility to inject fictitious tracks in a wide-area multilateration system that cannot be discerned from real ones (Moser, et al. 2016). Other attack vectors relate to the feasibility of hacking the system avionics via the entertainment network of an aircraft or through spoofed aircraft communications addressing and reporting system (ACARS) messages which are then processed by the aircraft's board computers in an automated way (Hugo, 2013).

## A Changing Threat Landscape

While many of these vulnerable ATM technologies have been in use for longer times, the risks associated to their usage have increased substantially over the past few years because of recent technology improvements (Strohmeier, Smith, Schäfer, Lenders, & Martinovic, 2016). The technological advances in wireless technology happening in the late 1990s and 2000s drastically changed the offensive capabilities of adversaries in wireless communication settings. One of the main drivers of this development has been software-defined radio (SDR) technology. SDRs were first developed for military and closed commercial use in the 1990s, followed by open-source projects such as GNU Radio or RTL-SDR. In conjunction with the availability of cheap commercial off-the-shelf SDR hardware, new technological capabilities became available to a large group of people. Anyone with a relatively basic technological understanding can now receive, process, craft, and transmit arbitrary radio signals such as those used in aviation systems. Where previously radio hardware needed to be purpose-built, an expensive and complicated endeavor feasible only for specialists, SDRs can be programmed and seamlessly adapted using software easily available on the Internet.

## Safety is not Security

Aviation stakeholder awareness about those new cyber security risks is increasing, yet the prevalent attitude in the aviation community is still "Why is security needed? Is air traffic communication not safe currently?" A recent survey with more than 200 pilots and air traffic controllers highlights that the aviation community has still not developed a strong sense of security and still focuses mainly on safety (Strohmeier, Schäfer, Pinheiro, et al. 2017). Arguably, the aviation community is used to cope with system failures and technology malfunctioning and has a sound and steadily improving safety record. Indeed, historically, few incidents have been recorded where technologies were to cause distress to aircraft.

Security, however, is not safety, and requires a different mindset. While system failures and malfunctioning can be addressed with redundancy, security cannot. In non-adversarial settings, it is very unlikely that two independent system components will fail simultaneously. Redundancy is therefore a valid concept to achieve high system reliance. In adversarial environments however, the situation is different. Nothing prevents an attacker to attack different independent technologies at once. Redundancy is therefore not an adequate response to cyber risks.

## The Need for Higher Security

The changing threat model in combination with the increasing use of digital technologies for automation calls for aviation security approaches that go far beyond today's safety concepts. Ideally, new communication and navigation technologies with built-in security should be developed and used. Major aviation organizations such as ICAO, IATA, AIAA, Eurocontrol or FAA have started establishing cyber security working groups and action plans but the challenge lies in the decade-long development, certification and deployment cycles in aviation (Strohmeier, Smith et al. 2016). As technologies with built-in security require changes to the current aircraft/ground station equipage, they are unable to meet the security requirements in the short and medium term.

In our opinion, the immediate focus should therefore be on cyber security solutions that do not require changes to the aircraft/ground equipage. Intrusion detection systems (IDS) such as those employed to protect computer networks are needed. A new approach under investigation at armasuisse suggests relying on crowdsourcing for this purpose (Strohmeier, Smith and al. 2017). Crowdsourcing is a sourcing model which relies on contributions from Internet users to obtain needed services or information. Crowdsourcing has become a very popular concept in various application domains but it has also shown to be highly useful in cyber security contexts. For example, software bug bounty programs or crowdsourced threat intelligence collection are extensively used today to improve the security of the Internet. The idea in the aviation context would be to leverage open community networks such as the OpenSky Network (https://opensky-network.org) to detect cyber attacks on the air traffic communications. The OpenSky Network maintains a crowdsourced sensor network of Mode S and ADS-B receivers which report all broadcasted aircraft messages to a backend over the Internet. The global coverage with more than 700 sensors is depicted in Figure 2 (as of July 2017). While new sensors are being added by volunteers, the coverage is quickly increasing.

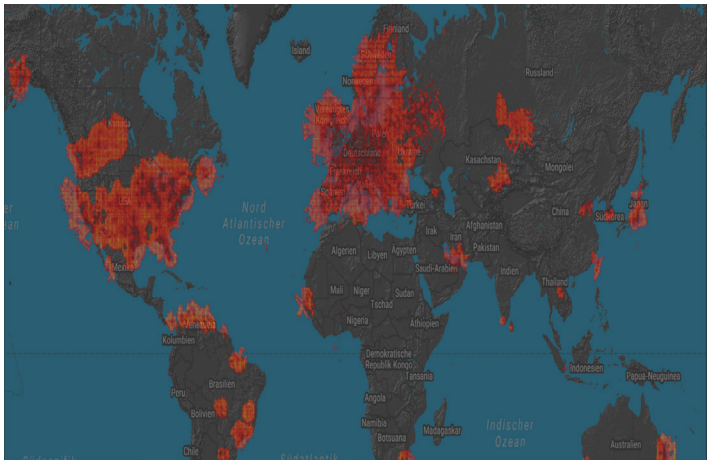



*Figure 2: OpenSky's reception coverage (July 2017) based on crowdsourced ADS-B and Mode S sensors.*

By analyzing the large amount of fused messages in the backend, it is possible to quickly detect cyber attacks that target the wireless communications in ATM. Possible detection methods range from simple plausibility or cross-sensor checks based on the content of the received data, to more complex statistical and cyber-physical analysis (Strohmeier, Smith et al. 2017). In (Schäfer, Strohmeier et al. 2014) and (Schäfer, Lenders & Schmitt, 2015) for example, we evaluated methods for secure track verification based on the time-of-arrival of aircraft messages. The Doppler effect is another signal characteristic that is useful for verifying the position and speed claims of aircraft (Schäfer, Leu et al. 2016). Since these intrusion detection methods are all passive, they provide the basis for an independent verification and alarming system on top of insecure ATM technologies.

## Conclusion

Fortunately, the aviation domain has not been exposed to serious cyber attacks so far. The media occasionally reports on incidents that could have been caused by potential impact of insecure technologies (Williams, 2014). However, except for hoax callers impersonating the voice of pilots or ATC (Johnston & Carmod, 2016), these incidents could so far not be attributed to real intentional attacks, being rather cases of technology malfunctioning and human errors (Moran & De Vynck, 2015). Given the recent developments in cyber technologies, the aviation community lost however a considerable technical advantage protecting its insecure communication from

potential attackers in the past. Until more secure technologies are deployed for communication and navigation in aviation, we suggest deploying intrusion detection systems that continuously inspect wireless communications and look for potential attacks in real-time. In the long-term, it is clear that the aviation community will have to move towards technologies and concepts that provide security by design.

### Dr. Vincent Lenders

is with armasuisse Science and Technology. He works as a Research Director leading the Cyberspace and Information research program for the Swiss Federal Department of Defense. He received the M.Sc. and Ph.D degrees in electrical engineering from ETH Zurich. He was Post-Doctoral Research Faculty with Princeton University. He is co-founder and a board member of the OpenSky Network Association and has contributed to the development of various information security concepts for the C4ISTAR systems of the Swiss Air Force.

### Dr. Martin Strohmeier

is a post-doctoral researcher in the Department of Computer Science at the University of Oxford. Before coming to Oxford in 2012, he received his MSc degree from TU Kaiserslautern, Germany and joined Lancaster University's InfoLab21 and Deutsche Lufthansa AG as a visiting researcher. He has received several best paper awards from both the aviation and computer security community.

### Matthew Smith

is a PhD student at the University of Oxford, as part of the Department of Computer Science and Centre for Doctoral Training in Cyber Security. His work focuses on the security of avionic data link systems, such as ACARS. Before this, he received a MEng. degree in Computer Science from the University of Warwick.

### Matthias Schäfer

is a Ph.D. candidate in the Department of Computer Science at the University of Kaiserslautern, Germany, where he also received his M.Sc. degree in computer science in 2013. Between 2011 and 2013, he worked for armasuisse Science and Technology and visited the Department of Computer Science of the University of Oxford, UK, as a visiting researcher. Matthias is a co-founder and board member of the OpenSky Network Association and the managing director of SeRo Systems GmbH.

### Prof. Ivan Martinovic

is an Associate Professor at the Department of Computer Science, University of Oxford where he leads a System Security Lab. Ivan's work is on authentication and intrusion detection using physical-layer information, traffic analysis, and the analysis of trade-offs between security and system's performance. Ivan is a board member of the OpenSky Network Association.

## Literature


- Hugo, T. (2013). Aircraft Hacking. HITB Security Conference.
- Johnston, C., & and Carmod, B. (2016, November 7). Lone-wolf radio hoaxer hacks Melbourne air traffic control: AFP. Retrieved June 12, 2017, from The Age: http://www.theage.com.au/victoria/lonewolf-radio-hoaxer-hacks-melbourne-air-traffic-control-afp-20161107-gsk12o
- Kerns, A., Shepard, D., Bhatti, J., & Humphreys, T. (2014). Unmanned Aircraft Capture and Control Via GPS Spoofing. Wiley Journal of Field Robotics.
- Moran, N., & De Vynck, G. (2015, January). WestJet Hijack Signal Called False Alarm. Retrieved September 2016, from Bloomberg: http://goo.gl/gSy2oa
- Moser, D., Leu, P., Lenders, V., Ranganathan, A., Ricciato, F., & Capkun, S. (2016). Investigation of Multi-device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures. ACM Conference on Mobile Computing and Networking (Mobicom).
- Schäfer, M., Lenders, V., & Martinovic, I. (2013). Experimental Analysis of Attacks on Next Generation Air Traffic Communication. International Conference on Applied Cryptography and Network Security (ACNS).
- Schäfer, M., Lenders, V., & Schmitt, J. (2015). Secure Track Verification. IEEE Symposium on Security and Privacy (S&P).
- Schäfer, M., Leu, P., Lenders, V., & Schmitt, J. (2016). Secure Motion Verification using the Doppler Effect. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec).
- Schäfer, M., Strohmeier, M., Lenders, V., Martinovic, I. & Willhelm, M. (2014). Bringing Up OpenSky: A Large-scale ADS-B Sensor Network for Research. ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN).
- Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V. & Martinovic, I. (2017). On Perception and Reality in Wireless Air Traffic Communications Security. IEEE Transactions on Intelligent Transportation Systems.
- Strohmeier, M., Smith, M., Schäfer, M., Lenders, V. & Martinovic, I. (2016). Assessing the Impact of Aviation Security on Cyber Power. International Conference on Cyber Conflict (CyCon).
- Strohmeier, M., Smith, M., Schäfer, M., Lenders, V. & Martinovic, I. (2017). Crowdsourcing Security for Wireless Air Traffic Communications. International Conference on Cyber Conflict (CyCon).
- Williams, A. (2014, June). Jets Vanishing From Europe Radar Linked to War Games. Retrieved September 2016, from Reuters: http://goo.gl/qKUrRp

# Explainable Artificial Intelligence

**The success of artificial intelligence (AI) approaches during the last years is impressive. Above all, deep learning techniques excel with high performance, exceeding the accuracy in predictions of human experts. However, accuracy is only one aspect of this performance. Due to the complexity of data and algorithms the explainability of these models suffers and yields the question about trust in these high quality results. Explainability of AI models becomes really important if essential decisions depend on their outcomes. Here we describe the emerging awareness of explainability in artificial intelligence approaches and its first countermeasures.**

**Keywords:** **Artificial intelligence, explainability, artificial neural network, machine learning, deep learning, causality, trust**

**Author:** **Dr. Albert Blarer**, armasuisse S+T

## Introduction

After many false dawns, artificial intelligence (AI) has made extraordinary progress in recent years, thanks to a versatile technique called deep learning. The current success story of deep learning is based on an old idea, with a modern twist: artificial neural networks (ANNs). They build the core of deep learning systems. ANNs have evolved and matured in several successful directions since their introduction around the middle of the last century. Two recent developments provided additional impulses for the success of deep learning systems: First, the emergence of big data technologies which offer appropriate methods to handle huge data volumes and to train deep learning models in a extensive manner. Second, the evolution of hardware which has multiplied computation power many times. Given enough data, deep neural networks can be trained to do all kind of complex tasks in extremely performant ways.

## Two showcases

The following examples may emphasize the impressive achievements of deep learning systems: Last year a group of medical researchers from the Netherlands organized a challenge called Camelyon16 (2016). One aim of the challenge was to detect cancer metastases in stained whole-slide images of lymph node sections. This classification task in digital pathology received a total of 32 submissions from 23 different teams. The leading submission, a convolutional neural network (CNN) of the type shown in Figure 1, achieved a significantly better accuracy (AUC of 0.9935 ; AUC stands for area under curve , see https://en.wikipedia.org/wiki/Receiver_operating_characteristic) in the results than the human pathologist benchmark (AUC of 0.96). Here, deep learning based algorithms outperformed the human experts in a defined recognition task if they are given a sufficient amount of correctly labeled training data.

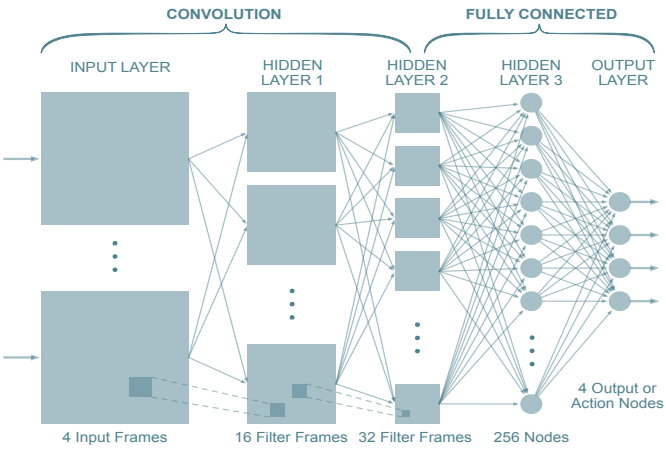



*Figure 1: A deep convolutional neural network (CNN), typically used in image classification.*

Another deep learning challenge, known as AlphaGo by Google's DeepMind, defeated last year, a human professional player in the game of Go by 5 games to 0 and achieved a winning rate of a 99.8% against existing Go programs (Silver et al., 2016). The classic game of Go has long been viewed as the most challenging game for artificial intelligence owing to its enormous search space and the tricky rules for moving the stones and evaluating the playing field (The rules of Go can be found here: https://en.wikipedia.org/wiki/Rules_of_Go). End of May 2017 AlphaGo hit the headlines again, defeating Ke Jie - the world's number one Go player - in all three games played in Wuzhen, China (DeepMind, 2017).

## The missing link

In view of such impressive outcomes, it is not surprising that the accuracy of deep learning outcomes receive particular attention. However, there is one important, but hidden aspect when evaluating deep learning results: explainability. We do not know how and why these impressive results come about.

Deep learning systems which are based on artificial neural networks represent black boxes. In supervised learning approaches, the deep learning models are trained with input data, such as the images of stained lymph node sections, which are labeled first manually by experts with healthy and non-healthy states. During the training phase, the model 'learns' to discriminate features for the classification task. However, the discrimination features which would help to explain the classification rules, are usually not part of the output. Figure 1 shows the simplified schema of a deep convolutional neural network now being the architecture of choice for large-scale image recognitions. The features to discriminate the two classes (healthy and non-healthy in our example) are prepared in the hidden layers between the input and the output layer. Looking at the model in Figure 1 it becomes obvious that tracing the features, captured inside a deep model, becomes a difficult task.

The same black-box behaviour occurs in unsupervised learning scenarios and in the third major scenario, the reinforcement learning, which sits somewhere in between supervised and unsupervised learning techniques. Reinforcement learning involves a training where the neural network interacts with an environment with only occasional feedback in the form of a reward. In essence, the training involves adjusting the network's weights to search for a strategy that consistently generates higher rewards. AlphaGo from Google's DeepMind is a specialist in this area of reinforcement learning. Again, the features that shape the deep learning model outcome in the end are not disclosed and therefore do not explain the model-chosen strategies.

It should be noted that the lack of explainability does not apply to machine learning approaches in general. Figure 2 suggests a trade-off between results of high quality versus the explainability of the results for different machine learning models. Modern and notably more complex algorithms as used for instance in deep learning, seem to supply more accurate results at the expense of their explainability. Models at the other end of the scale offer more transparency in their modes of action, but yield less precise results. For instance, decision tree models (at the lower right in Figure 2) offer a human readable

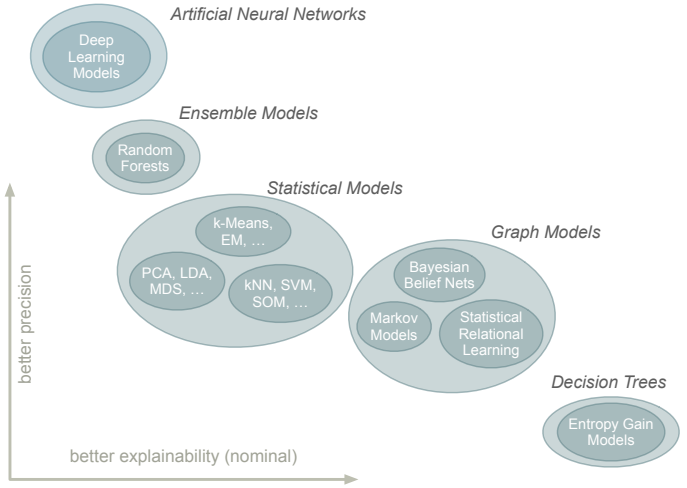



*Figure 2: Tradeoff between predictive precision and explainability shown for selected machine learning models.*

tree structure reflecting the importance of every feature in the learning process. However, decision trees usually won't achieve the precision levels of deep learning models.

## Explainability explained

What is the significance of explainability? Why is it important at all? For some learning tasks explainability is probably not much more than a question of interest. Explaining a winning strategy in AlphaGo is certainly interesting. However, when using machine learning for tasks where the consequences of a faulty result has strong legal or ethical consequences, explainability becomes crucial. Medical diagnosis, suspicious facts in terrorism detection, the motion control of a selfdriving car or the autonomous decision to launch a drone attack, cannot be acted upon on blind faith, as the consequences may be catastrophic. The major role of explainability lies in providing confidence-building measures for such learning tasks. Explainability is key for any predictive or causal analysis about the consequences of machine learning outcomes.

There is rising awareness about the significance of explainability in deep learning. DARPA recently initiated a four-year project to investigate explainability (Gunning, 2016)). Figure 3 shows an adapted schema of DARPA's view on explainability.

The basic idea is to extend machine learning models by an additional explanatory model. If features extracted from the machine learning process can be associated in some way with the learned functions of the machine learning model, then these associations might be used as an explanatory interface for human interpreters.

The association between the features and learned functions, marked with an asterisk in Figure 3, is key to this explainability approach. We next may ask about the nature of this association that helps to understand the machine learning outcomes.

At present, explainability has no formal technical meaning. However, there is large consensus that explainability should expand the confidence in the learning models and their results. The confidence question starts with selecting and preparing the initial steps of a machine learning model, for instance, the setup of training data in a supervised machine learning scenario. Often machine-learning algorithms make the common assumption that the data used to train the algorithm and the data to which the algorithm is later applied are generated in the same way (or what statisticians call sampled from the same distribution). When that assumption is violated, the algorithm can be fooled; but we need to trust the machine learning models and the data. Confidence further applies to individual predictions. Both levels of confidence are directly impacted by how much the human understands a model's behaviour, as opposed to seeing it as a black box. For this purpose the associations between the features and the learned functions need to be informative and interpretable to human users (see Ribeiro, Singh, and Guestrin (2016) and Lipton (2016) for a details).

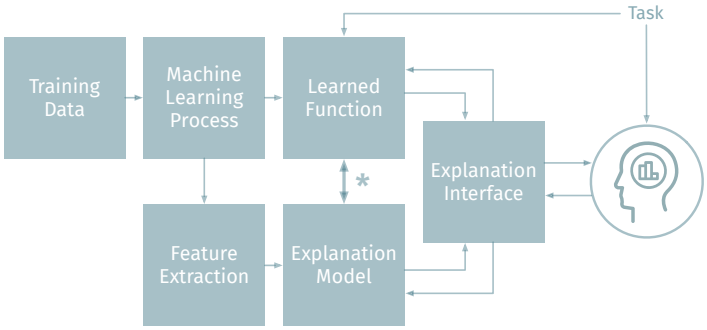



*Figure 3: Machine learning models extended by an explanation model and interface. Adapted from (Gunning, 2016).*

## Ultimate explainability includes causality

The optimization objective for many learning models is simply to minimize error, a feat that might be achieved in a purely correlative fashion. If the association between features and learned functions results purely correlative, that's a first step. However, the ultimate explainability arises from a causal inference. Explanation and causation are intimately related. Explanations often appeal to causes, and causal claims are often answers to implicit or explicit questions about why or how something occurred.

One of the most commonly repeated maxims in science is that correlation is not causation. Beyond that it is also generally known that the inference of causality is one of the most complex analytic tasks (see for example Pearl, 2009). But in the last few years, statisticians have begun to explore a number of ways to solve the causal inference problem. A very interesting approach has recently been published by Joris Mooij at the University of Amsterdam and his coworkers (Mooij et al., 2016).

They propose a new approach to separate cause and effect in observational data. The authors confine themselves to the simple case of data associated with two variables, $x$ and $y$ which are clearly correlated. But which is the cause and which the effect? The basis of the new approach is to assume that the relationship between $x$ and $y$ is not symmetrical. In particular, they say that in any set of measurements there will always be noise from various causes. The key assumption is that the pattern of noise in the cause will be different to the pattern of noise in the effect. That's because any noise in $x$ can have an influence on $y$ but not vice versa. So the set of data should reflect this asymmetry, and the task is to develop a statistical test that can tell the difference. Such a test already exists and is known as the additional noise model (ANM). ANM assumes that each dataset is made up of the relevant data as well as various sources of noise. The nonlinearity of this process can allow to determine the direction of cause and effect. Mooij et al. (2016) have tested how well ANM works on 88 datasets of cause-and-effect pairs that have been compiled for just this purpose from

different areas of science. Each dataset consists of samples of a pair of statistically dependent random variables where one variable is known to cause the other. The challenge is to identify which of the variables is the cause and which the effect.

The results of Mooij et al. (2016) look promising. The additive noise model is up to 80% accurate in correctly determining cause and effect. The method seems moreover robust against small perturbations of the data. That's a fascinating outcome, since it seems not impossible to determine cause and effect from observational data alone. The idea now would be to apply this model to our explainability model to infer causes and effects. If we could test observed features (corresponding to variable $x$) being the causes of learned function values (corresponding to variable $y$), i.e. the effect, then a causal association could be established. The explainability of machine learning models would step forward clearly.

It's worth pointing out that the model of Mooij et al. (2016) applies only in the very simple situation in which one variable causes the other. Of course there are plenty of much more complex scenarios where the current method will not be so fruitful. However, with an extended model that handles more complex causal scenarios, the additive noise model could be a game changer.

## Explainability as a teacher

To finish up with the discussion about explainability, a last aspect might be of interest. Let us return to the first example of the introduction. Deep learning models defeated human experts in cancer metastasis detection by a small but significant amount of accuracy. Suppose that we had a perfect explainability model at hand that would show us all additional patterns in the stained images that are classified correctly by the machine to healthy or not-healthy states.

If these patterns become manifest, explainability could help human experts to increase their cancer prediction skills. The explainability model would teach human experts to become even better experts. This idea could further increase the significance of explainability in artificial intelligence.


**Dr. Albert Blarer**

is scientific project manager at armasuisse Science and Technology. He currently is involved in different Deep Learning projects and focuses on the technical and scientific expertise of machine learning systems which might have implications for the Swiss armed forces and related organisations.

Albert Blarer can be reached at albert.blarer@armasuisse.ch.


## References


- Camelyon16 (2016). ISBI challenge on cancer metastasis detection in lymph node. url: https://camelyon16.grand-challenge.org/.
- DeepMind (2017). AlphaGo at The Future of Go Summit, 23-27 May 2017. url: https://deepmind.com/research/alphago/alphago-china/.
- Gunning, David (2016). Explainable Artificial Intelligence (XAI). url: https : / / www.darpa .mil / program / explainable - artificial -intelligence.
- Lipton, Zachary Chase (2016). "The Mythos of Model Interpretability". In: CoRR abs/1606.03490. url: http://arxiv.org/abs/1606.03490.
- Mooij, Joris M. et al. (2016). "Distinguishing Cause from Effect Using Observational Data: Methods and Benchmarks". In: J. Mach. Learn. Res. 17.1, pp. 1103– 1204. issn: 1532-4435.
- Pearl, Judea (2009). Causality: Models, Reasoning and Inference. 2nd. New York, NY, USA: Cambridge University Press.
- Ribeiro, Marco Tulio, Sameer Singh, and Carlos Guestrin (2016). "„Why Should I Trust You?": Explaining the Predictions of Any Classifier". In: Proceedings of the 22Nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. KDD '16. San Francisco, California, USA: ACM, pp. 1135–1144.
- Silver, David et al. (2016). "Mastering the Game of Go with Deep Neural Networks and Tree Search". In: Nature 529.7587, pp. 484–489.

# Visions of Warfare 2036: a futurist prototyping methodology to support military foresight

**Von Clausewitz wrote that the nature of war is constant but its character changes to suit contemporary conditions on the battlefield – doctrinal, technological and sociological. NATO's Supreme Allied Command Transformation harnessed a pioneering method for exploring the evolving character of future warfare through leveraging the power of science fiction storytelling to inform innovative and transformational thinking. This proof-of-concept developed an anthology of stories whose content was analysed for signposts to emerging changes in the future security environment. This project took on the challenge levied by Sergey Brin, one of the founders of Google, who said, "If what we are doing is not seen by some people as science fiction, it's probably not transformative enough."**

**Keywords:** **Foresight, conflict, future, warfare, science fiction**

**Author:** **Mark Tocher**, North Atlantic Treaty Organisation (NATO)

## Introduction

The military strategist Colin Gray wrote that one need only consult three great military thinkers to encapsulate all the strategy foundation that underlies war: Thucydides, Sun Tzu and Clausewitz [1]. These three writers wrote that the nature of war is constant. It is a contest of wills driven by fear, honour and interests where chance, the fog of war and friction play against intended end states. That said, conversely, the character of war is constantly changing as it reflects contemporary technology, doctrine, social norms, and legal and ethical constraints. It is on this character of war that military foresight is focused to determine how we should construct, train and develop forces to fight in the future.

Headquarters, Allied Command Transformation (ACT) recently conducted a proof-of-concept to evaluate the use of Futurist Prototypes as means to supplement other foresight activities to assess the future character of war. This activity sought to leverage the power of storytelling to lead readers into plausible futures and explore how evolving settings could come into play to bring about the introduction of new or novel use of technologies, different doctrines and shifting fundamental reasons for initiating military operations. The proof-of-concept sought to evaluate whether this type of methodology would improve longer-term thinking and reduce risk as ACT prepares to enter a new cycle of the NATO Defence Planning Process [2].

## The Power of Storytelling

For eons humans relied on stories to pass on from generation to generation and village to village, "key events, histories, beliefs and attitudes" [3]. This has hard-wired the human brain to register knowledge in the form of stories. Information that is delivered in storylines "reaches a listener's conscious mind and memory more accurately and vividly than if you put that same information into any other narrative form" [4].

*Stories create believability and engage and hold audiences.*

## Leveraging Science Fiction

Julian Bleeker points out in his seminal article on design and science fiction that, "science fiction can be understood as a kind of writing that, in its stories, creates prototypes of other worlds, other experiences, other contexts for life based on the creative insights of the author. [5]" Futurist Brian David Johnson goes further by highlighting that science fiction gives us a language in which to talk about the future [6]. While Tom Standage proposes that "to see what lies ahead for technology, it helps to look in three places: the past, the present and the imagined futures of science fiction." [7]. Science fiction "offers a way to imagine and envision the future in a whole new way." [8]. The Futurist Prototyping process sought to leverage the power of science fiction storytelling to assess the future character of war.

## The Futurist Prototyping Process

ACT engaged the services of SciFutures to facilitate the development of the proof-of-concept. SciFutures is an innovation company that specialises in leveraging science fiction to help companies understand and create the future. The company uses science fiction narratives to cast the future in a way that all members of an organisation can understand.

The foundation of the Futurist Prototyping process is set within the imaginations of professional science fiction authors and their narratives about the future. With ACT's collection of foresight documents [9] as a baseline, but unbounded by military strictures or the subliminal requirement to be "realistic", the authors developed an anthology of stories forming a prototype that described visions of plausible futures in 2036. The storylines were not meant to be an all-inclusive set of the plausible futures, but only as a sufficient set to make an analysis of some possible changes in the future character of war and the value of this process.

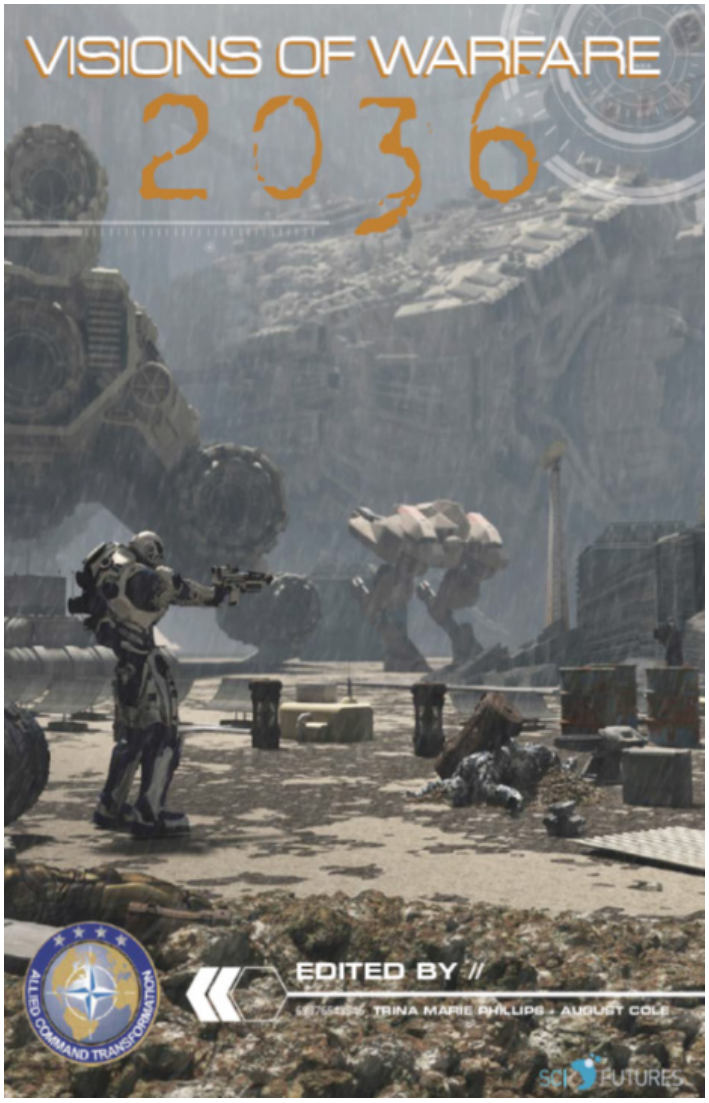
The prototype provided a basis for 'backcasting' [10] from the future to assess variations over time in how technology and other drivers could have changed how conflict is initiated, conducted and resolved. The stories provide signposts or indicators of the evolving character of conflict. The team at SciFutures identified five Themes [11] that linked together the storylines developed within the anthology:

**Blind Spots** - The global pace of change continues to increase. From culture to technology to the environment, it seems all systems are subject to massive, often violent shifts. The volatility of increasingly complex systems frequently creates unanticipated changes. Even actions with positive intent can result in unintended vulnerabilities. How can we predict and stay ahead of blind spots?

**No Borders** - Technology has changed the geometry of warfare. Global connectivity results in front lines that stretch and bend around the globe. The result is a transformed battlefield populated by combatants who can engage without the restrictions of time and space.

**Post-Truth World** - Many futurists predicted the Internet would bring about a great era of openness and transparency. While we may still reach that preferred future, technological and cultural forces have actually indicated a future in which shared "truths" are rare.

**Data=Life** - The era of "Big Data" has helped create general awareness of the potential value of data. However, we increasingly see data as a necessity, not a nice-to-have. As we become increasingly reliant on digital services, an ability to access and interpret the data will be critical. Data corruption or interruptions will not just be an inconvenience – data disturbances will be a matter of life and death.




**Human and Machine** - The relationship between people and machines continues to evolve. Rather than assuming complete human dominance or absolute machine superiority, the future increasingly seems to involve a balance of the two. What is the future relationship between organic systems and digital tools?

With this foundation in place, a workshop was held that brought together a wide array of defence and security specialists to assess the prototype. Represented at the workshop were the NATO International Staff, NATO Office of the Chief Scientist, ACT/Defence Planning, ACT/Strategy, Plans and Policy, the NATO Communications and Information Agency, The Hague Centre for Strategic Studies (HCSS), United States Marine Corps and SciFutures. Each of the attendees was provided with the anthology of stories and a set of discussion questions to ponder before the workshop.

At the start of the workshop, the attendees were briefed on the theory of science fiction prototyping and how the proof-of-concept would apply this theory in a military context. Through facilitated breakout discussions around the Themes and the provided discussion questions, the group sought to ascertain how the character of conflict would change based on the storylines found in the anthology.

## Findings

The proof-of-concept highlighted many issues that had been identified through other foresight methodologies. That the group identified nothing strikingly during the course of this short proof-of-concept does not invalid the methodology, it adds to our level of confidence on those issues, as they were raised using different methodologies. The workshop demonstrated the value of leveraging the anthology as a basis for discussing future conditions facing the Alliance. Below are several of the findings derived from the Futurist Prototype workshop:

- Geography will become even less relevant in the future. Cyberspace, hypervelocity weapons and externalities related to conflict will cross borders and bring about global disruptions. The entire globe will be a recruiting ground for organisations as the ability to search deeply through the internet becomes available and like-minded people can be reached and manipulated online. This becomes more likely as affiliations become stronger between people and commercial companies, diaspora, religion and other belief structures over nationality. Research will need to be done on how people with access to all available information still can be marginalized or radicalized.
- An agile and swift decision making process that can quickly assimilate and process new information and respond accordingly will be required to address future conflict. Speed will be an essential element to meet the challenge of cascading disruptions.
- Related to the above, NATO must be able to deal with 'Unknown Unknowns'. There is a strong need for more frequent instances of Red Teaming or unconventional explorations, such as the Futurist Prototype, to explore future possibilities in order the reduce the number of issues about which we have no information ergo increasing 'Known Unknowns'.
- As Eisenhower once said, "plans are nothing, planning is everything", an anticipatory mind set within the defence and operations planning communities would increase their ability to address emergent risks and opportunities. This process must include broader partnerships with both tradition and non-tradition groups. Increasing diversity within all planning groups will open avenues to broader thinking on emerging issues. This could include crowd sourcing.
- A flexible, adaptable and robust force pool and sets of capabilities that can be repackaged to address whatever threat arises in the future would reduce the risk of being unable to address unknown threats or take advantage of emerging opportunities. This capability package would serve as a hedge against unknowns.
- Systems must be more robust and resilient to sudden shocks. This process could retain and incorporate older, less technologically advanced systems for redundancy.
- There will be increasing difficulty in differentiating combatant from non-combatant. Rules of engagement will be extremely important to ensuring measured and appropriate application of force.
- The rise of decentralized and transparent networks using block chain technology will reduce the ability of both nations and others to manipulate networks, markets and currency.
- Information and disinformation will become more important, even existential, in the future. Mastering the media will be more important as it continues to be disaggregated. The truth will be balkanized as the same information is interpreted differently at the group and individual level. Echo chambers or bubbles on the Internet will curate their own truth.

- Artificial Intelligence (AI) will have an increasingly prominent role in the future. Competition between AIs will be common. Issues of affordability will highlight the difficulty in keeping AI up-to-date. Will we be able to trust AI systems that we cannot understand?
- The legal, moral and ethical considerations surrounding autonomous systems will need to be explored. Will humans remain in/on/out of the loop? How will we solve for possible emergent behaviour in complex machines? Would robotic warfare bring into question the enduring nature of warfare or just its changing character?
- The interoperability between high technology and lower technology member nations will become a growing concern. Would a commander order human troops to attack an objective if robotic resources were available? How does this affect 'fair burden sharing'? Do we have to follow both a high-technology approach as well as a parallel low-technology approach?

## Conclusion

This proof-of-concept set out to study how the power of science fiction storytelling could be leveraged to explore future conditions facing the Alliance. Will the character of war continue to evolve based on the exponential progress in technology forecast over the coming decades? Discussions based on the anthology of stories did lead to a number of interesting insights. The prototype was valuable as a trigger for free "out of the box" discussions.

Within the bounds of the design of the proof-of-concept, the Futurist Prototyping methodology proved to be useful in both expanding military thinking about the long term and adding diversity to the toolbox of methods used in long term capability derivation. This is especially fitting given the mandate of ACT to lead transformation within the Alliance and the challenge levied by Sergey Brin, one of the founders of Google, who said, "If what we are doing is not seen by some people as science fiction, it's probably not transformative enough. [12]".


**Mark Tocher**

is currently a Defence Planning Analyst at Supreme Allied Command Transformation (SACT) in Norfolk, Virginia. He specialises in the incorporation of foresight and future technology into the derivation of military requirements for the North Atlantic Treaty Organisation (NATO). In the past, he has worked in future policy and operations planning. He has post-graduate degrees from the University of Manitoba and the Florida Institute of Technology and is a graduate of the Canadian Forces Command and Staff College.


## References


[1] Colin S. Gray, Fighting Talk: Forty Maxims on War, Peace, and Strategy (Westport: Praeger Security International, 2007) 58.

[2] Through the NATO Defence Planning Process, NATO identifies capabilities and promotes their development and acquisition by Allies so it can meet its security and defence objectives. www.nato.int/cps/en/natohq/topics_49202.htm accessed 2 May 17.

[3] Kendall Haven, Story Smart: Using the Science of Story to Persuade, Influence, Inspire and Teach (Libraries Unlimited, 2014) 3.

[4] Kendall Haven, Story Smart: Using the Science of Story to Persuade, Influence, Inspire and Teach (Libraries Unlimited, 2014) 6.

[5] Julian Bleecker, "Design Fiction: A short essay on design, science, fact and fiction." drbfw5wfjlxon.cloudfront.net/writing/DesignFiction_WebEdition.pdf, 7

[6] Brian David Johnson, Science Fiction Prototyping: Designing the Future with Science Fiction (Morgan and Claypool, 2011) 11.

[7] Tom Standage, Megatech: Technology in 2050, edited by Daniel Franklin, (New York: The Economist, 2017) 11.

[8] Brian David Johnson, v.

[9] Allied Command Transformation has developed a collection of futures-related documents including the Strategic Foresight Analysis, the Framework for Future Alliance Operations, the Technology Trends Survey and the Long Term Aspects of requirements.

[10] Backcasting is a planning method that starts with defining a desirable future and then works backwards to identify policies and programs that will connect the future to the present. en.wikipedia.org/wiki/Backcasting, accessed 27 Apr 17.

[11] These Themes were described in a Discussion Guide for Visions of Warfare 2036 prepared by SciFutures that included discussion questions that were used to guide smaller group discourse and highlight relevant insights from the material.

[12] nbcnews.com/technology/googles-sergey-brin-explains-why-he-paid-330-000-lab-6c10853442, 5 Aug 13.

# La quatrième révolution industrielle et son impact sur les forces armées

**Les évolutions technologiques en cours constituent globalement une révolution dans la mesure où elles ouvrent des perspectives entièrement nouvelles. Elles vont avoir des répercussions sur le comportement des individus, des collectivités publiques, des organisations les plus diverses et des entreprises et ainsi avoir un impact croissant sur la sécurité des sociétés et des individus.**

**Mots-clés:** **4ème révolution industrielle, dual-use, robotique, intelligence artificielle**

**Auteur:** **Marc-André Ryter**, Armée Suisse

## De quoi s'agit-il?

Si l'on combine les opportunités naissantes avec les nouvelles vulnérabilités qu'elles vont créer, on peut prévoir que l'évolution technologique en cours va influencer les relations entre les États dans le domaine de la sécurité, dans un sens positif et négatif.

Le but de cet article est de sensibiliser aux conséquences de cette évolution et de mettre en évidence l'impact des nouvelles technologies sur la sécurité et de montrer à quel point elles sont pertinentes pour le développement des forces armées. Dans un futur prévisible, la plupart des innovations technologiques en cours seront intégrées dans le domaine de la défense, ceci indépendamment de la menace. Il est certain que des investissements importants seront nécessaires et donc qu'il y aura aussi des conséquences non-négligeables sur les budgets militaires.

La quatrième révolution industrielle consiste à intégrer les technologies digitales à toutes les fonctions constitutives de la vie et à intensifier le travail entre les humains et les machines par la délégation croissante aux machines de certaines qualités sensorielles, de mobilité et d'intelligence, ainsi que de certaines compétences décisionnelles. L'efficacité et l'efficience des systèmes de même que la coordination entre les systèmes et la gestion des actions peuvent être améliorées.

L'attrait de la quatrième révolution industrielle provient de l'immense potentiel d'amélioration présumé. Il sera donc très difficile de freiner, voire de contrôler les développements dans ce domaine, malgré des risques qui ne sont pas encore complètement évalués et qu'il ne faut pas sous-estimer. Il est cependant préoccupant de constater que la question de la sécurité est insuffisamment intégrée à cette évolution.

