European Defence Matters

2015 **Issue 09** | A magazine of

EUROPEAN DEFENCE AGENCY

Cyber threats: are you ready?

Interview: Mauro Moretti, CEO of Finmeccanica & President of the AeroSpace and Defence Industries Association of Europe

Cyber defence In focus

Publishing Director
Eric Platteau

Editor-in-Chief
Anna Gałyga

Editorial
Elisabeth Schoeffmann

Design
Simon Smith Associates

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

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

Front cover image; © Thinkstock
Other images; EDA, Thinkstock, Shutterstock

Contacts

Eric Platteau
Head of Media and Communication

Anna Gałyga
Media and 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 within national governments, European institutions and industry in Europe.**

Published three times per 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 & Security challenges.

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

Cyril Mikaïloff
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-15-003-EN-C
ISSN (1977-5059)

Contents

Welcome

European Defence News

Cover Story: Cyber defence In focus

In the spotlight

Events

Operations

Opinion

Highlight

Annual Conference

Key Quotes

The views expressed in the articles are those of the authors and do not necessarily reflect the official position or policy of the EDA.

European cyberspace in focus

Acknowledged as the fifth dimension of a conflict – along with land, sea, air and space – cyber defence is gradually moving beyond the scope of the purely national domain establishing itself as an issue to be tackled at the EU level

Cyber defence remains an area with great potential for capability development. In line with the 2013 EU Cyber Security Strategy, EU efforts aim at the creation of an 'open, safe, and secure cyberspace.' Above all, these efforts focus on the fundamental rights of every European citizen: freedom, democracy, and openness. In cyberspace, however, these rights bear certain vulnerabilities. Personal data, industrial know-how and military technology are integral components of the realm; as a result, they are of high market value and prime targets for cyber crimes.

Threats of this kind are of ongoing concern for governments, military organisations, civilian organisations and enterprises, as well as for individuals. The application of proper protection measures, therefore, requires the implementation of a holistic approach, with every stakeholder invited to come on board.

European Defence Matters will take a closer look at the nature of cyber threats and examine how the dual-use concept and PPPs work for cyber defence, in practice. It will also address the current condition of the European security and defence market, with a special focus placed on Small and Medium Sized Enterprises (SMEs). Subject matter experts from the European Defence Agency will discuss technology and skills, as two complementary elements of cyber defence capabilities, proving that defence starts with awareness and knowledge acquisition. At this point, multinational defence cooperation is also brought into the discussion, along with the Pooling & Sharing of know-how and technologies, as there is no way to tackle cyber threats other than through combining efforts.

The European Defence Agency is the right platform from which to launch such collaboration, allowing as it does for the different national capabilities of the respective Member States to meet halfway, at the EU level. When it comes to cyber defence, boosting the ability of Member States to counter cyber threats remains the Agency's ultimate goal. Naturally, the importance of close cooperation with other EU bodies, NATO, academia and other stakeholders cannot be underestimated. Cyberspace is a shared and vitally important realm, the protection of which must not be left to chance.

Discussions on cyber defence and other areas of capability development are still resounding after this year's European Defence Agency's Annual Conference. *European Defence Matters* will deliver an insight into key themes raised during the conference, as well as with an in-depth assessment of the European defence and security market by Mauro Moretti, Head of Finmeccanica and ASD.

Eric Platteau Head of Media and Communication **Anna Gałyga** Editor-in-Chief

News

Energy security as a defence capability

Under the framework of the European Defence Agency's (EDA) Energy & Environment programme, the European Commission and the EDA launched a Consultation Forum for Sustainable Energy in the Defence and Security Sector.

The Consultation Forum brings together European experts from the energy and defence sectors to support the European Commission's energy efficiency and renewable policies. The forum will examine how energy efficiency measures and renewable energy sources might be better implemented within the European defence sector, allowing the sector to be more competitive and efficient.

The Consultation Forum is divided into three working groups. The first examines the management and behavioural aspects of energy efficiency. The second primarily tackles energy efficiency in relation to infrastructure, but also in relation to the wider defence context and – at the request of Member States – in deployed camps within Europe and EU operations, as well as other military platforms. The third addresses the use and production of renewable energy sources.

