



European Defence Matters

FUTURE ADVANCED
MATERIALS

AUTONOMY IN
DEFENCE

ADDITIVE
MANUFACTURING

ROBOTICS IN
DEFENCE

DEFENCE INTERNET
OF THINGS

BLOCKCHAIN
TECHNOLOGY IN DEFENCE

BIG DATA ANALYTICS
FOR DEFENCE

AI FOR CYBER

NGS FOR BIOLOGICAL
THREAT PREPAREDNESS

AI & COGNITIVE
COMPUTING IN DEFENCE

10 Upcoming Disruptive Defence Innovations

Also in this issue:
Interviews with
Airbus CEO Dirk Hoke
and Estonian MoD
Jüri Luik

PROTECTING EUROPEAN SKY

PARTNER IN THE SUCCESS OF EUROPEAN COUNTRIES COLLECTIVE DEFENSE

ThalesRaytheonSystems provides NATO with Europe's first-ever integrated Air & Missile Command and Control System covering 10 million km² of territorial space.

ThalesRaytheonSystems has a unique international approach by working in concert with a network of industrial partners across 15 different European countries.

This is not a concept, it is an industrial reality which ensures the most resilient and efficient collective defense for Europe.

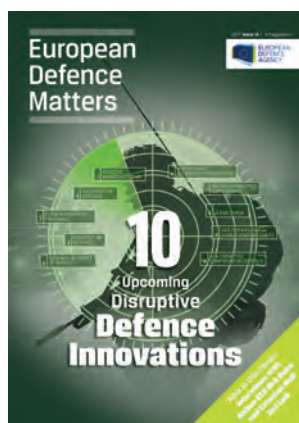
ThalesRaytheonSystems is a transatlantic joint venture positioned as a leader and pioneer in the defense industry.



ThalesRaytheonSystems

WWW.THALESRAYTHEON.COM

© 2017 THALESRAYTHEONSYSTEMS. ALL RIGHTS RESERVED.



Publication Director
Pauline Massart

Editor-in-Chief
Helmut Bröls

Design
Simon Smith Associates

Printing
Drukkerij Hendrix NV
Kiezel Kleine-Broegel 55, B-3990 Peer
Belgium

This document is published by the EDA in the interests of exchange of information

Front cover image;
Soldier image: © UK MoD/Crown copyright 2016
Other images; EDA, Shutterstock

Contacts

Pauline Massart
Head of Media & Communication

Helmut Bröls
Media & Communication Officer

European Defence Agency
Rue des Drapiers 17-23
B-1050 Brussels
www.eda.europa.eu
Contact: info@eda.europa.eu

European Defence Matters is the only dedicated official European defence magazine focusing on senior decision-makers in national governments, European institutions and industry in Europe.

Published twice a year, with a circulation of around 10,000 copies, the magazine provides a unique vehicle for the wider European defence community to debate the essential issues around capabilities, research, EU policies, industrial matters, armament programmes, procurement and larger defence and security challenges.

If you are interested in advertising to Europe's key decision-makers, please contact:

Cyril Mikailoff
Advertising Sales Director
T: +33.6.21.71.11.18.
cmikailoff@turbomedia.eu



EDA is a member of the
European Military Press
Association

Catalogue number QU-AC-17-002-EN-C
ISSN (1977-5059)



Mario Guerra © THALES

Contents

Welcome

- 4 Editor-in-Chief Helmut Bröls and Head of Media & Communication Pauline Massart introduce this edition of *European Defence Matters*

European defence news

- 5 Strong industry response to first PADR call for proposals; Multinational tanker fleet expands; Defence project gets ESIF funding

Cover story: A journey into the future

- 6 Introduction
- 8 Disruptive defence innovations ahead!
Introduction by Dr. Panagiotis Kikiras, European Defence Agency Head of Unit for Innovative Research
- 11 A constant eye on the future: identifying Europe's capability requirements for 2035
An analysis by RAND Europe and the Hague Centre for Strategic Studies (HCSS)
- 14 Artificial Intelligence (AI) & Cognitive Computing in defence
- 15 Defence Internet of Things
- 16 Big Data analytics for defence
- 17 Blockchain technology in defence
- 18 Artificial Intelligence (AI) enabled cyber defence
- 19 Robotics in defence
- 22 Autonomy in defence: systems, weapons, decision-making
- 23 Future advanced materials for defence applications
- 24 Additive Manufacturing in defence
- 25 Next Generation Sequencing (NGS) for biological threat preparedness

Industry talk

- 26 Interview with Airbus Defence & Space CEO Dirk Hoke

Focus

- 30 Step by step: European MALE RPAS takes shape

In the spotlight

- 32 CARD: Implementing European solidarity in defence
- 34 CYBRID conference in Tallinn: strategic responses to strategic threats

Opinion

- 36 Interview with Estonia's Defence Minister Jüri Luik about cybersecurity, European defence cooperation and more

In the field

- 38 Optimising Europe's Main Battle Tank Capabilities
- 40 Cleared for take-off: European Tactical Airlift Centre (ETAC) opens in Zaragoza

In pictures

- 43 3D-printed miniature A400M aircraft

© The European Defence Agency (EDA) November 2017. All rights reserved. The entire contents of this publication are protected by copyright. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means: electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the EDA. The reproduction of advertisements in this publication does not in any way imply endorsement of their content by the EDA. The views expressed in the articles are those of the authors and do not necessarily reflect the official position or policy of the EDA.

Daring a glimpse into the future

Strategic foresight is a necessity, not a luxury. European defence planners in governments, EU institutions and industry must anticipate technological developments and integrate them into their long-term capability planning. We must catch up with technology, lest the opposite happens.

As the European hub for inter-governmental defence capability planning, prioritisation and development, and with the unparalleled expertise stemming from its Capability Technology Groups (CAPTECHS) and network of defence Research and Technology (R&T) experts from Member States, the European Defence Agency (EDA) is in a privileged position to look out for what comes next.

In the following pages, closely guided by the EDA's R&T and Technology Watch experts, we venture a look into the future at 10 disruptive defence innovations. The list could easily be endless as technology develops at warp speed, but we chose to stick to the ten topics or domains which our experts deem likely to have the biggest impact on defence and subsequently on military capabilities in the next 5 to 20 years. Europe's governments will have to embrace and buy into these new technological trends to make sure European nations develop and built the defence capabilities they will need in the future.

Other topics in this 14th issue of *European Defence Matters* include 'Industry Talk' in which we speak to Airbus Defence & Space CEO Dirk Hoke about his organisation's innovation priorities, upcoming multinational defence programmes, the European Defence Fund and the future of European defence industrial cooperation.

We also sat down with Estonia's Minister of Defence, Jüri Luik, to discuss the results of EU CYBRID 2017, the first ever cyber defence table-top exercise with ministers jointly organised by the Estonian EU Presidency and the EDA in Tallinn in early September, and to hear his views about recent initiatives to boost European defence cooperation.

The European MALE RPAS project, ongoing preparations for the Coordinated Annual Review of Defence (CARD), the EDA's Main Battle Tank (MBT) project and the recent opening of the European Tactical Airlift Centre (ETAC) in Zaragoza also feature in this issue.

We hope this magazine will provide valuable food for thought and information about the EDA's work. Should you have comments or recommendations, please get in touch: info@eda.europa.eu 

News

Strong industry response to first PADR call for proposals


The Preparatory Action on Defence Research (PADR), launched by the European Commission in April 2017 to test and lay the groundwork for a possible European Defence Research Programme in the EU's next Multiannual Financial Framework after 2020, cleared the first hurdle.

The European Defence Agency (EDA), mandated by the Commission to implement the PADR, announced on 9 October that in response to the three calls for proposals issued last June, it received no less than 24 submissions with consortia including around 190 entities from 25 Member States (with some applying to various calls in different consortia).

The domains covered by these first calls are enhanced situational awareness in a naval environment, force protection and advanced



soldier systems, and strategic technology foresight. EDA Chief Executive Jorge Domecq welcomed the strong participation in the first calls which bodes well for the future. "What is noteworthy, besides the number of submissions itself, is the incredible amount of entities – research institutes, small and mediums size enterprises and prime companies – which have bid for the various calls. This reflects the urgent need for more

defence research funding, cross-border collaboration and harmonisation in Europe", he commented. The proposals are now being evaluated by the EDA with the support of independent subject matter experts. The first winner consortia are expected to be announced before the end of the year with grant agreements to be signed early 2018. The PADR will run over three years (2017-2019) with a total budget of €90 million. 

Multinational tanker fleet expands


On 25 September, the current Multinational Multi-Role Tanker Transport Fleet (MMF) contract was amended to include Germany and Norway as new members along with the Netherlands and Luxembourg.

The contract amendment increases the MMF's scope from the two A330 MRTT aircraft initially ordered by the Netherlands and Luxembourg to seven aircraft in total, including options for up to four additional aircraft. More nations are expected to join in the future and to exercise the available contract options. The delivery of the seven A330 MRTT aircraft currently on contract from Airbus Defence and



Airbus A330 MRTT

Space's tanker conversion line at Getafe near Madrid is expected between 2020 and 2022. The MMF was initiated by the European Defence Agency (EDA) in 2012; the Organisation Conjointe


de Coopération en matière d'Armement (OCCAR) manages the aircraft acquisition as the NATO Support and Procurement Agency's Contract Executing Agent. 

Defence project gets ESIF funding

In September, for the first time, a fully fledged defence research project – initiated by the Croatian Ministry of Defence and supported by the European Defence Agency (EDA) – was awarded EU co-funding under the European

Structural and Investment Funds (ESIF).

So far only 'dual-use' projects with both civilian and military applications had been able to secure ESIF funding. The granting of ESIF funding to this Croatian project, which

aims at developing a cyber conflict simulator, represents a landmark in the EDA's year-long efforts to open up EU funding opportunities for pure defence research projects, in addition to dual-use projects. 

A Journey into the future



Ever faster technological change is setting the pace of our societies and citizens' lives. It's no different in the defence realm: the level of protection a state or a group of nations can provide to its citizens is tantamount to its capability to defend against or embrace technological disruption, today and in the future.

Hence the importance of strategic and technological foresight to make sure Europe's armed forces invest today in the right capabilities for tomorrow.

With unparalleled expertise stemming from the Capability Technology Groups (CAPTECHS), which form a network of defence Research and Technology (R&T) experts from participating Member States, the European Defence Agency (EDA) is ideally placed to be a driving force in this domain.

This section presents an analyses by the EDA's Tech-Watch experts of 10 disruptive technological developments which are redesigning the defence capability landscape.

Index

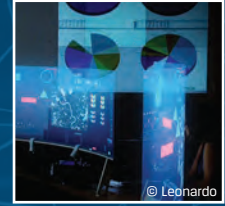
8. Disruptive defence innovations ahead!

Dr. Panagiotis Kikiras, the EDA's Head of Unit Innovative Research, sets the scene and explains how our shortlist came about



11. Identifying Europe's capability requirements for 2035

Alex Hall, James Black and Marta Kepe of RAND Europe and Frank Bekkers of the Hague Centre for Strategic Studies (HCSS)



10 Disruptive defence innovations

14. Artificial Intelligence (AI) & Cognitive Computing in defence

By Ignacio Montiel-Sánchez, EDA Project Officer, Information Technologies

19. Robotics in defence

By Marco Dettratti, EDA Project Officer, Guidance, Navigation, and Control

15. Defence Internet of Things

By Ignacio Montiel-Sánchez, EDA Project Officer, Information Technologies

22. Autonomy in defence: systems, weapons, decision-making

By Marek Kalbarczyk, EDA Project Officer, Land Systems Technologies

16. Big Data analytics for defence

By Ignacio Montiel-Sánchez, EDA Project Officer, Information Technologies

23. Future advanced materials for defence applications

By Patricia Lopez Vicente, EDA Project Officer, European Defence Research

17. Blockchain technology in defence

By Salvador Llopis Sanchez, EDA Project Officer, Cyber Defence Technology

24. Additive manufacturing in defence

By Patricia Lopez Vicente, EDA Project Officer, European Defence Research

18. Artificial Intelligence (AI) enabled cyber defence

By Salvador Llopis Sanchez, EDA Project Officer, Cyber Defence Technology

25. Next Generation Sequencing (NGS) for biological threat preparedness

By Shahzad Ali, EDA CapTech Chemical, Biological, Radiological and Nuclear (CBRN) & Human Factors Officer

› Disruptive defence innovations ahead!

Establishing a shortlist of the '10 most disrupting defence innovations to come' requires a thorough and methodical selection based on timeframes and clear criteria for terms such as 'innovation' and 'disruptive'. In this article, **Dr. Panagiotis Kikiras**, the European Defence Agency's Head of Unit for Innovative Research, sets the scene and explains how our shortlist came about.

Today, the notion of innovation is widely used in research, economics, politics and other areas. While there is a common understanding that innovation means the generation of new ideas and/or knowledge, there is much less of a consensus on what can or should actually be considered 'innovative'. Moreover, the meaning of innovation changed throughout the years: whereas innovation could have a negative connotation up to the early 20th century, it is nowadays seen as a key factor for long-term economic growth and international competitiveness¹.

Enhancing military capabilities

Innovation can be defined as the creation and application of new products, services and processes. This includes the creation of a new technology, product, process or service, as well as the application of an existing technology to a different problem or domain.

By introducing innovative technologies originating from other domains into the defence sector, both the initial investment risk and the lapse of time between the ideation and the delivery of a new military capability can be minimized. Nevertheless, innovation is not only meant to create new concepts but also to generate added value for end-users. Innovation in the defence sector should thus first and foremost aim at enhancing military capabilities.

In this context, innovation can be considered in different ways. A disruptive innovation is one which radically changes the way of operation ('of doing things'), and therefore has a significant impact on market, on economic activity of firms, and as far as the defence sector is concerned, on the way in which armed forces operate. It uses enablers (technical or otherwise) and new paradigms to reach a level of performance that, over

1. 16.ESI.OP.221 'Studies for Innovation in Defence Strand A' – Interim Report

"Successful defence innovation obviously requires both disruptive and capability-based incremental innovation in order to provide our Member States with the defence capabilities they need in the future."