Les technologies et leurs applications font l'objet de nombreuses publications et ne seront donc plus traitées en tant que telles dans cet article. Il faut cependant insister sur le fait qu'il est important de suivre l'évolution de ces technologies et de leurs applications potentielles, en particulier celles à double usage (dual-use), afin d'en déduire lesquelles sont susceptibles d'être utilisées par un adversaire et partant lesquelles devront au minimum être prises en compte pour le développement de l'armée suisse.

## Impact sur la sécurité

Les progrès technologiques impliquent une gamme très large de vulnérabilités et donc de perturbations et manipulations possibles. A ceci s'ajoute le fait que le risque d'erreurs humaines, en raison de la complexité toujours croissante, est plus élevé. La gestion de ces nouveaux risques nécessite des ressources et des compétences souvent nouvelles qui impliquent une élévation massive des interdépendances. Pour les forces armées, cela implique une interdépendance croissante entre les composantes, mais aussi et surtout envers l'extérieur.

On se dirige vers une hyperconnectivité [1] qui va encore accroître les inégalités dans le monde, et donc le fractionner encore plus. Cette hyperconnectivité donne plus d'options pour des actions criminelles, des actes de terrorisme ou de chantage, y compris à des acteurs possédant de faibles ressources et profite en particulier aux acteurs non-étatiques.

De nombreux risques faisant partie intégrante de l'évolution technologique peuvent remettre en cause le fonctionnement des sociétés et constituent donc des menaces existentielles. Leur potentiel destructeur est très élevé et génère un sentiment de vulnérabilité par rapport à cette évolution. Par ailleurs, les risques liés au stockage de données, respectivement à ce qui se passe avec les données accumulées, soulèvent de nombreuses craintes.

Un défi important consiste dans le triage et la vérification des informations. Déjà aujourd'hui, de fausses informations peuvent


***Figure 1:*** Possibilité d'améliorer les capacités du soldat. http://www.cnbc.com/2014/05/14/the-future-soldier-will-be-part-human-part-machine.html, consulté 12.07.2017

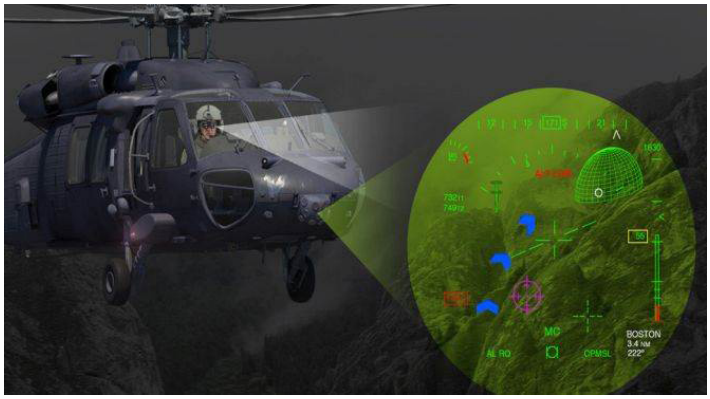


*Figure 2: Combinaison entre appareils de vision et analyse du champ de bataille, http://www.indiandefensenews.in/2015/06/elbit-systems-introduces-supervision.html, consulté 12.07.2017*

être créées intentionnellement et très rapidement distribuées à large échelle, poussant à des comportements irrationnels. Il devient de plus en plus facile de manipuler les foules et de créer des groupes de protestataires persuadés de leur bonne foi.

Le risque s'accroît de voir la sécurité de l'individu remise en question par le déni d'accès à des services essentiels comme la distribution d'eau, d'électricité ou d'hydrocarbures. La perturbation des communications, de l'approvisionnement en denrées alimentaires, du réseau de santé ou du trafic aérien, routier ou ferroviaire peut rapidement mettre en danger le fonctionnement des sociétés.

En résumé, les sociétés devront intégrer et maîtriser les risques issus des évolutions technologiques afin de garantir leur sécurité et en particulier la paix sociale. Il est difficile de prévoir les conséquences d'une automatisation à outrance et de la suppression des postes de travail pour les humains qui peut en découler.

## Impact sur la défense et les forces armées

Les évolutions en cours nécessiteront une adaptation constante des forces armées qui devront les intégrer. Le secteur de la défense devra de plus en plus s'adapter aux innovations venues de l'industrie civile qui ne constitueront pas simplement une évolution des technologies utilisées actuellement. Il s'agira d'aller au-delà du C4ISTAR, principalement en raison du développement de la dimension informationnelle et d'une automatisation plus poussée.

La supériorité dans le domaine de l'information qui pourrait être acquise grâce aux nouvelles technologies doit permettre d'assurer certains avantages sur le terrain, comme la capacité à surprendre l'adversaire, la disponibilité et l'adéquation des moyens, la rapidité de l'action ou la flexibilité de la réaction. La capacité à effectuer le bon choix et à concentrer les moyens au moment et à l'emplacement corrects demeureront des facteurs opérationnels décisifs. Les indications concernant les besoins de maintenance des systèmes permettront d'améliorer de manière substantielle leur disponibilité.

La capacité à choisir et décider mieux et plus vite que l'adversaire, en restant protégés de fausses informations et de manipulations de systèmes, est donc centrale. En plus, des systèmes permettant l'évaluation permanente de la situation seront aussi connectés afin d'améliorer la conduite. Cependant, même si les réactions sont plus rapides et plus précises, l'automatisation de la décision dans le domaine militaire et le fait que des machines puissent être programmées pour combattre de manière autonome restent des sujets sensibles, principalement en raison des dimensions éthiques.

D'un point de vue militaire, l'analyse de plus d'informations dans des délais plus rapides va créer un avantage en permettant d'ajuster en permanence les actions tactiques et la conduite interforces. Il y aura ainsi une amélioration sensible de la compréhension du champ de bataille (battlespace awareness) qui s'appuiera sur une meilleure transparence, malgré les contre-mesures qui seront immanquablement développées. Le soutien et la coordination interarmes seront eux-aussi améliorés, les munitions deviendront plus intelligentes, avec moins de dommages collatéraux. Ceci sera particulièrement avantageux en milieu urbain et lors de l'utilisation d'une stratégie hybride, où les civils seront toujours mélangés aux combattants et où ces derniers sont parfois difficiles à identifier. Les nouvelles technologies ne s'appliqueront pas seulement aux machines, mais aussi aux combattants. Ceux-ci pourraient voir leurs capacités au combat améliorées par des mesures techniques et chimiques. La „biosphère", soit ce qui se passe à l'intérieur des corps des combattants, va de plus en plus devenir un espace à considérer dans le contexte militaire.

Mais il y aura aussi des conséquences négatives comme les possibilités d'influencer et de perturber la conduite militaire de l'adversaire. L'adversaire aura la possibilité d'accéder aux informations-clés et de les modifier afin de créer une fausse image de la situation. Une protection suffisante des systèmes par des technologies de vérification (cross-check) basées sur l'intelligence artificielle constituera donc une absolue nécessité. La question qui se pose est de savoir si toutes les informations disponibles pourront être analysées avec la pertinence et dans les délais nécessaires.

L'engagement de robots dans les forces armées devrait avant tout libérer les soldats des tâches dangereuses, sales et répétitives [2], et dans des domaines où le besoin de conduite est limité voire absent. L'avantage est qu'il sera possible de déclencher certaines actions en donnant la mission aux robots ou drones et qu'ensuite, ces machines pourront agir de manière autonome et sans nécessiter de conduite. Mais les robots ont des limites lorsqu'il s'agit de réagir face aux changements, ce qui est particulièrement limitatif en phase de combat. C'est pourquoi, les robots offrent de très bonnes perspectives avant tout dans les domaines de la logistique.

Il y a donc deux domaines bien différents qui sont concernés par l'introduction de nouvelles technologies dans les forces armées: d'un côté l'amélioration des prestations de bases avec l'établissement de la disponibilité de base et de l'autre l'amélioration des processus de conduite ainsi que des performances des soldats et des armements.

## Impact sur la doctrine et le champ de bataille

L'évolution technologique va avoir un impact sur la nature des conflits et engendrer une métamorphose du champ de bataille. Il est cependant encore difficile de prédire exactement comment et jusqu'à quel point les nouvelles technologies vont changer la manière avec laquelle les pays vont conduire leurs opérations et quel sera leur impact sur les guerres. Il est possible de penser qu'il va être toujours plus difficile de clairement faire une distinction entre l'état de paix et l'état de guerre. De même, la distinction entre combattants et non-combattants

*Figure 3: Coexistence de l'homme et du robot sur le champ de bataille, http://www.thelondondailynews.com/terminators-battlefield-pose-threat-human-beings/, consulté 12.07.2017*

sera un défi majeur des conflits futurs [3]. Ces derniers seront toujours plus une combinaison d'actions à l'échelon local et à l'échelon global. Ils seront caractérisés par un mélange d'actions militaires, terroristes et/ou couvertes à une très petite échelle avec des campagnes de forces militaires étatiques classiques de grande envergure, le tout soutenu par de la propagande locale et globale. Les médias sociaux joueront un rôle de plus en plus grand, que ce soit dans le domaine de la propagande et de la désinformation ou du recrutement. Le potentiel exact des nouvelles technologies ne prête pas à beaucoup d'optimisme car les nouvelles armes au sens large seront plus faciles à acquérir et elles pourront plus facilement causer des dommages à large échelle.

A l'échelon des formations, l'évolution dans le domaine de la conduite pourrait remettre en cause la Auftragstaktik et favoriser une conduite plus rigide dans le sens de la Befehlstaktik. Il apparaît évident que le soldat devra garder une faculté d'analyse et de décision propre. Les qualités d'analyse des individus à tous les échelons resteront essentielles dans l'optique de garantir la résilience d'un système qui sera ainsi capable de mieux s'adapter à l'évolution du combat. La question de la confiance que pourront placer les chefs militaires et les soldats dans les systèmes sensés les aider sera centrale. Ainsi, il sera nécessaire d'engager les nouvelles technologies pour appuyer les militaires plutôt que pour les remplacer [4]. La question se posera de savoir jusqu'à quel point l'on pourra laisser des robots ou d'autres armes à intelligence artificielle mener le combat de manière autonome, c'est-à-dire sans que les actions ne soient dirigées par l'être humain.

L'un des défis majeurs posé par cette évolution pour les doctrines des forces armées sera de pouvoir évoluer rapidement, respectivement de pouvoir s'adapter aux nouvelles percées technologiques. Il faudra donc redéfinir ce que doit contenir une doctrine, comment elle peut évoluer et surtout identifier les évolutions significatives. La conséquence sera un décalage sans doute croissant entre les possibilités technologiques existantes et les systèmes en usage dans les forces armées.

Les principaux risques pour les forces armées sont les suivants:

- Erreurs dues à l'augmentation du nombre d'interactions tout au long de la chaîne de commandement;
- Ingérence des échelons supérieurs dans les décisions et dans la conduite de l'échelon tactique en raison de la nécessité de réagir rapidement;
- Mauvaise appréciation et décision en raison d'attentes toujours plus élevées de la part des décideurs;
- Problèmes liés aux volumes importants de données à transmettre;
- Incapacité à identifier les bonnes informations;
- Chaos que peuvent générer les nombreux intervenants dans la gestion d'un très grand volume d'informations.

*Figure 4: Appui des soldats par un robot sur le champ de bataille, http://i-hls.com/archives/77453, consulté 12.07.2017*

## Conclusions et conséquences

L'introduction des nouvelles technologies implique donc à la fois des opportunités et des risques pour les forces armées. Les limites seront constituées d'abord par le volume des données échangées et à analyser („infobésité" [5]). Ensuite, la maintenance de ces systèmes fragiles sera plus complexe qu'on ne l'estime à l'heure actuelle. Mais surtout, les coûts des systèmes eux-mêmes et de leur protection constitueront sans doute la limite la plus importante. Peu de pays seront à même de financer des forces armées disposant de tous ces nouveaux systèmes [6]. De nombreux pays n'auront pas les ressources nécessaires pour suivre le tempo des évolutions technologiques et introduire constamment de nouveaux systèmes complexes dans leurs forces armées. La dépendance envers la recherche et l'appui du secteur privé va s'accroître plutôt que diminuer.

L'intervention et le travail humains vont cependant garder toute leur importance, y compris dans le domaine de la collecte des données, de leur interprétation et de leur introduction dans les systèmes [7]. Tout ne pourra être automatisé. Il va s'agir de définir des espaces spécifiques dans lesquels les machines peuvent agir de manière autonome, et d'autres ou l'intervention de l'être humain demeure indispensable. La dimension humaine demeurera donc un enjeu essentiel, aussi pour la Suisse. Il faudra de plus en plus de spécialistes pour engager et entretenir les machines et pour interpréter les données. Dans le cas d'une armée de milice comme l'armée suisse, la question se pose de savoir si l'on pourra trouver le nombre nécessaire de spécialistes civils astreints au service militaire. Au final, la question de l'importance de l'intuition dans le processus de décision se posera. Celle-ci ne pourra pas être remplacée par des processus techniques, même si l'intelligence artificielle aura la capacité d'intégrer les expériences passées.

Ainsi, la capacité de la défense à suivre et intégrer le développement des nouvelles technologies sera la clé de la sécurité dans le futur. Ce développement, comme avec les anciens systèmes d'armes moins sophistiqués se déroulera sur deux axes opposés: d'un côté, les nouvelles technologies seront utilisées pour améliorer l'efficacité et de l'autre, pour améliorer la protection.

Il ne faut pas oublier que les évolutions technologiques profiteront aussi aux acteurs non-étatiques, principalement en raison de la miniaturisation et de la baisse des coûts de certains systèmes de base qui sont prévisibles. Cela ouvrira de nouvelles perspectives pour ces acteurs, et donc nécessitera une réponse des États dans le sens d'une capacité de réactions contre les nouvelles vulnérabilités.

En résumé, pour l'armée suisse, il doit y avoir quatre étapes fondamentales qui dirigeront l'intégration de nouvelles technologies:

- La définition des besoins en vue d'obtenir une véritable plus-value;
- L'identification des solutions possibles par rapport aux technologies existantes ou en développement;
- La définition du champ d'engagement possible des nouvelles technologies;
- L'adaptation des technologies choisies aux contraintes de l'utilisation militaire, en particulier dans le domaine de la sécurisation [8].

**Marc-André Ryter**
est collaborateur auprès de la doctrine militaire à l'état-major de l'Armée. Il suit les développements technologiques relevants pour les forces armées et pour les différentes sphères d'opérations, en particulier dans la perspective du développement de la doctrine.

Marc-André Ryter peut être joint sous:
marc-andre.ryter@vtg.admin.ch.

## Littérature

[1] Schwab, Klaus, „The Fourth Industrial Revolution", WEF, 2016, p. 80.

[2] Bloem, Jaap, van Doorn, Menno, Duivestein, David, Maas, René et van Ommeren, Erik: „The Fourth Industrial Revolution: Things to Tighten the Link Between IT and OT", VINT Research Report 3, Groningen, 2014, p.13. Il parle de la capacité des robots à s'occuper de tout ce qui est couvert par les 3 D: „dirty, dangerous and dull work".

[3] Schwab, Klaus: „The Fourth Industrial revolution", in Foreign Affairs, December 2015.

[4] Wood, Colin, D.: „The Human Domain and the Future of Army Warfare: Present as Prelude for 2050", in Small Wars Journal, August 2016, p. 3.

[5] Hémez, Rémy: „L'avenir de la surprise tactique à l'heure de la numérisation", Études de l'Ifri, No 69, Juillet 2016, p. 27.

[6] Bloem estime qu'entre 2013 et 2016, près de 95'000 robots de nouvelles générations, pour un coûts total de 14 milliards de dollars (soit près de 150'000 dollars pièce) ont été mis en service dans l'industrie. Voir: Bloem, op. cit., p. 14.

[7] Par exemple Zheng, Denise E. et Carter, William A.: „Leveraging the Internet of Things for a More Efficient and Effective Military", Center for Strategic and International Studies (CSIS, Report of the CSIS Strategic Technologies Program, September 2015, p. 19.

[8] Adapté de Goetz, Pierre et Cahuzac-Soave, Olivia: „Impact de la numérisation sur l'exercice du commandement", Compagnie Européenne d'Intelligence Stratégique (CEIS), Les notes stratégiques, décembre 2015, p. 34.

# Wonders at the Threshold: Operational Priorities,Tensions and the Future of Military Platforms and Systems

**"In my opinion, all previous advances in the various lines of invention will appear totally insignificant when compared with those which the present century will witness. I almost wish that I might live my life over again to see the wonders which are at the threshold". - Charles H. Duell, Head of U.S. Patent Office, 1902.**

**Keywords:** **C4ISTAR, Survivability, Expendability, Platforms, Military Systems**

**Author:** **Tate Nurkin**, Jane's by IHS Markit

For much of the 1990s and early 2000s, the United States defence community in particular was occupied with the concept of a Revolution in Military Affairs (RMA) that would fundamentally alter the ways in which militaries organized and prepared for and fought modern conflict. Driven by impressive innovation and development in C4ISTAR technologies and precision-guided munitions, the millennial RMA stressed operational concepts such as perfect situational awareness, long-range precision strike and full spectrum dominance in conflict with peer or near-peer competitors.

The RMA movement never quite reached altitude or caught fire outside of the United States. It stalled in the mid-2000s under the weight of the dual insurgencies in Iraq and Afghanistan, conflicts that looked different to those the RMA envisioned. Perfect situational awareness and future combat systems were waylaid by the improvised explosive device and asymmetric operational concepts for which the RMA and all its technological promise had little off-the-shelf response.

Nearly fifteen years after the halting of the RMA's momentum, militaries around the world once again are confronted by a moment of dynamic innovation and much anticipated disruption in the nature of conflict and the tools used to wage it.

This time, though, the complexion of the transformation is more complex and uncertain; the dimensions of innovation more expansive; the scale of possible effects more comprehensive. Militaries find themselves wading cautiously, but curiously, into a new revolution in military capabilities stemming primarily from multi-dimensional and multi-directional innovation in and diffusion of a diverse and growing set of emerging technologies with varied military applications (Table 1). On-going and future development of these technologies, both individually and collectively, portend radical shifts in the nature, characteristics, concepts and properties of future of military platforms and systems.

Indeed, contemporary visions of artificially intelligent and fully autonomous unmanned systems (Figure 1); drone swarms and mother ships; point of use 3-D printed payloads and parts; hypersonic weapons and planes; shape-shifting and self-healing platforms; and even biomaterial infused invisibility cloaks -among many other futuristic capabilities - instill thoughts of 'wonders at the threshold', some previously only contemplated by science fiction or video games.

## The Future of Platform and Systems

The specific nature, pace, parameters and trajectory of how these revolutions will unfold is, of course, highly uncertain. Development of emerging technologies - as welll as requisit accompanying innovation in concepts; business, procurement and development models; and organizational structures - is unlikely to follow a either a straight or, more importantly, single line.

Some militaries will seek to make big bets in high-end and expensive technologies and sophisticated capabilities that provide unassailable technologically advantage and fundamentally alter military and geopolitical competitions. Other actors - both state and non-state armed groups - will leverage more widely dispersed technologies to drive novel good enough and asymmetric capabilities that exploit adversary operational vulnerabilities or imbalanced cost curves.

Regardless, of the level of and approach to disruptive innovation, the future of platforms and system development and deployment will require militaries to balance competing priorities and objectives in and across three critical tensions.

| | | | |
|---|---|---|---|
| Artificial Intelligence | Smart, Advanced and Bio-Materials | Hypersonics / Supersonic Flight | Position, Navigation and Timing |
| Big Data Analytics | 3-D Printing | Directed Energy | Quantum Computing and Encryption |
| Enhanced Autonomy | 4-D Printing | Unmanned Systems | Virtual and Augmented Reality |
| Remote and Advanced Sensing | Synthetic Biology Manufacturing | Semiconductors | Energy Capture and Storage |
| Biometrics | Hybrid Engines / Combined / Variable Cycle Engines | Advanced Warhead and Munition Technologies | Electronic Warfare Technologies (i.e., cognitive and adaptive jamming) |
| Blockchain | Cyber-Security Technologies | | Robotics |
| Transient Electronics | Internet-of-Things | Space and Counterspace Technologies | Electro-Magnetic Weapons |

***Table 1:*** *List of technologies of interest for the future military platforms and systems*


***Figure 1:*** *MILREM's THeMIS modular unmanned ground vehicle (source: MILREM)*

## Specific Mission Effects vs the Adaptability Imperative

The breadth of possible innovation vectors coupled with geopolitical, economic and defence industry and market trends are facilitating the diffusion of emerging technologies and know-how, much of which is opaque or at the very least not fully transparent. More actors are now in command of more and better capability, creating an operational environment marked both by an expanding range of challenges and the growing potential for what U.S. Deputy Secretary of Defense referred to in a May 2017 speech to the U.S. Department of Defence Applied Physics Lab "endemic surprise."

The multi-layered, fast-moving and complex environment suggests disparate implications for the future of platforms and systems.

Many advanced militaries will focus on capabilities designed to meet a specific threat, engage a specific - usually difficult to engage - target set or carry out a specific mission. In a June 2017 internal Jane's workshop examining the future of munitions technologies and capabilities, analysts repeatedly stressed a robust and resilient need for high-powered or discrete effect weapons to better deal with specific threats - e.g., the "mother of all bombs" to deal with hardened targets - or in specific challenging environments. Specification of platforms and systems to establish dominance of domains or to deter, dissuade, degrade, deny or defeat specific capabilities, asymmetric or otherwise, will also be a priority of future platform and system development.

Simultaneously, the future of platforms and systems will be heavily influenced by a burgeoning imperative to provide commanders a heightened degree of flexibility and adaptability to operate in fast-moving and complex environments and meet spontaneously produced threats.

Modular platforms and systems is one means of delivering this operational flexibility at low costs. Plug-and-play payloads for unmanned platforms; modular warheads for anti-tank missiles; and the littoral combat ship's interchangeable mission packages all stand out as indicative examples.

So, too, is the development and recent deployment of explicitly designed multi-mission platforms and systems across all domains and many system types. Growing emphasis on multi-mission helicopters highlights this trend. A cursory review of press-releases and marketing collateral found on helicopter manufacturer websites reveals a distinct and consistent theme: as a press-release on Lockheed Martin's website articulated, next generation helicopters will need "to adapt to different situations – moving seamlessly from delivering supplies, to combat, to search and rescue."

Jane's contributor Dr. Lee Willett effectively captured the trade-offs and enduring appeal associated with multi-mission capabilities in the naval domain as well. In a March 2017 Jane's Navy International article exploring the future role of frigates, Willett noted that "the requirement for and capability fits and operation of today's frigates reflect how naval platforms - especially surface ships - are required to respond to the changing nature of the operational and wider strategic environments. While frigates may be seen as less capable, more affordable platforms, they can deploy globally and conduct many tasks across the operational spectrum: an affordable multi-tool for the naval strategist."

## Survivability vs Expendability

Platform and system development over the last two decades has become increasingly pre-occupied with the concept of survivability; that is, the capacity of a particular platform to operate in a contested environment without having its operational effectiveness degraded or destroyed.

Much of the approach to survivability during this time has focused on a combination of defencive measures and damage control mechanisms that make a platform harder to hit and that minimize the loss of life and potential for catastrophic failures


*Figure 2: A sample China's cruise missiles as displayed at the IDEX 2017 Exhibition in Abu Dhabi (credit: Tate Nurkin)*

if a platform is damaged. The result has been heavy investment in stealthy technologies, on-board defensive measures and counter-measures, and compartimentalized large platform designs that contain fire or flooding.

However, shfits in the global strategic context and operational threat environment are intersecting with the introduction of more and more sophisticated capabilities to force the incorporation of new technologies and approaches enabling survivability on the future battlefield.

For example, anticipated advances in and diffusion of sensing technologies - most notably quantum radars that cannot be jammed, can designate small objects and can transmit in lower frequency to avoid atmospheric absorption at longer ranges - could abrogate the advantages accrued by current iterations of stealthy technologies and designs.

Such iterative and interactive capability competitions necessitate technological innovations, but also will compel new concepts of survivability that deemphasize absorbing pressure from adversaries or competitors and instead feature placing more pressure on them through equipping platforms with more offensive firepower.

The U.S. Navy's distributed lethality concept stands out as a means of moving to a more 'front foot', flexible and deterrence-based approach to survivability. The concept includes arming surface vessels with more offensive weapons, integrating more advanced sensors and adapting new tactics and operational concepts that disperse vessels over larger areas, to reduce risk and enhance capacity of individual platforms to respond to fast moving threats. At a minimum, the concept provides an upgraded deterrent and could also cause U.S. adversaries and competitors to sacrifice offensive firepower for defensive capabilities, augmenting survivability in the process.

Survivability of platforms and systems in future warfare will also require an increased focus on the cyber domain and, especially, the capacity to organically and dynamically meet a broader range of threats in the increasingly crowded and contested electromagnetic spectrum.

Current adaptive electronic warfare systems are effective against many known electronic warfare (EW) threats, but in a future in which surprise and technology diffusion are both 'endemic', adaptive EW will be insufficient to respond to previously unknown threats. Survivability, then, will rest on adaptability and, specifically, the capacity of emerging technologies such as cognitive EW that allow platforms to enter any environment with no information about adversarial systems and independently and rapidly identify, understand and formulate countermeasures.

But survivability - even a reimagined concept of survivabilty - is not the only area of emphasis for future platforms and systems. Both state actors and non-state armed groups are

demonstrating heightened interest in the use of 'expendable', rather than survivable, platforms and systems to carry out a growing range of missions and achieve a growing range of effects.

Currently, use of expendable systems and unmanned platforms is predominantly focused on supporting saturation tactics - for example, China and Iran's development of more and more varieties of cruise missiles (Figure 2) to simply overwhelm regional missile defence systems - and to carry out dirty and dangerous missions, such as the use of unmanned underwater vehicles to perform port security and mine counter-measure missions.

But the future of expendable platforms and systems is more expansive and centers around swarms of autonomous unmanned systems. While iindividual systems within the swarm will have specific functions - decoy, strike, air-defence suppression, surveillance-all unmanned systems in the swarm communicate with each other with decisions being made by software exploiting artificial intelligence.

Redundancy and resilience are a key feature of swarms, meaning that some components of swarms will be expendable - in fact, some members of the swarm may well serve as decoys, soaking up defensive fires and distracting attention from other swarm components. The swarm concept and technologies to enable it are both still maturing. Still, new development thresholds are being crossed, demonstrating the potential for unmanned swarms to prominently shape the future of conflict and of military platforms and systems.

Notably, in June 2017, China Electronic Technology Group Corporation (CETC)'s claimed to have established a swarm of 119 micro unmanned systems, purportedly the largest drone swarm yet successfully tested (Figure 3). According to Jane's Defence Weekly, after the test a CETC engineer provided told state-run media outlet Xinhua that unmanned vehicles will become „a disruptive force" that will „change the rules of the game".

## Individual vs Integrated and Interactive Platforms and Systems

Discussions of the friction between survivability and expendability as contrasting-and sometiimes complementary-approaches to meeting the demands of future operational environments also gives rise to assessment of the tension between the future of platforms and systems as individual assets and as part of connected and highly integrated teams.

Development and deployment of multi-mission platforms and systems and new concepts of survivability highlight the capacity of individual platforms and systems to affect operational environments and meet more frequently difficult to anticipate challenges. Indeed, one of the core tenants of the U.S. Navy's distributed lethality concept is the capacity of individual platforms to address fast-moving or unanticipated threats if needed. Similarly, investments in armed intelligence, surveillance and reconnaissance platforms - both manned and unmanned and especially in support of special operations missions-are designed to allow not only for augmented defence, but also to strike imminent threats or targets of opportunity if required.

Even as these investments advance, though, there is deliberate and powerful movement toward even greater connectivity and consistent coordination between platforms and systems goes beyond swarms of autonomous unmanned swarms. Munitions that can be retargeted in-flight, either via human control, artificial intelligence or other autonomous platforms and systems (leaving aside important ethical concerns) offer commanders immense flexibility, but also rely on coordination between a broader set of closely and dynamically connected platforms and systems.

Concepts of manned – unmanned teaming (MUM-T) are particularly important to the future of platforms and systems over the next two decades, as the balance between manned and unmanned systems and the roles they play shift dramatically.

Some advanced MUM-T concepts include future manned 'fighter' aircraft serving as either 'mother ships' for unmanned systems or as directors of coordinated / swarmed unmanned aircraft. The former approach was demonstrated by the U.S. Air Force in October 2016 when three Boeing F/A-18 Super Hornets released 103 Perdix micro-UAVs as part of testing and evaluation.

Manned – unmanned teaming concepts will also be developed and deployed to help provide enhanced situational awareness and functionality to platform pilots and operations. Through the use of artificial intelligence, helmet displays and virtual and augmented reality, future operators will be able to view video feeds from networked unmanned ISR systems and even, potentially, to control and task those systems to collect information or engage targets, validating the concept that even manned platforms of the future should be interpreted as critical nodes coordinating much broader eco-system of linked platforms and systems.

*Figure 3: China's CETC claims to have set a record for the number of UAVs launched in a swarm (via CCTV)*

## Conclusion

Jane's Strategic Assessments and Futures Studies Centre tracks over two dozen technologies that multiple militaries around the world have identified as being of interest. This long (and growing) list is a potent indicator of the potential for layered and revolutionary changes in future military capabilities - from incremental improvements to effective asymmetric capabilities to game-changing 'wonders at the threshold.'

Capitalizing on the opportunity to drive and shape requires defence and security communities to effectively balance sometimes complementary, but frequently competing, strategic and operational objectives and priorities.

However, fully exploiting this expectant and potentially transformative moment will command more than innovation in technology and concepts. It also necessitates development of new and enhanced means of bounding and assessing implications of likely, possible and plausible futures for platforms and systems and, critically, for how iterative innovation will disrupt and reshape stabilizing balances and imbalances in the most important military, security and geopolitical competitions throughout the world.


**Tate Nurkin**

is Senior Director of the Strategic Assessments and Futures Studies (SAFS) Center with Jane's by IHS Markit. He is also a member of the IHS Markit Editorial Council, which is comprised of Chief Analyst equivalents from across IHS Markit's business lines. Since June of 2016, Tate has served as a member of the World Economic Forum's (WEF) Council for the Future of International Security, which is focused on the intersection of Fourth Industrial Revolution technologies and military capabilities.

# Materials by Design: Neue Ansätze in der Werkstoffentwicklung für Strukturwerkstoffe und ballistischen Schutz

**In den letzten Jahren gab es spannende neue Entwicklungen, welche die Vorgehensweise der traditionellen Werkstoffentwicklung umkehren, indem die strukturellen Merkmale eines Werkstoffs gezielt entworfen werden. Das Resultat sind Materialien mit komplexem hierarchischen Aufbau, der sich an natürlichen extrem widerstandsfähigen Materialien wie Perlmutt oder Knochen orientiert, mechanische Metamaterialien, die über ungewöhnliche mechanische Eigenschaften verfügen sowie dreidimensionale Gradientenwerkstoffe, die eine geforderte Funktionalität unabhängig von der Bauteilgeometrie exakt am gewünschten Ort liefern können. Materials by Design verfügen über ausgezeichnete mechanische Eigenschaften, insbesondere eine hohe Schadenstoleranz, und eignen sich daher als Struktur- und Schutzwerkstoffe für viele Anwendungen.**

**Keywords:** **Materials by Design, Top-down-Werkstoffentwicklung, Mechanische Metamaterialien, Auxetische Werkstoffe, Architectured Materials, Gradientenwerkstoffe, Biokomposite, Strukturwerkstoffe, Ballistischer Schutz**

**Autor:** **Dr. Ramona Langner & Dr. Heike Brandt**, Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen

Die Entwicklung neuer Werkstoffe für herkömmliche wie innovative Anwendungen geschieht zumeist evolutionär. Dazu werden Variationen in der chemischen Zusammensetzung oder bei den Herstellungsparametern durchgeführt, um die Werkstoffe in Bezug auf bestimmte Eigenschaften Schritt für Schritt zu verbessern. Diese müssen aber nicht notwendigerweise bereits im Hinblick auf bestimmte Funktionalitäten oder Anwendungen erfolgen. Erst die Auswahl spezifischer Werkstoffe sowie deren geschickte Kombination führen zu Werkstücken, die in Form und Funktion auf eine bestimmte Anwendung hin optimiert sind. In den letzten Jahren werden für die Werkstoffentwicklung jedoch zunehmend sogenannte Materials-by-Design-Ansätze verfolgt. Dabei steht in Umkehrung zur traditionellen Herangehensweise zunächst eine gewünschte Funktionalität bzw. Anwendung im Vordergrund. Von dieser ausgehend werden anschließend die strukturellen Merkmale des dafür benötigten Werkstoffs vorgegeben und der Werkstoff entwickelt.

## Der gezielte Entwurf von Werkstoffeigenschaften

Vor der Realisierung solcher Materials by Design steht zunächst der Entwurf der strukturellen Merkmale. Ausgehend von den gewünschten Eigenschaften werden die physikalischen Grundgleichungen, die diese beschreiben, mathematisch invertiert, um im Umkehrschluss einen passenden Werkstoff zu generieren. Aufwendige numerische Verfahren werden genutzt, um einzelne Baueinheiten, ihre Anordnung und die resultierenden Effekte theoretisch zu modellieren. Über entsprechende Schnittstellen können generierte Simulationsergebnisse auf technische Berechnungs- und Computer-Aided-Design-Programme übertragen werden. Auf diese so erzeugten digitalen Vorlagen wird dann bei der Herstellung der Materialien zurückgegriffen. Aufgrund dieses Paradigmenwechsels von der Bottom-up- zur Top-down-Werkstoffentwicklung, der bei den Materials by Design eine definitorische Rolle spielt, bestimmen der Aufbau der Baueinheiten, ihre Dimensionen und deren erforderliche hierarchische Anordnung das geeignete Verfahren zur Herstellung dieser Materialien. Die Auswahl des Fertigungsverfahrens ist somit einer der letzten Schritte bei der Herstellung.

Dieser Materials-by-Design-Ansatz wird bereits seit längerem unter anderem im Bereich neuartiger Werkstoffe wie bionischer Materialien oder Metamaterialien genutzt. Als übergreifendes Paradigma breitet sich der Materials-by-Design-Ansatz aber zunehmend auch auf klassische Materialsysteme wie z. B. hochfeste Stähle aus. Durch diesen Ansatz lassen sich Kombinationen von Eigenschaften erzielen, die mit der herkömmlichen Werkstoffentwicklung nicht oder nur schwer erzielt werden können. So weisen solche Materialien insbesondere eine hohe Schadenstoleranz und eine gute Schwingungsdämpfung auf. Auf Basis solcher neuen Werkstoffe könnten leichtere und gleichzeitig festere sowie steifere Leichtbauteile gefertigt werden, von denen generell eine große Zahl an Plattformen profitieren würde. Dadurch könnten Traglast, Reichweite und Einsatzdauer erhöht und Treibstoff eingespart werden. Materials by Design weisen zudem ein großes Potenzial als neuartige Schutzwerkstoffe auf. Ein leichterer und flexiblerer Körperschutz würde sowohl die Beweglichkeit als auch die Leistungsfähigkeit des Soldaten erhöhen. Beispielsweise ließen sich damit leichtere Einschübe für Schutzwesten fertigen und die Schutzwirkung von Helmen weiter verbessern. Als Teil passiver Schutzsysteme wie der Panzerung von Gefechtsfahrzeugen könnten sie mit ihrer geringen Dichte dazu beitragen, deren Gewicht zu senken, ohne den Schutz der Systeme z. B. gegenüber ballistischen Projektilen oder den Schockwellen von IED zu verringern. So könnten leichtere, mobilere Gefechtsfahrzeuge, für die schwere Panzerungssysteme nur begrenzt in Frage kommen, von leichten, aber enorm schadenstoleranten Panzerungsmaterialien profitieren. Auch eine Ergänzung herkömmlicher passiver Schutzsysteme wäre denkbar, zum Beispiel indem die neuartigen Schutzwerkstoffe im größten Teil der Plattform einen gewissen Grundschutz bieten und schwere Panzerungssysteme nur dort eingesetzt werden, wo sie tatsächlich notwendig sind.

## Architectured Materials – die Natur zum Vorbild

Ein Beispiel für Materials by Design sind sogenannte Architectured Materials. Diese verfügen über einen sehr komplexen strukturellen Aufbau, der zunehmend als Architektur bezeichnet wird. Diese Architektur etabliert sich dabei als eine gleichberechtigte Stellschraube – neben z. B. chemischer Zusammensetzung und Korngröße – zur Entwicklung völlig neuer Komposite. Vorbild für Architectured Materials sind häufig extrem schadenstolerante biologische Stoffe wie der menschliche Zahnschmelz oder Perlmutt. Ihre Basis bilden Bausteine aus sehr harten und steifen Materialien in Kombination mit einer zähen, elastisch dehnbaren Matrix. Die industrielle Nachbildung solcher biologischen Konzepte ist aufgrund der herausragenden Eigenschaftskombination von z. B. Flexibilität, Zugfestigkeit und Gewicht für die Entwicklung ballistischer Materialien für den Körperschutz von großem Interesse. Man erhofft sich davon vor allem Verbesserungen der herkömmlichen Multi-Schicht-Strukturen, bei denen ebenfalls weiche und harte Komponenten kombiniert werden. Nach diesem Vorbild könnten aber auch völlig neue Panzerungswerkstoffe und -strukturen entwickelt werden, die bei gleicher Schutzwirkung ein deutlich geringeres Gewicht aufweisen würden.

Die Größe der Bausteine natürlicher, harter Materialien liegt zumeist im Bereich von ca. 100 Mikrometern bis zu 100 Millimetern, also weit oberhalb dessen, was üblicherweise unter einer Mikrostruktur verstanden wird. Sie werden in unterschiedlichen zwei- oder dreidimensionalen Anordnungen

*Bild A: Perlmutt gehört zu den am häufigsten untersuchten nicht-menschlichen Biokompositen. Es ist in Form einer komplexen Struktur aus Aragonit-Plättchen und organischem Material aufgebaut.*

aneinandergefügt und durch die weiche Matrix verbunden. Die resultierenden Werkstoffverbunde sind häufig gezielt extrem heterogen, mit Gradienten in Chemismus und Mikrostruktur, und besitzen oft auch eine hierarchisch aufgebaute Struktur. So gibt es Biokomposite, die aus einem organischen Proteingerüst bestehen, welches die Grundlage für eine sich darauf aufbauende mineralisierte Matrix darstellt. Dieser Bottom-up-Prozess wird als Biomineralisation bezeichnet und ist derzeit noch sehr schwierig im Labor zu realisieren. Ein natürliches Vorbild hierfür sind die Keulen von Fangschreckenkrebsen, die aus Hydroxylapatit und Chitin bestehen. Ein anderes grundlegendes Konzept ist die Schichtung vieler verschiedener, verstärkender Lagen, bei der jede Materialschicht ihre eigenen Energieabsorptions- und Deformationseigenschaften aufweist. Ein Beispiel dafür sind Fischschuppen, die aus verschiedenen Materialien, wie z. B. Dentin oder Kollagen, bestehen. Hier liegt die härteste Schicht außen, während die Schichten nach innen weicher und elastischer werden.

Die Herstellung von an solche natürlichen Strukturen angelehnten Architectured Materials erfolgt üblicherweise bottom-up durch den Aufbau der Struktur aus ungeordneten Bausteinen. Beispielsweise wurden verschiedene Schichtstrukturen aus Mikro- oder Nano-Plättchen durch Schichtabscheidung oder Zentrifugieren hergestellt. Auch eine Ausrichtung der Bausteine durch Self-Assembly oder mittels Magnetfeldern wurde bereits demonstriert. Weiterhin werden auch offenporige Strukturen aus Keramiken oder Metallen genutzt, die ein stabiles Gerüst vorgeben, welches in einem nachfolgenden Prozessschritt mit einer elastischen Komponente gefüllt wird. Gänzlich neue Möglichkeiten der Realisierung solcher komplexen Strukturen stellen verschiedene Techniken der additiven Fertigung zur Verfügung, bei denen der Aufbau des Werkstoffs sukzessive Schicht für Schicht erfolgt. Insbesondere ist es von Vorteil, die härtere und die weichere Komponente gleichzeitig zu drucken und damit die Struktur in nur einem Schritt herzustellen. Architectured Materials können aber auch hergestellt werden, indem die gewünschten strukturellen Merkmale nachträglich in ein bestehendes Werkstück eingebracht werden. Beispielsweise lassen sich transparente dreidimensionale Werkstoffe wie Gläser durch eine Laser-Innengravur verstärken. Eine weitere Forschungsrichtung auf diesem Gebiet stellt die Verbesserung von Stählen und anderen Legierungen mittels starker plastischer Deformation dar. So konnten Stähle von enorm hoher spezifischer Festigkeit erzielt werden, ohne dabei Einbußen in der Duktilität hinnehmen zu müssen, indem zunächst ein Kohlenstoffgradient in den Stahl eingebracht und das resultierende Gefüge anschließend mittels Hochdruck-Torsion verformt wurde. Diese könnten zukünftig z. B. als verbesserte Panzerungswerkstoffe für schwere Gefechtsfahrzeuge zum Einsatz kommen.