The first plenary session of the Consultation Forum for Sustainable Energy in the Defence and Security Sector will take place in Brussels on 14-15 January 2016.

Franco-British partnership on missiles extended

© UK MoD

The French and British governments extended the funding of the Materials & Components for Missiles Innovation Technology Partnership (MCM ITP) up until 2018. This funding provides for a further 21 projects and offers new organisations the opportunity to propose new projects for the programme, due to start in September 2016. A total of 121 organisations are involved in the programme, including a strong representation of Small and Medium Sized Enterprises (SMEs) and academia.

The aim of MCM ITP is to consolidate the UK-French complex weapons capability, strengthen the technological base, and allow for a better understanding of common future needs. The programme manages a portfolio of over 121 cutting-edge technologies, all of which have the potential to facilitate major advances, but which currently remain at the laboratory stage. Once validated, the technologies can become part of future demonstrators of missiles, equipment or missile systems.

The programme covers all domains relevant to missile development, including systems, infrared and radar sensors, solid propulsion, air-breathing propulsion, warheads, safety and arming units and fuzes, materials and electronics. It manages an annual budget of up to €12.5 million, combining government and industry funding, with 30% of the budget targeting SMEs and academia.

France and the UK have also signed a new Intergovernmental Agreement, allowing for sharing technologies to support the development of future generations of missiles managed by missile contractor MBDA. In particular, the agreement refers to the helicopter-launched anti-ship weapon, Sea Venom, and other future national and joint programmes to meet British and French military requirements over the course of the next decade and beyond.

Italian Reapers will be armed

Italy has become the second country after the UK to be approved by the US State Department to arm its General Atomics MQ-9 Reaper unmanned aerial vehicles (UAVs). The $129.6 million deal, with General Atomics acting as prime contractor, will involve the purchase of 156 AGM-114R2 Hellfire II missiles, 20 GBU-12 laser-guided bombs, 30 GBU-38 Joint Direct Attack Munitions and other armaments.

After first flying Predators in 2004, Italy built up a fleet of six upgraded Predator A's, known as A+, and six Reapers, which are operated by the 28th squadron. In the last decade, the Italian fleet has also been used in Iraq, Afghanistan, the Balkans and Africa. Italy currently contributes a Predator and a Reaper to assist the European Union Naval Force (EU NAVFOR) Mediterranean operation, set up this year to stop human smuggling and trafficking across the Mediterranean.

News continued

© MoD Czech Republic

© Jan Kouba, MoD Czech Republic

Czechs opting for modernisation and new weapons

The Czech Ministry of Defence announced the purchase of new weapons and the modernisation of its existing gear, primarily designed for Czech land forces, air forces and reserve units.

The purchase will comprise, among other things: 57 wheeled vehicles supplied by Italy's Iveco and Czech manufacturer Tatra, 26,000 assault rifles CZ 805 Bren, and 800 grenade launchers CZ 805 G1. The Czech army plans to modernise five vehicles LOS (Light Observation System) and reconnaissance and observation sets Sněžka, mounted on the chassis of the 2x7-wheel armoured amphibious tracked infantry fighting vehicle BVP-1.

The aim of the procurements is to increase the capabilities of the Czech armed forces, in order to secure the country's border in the context of the deteriorating global security situation, and to ensure the Czech military is prepared to participate in joint activities.

The acquisitions are enabled by the country's higher defence budget for 2015. This year, Prague plans to spend 43.78 billion krona (US $1.78 billion) on the military, a 4.2% increase over the previous year, according to figures from the Defence Ministry. The Czech Republic is planning a gradual increase of defence spending, rising to 1.4% of its Gross Domestic Product by 2020.

Additionally, the Czech Republic is planning to purchase the RBS-70 NG short-range surface-to-air missile (SAM) system from Saab, potentially making the country the first operator of the system. The aim is to replace the ageing Strela 10-M Russian weapons with the latest generation of RBS-70. The programme will last until 2025, with the first stage taking place from 2017 – 2020.

Earlier this year, the Czech Republic decided to start the procedure of replacing its Mi-8, Mi-24V/35 and Mi-17/171 helicopters with new multirole helicopters.