Mario Guerra © THALES

time, exceeds by far the limits of traditional, evolutionary advances. In contrast to disruptive innovations, incremental innovations enhance or improve the performance of existing products, services, processes, organisations or methods.

Successful defence innovation obviously requires both disruptive and capability-based incremental innovation in order to provide Member States with the defence capabilities they need in the future. As shown in the graph below, defence innovation naturally stems from the need to confront new emerging threats when available solutions are insufficient and lay bare strategic capability gaps. Future scenarios must be identified at the long-term vision and strategy stage which is also when future technologies should be successfully

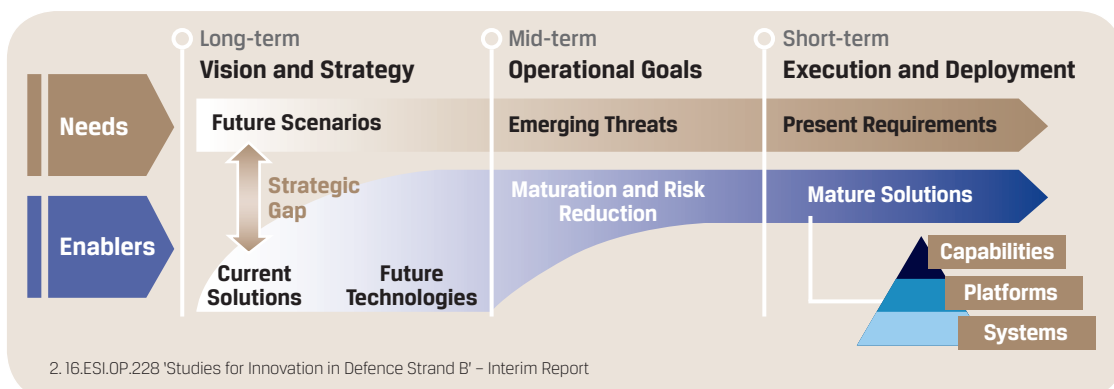
earmarked for their potential to disrupt the status quo and address emerging challenges².

While it may seem contradictory to mingle innovation and processes, best practice indicates that a structured process is a prerequisite to drive innovation and that without processes, there is only little chance of collecting great innovative ideas to be further developed. Nevertheless, although a predictable, repeatable innovation process is needed, the process in itself should be as light as possible so as not to inhibit innovation. Furthermore, in recent years, we have been experiencing a shift in innovation drive. The times are long gone when defence research was at the onset of key technological advances (GPS, Internet,...). Nowadays, civil and commercial markets drive innovation in most underlying technologies.

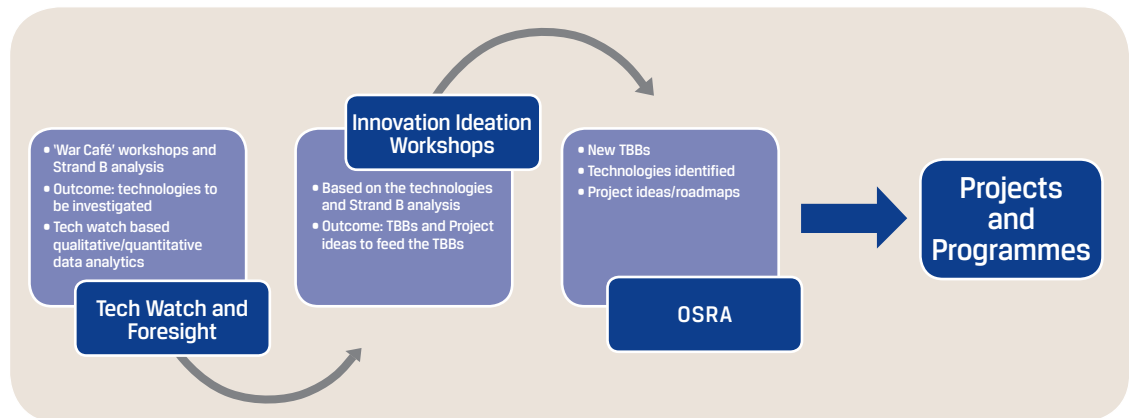
The EDA should engage with non-traditional defence R&D communities and innovators to speed up access to emerging and potentially disruptive research and identify areas for additional investment to fully address future defence capability needs. The Agency's Capability Technology Groups (CAPTECHS), which form a network of experts from participating Member States dedicated to a particular technology area, are key in this respect.

To support innovation and the incorporation of new topics and technologies into the defence domain, a toolchain has been developed by the EDA, covering all the steps from technology identification and project ideation to the enrichment of the Overarching Strategic Research Agenda (OSRA):

1. 'Technology Watch' is a new initiative launched by the EDA to allow all R&T experts to look for new information and to share it with their peers. In addition, a specific →



OSRA enrichment toolchain



technology foresight methodology was developed to enable the long term identification of emerging technologies;


2. Technologies identified by the CapTechs are addressed by the Technology Watch tool and the technology foresight workshops. This second step brings together the expertise of all participating Member States for the purpose of technological assessment, to identify bestpractices and implement tailored processes to be used when evaluating the interest of a technology;

3. The final step of the process is the selection of the most promising technologies to be included into the OSRA process.

The list of innovative technologies presented here is structured on the basis of the estimated timespan the technologies in question may take to mature enough to be included in defence platforms and systems.

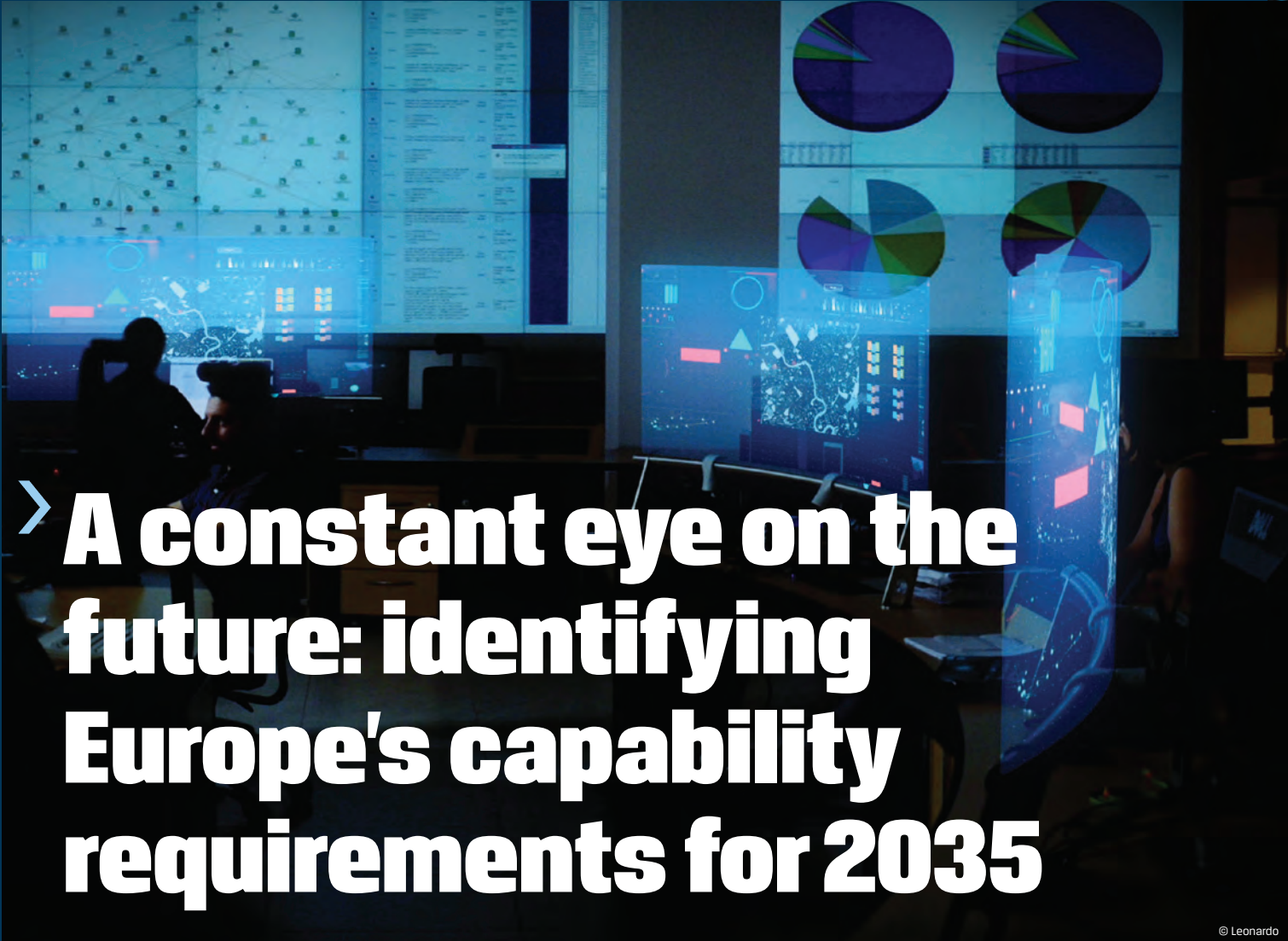
We distinguished between the five following time horizons:

- **Short term:** maturity to be reached within the next 5 years
- **Short to medium term:** maturity to be reached between 5-10 years
- **Medium term:** maturity to be reached between 10-15 years
- **Medium to long term:** maturity to be reached between 15-20 years
- **Long term:** maturity anticipated after 20 years.

This list is based on the analysis of the long term technological trends identified for the Capability Development Plan as well as of the disruptive technologies identified by the EDA's CAPTECHS during the OSRA process. 

Overview: The EDA's current Capability Technology Groups (CAPTECHS)

Capability, Armament and Technology		European Synergies and Innovation
Information Superiority	Intervention and Protection	Innovative Research
Communication Information Systems & Networks	Aerial Systems	Materials & Structures
Systems of systems Battlelab and Modelling & Simulation	Ground Systems	Technologies for Components and Modules
Cyber Research & Technology (working group)	Naval Systems	Radio Frequency Sensors Technologies
	Ammunition Technology	Electro-Optical Sensors Technologies
		CBRN Protection and Human Factors
		Guidance, Navigation & Control
		Energy and Environment WG



> A constant eye on the future: identifying Europe's capability requirements for 2035

© Leonardo

Effective military capabilities can take decades to research, develop, procure, field and integrate. But new threats can emerge with little warning. To address this imbalance, European militaries and the European Defence Agency (EDA) must plan ahead to anticipate future capability needs and adapt to the fast pace of change in the technology and threat environments. In the following article, **Alex Hall, James Black and Marta Kepe** of RAND Europe and **Frank Bekkers** of the Hague Centre for Strategic Studies (HCSS) describe and analyse the background and importance of the ongoing long-term revision of the Capability Development Plan (CDP).

In December 2016, the EDA contracted the not-for-profit, independent research organisations RAND Europe and HCSS to support the revision of the long-term strand ('Strand B') of the Capability Development Plan (CDP), a strategic picture of European military capabilities regularly updated by the EDA. Part of a wider effort by the Agency to develop European defence capabilities, this work is intended to provide military decision-makers and capability planners with an overview of the potential impact of technological advancements and strategic environment changes on

future operations and on European military capabilities up to 2035 and beyond.

Understanding the evolving technology landscape is an important input to the CDP for a number of reasons. Technology affects various aspects of conflicts and is therefore a critical component of defence planning (though non-technological aspects and solutions must not be overlooked either). New technologies have often shaped strategies and tactics, and inspired the development of defence innovations. In an increasingly connected, complex and information-rich global society, →

"Technology trends outside of the military are moving quickly, profoundly and unpredictably. This may require a more innovative approach on behalf of European defence planners."



© Finnish Defence Forces Research Agency

technological developments not only shape the ways and means by which wars are waged, but can also precipitate changes in what is perceived to constitute (military) conflict, and condition the role of defence institutions in preventing, preparing for, engaging in and moving away from conflict.

Historically, militaries have frequently driven innovation, often with 'spillovers' into civilian life – jet travel, satellite navigation or the Internet are just a few examples. Today, because of the growth of research and development in the commercial sector and the interconnected global innovation and production networks, the dynamics in defence innovation often work the other way around – with technologies primarily developed in a civilian context and then applied in military applications. This makes it ever more important that the EDA understands a broad spectrum of potential future technology trends, if it is to help European defence planners develop innovative military applications to respond to security threats.

Technology themes

Understanding this fast-evolving 'art of the possible' is a challenge for European militaries, governments and private organisations. Forward-looking institutions seek to map changes in the technology landscape through horizon scanning and technology watch activities. To help the EDA collate and prioritise the findings of this wider work, the RAND Europe-HCSS study team undertook a 'scan the scanners' review, compiling and analysing a wide range of horizon scanning outputs and technology trends. The most relevant and impactful technology trends were clustered into 'technology themes' – a combination of related future technology trends whose applications are likely to have a significant impact on societal developments, including on defence and security. Examples of key technology themes

included: sensorisation, datafication and sense-making of society; human-machine teaming and artificial intelligence; globalisation of technology and modularisation of systems; space as a battlefield; human enhancement; and renewable energy and energy weapons.

These themes are likely to have profound implications on the shape of future conflicts, in terms of actors, domains, duration and timing, and phasing, or, in short, ends, ways and means. As readers of Clausewitz will know, the fundamental nature of conflict is enduring: it has always been and will remain a violent contest – a mix of chance, risk and policy – that at times can be irritational, unpredictable and potentially volatile. Nonetheless, its specific characteristics will change over time, not least due to shifting technological paradigms.

New technologies have often shaped strategies and tactics, and inspired the development of defence innovations.

Sensors and network connectivity

Some – certainly not all – of the more striking potential changes arising from the technology themes might include the following examples.

Both the civilian and defence realms are experiencing an increasing proliferation of sensors and network connectivity, with vast amounts of different types of data being produced, captured and exploited for a variety of logistical, commercial, health, safety, security and other purposes. Cheaper and smaller sensors combined with better memory and processing power may therefore result in 'ambient intelligence' throughout society – the creation of an Internet of Everything, connecting a multitude of devices embedded in, on or around people, objects and the environment.