## Mechanische Metamaterialien ermöglichen ungewöhnliche Eigenschaften

Eine Untergruppe der Architectured Materials sind mechanische Metamaterialien, auch als elastische Metamaterialien bezeichnet. In Anlehnung an die für elektromagnetische Metamaterialien erarbeiteten Prinzipien, lässt sich mit ihrer Hilfe die Ausbreitung elastischer Wellen in einem Festkörper manipulieren. Dadurch wird es unter bestimmten Bedingungen möglich, Dichte, Schubmodul oder Kompressionsmodul für einen begrenzten Frequenzbereich in den negativen Bereich zu verschieben oder das Verhältnis von Kompressions- und Schubmodul drastisch zu ändern. Dadurch lassen sich besondere mechanische Eigenschaften erzielen, die auf herkömmliche Weise nicht erreicht werden können und oftmals kontraintuitiv wirken.

Beispiele für solche mechanischen Metamaterialien sind sogenannte auxetische Werkstoffe, die sich unter Zug nicht nur in Zugrichtung, sondern auch senkrecht dazu ausdehnen, sowie Materialien mit einer negativen Kompressibilität, die sich unter Last ausdehnen und so einem äußeren Druck entgegenwirken. Letztere sind bisher nur als theoretisches Konzept diskutiert worden, sie wären aber von besonderem Interesse für den ballistischen Körperschutz. Beim Auftreffen ballistischer Körper auf weichballistische Panzerungsmaterialien nehmen diese aufgrund ihrer sehr hohen Zähigkeit durch Verformung Energie auf, die dann auf eine möglichst große Fläche verteilt wird. Schutzkleidung aus solchen Materialien dehnt sich dabei jedoch in Richtung Körper aus, was zu Verletzungen wie stumpfen Traumata bis hin zu Knochenbrüchen führen kann. Materialien mit einer negativen Kompressibilität würden stattdessen einen Gegendruck nach außen erzeugen.

Ein weiteres Beispiel sind sogenannte Compliant oder Buckling Materials, die sich unter Last gezielt verformen und Energie aufnehmen, aber anschließend wieder in ihren Ausgangszustand zurückkehren. Dadurch können sie große Mengen von Energie kurzzeitig aufnehmen und so andere, unnachgiebigere Strukturen schützen. Ein Beispiel dafür wäre eine Stoßstange, die sich beim Aufprall auf ein Objekt so verformt, dass Objekt und Fahrzeug möglichst wenig Schaden nehmen, die sich anschließend aber weitestgehend zurückformt. Zudem wurden bereits erste Strukturen gefertigt, deren effektive Dichte für einen eng begrenzten Frequenzbereich elastischer Wellen kurzzeitig negativ werden kann. Dadurch können diese Frequenzen das Material nicht durchqueren und werden teilreflektiert und gedämpft. So könnte die Auswirkung von Schockwellen auf eine Struktur verringert werden.

Mechanische Metamaterialien sind aufgrund ihrer überragenden mechanischen Eigenschaften auch von großem Interesse als Strukturwerkstoffe und für Leichtbauanwendungen. Während in herkömmlichen Materialien mit sinkender Dichte auch die mechanischen Eigenschaften schnell nachlassen, ist dies bei mechanischen Metamaterialien nicht der Fall. Dadurch wurden bereits Werkstoffe hergestellt, die die sehr geringe Dichte eines Aerogels erreichen, gleichzeitig aber eine um vier Größenordnungen höhere Steifigkeit aufweisen. Zwar werden bereits Werkstoffe mit sehr geringer Dichte wie z. B. Schäume in Leichtbauanwendungen eingesetzt. Mechanische Metamaterialien würden diesen gegenüber aber noch weitere entscheidende Vorteile bieten. Durch ihre geordnete Struktur lassen sie sich durch Anpassung der Bausteine oder der Geometrie leichter für spezielle Anwendungen maßschneidern. Generell könnten von der Entwicklung solcher neuer Werkstoffe fliegende Plattformen wie UAS profitieren. Aber auch in leichten, mobilen Gefechtsfahrzeugen und anderen Plattformen könnten sie zum Einsatz kommen.

## Metasurfaces erleichtern die Übertragung in die Praxis

Neuere Entwicklungen im Bereich der Metamaterialien setzen auf das Konzept der sogenannten Metasurfaces, die im Allgemeinen als zweidimensionale Metamaterialien angesehen werden. Eine Motivation dafür ist neben ihrer leichteren Realisierbarkeit das potenziell sehr große Anwendungsspektrum flexibler, zweidimensionaler Strukturen. Solche Metamaterialien könnten beispielsweise auch auf gekrümmten Flächen aufgebracht werden. Die Herstellung der benötigten Nanostrukturen wird von lithographischen Methoden dominiert, wobei zwischen Verfahren unterschieden wird, die Strahlung zur Strukturierung nutzen, und sogenannten Soft-Lithographie-Verfahren, die zur indirekten Strukturierung die mechanischen Grundverfahren Prägen, Drucken oder Abformen nutzen. Häufig werden diese Strukturen nach der Herstellung noch weiterverarbeitet und erlangen erst durch unterschiedlichste Beschichtungsmethoden ihre Funktion. Abhängig von der zu erreichenden Tiefenschärfe des einzelnen Verfahrens, ist eine Strukturierung weitestgehend auf zwei Dimensionen beschränkt. Die Stereolithographie ermöglicht als additives Fertigungsverfahren den schichtweisen Aufbau der Struktur und erreicht damit eine Dreidimensionalität. Ein Vorteil dieser Technik wäre, dass einem Bauteil relevante zusätzliche Funktionen verliehen werden könnten, wie beispielsweise eine Tarnung des Objektes in einem breiteren Wellenlängenbereich. Auf diese Weise ließen sich Objekte am Boden, z. B. Flugzeuge oder Fahrzeuge, vor einer Entdeckung durch ein luftgestütztes Radarsystem schützen.

## Dreidimensionale funktional gradierte Werkstoffe

Abrupte Übergänge zwischen Materialien mit deutlich unterschiedlichen Eigenschaften können – speziell bei starker mechanischer Belastung – eine Schwachstelle darstellen, die, wie in natürlichen Materialsystemen, durch die kontinuierlichen Eigenschaftsänderungen eines Gradienten umgangen werden kann. Grundsätzlich können Gradientenwerkstoffe auch Werkstoffklassen-übergreifend für eine Vielzahl von Herausforderungen intelligente Lösungen bieten – beginnend bei dem Wunsch, spezielle Eigenschaften an exakt der Stelle des Bedarfs zu Verfügung zu stellen. Dies entspricht dem generellen Trend der bedarfsgerechten Fertigung. In Multi-Material-Systemen für ballistische Schutzanwendungen werden, speziell im Bereich des Fahrzeugschutzes, spröde hartballistische Materialien eingesetzt, um Schutz vor Hartkern- und Hochgeschwindigkeitsgeschossen zu erreichen. Ihre Kombination mit weichballistischen Materialien, wie einer Polymer-basierten Rückenplatte zur Abbremsung der Fragmente, erzeugt Unterschiede bezüglich Härte, Elastizitätsmodul und Dichte. Dies führt zu teils unerwünschten Rückstreu- und Überlagerungsprozessen bei der Ausbreitung der erzeugten Druckwellen. Diese Post-Impakt-Schäden können durch gradierte Übergänge zwischen den Materialien minimiert werden, indem sie eine zeitliche Verzögerung bei der Wellenausbreitung erzeugen. Sowohl optimierte Metall-Keramik-Gradienten als auch Gradienten bezüglich der Porosität könnten einen Beitrag zu einem verbesserten Energieabsorptionsverhalten leisten.

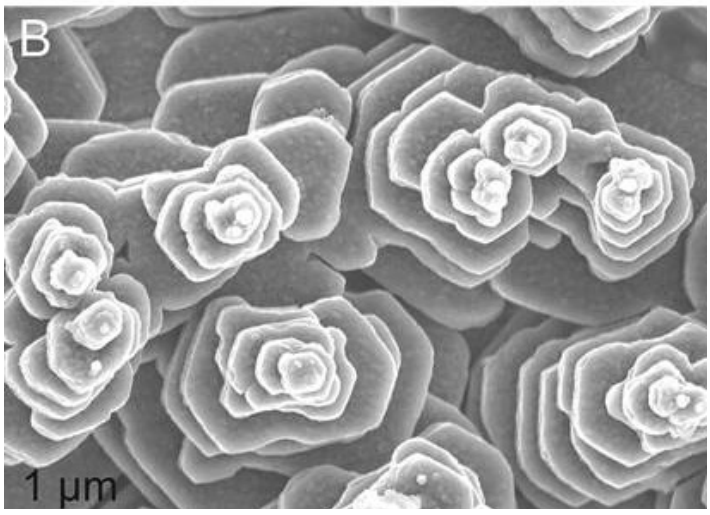



***Bild B:*** *Elektronenmikroskopische Aufnahme der Strukturdetails (cephalopod Nautilus pompilius, aus: Journal of Structural Biology, Volume 176, Issue 3, December 2011, Pages 330-339, Mineral bridges in nacre, Antonio G.Checa, Julyan H.E.Cartwright, Marc-GeorgWillinger)*

Die präzise Einstellung von Gradienten ist technisch aufwendig. Aus diesem Grund besteht ein hohes Interesse an additiven Fertigungsverfahren. Verfahren, bei denen lokal im Mikrometerbereich Ausgangsmaterialien verfestigt werden, sind für die Gradierung von Werkstoffen prädestiniert. Je nach Materialsystem werden in aktuellen Forschungsarbeiten zu Gradientenwerkstoffen vorwiegend zwei Strategien verfolgt. So können Gradienten durch eine gezielte Variation des Mischungsverhältnisses der pulverförmigen Ausgangsmaterialien während der Herstellung erzielt werden. Abhängig von der Anzahl der Zuführsysteme für diese Ausgangsmaterialien, aber auch der Präzision bei ihrer Steuerung, sind unterschiedlichste Materialgradienten, wie z. B. Wolframcarbid in Stahlmatrix oder Graphen in Polymermatrix, denkbar. Bei Legierungen kann darüber hinaus eine Gradierung der Mikrostruktur durch Variation der Prozessparameter erreicht werden. So ist beispielsweise die Härte eines Stahls oder einer Nickelbasislegierung von der erzeugten Mikrostruktur abhängig, die mit Hilfe der gewählten Leistung des zur Aufschmelzung verwendeten Lasersystems eingestellt werden kann.

## Offene Herausforderungen

Generell ist die Technologiereife von Materials by Design noch relativ gering und verschiedene Herausforderungen stehen einer verbreiteten Anwendung als Strukturwerkstoffe oder für den ballistischen Schutz im Weg. Zum einen stehen derzeit nicht genügend Verfahren für die Modellierung und Optimierung der Strukturen zur Verfügung, da sie entweder eine homogene Struktur voraussetzen oder nicht für die Simulation größerer Materialvolumen unter realistischen Lastkonfigurationen geeignet sind. Durch die Kommerzialisierung von Simulationskapazitäten gibt es jedoch zunehmend einen einfacheren Zugang zur Nutzung geeigneter simulationsbasierter Verfahren für Anwender wie beispielsweise mittelständische Unternehmen. Zum anderen fehlt eine systematischere Herangehensweise in der Entwicklung solcher neuartiger Materialien, beispielsweise in Form einer Strukturdatenbank.

Speziell für die Entwicklung mechanischer Metamaterialien ist zudem ein tieferes Verständnis der zugrundeliegenden Mechanismen der Wechselwirkung zwischen elastischen Wellen und der Struktur notwendig. Diese spielt sich auf mikroskopischer Ebene ab, deshalb müssen auch die Baueinheiten auf dieser Ebene beschrieben werden. Gleichzeitig werden die Eigenschaften von Materials by Design auch stark von lokalen Phänomenen bestimmt. Beispielsweise spielen Defekte oder Oberflächenphänomene eine große Rolle. Auch im Bereich der Herstellungsverfahren selbst gibt es noch Verbesserungspotenzial. Die Fertigung solch komplexer Strukturen erfordert eine hohe Präzision. Insbesondere wird hier daran geforscht, die Größe der Strukturbausteine weiter zu verringern, auch mit dem Ziel hierarchische Strukturen auf verschiedenen Größenskalen zu erzeugen. Dadurch ließen sich die mechanischen Eigenschaften noch viel präziser einstellen. Darüber hinaus stellt speziell bei Strukturdetails im Submikrometerbereich die Kombination von Präzision der Baueinheiten einerseits und Größe des Gesamtobjektes andererseits eine Hürde dar.

## Ausblick

Langfristig erhofft man sich neben den genannten Entwicklungen, mit Hilfe von Materials-by-Design-Ansätzen das große Potenzial multifunktioneller Werkstoffe ausschöpfen zu können. Dadurch ließen sich Strukturwerkstoffe mit zusätzlichen Funktionalitäten versehen, wie einer elektrischen oder thermischen Leitfähigkeit, sensorischen und aktorischen Eigenschaften, Fähigkeiten zur Energiegewinnung und -speicherung, einem verbesserten Flammschutz oder einer Abschirmung elektromagnetischer Strahlung. Beispielsweise könnte zumindest ein Teil der Flugsensorik oder Fähigkeiten zum Enteisen der Tragflächen direkt in die Tragflächenstrukturen integriert werden. Darüber hinaus könnten solche Sensoren für das Structural Health Monitoring in Strukturbauteile eingebettet werden. Ebenso könnte es auch möglich werden, intelligente Werkstoffe zu kreieren, die sich durch eine Rekombination ihrer Bausteine aktiv an eine Änderung der Umgebungsbedingungen anpassen können.


### Dr. Ramona Langner

studierte an der Universität Heidelberg Mineralogie und promovierte an der Universität Bochum im Bereich der Festkörper-Kernspinresonanzspektroskopie. Sie arbeitet seit 2011 als wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen in Euskirchen. Ihre Tätigkeitsschwerpunkte im Geschäftsfeld Wehrtechnische Zukunftsanalyse sind die Technologievorausschau sowie tiefergehende Technologienanalysen in den Bereichen Werkstoffe, Wehrtechnik, Geowissenschaften sowie Nachhaltigkeit und Ressourcenmanagement.

Sie ist erreichbar unter
ramona.langner@int.fraunhofer.de



### Dr. Heike Brandt

studierte Mineralogie an der Universität Münster und arbeitete am Forschungszentrum Karlsruhe, an der Virginia Polytechnic Institute and State University und an der Universität Erlangen-Nürnberg an Fragestellungen zur nuklearen Endlagersicherheit sowie zur Initiierung der Knochenbildung bei Implantaten. Seit 2013 ist sie als wissenschaftliche Mitarbeiterin im Institut für Naturwissenschaftlich-Technische Trendanalysen INT der Fraunhofer Gesellschaft tätig. Im Geschäftsfeld Wehrtechnische Zukunftsanalyse liegen ihre Tätigkeitsschwerpunkte auf der Technologievorausschau in den Bereichen Werkstoffe und Geowissenschaften sowie tiefergehenden Technologienanalysen in einem materialwissenschaftlich-wehrtechnischen Kontext.

Sie ist erreichbar unter
heike.brandt@int.fraunhofer.de

# The Impact of Autonomous Weapons Systems on International Security and Strategic Stability

**Autonomous weapons systems (AWS) are for most people akin to science fiction. Although fully autonomous weapons systems do not yet exist, recent rapid progresses in artificial intelligence compels us to think about the potential impact of this weapon on the conduct of war, international security and international stability. This paper starts by reviewing what artificial intelligence is all about, its recent progress and then looks at the likely impact of AWS on strategic stability. It argues that AWS will likely be very destabilizing for international stability because they favour the offensive. It follows that strategies of pre-emption are likely to emerge to thwart the use of AWS.**

**Keywords:** **Artificial intelligence, proliferation, strategic stability, autonomous weapons, swarming, deterrence, pre-emption**

**Author:** **Dr. Jean-Marc Rickli**, Geneva Centre for Security Policy (GCSP)

## What is artificial intelligence?

Artificial intelligence is not new and has been developed since the 1950s when computer scientists rallied around the term at the Dartmouth Conferences in 1956. In the words of the founders of the discipline of artificial intelligence, AI represents the ability of "making a machine behave in ways that would be called intelligent if a human were so behaving". [1] In other words it is the capability of a computer systems to perform task that normally require human intelligence.

For a very long time, AI was not considered seriously because scientific advances were almost inexistent. In the words of Sergey Brin, Google's cofounder, "I didn't pay attention to it (AI) at all. Having been trained as a computer scientist in the 1990s, everybody knew that AI didn't work. People tried it, they tried neural nets and none of it worked." Fast-forward a few years and Brin says that AI now "touches every single one of Google's main projects, ranging from search to photos to ads…everything we do. The revolution in deep nets has been very profound, it definitely surprised me, even though I was sitting right there." [2] If the development of AI is a surprise for specialist, imagine how disruptive it is for policy makers.

Two technological developments brought AI to the fore. Firstly, advances in the miniaturization of transistors, the building blocks of modern computer hardware, have allowed the doubling of the computing power in about every 18 months since the 1960s. This is known as the Moore's law. The size of the current smallest transistors is 14nm with 10nm semiconductors expected this year or in 2018. [3] 5nm seems to be a physical barrier but scientists are already working on bringing this limitation down to 1nm. As a way of comparison, the diameter of human hairs varies from 0.017 to 0.18 millimeters. This represents more than 1000x the size of current transistors.

Secondly, the number of data generated on a daily basis has exploded notably with the emergence of mobile and connected devices. It is estimated that 2.5 exabytes are produced every day. This is the equivalent of 250'000 libraries of Congress or 530'000'000 songs. [4] With the rise of the Internet of Things (IoT) it is estimated that 8.4 billion connected things will be in use worldwide by the end of 2017 and 20.4 billion by 2020. [5] These will generate 44 zetabytes of data which is the equivalent of 5'200 gigabytes for every individuals on earth. [6] By way of comparison, 1 gygabyte can hold the content of about 10 meters of books on a shelf, so 5'200 GB is about 52km of books.

The combination of increasing computing power and data has allowed making some breakthroughs in artificial intelligence notably by the application of machine learning [7] techniques such as artificial neural networks and especially deep learning. Deep learning represents a class of machine learning algorithms that are inspired by our understanding of the biology of our brains. Deep learning processes data through different layers of the neural network where at each step information is extracted. As this learning process is very data intensive, it is only recently with the explosion of big data that it became possible to run massive amounts of data through the system to train it. Thus, major milestone in AI were met recently.

In 2015, Baidu, Microsoft and Google managed to sort million of images with an error rate inferior to 5% which is the typical human error rate. [8] This is all the more remarkable as the best algorithm had an error rate of 28.2 percent in 2010 and is now down to 2.7 percent in 2017. [9] In 2016, Google Deepmind, created the AlphaGo algorithm and beat the second best player of the game of Go in four out of five games. Go is considered as the most complex board game as there are more positions (10p170) than atoms in the universe (10p80). [10] In January 2017, Libratus, an algorithm developed by Carnegie Mellon University, played more than 150'000 hands in no-limit Texas Hold 'Em Poker against four of the best world's human players. In the end, Libratus won $1'776'250. The player who lost the less lost $85'649 and the biggest loser lost $880'087.

The innovation with current algorithms is that unlike Deep Blue that was trained to beat Kasparov at chess though brute computational force to evaluate millions of positions, current algorithms are learning and are general purpose frameworks that can be applied to different issues. For instance, AlphaGo was then used by Google to manage power usage. It reduced by 40 percent the amount of electricity needed for cooling and that translated into a 15 percent reduction in overall power saving. [11 ¨By using reinforcement learning techniques and enough simulations, these algorithms are able to increasingly learn new tasks on their own. [12] Thus, while AlphaGo learned the game by analyzing 30 million Go moves from human players, Libratus learned from scratch. Libratus started by "playing at random, and eventually, after several months of training and trillions of hands of poker, it reached a level where it could not just challenge the best humans but play in ways they couldn't – playing a much wider range of bets and randomizing these bets, so that rivals have more trouble guessing what cards it holds." [13] Both AlphaGo and Libratus ended up playing in a very different way that humans play the game.

Unlike chess board games, poker is a game with incomplete information. Because of the possibility of bluffing at poker, "an AI player has to randomize its actions so as to make opponents uncertain when it is bluffing." [14] There is here no single optimal move. Because of this, Libratus is a milestone in AI as a machine can now out-bluff a human. Moreover, algorithms such as Libratus will be able to play a role with everything from trading to cybersecurity, political negotiations and warfare.

## The Militarization of AI

The militarization of artificial intelligence is translated in increasing autonomy in weapon systems. According to the US Department of Defense, "to be autonomous, a system must

have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation." [15] Autonomous systems can be of two categories: autonomy at rest and in motion: Whereas the former operate virtually such as software, the latter operate in the physical world such as robots or autonomous vehicles. [16] To be fully autonomous, autonomous systems in motion should fulfill three functions. They should move independently through their environment to arbitrary locations; select and fire upon targets in their environment and create and or modify their goals, incorporating observation of their environment and communication with other agents. [17] A recent study by Heather Roff and Richard Moyes of the Global Security Initiative at Arizona State University mapped 256 systems that contain some features of autonomous weapons systems (Figure 1). [18] The study shows that features of mobility (homing and navigation) are those that proliferated the most since they are also the oldest one. Target acquisition and identification technologies are the next technologies as they are a key component of early offensive systems especially air-to-air missiles. Self-engagement technologies such as target image discrimination and loitering are the most recent emerging technologies. Target image discrimination has been boosted by recent improvement in image recognition as mentioned previously. Though this technology is currently on a low number of deployed systems, this feature is prioritized in the development of new weapon systems such as LRASM and TARES. [19]

Loitering technologies are being incorporated in new unmanned aerial vehicles (UAVs) such as nEUROn and Taranis to make them persistent. [20] The combination of target discrimination combined with loitering represents as rightly stated by Roff and Moyes, "a new frontier of autonomy, where the weapon does not have a specific target but a set of potential targets and it waits in the engagement zone until an appropriate target is detected." [21] This represents a step towards offensive autonomous weapons.

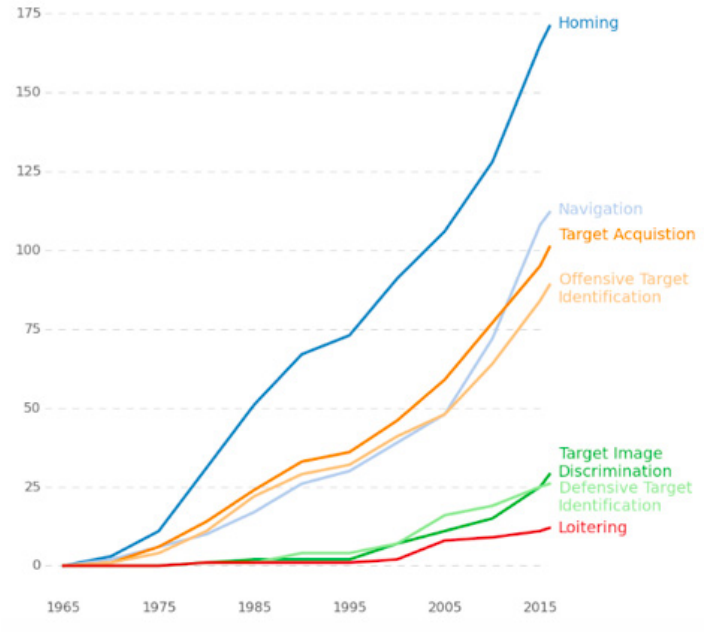



*Figure 1: Development of various autonomous technologies over time (Roff and Moyes) [22]*

These developments demonstrate that although fully autonomous weapons systems do not yet exist, they are probably within less than a generation reach. Indeed, artificial intelligence and the associated technologies of the so-called Fourth Industrial Revolutions are growing exponentially because they "can build on and diffuse over the digital networks" developed by the Third Industrial Revolution. [23] It is therefore crucial to think about their potential impact on international security and warfare. The next part looks at the impact of AWS on strategic stability and proliferation.

## The impact of AWS on strategic stability

One crucial aspect of the development of new weapons for international security is their impact on strategic stability. Strategic stability refers to "the condition that exists when two potential adversaries recognize that neither would gain an advantage if it were to begin a conflict with the other." [24] Strategic stability is neither simple nor static, but should be viewed broadly as a result of effective deterrence.

Throughout history, the major military modes of achieving deterrence has been to build a military force large enough to establish the credibility of threatened punishment if vital interests are impinged upon.

During the Cold War, deterrence was thought of as a mechanism to prevent the opponent's use of nuclear weapons through the threat of retaliation. Maintaining a second strike capability was the cornerstone of the doctrine of Mutual Assured Destruction (MAD) and also the key enabler of strategic stability. Strategic stability was thus achieved by "making sure that each side has enough offensive forces to retaliate after a first strike and it assumes that neither side has the defensive capability to impede the other sides' ability to deliver its devastating retaliatory strike." [25]

Moving beyond the nuclear dimension, deterrence can be more generally defined as "the maintenance of such a posture that the opponent is not tempted to take any action which significantly impinges on his adversary's vital interests". [26] Deterrence therefore relies on maintaining an offense-defense balance, which is in favor of the defense.

It follows that "conflict and war will be more likely when offense has the advantage, while peace and cooperation are more probable when defense has the advantage." [27] An important consideration when it comes to AWS is therefore the likely impact they will have on the offense-defense balance.

With the development of AWS, the threshold for the use of force will likely be lowered and thus favor the offense for two reasons. Firstly, even if the international community manages to impose limitations on targeting - which is debatable if we look at dynamics of contemporary conflict that make civilians, targets of choice - which could be more discriminate indeed, the key problem remains that states will likely exercise less restraint in the use of these weapons because the social cost incurred is lowered by the fact that no human life will be put at risk on the attacker's side. One constraint in the use of AWS is economic. One could argue that the price of these technologies is a significant restraining factor on the propensity of states using and developing them. While at the early stages of development of any technology, the initial cost may be high, however, as has been demonstrated with the development of the computer or digital technologies, the high price of early adopters is greatly reduced over time. The same is likely to be true for AWS, particularly because of the dual-use nature of AI technology, which is primarily driven by the private sector.

Secondly, the offensive nature of these weapons is also strengthened by their likely tactical use, which relies on swarming tactics. The latter relies on overwhelming and saturating the adversary's defense system by coordinating and synchronizing a series of simultaneous and concentrated attacks. Such tactics are aimed at negating the advantage of any defensive posture. In October 2016, the U.S. DoD conducted an experiment where 103 Perdrix micro drones were launched from FA/18 combat aircrafts and were assigned four objectives. In the words of William Roper, director of the Strategic Capabilities Office at the U.S. Department of Defence, the drones shared "one distributed brain for decision-making and adapting to each other like swarms in nature." [28] The drones collectively decided that a mission was accomplished, flew on to the next mission and carried out that one. [29] On 9 February 2017, two teams from Georgia Tech Research Institute and the U.S. Naval Postgraduate School pitted two swarms of autonomous drones against one another. This represented "the first example of a live engagement between swarms of unmanned air vehicles (UAVs). [30] Three days later, on 12 February 2017, China set a

world record when "a formation of 1'000 drones performed at an air show in Guangzhou." [31]

With the use of swarms of AWS it is very likely that the offense-defense balance will shift towards the former. In that case, deterrence will no longer be the most effective way to guarantee territorial integrity. In an international environment that favors the offensive, the best strategy to counter the offensive use of force is one that relies on striking first. It follows that strategies of pre-emption are very likely to become the norm if AWS are becoming the weapons of choice in the future. Striking first before being attacked will provide a strategic advantage. The concept of pre-emption, however, is a clear violation of the current international regime on the use of force, which relies on self-defense and authorization granted by the UN Security Council and falling under the Chapter VII of the UN charter.

Another consequence of favoring offense is the greater likelihood of international arms races.

As mentioned above, the ability to strike first represents a strategic advantage. In order to deny the adversary's ability to do the same, states are very likely to invest and improve current AWS technology. This, in turn, is likely to initiate an arms race. We can already observe this dynamic at play. Last year, for instance, the Defense Science Board of the U.S. Department of Defense released its first study on autonomy. The report stated that "autonomous capabilities are increasingly ubiquitous and are readily available to allies and adversaries alike. The study therefore concluded that DoD must take immediate action to accelerate its exploitation of autonomy while also preparing to counter autonomy employed by adversaries. (…) Rapid transition of autonomy into warfighting capabilities is vital if the U.S. is to sustain military advantage." [32]

AI and autonomy are seen pivotal technologies of the U.S. Third Offset strategy to secure military advantage over China and Russia. These two powers as well lesser one have also increasingly invested in autonomous weapons technologies. In August 2016, the state-run China daily reported that the country had embarked on "the development of cruise missile systems with a "high level" of artificial intelligence to counter the US Navy LRASM. [33] At the 2017 Russian Army Expo, Yermak, a fully automated, AI-powered anti-aircraft defence system was unveiled. [34] Russian famous AK-47 company, Kalashnikov, also recently announced that they are building "a range of products based on neural networks, including a fully automated combat module that can identify and shoot at its target." [35] This is in line with President Putin recent remarks that "the one who becomes the leader in this sphere (i.e. AI) will be the ruler of the world." [36]

When developing AWS, states and the international community should very carefully think about the consequences of this technology also falling into the hands of radical terrorist groups such as the Islamic State (ISIS). These groups massively rely on suicide bombings for tactical (breaching a front line, for instance) and strategic purposes (shocking the international community). The acquisition of AWS by these groups would act as a massive force multiplier as they could use the same suicide bombing tactics but with a greater concentration of mass (since they would rely on more machine acting as "suicide bombers").

The vertical proliferation of autonomous weapons systems to non-state actors will potentially democratise the access to the use of military force. As mentioned in a study by the Harvard Kennedy School Belfer Center [37], the commercial AI industry concentrates most of AI advances. Beyond the issues of double-use technologies, commercial applications become increasingly widely available with time passing. In addition, the cost of replicating algorithms, which are lines of codes, is almost non-existent. Thus, scenarios where violent non-state actors such as ISIS, terrorist groups or criminal organisations could acquire AWS on black markets, or by building their own cannot be excluded. [38] Current developments in the weaponization of drones are an indicator supporting this possibility. [39]

## Conclusions

Although autonomous weapons systems do not yet exist, the intended impact of these weapons on international security has the potential to be very destabilizing for the international system be it because it can upset the strategic balance and favor an offensive defense posture favoring pre-emptive strategies or because these technologies could be used beyond their intended limitations shall they fall into the hands of non-state actors or terrorist organizations. The international community – not only limited to the United Nations but also the AI industry players and scientific community – shall therefore be very vigilant about not granting too much power and autonomy to weaponised robots and algorithms as the consequences might well be dystopian.


### Dr. Jean-Mark Rickli

He is the head of global risk and resilience at the Geneva Centre for Security Policy (GCSP). He is also a research fellow at King's College London, where he was an assistant professor at the Department of Defence Studies, and a non-resident fellow in modern warfare and security at TRENDS Research and Advisory in Abu Dhabi. He is a senior advisor for the AI (Artificial Intelligence) Initiative at the Future Society at Harvard Kennedy School and an expert on autonomous weapons systems for the United Nations and for the United Nations Institute for Disarmament and Research (UNIDIR). Dr. Rickli received his PhD and MPhil in International Relations from Oxford University, UK, where he was also a Berrow scholar at Lincoln College.


## Literature


[1] McCarthy, John et al. (1955). "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence" 31 August, http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html

[2] Chainey, Ross (2017). "Google Co-Founder Sergey Brin: I Didn't See AI Coming," World Economic Forum, 19 January, https://www.weforum.org/agenda/2017/01/google-sergey-brin-i-didn-t-see-ai-coming/

[3] Galeon, Dom (2016). "Nevermind Moore's Law: Transistors Just Got a Whole Smaller,", Futurism, 8 October, https://futurism.com/nevermind-moores-law-transistors-just-got-a-whole-lot-smaller/

[4] Khoso, Mikal (2016). "How Much Date is Produced Every Day," Northeastern University, 13 May, http://www.northeastern.edu/levelblog/2016/05/13/how-much-data-produced-every-day/

[5] EGHAM (2017), "Gartner says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", Gartner, 7 February 2017: http://www.gartner.com/newsroom/id/3598917

[6] 1 zettabyte is approximately 1'000 exabytes. 1 exabyte is 1'000 petabytes and 1 petabytes is 1'000'000 gigabytes. 1 gygabyte can hold the content of about 10 meters of book a shelf, see http://whatsabyte.com, See also, Mearian, Lucas (2012). "By 2020 there will be 5'200 GB of data for every person on Earth", Computer World, 11 December, http://www.computerworld.com/article/2493701/data-center/by-2020--there-will-be-5-200-gb-of-data-for-every-person-on-earth.html

[7] Machine learning is "the practice of using algorithms to parse data, learn from it and then make a determination or prediction about something in the world." Copeland, Michael (2016). "What is the Difference Between Artificial Intelligence, Machine Learning and Deep Learning?" NVidia Blog, 29 July, https://blogs.nvidia.com/blog/2016/07/29/

whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/
[8] Hern, Alex (2015). "Computers Now Better than Human at Recognizing and Sorting Images," The Guardian, 13 May, https://www.theguardian.com/global/2015/may/13/baidu-minwa-supercomputer-better-than-humans-recognising-images
[9] Gershgorn, Dave (2017). "The Data That Transformed AI Research – and Possibly the World," Quartz, 26 July, https://qz.com/1034972/the-data-that-changed-the-direction-of-ai-research-and-possibly-the-world/
[10] Lei, Leon (no date). "Go and Mathematics", The American Go Foundation http://agfgo.org/downloads/Go%20and%20Mathematics.pdf
[11] Vincent, James (2016). "Google Uses Deepmind AI to Cut Data Center Energy Bills", The Verge, 21 July, https://www.theverge.com/2016/7/21/12246258/google-deepmind-ai-data-center-cooling
[12] Metz, Cade (2017). "Google's Alphago Levels Up From Board Games to Power Grids", Wired, 24 May, https://www.wired.com/2017/05/googles-alphago-levels-board-games-power-grids/
[13] Metz, Cade (2017). "Inside Libratus, the Poker AI that Out-Bluffed the Best Humans", Wired, 2 January, https://www.wired.com/2017/02/libratus/
[14] Metz, Cade (2017). "Inside Libratus, the Poker AI that Out-Bluffed the Best Humans", Wired, 2 January, https://www.wired.com/2017/02/libratus/
[15] Defense Science Board (2016). Summer Study on Autonomy. Washington, Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics June, p. 4.
[16] Defense Science Board (2016). Summer Study on Autonomy. Washington, Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics June, p. 5.
[17] Roff, Heather and Moyes, Richard (2016). "Autonomy, Robotics and Collective Systems", Global Security Initiative, Arizona State University, https://globalsecurity.asu.edu/robotics-autonomy
[18] Roff, Heather and Moyes, Richard (2016). "Autonomy, Robotics and Collective Systems", Global Security Initiative, Arizona State University, https://globalsecurity.asu.edu/robotics-autonomy
[19] LRASM is a stealthy long range anti-ship cruise missile developed in the United States while TARES (Tactical Advanced Recce Strike) is an unmanned combat air vehicle (UCAV) for standoff engagement developped by the German firm Rheinmetall.
[20] The nEUROn is an experimental stealthy, autonomous UCAV developped by an international cooperation led by French Dassault. Taranis is a British demonstrator programme for stealthy UCAV technology developed by BAE which first flew in 2013.
[21] Roff, Heather and Moyes, Richard (2016). "Autonomy, Robotics and Collective Systems", Global Security Initiative, Arizona State University, https://globalsecurity.asu.edu/robotics-autonomy
[22] Roff, Heather and Moyes, Richard (2016). "Autonomy, Robotics and Collective Systems", Global Security Initiative, Arizona State University, https://globalsecurity.asu.edu/robotics-autonomy
[23] Schwab, Klaus (2017). Shaping the Fourth Industrial Revolution: Handbook for Citizens, Decision-Makers, Business Leaders and Social Influencers, Geneva, World Economic Forum, p. 15 (forthcoming).
[24] Hildreth, Steven and Woolf, Amy. F (2010). Ballistic Missile Defence and Offensive Arms Reductions : a Review of the Historical Record. Washington : Congressional Research Service, p. 4.
[25] Hildreth, Steven and Woolf, Amy. F (2010). Ballistic Missile Defence and Offensive Arms Reductions: a Review of the Historical Record. Washington: Congressional Research Service, p. 7. When security is achieved through deterrence by punishment "the ability to retaliate supports a defensive strategy, while the ability to deny retaliatory capabilities, that is, to limit damage, could support and offensive strategy". MAD therefore is defense-dominant as retaliatory capabilities dominate damage limitation capabilities. Glaser, Charles L. (2014). Analyzing Strategic Nuclear Policy. Princeton: Princeton University Press, pp. 106-107, see also, Jervis, Robert (1978). "Cooperation under the Security Dilemma," World Politics, vol. 30, no. 2, January, pp. 206-210.
[26] Amoretta M Hoeber (1968): "Strategic Stability," Air University Review, July-August, http://www.airpower.maxwell.af.mil/airchronicles/aureview/1968/jul-aug/hoeber.html
[27] Sean M. Lynn-Jones (1995). "Offense-Defense Theory and Its Critics", Security Studies, vol. 4, no. 4, p. 691.
[28] U.S. DoD (2017). "Department of Defense Announces Successful Micro-Drone Demonstration" U.S. Department of Defense, 9 January, https://www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/
[29] Mizokami, Kyle (2017). "The Pentagon's Autonomous Swarming Drones are the Most Unsettling Thing You'll See Today." Popular Mechanics, 9 January, http://www.popularmechanics.com/military/aviation/a24675/pentagon-autonomous-swarming-drones/
[30] Toon, John (2017). "Swarms of Autonomous Aerial Vehicles test Dogfighting Skills" Georgia Tech News Centre, 21 April, http://www.news.gatech.edu/2017/04/21/swarms-autonomous-aerial-vehicles-test-new-dogfighting-skills
[31] Le Miere, Jason (2017). "Russia Developing Autonomous "Swarm" of Drones in New Arms Race with U.S., China." Newsweek, 15 May, http://www.newsweek.com/drones-swarm-autonomous-russia-robots-609399
[32] Defense Science Board (2016). Summer Study on Autonomy. Washington, Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics June, pp. iii and 3.
[33] Markoff, John and Rosenberg, Matthew (2017). "China's Intelligent Weaponry Gets Smarter," New York Times, 3 February, https://www.nytimes.com/2017/02/03/technology/artificial-intelligence-china-united-states.html?mcubz=0
[34] Jotham, Immanuel (2017). "Russian Army Expo 2017: Autonomous Anti-Aircraft Missile System Unveiled," International Business Times, 28 August, http://www.ibtimes.co.uk/russian-army-expo-2017-weapons-maker-tikhomirov-unveils-new-autonomous-anti-aircraft-missile-system-1636920
[35] Tucker, Patrick (2017). "Russian Weapons Maker to Build AI-Directed Guns," DefenceOne, 14 July, http://www.defenseone.com/technology/2017/07/russian-weapons-maker-build-ai-guns/139452/
[36] Associated Press (2017), "Putin: Leader in artificial intelligence will rule world", The Washington Post, 1 September: https://www.washingtonpost.com/business/technology/putin-leader-in-artificial-intelligence-will-rule-world/2017/09/01/969b64ce-8f1d-11e7-9c53-6a169beb0953_story.html?utm_term=.1aed353f12ac
[37] Allen, Greg and Chan Taniel, (2017). Artificial Intelligence and National Security, Harvard Kennedy School Belfer Center Study for Science and International Affairs, July: http://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf
[38] Horowitz C. Michael (2016). "Who'll want artificially intelligent weapons? ISIS, democracies, or autocracies?" Bulletin of the Atomic Scientists, 29 July: http://thebulletin.org/who%E2%80%99ll-want-artificially-intelligent-weapons-isis-democracies-or-autocracies9692
[39] Warrick Joby (2017) "Use of weaponized drones by ISIS spurs terrorism fears" The Washington Post, 21 February: https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?utm_term=.a64b5f10e771

# Why Quantum Technologies Matter in Critical Infrastructure and IoT

**As devices and systems in our critical infrastructures become ever more interconnected, it is increasingly important to ensure that they have adequate cryptographic protections. This is particularly challenging – yet even more essential – given the potential scalability of the attack vectors in this hyper-connected world. Action is required now, both to ensure current security, but also to prepare upgrade paths for future technology advances. This paper reviews how the emergence of new quantum technologies will impact IoT cryptographic security - both creating in new threat vectors, such as a quantum computer, as well as providing some immediate solutions.**

**Keywords:** **Quantum technologies, cryptography, critical infrastructure, internet of Things, photonics, random number generation**

**Author:** **Kelly Richdale**, ID Quantique SA

## Introduction

Such systems and assets have developed into a networked Internet of Things, where machines talk to machines and devices to devices without human interaction. This is already the case for Supervisory Control and Data Acquisition (SCADA) and industrial control systems (ICS) which are moving online and towards modern standardized networking protocols. Examples include the electricity grid and train networks, where commands can now be sent over open transmission networks using IP-based protocols, such as MPLS; or the connections to smart meters deployed in millions of homes; or to the devices underpinning smart cities; or in the future to the millions of smart cars driving autonomously on our roads which depend on embedded IoT devices.

Such hyper-interconnected infrastructures present new defense challenges:

- Rapid advancements in technology will add new attack vectors which were not conceived of or which were not feasible at the time that the devices were originally deployed – especially given the long field lifetimes of critical infrastructure devices
- The scalability of the attack vectors is unprecedented, where a single successful hack could affect millions of devices [2]. So far such attacks have been relatively benign, but this could change. This means that many previously isolated or siloed systems and devices forcibly become part of a networked critical infrastructure. For example, in the past, if one car crashed it was a matter for the police and possibly an ambulance. However, in the world of ubiquitous IoT, if a hack can cause an entire smart city infrastructure to fail, or the entire self-driving car or rail network to go down, then it becomes an issue of national security [3].