Alongside the modernisation and development of its existing gear, the Czech Republic is expected to increase its number of troops from 16,600 to 24,000 by 2025.

Saab's intent to modernise the Polish Navy

© MoD Poland

Saab has signed a Letter of Intent with Gdynia-based Naval Shipyard S.A. with the aim of increasing cooperation and contributing to the naval modernisation programme of the Polish Navy.

The agreement specifically focuses on strengthening Saab's standing within the Polish Ministry of National Defence's planned Orka submarine programme. The Orka submarine programme is a modernisation project that includes the construction of several new classes of ship, as well as plans for the Polish Navy to obtain three submarines and new cruise missiles. They will replace four Kobben-class boats and the single Project 877E submarine ORP Orzel. Deliveries of two submarines are scheduled to be completed by 2022, and a third one will be acquired by 2023.

The Orka submarine has been identified as a key focus for the Saab Kockums submarine business, bidding its new-generation A 26 design with the full backing of Sweden's Defence Materiel Administration.

Saab is not new to the Polish naval market. It has previously supplied RBS15 Mk 3 surface-to-surface missiles and Sea Giraffe AMB radars for the upgrade of the Polish Navy's three Orkan-class fast attack craft. In addition, the company's Double Eagle mine disposal vehicle has been selected for the navy's new Kormoran II minehunter programme.

News continued

© Wouter Engler

The Netherland's Presidency 2016: EU capabilities in focus

Holding the Presidency of the EU Council gives each Member State a valuable opportunity to draw the Union's attention to matters they deem to be of particular importance. On 1 January 2016, the Netherlands will take over the Presidency from Luxembourg, assuming the task of directing the Council's efforts for the subsequent six months.

The Netherlands has outlined its priorities in the defence field, focusing on a stronger Common Security and Defence Policy, deepened defence cooperation, and parliamentary involvement. The Dutch Presidency is set to coincide with the announcement of the new EU Global Strategy on Foreign and Security Policy, due to be made in June 2016 by Federica Mogherini, the High Representative for Foreign Affairs and Security Policy.

This global strategy will serve as a blueprint for the development of instruments and military capabilities to match the political ambitions of the EU. "We expect to see a clear, realistic level of ambition for the Common Security and Defence Policy, along with a description of the way ahead for the next ten years or so, particularly on the military side," says Jean Pierre Van Aubel, Head of Task Force Netherlands EU Presidency 2016. However, the Netherlands is very much interested in going one step further and translating strategic concepts into concrete tools closely linked to capabilities. For this reason, along with preparations for the strategy, discussions will be encouraged on the implementation and operationalisation of the strategy.

Close partnership among the European countries in the defence area, the second goal for the Dutch Presidency, is a prerequisite for the development of necessary defence capabilities and tools. In this regard, the Netherlands will advocate strengthening defence cooperation, stimulating commitment and increasing the responsibility of Member States. "We would like to promote 'peer pressure'. Even though you cannot oblige anybody to cooperate, by setting good examples of defence cooperation, we do hope others will follow," explains Van Aubel.

Another element of the Netherlands' programme will be to put capability development higher on the agenda of the Defence Ministers meetings. The Capability Development Plan, and the sixteen focal areas defined therein, should be at the forefront of the debate.

In terms of capability development, the Dutch Presidency underlines a substantial role for the European Defence Agency in stimulating Member States and groups of Member States to cooperate with each other. When it comes to projects, "the Netherlands will support projects directly addressing shortfalls in capabilities, however, the ongoing projects agreed upon by the EU Council in 2013 and 2015 deserve our utmost attention," stresses Van Aubel. These include air-to-air refuelling (with the Netherlands leading the multi-role tanker transport fleet), satellite communications, cyber defence and Remotely Piloted Aircraft Systems.

Finally, to facilitate European defence cooperation, to muster political will to deploy Common Security and Defence Policy missions, and to provide the European defence cooperation and Common Security and Defence Policy with legitimacy, the Dutch Presidency will work towards more effective and faster decision making by national parliaments.