At the same time, developments in automated and algorithmic analysis are improving the collation, processing and analysis of this 'Big Data', leading to a further reduction in the data-to-decision process

and enabling European commanders to grapple with the complexity, fog and friction of the battlefield. This sensorisation and datafication of society generates a wealth of real and near-real-time data, enabling remote monitoring of everything from individual soldiers' health or performance, through to analysis of civilian population movements, or early detection and warning of concealed threats. The result is a need to securely access, fuse and exploit data from a wealth of civilian and military sensors throughout the operating environment, so as to enhance situational awareness and decision-making – as well as to find ways to allow European forces to operate safely in sensor-rich environments where the adversary may always be watching.

Artificial Intelligence and human-machine teaming

Artificial Intelligence (AI) holds the potential to affect ever more aspects of civilian and military life. Varying degrees of sophistication of AI and machine-learning might be incorporated into virtually any application or service to improve efficiency and escape some of the limitations of human thinking. At the same time, keeping 'humans in the loop' remains essential or even required in many roles, meaning that intelligent machines must learn to work closely with humans and vice versa, with new concepts of man-machine teaming. Addressing the ethical and trust-related implications and risks associated with the integrity and security of these systems will not be easy, but is essential if the potential benefits of AI for defence are to be realised in full. If European defence organisations can get this balance right, this new technology offers vast potential in mitigating some of the adverse effects of conflict: improved speed of intelligence gathering and analysis to improve command functions; automation and optimisation of logistic systems; AI support to medical diagnosis and treatment; and a reduction in the number of human personnel to be deployed to dangerous environments and missions.

A wealth of other domains

Alongside advances in AI and unmanned systems, a range of technologies may allow both physical and cognitive improvements in the capabilities of human personnel. Advances in genetic engineering, nanotechnology, wearable technology and other fields are opening up a range of possibilities to push beyond traditional biological limits such as strength, endurance, intelligence or vulnerability to injury, infection, stress, and fear or pain. Cybernetic enhancement of human personnel through implanting of sensors, chips and other technology may similarly allow humans to better interface with machines and unmanned systems, or acquire wholly new abilities and senses. These developments may significantly transform individuals, their lifestyles and

consequently the way we think, plan for and engage in conflicts and crises. On the flip side, it also has the potential to create new faultlines of social or political strife between those who are enhanced and those who are not.

The space domain is similarly emerging as a growing focus for future operations. Space is already used to support military operational activities through observation, navigation and communication functions. There is a growing risk, however, of space becoming further militarised, and

evolving into a potential 'battleground' rather than a 'global commons'. With the potential establishment of military and civilian bases outside Earth's atmosphere, defence of assets in space will increasingly become an issue. Furthermore, space may be used for offensive actions, for example by placing surveillance and offensive cyber or kinetic strike capabilities. Operating in

this contested and congested environment will likely be a growing challenge for future European militaries.

All of these trends – and the many others considered in more detail throughout this ongoing study on the revision of military capability requirements for 2035 and beyond – are affected by the disruptive and unpredictable character of technology development. The results of this work, in concert with a wider analysis of the three CDP elements – short term (Strands A and D) and mid-term (Strand C) planning aspects – will inform the agreement on a new set of EU Capability Development Priorities expected in 2018.

Technology trends outside of the military are moving quickly, profoundly and unpredictably. This may require a more innovative approach on behalf of European defence planners regarding the assimilation of civilian technologies as well as considerations on how to face the potentially malignant applications of civilian technologies. Agility, adaptability and a constant eye on the future are crucial. ■

Agility,
adaptability and
a constant eye
on the future are
crucial.

About the authors

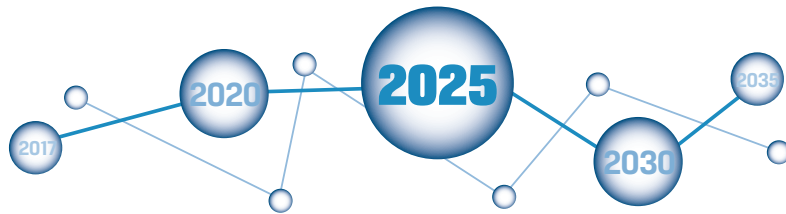
RAND Europe is a not-for-profit research organisation that helps to improve policy and decision making through research and analysis.

The Hague Centre for Strategic Studies (HCSS) has a mission to deliver evidence and insights to inform the strategic decision processes of its customers and to help them identifying and scoping their policy options.



EUROPE





Artificial Intelligence (AI) & Cognitive Computing in defence

Why it matters

An internet search using the keyword 'Artificial Intelligence' (AI) yields close to 95 million results, of which some 3 million only on the term's definition, which gives an idea of the growing popularity of the term.

AI can be understood as the theoretical creation and development of computer systems or algorithms able to perform tasks normally requiring human intelligence. There is a continuous, controversial debate going on in the media: on the one hand, about the potential of artificial intelligence as a game changer that will bring huge benefits to humankind; and, on the other, on the supposed threat it poses to our civilization given that the impact of AI in the future is difficult to evaluate at this time.

There are already calls for ethical regulation before we lose control on this technology. Commercial companies making huge profits on the global market are driving innovation in this field and developing new algorithms to provide intelligence through different applications exceeding recognition of images, voice and text.

In the last century, the arrival of digital computers made it possible to perform mathematical operations and data storage at a rate far beyond the capabilities of human beings. It then became possible to develop very complex algorithms and eventually programme machines in a way that allows them to learn and provide solutions comparable to what we call intelligence in human beings. This gave computer based systems the possibility to learn from data, the environment and from their own errors; something known as 'cognitive computing'.

Deep Learning, a technology based on specific kinds of Neural Networks, is responsible for the quantum leap observed in the field since 2009. It uses data analysis to predict trends and discover hidden information and patterns in the ocean of data provided by existing networks and sensors. The limits of this technology are not currently known but there are already some warning voices out there urging society to be prepared for an apocalypse as a result of this technology in a not so distant future.

What the EDA does

The EDA's network of experts working in the 'Radar' Capability Technology Group (CAPTECH) first drew attention to the growing importance of Deep Learning (DL) technologies during a workshop held in 2015, after which the 'DEEPLearn' project was launched.

The aim was to understand the possibilities for applying these algorithms in the Defence domain, motivated by the very successful results obtained in the civil area by companies like Google, Apple or Facebook. In fact, the use of massive amounts of data seemed

to be needed for the correct training and functioning of DL tools and the project aimed to show the operational limits of creating a mathematical framework to understand the applications in defence. Different applications like the detection of malicious traffic in encrypted networks for cyberdefence, the identification of gaits and gestures from people walking, or the detection of anomalous behaviour in maritime vessels traffic are currently being analysed in the realm of this project.

The way ahead

Another AI workshop in the field of Communication and Information Systems (CIS) together with Modelling and Simulation (M&S) was held in May 2017 aiming to find future areas of collaboration where AI can play a significant role.

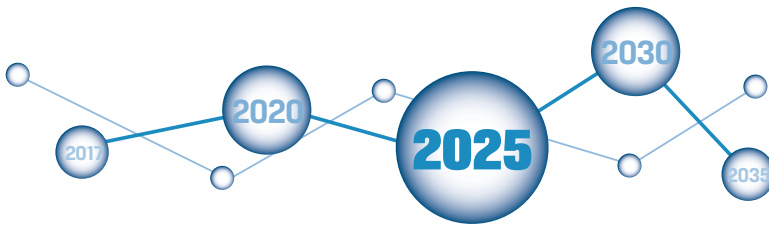
Member States' participation in collaborative projects is key to developing a European capability based on AI, for example in areas such as support to decision making for the Commanders, extraction of relevant semantic information to support Military Intelligence, creation of realistic behaviour for opposite computer generated

forces or intelligence for autonomous operation of unmanned vehicles.

The potential areas of application are so wide that joint investment programmes should be established to allow all Member States' Forces to have access to these new capabilities at all possible levels of operation.



*By Ignacio Montiel-Sánchez,
EDA Project Officer
Information Technologies*



Defence Internet of Things (dIoT)

Why it matters

The Internet came from the defence world. In the 1970s and 80s, DARPA Net, the US Defence Advanced Research Projects Agency Network, used switching and protocols to give Cold War survivability to communications networks.

The 1989 world wide web naming and addressing protocols allowed the Internet to evolve into the global phenomenon that we know today. More recently a new concept has come into being with the so-called Internet of Things (IoT), which is the extension of Internet connections beyond computers and communications systems to everyday objects such as cars, watches, food packaging, domestic appliances and many other products. Civil applications and commercial producers are the main drivers of this IoT technological revolution. The defence sector R&T has meanwhile continued Internet-related innovation – notably the concepts of Network Centric Warfare and Network Enabled

Capability (NEC) that were espoused at the beginning of the century and are now concepts regarded as 'business as usual' with capability platforms and soldiers systems increasingly becoming network nodes in wider system of systems capabilities.

Defence NEC, of course, needed to keep pace with the threat of cyber-attack; a constant battle which constrains the pace of change. The IoT trend has increasing defence utility: military intelligence and command and control systems use the myriad of sensors that can be deployed in all the domains, allowing them to acquire full situational awareness and control over diverse conflict zones or battle areas. The trend is towards an increase in urban scenarios where millions of sensors could provide military commanders with increased situational awareness and combat intelligence to carry out more effective operations on the ground.

What the EDA does

In 2007, the EDA launched the ARMS project ('HUGE Network Wireless Connectivity for Autonomous Remote Multi-Sensing Systems') which analysed the way of using multiple sensors in the military domain.

The conclusions of this project were that Command, Control, Communications, Computers, Information/Intelligence, Surveillance, Targeting Acquisition and Reconnaissance (C4ISTAR) systems at that time had a strong potential to provide a much wider situational awareness.

The main capability gap highlighted in that project was the lack of 24/7 surveillance capabilities for urban and large remote areas.

The development of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) components was identified as a possible solution to fill the gap with a wide area capable ISR sensor network.

This project was one of the initial attempts to develop a kind of military IoT. In MEDUSA (Multi Sensor Data Fusion Grid for Urban Situational Awareness), one of the EDA Ad-Hoc Cat A Joint Investment Programmes (JIP) in Force Protection (FP), a standard architecture from the civil IoT was used to connect and fuse the data from different sensors like RPAS, UGVs or soldier sensor nodes. A demonstration was conducted showing the feasibility of the concept.

The way ahead

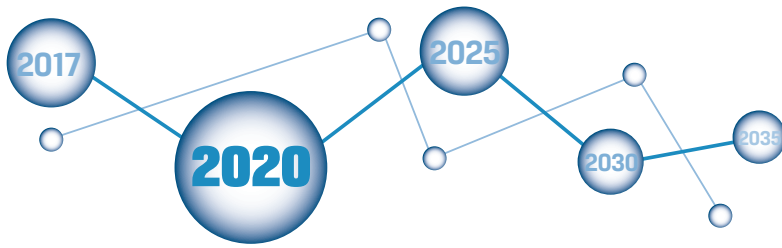
While existing civil IoT technology is being applied in the military domain, Member States' strong focus and continuous investment in this topic will be required to make it a success. The fast pace of technological change in this domain makes it necessary to increase defence research.

A new EDA project, WINLAS ('Wireless sensor Networks for urban Local Areas Surveillance'), currently under preparation, will analyse the behaviour of sensor networks, with a large number of heterogeneous devices for urban warfare. The effective management of sensor networks in hostile urban environments represents a true challenge and will require different issues to be addressed soon. Future work in

this domain to provide the Defence IoT (NEC 2.0) will in particular have to focus on making available secure connections through suitable topologies and distributed fusion of heterogeneous sensors that must be small, mobile, robust, self-organising, autonomous and resilient, in order to infer the state of the battlefield producing actionable situational awareness.



By Ignacio Montiel-Sánchez,
EDA Project Officer
Information Technologies



Big Data analytics for defence

Why it matters

Big Data is a consequence of the growth of digital data on the Internet and the number of objects connected to the Internet (see previous article on Internet of Things).

But when is data big? In essence, it is when traditional computing capabilities (storage, analysis, transfer networks and visualisation) can no longer cope with the quantity, speed, complexity or quality of the data which overwhelms us humans beings. Examples include: email, social data, XML data, videos, audio files, photos, GPS, satellite images, sensor data, spreadsheets, web log data, mobile data, RFID tags and PDF docs. This has called for investment in innovative hardware and software architectures (such as open-standard *Hadoop Distributed File System* and associated application *MapReduce*). Big Data is being seized upon by the private sector to improve decision-making and predict future events. For example,

using Big Data, telecommunications and transport companies can now better predict customer usage, supermarkets can predict what products will sell and car insurance companies understand how well their customers actually drive.

This is important because the ability to harness the ever-expanding amounts of data is transforming our capacity to understand the world and everything within it.

The advances in analysing Big Data allow us to, for example, decode human DNA in minutes, find cures for cancer, accurately predict human behaviour, foil terrorist attacks, pinpoint marketing efforts and prevent diseases. Big Data is used to better understand customers and their behaviours and preferences getting a more complete picture in order to create predictive models. So what does this mean for defence capabilities?

What the EDA does

The EDA study 'Big Data in Defence Modelling & Simulation environments' (BIDADEMS) sought to explore the Big Data domain to understand how its tools and techniques could best be applied to Modelling & Simulation (M&S) activities in the Defence environment.

The aim was to understand the impact on M&S across the full breadth of its use in the life cycle of future military systems. The output of the study is an Assessment Matrix mapping Big Data tools to M&S areas to facilitate future defence collaborative projects in developing the next generation of military simulation systems in a way that optimises the use of Big Data tools and processes. Those areas are:

- Programme Preparation: development of future operating concepts and capability management activities:

- Operational Analysis: analytical techniques used to inform defence decision making:
- System Development: acquisition, development and fielding of new or enhanced military capabilities:
- Training: development of in-service doctrine, analysis to identify training gaps, retention issues, alternative training methods, and Live, Virtual or Constructive military training:
- Support to Operations: decision making support to the planning and conduct of operational activities.