## Crypto Security Requirements

Many of the core requirements for security of modern critical infrastructures depend on cryptographic primitives. Clearly, cryptography is only a part of the whole but for the purposes of this paper, we will consider specifically the implications of the emergence of new quantum technologies on the cryptographic primitives - in the context of both creating new threat vectors, as well as providing some solutions. And the cryptography is crucial - If the underlying crypto primitives fail, then the security of the device(s) and the network fail as well.

The US Department of Homeland Security [4] (DHS) recommends certain key tenets for what they term "Life Critical Embedded Systems" which neatly summarise the ubiquity of cryptography in machine to machine security.

- All interactions between devices MUST be mutually authenticated
- Continuous authentication SHOULD be used when feasible and appropriate
- All communications between devices SHOULD be encrypted
- Devices MUST NEVER trust unauthenticated data or code during boot-time
- Devices MUST NEVER be permitted to run unauthorised code
- Devices SHOULD NEVER trust unauthenticated data during run-time
- When used, cryptographic keys MUST be protected

Moreover, the report goes on to state that devices and systems MUST be built to include mechanisms for in-field update, and that devices and systems for managing updates MUST be mutually authenticated and secured: "Threat models must recognize that some systems will need to be in place for decades, while others may refresh annually or more frequently….. Life critical embedded systems should be engineered to include enough compute capacity for stronger cryptographic and runtime protections that will need to be added within the lifetime of the systems."

However, in-field update mechanisms may also bring about new attack vectors, as an attacker, who manages to enter the system will be able to update it according to their needs.

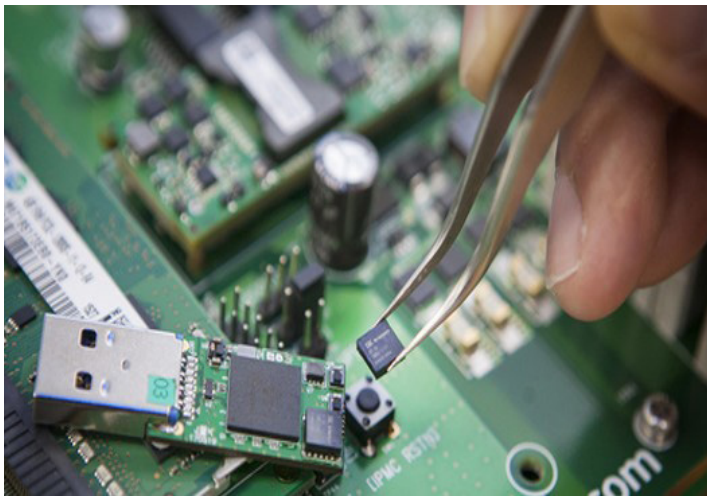


*Figure 1: New Photonics IoT QRNG (5x1x1mm)*

## Quantum Threats to Today's Cryptography

Recent breakthroughs in quantum computing have brought about a credible threat to the widely used cryptographic primitives which underpin our infrastructures and networks – notably to public key cryptography, such as RSA, Elliptic Curve Cryptography & Diffie Hellmann. Scientists have known about this threat since 1994 when a mathematician, Peter Shor, published his now-famous quantum algorithm for factoring large numbers into primes and finding discrete logarithms much faster than any classical algorithm. These are precisely the mathematical problems underpinning the above-mentioned primitives. A quantum computer running Shor will therefore break all the cryptographic systems based on these primitives.

The exponential speed-up brought about by quantum computers stems from the fact that they act as massively parallel computers. This is made possible by a weirdness of quantum mechanics known as "superposition". Crudely put, it is the ability for a quantum bit (or qubit) to be both a one and a zero at the same time. Properly implemented (and this is by no means an easy task), this weird property extends to any numbers of qubits. Ultimately, the whole quantum computer can now be in a superposition state, which provides exponential computing power.

And quantum computers already exist – albeit with a restricted number of qubits. IBM has launched the first quantum computing cloud, which allows external users to experiment with a small number of qubits [5]. Google has set itself a target for proving quantum supremacy (the ability of a quantum computer to resolve certain problems faster than the best available conventional processors ) by the end of 2017 [6]. D-Wave was the earliest to market and has already launched its 2000Q System quantum computer which - luckily for today's security – uses a quantum computing process which cannot run Shor's algorithm.

So the question is: when will a universal quantum computer run Shor's algorithm (or any variation thereof) on enough qubits to be able to break today's crypto primitives? One estimation is provided by Dr Michele Mosca from the Institute for Quantum Computing in Canada, who also runs a quantum risk assessment practice [7]: he estimates that large-scale quantum computing is 10-15 years away, and that there is a 1 in 7 chance of crypto primitives being affected by quantum attacks in 2026, and a 1 in 2 chance by 2031.

This may sound a long time away, but given the timescales for developing and deploying many critical infrastructure devices – which are often in the field for 20+ years, it would be prudent to start preparations now.

## Quantum-Era Solutions for Quantum-Safe Security

New cryptographic techniques have emerged in recent decades that do provide protection against quantum threats. These techniques are termed "quantum-safe" and consist of both techniques based on quantum properties of light that prevent interception of messages (Quantum Key Distribution or QKD [8], as well as new algorithms (known as Quantum Resistant Algorithms) that are resistant to known quantum attacks, like Shor's. Quantum technologies can also be used to improve the overall safety of critical infrastructure by improving cryptographic key generation. The devices are known as Quantum Random Number Generators, or QRNGs.

## Hardware Protections & Key Generation

While the algorithms in devices may be upgraded remotely, the hardware aspects of the device must be secure from the outset, unless they are recalled physically for upgrade. Mission critical devices often have long lifetimes in the field – stretching over decades – so the hardware must be adapted or adaptable to counter future threats. This is particularly relevant for the multitude of field-deployed devices, where cost and size is a major factor and which today are frequently deployed without any of the required security protections or upgrade paths. Again, while individually each device, sensor or actuator may not present a major threat, a single hacked device may provide an entry point to the whole system. Therefore, critical systems should already have implemented strong cryptographic protocols on all their components, with enough computing capacity built in for this to be upgraded in the future to address new crypto primitives and runtime protections.

Another aspect fundamental to security is the random number generator (RNG), essential to all crypto operations. Generating strong keys, based on true randomness, is the cornerstone of security – good keys must be unique, unpredictable and truly random. Having strong crypto algorithms with weak keys is akin to putting a huge padlock on your front door and then hiding the key under the mat [9]. Software-based RNGs are not sufficient, as the computer programs they run are purely deterministic and cannot generate true randomness without external entropy sources. Since many critical infrastructure and IoT deployments are in isolated locations with limited external interaction, such sources of external entropy are limited.

Therefore RNGs should be based on hardware, and the resulting crypto key should also be protected in hardware. This need for hardware-based root of trust, and hardware protection of the keys is recognized also in the DHS recommendations, which state "Ideally life critical embedded systems would include a hardware root of trust and system integrity, as without such system hardening, updates could be unreliable or untrustworthy."

Moreover in critical infrastructures RNGs need to be able to withstand the extremely harsh environments in field deployments often over many decades without losing quality of the randomness. They should not degrade with time, and they need to withstand extremes of temperature, vibrations, and electromagnetic noise. Photonics-based quantum random numbers generators (QRNG) meet these requirements well. Firstly quantum systems are intrinsically random, and therefore do not need to accumulate entropy to generate secure keys – every bit has what is termed "full entropy". This is important to ensure adequate security during boot time and for the first trusted handshake with other devices. Secondly, photons (single light particles) are more resilient to external influences, such as heat and electromagnetic signals than other types of thermal-noise based RNGs . Photonics-based QRNGs are already used for transport encryption of critical infrastructures by vendors, such as ABB [10], and a next generation of low cost, miniaturized QRNGs meet the requirements for widespread field-based deployments of IoT devices [11].

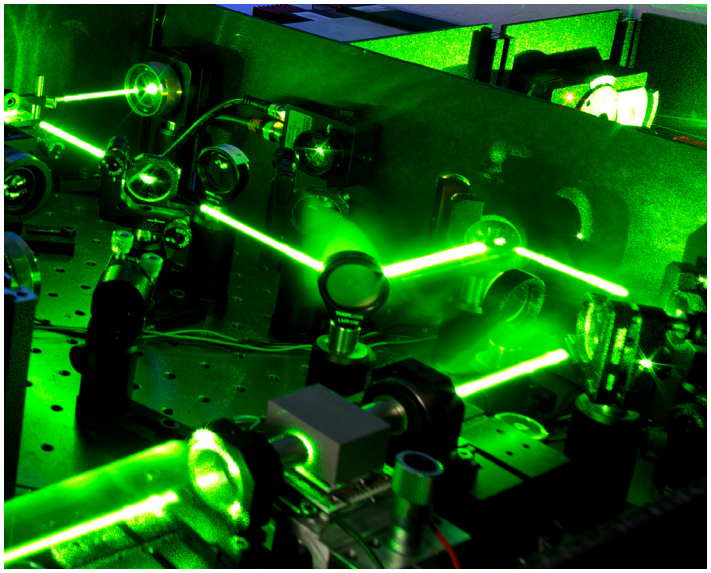


*Figure 2: Photonics principles in the laboratory*

## Quantum Key Distribution

Wide-scale QKD is already being deployed on transport networks to provide quantum-safe protection to critical infrastructures in countries such as China. However, QKD is not yet adapted for edge or hyperconnected networks. Applications of QKD are currently restricted to specific cases, such as highly critical links between major infrastructure components rather than IoT field deployments. Therefore we will focus currently on the two key components for a quantum-safe solution in the IoT world – the secure key generation mechanism above, and Quantum Resistant Algorithms below.

## Quantum-Resistant Algorithms

Quantum Resistant Algorithms (also known as Post Quantum Cryptography) refer to cryptographic primitives (such as lattice-base or code-based), that are thought to be secure against an attack by a quantum computer, or at least against known attacks such as Shor's.

Since such algorithms are not provably secure from a mathematical perspective (unlike QKD), they must be rigorously tested and analysed before being deployed. NIST, the American National Institute for Standards and Technology, has launched a solicitation and evaluation process [12] with the goal to standardize on one or more quantum resistant public key crypto algorithm. The process will take at least 5 years.

What is clear is that – while such quantum resistant algorithms are not yet ready for deployment – manufacturers and users must already start to prepare by implementing crypto-agility into their devices and systems today, so that these may be securely upgraded in a timely manner as the threat to today's asymmetric algorithms becomes relevant.

## Recommendations

In summary, the recommendations come in two different categories: Prepare Now, and Act Now.

*Prepare Now*:

- Understand and document the threat models which might affect your critical infrastructure deployments, including dependencies resulting from high interconnectivity between devices and (your and third party) systems.
- Build a process for continual evaluation for such threat models as new technologies and attack vectors emerge, based on an estimation of the lifecycle and field deployment conditions, as well as expected renewal rates.
- Prepare for the upcoming quantum era by investigating the impact of quantum technologies upon your devices, systems and deployment. Conduct a quantum risk assessment, specifically for the trust models based on cryptographic primitives, and how this will impact your devices and systems.

*Act Now*:

- Build crypto agility into your devices, systems and deployments to ensure an upgrade path in the future. Ensure the ability to conduct remote upgrades in a secure, timely and pro-active manner.
- Build hardware devices and systems with a view to long term security in the field, and notably with:
  - Spare computing power able to support upgraded crypto primitives and run time protections, and
  - Hardware based key generation for adequate security of cryptographic operations throughout the lifetime of the device, ideally based on quantum photonics for re silience to environmental influences.
- Demand these same security criteria from your suppliers and everyone in the value chain bringing your systems into field deployment.


### Kelly Richdale

heads the Quantum Safe Security division of ID Quantique SA. She has 20 years experience in the security industry, focusing on cryptography, network security, identity management and strong authentication solutions. Ms. Richdale is a qualified CISSP and president of the Swiss ISC2 chapter. She holds an MBA from INSEAD and a masters degree from Cambridge University. She is a member of the Innovation Council of Innosuisse, and of the advisory boards of the UniGE Infosec course and EPFL's Management of Technology course.


## References


[1] http://www.babs.admin.ch/en/aufgabenbabs/ski.html Nationale Strategie zum Schutz kritischer Infrastrukturen, 17.06.2012

[2] https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

[3] For this reason in the paper it is considered that ultra-networked IoT devices in certain industries form part of the nation's critical infrastructure, and the terms IoT and critical infrastructure are used interchangeably.

[4] DHS Security Tenets for Life Critical Embedded Systems https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

[5] https://www.forbes.com/sites/aarontilley/2017/03/06/ibm-quantum-computing-cloud/#b6b65e877a2c

[6] https://www.newscientist.com/article/2138373-google-on-track-for-quantum-computer-breakthrough-by-end-of-2017/

[7] http://globalriskinstitute.org/publications/3423-2/

[8] For more information on QKD see http://www.idquantique.com/quantum-safe-crypto/qkd-overview/

[9] A more scholarly version of this example is stated in Kerckhoff's principle: "A cryptosystem should be secure even if everything about the system, except the key, Is public knowledge". This encapsulates the importance of the encryption key in crypto systems.

[10] See the SECU1 Encryption card by ABB: http://new.abb.com/network-management/communication-networks/optical-networks/mission-critical-communications/security

[11] http://www.idquantique.com/random-number-generation/

[12] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

# Sécurité, défense et l'Internet des objets: entendons ce que 1000 étudiants suisses ont à dire à ce sujet

**L'intelligence ambiante permet d'imaginer un très grand nombre d'innovations mais elle comporte aussi des risques. Au-delà des experts, les citoyens ont un véritable rôle à jouer. Connaître leurs comportements et leurs pratiques est essentiel. Pendant cinq mois, de septembre 2016 à janvier 2017, une étude a été menée en Suisse occidentale auprès de 1000 étudiants pour explorer les futurs possibles de l'intelligence ambiante en Suisse. L'utilisation de Futurescaper, une plateforme à destination d'organisations engagées avec leurs parties prenantes dans des activités de prospective participative, a permis de dégager plusieurs éléments de discussion autour des questions suivantes: quels sont les futurs possibles de l'intelligence ambiante en Suisse et comment entreprises, administrations publiques et individus peuvent-ils agir dès à présent pour saisir les opportunités et faire face aux menaces qui lui sont liées?**

**Mots clés:** **Intelligence ambiante, prospective, Suisse occidentale, production collaborative**

**Auteurs:** **Prof. Thomas Gauthier**, HEG-Genève & emlyon; **Dr. Sylvaine Mercuri Chapuis**, ESDES, The Business School of Ucly

## Introduction

L'«intelligence ambiante», le système constitué par l'ensemble des objets connectés (ordinateurs, tablettes, montres et bracelets connectés etc.) et capables d'analyser rapidement les données qu'ils enregistrent, permet aux individus d'accéder à l'information plus simplement, «la proactivité de l'environnement venant alléger la charge cognitive que l'usager doit actuellement mobiliser pour accéder à cette information via des ordinateurs» (Entretien, 2009; p. 482). L'intelligence ambiante permet d'imaginer un très grand nombre de nouvelles applications et de nouveaux services mais elle comporte aussi des risques, en particulier dans le domaine de la sécurité et de la défense informatique. Face à des hackers de tous horizons, la protection des données sensibles est indispensable et elle doit faire l'objet d'une attention permanente autant d'un point de vue individuel que collectif. Les derniers scandales en date, celui de la cyberattaque du 12 mai 2017 via le virus «Wannacry» qui a touché plus de 150 pays dans le monde, infectant plus de 200 000 ordinateurs (seulement 200 en Suisse) (Le Temps, 2017) ou celui de la cyberattaque du 27 juin 2017, impliquant plusieurs multinationales européennes et américaines ainsi que des structures gouvernementales ne sont qu'une illustration de ce qui pourrait se multiplier à l'avenir. Pour assurer la protection de leur vie privée, les individus doivent redoubler de vigilance et ils sont les premiers à jouer un rôle. En 2016, dans son rapport semestriel sur la sureté de l'information, la Confédération Suisse, réalisant un état des lieux sur le plan international, indiquait que la barre des 20 milliards d'objets connectés (contre 6 milliards à cette époque) devrait être franchie d'ici 2020 [1] . Elle indiquait également que la vulnérabilité de l'Internet des objets tenait «surtout à la culture de sécurité» (p. 8) des fabricants et des utilisateurs des objets communicants. A la lecture de ce rapport, on comprend qu'il s'agit alors d'agir sur les cultures qui coexistent aujourd'hui afin de définir de bonnes pratiques individuelles et collectives qui permettraient de développer une «bonne» culture de la sécurité (Chevreau et Wybo, 2007). En s'intéressant aux valeurs, aux normes ou aux symboles partagés et qui sont supposés être liés à la sécurité, il s'agit de mobiliser au-delà des experts, un collectif plus large, l'ensemble des citoyens, premiers vecteurs de risque, qui ont ici un véritable rôle à jouer.

Une réflexion autour de leurs comportements et de leurs pratiques est alors indispensable. Elle permet notamment une sensibilisation voire une prise de conscience, permettant de stimuler des comportements plus vigilants. De manière à faciliter ce changement, le recours à des activités de prospective est intéressant car celles-ci consistent pour n'importe quel individu, compte tenu de tendances lourdes et de signaux faibles perceptibles dans son environnement et qui sont d'ordres politique, économique, socioculturel, technologique, écologique ou encore légal, à imaginer des scénarios d'avenir plausibles pour faciliter sa prise de décision et son action. Ainsi, plutôt que d'anticiper des changements prévisibles pour mieux s'y préparer et en tirer parti (notion de préactivité), l'individu cherchera à provoquer les changements souhaités par des actions spécifiques (notion de proactivité) (Godet et Durance, 2011). Cette différence est notable car l'action individuelle et collective change de statut : elle est perçue de manière plus positive par les individus car ils sont responsables de l'avenir qu'ils contribuent à façonner à travers les actions qu'ils entreprennent.

Pour mener une réflexion plus large, la question suivante peut être posée : quels sont les futurs possibles de l'intelligence ambiante en Suisse et comment entreprises, administrations publiques et individus peuvent-ils agir dès à présent pour saisir les opportunités et faire face aux menaces qui lui sont liées ? De manière à répondre à cette question, une étude a été menée entre septembre 2016 et janvier 2017 auprès de près de 1000 étudiants en Suisse occidentale. A cette occasion, Futurescaper, une plateforme créée en 2011 à Londres par Noah Raford et Nathan Koren, a été utilisée.

## Futurescaper, animer la réflexion collective et prospective

Depuis 2011, la plateforme Futurescaper est utilisée pour animer de nombreuses réflexions prospectives. Il s'agit d'imaginer des solutions futures avec plusieurs participants à même d'apporter des contributions et des éclairages significatifs sur des situations précises. Il s'agit aussi de rendre l'action individuelle plus qualitative en favorisant une dynamique intellectuelle permanente.

Développée par deux diplômés du MIT et de l'Université d'Oxford, la plateforme Futurescaper propose de suivre une série de quatre étapes: la préparation du projet (étape 1), l'engagement des parties prenantes (étape 2), l'interprétation et l'analyse (étape 3) et la restitution et la présentation des résultats (étape 4). Les réflexions autour de l'environnement correspondent au point de départ pour définir des scénarios plausibles, qui sont non figés et qui permettent de prendre des décisions immédiates (Godet, 2004). Cette manière de fonctionner permet de caractériser la plateforme Futurescaper comme une véritable innovation incrémentale car son ingénierie permet d'aller au-delà de raisonnements causaux en créant une réticulation de la pensée entre plusieurs participants.

Les contributions vers lesquelles la plateforme Futurescaper oriente sont quant à elles d'ordre qualitatif (Figure 1) car il s'agit d'imaginer collectivement des tendances, les conséquences de ces tendances, et les conséquences de ces conséquences. Elle facilite une réflexion collective qui permettra ensuite aux participants de proposer des combinaisons nouvelles, des scénarios, dans lesquels figureront des opportunités et des

menaces à saisir ou à éviter. Compte tenu de ces opportunités et menaces, les participants pourront alors s'exprimer sur les attitudes à avoir pour changer ou pour poursuivre le scénario qu'ils imaginent. Les participants sont force de proposition car ils verbalisent des pistes d'actions compte tenu de tendances qu'ils n'auraient peut-être pas identifiées individuellement.

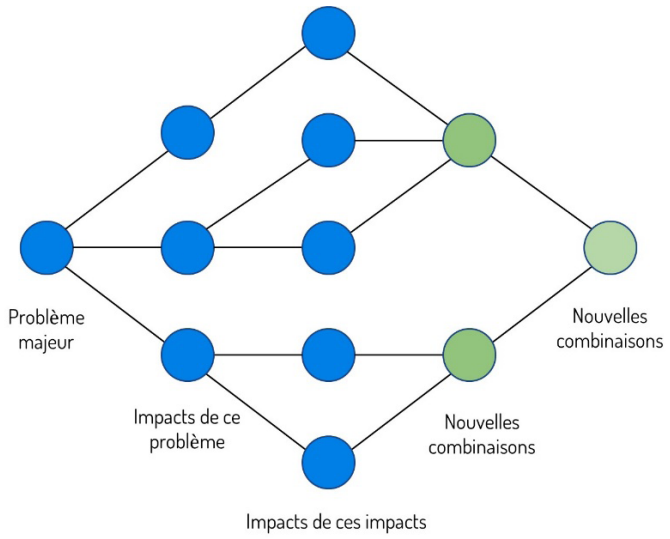



*Figure 1: Contributions obtenues en utilisant la plateforme Futurescaper*

## Déterminer les futurs possibles de l'intelligence ambiante en Suisse

Entre septembre 2016 et janvier 2017, près de 1000 étudiants de Suisse occidentale ont été sollicités pour participer à une démarche de production collaborative (crowdsourcing). Les étudiants préparant un Bachelor ou un Master étaient issus de filières économiques et de gestion mais aussi de filières d'ingénierie, d'art et de design [3] . Lors d'une séance de 45 minutes environ, dans leur classe habituelle (de 10 à 80 étudiants), une intervenante préalablement identifiée par le directeur de l'étude commençait par diffuser une vidéo de présentation de l'intelligence ambiante. Les participants étaient ensuite interrogés de manière ouverte sur leur connaissance du sujet puis trois exemples leur étaient proposés : les véhicules autonomes, les drones et la montre connectée d'Apple, l'Apple Watch. L'intervenante indiquait ensuite une adresse Internet à laquelle les participants étaient invités à se rendre afin de participer à l'étude. Elle les informait que d'autres classes avaient été interrogées en amont et que les réponses d'autres étudiants étaient déjà enregistrées et visibles sur la plateforme. A partir de là, les participants étaient invités à répondre à cinq questions:

- quelles tendances associez-vous à l'intelligence ambiante? (question 1), les tendances peuvent être politiques, économiques, sociales, technologiques, écologiques ou juridiques, veuillez choisir de 1 à 3 éléments (consigne 1);
- quelles pourraient être les conséquences directes de la/des tendance(s) lambda (il y a ici une personnalisation de la/des tendance(s) compte tenu de la réponse faite à la question 1)? (question 2), veuillez choisir de 1 à 3 tendances (consigne 2);
- quelles pourraient être les conséquences directes de votre réponse ci-dessus? (question 3), vous devez entrer de 1 à 3 réponses pour chaque tendance (consigne 3);
- quelle opportunité ou menace vous paraît la plus importante? (question 4), vous devez ajouter un élément (consigne 4);
- afin de saisir cette opportunité ou faire face à cette menace, que devraient faire dès à présent... Les entreprises?... Les administrations publiques?... Les individus? (question 5).

Au moment de la préparation de l'étude (étape 1), 52 tendances tirées de documents identifiés sur le web ont été préenregistrées sur la plateforme Futurescaper. Des articles de presse, des études scientifiques ou professionnelles, des articles de blogs, et d'autres documents ont été identifiés puis analysés pour alimenter cette étape. C'est uniquement lorsque l'information contenue dans ces documents est arrivée à saturation [4] que le directeur de l'étude a consenti à passer à l'étape d'engagement (étape 2). À l'issue des étapes 2 et 3, les tendances étaient au nombre de 337.

La tendance «baisse de la protection de la vie privée» est celle qui a suscité le plus de recommandations (43 précisément). Trois autres tendances sont également à relever: la tendance «baisse de l'intelligence humaine» a suscité 25 recommandations, la tendance «hausse de l'addiction et de la dépendance aux objets connectés» en a suscité 21 et la tendance «hausse des cyberattaques et des piratages» en a suscité 15.

## Sécurité et défense à la rencontre de l'Internet des objets, explorer les futurs possibles pour agir aujourd'hui

Le travail de production collaborative a permis d'identifier de nombreuses tendances originales (Tableau 1) qui sont venues compléter celles qui avaient été pré-enregistrées sur la plateforme Futurescaper (Tableau 2) avant le début de l'étude.

| | |
|---|---|
| **Politique** | Chômage |
| **Economique** | Flux d'information, télétravail, nombre d'emplois, interactions machine/machine, performance logistique, automatisation, décisions prises directement par les machines et les objets, qualité du travail |
| **Social** | Interactions humaines, temps libre disponible, maintien et suivi à domicile des personnes âgées |
| **Technologique** | Hyper connectivité, télésurveillance, géolocalisation, confort, sécurité, traçabilité, identification des objets, observation de l'environnement, capacité d'action à distance, assistance à l'humain, brevets, autonomie des machines et des objets |
| **Ecologique** | Pollution, fluidité du trafic, consommation d'énergie, ondes électromagnétiques |
| **Légal** | Cyberattaques, protection des données, protection de la vie privée, échanges d'information, normes de sécurité, collecte de données, transparence |

*Tableau 1: tendances initiales*

| | |
|---|---|
| **Exemples** | Accidents de la route, activités en extérieur, addiction et dépendance aux objets connectés, apocalypse, bien-être, collaboration et entraide, confiance aveugle envers la technologie, méfiance vis-à-vis de l'État, conflits et guerres, création de nouvelles énergies, variété des emplois, exigence, fainéantise, médicalisation, société de contrôle, manipulation, spectateurs, individualisme, incompréhension, intelligence humaine et artificielle, isolement, dépression, paranoïa, insécurité, justice, perte de libertés individuelles, agilité, capitalisme, pauvreté, prévention, pression étatique, profits, substitution de l'homme par la machine, réalité virtuelle, sécurité, savoir, totalitarisme, humanoïde, violence, valeurs superficielles, équilibre vie privée/vie professionnelle, stupidité humaine, chantage, éducation, ennui, déqualification, disparition des entreprises, éthique, permanence, dépendance, sens de la vie, espérance de vie, ressources, créativité… |

*Tableau 2: quelques exemples de tendances finales originales*

Ces tendances sont à la source d'une réflexion autour de futurs possibles pour la sécurité et la défense informatique et elles permettent d'établir quatre scénarios qui peuvent ainsi être proposés au débat (Figure 2). Ces scénarios sont construits autour des deux variables jugées les plus incertaines et dont on pense que l'évolution aura l'impact le plus élevé: la datafication [5] des individus et leur intérêt pour les objets connectés.

### Scénario «défendre»

Un fort intérêt pour les objets connectés combiné avec une forte datafication des individus constitue la base du scénario «défendre» pour la sécurité et la défense informatique.

Dans ce scénario, les individus portent un regard enthousiaste sur les nouvelles technologies. Pour la plupart, ils sont devenus des utilisateurs experts des objets connectés et ils sont en mesure d'exploiter pleinement leur potentiel de véritables assistants personnels.

Les individus sont proactifs et transmettent volontiers les données qu'ils génèrent aux fabricants d'objets connectés, si possible en temps réel. Ils sont convaincus qu'il s'agit là du

meilleur moyen de contribuer à l'amélioration continue de l'expérience utilisateur.

Dans le scénario "défendre", l'objet connecté est devenu le prolongement naturel du corps humain. Dans le même temps, les individus ont développé une sorte de sympathie sincère vis-à-vis de l'intelligence ambiante que rend possible le déploiement des objets connectés. Cette intelligence ambiante rassure, accompagne et soutient.

Dans le scénario "défendre", les experts de la défense et de la sécurité font face à une question surprenante: que leur reste-t-il à faire? Qu'est-ce que la société attend d'eux?

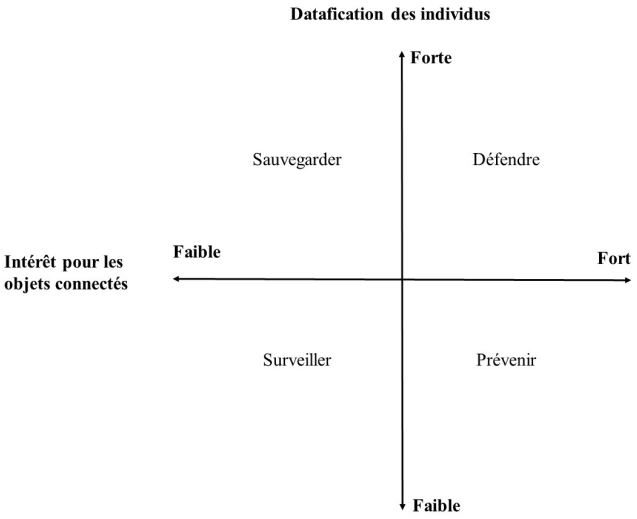



*Figure 2: scénarios pour l'intelligence ambiante, la sécurité et la défense informatique*

## Scénario: «prévenir»

Un fort intérêt pour les objets connectés combiné avec une faible datafication des individus sont les deux piliers du deuxième scénario: «prévenir».

Tandis que les objets connectés s'accumulent, ils ne semblent apparemment ni offrir beaucoup de nouvelles opportunités, ni présenter de nouveaux risques. La raison? Personne ne semble être en mesure de transformer systématiquement les données collectées en informations et en connaissances actionnables.

Dans le scénario «prévenir», la question clé que se posent les experts de la défense et de la sécurité est la suivante: quand est-ce que les objets connectés réaliseront pleinement leur potentiel de transformation?

En conséquence, lesdits experts se doivent d'agir en utilisateurs précoces afin de se donner les moyens d'estimer le plus tôt possible les menaces et opportunités potentielles que véhiculent chaque nouvel objet ou nouvelle classe d'objets connectés.

## Scénario «sauvegarder»

Un faible intérêt pour les objets connectés combiné avec une forte datafication des individus constitue la base du scénario «sauvegarder».

Dans ce scénario, les individus ne sont que modérément intéressés par les objets connectés, bien qu'ils continuent de contribuer individuellement et collectivement à générer des quantités sans cesse croissantes de données au travers de leurs nombreuses transactions quotidiennes qui n'impliquent pas nécessairement le recours à des objets connectés personnels.

Ces données ont le potentiel d'être converties en informations et en connaissances à haute valeur ajoutée.

Dans le scénario «sauvegarder», les données ainsi produites sont versées dans un "commun de connaissances" (knowledge commons), qui, à son tour, est mis à disposition des innovateurs afin de leur permettre d'accélérer le développement de leurs prototypes et de raccourcir les délais d'accès au marché. Les individus contribuent de manière consciente aux dynamiques d'innovation ouverte, lesquelles ont été adoptées largement par la plupart des acteurs dont les experts de la défense et de la sécurité informatique.

Dans le scénario «sauvegarder», c'est finalement une plus grande proximité entre individus et experts de la défense et de la sécurité informatique qui permet l'amélioration continue de la sécurité des données et des infrastructures ainsi que la conscience collective des enjeux liés au cyberespace. Ensemble, experts et individus se sentent concernés par le besoin d'établir et de maintenir des standards élevés en matière de cybersécurité à travers tout le territoire.

## Scénario: «surveiller»

Un faible intérêt pour les objets connectés combiné avec un faible niveau de datafication des individus sont les deux piliers du quatrième et dernier scénario: «surveiller».

Dans ce scénario, les objets connectés en sont toujours au stade de gadgets.

La plupart des individus ont peur: ils craignent que tôt ou tard, une catastrophe surviendra. Ils se demandent: quand est-ce qu'un véhicule autonome et connecté sera hacké et causera la mort d'un ou plusieurs passants?

Dans le même temps, les personnes sont méfiantes à l'égard de grandes entreprises qui collectent, analysent et peut-être même revendent leurs données personnelles.

Du point de vue des experts de la défense et de la sécurité informatique, le scénario «surveiller» ne présente pas de difficultés particulières: personne ne remet en cause l'importance et la nécessité de surveiller en continu le trafic des données de sorte à détecter le plus rapidement possible les attaques et autres comportements frauduleux aux conséquences potentiellement catastrophiques.

## Conclusion

Grâce à un travail collaboratif auquel ont participé un millier d'étudiant-e-s de toute la Suisse romande, nous disposons désormais de quatre scénarios prospectifs contrastés, riches des intuitions, des craintes et des espérances que portent les participant-e-s à la démarche.

Ces quatre scénarios ont vocation à servir de véritable "banc d'essai" sur lequel professionnels de la sécurité et de la défense, administrations publiques, associations etc. peuvent désormais tester un certain nombre d'options stratégiques, de choix politiques, d'arbitrages, etc.

Il s'agit, pour les organisations qui le souhaiteront, de répondre à quelques questions: mon choix stratégique est-il pertinent dans chacun des scénarios? Est-il efficient? Souhaitable?

Fortes des enseignements tirés de ce questionnement, les organisations pourront, au besoin, ajuster leurs choix stratégiques voire même repartir à zéro et envisager des options alternatives, jusqu'alors impensées.

En résumé, bâtir des scénarios prospectifs puis y tester des options stratégiques ou politiques, c'est se donner l'opportunité, à moindre frais, d'anticiper les impacts directs et indirects de décisions qui pourraient s'avérer capitales pour l'avenir de son organisation. Dans le secteur clé de la sécurité et de la défense, marqué par d'innombrables turbulences, incertitudes, contradictions, etc., il paraît fort sage d'institutionnaliser une telle démarche qui se révèle, dans la pratique, peu coûteuse au regard des gains stratégiques qu'elle procure.

S'il est nécessaire de citer un exemple, rappelons-nous l'épisode de la crise pétrolière de 1973 et la remarquable résilience dont l'entreprise Royal Dutch Shell a fait preuve ; une entreprise qui, depuis de nombreuses années déjà, avait inscrit dans son ADN le recours systématique aux scénarios prospectifs pour challenger les orientations stratégiques actuelles et envisagées.


**Prof. Thomas Gauthier**
est Professeur à la Haute école de gestion de Genève et à emlyon business school. Il débute sa carrière en tant qu'assistant de recherche à l'université Harvard. Il rejoint ensuite la société Philips où il occupe successivement les fonctions d'ingénieur, directeur de recherche clinique puis chercheur. Il est titulaire d'un doctorat en médecine expérimentale de l'Imperial College London et est également diplômé du Massachusetts Institute of Technology et de l'École Supérieure de Physique et Chimie Industrielles de Paris.



**Dr. Sylvaine Mercuri Chapuis**
est Enseignant-Chercheur en Sciences de Gestion à l'ESDES, The Business School of UCLy. Partenaire de la Haute école de gestion de Genève, ses travaux portent sur la Responsabilité Sociale des Organisations, la prospective stratégique et le management des ressources humaines. Elle est titulaire d'un doctorat de l'Université Jean Moulin Lyon 3 et elle est également diplômée de HEC Paris, de l'Helsinki Business Polytechnics School, de l'Université Savoie Mont-Blanc et l'École Nationale d'Assurance de Paris.


## Liens & Explications

[1] https://www.newsd.admin.ch/newsd/message/attachments/47967.pdf, consulté en mai 2017.

[2] http://www.futurescaper.com, consulté en mai 2017.

[3] Au sein de la Haute Ecole Spécialisée de Suisse occidentale, la Haute Ecole de Gestion de Genève (HEG), la Haute École Arc (HE-Arc), la Haute Ecole du Paysage, d'Ingénierie et d'architecture de Genève (HEPIA), la Haute Ecole d'Art et de Design de Genève (HEAD), la Haute Ecole de Santé de Vaud (HESAV) ont été mobilisées. Des étudiants de l'école Changins, Haute Ecole de Viticulture et Œnologie ainsi que de l'Ecole Polytechnique Fédérale de Lausanne ont aussi participé à l'étude.

[4] La saturation des données est atteinte lorsqu'il n'y a plus d'information nouvelle dans les documents analysés.

[5] Étape qui consiste à passer de la donnée à l'information utile: «les assurances peuvent par exemple exploiter les données relatives aux déplacements des véhicules de leurs assurés afin d'établir des contrats qui soient le plus proche possible des risques réellement présentés par leurs clients (et non plus des contrats tenant compte de leur âge, de leur sexe et de l'historique de leur conduite)» (Chamaret, 2014; p. 95).

## Bibliographie


- Von Bertalanffy, L. (1973), Théorie générale des systèmes, Paris: Dunod
- Chamaret, C. (2014), «La révolution big data», Annales des Mines - Gérer et comprendre, vol. 116, n°2, p. 94-96.
- Chevreau, F.-R., Wybo, J.-L. (2007), « Approche pratique de la culture de sécurité. Pour une maîtrise des risques industriels plus efficace », Revue française de gestion, vol. 5, n° 174, p. 171-189.
- Courrier international (2016), Automobile. Premier accident mortel pour la voiture autonome Tesla, 01 juillet, disponible sur http://www.courrierinternational.com/article/automobile-premier-accident-mortel-pour-la-voiture-autonome-tesla.
- David, A., Hatchuel, A. (2007) « Des connaissances actionnables aux théories universelles en sciences de gestion », AIMS, XVIème Conférence Internationale de Management Stratégique, Montréal.
- «Entretien», Distances et savoirs, vol. 7, n°3, p. 479-500.
- Freeman, R. E. (1984), Strategic management: a stakeholder approach, Boston: Pitman series in business and public policy.
- Frenchweb.fr (2011), 600 000 comptes Facebook victimes de tentatives de hacking chaque jour, 31 octobre, disponible sur http://www.frenchweb.fr/infographie-600-000-comptes-facebook-victimes-de-tentatives-hacking-chaque-jour-50227/32364.
- Godet, M. (2004), Manuel de prospective stratégique, tome 2: L'art et la méthode, Paris: Dunod.
- Godet, M., Durance, P. (2011), La prospective stratégique pour les entreprises et les territoires, Paris: Dunod.
- Johnson, G., Whittington, R., Scholes, K., Angwin, D., Regner, P., Fréry, F. (2017), Stratégique, 11ème édition, Paris: Pearson Education.
- Le Temps (2017), Le rançongiciel Wannacry a peu touché la Suisse, 15 mai, disponible sur https://www.letemps.ch/economie/2017/05/15/rancongiciel-wannacry-touche-suisse.