In order to fulfil all the objectives, the Netherlands has scheduled an informal meeting of Defence Ministers, a Defence Policy Directors meeting, and five seminars. Two of the seminars will be co-organised by the Dutch Ministry of Defence and the European Defence Agency, and devoted to the Research & Technology domain (25-26 April 2016) and to capabilities used for deployment (21-22 June 2016). The other three will also be closely linked to the Netherlands' priorities: "A stronger CSDP: Deepening Defence Cooperation" (20-21 January 2016), "The Parliamentary Dimension of Defence Cooperation" (14-15 March 2016) and "A New Strategy – Implications for CSDP" (10 June 2015).

European secure cyberspace: our common realm

In the following pages, *European Defence Matters* reports on continually rising cyber threats and European collaborative efforts to tackle them.

It presents the European Defence Agency's approach to address technological advancement and innovation, to educate about cyber risks, and to improve cyber defence skills and capabilities.

It reports on research and training opportunities in cyber defence in the NATO context, as well as EU-NATO complementarity in facing cyber threats.

It outlines the benefits of dual-use solutions for cyber defence capabilities, the landscape of the European industry and the need to strive for a harmonised European security market and industrial security of supply.

Index

Bricks to build a cyber shield

In today's world, the cyber dimension is an inescapable, ever-present reality. It is crucial, therefore, to identify both the advantages and risks associated with operating in cyberspace. Our subject matter expert explains why cyber defence is vital and how the European Defence Agency is pushing cyber security forward

Within the Information Superiority Unit, a lot of work is devoted to cyberspace and cyber defence. But how would you define cyberspace and its defence aspect?

Cyberspace is a virtual space built from information and not limited by time or location. It is limited only by hardware and software. If we take the topic of quantum computing, for example, there is a sense of almost endless power, without any boundaries at all. Cyber defence, on the other hand, provides a security service for the information. Here at the Unit, we deal with the creation of information, its collection, transmission, communication and management. It is also necessary, therefore, to add a security feature to the information, in order to protect it. I think it is important to see that cyber defence does not work on its own.

And why has everybody 'gone so cyber'?

Cyberspace as the fifth dimension of a conflict is critical. We could even call it a dangerous asset, since weapon systems and platforms rely heavily on information that generates power but also bears certain vulnerabilities. This is on the military side. And, in general, a citizen cannot escape a single one of their so-called 'cyber footprints', so there is an increasing awareness and concern for cyber security and privacy.

How can cyber defence be tackled from a strategic point of view?

Cyberspace is much more than defence; it is a typical dual-use issue and the ambiguity of cyberspace today requires that responsibility for shaping future cyberspace is shared among governments and administration, industry and academia. This is very well reflected in the EU Cyber Security Strategy.

For us, the defence people, who cope with cyber threats, the dual-use concept makes us feel that we are not alone: our challenges are more or less mirrored in the civil world. Even a civil nuclear plant may be considered to be a dangerous asset and it has to be protected. This opens up a possibility: to share the effort of meeting the challenges. Obviously, smart clustering allows us to make the best use of what the industrial landscape has to offer, but on the other hand, some smart regulations are required to avoid counter-productivity.

The good thing is that we have all the necessary bricks to build, most of the players involved, a technological way forward and a very important EU instrument ahead of us: the Preparatory Action. Cyber defence has already gained initial support from the Member States and it should be taken under the umbrella of the future EU budget.

> "Privacy is not only about a citizen but also about protection of know-how. The same requirements for protecting citizens' privacy are valid for protecting industrial knowledge"

What is the EDA's role in the building of cyber defence in the European context?

Our aim is not to develop strictly EU capabilities on cyber defence. The Agency is like a transmission mechanism, leveraging inhomogeneous national capabilities in order to make them accessible to all Member States. The EDA initiated a stocktaking study in 2011, which displayed the maturity of single Member State capabilities regarding cyber defence. Now, we are coming back to that study to examine what has changed. The overall idea is to establish a minimum standard for the Member States to confront their position themselves, and also to guarantee Common Security and Defence Policy operations run smoothly.

In the category of developing cyber work strands of structured thinking and acting, I think the Agency is very mature. We may play a leading role in pushing forward cyber security, but, at the end of the day, we are more the brain, or the think-tank, and we need to rely on external resources from our Member States, as well as from industry and academia.