The way ahead

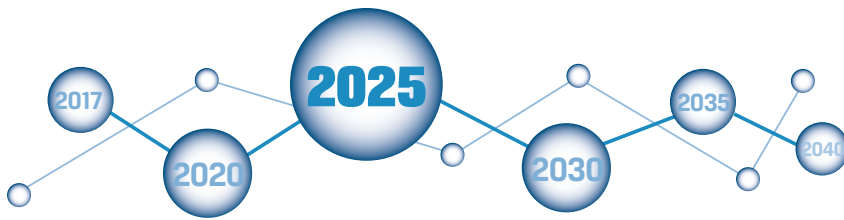
Further analysis is needed to see how commercial Big Data applications can serve the security and defence sector and examine the potential benefits.

Careful concurrent R&T and capability management will be required if Big Data benefits are to be realised. Defence has to face the challenge and invest in Big Data technologies and associated infrastructures that will be adapted and oriented to the characteristics of the defence priorities. EDA collaborative projects will serve this

purpose as the requests of support to decision making for Operational Analysis or Support to Operations, Defence Systems development and Training are increasing for the success of Joint Force Operations and the European Military Bodies.



By Ignacio Montiel-Sánchez,
EDA Project Officer
Information Technologies



Blockchain technology in defence

Why it matters

At present, blockchain and other distributed ledger technologies are drawing the attention of researchers due to their potential cross-sectorial applications beyond finance where it emerged.

Because of the expected impact on the financial sector, banks are serious in further exploring this technology. Blockchain was born as the underlying protocol to sustain the Bitcoin 'virtual currency' by incorporating a data security layer and providing user trust and confidence about digital transactions.

A blockchain is all about organizing and storing information in accordance with a predefined logic. Instead of data being accounted and stored on a central server's database, it's encrypted, and a copy is stored on every node connected to the network. This disruptive technology is recognised as a possible revolution of the way the Internet functions and opens infinite possibilities. Blockchain is based

on distributed databases that are shared among peers. It can thus be seen as a huge file which stores data in a logical, historical, secure, and immutable way.

This peer-to-peer system stores and shares a digital ledger of data using cryptography to ensure confidentiality and integrity. As a result, blockchain networks not only reduce the probability of compromise but also impose significantly greater costs on an adversary to do so. The importance of this technology is the creation of trust in digital data because a large decentralised network is able to attest the validity of data and it holds a permanent secure digital record. Other possible applications come in the implementation of smart contracts on the blockchain, identity protection or data protection. However, the benefits and real applications in the fields of communications and countering cyber threats will likely not be seen until 2025 at the earliest.

What the EDA does

Given its high disruptive potential, blockchain technology is a research topic of interest for the upcoming Cyber Strategic Research Agenda within the EDA framework.

Firstly, encryption is one of the cornerstones of Communication and Information Systems (CIS) security and is becoming increasingly important when ensuring the confidentiality of information. Secondly, the novel approach brought about by blockchain may lead to new

findings on defence applications; notably on, information security, authentication, data integrity and resilience, among many others.

Furthermore, some other aspects of the blockchain technology, mainly the distributed database, the peer-to-peer transmission and the computational logic will be candidate technological building blocks of the next version of the Overarching Strategic Research Agenda (OSRA).

The way ahead

Due to the nature of blockchain, challenges may require further research on areas such as interoperability, network infrastructure and a thorough analysis on its regulatory framework.

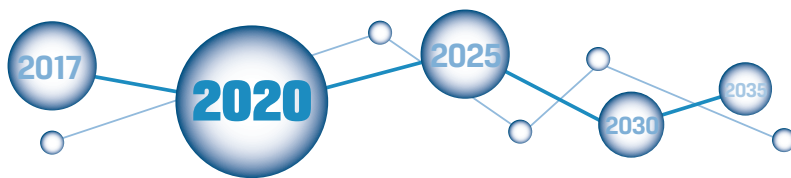
In the coming years, the defence research community is expected to search for new applications for the military based on blockchain technology with predominant candidate areas such

as cyber defence, secure messaging, resilient communications, logistics support and the networking of the defence Internet of Things.

It seems unavoidable that the work on CIS and neighbouring fields as Modelling and Simulation will strongly be affected by the advances to come from this disruptive technology.



*By Salvador Llopis Sanchez,
EDA Project Officer
Cyber Defence Technology*



Artificial Intelligence (AI) enabled cyber defence

Why it matters

The flow of digital information is expanding on a daily basis making it increasingly difficult to manage and structure it or even to separate what is important from what is superfluous.

Faced with this challenge, new promising breakthrough technologies are being developed to bring 'data analytics' to the next evolutionary level. Artificial Intelligence (AI), in particular, is expected to become significant in many fields. Some forms of AI enable machine learning like deep learning can be used to perform predictive analytics. Their potential for the defence domain is huge as AI solutions are expected to emerge in critical fields such as cyber defence, decision-support systems, risk management, pattern recognition, cyber situation awareness, projection, malware detection and data correlation to name but a few.

We have already seen tremendous technological progress on self-driving cars where an analysis of the surrounding environment is made in real-time and AI systems steer cars autonomously under specific circumstances. One of the potential applications of AI in cyber defence may be to enable the setting up of self-configuring networks. It would mean that AI systems could detect vulnerabilities (software bugs) and perform response actions like self-patching. This opens new ways to strengthening communications and information systems security by providing network resilience, prevention and protection against cyber threats. Cyber experts agree that the human system integration is a key

element that must be present in an AI cyber security system. If we take into account the high speed required to perform any cyber operation, it's obvious that only machines are capable of reacting efficiently in the early stages of serious cyber-attacks. AI can thus overcome the shortfalls of traditional cyber security tools. It is also a powerful mechanism able to improve malware detection rates using a baseline of cyber intelligence data. AI cybersecurity systems can learn from indicators of compromise and may be able to match the characteristics of small clues even if they are scattered throughout the network.

Another aspect relevant in building an AI enabled cyber defence could be the future implications of Quantum computing or high processing computers. This enhancement to support data-processing may increase the efficiency of algorithms. Algorithms are key components of running AI and may be tailored to counter complex cyber threats. An algorithm is a set of step-by-step instructions given to a computer to accomplish a specific task. AI may push this technology to another level, to achieve intelligent autonomous algorithms. To illustrate these research challenges, Facebook recently abandoned an AI experiment after 'chatbots' invented their own language which was not understandable by humans. Computer machines had demonstrated better skills than humans in playing chess or poker. This breakthrough technology is likely to be disruptive in many ways nobody can predict today.

What the EDA does

The EDA organises 'Cyber Innovation Days' to provide Project Team Cyber Defence members and Cyber Research and Technology working group representatives with examples of European research efforts in the cyber defence domain and to foster discussion between and within academia, industry and the armed forces on relevant research and emerging research topics.

It is considered one of the initiatives to facilitate the necessary innovation in the cyber field. The EDA has included AI in the Cyber Strategic Research Agenda as a recognition of its high potential for defence and the tremendous impact it is likely to have on current state-of-the-art technologies.

The way ahead

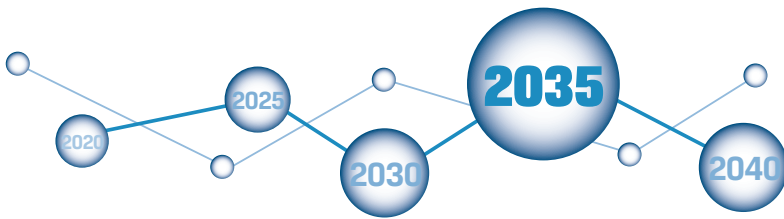
The practical implementation of AI cyber security systems may lead to changes and new approaches on cyber system engineering and cyber defence architectures.

New AI applications are emerging on Intent Based Network Security (IBNS), on AI platforms for cyber defence or immune computer systems which have the ability to self-adapt. On the other hand, the rise of AI-enabled cyber-attacks is expected to cause an increase of sophisticated cyber threats. Ongoing and future research activities should be explored

in countering complex cyber threats, malware reverse engineering and projection to enhance a cyber situation awareness among many others.



*By Salvador Llopis Sanchez,
EDA Project Officer
Cyber Defence Technology*



Robotics in defence

Why it matters

Robotics and autonomous systems (RAS) are already extensively used in many civil domains, especially since technological progress render them less expensive and bulky while, at the same time, more flexible and easier to interact with.

As such, robots and multi-robots (or swarm) systems (MRS) also have the potential to play, in the foreseeable future, a disruptive role in military operations in the sense that they will allow to perform task

that today are considered too risky, complex or even impossible for humans.

But RAS not only have the potential to perform conventional dirty, dull and dangerous military tasks like surveillance and counter mining; they are also likely to change the way military operations are conducted in the future, and even to make it possible to envisage new type of missions.

What the EDA does

An assessment of different defence scenarios in which heterogeneous (ground, air, maritime) teams of robots could provide added value was performed by the EDA in the SMUVO (Scenarios for Multiple Unmanned Vehicles Operations) project.

The EDA's MUROC project (Multi Robot Control in support of the Soldier) provided a survey on the state of play in robotics research with a focus on multi-robot control and man-machine teamwork.

The project has clearly shown that there is a strong interest from the defence sector for cooperatively working with robot systems. More R&D work is needed and a variety of new technologies need to be further developed, improved and tested before the military can harvest the full potential of RAS. This is especially true for safety critical tasks related to warfare where the level of dependability has to be maximum.

In this domain, several R&D projects have already been or are

currently being carried out within the EDA framework. The ASIMUT project (Aid to Situation Management based on Multimodal, MultiUAVs, Multilevel acquisition Techniques) aims at decreasing operator workflow during a surveillance mission lead by swarms of UAVs. To this end, new algorithms were developed to increase detection and data fusion capabilities, and increasing the autonomy of UAV swarms. SPIDER (Inside Building Awareness and Navigation for Urban Warfare) aims to provide a proof of concept for an innovative system to improve the soldier's inside-building awareness through the support of mobile robots.

Finally, EuroSWARM (Unmanned Heterogeneous Swarm of Sensor Platforms) will develop and demonstrate techniques and technologies for adaptive, informative and reconfigurable operations of unmanned heterogeneous swarm systems.

The way ahead

The next big challenge for defence will be to bring these technologies from the lab to real operations where robots will have to co-exist and cooperate with humans. To have a usable and useful RAS, simply increasing the level of automation will not be sufficient. Achieving trusted autonomy will be essential.

Just as it is the case in human relationships, robots must earn the trust of their teammates and operators through proven reliability. Barriers to establishing trusted autonomy include those normally associated with 'standard' human-human trust relationships. But there are additional barriers associated with human-machine trust: different ways of thinking (digital vs. analogue) and expression, low transparency and traceability (robots can't explain their own decisions), low mutual understanding of goals. The further the level of autonomy will be pushed by technology, the more the following questions will need to be answered: How far can robots be 'trusted' to perform their allocated tasks without the need for human supervision? Which level

of trustworthiness can be associated with a task performed by an autonomous system? This is even more challenging in MRS where agents must also 'trust' other agents.

Trusted autonomy represents a complex 'socio-technological' research area which is still at an early stage and which will require, in addition to the establishment of the relevant legal and ethical framework, significant research in the following fields: development of more performing, robust and reliable sensing and data acquisition; human-machine communication and integration; and verification, validation and evaluation methods.



*By Marco Detratti,
EDA Project Officer
Guidance, Navigation, and Control*

GO ONLINE & GET MORE:

In addition to the print version, *European Defence Matters'* online edition offers expanded articles and pictures

STEP: EUROPEAN MALE RPAS TAKES SHAPE

For over 20 years, a number of defence specialists have repeatedly pointed out a growing operational need for long range remotely piloted aircraft systems (RPAS) in the European armed forces, and the existence of a recognised competent and competitive aeronautic industrial base in Europe. Member States are still dependent on non-European suppliers for large RPAS.

Read more >



EUROPEAN DEFENCE: 'ONLY BE MASTERED CO

In an exclusive interview with European Defence Matters, Airbus Defence & Space CEO Dirk Hake shares his views and analysis on the prospects and challenges of future European collaborative defence projects. He also touches upon cyber defence, the potential of the proposed European Defence Fund, possible Brexit implications on defence as well as the European Defence Agency's role in facilitating defence cooperation and strengthening Europe's defence technological and industrial base.

Read more >



GO ONLINE & DISCOVER

the new *European Defence Matters* magazine on www.eda.europa.eu/webzine for access to the latest issue and an archive of previous editions

OPTIMISING EUROPE'S MAIN BATTLE TANK CAPABILITIES

In the light of current threat assessments and the evolving strategic situation in Europe and its wider neighbourhood, Main Battle Tank (MBT) capabilities have massively gained in importance. While some EU Member States exhibit conspicuous and disconcerting MBT gaps, others have large and costly overcapacities they currently don't use. Hence the European Defence Agency's (EDA) initiative to optimise existing MBT capabilities by Pooling & Sharing available assets for the benefit of all.

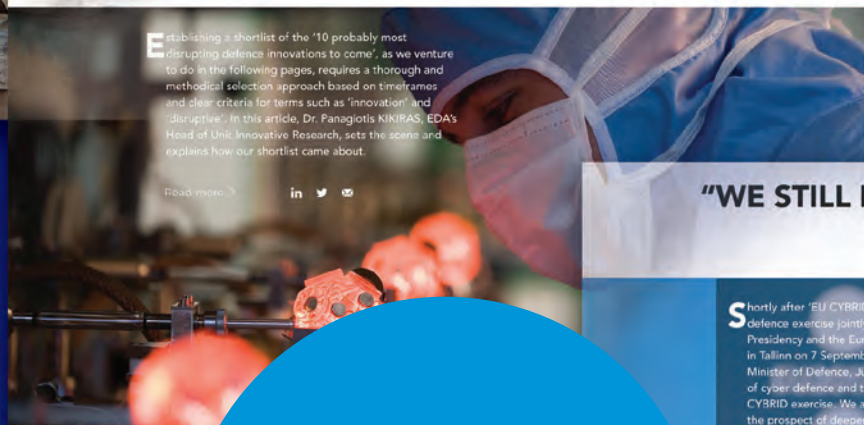
Read more >



DISRUPTIVE DEFENCE INNOVATIONS AHEAD!