# L'édition génomique: premières batailles pour le contrôle du vivant au 21e siècle

**CRISPR-Cas [1], nouvelle technologie d'édition du génome, a le potentiel de révolutionner le vivant. Elle ouvre aussi la voie à de nouvelles armes biologiques, ce qui nécessite son suivi, comme discuté dans l'article «CRISPR and the hype cycle». Pour identifier quels acteurs sont les mieux positionnés pour contrôler cette technologie pendant les 20 prochaines années, l'étude des investissements dans les brevets associés à cette technologie est particulièrement pertinente. Dans cet article, nous présentons les applications les plus marquantes, parfois controversées, et les premières réglementations dans un contexte international particulièrement dynamique. Nous décrivons divers «faits d'armes» qui mettent en lumière les premières étapes de la guerre technologique, économique et juridique pour le contrôle du vivant au 21e siècle.**

**Mots-clés:** **CRISPR, Cas, édition génomique, brevets, licences, guerre économique, soldat modifié, bio-hacking, startups, transhumanisme**

**Auteurs:** **Dr. Corinne Le Buhan & Dr. Fabien Palazzoli**, IPStudies Sàrl

## Une technologie qui se démocratise, pour des applications très diversifiées… et en partie controversées

Jusqu'en 2012, l'édition génomique était un domaine réservé à des laboratoires et experts capables de maîtriser la complexité des premières solutions développées dans les années 1990 et 2000, telles que les Zinc Finger Nucleases (ZFN), les méganucléases ou les Transcription Activator-Like Effector Nucleases (TALEN). Depuis son invention, le système CRISPR-Cas9, plus facile à mettre en œuvre, moins coûteux et au moins aussi efficace, a entraîné un développement exponentiel de la recherche et des investissements pour des applications très variées:

- **Dans le domaine des plantes et des animaux**, aux États-Unis la FDA a approuvé en avril 2016 la mise sur le marché alimentaire des premiers aliments «OGE» (Organisme Génétiquement Edité), indépendamment des régulations «OGM» (Organisme Génétiquement Modifié): des champignons sans le gène du bleuissement. Pour les animaux, la FDA n'a pas encore donné son approbation mais les applications sont déjà bien avancées et prêtes à entrer sur le marché dès qu'elles seront autorisées [2]. En Chine, l'une des premières applications est la modification de chiens de défense pour développer leur masse musculaire, notamment à des fins policières ou militaires [3]. En Europe, la législation actuelle ne fait pas de différence claire entre «OGE» et «OGM» ce qui entraîne de nombreux questionnements et des positionnements différents des pays membres en fonction de leurs intérêts nationaux, en attendant une prise de position attendue pour 2018 [4]. Dans le domaine environnemental, l'édition génomique permet aussi le «forçage génétique» en modifiant génétiquement des moustiques pour les empêcher de transmettre des maladies telles que le paludisme. L'édition génomique offre donc pour la première fois la possibilité à l'homme de modifier son milieu vivant à grande échelle, directement au niveau biologique, ce qui soulève de nombreuses questions éthiques et scientifiques.
- **Dans le domaine médical**, de nouvelles applications de CRISPR sont régulièrement publiées. Celles-ci peuvent avoir un impact significatif sur l'industrie pharmaceutique mondiale à moyen-long terme, tant le changement de paradigme est important. Outre ses applications aux maladies génétiques et au traitement des cancers, l'édition génomique peut trouver des utilisations dans des domaines non directement liés à la génomique, comme le diagnostic de maladies infectieuses [5]. La Chine est le pays le plus avancé avec plusieurs essais cliniques en cours en cancérologie [6], sur des cellules somatiques modifiées par la technologie CRISPR. Dans le domaine nettement plus controversé de la recherche sur les embryons humains, plusieurs travaux y ont déjà été conduits, entraînant une controverse internationale dès 2015. Ces travaux sont en effet jugés contraires à la Convention sur les Droits de l'Homme. Actuellement plus de 40 pays ont adopté des législations restrictives dans ce domaine, dont la Suisse. Les Académies des sciences et de médecine américaines ont donc appelé à un moratoire international, également soutenu par l'Académie nationale des sciences Leopoldina et plusieurs institutions scientifiques en Allemagne [7]. Il semble néanmoins difficile de freiner le développement de la technologie CRISPR, tant les attentes sont grandes pour traiter certaines pathologies pour lesquelles il n'y a aujourd'hui aucun traitement. De plus, les opinions évoluent: début 2016, une équipe de chercheurs en Grande-Bretagne a ainsi obtenu l'autorisation de démarrer des recherches d'édition génomique sur des embryons humains. Début 2017, l'Académie nationale des sciences aux États-Unis a publié son rapport sur l'édition du génome humain en encourageant pour la première fois la recherche sur les embryons humains, mais seulement dans un cadre très strict, lorsqu'il n'y a pas d'alternative [8]. Une position similaire a été proposée en Europe par l'EASAC en mars 2017 [9].
- **Dans le domaine industriel**, les utilisations de CRISPR en tant qu'outil sont très variées: modifications de bactéries ou d'algues pour la production de biocarburants, création de lignées cellulaires pour la production de protéines d'intérêt économique, réactifs pour la recherche en biologie mais aussi pour une meilleure compréhension du vivant (génomique fonctionnelle)… Et les premières applications au domaine de la défense émergent déjà. Par exemple, des vers à soie ont été génétiquement modifiés pour produire un fil synthétique, dont les protéines constituantes proviennent d'araignées, bien connues pour tisser des fils très résistants. Celui-ci est en cours d'étude pour développer des gilets pare-balles aux caractéristiques inégalées (résistance, poids…), mais aussi de meilleurs parachutes pour les soldats.
- **En dehors de ces domaines**, la technologie CRISPR soulève également des questions de sécurité nationale par ses potentielles applications au domaine militaire, au « do-it-yourself-bio» [10] et au transhumanisme, avec à court-moyen terme le développement facilité de nouvelles armes biologiques. À plus long terme, la modification des embryons humains ouvre aussi la voie au développement de super-soldats en leur ajoutant des gènes de résistance, par exemple à la déshydratation ou même à l'irradiation nucléaire, comme récemment découvert par une équipe japonaise [11]. Afin de mieux contrôler l'utilisation de ces technologies par des amateurs, l'Allemagne a légiféré il y a quelques mois pour rendre obligatoire leur supervision par un expert [12]. En France, un Conseil National Consultatif pour la Biosécurité a été mis en place par le

gouvernement dès décembre 2015 afin de mieux traiter les questions soulevées par le développement rapide de l'édition génomique et de la biologie de synthèse [13]. Depuis 2016 aux États-Unis, l'édition génomique est classée en tant que menace dans la liste des armes de destruction massive par le directeur des renseignements dans son rapport annuel. Celui-ci émet toutefois une réserve sur la faisabilité scientifique d'une telle arme à grande échelle, à partir de technologies qui n'en sont encore qu'au stade de recherches [14][15].

## Derrière le « hype », une véritable guerre technologique, économique et juridique se met en place

En pratique, qui aujourd'hui maîtrise et contrôle la technologie CRISPR? L'analyse quantitative de l'information brevets, en particulier aux États-Unis et en Europe, montre que les dépôts liés à CRISPR (Figure 1) suivent depuis 2013-2014 un développement aussi important que celui des télécommunications numériques au début des années 1990 [16].

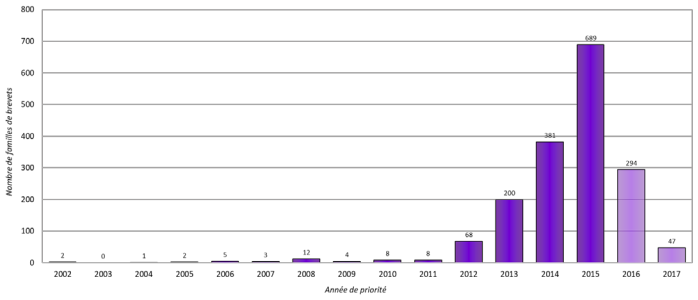



*Figure 1: Evolution temporelle du nombre de dépôts de brevets liés à CRISPR*

En complément des informations publiques sur les licences, partenariats, fusions-acquisitions et premières sociétés «CRISPR» entrées en bourse depuis 2016 [17], ces analyses mettent en lumière la diversité des tactiques mises en œuvre par les divers acteurs. L'objectif: maximiser le contrôle de la technologie et de son immense potentiel économique. C'est en effet une véritable bataille qui se joue sur tous les plans: technologique, juridique, financier, voire personnel (prix Nobel…). Sur le plan mondial, l'Europe semble à l'heure actuelle plus un territoire à contrôler qu'un leader stratégique loin derrière les États-Unis et la Chine, avec une seule société européenne (Cellectis) positionnée dans les 30 principaux détenteurs de brevets sur CRISPR (Figure 2).

Voici quelques-unes des observations les plus marquantes que nous avons faites sur ce „champ de bataille", dans l'ordre chronologique:

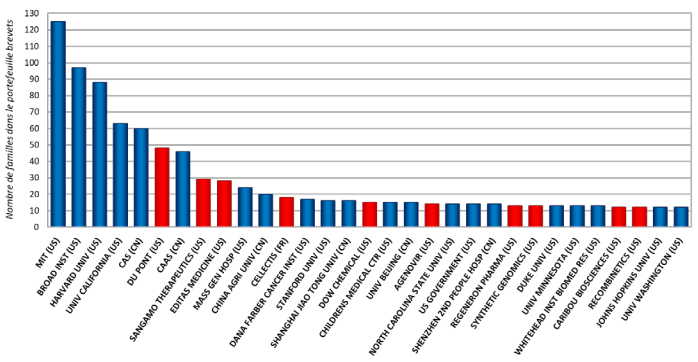



*Figure 2: Représentation des 30 principaux détenteurs de brevets CRISPR*

1. *Premières prises de position:* la mise au point du système CRISPR-Cas9 au printemps 2012 par des chercheurs des Universités de Californie et de Vienne a tout de suite fait l'objet d'une demande de brevet avant la soumission d'un article scientifique. À peu près au même moment, une équipe américaine du Broad Institute (MIT-Harvard) a développé et protégé par des dépôts de brevets ses propres méthodes pour les cellules eucaryotes, applicables notamment aux animaux et aux humains. En Europe, l'Université de Vilnius, en coopération avec Thermo Fisher aux États-Unis, et en Asie la société coréenne Toolgen ont également déposé très rapidement leurs propres demandes de brevets sur CRISPR-Cas9. Une des questions majeures liées aux brevets est donc la suivante: de tous ces pionniers, qui détient le contrôle de la technologie? La réponse n'est pas encore complètement établie, et elle peut même varier selon le territoire géographique (États-Unis, Europe, Chine…).
2. *Divisions internes:* entre 2013 et 2014, les premiers conflits d'intérêt sont apparus entre les pionniers du système CRISPR-Cas9. La scientifique d'origine française Emmanuelle Charpentier a demandé à être représentée par un autre avocat que celui de l'Université de Californie, pour défendre ses propres intérêts dans leur invention commune. Elle a aussi assigné ses droits à deux startups incorporées en Europe, CRISPR Therapeutics (pour le domaine thérapeutique humain) et ERS Genomics (pour les autres domaines), tandis que ses partenaires restaient liés à Caribou Biosciences, une spin-off de l'Université de Californie. En parallèle, le principal inventeur du Broad Institute, Feng Zhang, a créé sa propre société, Editas Medicine, pour le domaine thérapeutique, initialement avec la scientifique américaine Jennifer Doudna de l'Université de Californie comme co-fondatrice. Mais, à l'annonce du premier brevet américain délivré au nom de Feng Zhang et du Broad en avril 2014, cette dernière a quitté Editas Medicine, puis elle a fondé aux États-Unis fin 2014 une nouvelle startup dédiée au domaine thérapeutique, Intellia Therapeutics. Jennifer Doudna n'a pas été la seule à se retourner contre Feng Zhang et la stratégie «solo» du Broad Institute. Un de leurs partenaires historiques, l'Université de Rockefeller veut également sa part du gâteau, car le premier dépôt de brevet de Feng Zhang s'était fait en collaboration avec un de ses scientifiques, Luciano Maraffini, lui aussi co-fondateur d'Intellia Therapeutics…
3. *Déminage préventif:* dès les premières publications des demandes de brevets courant 2014, différents acteurs ont immédiatement cherché à affaiblir les revendications de leurs concurrents en utilisant toutes les armes juridiques à leur disposition. En Europe, ainsi qu'à l'Organisation Mondiale de la Propriété Intellectuelle, de nombreuses «observations de tiers» ont été déposées, souvent de façon anonyme. En soumettant par exemple des références scientifiques antérieures à l'invention CRISPR-Cas9, les acteurs tentent d'invalider des revendications jugées non nouvelles ou pas suffisamment inventives.
4. *Appel aux vétérans:* dès 2013, le plus gros agrégateur de brevets américains, Intellectual Ventures, a financé les dépôts de brevets relatifs à CRISPR par deux des inventeurs prodiges les plus célèbres de l'industrie nucléaire américaine et de la guerre des étoiles au temps de Ronald Reagan: Lowell Wood et Rod Hyde [18], anciens du laboratoire de Livermore.
5. *Jeunes guerilleros:* les brevets révèlent également les travaux de quelques bio-hackers émergents, par exemple l'adolescente Katriona Guthrie-Honea, une autodidacte du «do-it-yourself bio» basée à Seattle [19].
6. *Guerre des tranchées:* dès que les premiers brevets ont été accordés, une nouvelle phase a commencé avec une guerre d'usure. Celle-ci comprend les oppositions, une arme d'invalidation de brevets spécifiques à la procédure européenne, ainsi que les interférences, une procédure spécifique à la loi américaine sur les brevets. Ces derniers

dossiers, très médiatisés, prennent une ampleur hors du commun, avec des milliers de pages d'argumentations et de documentations, rédigées par des avocats spécialisés. Aux États-Unis, après un premier avis en faveur du Broad pour les applications aux eucaryotes, un appel est en cours et la situation pourrait se renverser de nouveau (ou pas) en faveur de l'autre camp d'ici fin 2017. En Europe, le Broad a demandé un délai supplémentaire pour examiner la masse inhabituelle de données qui lui ont été opposées par une dizaine d'acteurs, souvent anonymes: de nouveaux développements sont attendus début 2018.

7. *Tactiques de contournement:* La problématique et le flou autour des brevets – et donc du contrôle de la technologie – concernent aujourd'hui le système pionnier CRISPR-Cas9. Pour tenter de contourner ce système par des moyens techniques et peut-être améliorer encore l'efficacité de l'édition génomique, d'autres systèmes émergent: Cpf1, C2c2, CRISPR–CasX et CRISPR–CasY… Même s'ils ont également été protégés par des demandes de brevets, la situation est moins complexe que pour CRISPR-Cas9, car ils sont généralement sous le contrôle d'un seul acteur. Mais qu'en sera-t-il dans 5, 10, 20 ans?
8. *Jeux d'alliances stratégiques:* Comme dans toute guerre, avoir un allié peut se révéler intéressant d'un point de vue stratégique… quitte à tomber avec lui. Certains acteurs ont noué des partenariats exclusifs, par exemple CRISPR Therapeutics avec Bayer, Intellia Therapeutics avec Novartis. D'autres détiennent des licences exclusives pour un large domaine d'applications, comme DuPont auprès de l'Université de Vilnius et d'ERS Genomics dans le domaine agricole et les applications aux plantes. À la vue de la complexité et du flou de la situation sur les brevets, d'autres ont préféré sécuriser leur business plan et négocier avec les deux principaux camps plutôt que de parier sur un vainqueur. C'est par exemple le cas de la société anglaise Horizon Discovery, licenciée de ERS Genomics mais aussi du Broad Institute.
9. *Propagande:* début 2016, un article d'Eric Lander, directeur du Broad Institute, sur «Les héros de CRISPR» décrivait l'historique des recherches dans le monde ayant conduit à la mise au point de la technologie CRISPR-Cas9, y compris des recherches militaires peut-être restées secrètes, notamment en France. Cet article a été immédiatement très critiqué pour son approche partisane, car il minimisait les avancées des équipes de Jennifer Doudna et Emmanuelle Charpentier au profit de celles des chercheurs du Broad, Feng Zhang et George Church.
10. *Nouvelles coalitions:* début 2017, les conflits internes au camp Doudna-Charpentier se sont apaisés avec un accord global de licences croisées entre leurs différentes sociétés. En parallèle, le leader mondial en concession de licences MPEG-LA a lancé un programme dédié à CRISPR et annoncé officiellement en juillet 2017 la participation du Broad Institute. Bien que les autres participants ne soient pas encore connus, cette initiative pourrait, en cas de succès, simplifier l'accès à la technologie à l'échelle commerciale.

## Conclusions – à quoi devons-nous nous préparer?

Après la révolution industrielle au 19ème siècle, celle des communications au 20ème siècle, c'est une vraie révolution du vivant qui se déroule au 21ème siècle, et les technologies d'édition génomique en font clairement partie. C'est pourquoi les batailles pour le contrôle économique de la nouvelle technologie CRISPR font rage. Les applications sont si variées qu'elles auront nécessairement un impact sur les opérations militaires. Il est aussi frappant de mesurer actuellement un certain retard de l'Europe dans le développement technologique et le contrôle économique de ces technologies, ce qui pourrait appeler le Vieux Continent à anticiper ces nouvelles applications sous l'axe défensif en priorité.

Pour résumer, l'étendue de l'édition génomique semble n'avoir comme limites que l'imagination des Hommes. Toutefois, les investissements sont encore au stade de recherche et développement: il est encore temps d'anticiper leur démocratisation, et peut-être même de les contrôler, comme l'Allemagne essaie de le faire avec une nouvelle loi plus restrictive sur le bio-hacking. De la même manière que les compétences en cryptographie, cyber-surveillance et cyber-sécurité se sont développées avec la numérisation des communications, l'optimisation génétique, la surveillance et la neutralisation biologiques pourraient donc devenir des spécialités recherchées au sein des armées du 21ème siècle.


**Dr. Corinne Le Buhan**

est Dr. En Sciences des Communications de l'EPFL et diplômée de l'Université de de Strasbourg en gestion stratégique de propriété industrielle et innovation. Elle a travaillé une quinzaine d'années dans l'industrie des technologies d'information et de télécommunications avant de créer sa société de conseil IPStudies en 2010 pour accompagner les PME technologiques suisses dans le positionnement de leurs brevets et licences, notamment aux États-Unis.



**Dr. Fabien Palazzoli**

est titulaire d'un Master Professionnel en Biotechnologies & Droit et d'un doctorat en Sciences de la Vie de l'Université de Tours. Il possède une expertise dans les domaines de l'ingénierie génomique, de la bioproduction et des thérapies géniques et cellulaires, associée à la maitrise d'outils de recherche, d'analyse et de cartographie d'information brevets. Depuis 2013 il développe les services d'IPStudies dans le domaine des Sciences de la Vie, et notamment les études des brevets CRISPR et de leurs applications.


## Références


[1] CRISPR: Clustered Regularly Interspaced Short Palindromic Repeats.

[2] http://www.nature.com/news/gene-edited-animals-face-us-regulatory-crackdown-1.21331

[3] http://www.independent.co.uk/news/science/mutant-extra-muscular-dogs-created-by-chinese-scientists-a6701156.html

[4] http://www.nature.com/news/gene-editing-in-legal-limbo-in-europe-1.21515

[5] http://www.latribune.fr/entreprises-finance/industrie/chimie-pharmacie/crispr-peut-il-uberiser-les-diagnostics-687411.html

[6] http://www.genethique.org/fr/crispr-un-troisieme-essai-clinique-autorise-chez-lhomme-67512.html#.WVC3fopLdE4

[7] https://www.leopoldina.org/uploads/tx_leopublication/2015_3Akad_Stellungnahme_Genome_Editing.pdf

[8] https://iatranshumanisme.com/2017/02/19/rapport-du-nas-sur-ledition-du-genome-humain/

[9] http://www.easac.eu/home/press-releases/detail-view/article/new-easac-re.html

[10] https://www.technologyreview.com/s/603530/a-biohackers-plan-to-upgrade-dalmatians-ends-up-in-the-doghouse/

[11] https://www.nature.com/news/tardigrade-protein-helps-human-dna-withstand-radiation-1.20648

[12] http://gizmodo.com/germany-is-threatening-biohackers-with-prison-1792143993

[13] http://www.sgdsn.gouv.fr/missions/lutter-contre-la-proliferation/le-conseil-national-consultatif-pour-la-biosecurite-cncb/

[14] https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

[15] Lire aussi à ce sujet l'article « CRISPR and the hype cycle » de Cédric Invernizzi.

[16] En Europe et aux Etats-Unis, les brevets sont généralement publiés 18 mois après leur dépôt (« date de priorité »), un peu plus tôt en Chine. Les statistiques sont donc encore incomplètes pour les années 2016 et 2017.

[17] Au NASDAQ: Editas Medicine, Intellia Therapeutics et CRISPR Therapeutics.

[18] https://fr.wikipedia.org/wiki/Initiative_de_d%C3%A9fense_strat%C3%A9gique

[19] https://www.geekwire.com/2013/biotech-space

# Winning the Cyber Battle: Trusting Your Digital Assets

**Digital assets have been mission-critical elements in combat environment, from their use in communication and intelligence gathering, to their direct presence inside weapon systems. These assets could be as simple as an air purity sensor, as complex as a modern fighter jet or as commonplace as the cell phones that soldiers carry on them and use to gather and communicate live field intelligence. Over the years, these digital assets have become increasingly complex ecosystems and their exposure to risk of interference by third parties has increased commensurately. In this article, we consider the cybersecurity issues around military digital equipments as well as the systems and the reasons for lack of trust among the armed forces in adapting them for critical-missions.**

**Keywords:** **Security, defense, ensure trust, armed forces, technology, digital assets, hardware vulnerabilities, warzones, threat intelligence, embedded security, cybersecurity**

**Author:** **Vishruta Rudresh**, Kudelski Security

## Introduction

Technology has always played a crucial role in combat environments and has evolved immensely over time. In this digital era, nation states are researching [1] the utility, risks and challenges of deploying digital devices into war zones. Digital devices here refer to electronic systems with digital logic. Each such system depends on an embedded circuit that runs some sort of firmware or software or both. Over the years, dependency on such digital devices in war zones has increased dramatically. Lenk, chief of service strategy and innovation, NATO Communications and Information Agency predicts that in 5 or 10 years from now, the military world will be full of devices that are talking to each other, talking to command and control systems and talking to everything! [2]

When you think about it, the benefits of using digital devices in the armed forces and in wars is fairly obvious: - improved situational awareness and logistics support, expert medical care/assistance anywhere and anytime, enhanced surveillance, secure communication, and efficient intelligence gathering that enables effective decision making. The low cost of much of these technologies (sensors, drones) and their usability are other factors that also facilitate their adoption/adaption. Indeed, in modern warfare with its asymmetrical dimension, it is difficult to imagine military successes without the use of these technologies. However, the adaption of digital devices in the armed forces hasn't been easy. There has been a looming sense of distrust in these devices among the armed forces.

## Why the distrust?

Past security vulnerabilities. Our dependence on digital technologies, however, is at odds with the level of trust we can place in them. One of the primary reasons for this distrust is that the developers have done an inadequate job of either building or integrating secure hardware and software onto the device (basic safeguards that can protect devices against digital threats) resulting in the apparent leakage of sensitive, classified information from these devices either when they are remotely compromised or when intercepted by an adversary. One such example is drones; drones are used by the military to generate interference in enemy signals and for long range surveillance. However:

- In 2009, insurgents in Iraq compromised the drones using software available on the Internet for $26 a piece, and intercepted live video feeds from the drones being relayed back to a US controller. This information leakage revealed potential targets, thereby aiding the insurgents to take evasive actions. [3]
- In 2011, a computer virus infected the drone control center of Predator and Reaper drones and monitored keystrokes during missions carried out in Afghanistan and other warzones. Monitoring and relaying of the keystrokes during missions potentially revealed classified information to the enemy. [4]
- At the 2015 DEF CON event, security researchers successfully compromised a Parrot A. R. Drone using open WIFI and an open Telnet port to remotely terminate the process that makes it hover. [5]
- In early 2016, hackers at AnonSec claimed to have developed a method for gaining partial control over one of the Global Hawk drones used by NASA [6]. However, NASA has completely denied that its drones were hijackd [7].

There are several reasons why an adversary would want to compromise a device, as part of the overarching aim to gain strategic or tactical advantage. If they can disrupt its functionality, deny its services to legitimate users, degrade its performance, deceive its users into performing unintended actions or destroy it completely, their position becomes stronger. Adversaries can do so by compromising vulnerabilities present in the devices. A vulnerability in devices can mainly be attributed to the improper development or implementation of security measures in the devices. Some common hardware vulnerabilities/attacks include:

- Hardware Trojan [8]: is a malicious modification of the circuitry of an integrated circuit (IC). Hardware Trojans could be placed into the system by the manufacturer themselves for debugging and maintenance tasks. However, the effects of Trojans on the target hardware can range from subtle disturbances to catastrophic system failures in the hands of an adversary. The hardware can accept inputs that should otherwise be rejected such as co-ordinates over a no-fly zone. They can also leak cryptographic keys used for secure communication or perform Denial of Service attacks. All of which completely undermines trust in the system using that IC.
- Hardware backdoors [9]: are similar to Hardware Trojans, but involves code that might reside in the firmaware of computer chips. These can be deliberately placed by the manufacturer for testing, debugging and maintenance purposes or could be placed by an enemy after a device has been compromised. Hardware backdoors can also enable attackers to control the system remotely [10]. Hence, their effect is as catastrophic or maybe even more so, than that of a Hardware Trojan.
- Unified Extensive Firmware Interface (UEFI) vulnerabilities [11]: UEFI is a specification that defines a software interface between operating system and platform firmware. Vulnerabilities in UEFI can be exploited to install highly persistent malwares on to the device [12], regardless of any security measures that might be in place. Compromise of this vulnerability can also let the enemy control the entire system to their will.
- Semiconductor doping: is the process of adding impurities

to silicon-based semi-conductors to change or control their electrical properties. Chemicals such as phosphorous and arsenic are used to alter the properties and are widely and easily available. Doping performed by an adversary on the device aids malicious Trojans to pass build-in tests that are primarily designed for reporting manufacturing or operational defects in the devices [13].

- Hardware devices in general are susceptible to hardware side-channel attacks such as timing attacks, power analysis and fault injection that could be used to steal sensitive information, eavesdrop etc [14].

It is to be noted that these vulnerabilities and subtle modifications of chips in the devices are virtually impossible to detect on the battlefield, thereby, forcing the soldiers into a position of strategic disadvantage, without even being able to pinpoint the cause. Hence, the raging distrust in digital devices among the armed forces.

Poor response to vulnerabilities: Delayed remediation of vulnerabilities in devices has been a consistent concern among the armed forces. The flaw in the 2009 drone attack by the Iraqi insurgents on US drones is said to be dated back to the 1990s according to a military technology analyst, Peter Singer [15] and another US official stated that the flaw was finally identified and fixed over a period of 12 months [3]. Though the military had known about the flaw, it assumed its adversaries would not be able to take advantage of it.

The same inaptness has persisted with other maintenance processes (for example timely patching and upgrading processes) of combat digital devices. With increased complexity of devices, their upgrade/patching processes is becoming tedious and expensive; in summary maintenance is becoming a burdensome task to most nation states and there is confusion over legal responsibility for security with no single party (either manufacturer, integrator or end user) assuming this role.

Globally sourced technology: Nations are concerned about the risks generated from using globally sourced technology for implementing and manufacturing digital devices in parts or in whole. Counterfeit computer hardware components are viewed as a significant problem by private corporations and military planners [16].

A recent White House review noted that there had been several "unambiguous, deliberate subversions" of computer hardware components. The specter of subversion causing weapons to fail in times of crisis, or secretly corrupting crucial data, has come to haunt American military planners. This problem has grown more severe as most American semiconductor manufacturing plants have moved offshore (to countries such as China) [17][18].

The same is true for other nations as they lack the ability to fulfill the capacity requirements needed to manufacture computer chips for classified systems. Consequently, certain nations such as China have acquired monopoly over the manufacturing and implementation of chips and devices in parts or in whole. Also, the Chinese government has been known to include hardware backdoors in some commercial components manufactured in China on the pretext of prevention and investigation of terrorists' activities. Thereby, putting third-party nations at a risk of being snooped or digitally hacked by the Chinese [19][20][21][22][23].

Opaque decision making: Digital devices can make many thousands or millions of decisions each second that govern its operation and actions. Users and operators often have no visibility into the reasoning behind these decisions, so it becomes difficult to evaluate their accuracy. The uncertainty in determining if a device would make the "right" decision on the battlefield is a matter of concern. One instance of this is the malfunctioning of an antiaircraft cannon (Oerlikon GDF-005) on the battlefield that killed 9 persons and injured 14 others. The anti-aircraft weapon used by the South African National Defense Force is computerized and designed to use passive and active radar to obtain its target data. The malfunctioning of the device is attributed to a software glitch in the machine [24]. Another instance is the malfunctioning of G36 assault rifles used by the Germans. The German troops reported that the rifles lost accuracy after sustained firing in hot environments [25]. Also, during an Indonesian Navy exercise on September 14, 2016, two Chinese made C-705 missiles failed to hit their targets after launching from two KCR-40 attack ships [26].

Dependence on insecure third-party networks for communication: On April 8, 2010, state-owned China Telecom rerouted U.S. and other foreign Internet traffic, causing 15 percent of the all internet traffic to travel through Chinese servers for nearly 20 minutes. The long-term impact of this rerouting remains unknown [27]. However, there is a gaping possibility of military information being leaked during this incidence. In accordance, it is to be noted that third-party network providers are inherently insecure and susceptible to man-in-the middle attacks, snooping, etcetera [28]. Along with the lack of knowledge or use of cryptographic primitives in communication channels, the armed forces' reliance on insecure third-party networks only adds to their security concerns. Establishment of secure private communication channels can also be cumbersome and expensive, and would only add to their woes.

## Why the need for trust and adaption?

Digital assets may be a strong target during Phase Zero, or pre-conflict operations. In the Internet age, controlling information is as important as influencing opinions on an international platform such as the United Nations (UN). For instance, network attacks widely believed to have originated in China have targeted diplomats from the United States and partners, politicians, human-rights campaigners, military networks, and corporations to glean confidential information to influence in matters of interests to China. [29]

The Chinese government abides by the strategic culture of defeating an enemy prior to the onset of hostilities. Its intentions are to bend the will of an adversary nation without having to resort to force [30]. In accordance to its philosophy, the Chinese government has carried out not only sophisticated computer-network operations [31], but that it has also been taking measures to target embedded devices. In 2007, Jonathan Evans, the Director „General of the UK Security Service, MI5, stated that the Chinese"continue to devote considerable time and energy trying to steal our sensitive technology on civilian and military projects and trying to obtain political and economic intelligence at our expense." [32]

Another instance of Phase Zero operations include the injection of Trojan horses by the United States in the 1980s. The American Intelligence added a Trojan to a gas pipeline control software to ensure that the machine - being shipped through Canada to Russia - would work erratically and could be disabled remotely. The machine was bought by the Soviet Union from Canadian suppliers to control a Trans-Siberian gas pipeline. However, the doctored software failed, leading to an explosion in 1982, an outcome that met the interests of the United States [33][34].

Similarly, Crypto AG, a Swiss maker of cryptographic equipment (Enigma) is believed to have colluded with NSA to rig the equipment provided to certain countries. The Swiss reputation for secrecy and neutrality lured Iranians and other nations to buy the equipment. In the aftermath, NSA's access to the hardware back door in the company's encryption machine made it possible to read electronic messages transmitted by many governments [35][36].

However, other nations focus on building capacity of partners and influencing potential adversaries to avoid wars. Such nations do not engage in tactical approaches as the Chinese do. As a result, these nations lack the strategic advantage that the Chinese government possesses. Therefore, in order to stand side-by-side on international platforms such as the UN without being tactically coerced by adversary nations, these nations need to adapt and trust their devices. They need to employ trust measures to safeguard their devices and eventually their will.

## What does it mean to trust a digital asset?

The word "trust" in this context means relying on a device to effectively perform a functionality. In other words, devices should not function to aid the enemy. Examples of device abuse include:

- Spying on behalf of the enemy to glean confidential information to undermine the efforts of the armed forces using the device.
- Providing false or dated information to allies that could jeopardize a mission. An instance of this could be providing wrong location co-ordinates for the launch of a missile. The outcome of the launch could potentially kill innocent civilians.
- Inadvertently revealing confidential information to the enemy. This can be attributed to employing insecure communication channels where in the data is not encrypted or that the enemy possess the encryption key to the encrypted data transmitted over the communication channel.
- Acting as a launchpad for enemy attacks or take false inputs from an adversary to mar the outcome of a critical functionality. An instance of this could be the use of the kill switch by the enemy at their will, thereby undermining the efforts of the armed forces in a mission.
- Revealing its location or the location of other assets to the enemy in the event of stealth operations. This is made possible either by insecure communication methods or by compromising the device by a Trojan.
- Performing in a reduced capacity so as to disrupt the supply-chains. Thereby, drastically impacting the performance of the military due to shortages of food, water, ammunition and other basic supplies.

## How to ensure trust in digital devices?

Trust must be established and remain consistent across all domains of device operation. Accordingly, Lenk, chief of service strategy and innovation, NATO Communications and Information Agency believes that trust in digital devices in the armed forces can be ensured by means of demonstrations and by clearly evaluating risks vs benefits.

While presuming that the attackers/insurgents/enemy have the technical prowess to hack into digital devices remotely or extract information from the devices when in possession of it, some measures that could be employed for ensuring trust include (Figure 1):

- Threat intelligence and monitoring: effective threat intelligence operations can inform operators of vulnerabilities before they impact a mission. Although not specific to device security, these operations are vital to ensure proper countermeasures are developed and deployed in the field.
- Secure update mechanisms: no system is resilient against all future threats at inception. Digital devices must allow for secure updates of its software and firmware to allow for countermeasures against new threats.
- Device Security Assessment: hardware is the foundation of a digital asset. If the hardware is compromised, all components -firmware, software- stands compromised. As security assessments and evaluations increase trust in the security of the technology, employing advanced labs for hardware and software evaluations that identify and address security vulnerabilities is imperative. Assessments also require expertise in embedded security for TEE (Trusted Execution Environment), white box cryptography, Security on chip (SOC), and IoT-enabled devices. Security Assessments may include:
  - Audit of communication protocols: perform checks for man-in-the middle attacks, integrity and authentication.
  - Source code audit: by means of de-obfuscation and fuzzing (checks implementation errors and ensures the outcome of an input is as expected).
  - Cryptography audit: for leakage of secret keys, implementation errors etc.
  - Software/Application vulnerability assessment.
  - In-depth security evaluations for side channel, fault injection, imaging and IC modification attacks on the device hardware.
  - Hardware audit: for covert channels, backdoors and Trojans, semiconductor doping, etc.
  - Evaluating supply chain vulnerabilities.
- Embedding anti-tampering technology and compromise detection mechanisms in the device: countermeasures that enable the detection of a compromise or a break-in need to be implemented. Some techniques include Encryption Wrappers, Code obfuscation, software watermarking and fingerprinting, Trusted Execution Environments (aids in detection and reporting of unauthorized changes to the operating system or programs, detects rootkits), etc. [37]. This also requires proper implementation of PKI (public key infrastructure), access control mechanisms and identity management systems to prevent the emergence of rogue devices and impersonation.
- Having a fail-safe approach: if tampering is detected, the device should be able to fail in a safe manner. Hidden kill switches could be included to make it possible to disable computer-controlled military equipment from a distance. Such switches could be used as a safeguard if the technology fell into enemy hands.

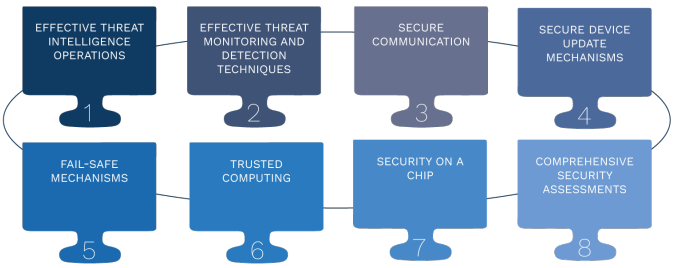



*Figure 1: Ensuring trust in digital devices*

- Securing device feeds and operations using cryptographic primitives: it is increasingly important in today's combat environment to use cryptographic primitives because enemies and potential adversaries are rapidly acquiring "jamming" and "hacking" technologies giving them an ability to interfere with or compromise device operations. To achieve secure communication, device manufacturers can embed secure elements like Trusted Platform Module (TPM) into the device. Secure elements are specialized chips on an endpoint device that stores encryption keys specific to the host system for hardware authentication. They also provide an opportunity for over-the-air patching and updates to the devices. Finally, secure elements also mitigate the threats imposed by using third-party networks for military communication and eliminates the need to establish expensive private network communication channels.
- Implementing trusted computing: this involves memory curtaining, securing input/output, sealed storage and remote attestation. It also involves the development of Trusted Computing Base (TCB). TCB is the set of all hardware, firmware, and/or software components that are critical to the devices' security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system. It contains four primary security mechanisms - a security policy, identification and authentication, labeling, and auditing. TCBs are usually accompanied by Trusted Execution Environments (TEE), a

secure area of the main process that evaluates the code and data loaded onto the chip for confidentiality and integrity and provides hardware root of trust functionality. Root of trust supports features such as:

- Secure boot and secure access control.
- Secure identification and authentication.
- Firmware integrity assurance.
- Secure storage for the rest of the chip.
- Secure debug and test access control.
- Runtime protection.
- Secure field updates.

## Conclusion

War zones are being digitized and digital chips and devices are permeating the military and industry at a rapid pace. Complexity of the chips and device functions are making it hard for device manufacturers to embed robust security controls. A race condition is established between feature requirement and security implementation, it has become a norm to have a trade-off of sorts against security to have a required functionality in place.

Countermeasures as well do not cover all scenarios at the moment, making it all the more difficult to trust digital devcies. Hence, it has become imperative to find and implement a process for testing chips and devices for vulnerabilities and remove unwanted "features" to establish a sense of trust in these devices. Nation states need to take the responsibility to establish a responsible and accountable supply chain system and all parties – from device manufacturer to end users need to make an effort to enforce trust measures in digital devices.


**Vishruta Rudresh**

is a Senior Cybersecurity Researcher at Kudelski Security focusing on fundamental new approaches to IoT and OT environment security, including but not limited to machine learning, edge device decision making, and low power environment security. She has been working in the Information Technology industry since 2011 specializing in IoT security, malware reverse engineering, system and application administration, incident response, digital forensics and mobile security and has a master's degree in Information Technology-Information Security from Carnegie Mellon University.


## References


[1] https://www. cso. nato. int/ACTIVITY_META. asp?ACT=8647

[2] https://www.afcea.org/content/?q=Article-nato-studying-military-iot-applications

[3] https://www. theguardian. com/world/2009/dec/17/skygrabber-american-drones-hacked

[4] https://www. wired. com/2011/10/virus-hits-drone-fleet/

[5] https://www.csoonline.com/article/2970932/security/ten-scary-hacks-i-saw-at-black-hat-and-def-con.html

[6] https://www.hackread.com/nasa-data-leaked-nasa-drone-hacked/

[7] https://www.hackread.com/nasa-denies-anonsecs-claim-of-hacking-global-hawk-drone/

[8] https://en.wikipedia.org/wiki/Hardware_Trojan

[9] https://en.wikipedia.org/wiki/Hardware_backdoor

[10] http://www.dailymail.co.uk/sciencetech/article-2152284/Could-vulnerable-chip-allow-hackers-Boeing-787-Back-door-allow-cyber-criminals-way-in.html#ixzz28fcdeOdm

[11] http://www.securityweek.com/researchers-find-several-uefi-vulnerabilities; https://threatpost.com/cert-warns-of-uefi-hardware-vulnerabilities/110213/

[12] https://www.pcworld.com/article/3187264/security/uefi-flaws-can-be-exploited-to-install-highly-persistent-ransomware.html

[13] https://arstechnica.com/information-technology/2013/09/researchers-can-slip-an-undetectable-trojan-into-intels-ivy-bridge-cpus/

[14] http://gauss.ececs.uc.edu/Courses/c653/lectures/SideC/intro.pdf

[15] http://www.cnn.com/2009/US/12/17/drone.video.hacked/index.html

[16] https://www.scientificamerican.com/article/the-pentagon-rsquo-s-seek-and-destroy-mission-for-counterfeit-electronics/

[17] http://www.nytimes.com/2009/10/27/science/27trojan.html?mcubz=3

[18] http://www.homelandsecuritynewswire.com/fake-chips-china-threaten-us-military-systems

[19] https://www.theguardian.com/technology/blog/2008/oct/06/security.china

[20] http://gizmodo. com/5897493/all-chinese-made-electronics-could-be-bugged-says-former-head-of-us-counterterrorism

[21] https://www.schneier.com/blog/archives/2012/05/backdoor_found.html

[22] http://www.popsci.com/technology/article/2013-07/spy-agencies-have-banned-lenovo-computers-because-theyre-chinese

[23] http://www.reuters.com/article/us-china-security/china-passes-controversial-counter-terrorism-law-idUSKBN0UA07220151228

[24] https://www.wired.com/2007/10/robot-cannon-ki/

[25] http://www.popularmechanics.com/military/weapons/a21427/german-troops-dont-trust-their-weapons/

[26] http://www.janes.com/article/63815/indonesian-president-watches-failed-firings-of-chinese-made-c-705-missiles-at-naval-exercise

[27] http://www.foxnews.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers.html

[28] https://www.wired.com/2014/03/how-huawei-became-nsa-nightmare/

[29] http://diplomacydata.com/cyber-security-and-cyber-espionage-in-international-relations/

[30] Phase Zero: How China Exploits It, Why the United States Does Not Scott D. McDonald, Brock Jones, and Jason M. Frazee (https://www.usnwc.edu/getattachment/eef71cb7-abe7-4410-adaf-d78d085d933e/Phase-Zero--How-China-Exploits-It,-Why-the-United-)

[31] http://www.npr.org/2013/02/19/172373133/report-links-cyber-attacks-on-u-s-to-chinas-military

[32] http://www.telegraph.co.uk/news/worldnews/asia/china/8597485/China-and-Britain-locked-in-cyber-war.html

[33] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm

[34] http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=1&ref=science&pagewanted=all

[35] https://web.archive.org/web/20080202225034/http://www.inteldaily.com/?c=169&a=4686

[36] http://www.atlasobscura.com/articles/a-brief-history-of-the-nsa-attempting-to-insert-backdoors-into-encrypted-data

[37] A Survey of Anti-Tamper Technologies by Dr. Mikhail J. Atallah, Eric D. Bryant, and Dr. Martin R. Stytz (https://pdfs.semanticscholar.org/50b5/e90d919cc7641225281bfb84cbdaf5751d17.pdf)

# CRISPR and the Hype Cycle

**CRISPR, a novel technology to edit genes, is a classic example of an enabling technology that rapidly emerged. A recent statement by the US intelligence community added gene editing to a list of threats posed by weapons of mass destruction. This sparked a controversy about looming doomsday scenarios, the main actor being a nascent technology that is arguably moving closer to the culmination point of potentially inflated expectations. Over the past few years, CRISPR has undeniably proven to act as a game-changer for studies on certain organisms hitherto difficult or impossible to genetically modify. Upon closer investigation, this does not however automatically translate into a markedly increased threat posed by biological weapons that would radically 'change the game'.**

**Keywords:** **CRISPR, Cas, gene editing, genome editing, enabling technology, hype cycle, tacit knowledge, adaptive immune system, biological weapons, security**

**Author:** **Dr. Cédric Invernizzi**, Spiez Laboratory

"CRISPR – a weapon of mass destruction" [1]. "Top U.S. intelligence official calls gene editing a WMD threat" [2]. Such headlines spread like wildfire through the scientific news landscape in early 2016. What particularly struck scientists was the question of how did an enabling technology of the life sciences find its way into the limelight of intelligence and security communities, and cause acute fears about looming doomsday scenarios. Notably a technology that is nowadays applied on a daily basis in a myriad of laboratories all over the globe. One reason may be attributed to the applicability of CRISPR as a powerful gene editing tool, the potential of which was first suggested only recently in 2012 – a mere five years ago [3]. As a consequence, the fulminant rise of CRISPR for gene editing may have caused this kind of drawn conclusion by the US intelligence community. But why is CRISPR causing nightmares to certain communities at all? To answer this question, it may be useful to have a closer look at what CRISPR is, how it was discovered, what it is used for and what future applications are currently under basic scientific investigation.