A very good example of the targeted use of military funds is the Advanced Persistent Threats detection, which aims at countering cyberespionage. Civil products achieve 80% malware detection at best, which is not acceptable from our perspective. Thus, we launched research and a consortium will deliver a demonstrator later this year.

What are the focus areas for the EDA regarding cyber defence?

One may distil two big areas that are being dealt with: technology and skills.

Michael Sieber has been working for the European Defence Agency (EDA) since 2010. As the Head of the Information Superiority Unit within the Capability Armament & Technology Directorate, he is in charge of running the EDA's activities in cyber defence. In the interview, he talks about the lack of boundaries for cyberspace, civil-military mirror and 99 cyber projects to come

Technology is much about overcoming archaic architecture, achieving "a bandwidth to the last village", so to speak. In this regard, the EDA has taken up the challenge.

Following the Cyber Defence Research Agenda, 99 projects to improve cyber defence capabilities have been proposed for the upcoming four years. This is a lot. They are now being examined and prioritised by the Member States because, obviously, we will not be able to accomplish them all. Nevertheless, topics will touch upon areas, such as cryptology, protection of military systems and Advanced Persistent Threats detection. Considering what we have started working on in the Agency with the Member States permission, I think we are well on track.

When it comes to security and privacy – two important concerns in the technological domain – the EDA has been turning towards cryptology (or 'crypto'). This is a very sensitive notion in the national context. Looking to the future, given that the Internet of Things has already been introduced to the military world, the classical crypto axis used to protect communication channels is not sufficient: more innovation in the crypto world is required. In the interests of security of supply and European strategic non-dependence, the EDA has already recognised that shaping a crypto strategy will be necessary at some point. Consequently, a crypto landscaping study was launched to gather information for future discussions among the Member States.

Another issue is protection of military systems and platforms, the so-called 'embedded systems.' These electronic devices, which are the driving force for weapon systems, rely on information flow. They used to be detached from networks, as in the case of tanks, for example, but this is changing. We have to step out of our comfort zones – simply leaving an airgap is no longer any guarantee of safety. With a rapid advancement of autonomous systems, there is an ever-increasing need to protect our weapon systems.

"It is important to see that cyber defence does not work on its own"

Other EDA initiatives, such as a project on Cyber Ranges or deployable Cyber Situational Awareness Packages (CySAP) for headquarters, lead us to the second overarching focus area for the EDA: skills development. Even the most advanced technological solutions are worth little without properly trained staff. Following this path, we conducted a training needs analysis, developed a couple of curricula and initiated a series of training and exercises to address decision-makers, their support staff and experts. This also includes our 'on the spot' training offered to the military staff of Common Security and Defence Policy operations.

To sum up, technology and skills are considered to be the key to improving cyber defence capabilities across the Member States. The EDA has been doing its best to contribute to their development, acting as a launchpad for projects and initiatives. In so doing, it is helping to build, brick by brick, a shield capable of protecting against future cyber threats.

The European Defence Agency contributes to strengthening EU cyber defence

The EU strives for increased cyber defence capabilities and a trained cyber workforce. ***Wolfgang Röhrig***, who has been a project officer on cyber defence at the European Defence Agency since early 2014, explains how research, technology advancement and collaborative training lead to capability development and an increased awareness of cyber threats

The EU Member States that participate in the European Defence Agency (EDA) identified cyber defence as an area for consideration in 2011. Since then, the Agency has been addressing cyber threats in a way that is varied and comprehensive, while also well-structured and systematic. Taking a two-pronged approach, one area of focus has been on increasing awareness, educating people about cyber risks, and improving cyber defence skills in order to improve responsiveness to and resilience against attacks. The EDA also focused on technological aspects. To achieve all of this, the EDA has been implementing a multifaceted strategy and performing actions in various cyber domains.