Establishing a shortlist of the '10 probably most disrupting defence innovations to come', as we venture to do in the following pages, requires a thorough and methodical selection approach based on timeframes and clear criteria for terms such as 'innovation' and 'disruptive'. In this article, Dr. Panagiotis KIKIRAS, EDA's Head of Unit, Innovative Research, sets the scene and explains how our shortlist came about.

Read more >



GO ONLINE & GET BETTER SERVICE:

Share articles and pictures instantly via Twitter, LinkedIn and email

GO ONLINE & ENJOY READING:

The magazine's 'Explore' section allows you to easily access the *European Defence Matters* archive and revisit articles of previous editions

"WE STILL HA

Shortly after 'EU CYBRID', the defence exercise jointly organised by the European Commission, the Presidency and the European Council, in Tallinn on 7 September, the Minister of Defence, Jüri Luik, set the scene for the CYBRID exercise. We also saw the prospect of deeper European defence cooperation and the implementation of the defence field as well as on

Read more >



NEXT STEPS CAN
COLLABORATIVELY"



European Defence Matters magazine: GO ONLINE & GET MORE

HAVE SOME WORK TO DO ON
CYBERSECURITY"

the strategic table-top cyber
organised by the Estonian EU
an Defence Agency (EDA)
ve sat down with Estonia's
ik, to discuss the importance
ain lessons learned from the
asked him about his views on
european defence cooperation,
atest EU initiatives in the
he EDA's future role.



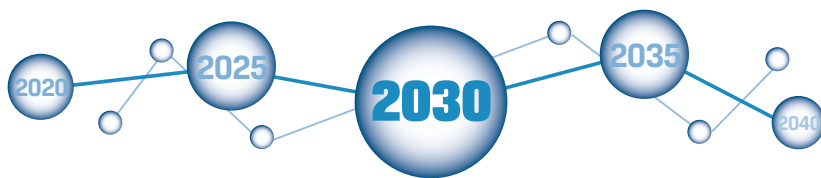
Your *European Defence Matters* magazine is now online at www.eda.europa.eu/webzine, in a user-friendly, state of the art responsive lay-out and accessible via all your devices: smartphone, tablet or desktop!

Intuitive navigation allows you to click your way easily through the various sections of the magazine, from the 'Cover Story' through 'Industry Talk' to 'Focus', 'In the Spotlight', to 'Interviews' and others.



Subscribe for free and follow
European Defence Matters:
www.eda.europa.eu

To advertise in *European Defence Matters*
Cyril Mikailoff, Phone: +336 21 71 11 18
or: cmikailoff@turbomedia.eu



Autonomy in defence: systems, weapons, decision-making

Why it matters

Over the last decade unmanned systems have become regular features of conflicts. The use of drones (unmanned aerial systems), in particular, illustrates the huge potential of unmanned systems.

While remotely-controlled drones are probably the most prominent example of unmanned systems technology, the latter's true potential covers all military services and environments (land, sea, air and space).

The use of remote-controlled unmanned systems is only a first step. Future unmanned systems will see higher degrees of autonomy provided inter alia by Artificial Intelligence (AI) or cognitive computing. The search for autonomy first focused on navigation aspects and later extended to self-protection aspects. The focus currently is on the exploitation of sensors and effectors to execute specific missions.

What the EDA does

The EDA has conducted several collaborative R&T projects focusing on different degrees of autonomy (tele-operated, semi-autonomous or autonomous) for ground, naval or air applications.

In the ground domain some aspects of autonomy in terms of vehicle following or obstacle avoidance have been addressed in the HyMUP (Hybrid Manned-Unmanned Platooning) project aiming to prove the feasibility of mounted combat missions of unmanned systems coordinating with regular manned vehicles. Additionally protection of autonomous systems against enemy interference and safety requirements for combined manned-unmanned mission will be addressed in the EDA's PASEI project (Protection Against Enemy Interference).

In the naval domain the Unmanned Maritime Systems (UMS) programme consists of 15 coordinated projects that address the specific challenges posed by Maritime Mine Countermeasure (MMCM) operations. Completed projects such as MLM (Modular Lightweight Minesweeping) focus on removing staff from minefields and replacing expensive manned vessels with an unmanned solution. The dominant vision for future minesweeping is smaller lightweight unmanned surface vehicles equipped with lightweight sweep sources, either operating alone or together with other vehicles in a formation. A follow on project is currently under preparation. Other projects such as NECSAVE (Networked Enable Cooperation Systems) focus on the swarm concept

for communication networks. Finally, the challenge of underwater communications is one of the keys to unlocking the possibilities of persistent autonomy. RACUN (Robust Acoustic Underwater Communications Networks) is an EDA project that addresses this topic. A follow on project entitled SALSA (Smart Adaptive Long and Short Range Underwater Acoustics Networks) is under preparation.

In the air domain, Remotely Piloted Aircraft Systems (RPAS) are an area in which automation and autonomy are key elements. The EDA is involved in the development and standardisation of these capabilities with a clear objective: the integration of military RPAS in the European airspace. MIDCAS (MID air Collision Avoidance System) and ERA (Enhanced RPAS Automation) are the main projects in this area.

Guidance, Navigation and Control (GNC) is a cross cutting domain where the ADM-H (Autonomous Decision Making based coordination techniques for Heterogeneous Autonomous Vehicles) project was conducted by the EDA to improve decision-making algorithms for the coordination of groups of unmanned systems engaged in a military mission and the exploitation of the operational advantages of using such systems in future defence theatres. The performance assessment has shown that through adequately coordinated unmanned heterogeneous vehicles even complex tasks directed by a Commander can be handled autonomously, reducing the human workload except for the most critical decisions.

The way ahead

Successful implementation of autonomous systems in defence does not depend exclusively on technology development.

Doctrines will need to be reviewed and updated as military tactics and procedures may change with the introduction of autonomous systems. Political, cultural, sociological and regulatory issues as well as their potential ethical and legal implications and safety constraints will

also need to be considered especially when autonomous systems are armed with lethal weapons.



*By Marek Kalbarczyk,
EDA Project Officer
Land Systems Technologies*



Future advanced materials for defence applications

Why it matters

Military systems are becoming ever more complex, and so are the materials used to build them. In this context, advanced materials have sparked considerable interest as their use has the potential to significantly shape future operational effectiveness in military missions.

Advanced materials can be used in a wide range of domains and hostile environments where risks and damages can be reduced with the use of protective solutions. The most disruptive effects are expected to

derive from the integration of functionalities such as energy harvesting, camouflage, structural and personnel health monitoring, protection in 'super-intelligent' materials for platforms and soldiers.

Other potential applications of advanced materials to be explored in the future include the potential of self-healing materials, cyber-protective material (reacting to electromagnetic interference), biomimetic material designs, morphing aerofoils, or the integration of metamaterials.

What the EDA does

Several EDA projects have already been conducted in key areas of advanced materials. In smart textiles, for example, the EDA's work has been concentrated on ground systems, materials and CBRN domains.

The CEDS (Combat Equipment for Dismounted Soldier) feasibility studies addressed topics such as adaptive camouflage, architecture approaches and soft ballistic protection. Within the Joint Investment Programme on CBRN, the PROSAFE project explored the use of nano-fibres for permeability.

Notable efforts in researching improved repair methods and structural health monitoring were undertaken in the PATCHBOND project. Advanced Low Observable Materials have been explored in the ALOA project and are currently researched further under the ALOMAS project.

The CERAMBALL project has addressed lighter ballistic protections for soldiers while projects such as ECOCOAT and CCNS have been centred on environmentally compliant coatings.

The way ahead

Through its activities, the EDA R&T community has already identified some of the next strategic steps needed for advancing the development and use of these technologies in European defence.

For instance, the need for setting priorities in the area of smart textiles is increasingly recognized, with a long-term objective of achieving multifunction soldier uniforms which have to be washable, repairable, reusable and recyclable. Today, efforts in this field are focused on the development of standards to define terms, technical specifications and requirements for smart textiles. Manufacturing and commercialization of smart textiles represents a growing market and opportunities stem from the technological developments taking place in the civilian sector. Furthermore, the certification and standardization aspects are coming into focus, with particular attention paid to ensuring product quality and development of legislation.

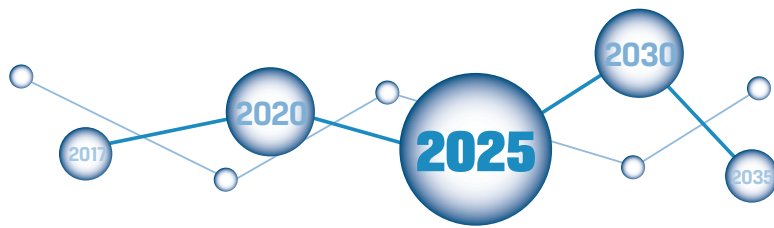
The major land, sea and air platforms currently in service are not expected to be retired for another two to three decades which means that the existing platforms will have to be upgraded with new materials. As a consequence, new opportunities for the implementation of new materials will most certainly arise through mid-life upgrades, incremental improvements, urgent operational needs, lifetime extension, legislation and a growing need for European technological and material non-dependency. These materials will make platforms and soldier systems lighter and better

performing, while at the same time reducing their maintenance periods and cost. The incremental adaptations of platforms should not be the only aim as new technologies such as unmanned aerial vehicles and emerging directed energy weapons (DEW) are maturing rapidly, and will need new materials to enhance their capabilities (UAVs) or to counter-measure them with new protections.

The development of the materials to be integrated into new design platforms is critical to ensure the capabilities of the European Armed Forces in the future. For the application of these technologies in defence, it is becoming increasingly important for industry to gain a deeper understanding of operational military needs. In addition, the specification of environmental properties of materials is viewed as necessary for guiding the production and design of future materials. More cooperation between defence structures, industry and academia, coupled with appropriate financial resources are key elements for the advancement of research work in this area.



*By Patricia Lopez Vicente,
EDA Project Officer
European Defence Research*



Additive manufacturing in defence

Why it matters

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 for rapid, delocalised and flexible manufacturing.

AM is already used in civil industry and by defence producers. However, the armed forces are still far from exploiting the full potential of this technology.

The expected growth of the AM market could generate many advantages for the European defence community: cost reduction on the production of tools and parts, design enhancements, reduced time to reach the 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 because of the processing and time limitations. Furthermore, AM technologies can be highly promising for enhancing defence capabilities such Logistic Support for Deployed Forces in remote or hostile environments.

Having AM technologies in the area of operation might significantly impact the course of CSDP 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.

What the EDA does

To further explore the deployability of AM technologies, in 2016 the European Defence Agency launched a project aimed at raising awareness of 3D-printing in defence.

The 'Additive Manufacturing Feasibility Study & Technology Demonstration' project successfully deployed a 3D-printing lab to Zaragoza (Spain) for the duration of the third European Advanced Airlift Tactics Training Course in June 2017 (EAATTC 17-3). The successful test flight of the AM lab was pivotal to examining the feasibility of deploying the facility 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), who were keen to learn how 3D-printing could benefit their area of expertise.

The project represents a clear example of how cross-fertilization of ideas from different domains, from R&T to operations, will enhance defence capabilities, especially when supporting missions. The lessons learned from this deployment will contribute to shaping the design and requirement of future 3D-printing facilities.

The way ahead

Increasing awareness of AM's potential for defence is crucial. Equally important will be to create synergies between the Materials R&T community and the operational military staff, and helping the R&T community 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 AM can generate will be widened and improved. In addition, training is required to make this technology effective and accessible to military users. On the technology side, further work is foreseen 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 the standardisation of the processes, certification of the parts produced and the legal aspects.

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 this technology gap can enhance the logistical and operational agility of armed forces and give European defence a game-changing competitive advantage in a rapidly evolving technological and conflict landscape.



*By Patricia Lopez Vicente,
EDA Project Officer
European Defence Research*



Next Generation Sequencing (NGS) for biological threat preparedness

Why it matters

Novel sequencing technologies provide new opportunities in infectious disease detection and diagnostics, such as rapid sequencing in response to the early phase of an epidemic or the determination of genotypes during the investigation of a bio-threat event. Portable near-future sequencing instruments should be low cost to use and widely deployable.

NGS, also often referred to as High-Throughput DNA Sequencing (HTS) methods, will enable a paradigm shift. Biological field detection is currently based on PCR¹-related methods which rely on customised reagents targeting only a limited set of B agents, while NGS targets any B agent ('wide-spectrum' or 'agnostic' method). It also enables strain-level identification without a priori information on the investigated B-agent (which PCR does not) which is useful for forensics purposes. The use of NGS in the defense context can be wider than just biodefense (general water and food quality control, sanitary medical purposes etc).

One of the key challenges in investigating alleged use of biological weapons is the ability to differentiate intentional spread from naturally-

occurring biological events through a scientific assessment, including molecular characterisation of the suspected pathogen. Presence of a pathogen outside its natural area of occurrence or changes in its genetic sequence may indicate deliberate spread. Therefore, molecular characterisation of a pathogen is an important part of a strong response to biological threats as the origin(s) of the outbreak can be identified and an appropriate course of action followed. Genetic sequencing identifies the exact genetic code of the pathogen, thus identifying the species and/or strain in question. Currently, sequencing requires massive hardware, although the recent, next generation sequencing methods, especially their portable/field deployable applications, have become a strong alternative for detection and typing of bio-threat agents. Novel sequencing technologies however require special expertise such as advanced bioinformatics.

1. Polymerase Chain Reaction targeting a specific genetic motif in a genome.

What the EDA does

The EDA supports Member States in addressing CBRN defence topics through a Joint Investment Programme on CBRN Protection (JIP CBRN) on several topics where three projects specifically address Next Generation Point Detection for B Agents.