What is known today as CRISPR, the abbreviation for 'clustered regularly interspaced short palindromic repeat', was first described in the early 1990s. More than ten years later, a 2005 report [4] recognized these CRISPR regions in bacterial DNA as containing short pieces of foreign genetic material which led the researchers to hypothesize that CRISPR was some sort of adaptive immune system – something never described before in bacteria. Further research carried out by different groups was finally pieced together in 2012 [5], when a report elaborated on the mechanistic details of this novel adaptive immune system that relies on Cas (CRISPR-associated) proteins. For the first time, this same report also hypothesized on CRISPR's potential for exploitation as genome editing tool. Further investigations carried out by other groups in that vein quickly led to the demonstration of CRISPR's versatility in terms of gene editing applications in a multitude of cell types, including human cells [6][7].

These landmark articles literally kicked-off a gold rush on researching CRISPR applications, seemingly without any borders. By now, CRISPR's value as a tool to engineer genetic information at will has been demonstrated in a multitude of cell types and organisms. With CRISPR, researchers can turn to cells and organisms which so far were difficult or almost impossible to genetically manipulate and can rely less on model organisms such as mice and fruit flies. Whether it be for gene editing, i.e. to change genetic information, or for purposes of silencing or activating genes, i.e. interference with genetic expression patterns. Exploiting these basic concepts as genetic engineering tools allowed the fulminant rise of CRISPR in an ever growing variety of applications, as observed over the last few years, e.g.:

- As a research tool for reverse genetics to probe gene function in specific cells and tissues, or to screen for genome-wide loss-of-function or gain-of-function;
- As a design tool for synthetic biology by engineering metabolic pathways in industrial microbes for the production of therapeutic drugs, biofuels and biomaterials;
- As an animal or cell-based modeling tool for human diseases through engineering of specific mutations, in order to mimic human disorders, or for screening and target validation purposes;
- As a tool for gene therapy by correcting genes ex vivo or through vector-mediated delivery into specific tissues or organs.

According to some critics, a significant amount of this research took place without understanding the how or why as long as it worked. Eventually, these critics voiced their worries that too little time was spent on addressing ethical and safety concerns [8]. Arguably, one of the latest experiments in a series that fueled these controversies over CRISPR were the published results on correcting genetic mutations in viable human embryos [9]. Finally, another CRISPR application that triggered a controversial debate over ethics and safety are 'gene drives'. The concept of a gene drive was until very recently of a theoretical nature. With the advent of CRISPR, gene drives have however made their way into the real world. Gene drives tweak the standard inheritance pattern that was first described by Mendel in dipolid or polyploid organisms, i.e. organisms that contain more than one set of chromosomes [10]. Gene drives namely convert heterozygosity to homozygosity, i.e. a specific mutation on one chromosome is selectively copied by CRISPR/Cas9 to the other chromosome(s), with the effect that all offspring will inherit the specific mutation. Accordingly, gene drives are now under investigation as a means of combating diseases like malaria, dengue or zika through genetic engineering of the respective mosquitoes that act as vectors [11].

All these dazzling reports constantly hitting the news pipeline suggest that CRISPR renders genetic engineering cheap, fast and easy, and that it opens up a plethora of applications previously hardly imaginable. Or is there in fact more to the story? In general, technological breakthroughs trigger a cornucopia of promises, culminating in a 'peak of inflated expectations'. As a consequence, experiments fail to deliver and a 'trough of disillusionment' has to be crossed to get back on a 'slope of enlightenment' to eventually reach a 'plateau of productivity' with sustainable, commercially viable output – not just proof-of-concepts. This sequence of stages has been labeled the 'hype cycle' by Gartner [12]. Transposing the hype cycle to the only recently emerged CRISPR applications, it is reasonable to say that this technology stands at the earlier stages of the hype cycle, i.e. arguably close to the peak. In other words, are there already signs that CRISPR may be faced with obstacles inherent to this novel technology? And what about gene drives, will this

technology be readily usable to e.g. alter or even eradicate entire populations of a given species? To approach these questions it is once again worthwhile to have a closer look at recent literature.

One well-noted proof-of-concept study was published in 2014 on the potential applicability of CRISPR as a tool for putting gene therapy into practice [13]. The study demonstrated the potential of the CRISPR/Cas9 system to correct human genetic diseases in a mouse model. A more in-depth look at the publication however identifies two important areas where improvements are indispensable for future success: 1) efficiency of delivery, and 2) precision (cut and repair) as well as the problem of off-target effects. Since then a lot more research has been carried out that at least partially addressed these outstanding issues. For instance, targeted delivery has been described in mice by using viral mediated approaches [14]. However, experimental conditions would never have been applicable in a human setting. Talking of precision and off-target effects, research, on the one hand, has focused on enhancing the yet rather well-characterized Cas9 protein by making it more reliable in terms of increased fidelity and lowered off-target effects [15]. On the other hand, several research groups have contributed to an ever growing set of CRISPR-associated proteins with alternate 'specialties' in terms of target and performance [16], such as Cpf1 or Cas13a (formerly C2c2), a development that much resembles the gold rush days of PCR technology [17]. Nevertheless, the precision problem may be more fundamental than so far assumed. A most recent study of CRISPR-Cas9 in an in vivo mouse model namely found an unexpectedly high number of off-target mutations in the form of single-nucleotide variants with potentially devastating effects, depending on their exact location [18]. But also this study is already starting to be scientifically scrutinized and criticized [19].

As already mentioned, gene drives have also reached the stage of early proof-of-concepts [20]. Further experiments investigating the longer term behavior of such a particular gene drive system demonstrated the obviously inevitable when nature is part of the game: resistance [21]. Apparently, in order for a release into the wild to be successful, strategies still need to be developed that would lower the technology's inherent potential of causing resistance. From all these reports on gene drives as well as CRISPR in more general terms, it is evident that numerous obstacles requiring further attention have been identified over the last few years. It is also reasonable to assume that there is even more to come, and that CRISPR will also eventually face the other stages of the hype cycle – as was the case with other technologies in the past. But what does that mean in terms of trying to assess the potential impact of CRISPR on the biological weapons threat?

As with a multitude of other enabling technologies, it cannot be excluded that CRISPR, in whatever form, could prove useful and be applied in a future biological weapons program. The relevant question is, however, would CRISPR make a game-changing difference? CRISPR is a burgeoning field of active research and growing financial investment. Under such highly dynamic conditions with surprises chasing each other at a rapid pace, any predictions for the future equate to crystal ball gazing. Who would have guessed at the beginning that, based on the elucidation of the mechanistic details of CRISPR as an adaptive immune system, this 'unexpected discovery' would outperform any other gene editing technology already in existence in terms of simplicity, speed and costs?

Nevertheless, the potential impact on the biological weapons threat can be somewhat deduced from the current state of CRISPR. Although it cannot be excluded that CRISPR will find its way into a biological weapons program, it does not enable things previously impossible. It rather renders the already possible less cumbersome, less time-consuming and less expensive. Especially when thinking of biological agents with biothreat potential, i.e. first and foremost certain strains of viruses and bacteria, such organisms have been molecularly investigated for decades and genetic alterations have been performed on a regular basis. This is in stark contrast to other organisms, e.g. higher organisms, for which CRISPR presents itself as nothing short of a game-changer – provided that the necessary tacit knowledge is at the experimenter's disposal, the lack of which may present itself as an unsurmountable obstacle in order to make it work. With regard to gene drives, its potential usefulness is limited to diploid or polyploid organisms, which already rules out bacteria and viruses. Furthermore, short population turnover times, i.e. organisms with fast reproduction rates like for instance mosquitoes or other insects, are required for gene drives to be efficient and effective. Hence, so far the spectrum for potential biological weapons applications of gene drives seems very limited. This precludes as well any meaningful involvement of gene drives in future 'cyborg' aspirations that would be based on genetic enhancement in a given population. Also for CRISPR to prove useful in any future human enhancement aspiration by genetic means, a lot of biologically unchartered territory is yet to be uncovered through ground-breaking work by basic scientific research. In practice, the current state of 'omics' research reflects a wealth of accumulated sequence data in the form of letters (A-T-G-C), however the lack of consistent knowledge of the full vocabulary ('what constitutes a gene'?) and the correct grammar ('how is regulation and interaction taking place?') is blatant.

These impressions are also somewhat reflected in opinions and perceptions expressed in literature available to date: CRISPR and gene drives are seen as a challenge to safety and ethics considerations, but are so far not associated with concrete security concerns. Nevertheless, given the dual use nature of this novel technology, a reasonable approach should include raising awareness amongst researchers in the life sciences about the dual use problem when conducting research. Furthermore, given the potential of this novel technology, further monitoring is warranted, also in terms of its potential as a biological weapons threat [22]. This said, it is certainly not the time to panic [23]. The continued evolution of CRISPR is of utmost importance, as this could once again lead to an unexpected revolutionary result. This will allow for maximum use of the huge potential of added benefits for humankind. And as we can see from a recent report, this even applies to CRISPR becoming useful in relation to new avenues for the rapid field detection of pathogens and threat agents [24]. In other words, CRISPR may in the end itself mitigate concerns associated with CRISPR!


### Dr. Cédric Invernizzi

Cédric Invernizzi joined Spiez Laboratory in 2009 and is concerned with arms control issues related to biological weapons and dual use. He supports the Swiss delegations to the Biological and Toxin Weapons Convention and the Australia Group with technical expertise, including monitoring of relevant developments in science & technology, such as the convergence of biology and chemistry. Cédric Invernizzi graduated with an M.Sc. in chemistry and completed his Ph.D. studies in biochemistry at the University of Bern. In 2004 he pursued research in virology, immunology and epidemiology at McGill University in Montréal, Canada.

## Literature


[1] Science, 11 Feb 2016: http://www.sciencemag.org/news/sifter/crispr-weapon-mass-destruction

[2] MIT Technology Review, 9 Feb 2016: https://www.technologyreview.com/s/600774/top-us-intelligence-official-calls-gene-editing-a-wmd-threat/

[3] Jinek M et al. A programmable dual-RNA-guided DNA endonuclease in adaptive bacterial immunity. Science. 2012 Aug 17;337(6096):816-21.

[4] Mojica FJ et al. Intervening sequences of regularly spaced prokaryotic repeats derive from foreign genetic elements. J Mol Evol. 2005 Feb;60(2):174-82.

[5] Jinek M et al. A programmable dual-RNA-guided DNA endonuclease in adaptive bacterial immunity. Science. 2012 Aug 17;337(6096):816-21.

[6] Cong L et al. Multiplex genome engineering using CRISPR/Cas systems. Science. 2013 Feb 15;339(6121):819-23.

[7] Mali P et al. RNA-guided human genome engineering via Cas9. Science. 2013 Feb 15;339(6121):823-6.

[8] Nature, 3 Jun 2015: http://www.nature.com/news/crispr-the-disruptor-1.17673

[9] Tang L et al. CRISPR/Cas9-mediated gene editing in human zygotes using Cas9 protein. Mol Genet Genomics. 2017 Jun;292(3):525-533.

[10] Nature, 3 Jun 2015: http://www.nature.com/news/crispr-the-disruptor-1.17673

[11] Hammond A et al. A CRISPR-Cas9 gene drive system targeting female reproduction in the malaria mosquito vector Anopheles gambiae. Nat Biotechnol. 2016 Jan;34(1):78-83.

[12] http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

[13] Yin H et al. Genome editing with Cas9 in adult mice corrects a disease mutation and phenotype. Nat Biotechnol. 2014 Jun;32(6):551-3.

[14] Maddalo D et al. In vivo engineering of oncogenic chromosomal rearrangements with the CRISPR/Cas9 system. Nature. 2014 Dec 18;516(7531):423-7.

[15] Kleinstiver BP et al. High-fidelity CRISPR-Cas9 nucleases with no detectable genome-wide off-target effects. Nature. 2016 Jan 28;529(7587):490-5.

[16] Zetsche B et al. Cpf1 is a single RNA-guided endonuclease of a class 2 CRISPR-Cas system. Cell. 2015 Oct 22;163(3):759-71.

[17] Nature, 17 Feb 2017: http://www.nature.com/news/why-the-crispr-patent-verdict-isn-t-the-end-of-the-story-1.21510

[18] Schaefer KA et al. Unexpected mutations after CRISPR-Cas9 editing in vivo. Nat Methods. 2017 May 30;14(6):547-548.

[19] https://www.ncbi.nlm.nih.gov/pubmed/28557981#comment

[20] Hammond A et al. A CRISPR-Cas9 gene drive system targeting female reproduction in the malaria mosquito vector Anopheles gambiae. Nat Biotechnol. 2016 Jan;34(1):78-83.

[21] Unckless RL et al. Evolution of Resistance Against CRISPR/Cas9 Gene Drive. Genetics. 2017 Feb;205(2):827-41.

[22] Spiez Convergence Workshop series: https://www.labor-spiez.ch/pdf/de/rue/Spiez_Convergence_2014_web.pdf and https://www.labor-spiez.ch/pdf/en/Report_on_the_second_workshop-5-9_September_2016.pdf

[23] Revill J. „We're Doomed!". CBRNe World. 2017 Feb;39-41: http://www.cbrneworld.com/_uploads/download_magazines/Doomed.pdf

[24] Gootenberg JS et al. Nucleic acid detection with CRISPR-Cas13a/C2c2. Science. 2017 Apr 28;356(6336):438-42.

# Legal By Design - Quelle régulation pour les systèmes d'armes létaux autonomes ?

**Faut-il interdire les systèmes d'armes létaux autonomes? La thèse prohibitionniste est soutenue par un fort mouvement de la société civile. Cette option présente deux défauts majeurs. D'une part, l'objet de l'interdiction est pour le moins complexe à définir en termes juridiques. D'autre part, l'effectivité d'une norme de ce type peut paraître incertaine. Le développement et la mise en œuvre de nouveaux systèmes d'armes robotisés pourraient donc être mieux assurés par des mesures prudentielles applicables dès les premiers stades de la conception de ces systèmes. Ce pourrait être l'objet d'un processus «Legal by Design», inspiré des démarches de «Privacy By Design».**

**Mots-clés:** **Killer Robots, Système d'armes létal autonome, Innovation militaire, Robot militaire, Régulation, Legal by Design**

**Auteur:** **Didier Danet,** Centre de recherche des écoles de Saint-Cyr Coëtquidan

## Introduction

La victoire du logiciel Alphago de Google ou, en sens inverse, l'échec brutal du Chatbot Tay de Microsoft ont brusquement placé sous les feux de l'actualité les développements de l'intelligence artificielle, présentés comme un enjeu scientifique majeur du XXI° siècle. Les possibles applications militaires de l'intelligence artificielle figurent au premier rang de ces questionnements. Le but de cet article est de montrer que la meilleure manière de maîtriser ces applications n'est pas tant de proclamer une interdiction générale que de veiller à l'effectivité des règles existantes par la mise en place de processus innovants.

## Une interdiction populaire

De l'ouverture de discussions au sein de la Conférence sur certaines armes conventionnelles (CCW) à l'initiative de grandes organisations non gouvernementales jusqu'à la signature d'une pétition réclamant l'interdiction préventive des «Killer Robots» par plusieurs milliers de spécialistes, (Russell et al., 2015) le mouvement qui s'oppose à l'avènement d'hypothétiques systèmes d'armes létaux autonomes (SALA) a rencontré d'emblée un succès médiatique notable. Il est désormais appuyé par certains États comme le Pakistan, l'Équateur, l'Egypte ou l'Argentine qui mènent une campagne active au sein de la CCW. De fait, qui souhaiterait se trouver un jour face à un engin militaire capable de choisir lui-même sa cible et de la «traiter» sans aucune forme d'intervention humaine? (Garcia, 2015) Les opposants aux «Killer Robots» demandent en conséquence l'interdiction sans attendre des programmes de recherche susceptibles d'aboutir à ce type de systèmes d'armes. A fortiori, la production et le déploiement de tels équipements serait-il prohibé. (Wareham, 2014)

Trois familles d'arguments sont généralement avancées à l'appui de cette prohibition. (Asaro, 2012, Sharkey, 2010)

La première n'est pas propre à la catégorie particulière des robots autonomes mais ressortit au phénomène de la robotisation en général. La substitution de la machine au combattant sur le champ de bataille est supposée réduire le coût politique des engagements militaires. Il pourrait en résulter un abaissement du seuil d'entrée en guerre susceptible de favoriser le caractère conflictuel des relations internationales, voire l'aventurisme militaire de certains États belliqueux. Les SALA seraient donc condamnables pour le même motif que tout progrès technique permettant à un État de diminuer l'exposition de ses propres forces au risque des conflits armés dans lesquels il est prêt à s'engager. (Lin et al., 2009) (Howlader et al., 2013) Dans le même esprit, de nombreux auteurs dénoncent une menace de prolifération incontrôlable de robots dont le coût est appelé à baisser de manière drastique. (Russell et al., 2015) D'autres enfin, estiment que ces systèmes d'armes minent les valeurs des sociétés démocratiques.(Williams, 2015)

La deuxième famille d'arguments tient aux limites du progrès technique. Certains auteurs comme Ronald Arkin estiment que le comportement des robots peut être assujetti au respect des valeurs et des normes qui régissent les conflits armés. (Arkin, 2009) Au contraire, les opposants aux SALA considèrent qu'aucune intelligence artificielle n'est capable de faire face à la complexité du champ de bataille et ne possède le discernement nécessaire à la prise de décision engageant la vie et la mort d'un être humain. Il résulterait de la délégation au robot d'une telle responsabilité, la perte définitive de la fragile part d'humanité qui prévient la transformation de tout affrontement armé en processus barbare. (Docherty, 2012) Allant plus loin encore dans ce sens, Alex Leveringhaus soutient que, même si le progrès technique permettait de concevoir un SALA sans défaut, il ne serait pas pour autant l'égal d'un combattant humain dans la mesure où il lui manquerait ce qui fait l'humanité du soldat: l'aptitude à ne pas user de la force même si elle est légitime. (Leveringhaus, 2016)

Troisième famille d'arguments, juridique, l'apparition de «robots autonomes» aurait enfin pour conséquence de créer un «vide» dommageable pour les victimes potentielles des erreurs commises par ces robots.

La possibilité pour la machine de prendre des décisions seule, indépendamment de toute volonté humaine ou de tout contrôle humain, rendrait très aléatoire le traitement pénal ou indemnitaire d'un comportement non conforme de cette machine. (Roff, 2013) Dans l'hypothèse de machines véritablement autonomes, cette absence d'effectivité du droit applicable ne pourrait être compensée par la recherche de responsabilités humaines qui auraient été totalement écartées de la boucle de décision.

## Réguler plutôt qu'interdire les «Killer Robots»?

Rappelons le ici pour qu'il n'y ait aucune ambiguïté: nul ne souhaite voir arriver sur le champ de bataille des systèmes d'armes létaux autonomes. Les autorités militaires qui se sont exprimées sur le sujet affirment la nécessité de garder l'homme dans la boucle de décision. La question n'est donc pas d'être pour ou contre les «Killer Robots» mais de savoir s'il est préférable d'interdire préventivement les recherches susceptibles d'aboutir à d'hypothétiques SALA ou s'il vaut mieux réguler les progrès scientifiques et leurs applications militaires au fur et à mesure de leur avancée. (Karppi et al., 2016) (Müller et al., 2015) C'est cette seconde option qui est défendue ici pour plusieurs raisons qui procèdent d'un même constat: les SALA n'existent pas. (Danet, 2016)

Les SALA n'existent pas. Toutes les parties au débat s'accordent au moins sur ce point. Pour ceux que l'on pourrait qualifier de «prohibitionnistes», il s'agit simplement d'une question de temps. Les SALA sont voués à apparaître du fait du croisement des progrès réalisés en robotique, en intelligence artificielle, en mécanique… (Roff, 2014) Pour d'autres, dont l'auteur de ces lignes, cette apparition est plus largement hypothétique. En tout état de cause, aucun système d'armes existant ou en développement ne peut être considéré comme répondant aux

caractéristiques d'autonomie définissant un système totalement autonome. (Danet, 2015)

Il en résulte plusieurs conséquences essentielles.
La **première** est que l'on ne saurait traiter dans le même cadre des systèmes autonomes et des systèmes télé-opérés ou automatisés. Or, c'est la tentation d'un certain nombre d'auteurs (Chamayou, 2013) ou d'organisations (Article_36, 2017) qui souhaitent étendre le domaine d'une éventuelle interdiction à des équipements comme les drones aériens qui n'ont rien d'autonomes puisque la gestion de leurs déplacements aussi bien que les décisions de tirs sont commandées par des équipages intégrés dans une chaîne de décision remontant, pour les plus importantes d'entre elles, aux plus hautes autorités politiques. Si ces systèmes peuvent soulever des questionnements, ce n'est pas à raison de l'autonomie dont ils seraient dotés mais des conditions de leur utilisation, ce qui n'est pas la même chose. (Carvin, 2012, Downes, 2004, Sterio, 2012)

La **deuxième** conséquence révèle le caractère fallacieux du parallèle avec l'interdiction des lasers aveuglants, souvent avancé comme démontrant la possibilité pour la communauté internationale de s'accorder sur le caractère inhumain d'un certain type d'armes et sur la faisabilité d'une interdiction effective. (Grut, 2013) En effet, dans le cas des lasers aveuglants, la technologie prohibée était connue et il était possible de définir la nature, les caractéristiques et le périmètre de l'objet de la mesure d'interdiction. Rien de tel dans le cas des «Killer Robots».

**Troisième** conséquence en effet, et la plus substantielle, les promoteurs d'une interdiction préventive ne sont pas en mesure de définir ce qu'il conviendrait de prohiber. Pour les uns, il s'agirait d'interdire uniquement les armes offensives. Pour d'autres, les systèmes visés ne sont pas ceux qui sont véritablement «autonomes» mais ceux qui sont «Beyond Meaningful Control», cette notion restant à définir. (Crootof, 2016)

Il en résulte que, de confusions en désaccords sur l'objet même du cadre normatif, on ne saurait rien présager de bon quant à la qualité et à l'effectivité des dispositions impératives qui pourraient survenir en vue de l'interdiction des «Killer Robots». La seule solution nous semble donc être de renoncer à un régime d'interdiction et de lui préférer un régime de régulation adaptable au fur et à mesure des progrès constatés dans le champ de l'intelligence artificielle.

## Le processus « Legal By Design »

Faut-il désespérer de l'encadrement juridique des «Killer Robots»? La réponse est assurément négative pour deux raisons.

En premier lieu, il convient de rappeler une évidence : tout système d'armes conçu, développé et mis en œuvre par les forces arrmées doit répondre aux exigences du droit applicable aux situations de conflit. Cela signifie notamment que l'ensemble des prescriptions relatives à la sélection des cibles légitimes et à l'usage de la force à leur encontre vaut pour les «Killer Robots» comme pour les autres équipements létaux. (Melzer, 2013) Il n'y a par conséquent aucun «vide juridique» du fait de l'absence de règles propres aux « Killer Robots ». Au contraire, ne pas introduire de cadre juridique dérogatoire, propre aux seuls SALA, nous semble être de nature à conserver l'unité d'une réglementation déjà complexe et à ne pas faire naître de difficulté nouvelle quant à la question toujours délicate des domaines d'application respectifs de l'exception par rapport à la règle. D'ores et déjà, sans même attendre un hypothétique accord pour la signature d'une convention internationale, les chercheurs, les ingénieurs ou les militaires sont soumis à une obligation de conformité par rapport aux principes juridiques qui gouvernent la mise en œuvre de la force dans les relations internationales et sur le champ de bataille.

La question est donc moins de savoir si les SALA sont encadrés par le Droit (ils le sont) mais comment s'assurer que les obligations qui valent pour eux comme pour tout matériel militaire sont bien mises en pratique dès le stade le plus précoce des travaux de recherche en intelligence artificielle.

L'une des réponses possibles pourrait consister à s'inspirer des processus de «Privacy By Design» qui se sont généralisés dans l'industrie et qui constituent un rempart utile contre les risques induits par la multiplication des systèmes d'information et des objets connectés susceptibles de recueillir des informations personnelles, de les traiter et de les transmettre à des entreprises spécialisées. (Cavoukian et al., 2010, Schaar, 2010) Ces processus obligent les concepteurs des technologies nouvelles à garantir la protection effective des données personnelles depuis la conception de la technologie jusqu'à sa mise en œuvre sur le terrain. Les modalités de mise en œuvre de la «Privacy By Design» (PbD) pourraient-ils valoir pour développer une approche «Legal By Design» à propos des SALA?

Rappelons que l'implantation d'un processus de PbD se déroule en deux temps.

**Le premier** consiste dans la définition (par consensus ou par une autorité régulatrice) d'un certain nombre de principes gouvernant l'action des chercheurs et des industriels afin de promouvoir le meilleur niveau de protection des données personnelles. Les acteurs doivent anticiper les risques susceptibles de survenir et mettre en place une protection par défaut. Le processus doit placer l'utilisateur au centre des préoccupations et présenter des garanties de transparence et de contrôle. Même si ces principes sont parfois soumis à discussion et peuvent varier selon les auteurs (Langheinrich, 2001), leur esprit pourrait être transposé à un processus de type «egal by Design». On y retrouverait les trois dimensions du contenu (Quelles corpus de normes faudrait-il intégrer?), du cycle de vie du robot et du contrôle (Quelles procédures de vérification de l'application «LbD»?)

**Le second temps** de l'implantation d'un processus de «Privacy by Default» consiste dans la mise en œuvre de ces principes à travers des mesures techniques, organisationnelles, humaines… (Kroener and Wright, 2014) qui ne sont pas forcément très éloignées des processus de «compliance» que l'on peut rencontrer dans de nombreuses industries. (Cavoukian et al., 2012) Ce processus pourrait en particulier s'organiser autour des cinq étapes suivantes:

- Identification des projets susceptibles de conférer à un système d'armes une forme plus ou moins aboutie de décision dans la sélection et/ou le tir à l'encontre d'une cible et dès lors soumis à l'obligation du «Legal by Design»
- Evaluation des risques associés à ce programme en fonction des capacités du robot, de l'environnement dans lequel il pourrait être déployé, des missions qui lui seraient confiées, du contexte d'emploi…
- Définition des mesures impératives ou facultatives devant être intégrées par les chercheurs, les industriels et les utilisateurs tout au long du cycle de vie du robot;
- Concertation avec les acteurs concernés afin de mettre en place les mesures opérationnelles aux fins de mise en conformité avec les préconisations;
- Procédures d'audit permettant de s'assurer de la conformité des pratiques à l'égard des règles et des mesures mises en place.

## Conclusion

Les développements à venir de l'intelligence artificielle sont porteurs d'enjeux importants, en particulier pour ce qui est des applications militaires qui ne manqueront pas d'en résulter. Le risque dénoncé par certaines organisations d'abandonner à des systèmes d'armes autonomes, c'est à dire échappant à tout contrôle humain, la responsabilité de sélectionner leurs cibles et d'ouvrir le feu lors de conflits armés, doit être pris en compte. La question n'est pas tant celle du principe d'un encadrement juridique des systèmes d'armes létaux autonomes (ils sont déjà encadrés) que les modalités d'une mise en œuvre effective des normes applicables dès le stade de la recherche et du développement de ces sytèmes. Sur ce point, nous proposons de prendre appui sur l'exemple des mécanismes de «Privacy by Design» qui ont permis un renforcement effectif de la protection des données personnelles et dont les principes pourraient être transposés à l'hypothèse de solutions «Legal by Design».

**Didier Danet**
est responsable du pôle „Mutations de la conflictualité“ au Centre de recherche des écoles de Saint-Cyr Coëtquidan. Avec Ronan Doaré et Gérard de Boisboissel, il a dirigé l'ouvrage „Killer Robots. Faut-il les interdire?“ aux Presses Universitaires de Rennes. Il est par ailleurs Directeur du Mastère Spécialisé „Opérations et gestion des crises en Cyber Défense“.

## Littérature


- ARKIN, R. C. 2009. Governing Lethal Behavior in Autonomous Robots, Boca Raton, Fla, Chapman & Hall/CRC Press.
- ARTICLE_36. 2017. Autonomous Weapons [Online]. Available: http://www.article36.org/issue/autonomous-weapons/.
- ASARO, P. 2012. On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making.“. International Review of the Red Cross 94, 687-709.
- CARVIN, S. 2012. The trouble with targeted killing. Security Studies, 21, 529-555.
- CAVOUKIAN, A., CHIBBA, M. & STOIANOV, A. 2012. Advances in biometric encryption: taking privacy by design from academic research to deployment. Review of Policy Research, 29, 37-61.
- CAVOUKIAN, A., TAYLOR, S. & ABRAMS, M. E. 2010. Privacy by Design: essential for organizational accountability and strong business practices. Identity in the Information Society, 3, 405-413.
- CHAMAYOU, G. 2013. Théorie du drone, Paris, La Fabrique Editions.
- CROOTOF, R. 2016. The Meaning of'Meaningful Human Control'. Temple international and Comparative Law Journal, 30, Crootof, Rebecca, A Meaningful Floor for ‚Meaningful Human Control' (December 18, 2015). Temple International & Comparative Law Journal, Vol. 30, 2016. Available at SSRN: https://ssrn.com/abstract=2705560
- DANET, D. 2015. Un enfer pavé de bonnes intentions: interdire les killer robots. Drones et killer robots: Faut-il les interdire? Rennes: Presses Universitaires de Rennes.
- DANET, D. 2016. La notion d'autonomie et les Systèmes d'armes létaux autonomes. Third CCW Meeting of Experts on LAWS UNOG - Genève.
- DOCHERTY, B. 2012. Losing Humanity. The Case Against Killer Robots, USA, Human Right Watch & IHRC.
- DOWNES, C. 2004. 'Targeted killings' in an age of terror: the legality of the Yemen strike. Journal of Conflict and Security Law, 9.
- GARCIA, D. 2015. Killer robots: Why the US should lead the ban. Global Policy, 6, 57-63.
- GRUT, C. 2013. The challenge of autonomous lethal robotics to International Humanitarian Law. Journal of conflict and security law, 18, 5-23.
- HOWLADER, D., GIORDANO & JAMES 2013. Advanced Robotics: Changing the Nature of War and Thresholds and Tolerance for Conflict-Implications for Research and Policy. . The Journal of Philosophy, Science & Law,, 13, 1-19.
- KARPPI, T., BÖHLEN, M. & GRANATA, Y. 2016. Killer Robots as cultural techniques. International Journal of Cultural Studies, 1367877916671425.
- KROENER, I. & WRIGHT, D. 2014. A strategy for operationalizing privacy by design. The Information Society, 30, 355-365.
- LANGHEINRICH, M. Privacy by design—principles of privacy-aware ubiquitous systems. In: ABOWD, G.-D., BRUMITT, B. & SHAFER, S., eds. UbiComp 2001 : International conference on Ubiquitous Computing, 2001 Berlin. Springer, 273-291.
- LEVERINGHAUS, A. 2016. What's So Bad About Killer Robots? Journal of Applied Philosophy.
- LIN, P., BEKEY, G. A. & ABNEY, K. 2009. Robots in war: issues of risk and ethics. In: CAPURRO, R. & NAGENBORG, M. (eds.) Ethics and Robotics. ISO Press.
- MELZER, N. 2013. Human rights implications of the usage of drones and unmanned robots in warfare, Bruxelles, European Parliament.
- MÜLLER, V. C., SIMPSON, T. W. & QUERRIEN, A. 2015. Réguler les robots-tueurs, plutôt que les interdire. Multitudes, 77-81.
- ROFF, H. M. 2013. Responsibility, liability, and lethal autonomous robots. Routledge Handbook of Ethics and War: Just War Theory in the 21st Century. Routledge, 352-364.
- ROFF, H. M. 2014. The strategic robot problem: Lethal autonomous weapons in war. Journal of Military Ethics, 13, 211-227.
- RUSSELL, S., NILSSON, N. J., GROSZ, B. J., MITCHELL, T. & HORVITZ, E. 2015. Autonomous Weapons: an Open Letter from AI & Robotics Researchers. IJCAI. Buenos Aires, Argentina.
- SCHAAR, P. 2010. Privacy by design. Identity in the Information Society, 3, 267-274.
- SHARKEY, N. E. 2010. Saying 'no!'to lethal autonomous targeting. Journal of Military Ethics 9, 369-383.
- STERIO, M. 2012. The United States' use of drones in the War on Terror: the (il) legality of targeted killings under international law. Case W. Res. J. Int'l L., 45, 197.
- WAREHAM, M. 2014. Pourquoi doit-on interdire les «robots tueurs». Revue internationale et stratégique, 97-106.
- WILLIAMS, J. 2015. Democracy and regulating autonomous weapons: biting the bullet while missing the point? Global Policy, 6, 179-189.

# Performances, contraintes et acceptabilité: quelle approche pour l'augmentation du soldat par les forces armées?

**Exosquelettes, réalité augmentée, prises de substances, gestion du stress, etc. : les progrès scientifiques et techniques ainsi que la convergence actuelle des nanotechnologies, des biotechnologies, de l'informatique et des sciences de la cognition (NBIC) ouvrent des perspectives inédites de renforcement des capacités humaines pour les militaires, tant sur le plan physique qu'intellectuel. Néanmoins, s'il convient pour un soldat d'être le plus efficient possible en opération, les enjeux de l'augmentation des capacités ou des performances humaines sont d'importance car de nouveaux risques médicaux, sociologiques, éthiques et juridiques peuvent découler de leurs usages sur le champ de bataille. Cet article recense les points majeurs abordés par le centre de recherche des écoles de Saint-Cyr Coëtquidan lors de recherche menées sur le sujet en France depuis 2015.**

**Mots-clés:** **Augmentation des performances, augmentation des capacités, combattant, fonctions cognitives, irréversibilité, fonctions physiques, enjeux et risques de l'augmentation, anthropotechnie, acceptabilité**

**Auteur:** **Gérard de Boisboissel,** Centre de recherche des écoles de Saint-Cyr Coëtquidan

## Pourquoi une augmentation du soldat

L'homme est par essence contraint par ses propres limites physiques et mentales, lesquelles sont soumises aux pires conditions dans l'exercice du métier militaire. Pour dépasser ses faiblesses, le soldat a cherché de tout temps à augmenter ses performances afin de répondre à plusieurs exigences :

- Face au nivellement de la supériorité des forces occidentales, nécessité de se servir de la technologie pour maintenir notre supériorité sur le terrain face à des menaces protéiformes dans des environnements incertains et des milieux complexes comme le milieu terrestre.
- Le retour d'expérience terrain montre l'extrême difficulté pour le combattant à durer, notamment dans les missions opérationnelles en Afghanistan ou au Mali, et à être au maximum de ses capacités au moment le plus intense de l'action.
- L'apport de nouvelles technologies nous pousse à réfléchir sur les offres d'augmentation que ces dernières peuvent apporter au combattant. A titre d'exemple, le système FELIN [1] intègre plusieurs nouvelles technologies centrées sur le combattant.
- Parmi ces technologies, la révolution des NBIC (Nanotechnologies, biotechnologies, informatique et sciences cognitives) ouvre un champ de recherche scientifique multidisciplinaire et des perspectives nouvelles dans l'ingénierie du corps humain.
- Le tout participant à une interrogation millénaire qui est de savoir comment augmenter les performances du combattant en opération, en étant mieux équipé, allégé et informé sur son environnement tactique et sur ses capacités physiologiques [2].

## Quels sont les besoins exprimés

Avant d'aller plus loin dans les nouvelles opportunités technologiques, il convient de définir précisément quelle est la juste expression du besoin pour les militaires: celui de durer malgré les faiblesses humaines et de pouvoir ainsi remplir sa mission en contraignant son adversaire et contrôlant son milieu qui n'est pas forcément naturel pour le soldat comme le montre actuellement l'engagement des militaires français dans l'opération Barkhane au Mali.

Fort de cette remarque, le Centre de recherche des écoles de Saint-Cyr Coëtquidan a considéré deux familles d'augmentations possibles pour le futur combattant : les augmentations des capacités cognitives et de soutien psychologique et les augmentations des capacités physiques et de soutien physiologique. Après échanges entre militaires, chercheurs et industriels, il ressort la liste des solutions d'augmentation les plus prometteuses suivantes :

Fonctions cognitives :

- Améliorer la perception de l'environnement,
- Mieux comprendre son environnement,
- Gérer son stress,
- Développer sa force morale,
- Récupération mentale (résistance à l'agression et aux images traumatisantes),
- Aider le chef à faire les bons choix.

Fonctions physiques :

- Récupération physique (fatigue, sommeil),
- Améliorer la mobilité du combattant,
- Développer ses capacités nocturnes,
- Se protéger face aux agressions cinétiques et NRBC.

Les augmentations peuvent être d'ordre technologique par des équipements portés par le combattant et faisant corps avec lui, d'ordre pharmacologique par des apports non thérapeutiques, ou d'ordre chirurgical par des implantations statiques ou dynamiques comme les prothèses, sans omettre les traditionnelles façons de s'augmenter par la formation ou l'entraînement.
Les capacités augmentées (voire supplémentaires comme la nyctalopie) fournies grâce à l'apport technologique devront favoriser l'adaptation du soldat à son milieu et à sa mission. Elles amèneront probablement à une évolution future du rôle du combattant ainsi que des doctrines d'emploi correspondantes.

## Les contraintes et enjeux du métier militaire sur l'intégrité de la personne

«Etre meilleur que l'adversaire pour survivre et remplir la mission»: telle pourrait être la devise du soldat en opération.

Mais si le militaire risque de donner sa vie pour sa mission, il s'avère que sa valeur humaine implique de tout faire en sorte pour protéger au mieux le combattant, tant dans son action militaire que dans son intégrité physique et mentale.

L'individu doit donc être considéré avec son humanité qu'il faut à tout prix préserver, car le combattant n'est ni un objet ni un pion tactique, mais un frère qui se bat pour vous et la Nation. On lui doit donc le meilleur, en développant les capacités de son corps et son esprit mais sans les altérer. Cette remarque est fondamentale dans le sens où la question de l'augmentation ne doit pas poser de problème d'irréversibilité, sauf en cas d'accord express de l'individu.

Néanmoins toute décision d'augmentation sera soumise aux contraintes du moment, notamment les contraintes opérationnelles. Actuellement, le militaire a pour devoir la réussite de sa mission, même au péril de sa vie. Si demain des

augmentations du combattant permettent de réduire le risque pour lui ou d'augmenter ses performances, et par conséquent permettre de mener à bien la mission qui sans elles risquerait d'être un échec, alors elles devront être prises en compte. Ce sera toujours au chef militaire de décider selon les circonstances du moment si oui ou non l'augmentation prévue est nécessaire et bénéfique à l'opération.

## L'acceptabilité de l'augmentation

Si les applications à venir de ces technologies sont assez facilement acceptables dans le cas de la réparation du corps humain pour des soldats ayant été blessés ou handicapés lors d'opérations militaires, leur acceptation sur des sujets sains pose plus de problème.
En pratique, il conviendrait que la réversibilité de l'augmentation soit totale pour l'individu et sans effet sur lui. En outre, qu'elle n'entraîne pas de diminution par des effets secondaires, et aucune conséquence physiologique ou physique sur l'individu.
L'individu doit également donner son plein consentement en amont de la situation opérationnelle, après un avis médical, notamment dans le cadre d'augmentations d'ordre pharmacologique ou chirurgicale.
Ces augmentations devront également être acceptées par la société, et sur ce point, les blocages seront d'abord culturels: l'acceptation dépendra des cultures. Si les pays asiatiques sont très friands de ces évolutions car pour eux un individu doit se démarquer des millions d'autres, si le continent nord-américain y voit l'intérêt scientifique, l'Europe, elle, y sera probablement plus réticente suivant un principe de précaution tout comme les communautés religieuses. Mais on peut noter que beaucoup d'étudiants d'aujourd'hui seront les soldats de demain, lesquels tout naturellement auront tendance à répliquer les usages et comportements qu'ils ont dans le civil –tels que la prise de substances avant les examens, ou le dopage dans le monde sportif - lors de leurs missions et tenter de faire admettre de telles pratiques. Le combat représente en effet le paroxysme de danger et de violence pour un individu et ce dernier cherchera naturellement par tous les moyens à augmenter ses capacités pour survivre dans cet environnement, par essence très dangereux.

## Toute augmentation doit être validée

Selon le Médecin chef des Services Frédéric Canini, toute augmentation devra être validée, ce qui est déjà le cas aujourd'hui, le processus permettant d'évaluer une substance ou un matériel obéissant à un nombre de règles permettant de s'assurer de son innocuité et de son efficacité.
Sur le plan pharmacologique, les armées seront susceptibles d'utiliser des substances améliorant la performance. Actuellement, en France [3], seules sont autorisée les substances accroissant la vigilance, c'est-à-dire la caféine à libération prolongée. Son utilisation est très encadrée. L'état-major désigne les unités autorisées à prendre de la caféine pour une mission donnée. La prescription est faite par le médecin de l'unité en respectant le consentement des combattants dûment informés des effets attendus, comme ceux potentiellement négatifs, de la substance. La prescription comme les résultats de la prise sont soumis au secret médical. La caféine est ensuite délivrée par un pharmacien. La maitrise des effets secondaires est assurée grâce à un test lors d'un exercice. Les combattants sont alors considérés d'un point de vue médical comme des sujets à suivre nécessitant a posteriori des tests sur ces derniers.