In addition, another project named EBLN (European Biodefence Laboratory Network) focused more on the design and organisation of a shared database with reference typing data as a necessary common resource for typing and identification of B-agents. The

EBLN II project (under preparation) will aim at fostering microbial strains characterisation. It will encourage Member States to develop their capacity in NGS, as well as the comparison of data obtained in different pMS laboratories.

This could in turn lead to the development of bioinformatics analysis tools or the harmonisation in the processing of the data obtained. However, this project focuses on reach-back laboratories and not on technology developments for field use.

The way ahead

Development of field-ready sequencing technology could be used as part of a real-time response to an alleged bio-attack or an infectious disease outbreak, if the necessary equipment is highly portable/field deployable and the protocols could be simple, rapid and robust.

Real-time data of an outbreak could reveal key indicators of an emerging epidemic including intentional spread of a pathogen. Furthermore, data not considered sensitive can be shared through on-line cloud servers.

Next stages would require improvements in the following areas:

- Developing of sample preparation and sequencing method for complex field samples. At the moment NGS is best applied when analyzing nearly pure cultures or other non-high background samples:
- Development of secure real-time exchange capabilities and platforms for sharing of data and information from the field would allow the

bioinformatics analysis to be performed by other laboratories than the ones doing the sequencing:

- There is also a need for improving the accuracy of reference databases which could be used in an investigation:
- Developing end user-friendly interface for field sequencing is also required.



*By Shahzad Ali,
EDA CapTech CBRN &
Human Factors Officer*

"Guaranteeing Europe's security requires a strong joint effort by its member states. The Defence Fund can surely be one part of that"



> **European defence: "Next steps can only be mastered collaboratively"**

In an exclusive interview with *European Defence Matters*, Airbus Defence & Space CEO **Dirk Hoke** shares his views and analysis on the prospects and challenges of future European collaborative defence projects. He also touches upon cyber defence, the potential of the proposed European Defence Fund, possible Brexit implications on defence as well as the European Defence Agency's role in facilitating defence cooperation and strengthening Europe's defence technological and industrial base

What are Airbus' defence innovation and development priorities for the coming years and how important are collaborative European projects in your planning?

We have to adjust our existing products to the era of digitalization and we need to ensure that our new developments are capable of translating all the accessible data into useful information. Large defence products with a high degree of complexity come with a high price tag. Those next steps into the future of European defence can only be mastered collaboratively, bringing together financial and technological resources. Projects like the European MALE drone and a common next generation weapon system can act as blueprints for the future in defence. Innovation is key to guarantee the sovereignty of Europe in the decades to come.

Germany and France have pledged to develop a European combat aircraft. What's your assessment, can this be done? Under which conditions?

This was a very forward looking step, which we welcome. The time is now, when our existing fighters are in their best years, to decide about the succession. If you look into the development cycle of an aircraft it's simply too late to enter into discussions at the end of the current platform's lifecycle. We see that both countries seem willing to break with the past and try to avoid individual solutions from the onset. I am convinced the project can be successful if both governments and industry thoroughly analyse the lessons learnt from

previous attempts. What we should be clear about is that a next generation weapon system will always be more than a simple replacement of current platforms. It will be about connectivity, real time data exchange, commanding swarms of smaller drones – and all this in a highly digitalized environment.



The EDA should intensify its work on harmonising military requirements, through Common Staff Targets"



MALE RPAS is another European programme in which Airbus DS plays a central role.

What are in your view the main remaining challenges to make it a genuine success?

So far the project can only be labelled a success since all major European companies are closely working together on the project at our Military Aircraft Centre in Manching near Munich. The results of the definition study are expected mid-2018. Then two things will be critical. Firstly, a quick and robust commitment by the interested nations for further development. Secondly, the finalization of European standards for qualification and certification of drones in public airspace.

Multinational defence programmes, by nature, can be problematic, as the A400M

has shown. Are there lessons to be learned from that experience for future European defence industrial projects?

Past experiences show us that the problem is very often not the multinational approach itself, but the rules of engagement. Clearly many consumer products are manufactured in several places and then assembled in another one. More significantly, the concept is also proven in Airbus when producing commercial aircraft. But the selection of suppliers and locations should be an economic one and not driven by politics. Additionally the nomination of what we call a "lead nation" will be a decisive success factor. I am convinced that we need to tear down national borders and also to rethink our attitude towards 'juste-retour' demands for national work shares that often do not allow for efficient programme structures and the selection of best performing partners and suppliers.

Cybersecurity is crucial for defence, today and even more so in the future. Is Europe, governments and industry alike, making the best of its potential in this domain?

The first question must be: Is Europe capable of securing its own IT infrastructure? For many institutions and companies I am not so sure. Furthermore cyber-security standards within the EU nations differ very considerably. As web-based solutions do not stop at national borders we need to achieve common industrial standards.

That's why Airbus decided to build up →



"We have to adjust our products to the era of digitalization"

its own defence shield first and only then to offer cyber security solutions to other parties. It is a testament to our capabilities that now several EU institutions trust in cyber-secured infrastructure from Airbus. We are doing our utmost to live up to our responsibility here.

What is your assessment of the proposed European Defence Fund? Can it be a game-changer for boosting joint development and procurement of defence capabilities?

I am convinced that guaranteeing Europe's security requires a strong joint effort by its member states. The Defence Fund can surely be one part of that.

SMEs fear that the European Defence Fund might first and foremost benefit prime defence suppliers, including Airbus DS. What would you respond to them?

Look at the situation we have today. All primes rely heavily on their suppliers. Why should that change just because the money for the final product comes from another source? In addition, the consolidation of Europe's defence industry can only be in the interest of the customer.

What impact do you expect Brexit to have on European defence? Politically, but also for Europe's defence industry and future collaborative projects?

As a truly European company we deeply regret this process. Currently we can't foresee the outcome of the Brexit negotiations and therefore have to be prepared for different

scenarios. Of course we still hope that there will be finally a pragmatic solution where the UK will remain an important part of our supply chain and of our talent pool.



We need to tear down national borders and rethink our attitude towards 'juste-retour' demands for national work shares



One of the EDA's core missions is to facilitate defence cooperation and strengthen Europe's defence technological and industrial base. In your view, what could the Agency do more, or perhaps differently in this respect?

The EDA was at the forefront of the recent pooling and sharing initiative involving an increasing number of nations around the acquisition of multi-role tanker/transport aircraft. This has been a true success for the

Agency, with the potential for more nations to join, and should therefore encourage it to replicate this process with other existing military capabilities.

In an even less visible area, but nonetheless very important, the EDA should intensify its work on harmonising military requirements, through Common Staff Targets and ultimately Common Staff Requirements, be it in future military Govsatcom, military Earth observation or Maritime Patrol Aircraft.

The EDA has also a card to play in the soon-to-be created EU defence research programme and also in the EU defence industrial development programme (EDIDP) which should focus on late-stage development, prototyping and demonstration activities for high end capabilities. For these new initiatives the Agency will undoubtedly need additional staff and experts. But in any case it can count on the complete support and cooperation of the defence industry, because the coordination should take place as early as possible, ideally even in the definition and selection of priorities. ■



Dirk Hoke has been the Chief Executive Officer (CEO) of Airbus Defence and Space since 1 April 2016. He is a member of the Group Executive Committee. He joined Airbus on 1 January 2016 from Siemens, where he had been CEO of the Large Drives Business Unit since 2014. He has held various executive-level positions at Siemens since becoming CEO of the Cluster Western & Central Africa in 2008. His career spans 21 years and five continents.

DEFENCE & SECURITY INTERNATIONAL EXHIBITION

2018

EUROSATORY

11 - 15 JUNE 2018 / PARIS

**THE
LAND & AIRLAND
REFERENCE**

Identify your company
as a key player



GICAT

www.eurosatory.com

 **COGES**

Step by step: European MALE RPAS takes shape

Over the past 20 years, a number of defence specialists and observers have repeatedly pointed out a paradox. Despite a growing operational need for long endurance remotely piloted aircraft systems (RPAS) in European armed forces, and the existence of a recognised competent and competitive aeronautic industrial base in Europe, Member States are still dependent on non-European suppliers for large RPAS.

Building on lessons learned from several cooperative projects, including projects run within the European Defence Agency (EDA) framework, and on the announcement made in June 2013 by three major European companies that they would cooperate in this field, the December 2013 European Council stressed the need for Europe to move forward in this capability domain. This set in motion a positive political momentum.

In May 2015, France, Germany and Italy declared their intention to conduct a definition study to prepare the development of a European Medium Altitude Long Endurance RPAS. Since then, Spain has become the fourth participating member and, more recently, Belgium joined as an Observer Nation with a view to becoming a Participating State in due course.

Definition study

The main purpose of the two-year study was to identify a set of achievable operational capabilities, to define the corresponding set of system requirements and to perform preliminary design activities to allow for the launch of a potential development and production phase with minimum residual risk.

In August 2016, the European MALE RPAS Programme was officially integrated into OCCAR, a dedicated programme division was established in Munich/Hallbergmoos (Germany) and the Definition Study contract was awarded



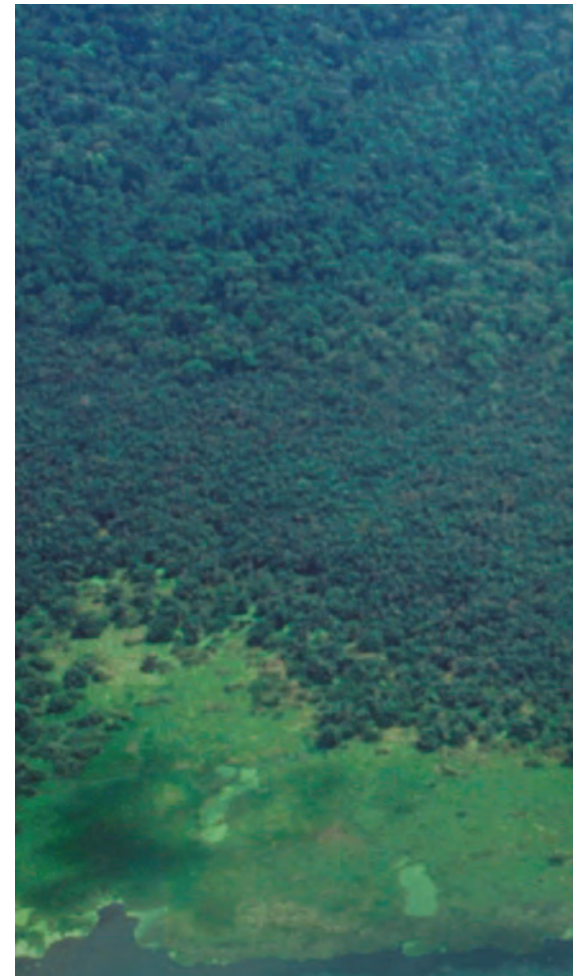
"This new system must be a game changer in the MALE RPAS world in 2025, not only as a platform but as a global system, as a capability"

Jorge Domecq, EDA Chief Executive



by OCCAR to Airbus Defence and Space GmbH, Dassault Aviation and Leonardo S.p.A. as a Co-Contracting Group (CCG).

This contract award marked the initial phase for delivering a competitive European solution for a growing capability need across the EU. Subject to a decision in 2018 of the Participating



States to continue with development and production phases, the entry into service of the first European MALE RPAS is envisaged for 2025.

Once operational, the system will be operated worldwide, in particular to support ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) missions with a variety of payloads as well as ground support missions with precision weapons engagement.

Design of the future

In July 2017, after an intensive 10 months trade-off period, the European MALE RPAS Co-Contracting Group provided a substantial set of data that allowed the Participating States (France, Germany, Italy and Spain) to agree on the basic remotely piloted aircraft (RPA) configuration and several main design drivers for the system. The selected twin engine turbo-prop configuration will be the basis for further trade-off studies until the upcoming Systems Requirements Review (SRR) planned by the end of 2017.

From the outset, the EDA was asked by Participating States to provide support to the programme, with a specific focus on the air traffic integration of the future system, and on the support to the integration of other



© Airbus

European Member States potentially willing to join the upcoming development phase.

The OCCAR Director, Arturo Alfonso Meiriño, explained: "I'm very proud that Nations have entrusted this major armaments programme to OCCAR, which provides the opportunity for OCCAR and the EDA to work closely together, specifically on air traffic insertion but also to explore opportunities to welcome other participants into the Programme."

Challenging requirements

Several factors drive the definition and will shape the development of the future system.

Competitiveness is an overarching objective that must make this new European solution the best choice for its future users. This will mean operational performance giving the end user a clear edge in the battlefield, smooth scalability to facilitate quick adaptation of the system to new missions and threats, enhanced interoperability ensuring seamless integration of the capability in multinational operations, and, of course, affordability through the whole life cycle of the system. This was reinforced by the OCCAR Programme Manager, Klaus Seitz: "the challenge for the programme is to balance the demanding operational capabilities, affordability and certification requirements".

The ability to operate with a high level of safety for mission or training purposes, in non-segregated air space, will also be an important driver for the design. The technical support provided by the EDA in that domain to the programme is closely linked with the wider activity of the Agency with its Member States and other European stakeholders (European Commission, EASA, Eurocontrol, SESAR JU) in preparing the regulatory framework and the technical solutions that will enable safe integration of RPAS in the Single European Sky.

As the EDA Chief Executive Jorge Domecq put it, "This new system must be a game changer in the MALE RPAS world in 2025, not only as a platform but as a global system, as a capability".

Way ahead

The successful completion of the next steps and the future of the first European MALE RPAS capability as such will greatly depend on two fundamental aspects of the programme.

Firstly, the links between the breakthrough the system will provide to its future operational users, on the one hand, and the development of the European industrial know-how and skills

in the related technological areas (through the consolidation of a competitive supply chain across Europe), on the other. In practice, these dimensions are two sides of the same coin: no full operational efficiency and real freedom of action can be guaranteed without making sure Europe has control over the development, production, maintenance and upgrades of such a complex defence system that will have to interact with many other defence systems in the field.