## Les risques et impacts qui en découlent

Les risques seront sanitaires avec des effets possibles sur sa santé à moyen ou long terme, avec des risques d'addiction et des risques psycho-traumatiques une fois que les effets de l'augmentation et du sentiment d'invulnérabilité se seront dissipés.
En outre, apparaitront relativement rapidement des risques sociaux car l'augmentation des performances individuelles induira inéluctablement une culture de l'augmentation qui aura pour effet de faire naître des tensions entre les unités qui pourront bénéficier de cette augmentation, celles qui seront autorisées à les mettre en œuvre et enfin celles qui ne le pourront pas faute de moyens ou faute d'autorisation (médicale, légale).
Un autre risque social correspondra à une escalade non maîtrisée de l'augmentation, une sorte de course à la surperformance dans certaines unités de combat pour se rendre plus fort, ce qui aura pour conséquence une obligation de s'augmenter, non pas pour être meilleur mais pour tout simplement pour pouvoir intégrer le groupe et être accepté par lui.

A moyen terme, un impact majeur des effets de l'augmentation de l'individu va concerner les politiques de recrutement des Armées, avec son devoir de justice envers les candidats appelés à rejoindre les Armées ou être sélectionnés pour tel ou tel spécialité ou mission.

En effet, la lecture du code génétique d'un individu et la connaissance de ses potentielles faiblesses ou prédispositions pose de redoutables questions. Si la modification génétique ne semble pas envisageable pour les forces à un horizon court, la question du dépistage en amont va profondément remettre en question les traditionnels moyens de sélection des postulants aux Armées. Un dépistage génétique étant rapide et peu onéreux de nos jours, les Armées pourront très prochainement se procurer le séquençage du génome de chaque postulant et le sélectionner non plus uniquement sur des critères physiques, mais aussi sur des critères génétiques: pourra-t-on recruter un individu dont un gène lui donne un risque à 60% de développer un cancer à 40 ans? Est-il acceptable de l'engager uniquement pour un contrat court?

De la même façon, sera-t-il acceptable de sélectionner selon des critères génétiques les meilleurs candidats à un type de métier militaire (tireurs d'élite, Forces Spéciales, aptitude à commander) ou bien à un type de fonction préconisant certaines aptitudes spécifiques? Le traditionnel SIGYCOP [4], qui est un profil médical permettant de déterminer l'aptitude d'un individu à exercer dans l'armée française, devra-t-il être complété par une lecture et une étude de la signature génétique de chacun?

## La pression du monde civil

Ce dernier point sera amplifié par le fait que demain dans le monde civil, une enquête sur les gènes à risque sera très probablement systématiquement effectuée par certaines assurances pouvant empêcher de contracter un emprunt par exemple. Les Armées seront-elles assez fortes pour préserver la possibilité à tout individu de la rejoindre selon des critères d'aptitude mesurés et factuels? Et non pas sur des taux d'occurrence de potentiels risques estimés qui enfermeraient l'individu dans un monde normé tel que décrit dans le film « Bienvenu à Gattaca » de Andrew Niccol (1997).

Les Armées vont être également confrontées à une acceptation individuelle de l'augmentation pour augmenter les performances d'individus dans les milieux des loisirs, des études et du sport. Les mondes de l'athlétisme, du football et du cyclisme sont d'ailleurs déjà fortement contaminés par le dopage, tout simplement car la société attend d'eux des performances extraordinaires qui sont généralement inatteignables sans augmentation. L'Institution militaire devra prendre en compte ses soldats qui se sont déjà augmentés par eux-mêmes et apporter une réponse forte via une politique d'augmentation claire.

## Les augmentations irréversibles à travers l'exemple de l'anthropotechnie

Selon le médecin général Lionel Bourdon de l'IRBA, Institut de Recherche Biomédicale des Armées, l'anthropotechnie va devenir un phénomène de société à l'avenir et permettra d'effectuer de façon irréversible des améliorations sur l'homme, qui seront totalement acceptées par celui-ci, voire encouragées par la société civile. Déjà, la réparation prothétique de l'ouïe est devenue banale, celle de la vue est naissante et les premières prothèses totales de membres sont désormais testées.

Si ces performances sont avant tout réparatrices, il est tout à fait

envisageable dans un avenir très proche que ces transformations n'aient pour but qu'une amélioration brute de la performance, sans optique de soins curatifs. Par exemple, si la correction de la myopie est vue comme une réparation, une augmentation de la vision à 12/10ème au lieu de 10/10ème sera considérée comme une amélioration et une augmentation des capacités de la personne, notamment pour des métiers nécessitant une forte acuité visuelle.

Dès lors, 12/10ème ou plus ne va-t-il pas devenir la norme pour les pilotes de chasse ou les tireurs d'élite? Auquel cas, est-ce que ce sera à l'Institution d'assurer l'augmentation de la vision des candidats ? Et sur quels critères seront-ils recrutés: en fonction du futur meilleur candidat augmentable ou bien en fonction du meilleur actuel augmenté?

## La position des Forces

Face à de telles questions nouvelles pour notre société, une institution militaire se doit d'interdire certaines dérives potentielles même s'il faut pour cela accepter de ne plus tendre vers le risque zéro pour ses soldats sur le terrain. Elle doit pour cela définir des lignes rouges à ne pas dépasser pour respecter la dignité humaine du combattant et le protéger face aux mirages d'une invincibilité artificielle. Elle doit en outre se positionner face à la révolution idéologique du Transhumanisme dont les prises de position vont devenir des thèmes de discussion phares pour les prochaines années dans le monde civil.

La position de la France est pour l'instant très mesurée sur la question de l'augmentation individuelle. En effet, notre Nation a depuis fort longtemps mis en avant les qualités du groupe avant celui de l'individu. C'est l'esprit de corps et la cohésion qui soude un groupe comme l'indique le colonel Eric Ozanne [5], car une troupe a le niveau physique de son soldat le plus faible. Si au sein d'une section un seul flanche, c'est toute la section qui sera ralentie dans sa manœuvre et dans l'accomplissement de sa mission. C'est donc principalement par l'entraînement et la préparation physique qu'une unité sera apte à durer dans le temps, avec l'aide des équipements appropriés intégrant les nouvelles technologies.

Il reste que l'augmentation, si elle respecte l'individu, doit être étudiée sous l'angle de l'efficacité militaire. Une opération commando extrêmement délicate dont le succès est primordial pour les Forces ou la Nation devra se poser la question de l'augmentation des performances des commandos pendant le temps de leur intervention. Comme par exemple prendre des substances pour ne pas dormir pendant 72H. Ainsi l'intérêt collectif pourra-t-il supplanter les principes de droit à la libre disposition de son corps, notamment en fonction des contraintes qui pourraient être imposées au soldat à raison de son état ou de la situation de crise ou de guerre? Ces contraintes pourront par exemple impliquer d'aller outre son consentement libre et éclairé au regard des risques probables ou possibles pour la mission en cours, de son importance pour la manœuvre, et voire même au-delà pour préserver la santé de la personne.

## Conclusion

Les différentes méthodes d'augmentation des performances du soldat se déclinent via différents moyens: les moyens technologiques embarqués sur des équipements faisant corps avec lui et qui ne posent pas de questions majeures, mais aussi des moyens pharmacologiques par des apports non thérapeutiques ou des moyens chirurgicaux par des implantations statiques ou dynamiques qui eux posent question car ils touchent à l'intégrité de l'homme.

Deux instances doivent intervenir dans le contrôle des pratiques possibles:

a) l'instance politique afin d'assurer une réglementation nationale et internationale, car si la France se veut restrictive et prudente, ne perdons pas de vue que plusieurs autre pays ou organisations ne le seront pas car poussés par des ambitions de rayonnement ou d'efficacité directe sans considération éthique. Seule une règlementation internationale permettra de contrer de nouvelles pratiques néfastes pour l'homme.

b) l'instance militaire avec le soutien du service de Santé des Armées. Si elle se doit d'être prudente en évitant tout potentiel état séquellaire consécutif à une augmentation octroyée au soldat, elle devra aussi être réaliste et pour toute mission opérationnelle:
   - raisonner en termes d'effets sur la mission et sur le collectif, notamment au niveau du groupe ou de l'unité de combat.
   - considérer à la fois l'acceptation individuelle et l'acceptation collective de l'augmentation.
   - Prendre les mesures pour avoir le soutien et l'accompagnement du milieu médical militaire, sur le court terme et sur le long terme.
   - Préciser la juste place du médecin militaire dans son rôle nouveau de traducteur et effecteur d'une demande d'augmentation, demande qu'il n'a pas prescrite lui-même car elle a été formulée par un opérationnel en opération.
   - S'imposer des garde-fous juridiques pour éviter toute dérive.

En amont, elle doit se donner des règles précises quant aux impacts inévitables qu'une éventuelle augmentation pourra avoir sur le recrutement des soldats, comme par exemple s'assurer que dans notre société ultra judiciarisée, un postulant ne pourra pas se retourner vers l'institution militaire s'il n'a pas été sélectionné à cause de critères qu'il considère comme subjectifs, ou bien si celle-ci n'a pas permis à un soldat d'être «augmenté» afin d'être retenu pour certaines spécialités militaires.

Pour conclure, il est important que les Armées se saisissent des questions médicales, sociologiques, éthiques et juridiques, que posent les perspectives de l'augmentation des performances du soldat, avant que le monde civil ne prenne position pour elles selon des orientations qu'elles ne souhaiteraient pas.


**Gérard de Boisboissel**

est ingénieur de recherche au centre de recherche des écoles de Saint-Cyr Coëtquidan (CREC). En lien avec les pôles d'excellence, notamment le pôle Mutation des conflits, il développe les contacts entre le CREC et le monde industriel et les institutions extérieures, et co-organise les évènements scientifiques de certains programmes de recherche dont la robotique militaire et le soldat augmenté.
Il est également le secrétaire général de la chaire „Cyberdéfense et cybersécurité" Saint-Cyr/Sogeti/Thales depuis la fin de l'année 2013.


## Informations


[1] Fantassin à Équipements et Liaisons INtégrés développé par la société Safran Electronics & Defense.

[2] Hors-série de la revue Défense et Sécurité Internationale (DSI) sur le soldat augmenté, décembre 2015.

[3] Médecin chef des Services Frédéric Canini, IRBA, lors du colloque du 19 juin 2017 sur « le soldat augmenté », Paris.

[4] S: membres supérieurs / I : membres inférieurs / G : état général / Y: yeux et vision / C : sens chromatique / O : oreilles et audition / P : psychisme.

[5] Ancien chef de corps du 2ème Régiment étranger d'infanterie, chef d'état-major interarmées des forces armées en Guyane.

# Cyber warfare in smart environments

**Future conflicts will increasingly involve creative use of the "full-spectrum" warfare. The future battles might take place in the areas characterized by high penetration of IT technology, such as smart cities. The combination of opportunities and threats introduced by the proliferation of (semi-)autonomous vehicles and IoT devices will have a profound impact on both defensive and offensive side of future cyber operations. At the same time, the increasing pressure on ensuring cost-effectiveness of defense investment will lead to increased re-use of the infrastructure for both civilian and military purposes and focus development on dual-use technologies.**

**Keywords:** **Cyber operations, data-centric security, dual use, humanitarian assistance and disaster relief, Internet of Things, smart spaces**

**Author:** **Dr. Konrad Wrona,** NATO Communications and Information (NCI) Agency

## What will bring the future

Probably the only sure thing about the future of warfare is that it will be different than the present. However, despite of this uncertainty there are several visible trends in evolution of military operations, which will with high probability shape the future conflicts, especially in respect to the cyber domain.

First of all, the conflicts increasingly involve creative use of the "full-spectrum" of warfare, including the use of regular and irregular tactics across all dimensions of war [1] and, in particular, extensive use of cyber operations. This implies that the future wars will most probably involve use of both regular and rebel-like forces and will often operate in a grey-zone between peace and open war. Such "hybrid" tactics have been already observed in cyber space, where large scale attacks can be performed by national actors, also with help of black-hat hackers and volunteers [2][3].

Secondly, the conflicts adapt to the changing human living environment and available technologies [4]. This means that the future battlefields might take place in the areas characterized by high penetration of IT technology, such as smart cities. But, in fact, even farmlands of the future will be characterized by a high density of sensors and actuators, which could be leveraged for military operations. Moreover, the recent advances in robotics and artificial intelligence (AI), might ultimately lead toward the situation where future wars will be increasingly fought in smart connected environments and using (semi-) automated unmanned vehicles and equipment. This would also result in moving decision power down in the chain of command.

Finally, the need to counter the rebel-like tactics and to ensure financial effectiveness of military operations, leads to an increased focus on civilian-military collaboration during both war and the peacetime. This includes both involvement of volunteers into the defense activities during wartime and re-use of military capabilities and technologies for civilian purpose during peacetime.

## Future of cyber operations

In the context of a full-spectrum warfare, cyber operations will be an integral element of any future military operations, especially as the increased connectivity and remote management capability of cyber-physical systems offer opportunities to perform successful attacks on national infrastructure, as was demonstrated by some recent events [5][6][7].

Use of unmanned and autonomous equipment is becoming wide-spread in military operations – such vehicles offer several advantages, both in respect to operational capabilities and reducing risk to soldiers' life. However, they also bring some security risks [8] and can be suspect to remote cyber-attacks [9].

It is likely that the Alliance Future Surveillance Capability (AFSC), which is planned to replace the current AWACS capability by 2035, will rely to a large extent on unmanned vehicles, as well as on data fusion from various sources, including civilian systems operated by individuals and communities. The increased availability of highly capable commercial-of-the-shelf (COTS) sensor platforms and drones make them also a plausible extension to specialized military-grade equipment, as well as an affordable alternative for mission non-critical operations. Nevertheless, such use of COTS devices for military purposes introduces several security challenges [10] and require deployment of some additional security mechanisms [11]. Moreover, it is plausible that also the adversaries, which we will face in the future conflicts, including insurgents and irregular forces, will use the COTS IoT devices in their operations, thus introducing new threats and attack paths. An example of such new threat might be use of inexpensive COTS drones for transport of explosives and for intelligence gathering.

The combination of opportunities and threats introduced by the proliferation of (semi-)autonomous vehicles and IoT devices will have a profound impact on both defensive and offensive side of future cyber operations. In particular, it will have an impact on existing approaches to risk assessment and operational scenarios, increasingly requiring real-time correlation and analysis of large amount information from diverse physical and virtual sources.

Increased dependence of machine learning and artificial intelligence (AI) techniques for the definition of the operational picture brings also risk related to potential targeted attacks on machine learning algorithms by a knowledgeable adversary. The practicality of such attacks was presented in several recent studies, e.g., [12]. The adversary AI techniques are applicable to both dedicated military systems as well as to dual-use and civilian systems; however, the systems operated by civilian authorities might be particularly susceptible to analysis and reverse engineering of data fusion mechanisms due to their greater exposure and possible open access.

## Smart city as a future battlefield against human adversaries and nature

The increasing pressure on ensuring cost-effectiveness of defense investment will lead to increased re-use of the infrastructure for both civilian and military purposes and focus development on dual-use technologies. One of the obvious areas of such re-use of military capabilities is humanitarian assistance and disaster relief (HADR).

During both HADR and military operations, it is vital for the responders to understand the situation in the affected area, which is often referred to as situational awareness (SA). Obtaining and maintaining an up-to-date situational awareness is critical to planning and executing the recovery as well as military operations, including making decisions about where to allocate resources and how to prioritize operations. As the operations continue, situational awareness needs to

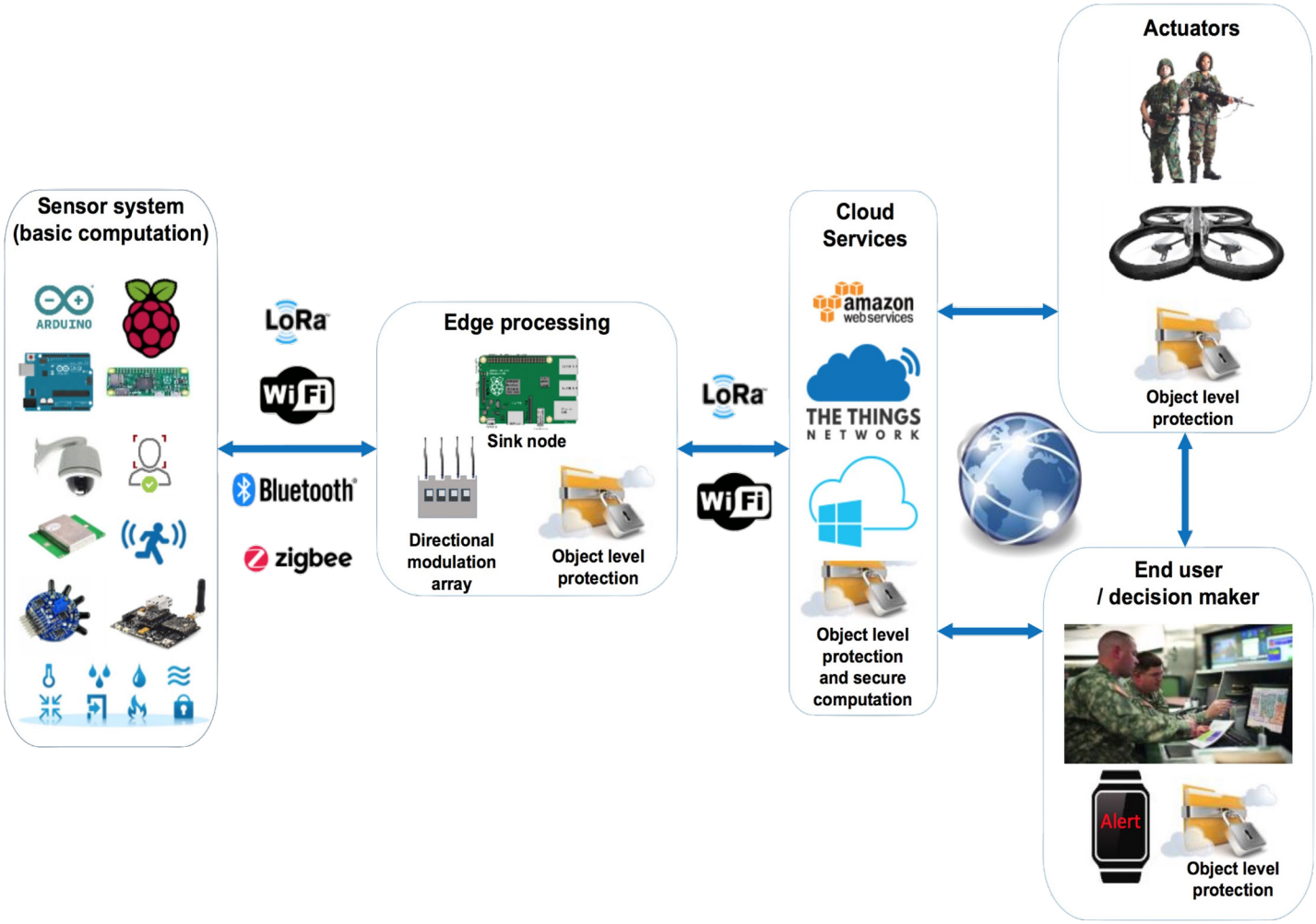



*Figure 1: Example of a system architecture for secure HADR applications developed within the NATO STO IST-147 working group.*

be continuously updated based on changing conditions in the areas of operation.

As the amount of world population living in urban areas will be increasing, more and more HADR operation will take place in cities. In a smart city environment, with a significant deployment of Internet of Things (IoT) sensors, IoT has a potential to enhance SA by providing more accurate reporting of conditions in the area, status of available services, and logistics. An example of a system architecture for HADR operations involving military personnel is depicted in Figure 1.

Integration of the multiple available IoT information sources is critical to providing and maintaining SA and enabling effective HADR operations. However, it also raises significant security challenges.

In particular, when designing federated situational awareness applications that incorporate information obtained from various sources, a number of objectives related to security, privacy, and trust should be considered. In fact, some of these objectives can be conflicting and might require implementation of sophisticated cryptographic mechanisms in order to fulfill expectations of all stakeholders.

From the perspective of personnel involved in a military or a HADR operation, it is of paramount importance that the SA data is readily available when required, and that its authenticity and integrity can be determined. The trustworthiness of this data must be effectively assessed, based on factors such as origin, ownership, pedigree, or other metrics. Moreover, the interconnected smart city system can also constitute an additional attack surface during both military and disaster response activities – in fact a recent study has shown that many of the systems operated by cities are insecure or misconfigured [13]. Therefore, appropriate security measures must be implemented when interconnecting mission-critical SA systems with the existing smart city IoT infrastructure, as well as with the emergency services operated by cities in order to prevent potential cyber-attacks.

On the other hand, from the perspective of users and operators of IoT systems available in a smart city, it is important that their personal data is properly protected against unauthorized access and that wherever possible, data is properly anonymized or removed as long as it does not affect mission critical information needs. Indeed, data may need to be provided at different access levels (e.g., anonymized and summarized data to the regular citizens and more detailed data to emergency responders).

Providing access to information available in a smart city may rely on two basic approaches and the choice of the approach may depend on the source of the information that is to be accessed.

In the case of information harvested from publicly owned infrastructure (e.g., city government), the most efficient approach might be a priori federation of identity and access management techniques, enabling emergency response teams to authenticate themselves to the smart city systems and access the information in accordance with a predefined access control policy.

When this approach is not feasible, either from a practical perspective (e.g. access to private IoT sensors in home environments), or due to policy reasons (e.g. lack of pre-existing trust between organizations), a breaking-glass policy could be used. A breaking-glass policy enables overriding of a standard security policy in an exceptional situation, typically in combination with strong auditing / logging measures, enabling a-posteriori analysis of information usage.

In addition to information harvested from existing smart city infrastructure, it is reasonable to assume that disaster response teams would also deploy their own IoT systems. Such systems would most likely be specifically implemented in order to

support HADR operations and would be better integrated with SA systems and be able to reliably function in challenging environmental conditions.

One of the major problems of security and trust management in the federated IoT domain is ensuring that parties/objects unknown to each other can communicate securely. A critical enabler is effective identity management, which might rely on Trusted Platform Modules (TPM) to confirm the identity of users/objects in IoT [14], [15]. Establishment of trust in remote IoT devices could be attained via remote attestation, which is a well-known technique for verifying the state of remote computing devices [16]. Hardware-based techniques based on TPM are very effective and applicable especially to high-end devices that can accommodate the additional layouts. With the use of TPM it is possible to achieve strong authentication within a group of COTS IoT devices by creating trusted security domains [17]. TPM also provides a tamper resistant element for secure storage of cryptographic material, such as keys, and other sensitive information on the devices.

## Cryptographic countermeasures and data-centric security

The military environment has been traditionally very conservative and risk averse (and rightly so) when it comes to adoption of new cryptographic mechanisms. Protection of sensitive information relies on use of secret cryptographic algorithms, whereas use of commercial cryptography is limited to unclassified and restricted systems, mostly at the network and session layers, as well as for non-repudiation. However, the use of commercial cryptographic solutions within military systems is being currently reconsidered. This change is driven by several facts. Firstly, it is caused by the changes in the way modern military operations are performed, requiring more active collaboration with non-NATO nations and tighter civilian-military collaboration. Secondly, changes in the technological landscape result in an increased use of IT services operated by third parties, such as public cloud.

Current information protection practice relies to a large extent on network-layer mechanisms for compartmentalization of information and separation between different COI and security domains. Improving data protection and information sharing relies on achieving efficient compartmentalization of information within a single network. This requires deployment of security measures internal to the network that enforce security policies at the data object level – this approach is often referred to as data-centric security. These security measures are needed to support the whole lifecycle of data, including storing, transmitting and processing data. Furthermore, the enforced security policy needs to capture both need-to-know and responsibility-to-share requirements.

The collaboration with external partners, often with a limited trust relationship, introduces several challenges related to information sharing – in respect to both enforcement of data-centric access control policies, as well as authentication and deployment of required security mechanisms. In particular, cryptographic enforcement of access control policies introduces several important challenges, such as translation of traditional access control policies into the access structures used for encryption [18], [19] and an appropriate choice of encryption mechanism [20].

The increasing use of IT resources provided by third party providers, such as public clouds, is another main driving factor behind implementation of data-centric security measures – especially of cryptographic access control [21]. Public clouds offer an attractive and cost-effective platform for executing computation on large sets of data, such as aggregation of information acquired from both civilian and military sensors. However, these benefits can be only realized, when appropriate cryptographic mechanism supporting secure computation, such as homomorphic encryption and secure multi-party computation, are in place.

## Conclusions and way ahead

Future military operations will be often performed in a smart environment and will involve increasing amounts of smart technologies, ranging from sophisticated sensors to autonomous vehicles and equipment. Ability to provide an effective and trustworthy data fusion from a broad range of sources, operated by different parties, will be critical for development of appropriate situational awareness and appropriate execution of operations.

The increasing pressure on ensuring cost-effectiveness of defense investment will lead to increased re-use of the infrastructure for both civilian and military purposes and focus on development of dual-use technologies. However, this paradigm introduces important security challenges, which need to be adequately addressed in order to ensure its acceptance within both the military and civilian communities.

Although, the military systems will continue to rely mostly on well-tested cryptographic techniques, such as symmetric encryption algorithms, the importance of more advanced cryptographic techniques will be increasing, opening new opportunities for military and civilian research collaboration.

Finally, more investigation needs to be performed to understand the accreditation requirements related to integration of military systems with civilian IoT solutions.


### Dr. Konrad Wrona

currently holds a Principal Scientist position at the NATO Communications and Information (NCI) Agency in The Hague, The Netherlands.

He has almost 20 years of work experience in an industrial (Ericsson Research and SAP Research) and in an academic (RWTH Aachen University, Media Lab Europe, and Rutgers University) research and development environment.

He has received his M.Eng. in Telecommunications from Warsaw University of Technology, Poland in 1998, and his Ph.D. in Electrical Engineering from RWTH Aachen University, Germany in 2005.


## References


[1] D. Van Puyvelde, "Hybrid war – does it even exist?," NATO Review Magazine, 2015.

[2] J. Nazario, "Politically motivated denial of service attacks," in The Virtual Battlefield: Perspectives on Cyber Warfare, vol. 3, C. Czosseck and K. Geers, Eds. 2009, pp. 163–181.

[3] A. Schmidt, "The Estonian Cyberattacks," in The fierce domain – conflicts in cyberspace 1986-2012, J. Healey, Ed. Washington, D.C.: Atlantic Council, 2013.

[4] M. van Creveld, "The Transformation of War." The Free Press, 1991.

[5] A. Greenberg, "How an entire nation became Russia's test lab for cyberwar," Wired, 20-Jun-2017.

[6] Dragos Inc., "CRASHOVERRIDE - Analysis of the Threat to Electric Grid Operations," 2017.

[7] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier - Version 1.4," 2011.

[8] K. Kirkpatrick, "Can we trust autonomous weapons?," Commun. ACM, vol. 59, no. 12, pp. 27–29, 2016.

[9] J. A. Marty, "Vulnerability Analysis of the MAVLink Protocol," Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2014.

[10] K. Wrona, "Securing the Internet of Things: A military perspective," in Proc. of the IEEE World Forum on Internet of Things (WF-IoT), 2015, pp. 502–507.

[11] K. Wrona, A. De Castro, and B. Vasilache, "Data-centric security in military applications of commercial IoT technology," in 2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016, 2017, pp. 239–244.

[12] I. Evtimov, K. Eykholt, E. Fernandes, T. Kohno, B. Li, A. Prakash, A. Rahmati, and D. Song, "Robust Physical-World Attacks on Machine Learning Models," 2017.

[13] N. Huq, S. Hilt, and N. Hellberg, "US Cities Exposed," 2017.

[14] NIST, "Security Requirements for Cryptographic Modules," 140–2, 2002.

[15] Trusted Computing Group (TCG), "TPM Main Part 1 Design Principles Specification Version 1.2 Revision 116," 2011.

[16] T. Abera, L. Davi, A. Paverd, and G. Tsudik, "Invited: Things, trouble, trust: On building trust in IoT systems," in 53nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2016.

[17] J. Furtak, Z. Zieliski, and J. Chudzikiewicz, "Security techniques for the WSN link layer within military IoT," in IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016, pp. 233–238.

[18] A. Armando, S. Oudkerk, S. Ranise, and K. Wrona, "Formal Modelling of Content-Based Protection and Release for Access Control in NATO Operations," in Proc. of the Foundations and Practice of Security (FPS), 2013, vol. 8352, pp. 227–244.

[19] A. Armando, S. Ranise, and K. Wrona, "SMT-based Enforcement and Analysis of NATO Content-based Protection and Release Policies," in Proc. of the 1st ACM Workshop on Attribute Based Access Control (ABAC), 2016, pp. 35–46.

[20] S. Oudkerk and K. Wrona, "Cryptographic Access Control in support of Object Level Protection," in Proc. of the Military Communications and Information Systems Conference (MCC), 2013.

[21] A. Armando, S. Ranise, R. Traverso, and K. Wrona, "Compiling NATO Authorization Policies for Enforcement in the Cloud and SDNs," in Proc. of the Computer and Network Security Conference (CNS), 2015, pp. 741–742.

# Prediction and Trends about Governmental Satellite Activities

**This article introduces the reader to the current, aggregate trends in the development and deployment of space related satellite systems providing a world-wide overview of both classified and civilian capabilities. Defense satellite and space systems are grouped into one category ranging from optical and synthetic aperture radar (SAR) sensors based payloads, to signal jamming, and cyber-attacks, to environmental threats such as electromagnetic radiation up to collisions with other objects and or antisatellite weapons are in use today. In addition to the military category, civil space applications are essential for a broad array of functions increasing not only security but also a variety of unintentional threats, even for Switzerland. Decreasing launch costs in combination with Space 2.0 are opening Earth's orbits to almost all countries worldwide.**

**Keywords:** **Satellite navigation, Earth Observation, Imagery Intelligence, GPS, Space Situation Awareness, Megaconstellations, ComSats, Commercial off the Shelf components**

**Author:** **Eric Wiesmann,** RUAG Schweiz AG

## Decreasing launch costs are reducing the barriers to space access

Due to increasing "small launcher" capabilities and due to decreasing launch costs of US and Russian launch services, totally 61 countries worldwide have completed or are running one or more satellite programs by their governments. Governments around the world launched 692 satellites in various orbits between 2006 and 2015, of which two-thirds were for exclusive civilian use or for dual use capabilities. Over half of those satellites (56%) were placed in Low Earth Orbit (LEO). The majority of these programs are of a civilian nature.

However, the USA, Russia, China, the UK, France, Germany, Israel, Italy, Japan, South Korea, Australia, Canada, Peru, Turkey and NATO, whose space activities are clearly led by the USA, are the only countries worldwide with classified space-born object supported defense systems. Those systems can be roughly grouped into the following categories: Earth Observation (EO) with imagery intelligence (IMINT), space situational awareness (SSA) (Figure 1) including early warning, space surveillance and tracking, secured and clustered communication capabilities, Navigation, secured space-born Data Relays, and Electronic and Signal Intelligence (ELINT/SIGINT).

*Figure 1: Space Situation Awareness provides additional protection to military SIGINT. Credit: Globvision*

## Satellites within the military space programs are not limited to Earth Observation

Within military space, Navigation, Earth Observation and Telecommunications are the three largest military satellite applications worldwide. As more governments become involved in space activities through their respective national space agencies, Earth Observation (EO) including reconnaissance, imagery intelligence and meteorology remains the largest civilian satellite application with governmental space involvement. Notwithstanding, the official civil nature of these EO missions, most are equipped with optical instruments, or at least with powerful cameras, as well as with electromagnetic sensors that might offer defense agencies additional value through the data they generate. Earth observation is more widely distributed geographically as more countries in Europe and Asia are acquiring satellite systems. Strong growth is expected in Asia thanks to China's demand for Earth observation missions and the deployment of the country's navigation system (Beidou). Japan and South Korea are also becoming more active in defense-related Earth observation.

## Satellites with a defense purpose still dominate the governmental satellite market

Operators of defense satellites are the largest participants of the satellite manufacturing and space transportation industries (Launcher) because of the enormous costs that such classified satellite systems incur. These companies are principally found in the USA, Russia and China, but also in minor form in the UK, Israel, France, Germany, Italy, India and Japan. The USA dominates the space related defense market in market value (economic driver) and in number of satellites. Both historical military space powers, the USA and Russia will contribute more than two-thirds of the military demand for satellites by number and will launch about the same number of satellites in the coming decade as they did in the past decade. However, the coming missions will have different aims than past missions. USA will further focus on new initiatives in missile defense -even though delayed-, and hosted payloads such as SSA and ELINT. USA will continue to invest in increasing their communication capabilities and GPS in the next ten years, while Russia, in contrast to USA, having higher country prioritizes such as focusing on enhancing their own GPS (Glonass) and improvement lifetime of the new generations of military spacecraft by upgrading civilian ComSats with dual-use capacities.

## The dominance of established space capabilities is the result of large governmental spending

As of mid 2017, a dozen countries have a history of using satellite systems and an established domestic space industry to design and launch the satellites required by government agencies. The USA, Russia, China, Japan, India and the European countries (driven by France, Germany, the UK and Italy) will continue to comprise most of the future demand (80% of all government satellites). This dominance is the result of large governmental spending to replenish and maintain existing satellite capabilities in various application

domains (e.g., meteo, nav., comm., imagery and data relay) and to develop new ones (e.g., missile defense) with the corresponding launch autonomy.

Another dozen countries have development programs ongoing to domestically design and manufacture the operational satellites needed by their governments (and possibly to launch them): Canada, Israel, Brazil, South Korea, Argentina, Turkey, Kazakhstan, the UAE, Saudi Arabia and the Ukraine.

Both of these groups of countries, with an established space program or with development programs, are focusing on Earth observation (IMINT, meteorology), ELINT, SIGINT, space situational awareness (SSA) for missile defense/early warning, space surveillance, telecommunications (either on dedicated satellites or on dual-use satellites), navigation, data relay.

Another 40 countries are showing a large interest in satellite capabilities, in order to be more responsive to social and economic development and to develop a national space industry. Governments in these countries have two objectives: developing communications infrastructure and preserving sovereignty over territories and natural resources. Most countries in this category do not have national engineering or industrial capability in satellite systems; as such, they contract with foreign industries to procure and launch their satellites. During the past decade, a dozen new space agencies have been created around the world - by countries as diverse as Bahrain, Chile, Algeria, Iran, Bolivia, Mexico, South Africa, Belarus, Turkmenistan and Kazakhstan - to manage investments in satellite systems and technologies. Other countries are considering the creation of a national space agency to promote and coordinate their investment in satellite systems and technologies.

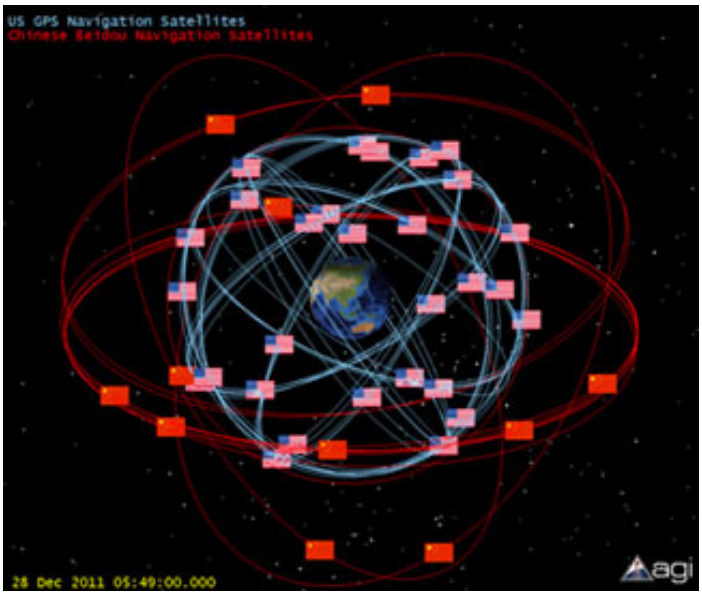



*Figure 2: The above graph is impressively showing the difference of orbits chosen by USA and China. Taking into account the expansion of the Chinese navigation system in MEO, much higher accuracy can be inferred.* ***Credit:*** *AGI Business Partners*

Altogether, these three categories of countries contribute to growth in satellite demand by procuring Earth observation, communications, navigation, space science and exploration, and technology demonstration satellites. Civilian satellite systems are developed jointly between two or more countries (such as China/Brazil for CBERS, USA/Argentina for SACAquarius and France/Israel for Venus) when bi-/multilateral cooperation brings greater benefits to the parties. Military-dedicated satellite systems for electronic intelligence (ELINT), signal intelligence (SIGINT) and imagery intelligence (IMINT) are procured in a limited number of countries (such as the USA, Russia, European countries, China, Japan and Israel) where the national defense and security priorities require a dedicated infrastructure.

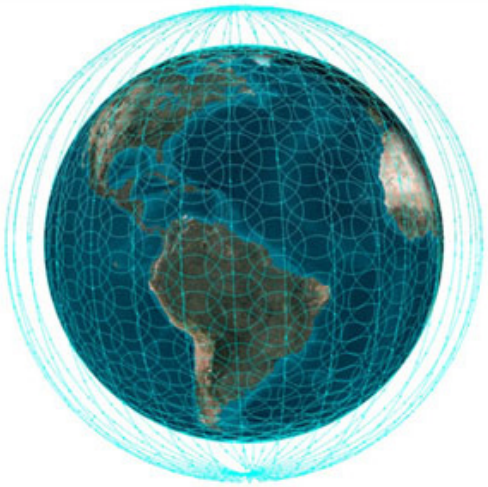


*Figure 3: Each spot on the picture above represents a spot of the array antenna system of one OneWeb satellite. With the first 643 satellites a high redundancy is already reached. Credit: OneWeb.world*

## The growth dynamics differ between civilian and military agencies

The number of civilian satellites will increase by 39% in the next decade, whereas the number of defense satellites will increase more modestly by +9% relative to the past decade. Two-thirds of the 880 government satellites to be launched between 2016–2025 are for civilian or dual use applications, and the remaining 290 satellites are for exclusive defense use. Due to the significant increase of governmental satellites, the proportion of civilian satellites has grown in the last 10 years because 1) proprietary military satellites remain concentrated in a limited number of countries and 2) a growing number of countries are ordering civilian and dual-use satellites to deploy in constellations with several identical satellites.

## Military satellite navigation is driven by the USA (GPS), but China's Beidou system is catching-up

In addition to the US GPS satellite navigation system, Russian (GLONASS), European (Galileo), China (Beidou), Japanese (QZSS) and Indians (IRNSS) system are all employed by developed and developing countries in various ways according to the level of socio-economic development of a particular country. Highly accurate navigation is not only needed for civilian needs for the transportation of goods and people but also for agricultural production. However, the associated functionality for redeployment of troops, intelligence services and finally for highly precise bombardments of selected targets, which is why defense agencies and military need full and independent access to such navigations systems. The Japanese satellite navigation system is an operating from inclined, elliptical geosynchronous orbits to achieve optimal high-elevation visibility in urban canyons and mountainous areas. The navigation system aims to broadcast GPS-interoperable and augmentation signals, but besides the original Japanese Quasi Zenith Satellite System (QZSS) signals from a three-spacecraft constellation, the Michibiki series, to improve independency of the US GPS signals.

The Chinese Beidou satellites navigation system are, in contrast to GPS and GLONASS, using both geostationary satellites and satellites in intermediate orbits (Figure 2), and featuring a phased array antenna for navigation signals and a laser retroreflector and additionally an S/L-band dish antenna and a C-band horn antenna. Even though most of the first generation satellites failed early in operation, the Chinese intend to control missiles, fighters, marine and troop logistics with their navigation systems, which will be as accurate as the GPS layer for governmental use when the next generation satellites are deployed. Lamentably, by using spin-off products such as GNSS RF front-end modules, terrorist organizations may be able to increase their capabilities.

## Enhanced milsatcom capabilities needed

The telecommunication domain of space systems is driven by the replacement of existing milsatcom capabilities in the USA, Russia, China and European countries. Nevertheless, Turkey, Egypt and Indonesia are establishing their own communication capabilities. Both the Russian and Chinese governments have expressed willingness to place more Comsat orders with their national industries at the expenses of foreign suppliers. Telecommunications remain by far the dominant military application in GEO, while other applications (such as meteorology and space security) are marginal. In December 2015, China launched Gaofen-4, their first satellite for permanent observation of the Earth into the geostationary orbit. India will do the same in 2017 with Gisat-1. For instance, Apstar 9 was developed by CAST while all previous Apstars were ordered from Western manufacturers. The following Apstar 6C and 6D were also booked by CAST in 2015-2016; In Russia, RSCC contract with ISS with payload supplied by TAS and MDA. GEO related classified telecommunication satellite for the period between 2018-2025 are forecasted with 34, incl. WGS, AEHF, Syracuse, DSN, Radugo, Feng Huo.