"This major armaments programme provides the opportunity for OCCAR and the EDA to work closely together"

Arturo Alfonso Meiriño, OCCAR Director

Secondly, the absolute need to embrace the development at system level with all its components: the platform, the payloads, the ground segment, but also the radio spectrum management, the information assurance or the dissemination of the information. Indeed, this programme is far more than an aircraft: it aims at being a global capability. ■

> Implementing European solidarity in defence

When the European Coal and Steel Community was created in 1950, French Foreign Minister Robert Schumann declared that "Europe will not be made all at once, or according to a single plan. It will be built through concrete achievements which first create a de facto solidarity." This pursuit of solidarity is the leitmotif that runs through the evolution of the Union as we know it today, which over time has formed one of its fundamental pillars. Today, nowhere is this solidarity more relevant than in the area of defence and security, where Europe faces renewed challenges such as instability on its borders, terrorism and hybrid threats.

The European Defence Agency (EDA) has been striving to translate this solidarity into concrete capability-oriented projects from the day it was created. In 2007, a series of collective benchmarks were identified and agreed by Defence Ministers who recognised that investment in the future was falling short of what was required and that significant challenges and fragmentation resulted from the predominance of national spending in defence capabilities.

a 'Code of Conduct on Pooling & Sharing' in November 2012 to encourage Member States to systematically consider cooperation from the outset. Two years later this commitment was further refined through the adoption of a Policy Framework for Systematic and Long-Term Defence Cooperation. Whilst these efforts all constitute steady steps towards greater coherence, they lack a coordination mechanism that allows Member States to come together to discuss and present national and cooperative

efforts towards common capability goals and to take stock of progress.

Taking the next step to increase convergence between national defence plans and EU collective support efforts

synchronisation and mutual adaptation on national defence planning cycles and capability development practices, which should also enable more systematic cooperation."

Addressing security challenges together requires political commitment from each and every Member State. The CARD can play an important role in bridging national efforts and EU collective endeavours in defence. The CARD seeks to ensure consistency between Member States' commitments on EU security and defence and related national plans, by gradually synchronising defence planning and promoting cooperation.

What was agreed

The EUGS states that "gradual synchronisation and mutual adaptation of national defence planning cycles and capability development practices can enhance strategic convergence between Member States" and that "an annual coordinated review process at EU level to discuss Member States' military spending plans could instil greater coherence in defence planning and capability development".

The November 2016 Council Conclusions on the implementation of the EUGS responded to the call for an annual coordinated review process and tasked the High Representative / Head of the Agency to present proposals on the



"The CARD seeks to take the discussion on European defence to the next level and pursue greater cohesiveness with a view to overcoming fragmentation and breaking through some of the barriers to increased and deeper cooperation"

Jorge Domecq, EDA Chief Executive

Notwithstanding these benchmarks and the agreed priority actions derived from the Capability Development Plan (CDP) in 2007/2008, the concrete impact on national defence decision-making processes remained limited. With a view to promoting the implementation of these benchmarks and priorities through a systematic process, defence ministers adopted

requires political will. Member States have made individual commitments and an 'engagement' at the European level to shoulder more when it comes to providing security in Europe. As stated in the Implementation Plan on Security and Defence under the EU Global Strategy (EUGS), an intergovernmental Coordinated Annual Review on Defence (CARD) would "foster a gradual

scope, method and content of such a review. The EDA, in cooperation with the European External Action Service (EEAS), produced a concept paper detailing these elements. This paper received advice from various EU bodies and wide support from Member States. On the basis of that work, the Council endorsed, on 18 May 2017, the modalities to establish the CARD, starting with a trial run involving all Member States as of autumn 2017. This trial run will allow the process to be tested and subsequently adapted based on lessons learned, ahead of the first full CARD cycle planned for autumn 2019.

The EDA's role

Article 45 of the EU Treaty mandates the EDA to identify capability objectives and evaluate observance of commitments, promote harmonisation and propose multilateral projects. These functions make the EDA the ideal secretariat for the CARD, supporting Member States by gathering information on national capability plans and analysing this information to provide an aggregate view of the capability development landscape in Europe. Three information blocks will cover Member States' aggregated defence plans, the implementation of the EU capability development priorities resulting from the CDP, and the development of European cooperation.

Member States' CARD Initial Information

The EDA will make extensive use of existing information sources – the Agency will first analyse information already available in EDA databases and Member States' replies to the EU Military Capability Questionnaire, or any other information Member States' are willing to provide to the EDA. A "Member State CARD Initial Information" document will be produced by the EDA and sent to each individual Member State. This will provide the basis for bilateral discussions in capitals during which members of the EDA CARD team will meet with the Member States' designated representatives to validate and supplement the information collected. A second, no less important part of the bilateral dialogue will focus on opportunities for cooperative capability development.

The CARD does not aim to assess or measure a Member State's performance according to pre-set metrics. What it will instead do is perform a forward-looking analysis with a view to identifying means of achieving its stated goals: greater cooperation and more consistency between national defence plans and commonly agreed European capability

development guidance while preserving Member States' sovereignty.

By presenting progress achieved within the European capability development landscape, the CARD should thus provide an opportunity to collectively review EU defence efforts in support of operational activities. Such contributions could include joint R&T, joint development or procurement, joint training, or common approaches to critical enablers. Member States' participation in multinational operations and large scale military exercises could also be considered in the context of this European defence review.

CARD aggregated analysis

As an outcome of the bilateral dialogues, consolidated information will be aggregated to produce a snapshot of the overall European situation. Through regular review cycles, the CARD's ambition is to capture the evolution of Member States' situations over time. This analysis will not seek to assess the performance of any individual states, but rather to present a realistic overview of European Defence by aggregating national and EU data and identify opportunities to strengthen capabilities through cooperation. Building on individual Member States' strengths, the intention is to project a potential way forward for the EU in terms of cooperative capability development in the defence domain.

The CARD report

The result of the CARD process will be a consolidated report to Ministers of Defence at the EDA Steering Board. It will provide Ministers with the basis for an open and frank discussion among peers on the review of European defence and to agree on ways to increase cooperation and harmonisation. Member State ownership of

the process combined with a sufficient level of political visibility should maximise the chances for real tangible results over time.

CARD: the right format at the right time

Many technical elements have been put in place over the past ten years through the EDA: a coordinated approach to identifying capability priorities, a mechanism for encouraging the pooling and sharing of capabilities, and ways of contributing to cooperative research and technology projects on specific capability elements and of preparing EU capability programs. What has been lacking is a high level coordination format with a specific forward-looking capability-oriented mandate, giving the Member States who finance and implement this political guidance through their national processes the central role.

This new format comes at a time when Europe is re-examining its defence role. The EUGS has recognised the need for strategic autonomy. Several other initiatives are in the works. The European Commission has launched the European Defence Action Plan. In parallel, Member States are looking to strengthen cooperation through Permanent Structured Cooperation (PESCO). The CARD constitutes the framework to ensure consistency between national defence plans and EU defence efforts, enriched by these new initiatives.

By looking at defence spending, cooperation amongst member states, and the implementation of agreed capability priorities, the CARD will seek, over time, to maximize the potential for combined efforts. With the right combination of Member States' engagement, the EDA's analytical capacity and the necessary political commitment to take EU defence cooperation to the next level, the CARD has the potential to be a real game changer. ■





➤ Strategic responses to strategic threats

For Estonia's first EU Presidency, the country's Ministry of Defence teamed up with the European Defence Agency (EDA) to host EU CYBRID 2017, the first ever European strategic cybersecurity table-top exercise.

Held in Tallinn on 7 September, the exercise brought together EU Defence Ministers, the High Representative of the Union for Foreign Affairs and Security Policy and Head of the EDA Federica Mogherini, senior representatives of the European Commission as well as the heads of cyber-related EU agencies.

CYBRID's main objectives were to raise cyber awareness at the highest political level and to practice strategic decision-making procedures to be followed in case of a cyber-attack against EU military structures. Reflecting the spirit of the new EU/NATO Joint Declaration, the exercise was also attended by NATO Secretary General, Jens Stoltenberg.

Cyber + hybrid = CYBRID

The exercise name in itself is a reminder of the fact that cyber and hybrid warfare have become a new threat cocktail that can

no longer be ignored by defence planners. Blending traditional military with non-military tools, hybrid strategies seek to incrementally undermine a system, destabilise a region or state and fuel conflicts. Another key feature of hybrid warfare is that attacks are very difficult to attribute with certainty to a certain state or group, in effect allowing attackers to remain incognito. At the same time, hybrid aggressions come in such small doses that it is difficult to categorise them as clear-cut armed attacks under international law. This, in turn, makes it harder for any victim country to use its legitimate right to self-defence.

Awareness at the top level

Cyber is nowadays widely acknowledged as a major threat to Europe's security and, subsequently, has its place in the EU's Common Security and Defence Policy (CSDP). Yet, crucial aspects such as CSDP missions and operations' resilience to

such threats have to date been given only limited attention. How far a third country's dubious cyber activities can be considered an indicator for active hybrid warfare also requires further reflection and debate. What is beyond doubt, however, is that aggressive cyber campaigns orchestrated by adversaries in combination with other hybrid actions (such as propaganda, fake news, use of proxies, etc.) can easily provoke massive disruption in whatever country, organisation or infrastructure targeted by such attacks, including CSDP missions and operations. Such crisis inevitably involves the full chain of command, up to the top military and political level. Hence the need to raise 'Cybrid' awareness at the highest level throughout Europe and to improve cyber defence incident coordination.

Political guidelines in case of cyber-attack

Against this backdrop, the goal of



Joint effort: HR/VP/Head of the EDA Federica Mogherini, EDA Chief Executive Jorge Domecq and Estonian Defence Minister Jüri Luik (from right to left) at the Tallinn meeting

"Blending traditional military with non military tools, hybrid strategies seek to incrementally undermine a system."

EU CYBRID 2017 was to practice strategic contingency procedures in a situation in which a cyberattack campaign was underway against the European Union's military structures. In other words: to test existing EU policy guidelines to be followed in case of such an event.

Ministers' discussions in particular focused on:

- **situational awareness** and the importance of reaching a common understanding and political assessment of a given crisis, as well as of the impact a cyber-attack and/or other subversive activities can have on EU military structures;
- **crisis response tools** available at EU-level to give strategic-political guidance on the response to give to a major offensive cyber-campaign against CSDP structures in a hybrid warfare context;

- **strategic communication** and the need to properly coordinate the information flow between EU Member States at the highest political-strategic level;
- **cybersecurity incident coordination mechanisms** at political level;
- the application of the '**Cyber Diplomacy Tool Box**' (based on first lessons learned from the crisis scenario studied at the Tallinn exercise) for responding to similar crises in future.

More technical aspects related to these topics have been and will be addressed in future follow-up exercises to be held at expert level. A first such exercise, EU PACE 2017, took place from 28 September to 4 October 2017.

Orchestrated cyber-attack

The practical exercise scenario discussed by ministers in Tallinn was based on an hypothetical orchestrated cyberattack

campaign against a fictive EU-led military operation in the maritime domain, which targeted both the mission's operational headquarters and its subordinated maritime assets.

Ministers, who were provided with incident information in real time, had only a limited amount of time to decide how to react. Other successive activities like third party orchestrated propaganda against the operation, the use of social media to organise a protest against the operation, the launch of fake news about the operation etc. left no doubt that the cyber-attack campaign was part of a wider hybrid strategy.

Multiple cyber-attack scenarios using a wide range of cyber tools were run through, combined with other incident scenarios. The exercise obviously referred to fictitious countries, organisations and operations but under conditions deemed as realistic as possible. ▀

> "We still have some work to do on cybersecurity"

Shortly after 'EU CYBRID', the strategic table-top cyber defence exercise jointly organised by the Estonian EU Presidency and the European Defence Agency (EDA) in Tallinn on 7 September, we sat down with Estonia's Minister of Defence, Jüri Luik, to discuss the importance of cyber defence and the main lessons learned from the CYBRID exercise. We also asked him about his views on the prospect of deeper European defence cooperation, the implementation of the latest EU initiatives in the defence field as well as on the EDA's future role.

Minister, since Estonia suffered a massive cyber-attack in 2007, the country has been driving and championing the cyber-security agenda in the EU and NATO. In your view: have the lessons been learned?

What happened in Estonia in 2007 was a wake-up call for many countries. Just as Estonia realized that there was a need for a national cyber-security strategy to face similar cyber-threats also in the future, many other countries followed. Within the EU and NATO now, most of the countries have their cyber security strategies, if not even second or third versions of these.

I would like to bring out two concrete lessons that Estonia identified: first, the importance of public-private cooperation. As Estonia's society has been heavily dependent on e-solutions and e-governance, these solutions are widely used by the private sector. This means that the 2007 attacks disturbed the activities of both government and the private sector. Managing these threats and attacks was thus in the interest of both sides. As a lesson learned, we then formalized this partnership.

The second identified lesson was about the nature of the attacks – while these were distributed denial of service attacks that we nowadays see on a daily basis, it was the first

time that there was a coordinated nation-wide attack that we were not prepared for. This showed that cyber-security clearly forms an integrated part of national security.

On 7 September, Estonia hosted the EU CYBRID table-top exercise, co-organised with the EDA. What are for you the most important take-aways of that exercise?

EU CYBRID 2017 was a strategic table-top exercise where the ministers played through a scenario about a cyber campaign against EU military structures. Our goal was to take the cyber-security issues to political level, to show that cyber is not merely a technical matter. Rather, cyber-attacks can easily lead to the political level where ministers need to make political decisions. The focus of the exercise was on situational awareness, crisis response and strategic communications. The exercise clearly showed the importance of how we comprehend what is going on, what measures are at our disposal to mitigate these kind of attacks and how we communicate these to the public. All of these points are strategic in their nature and thus very relevant to the ministers.

Another take-away from the exercise relates to EU-NATO cooperation. This was something that the NATO Secretary-General of NATO who observed the exercise, emphasized

as a matter of importance. EU-NATO cooperation is also a topic of general interest throughout the Estonian Presidency of the EU Council – we dedicated a seminar on 2-3 November on this partnership with a focus on cyber-matters.

Do the EU's efforts to counter cyber-threats and the revised Cyber Security Strategy give sufficient prominence to the defence dimension?

Defence matters are generally more thoroughly dealt with by NATO, also in the cyber dimension. As the EU CYBRID 2017 exercise showed, we still have some work to do in terms of cyber-security of EU military structures and missions. Let me make one more general observation – no matter what kind of policies we decide (including the revision of the EU Cyber Security Strategy), we need to implement them – to make sure that the agreed policies work in practice and that we all comprehend them in the same way.

What is Estonia's assessment of the renewed momentum of European defence cooperation since the publication of the EU Global Strategy in 2016?

There is indeed a political momentum in Europe to actively strengthen European defence



"There is political momentum to strengthen European defence cooperation. This is an opportunity we must use."

© Raul Mee EU2017EE

cooperation. This is an opportunity we must seize. European citizens want more security therefore we need to deliver concrete results

The European Union has taken significant steps to advance defence cooperation. We share the overall vision of a more militarily capable Europe based on more cooperation and more investment. The goals set in the Global Strategy are ambitious and we must be ambitious if we really want to take European defence forward. At the same time the ambition must remain realistic.

More specifically, what role does your country intend to play in the implementation of critical new European defence initiatives such as the European Defence Fund, CARD and PESCO?

We will continue to foster discussions on these topics to lead the ongoing work towards tangible results by the end of our Presidency. The overall aim is to create more capabilities and more political will to enable the EU and Member States to fulfil the ambitions set out in the Global Strategy.

We need to make full use of existing and new mechanisms – like PESCO and the European Defence Fund (EDF). Regarding the EDF, we are chairing the Friends of Presidency group working on the European Defence

Industrial Development Programme's (EDIDP) regulation and we plan to reach an agreement on the regulation by the end of this year. Estonia places particular importance on cross-border participation of Small and Medium Sized Enterprises as well as the need to focus on competitiveness and development of innovative capabilities. Regarding PESCO, we hosted a workshop in July and we will continue to support the discussions on commitments and governance. Estonia proposed adding a commitment about simplifying the movement of troops in Europe. This would advance the EU Battlegroups and serve as a practical example of EU-NATO cooperation. For us, it is important that capability projects developed in the PESCO format are also in coherence with NATO defence planning requirements and have 'regional added value'. Coherence with NATO planning processes is also important when we talk about CARD. The aim should be to use all the resources and data already made available by the member states. That would

avoid duplication and additional administrative burden for the member states. We are looking forward to the trial-run of CARD and hopefully it will produce the desired results.

How do you see the EU/NATO relationship evolve in the future and what is your assessment of the implementation of the Joint Declaration so far?

It is both natural and essential that the EU and NATO should work towards more coherence and complementarity in defence issues. Strengthening EU defence also means a stronger NATO as 22 EU Member States are also NATO member states. Therefore the projects and initiatives should take into account NATO's defence planning and already existing capability targets. We should seek cooperation in areas with very practical value, for instance in cyber as it is a transnational and trans-institutional issue. Organizing parallel and coordinated exercises such as the table-top exercise between the EU and NATO improves situational awareness and decision making. Simplifying military movement in Europe is another area for cooperation with tremendous potential both for the EU and NATO. Together with five countries, Estonia has proposed to start such a PESCO project.

The EDA's recent Long Term Review led to the Agency's reinforcement and a strengthened role as the central operator for EU funded defence activities. How do you see your country's role in the EDA evolving in the coming months and years, and how would Estonia like to see the EDA develop in the future?

The EDA is and will continue to be an important part of EU capability development. The Agency has valuable expertise and resources that can provide beneficial support to new capability initiatives. We should use all the tools available and if necessary adjust them to meet the current capability needs of the member states. The EDA has been appointed as the implementing agency for the Preparatory Action on Defence Research and it is a good opportunity for the Agency to show its competence and ability to lead such projects. ■

Jüri Luik is Estonia's Minister of Defence, having held this position twice before: from 1993 to 1994 and from 1999 to 2002. He also served as the country's Foreign Minister (1994-1995) as well as Ambassador to Moscow, NATO and Washington. Luik is a valued expert on defence and security policy. From 2015-2017, he was the Director of Estonia's International Centre for Defence and Security.

➤ Optimising Europe's Main Battle Tank Capabilities

In the light of current threat assessments and the evolving strategic situation in Europe and its wider neighbourhood, Main Battle Tank (MBT) capabilities have regained importance. While some EU Member States exhibit conspicuous and disconcerting MBT gaps, others possess large and costly overcapacities. Hence the European Defence Agency's (EDA) initiative to optimise existing MBT capabilities by Pooling & Sharing available assets for the benefit of all.

With their unique ability to provide a combination of mobility, firepower and protection, MBTs are crucial for defending European territory. Considering a currently tense security environment, especially along the Eastern European borders, it is of utmost strategic importance that Europeans have the required tank capacities to react swiftly and with the needed operational strength.

The number of MBTs in EU Member States has regularly decreased, from 15,000 in the year 2000 to just 5,000 today. Modernisation plans for existing main battle tank assets are limited, with no substantial increase of European MBT capabilities to be expected in the short or medium term. Traditionally, most EU countries use European or Soviet legacy equipment. Since the dependency on Soviet legacy technology raises a number of concerns it can be anticipated that next-generation MBTs should be more procured from sources that can guarantee security of supply in the longer term.

Against this backdrop, the EDA launched in spring 2017 the 'Optimisation of the Main Battle Tank Capability in Europe with initial focus on Leopard 2 (OMBT-Leo2)' project.

The initiative is an important pilot to test a new innovative Pooling & Sharing concept potentially applicable to other areas. The system works as follows: surplus 'Leopard' platforms available in certain Member States (the 'providers') are leased/rented for a defined period of time to one or several other interested Member States (the 'receivers'). At the end of the transfer period, the MBTs can either be returned to the providers (for further use or subsequent sale to third parties) or be sold to the receivers. The Pooling & Sharing of training, exercises and maintenance between providers and receivers, using already existing facilities complete the concept. This approach requires European

industrial partners to be involved in support of its implementation.

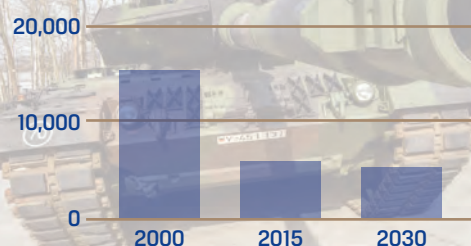
Technical upgrade

As a first step, an upgrade of all participating Leopard 2A4 platforms to the latest Leopard configuration (2A7) is foreseen as part of a comprehensive package including training and logistics support.





MBTs in the European Union, Switzerland, Norway and Serbia




Source: CODABA

© Klaus-Martin Wegmann

Receiving countries will nevertheless retain some degree of flexibility; the upgraded Leopard 2A7 they receive will be in line with the technical configuration developed by the Original Equipment Manufacturer and used by all Leopard Benutzerstaaten (LeoBEN) but not automatically equipped with all available features. This leaves the receivers with the choice of equipping their MBTs only with features they deem necessary (e.g. cooling, auxiliary power units, specific mission equipment, additional protection, etc.). The EDA project not only includes the Pooling & Sharing of the tanks themselves, but also of related services to make it a 'full capability' i.e. training and logistics support, including related special Leopard vehicles such as recovery vehicles, combat engineering vehicles or bridge layers.

The idea behind this coordinated and comprehensive upgrade to one single type of platform (Leopard 2A7) throughout all

participating Member States is to overcome the complexity caused by the high number of different types of fighting vehicles currently in operation, in anticipation of a future European generation of MBT.

 The number of MBTs in EU Member States has been steadily decreasing, from 15,000 in the year 2000 to just 5,000 today

Win-win situation

The benefits for all parties involved in this project are clear.

For the 'providers', the lease/rent and/or sale of excess MBTs not only generates revenue but also helps to substantially cut

down maintenance costs for spare assets and equipment. The 'receivers', on the other hand, get easy and rapid access to additional and modern tank capabilities, including the support and expertise (maintenance, training, industrial contacts, etc.). Finally, the 'upgraders' benefit from considerable economies of scale resulting, compared to the costs of individual, national MBT upgrade programmes. Furthermore, MBT capability can be obtained faster through this scheme than through normal acquisition processes.

Way ahead

In March 2017, the EDA's Steering Board in Capabilities Directors formation tasked the Agency with optimising Europe's Main Battle Tank capability and asked it to define the technical, logistics and training requirements as well as the contractual, financial, industrial and management schemes. A Request for Information (RFI) to European Defence Technological and Industrial Base (EDTIB) companies was launched at the end of September. The outcome of this RFI, expected by the end of 2017, will be analysed and processed by the EDA and its Member States in early 2018 with a view to determine the next step of this programme. 





➤ Cleared for take-off: ETAC opens in Zaragoza

8 June 2017 marked a significant day in the history of the European Defence Agency (EDA) with the opening of the European Tactical Airlift Centre (ETAC) in Zaragoza, Spain. The Head of the Agency, High Representative of the Union for Foreign Affairs and Security Policy Federica Mogherini and the EDA Chief Executive Jorge Domecq were welcomed by Dolores de Cospedal, Minister of Defence of Spain for the opening ceremony of Europe's first dedicated centre for tactical airlift.



The opening of ETAC marked the largest ever transfer of a project from the EDA to a host nation on a permanent basis. The project, the European Air Transport Fleet (EATF) Training Programme, was created by the EDA in 2011 and signed by 20 participating nations. EATF had a simple rationale: increase the EU's airlift capabilities by addressing shortages and increasing interoperability. Following six years under the guidance of the Agency, EATF saw 87 aircrews trained, 50 tactical instructor pilots graduate, and 94 European transport aircraft involved.

ETAC: The new home of European tactical airlift

The official transfer from the EDA to ETAC was marked by a flag handover ceremony between the EDA Chief Jorge Domecq and Colonel Jose Luis Romero, the ETAC Commander.

In his address, Mr Domecq commented: "This new centre is the culmination of 6 years of development in the EDA. ETAC demonstrates exactly how the EDA enables positive defence collaboration and delivers real capability

improvement for our Member States."

Visiting delegations also attended a tactical display, followed by the graduation of 4 aircrews from three Member States (Spain, Germany, Poland) of the latest edition of the European Advanced Airlift Tactics Training Course (EAATTC 17-3), and visited the EDA's innovative 3D-printing in defence project. The main ceremony was also addressed by HR/VP Federica Mogherini and Minister Dolores de Cospedal.

Following the establishment of ETAC, the 11 nations who are the owners of this agreement (Belgium, Bulgaria, Czech Republic, Germany, Spain, France, Italy, Luxembourg, The Netherlands, Portugal and Norway), will now share the burden to plan, organize and execute Advanced Airlift Courses, Training and Symposia in different locations (France, Italy, Bulgaria, Portugal & Sweden) by using the lean command and control structure based at Zaragoza.

ETAC will be manned by experts from the different participating nations on a rotational basis. The first composition will be made up from Spanish, Italian, German and French officers, who will be replaced within 3 to 4 years with staff from the remaining signatory nations. →



The EDA's 3D-printing lab successfully deployed

As described in this magazine's cover story (page 24), the EDA has launched in December 2016 the 'Additive Manufacturing (AM) Feasibility Study & Technology Demonstration' which aims to raise awareness and promote better understanding of AM's application and potential in different military contexts, and contribute to the timely and effective implementation of 3D-printing in defence specific areas.

In creating this ground-breaking project, the EDA contracted the research centre Fundación Prointec and MBDA France, to support a three work strand approach to AM. First of all, a desktop study was conducted which placed AM and its potential in a defence context. This first step summarised the cutting edge abilities of relevant technologies, identified existing R&T and manufacturing capabilities in Europe, and set out areas where further defence activities in different domains, such as R&T, logistics or training, should be carried out.

Test Deployment in Zaragoza

To truly test the feasibility of 3D-printing in defence, the EDA commissioned the construction of a fully deployable 3D-printing lab which was put to the test during the EDA's airlift training course (EAATC 17-3) in Zaragoza. State of the art AM printers and hardware were installed by Fundación Prointec in a customised container. Following its arrival in Zaragoza, the lab was loaded on board of a Spanish C-130 and successfully completed a 30 minute flight. This test was pivotal to examining the feasibility of the facility to be deployed by air to an operational military base.

After landing, the lab and its equipment were inspected and found to have encountered no issue from the airlift, being fully operational within just one hour.

During the subsequent deployment at EAATC 17-3, technicians presented the possibilities offered by AM and worked closely with officials to identify and produce a range of test parts which were then produced on site. The Head of the EDA, High Representative Federica Mogherini, and the Spanish Defence Minister, Dolores de Cospedal, visited the AM facility and were briefed by EDA staff.

Moving Forward

The final work strand of this project took place in Gijón, Spain in September, during an EDA exhibition on 'Exploring Additive Manufacturing impact in Defence capabilities'. Member States representatives were presented with the final conclusions of the project, including the equipment used and typical objects and materials produced during the deployment of the AM facility in Zaragoza.

The exhibition was an important step in raising awareness among the defence community about the capabilities AM technologies bring to the defence sector as well as their potential for different applications. The EDA's AM in defence project is a clear example of how cross-fertilization of ideas from different domains, stretching from R&T to operations, can enhance defence capabilities, especially when supporting deployed missions.

Small but meaningful

The print out of a miniature A400M aircraft produced in the EDA's 3D-printing lab deployed at the Agency's airlift training course EAATTC 17-3 in Zaragoza

(see related article on page 40)

Excellence at your side

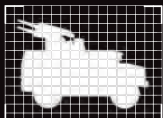
OUR COMMITMENT TO YOU

Armed forces face increasingly complex engagement scenarios where there is no room for error. In this demanding environment you can count on our expert teams who are committed to bringing you cutting edge, combat-proven technology and autonomy in defence.

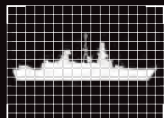
AIR
DOMINANCE



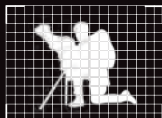
AIR
DEFENCE



MARITIME
SUPERIORITY



BATTLEFIELD
ENGAGEMENT



www.mbda-systems.com