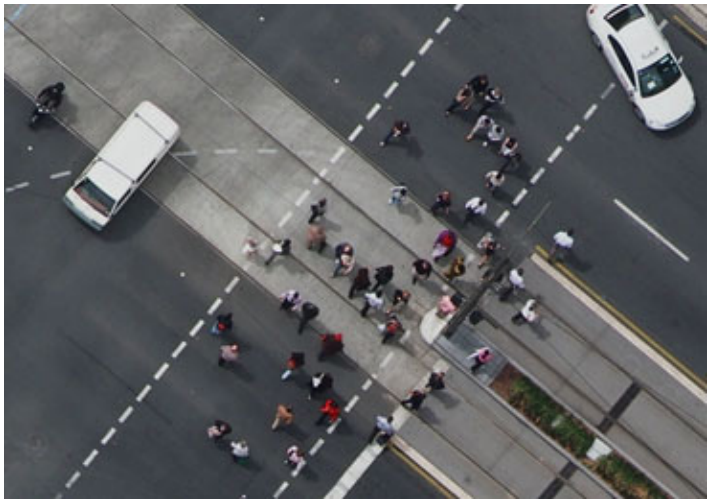


*Figure 4: 30cm resolution of a COTS camera before digital zooming Credit: Aerometrex*

## ELINT still remain niche capabilities

Space security related applications account for just over 10% of the satellite market with a total of 40 satellites. Early warning and electronic intelligence (ELINT) remain niche capabilities but are expanding outside the United States and Russia, with France preparing an operational system (Ceres) and China launching the Shi-Jian satellite series. In the United States and Russia, early warning and electronic intelligence (ELINT) payloads are hosted on classified satellites in HEO in addition to GEO satellites. Strong growth is expected in Asia thanks to China's demand for Earth observation missions and the deployment of the country's navigation system (Beidou). Japan and South Korea are also becoming more active in defense-related Earth observation. Asia will represent about 20% of military satellite demand, up from 10% in the previous decade. In contrast, Europe is stable as the replacement of its milsatcom capabilities will only start at the very end of the forecast period and as dual-use and hosted payloads limit the demand for additional dedicated military systems. In the next 6 years, SBIRS, Mercury, F/O, US-KMO, Tundra, will be sent to a GEO orbit.

## OneWeb recognized as a game changer

Driven by the reality of constant outlays for military expenditures, military operators are finding commercial satellite systems to be an increasingly attractive solution. In fact, current military doctrines are stressing information superiority as a core tenet, which would necessitate an increase in satellite deployment and costs, if this ability cannot be otherwise outsourced. The multiplication of theaters of military operations and the increasing use of UAVs require growing strategic and tactical communications capabilities. Commercial leases are the most developed at the USA's DoD, which, along with two media companies (Echostar/Dish and the News Corp), is one of the largest customers for commercial satellite bandwidth. Commercial bandwidth is mainly used for UAVs' return and dissemination links and for troops' comfort communications.

Compared to classified satellites, civilian governmental and commercial satellites are generating large amounts of data, which can be used by terrorist organizations or their networks for communication, navigation and target evaluation. Google maps is today very accurate and presents with real time traffic data promising information for attacks. The megaconstellation Oneweb offers in 2020 from any place on the world with a simple, USD 800 expensive access point, connection to the internet and therefore to the darknet as well. The current OneWeb satellite network design consists of 648 micro satellites (a total of 900 satellites are planned to put in LEO) of about 150 kg operating in a 1250 km LEO (Figure 3).

Each satellite is capable of delivering at least 8 gigabits per second of throughput to provide Internet access to homes and mobile platforms using its high throughput Ku-band payload. Apart from OneWeb, the second megaconstellation of civil communication type satellites will be deployed by Space X. The megaconstellations introduce a clear paradigmatic change in the space industry by the two new categories of small satellites have started to revolutionize satellite design, testing and production, and the use of Commercial off the Shelf components (COTS) allows operators to develop a satellite within less than 24 months. Those operators are taking shorter lifetimes into account but getting better imageries than with best space qualified cameras (Figure 4) used by Lockheed Martin. Technology development is growing as more countries test technologies in-orbit with pathfinder and demonstration missions.


**Eric Wiesmann**

is "Head of Marketing and Sales" at RUAG Schweiz AG, RUAG Space in Zurich, Switzerland. Started in 2001 as a development engineer for Laser Communication systems, he has held a number of engineering and management positions at RUAG Space, Oerlikon Space and Contraves Space. Eric completed studies in electrical engineering, business administration and law with area of specialization „transfer of know-how of dual-use technologies".

# The impact of Additive Manufacturing in future defence operations

**Additive Manufacturing technologies, most widely known as 3D-printing, are meant to play a key role in the industry. These technologies are already enabling the improvement of current commercial products, and also the development of new ones. However, their full potential goes beyond the civil sector, as they provide the flexibility, customization, on-site and on-demand manufacturing which is needed for defence operations. To further explore the potential deployablity of these technologies, the European Defence Agency (EDA) launched in 2016 a project, aiming at raising awareness on 3D-printing in defence. The future is already here, but there is still work to be done together in making out of these technologies a real game-changer for defence operations.**

**Keywords:** **Technology foresight, defence technologies, dual use, research and innovation, additive manufacturing, deployable 3D-printing, logistics, support to operations, platform availability, circular economy.**

**Author:** **Patricia Lopez Vicente,** European Defence Agency (EDA)

## The impact of Additive Manufacturing in future defence operations

Additive Manufacturing (AM), widely known as 3D-printing, has been identified by the European Commission as one of the key enabling technologies to improve European industrial competitiveness given its ability of rapid, delocalised and flexible manufacturing. Therefore, 3D-printing is meant to play a key role in the industry, as it is already enabling the improvement of current commercial products, and also the development of new ones. Although AM technologies are already introduced in the civil industry and are currently used by many defence companies, it is considered that the defence sector is not exploiting AM benefits to the maximum. There is significant potential for additive manufacturing technologies to enhance defence capabilities including mobility, sustainability, effect and protection through field repair & maintenance, improved logistic support for deployed forces or sustainability in warfighting and peacekeeping missions.

Indeed, the expected growth of the AM market could generate many advantages for the European defence community: cost reduction on production tools and parts, design enhancements, reduced time to end-user, increased technical and commercial competitiveness. At the same time, 3D-printing is set to considerably impact the maintenance of military platforms through the production of spare parts and equipment components. Since the European air, land and maritime defence systems have complex and particular underlying structures, the customization facility of AM and its on-site and on-demand characters are particularly interesting for defence. Equally beneficial are the weight reductions and the increase in resistance and durability of components which in conventional subtractive manufacturing processes were more difficult to achieve due to the processing and time limitations. Having AM technologies in the area of operation might significantly impact the course of CSDP [1] missions. Time between failure and restore the availability of platforms, transportation and storage of significant quantities of spares can be decreased, with the associated costs reduction, reducing the logistic footprint of an operation.

## EDA Technology identification, assessment and prioritization

In order to be aware of emerging technologies, such as Additive Manufacturing, which can disrupt defence capabilities, EDA needs a systematic understanding of evolving technical trends and their effect on future European defence capabilities, both long and short term. To this end, EDA established a Tech Watch and Foresight activity, providing the input for the EDA process of technology assessment and prioritization. This activity defines the processes to systematically collect information about new technologies and technological trends, based on well-known methodologies such as technology watch, horizon scanning and technology foresight.

The EDA Technology Watch and Horizon Scanning activities are based in IT tools specially developed for the identification of emerging and emerged technologies with potential interest for defence applications. These tools collect state of the art information on different technological areas. The Technology Foresight [2] activity, provides EDA Research & Technology (R&T) [3] community with a long term vision on technologies, in response to EDA and its Member States (pMS) need to have a wide and systematic view of the technological landscape of common interest when planning R&T activities. The activity supports the identification of the future of emerging technologies and their impact in defence capabilities in 20 or 30 years. When considering different futures, the long-term work and scenarios from Capability Development Plan (CDP) are taken into account.


*Figure 1: EDA 3D-printing Lab transported to the C-130 aircraft, ready for the airlift.* © Source EDA

The positive effects of these activities are to boost the interest and increase the technology culture within the EDA R&T community, and also the identification of new technologies, such as 3D-printing, coming from the civil sector. Their tangible outcome is that the information gathered though these activities fed the Overarching Strategic Research Agenda (OSRA) and CapTechs Strategic Research Agendas (SRAs) technology mapping processes and their long-term vision. As a result, in the Strategic Research Agenda of the CapTech Materials & Structures 2014, additive manufacturing was included as one of the technology gaps to address [4]. To identify the possible areas for cooperation, a workshop on the impact of AM in defence was held in November 2014. The main conclusions

*Figure 2: EDA 3D-printing Lab during the airlift, inside a C-130 aircraft.* © Source EDA

of the workshop included a need to raise awareness of the defence potential of additive manufacturing technology and for a demonstration of the utility of additive manufacturing in an operational situation.

## EDA project on Additive Manufacturing

Therefore, the project "Additive Manufacturing: Feasibility Study & Technology Demonstration" was launched in 2016 to assess the areas where additive manufacturing can make a greater contribution to defence capabilities. It also has the objective of raising awareness in the defence community, promoting a better understanding of the potential of these technologies, thereby stimulating their implementation in defence specific areas. To achieve these objectives, the project was divided in three main work strands: A) A desktop study to place additive manufacturing and its potential in a defence context; B) A deployment of a 3D-printing facility in a simulated scenario; and C) An Exhibition to showcase the potential of AM [5].

### *State of the art and strategic reports*

This work summarised the state of the art of relevant additive manufacturing technologies, comparing it with existing R&T and manufacturing capabilities in Europe. The main outcome of this work strand is the identification of opportunities and weaknesses for AM in the European defence sector, highlighting the technology and non-technology factors delaying or preventing European armed forces from benefiting from the technology. The acknowledgement of the showstoppers is essential to maximize the impact of future activities which will have to address technology and non-technological issues such as gaps in the value chain, intellectual property rights, standardization and certification, test and evaluation, or skills and education. The analysis is completed by an impact and risk analysis on the main defence areas defined (i.e. logistic support-spare parts, maintenance-repairing in operations), indicating what defence capabilities might be impacted and which economic benefits may be expected in the near-term, mid-term and long-term. A complete roadmap for implementation of AM in the most promising defence areas has been developed, identifying specific sector value chains (VC) in key areas where the implementation of AM technologies have greater potential to impact defence capabilities.

A wide consultation took place with public and private, defence and civil stakeholders and policy makers, and different initiatives at European level, such as the AM Platform [3], European Standardisation in AM, the PPP "Factories of The Future (FoF)", or projects launched under Horizon 2020 (AMAZE Project, CAxMan, FoFAM, etc.). This consultation not only helped to gather information about 3D-printing in defence, but also raised the awareness of the availability of the technologies to the defence sector, and of the interest of AM in defence to the civil sector.

### *3D-printing facility deployment*

With the objective of raising the awareness of the impact of AM technologies, and due to the lack of operational experience of additive manufacturing, a deployment of an AM facility in a simulated deployed scenario was organized. The objective was to demonstrate the feasibility of deploying these technologies in support of a military operations and to demonstrate the operational utility of the technology (Figure 1-2). The design of the 3D-printing Lab included the selection of the equipment to be installed in a standard container, meeting the requirements of military airlift (Figure 3). The 3D-printing Lab is independent, self-contained and self-sufficient, in order to prove its deployability, and it was fully prepared meeting regulations for air transport. To achieve these objectives, the EDA 3D-printing Lab was deployed, testing its performance prior to and during deployment, producing parts to demonstrate the utility of the facility.

*Figure 3: The interior of the EDA 3D-printing Lab, including two AM machines, post-processing, storage, and working/ design area.* © Source EDA

The simulated deployed scenario was the EDA sponsored European Advanced Airlift Tactics Training Course (EAATTC 17-3), which took place in Zaragoza airbase (Spain) from 22 May to 9 June 2017. The 3D-printing Lab was successfully deployed and the test flight [7] of the AM lab was pivotal to examining the feasibility of its deployment by air. During the deployment, the AM lab generated a lot of interest from the multinational units involved in EAATTC 17-3. The deployment also underscored the strong interest and potential of AM technologies across all military branches (pilots, maintenance, technicians and logistic support).

### *Exhibition "Exploring Additive Manufacturing impact in Defence capabilities"*

The conclusions of the project, including the equipment used and typical objects and materials produced were presented in the exhibition "Exploring Additive Manufacturing impact in Defence capabilities", on 12 September 2017. The objective of this activity was again to raise the awareness of additive manufacturing technology and their defence potential, exemplifying how the technology could change the way operations, logistic support or maintenance of platforms is performed and to discuss the possible impact on defence capabilities. The event brought together both the operational and the technical communities, and defence and civil sectors, creating a setting to exchange ideas and boost the level of awareness of the potential benefits of additive manufacturing technologies to support defence needs (Figure 4).

The participants had the opportunity to attend different talks from EU bodies, Ministries of Defence responsible for operations, and from industry and academia. Exhibitors with experience of additive manufacturing at different stages, from research to equipment and materials production and industrial applications were also present, creating a balance

between academia, applied R&T and industry, including small and medium enterprises (SMEs). This composition provided a forward looking perspective, at high level and focussed on defence applications.

This project represents a clear example of how cross-fertilization of ideas from different domains, from R&T to operations, enhances defence capabilities, especially when supporting missions. Through this work, the project aims to directly support different R&T groups at EDA, as the CapTechs Materials & Structures, Ammunition, Components, Air, Maritime or Land, and other work strands such as Logistic Support, Spare Parts, Support to Operations, Education and Training, Skills & Competences, Test & Evaluation, or Standardization & Certification. Furthermore, as it is highly relevant to increase awareness on AM, this project helped the dissemination of AM in different defence contexts.

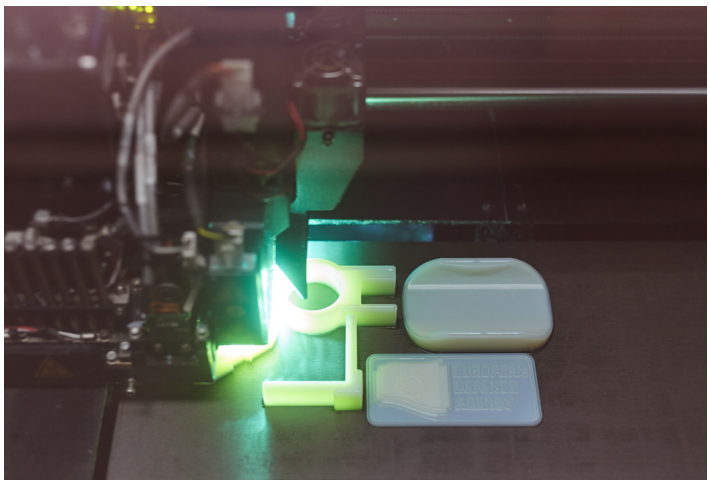


*Figure 4: One of the AM equipment of the EDA 3D-printing Lab producing parts on demand.* © Source EDA

## AM and circular economy

Additive manufacturing is allowing not only reductions in weight or increased strength, but also reduction of waste material and increase the repairability of complex parts. However, to obtain these benefits, the new products will have to be designed taking into account these new production method, the sustainability throughout the whole life cycle and the reuse of the production and waste materials. The complexity allowed by additive manufacturing provides great benefits in different applications, but also new considerations have to be taken into account to ensure the use of advanced materials, their performance thought out their life cycle, and, to close the loop, their repairing, appropriate disassembly and the reuse of the materials in production processes.

All these considerations, if taken into account when designing new products to be 3D-printed, can provide great benefits, from job creation to availability of raw materials. Therefore, the research and development activities in this area could have a significant impact by embracing the circular economy principles already from the design face. Furthermore, in order to fully embrace the circular economy principles there is a need to identify the types of 3D-printers "compliant" with the circular economy principles. Also important is to identify regulatory barriers or enablers towards the full implementation of AM technologies. Exploring the feasibility and applicability of the principles of the circular economy in the broader sector of defence, could further facilitate the transformation process envisaged in the European Commission communication also through defence stakeholders. The European Defence Agency positioned in the crossroad of the Member States, the European Union Institutions, the European Defence Industry and the European Defence R&T community, is enabled to facilitate the transition of the circular economy principles to the defence sector [8].

## The future of AM in defence

Increasing awareness of AM's potential for defence is crucial. Equally important will be to create synergies between the R&T community and the operational military staff, helping to understand the capability requirements from the defence side. Further exploration of 3D-printing facilities deployed in operations will be highly beneficial to gather data on their impact. With this, the awareness and knowledge about the capability improvements that AM can generate will be widened and improved. In addition, specific training will be required to make this technology effective and accessible to the military users. On the technology side, further work is foreseen at EDA regarding the use of additive manufacturing for energetic materials, light weight ballistic protections and packaging and cooling of electronic components. Other key challenges to address are standardization of processes, certification of parts and legal aspects, among others.

The dissemination of these developments, along with the exchange of information on efforts in participating Member States, will help create momentum at European level and support the identification of potential collaborative activities. Fulfilling the technology and non-technological gaps will enhance the logistical and operational agility of armed forces, giving European defence a game-changing competitive advantage in a rapidly evolving technological and conflict landscape.

The future is already here, but there is still work to be done together in making out of these technologies a real game-changer for defence operations.

© Source EDA – pictures taken by contractor Fundación Prodintec within the project 16.ESI.OP.144 "Additive Manufacturing: Feasibility Study & Technology Demonstration"


### Patricia Lopez Vicente

Since 2013, working at the European Defence Agency as Project Officer and CapTech Moderator (R&T Group) on Materials & Structures Technologies, and from September 2017, as Project Officer on European Defence Research. Supporting the development of a comprehensive R&T Planning process, thought: horizon scanning, technology watch and technology foresight, assessment and prioritization, and promoting technologies such as Additive Manufacturing. From 2004 until 2013, working in Isdefe´s Technology Foresight Unit, supporting the Spanish Ministry of Defence R&T Directorate. Academic background as Master in Science (Materials Physics) and MBA on R&T management.


## References


[1] CSDP: Common Security and Defence Policy of the European Union.

[2] It is proposed to pursue technology foresight, as a solid and comprehensive method to assess the future impact of technologies on defence capabilities, in order to build resilient European Defence Technology and Industrial Base (EDTIB) and Armed Forces.

[3] http://eda.europa.eu/what-we-do/our-current-priorities/research-technology

[4] https://www.eda.europa.eu/what-we-do/activities/activities-search/captech-materials-structures

[5] http://eda.europa.eu/info-hub/press-centre/latest-news/2016/12/22/3d-printing-eda-launches-new-project-to-test-feasibility-in-the-defence-field

[6] European Union Additive Manufacturing Platform: http://www.rm-platform.com/

[7] http://eda.europa.eu/info-hub/press-centre/latest-news/2017/06/02/successful-test-flight-for-eda-3d-printing-lab-during-deployment-at-eaattc-17-3

[8] http://eda.europa.eu/info-hub/press-centre/latest-news/2017/01/13/eda-project-to-push-circular-economy-in-defence

# Die Bedeutung von Modellbildung und Simulation für die Zukunft der Streitkräfte

**Modellbildung und Simulation (M&S) unterstützt die Streitkräfte heutzutage in vielen Bereichen. Die Komplexität der Systeme moderner Streitkräfte macht den Einsatz von Simulationssystemen für Tests, Bewertungen und Leistungsnachweise zwingend erforderlich. Grundsätzlich bieten sie die Möglichkeit, komplexe Aufgaben mit geringerem Risiko für die Umwelt sowie für Leib und Leben wirtschaftlich zu erfüllen. Dieser Artikel zeigt die Anwendungsbereiche von M&S im militärischen Kontext sowie Trends und Herausforderungen im Hinblick auf die zukünftige Bedeutung für die Streitkräfte.**

**Keywords:** **Modellbildung & Simulation, Angewandte Forschung, Trends, Chancen, Herausforderungen, Streitkräfte**

**Autoren:** **Matthias Lochbichler & Klaus Kappen,** IABG mbH - Defence & Security

## Einleitung

Aufgrund der steigenden Komplexität heutiger Systeme, Aufgaben und Prozesse gewinnt M&S ständig an Bedeutung. M&S ist eine querschnittliche Disziplin, die in vielen Bereichen Anwendung findet. Sie dient im Wesentlichen zur Vorhersage und Entscheidungsunterstützung, zur Ausbildung und zur Unterstützung von Systementwicklungen. Im Zuge des Systems-Engineering und der modellbasierten Entwicklung werden in der Forschung und Entwicklung bereits heute immer mehr virtuelle Prototypen eingesetzt, wodurch sich die Anzahl an realen Prototypen reduziert.

Besonders im militärischen Bereich unterstützt M&S die Streitkräfte seit Beginn der Computerentwicklung in vielen Bereichen. Das Gesamtziel der militärischen Systemanalyse ist, einen Einblick in dynamische militärische Systeme und deren Fähigkeiten zu erlangen. Simulationssysteme liefern dabei wertvolle Werkzeuge für Test, Bewertung und Leistungsnachweis von komplexen Systemen.

Die Zukunft der Modellbildung und Simulation ist stark abhängig von der Leistungsfähigkeit von Computern, die jedoch weiterhin wachsen wird. Auch im Hinblick auf zukünftige Technologien und Technologiefelder wird M&S als wichtiger Bestandteil genannt. Schlagworte in diesem Zusammenhang sind u.a. Industrie 4.0, Künstliche Intelligenz, Autonome Systeme, Virtual & Augmented Reality, Cyber Defense & Warfare und Big Data. Aus rüstungstechnischer Sicht wird M&S für die Entwicklung von Wehrmaterial an Bedeutung gewinnen. Aus militärischer Sicht wird M&S einen zunehmend wichtigeren Beitrag für die moderne Kriegsführung, die Ausbildung und das Training sowie zur Unterstützung im Einsatz liefern.

Dieser Artikel gibt einen Überblick über M&S in den Anwendungsbereichen der Streitkräfte und zeigt Trends und Herausforderungen im Hinblick auf die zukünftige Bedeutung für die Streitkräfte.

## Anwendungsbereiche und Aufgaben von M&S

Es existiert eine große Bandbreite an Anwendungsmöglichkeiten von M&S zur Unterstützung der Streitkräfte. In der Literatur findet man häufig die Unterteilung in vier Anwendungsbereiche (vgl. [1], [2], [3]):

A. Analyse und Planung,
B. Entwicklung und Beschaffung,
C. Ausbildung und Training sowie
D. Einsatzunterstützung.

Im Rahmen der Anwendungsbereiche werden Systeme und Szenarien auf unterschiedlichsten Systemebenen analysiert und bewertet. Hierzu gehören die strategische, die operative, die taktische und die technische Ebene. Bei M&S-basierten Analysen wird auf den verschiedenen Systemebenen grundsätzlich die gleiche Art von Fragestellungen behandelt. Die grundlegenden Fragen sind:

- Warum sollen Kräfte verwendet werden?
- Was sind die Aufgaben der Kräfte, um das erforderliche „Warum" zu erreichen?
- Wie soll das erforderliche „Was" erreicht werden (durch welche Kräfte)?

Untersuchungsgegenstand der Analyse und Bewertung sind Systeme, die sich wiederum aus weiteren Systemen zusammensetzen. Daher ist ein „System-of-System"-Ansatz erforderlich. Vernetzte Systeme stehen im Mittelpunkt von Analyse und Bewertung, aber auch die Vernetzung von Ausbildungssimulatoren wird weiter vorangetrieben. Dabei werden auf den unterschiedlichen Systemebenen bei der Analyse verschiedene Dimensionen von Raum und Zeit verwendet. Die Analyse beschränkt sich nicht ausschließlich auf militärische Systeme, sondern muss je nach Fragestellung auch relevanten Rahmenbedingungen der weiteren Umwelt berücksichtigt werden. Neben militärischen Aspekten sind dies politische-rechtliche, sozio-kulturelle, ökonomische und Informationseinflüsse sowie die allgemeine Infrastruktur.

### *A. Analyse und Planung*

Im Anwendungsbereich der Analyse und Planung unterstützt M&S bei der Beantwortung sicherheitspolitischer und militärstrategischer Fragestellungen. Hierzu gehören das Erkennen und das Analysieren von Konflikten und Krisen sowie das Entwickeln von Handlungsalternativen. Im Rahmen der Streitkräfteplanung, welche Fähigkeitsanalysen und Analysen zur Streitkräftestruktur, -umfang und Ausrüstung unter Berücksichtigung von Kosten, Leistung und Wirkung im Einsatz umfasst, unterstützt M&S ebenfalls. Die Schwerpunkte von M&S liegen hier auf der schnellen und umfangreichen Analyse komplexer Prozesse und großer Datensätze. Simulationen werden eingesetzt zur [3]:

- Erstellung und Bereitstellung von Szenaren u. a. bei Wargames,
- in der Analyse von Fragestellungen mit den Methoden des Operations Research (OR) und
- im Einsatz schneller Analysekapazität für die Entwicklung, Bewertung und Optimierung von Lösungsansätzen.

Operations Research ist die Anwendung wissenschaftlicher, vorwiegend mathematischer Methoden zur Unterstützung im Entscheidungsprozess durch Bewertung und Auswahl von alternativen Lösungsansätzen unter der Berücksichtigung von Wirksamkeit, Kosten und Risiken. Es dient sowohl zur Entscheidungsvorbereitung als auch zur Beratung des Entscheidungsträgers. Zu den OR-Methoden gehören

z. B. Verfahren der Statistik, lineare und nichtlineare Planungsrechnung, Netzplantechnik, dynamische Optimierung, Warteschlangentheorie, Spieltheorie und eben Simulation.

## *B. Entwicklung und Beschaffung*

Der zweite Anwendungsbereich von M&S umfasst die Entwicklung und Beschaffung von Produkten und Services. Der Anwendungsbereich deckt den gesamten Lebenszyklus technischer Systeme ab. Dabei wird M&S sowohl bei der Bedarfsermittlung als auch bei der Bedarfsdeckung (Analyse, Projektierung, Einführung) sowie in der Nutzung von Systemen eingesetzt. M&S unterstützt

- bei der Analyse und Bewertung von Fähigkeitsbeiträgen technischer Lösungen,
- bei der Erarbeitung, Auslegung, Bewertung und Auswahl von Lösungskonzepten (gemäß der virtuellen Produktentwicklung),
- bei der Minimierung von Realisierungsrisiken und -kosten,
- beim Nachweis der Herstellbarkeit und Realisierbarkeit von Produkten sowie
- bei der Abnahme in Form einer integrierten Nachweisführung.

In der Phase der Analyse muss der militärische Nutzer die erforderlichen militärischen Fähigkeiten definieren, die er braucht, um seine verschiedenen Aufgaben und Missionen zu erfüllen. Diese Anforderungsdefinitionen berücksichtigen technische Einschränkungen und Prognosen von Forschungs- und Technologie bzw. Entwicklung-Aktivitäten.

In der Phase Konzeptentwurf / Risikominimierung werden in der Regel technische Anforderungen definiert und Machbarkeiten getestet. In dieser Phase findet die Prüfung von technischen Konzepten in Bezug auf die Erfüllung der erforderlichen militärischen Systemfähigkeiten (Eignungsprüfung) statt.

In der Phase der Nutzung ist die Aufrechterhaltung der genehmigten Leistungen und der erforderlichen militärischen Fähigkeiten zu prüfen.

Alle diese Analyse- und Testaktivitäten erfordern die Unterstützung von M&S und seinen Werkzeugen.

## *C. Ausbildung und Training*

Im Bereich der Ausbildung und des Trainings existiert eine Vielzahl von Anwendungen für M&S. Militärische Ausbildungssimulationen verfolgen stets das Ziel, den einzelnen Soldaten als Individuum oder als Teil eines Teams zu verbessern. Dabei werden mit Simulation in der Regel kognitive, psychomotorische oder methodische Lernziele verfolgt. Häufig dominieren wirtschaftliche Gründe bei der Entscheidung für den Einsatz von Simulation. Das kann jedoch dazu führen, dass die Wirklichkeit nicht hinreichend realitätsnah abgebildet wird und so zur Ablehnung durch den Soldaten führt. Insbesondere bei Systemen, die auch psychomotorische Fertigkeiten des Soldaten verbessern sollen, kann es so zum „negative Learning“ führen. Der Soldat erlernt im Extremfall die Bedienung des Simulators und des Realsystems parallel. Dieses Phänomen ist zwar bekannt, wird bei Auswahlentscheidungen jedoch viel zu wenig betrachtet.

Die Simulation kann in der Ausbildung nur dann weiter an Bedeutung gewinnen, wenn der Fokus wieder weniger in Richtung des technisch Machbaren sondern wieder mehr in Richtung des pädagogisch Notwendigen verändert wird. Wo in der Vergangenheit die beschränkten technischen Möglichkeiten eine Konzentration auf das Wesentliche notwendig machten, müssen heute wieder verstärkt detaillierte Lernzielanalysen die Fokussierung auf den Anwendungszweck erzwingen.

Ein Trend in der Ausbildungssimulation ist die Embedded Simulation. Dabei werden die Simulationen im realen System eingesetzt. Eine Idee ist dabei, dass der Soldat mit seinem System in einer realen Umgebung übt und damit die Gefahr von „negative Learning“ verringert wird. Diese Form der Simulation hat allerdings andere Schwächen gezeigt. So ist das Ausbildungsmittel nur dann verfügbar, wenn das Realsystem verfügbar ist, das Waffensystem wird erheblich komplexer, es müssen Probleme der funktionalen Sicherheit gelöst werden und das Realsystem ist während der Ausbildung für Einsatzaufgaben nicht nutzbar. Dabei hat die Nutzung durchaus Vorteile.

Das volle Potential der Embedded Simulation kann aber erst mit dem Einsatz von Augmented oder Mixed Reality ausgeschöpft werden. Durch die Verschmelzung von Live Simulation mit virtuellen Elementen gelingt es, dass die Sinne des Soldaten mit wirklich realen Umwelteindrücken stimuliert werden und trotzdem die bereits genannten Vorteile der Simulation zum Tragen kommen.

Ein bisher vernachlässigter Aspekt in der simulationsgestützten Ausbildung ist die Simulation des Informationsumfeldes. Im realen Einsatz ist der Soldat auf allen Ebenen vom Fahrer bis zum operationellen Entscheider einem kontinuierlichen Informationsfluss ausgesetzt. Synthetische Ausbildungsumgebungen vernachlässigen diesen Aspekt häufig. In der klassischen Aufteilung Live-Virtual-Constructive wäre die Simulation dieses Informationsflusses als konstruktive Simulation zu entwerfen. Ein einfaches Koppeln, wie es häufig rein technisch gefordert wird, genügt der Abbildung der Einsatzrealität nicht. Die ungefilterte Stimulation der C2-Systeme mit simulierten taktischen Lagen führt insofern zum „negative Learning“, dass der Soldat verlernt, den verfügbaren Informationen grundsätzlich zu misstrauen. Dabei war es stets eine Stärke der simulationsgestützten Ausbildung, Überraschungen und (scheinbare) Zufälle als Trainingsreiz gezielt einzusetzen.

Die Repräsentation der Information im simulationsstimulierten C2-System muss alle Elemente der Einsatzrealität haben, wie z.B. Falschinformationen, Doppelungen, Verwechslungen, Übertragungsverzögerungen, manipulierte Informationen oder gar den massiven Ausfall durch Störungen. Demgegenüber steht die mathematische Genauigkeit der Abbildung der Realität im Simulator, der die notwendigen Berechnungen nur mit der „Ground Truth“ durchführen kann. Außerdem müssen alle vorgenommenen Veränderungen der Informationen nachvollziehbar bleiben, um die simulationsgestützte Ausbildung lückenlos auswerten und Ausbildungsabschnitte wiederholen zu können.

## *D. Einsatzunterstützung*

In den Phasen der Einsatzplanung, der Einsatzdurchführung und der Nachbereitung von Einsätzen werden entscheidungsunterstützende Systeme und OR-Methoden angewendet und eingesetzt. Ziel ist es, Einsätze und den Einsatz von Systemen effektiv und effizient zu gestalten. Typische Aufgaben sind unter anderem:

- die Bewertung der optimalen Nutzung vorhandener Systeme und Arbeitsprozesse,
- die Bestimmung der erforderlichen Einsatzfähigkeiten,
- Bewertung und Vergleich von Handlungsoptionen,
- die Zusammenstellung der geeigneten Truppenteile sowie
- die Planung und Bewertung von bestimmten Wirksamkeiten (z.B. der strategischen und operativen Mobilität oder bestimmten Aktivitäten im Einsatzgebiet).

In der Einsatzdurchführung unterstützt M&S u.a. durch automatisierte Berechnungen und Abschätzungen, durch Visualisierung von Vorgängen und dient zur Optimierung von Prozessen oder Bewertung von Handlungsoptionen. M&S bietet den Vorteil, große Datenmengen in kurzer Zeit zu verarbeiten, dabei eine Vielzahl von Faktoren berücksichtigen zu können und so den Entscheidungsprozess zu unterstützen bei gleichzeitiger Reduktion des Personalaufwandes. M&S findet ebenfalls Anwendung in der Nachbereitung von Einsätzen, insbesondere bei der Verarbeitung, Analyse bis hin zur Visualisierung von im Einsatz erfassten Daten.

## Trends und Ausblick für Modellbildung und Simulation

Was im Jahr 2037 mithilfe von M&S möglich sein wird und wie es die Streitkräfte beeinflusst, kann man zum jetzigen Zeitpunkt nur erahnen. Nicht selten wurden Vorhersagen und Prognosen über die Zukunft oder die Entwicklung von Technologien falsifiziert.

Eines ist jedoch sicher: Computer, die einen wesentlichen Bestandteil von M&S darstellen, werden in Zukunft über (deutlich) mehr Leistung verfügen. In diesem Zusammenhang werden häufig Quantencomputer genannt [4]:

*"Quantum Computing: A kind of computing that takes advantage of the ability of subatomic particles to exist in more than one state at any time, thus allowing operations to be done faster and using less energy than regular computers while also being able to store more information."*

Ob Supercomputer 2037 auf den Gesetzen der Quantenmechanik beruhen oder nicht, ist an dieser Stelle nicht relevant. Sie werden in jedem Fall Rechenoperationen schneller durchführen können, als es die Rechner heutzutage können. Für den Einsatz von Modellbildung und Simulation bedeutet das, dass einerseits Simulationsergebnisse in immer kürzerer Zeit zur Verfügung stehen werden – selbstverständlich ist die Simulationszeit vom Detaillierungsgrad des Modells abhängig. Andererseits werden Prozesse und Phänomene detaillierter abgebildet werden können und es wächst die Anzahl an Wechselwirkungen, Stör- und Einflussgrößen, die bei einer Simulation berücksichtigt werden können bzw. müssen. Dadurch ist auch ein immer aussagekräftigeres Gesamtergebnis gewährleistet. Darüber hinaus wird es möglich sein, Dinge zu simulieren, die aktuell aufgrund der Rechenleistung noch nicht oder nur sehr langsam simuliert werden können.

Im Zuge des Systems Engineering und des modellbasierten Entwickelns werden in der Produktentwicklung bereits heute immer mehr virtuelle Prototypen eingesetzt, wodurch sich die Anzahl an realen Prototypen reduziert. Dies lässt nicht nur Kosten-, sondern vor allem auch Zeitersparnisse erwarten.

TAYLOR et al. sehen M&S als eine Schlüsselrolle für die Zukunft. Sie stellen in [5] "Grand Challenges" für M&S dar und geben einen guten Überblick über Herausforderungen, wie z.B. simulationsbasierte Beschaffung, Simulations-Interoperabilität, Hochgeschwindigkeitsoptimierung, Multidomänenmodelle und die Simulation des menschlichen Verhaltens. In [6] nehmen TOLK et al. Stellung zu Herausforderungen von M&S hinsichtlich der Unterstützung des Verteidigungs- und Sicherheitssektors. Hierzu gehören u.a. neue Fragen der Interoperabilität, Analysen in Echtzeit, neue Ausbildungs- und Trainingsmöglichkeiten, Modellierung von menschlichem Verhalten und operationelle Zukunftskonzepte. Für weitere Herausforderungen sei an dieser Stelle auf [7] verwiesen.

LADETTO beschreibt die militärische Relevanz von Simulation im Hinblick auf die Zukunft für Information und Kommunikation wie folgt [8]:

*„Durch den Echtzeit-Zugriff auf Risikoanalysen, fortschrittliche Simulationsergebnisse und Fachkenntnisse wird die künstliche Intelligenz den Entscheidungsprozess auf dem Schlachtfeld wandeln, indem sie Vorhersagen macht und die gesamten militärischen Weisheiten und Erfahrungen an die Soldaten im Einsatz bringt […]."*

In Bezug auf die Zukunft der Streitkräfte spielt neben den Technologien und dem Fortschritt von Computern und Simulationsverfahren vor allem die Art der Kriegsführung eine entscheidende Rolle. Doch wie wird Kriegsführung im Jahr 2037 aussehen? Das Australische DEPARTMENT OF DEFENCE zeigt in [9] seine Sicht auf die Zukunft von „Joint Operations" im Jahr 2030, bei welcher der Cyberraum eine immer wichtigere Rolle einnehmen wird. Besonders in dieser Operationssphäre ist die Verwendung agiler und schneller, entscheidungsunterstützender Systeme von enormer Wichtigkeit, wozu M&S einen relevanten Beitrag geben wird.

Durch M&S werden neue und realistischere Ausbildungs- und Trainingsmethoden zur Verfügung stehen. PAGE nennt hier den Einfluss von Virtual and Augmented Reality und insbesondere virtuelle Menschen. Sie stellen computerbasierte Charaktere dar, die im Training mit den Auszubildenden interagieren [7]. Weiterhin werden noch realistischere Simulatoren (z. B. Flug- und Fahrsimulatoren) zur Ausbildung und zum Training verfügbar sein. Eine Prognose zur globalen Marktentwicklung von militärischer Simulation und virtuellem Training bis zum Jahr 2025 wird in [10] gegeben. Ein wichtiger Bestandteil wird in diesem Bereich die Vernetzung unterschiedlicher Simulatoren sein und die simulationsgestützte Ausbildung, bei der reale Plattformen mit verschiedenen Simulationssystemen vernetzt werden.

Modellbildung und Simulation wird in Zukunft eine immer wichtigere Rolle einnehmen und bei vielen Aufgaben der Streitkräfte unterstützen.


**Matthias Lochbichler**
studierte Maschinenbau mit den Schwerpunkten Regelungstechnik und Mechatronik an der Universität Paderborn. Von 2009 bis 2015 war er wissenschaftlicher Mitarbeiter am Lehrstuhl für Regelungstechnik und Mechatronik des Heinz Nixdorf Instituts der Universität Paderborn. Im Rahmen seiner Promotion befasst er sich mit der Modellierung und Simulation des dynamischen Verhaltens mechatronischer Systeme und der Antwort auf die Frage nach einem geeigneten Detaillierungsgrad. Seit 2016 ist er bei der IABG in der Abteilung für Operationen und Plattformen Land tätig.

**Klaus Kappen**
studierte Elektro- und Informationstechnik an der Technischen Universität München. Er ist seit 1996 tätig bei der IABG in der Beratung von Auftraggebern im öffentlichen Sektor, insbesondere für das Bundesamt für Ausrüstung, Information und Nutzung in der Bundeswehr (BAAINBw), für die Bundeswehr (das Heer / die Landstreitkräfte) und für das BMVg. Die Schwerpunkte liegen im Bereich des Rüstungsprozesses und dem damit verbundenem Projekt- und Programmmanagement. In den Jahren 2001 und 2002 war er für 15 Monate als Scientist am US Army Research Laboratory in Maryland. Seit 2011 leitet er die Abteilung Operationen und Plattformen Land und ist für alle Aktivitäten in Bezug auf Technologien und Operationen von Landstreitkräften bei der IABG verantwortlich.


## Literature


[1] HUBER, R. K.: Modellbildung und Simulation im erweiterten Aufgabenspektrum der Bundeswehr. Hochschulkurier der Universität der Bundeswehr München, 2003.

[2] LEHMANN, A.: Das Potenzial von Operations Research (OR), Modellbildung und Simulation (M & S) aus akademisch akademisch-wissenschaftlicher Sicht. Seminar für Führungskräfte der Bundeswehr, Heeresfliegerwaffenschule Bückeburg 03.-05. Juni 2008.

[3] LÜBBERS, H.: Modellbildung und Simulation in der Bundeswehr. In: Wehrtechnischer Report, Ausgabe 6, Dezember 2007.

[4] ENVISIONING: DEFTECH VISION 2015. Envisioning Defense Technology, 2017. URL: http://envisioning.io/deftech

[5] TAYLOR, S. J. E.; BRAILSFORD, S.; CHICK, S. E.; L'ECUYER, P.; MACAL, C. M.; NELSON, B. L.: Modeling and Simulation Grand Challenges: An OR/MS Perspective. In: Proceedings of the 2013 Winter Simulation Conference, 2013.

[6] TOLK, A.; ADAM, N. R.; CAYIRCI, E.; PICKL, S.; SHUMAKER, R.; SULLIVAN, J. A.; WAITE, W. F.: Defense and Security Applications of Modeling and Simulation – Grand Challenges and current Efforts. In: Proceedings of the 2012 Winter Simulation Conference, 2012.

[7] PAGE, E. H.: Modeling and Simulation (M & S) – Technology Landscape. In: MITTAL, S.; DURAK, U.; ÖREN, T.: Guide to Simulation-Based Disciplines – Advancing Our Computational Future, Springer-Verlag, 2017.

[8] LADETTO, Q.: Technologie-Früherkennung. Trends und Potenziale 2015-2025. Eidgenössisches Departement für Verteidigung Bevölkerungsschutz und Sport VBS, armasuisse Wissenschaft + Technologie, Thun, 2015.

[9] AUSTRALIAN GOVERNMENT – DEPARTMENT OF DEFENCE: Future Joint Operating Concept 2030. Commonwealth of Australia, 2011.

[10] STRATEGIC DEFENCE INTELLIGENCE: The Global Military Simulation and Virtual Training Market 2015°–2025. 2015.

**armasuisse**
Science and Technology

Feuerwerkerstrasse 39
CH-3602 Thun

phone: +41 58 468 28 00
fax: +41 58 468 28 41

e-mail: wt@armasuisse.ch
web: www.armasuisse.ch/wt

ISBN: 978-3-9524890-0-0