> "Nowadays, we are living in cyberspace in the condition of 'insecurity by design'. We have to acknowledge that a fully safe and secure Europe is a utopia. But we can do a lot to make it safer"

Concepts

A reference point and a driving force for the majority of the EDA's initiatives was a landscaping study launched in 2011, performed by Rand Europe and the Foundation pour la Recherche Stratégique (Paris). Its aim was to assess the level of cyber defence capabilities of the Member States and EU institutions. Using complex threat assessment methodology, defence capabilities were analysed against eight lines of development: Doctrine, Organisation, Training, Material, Leadership, Facilities and Interoperability (DOTMLPF-I). Concurrently, a five-step maturity model created along those lines of development allowed a detailed picture to be created of the 'Cyber Defence Readiness' of all the analysed entities.

In parallel, the EDA work went in two broad directions. The first was built around shaping a cyber defence architecture for the EU-led Common Security and Defence Policy operations, and the second addressed shortages in education, training and exercises in military cyber defence.

The Agency's efforts were closely correlated with EU conceptual work, leading to the creation of the Cyber Security Strategy of 2013. It was the first ever joint publication of the EU Commission and EU External Action Service, supplemented by EDA contributions. The strategy comprehensively addressed EU responsibilities and listed key priorities: cyber defence in the framework of the Common Security and Defence Policy; the need for an EU cyber defence policy framework; the improvement of cyber defence capabilities in the Member States; civil-military synergies; and cooperation with relevant stakeholders, even beyond EU boundaries. As a follow-on to the Strategy, the European Council adopted a 'Cyber Defence Policy Framework' in 2014.

Strong advocacy for cyber defence has placed it as one of four topics for the next Preparatory Action within the EU Commission framework. This, along with the active involvement of the EU Structural & Investment Funds in the dual-use domain, brings the prospect of additional and adequate funding of future cyber projects to the table.

The Capability Development Plan (CDP), the EDA's key document outlining the way ahead in terms of capability development, naturally encompasses cyber defence. The most recent edition, published in 2014, draws attention to building a cyber defence military workforce and the availability of proactive and reactive technologies.

Additionally, the EDA plans to launch a Joint Investment Programme (JIP) to enable flexible management of ad hoc projects financed by the involved

Member States, projects fully covered by an EDA operational budget and capability development projects. The proposed five pillars of the JIP are as follows: building a skilled military cyber workforce, improving cyber situational awareness, ensuring proactive and reactive capabilities and enabling cyber defence.

Practical applications

With regard to creating a step-by-step roadmap to capability improvement, the Cyber Defence Research Agenda has turned out to be an especially useful tool. The way ahead for the next ten years in the Research & Technology domain was identified along ten research lines. Important variables encompassing threats and vulnerabilities, civil-military synergies (dual-use) as well as cooperation with civilian communities (national and EU institutions) and NATO. An outcome of the research was 99 project proposals addressing various capability shortfalls, all of which were presented to the Member States for closer analysis and prioritisation.

A blueprint for mitigating human risk in organisations is provided by the cyber hygiene initiative introduced by Estonia and Latvia under the Latvian Council Presidency. The document was signed by Austria, Estonia, Finland, Latvia, Lithuania, the Netherlands and the High Representative of the Union for Foreign Affairs and Security Policy/Head of Agency on behalf of the European External Action Service, EU Military Staff and the European Defence Agency in May 2015. The initiative aims to establish internal public sector guidelines for best practice behaviour against cyber threats by the end of 2016. This includes, for example, mandatory successful attendance of e-learning courses hosted on a common e-learning platform. The initiative also contributes to the EU Cyber Defence Policy Framework by raising awareness of the Common Security and Defence Policy structures, missions and operations.

Among a number of other EDA activities, it is important to underline research into the human factor impact on cyber defence as well as identification of areas for the military to explore and improve within the Research & Technology domain. The latter initiative led to the first cyber defence technology flagship project on Advanced Persistent Threats (APT) detection.

"What makes a cyber capability? People, technology and processes. The Agency, following its mandate, addresses two of them: people and technology"

Advanced Persistent Threat (APT) detection is a counter measure that aims at early and efficient detection of sophisticated malware, which uses one or a sample of 'zero-day' exploits (a vulnerability left undisclosed until released to the public, giving 'zero' days for correction), in information systems. As the current level of market available intrusion detection products is not high enough, such malware continues to pose a serious threat to operations, industry and politics.

Strategic Decision Making Course & Exercise on Cyber Crisis Management, Vienna, September 2015

Privacy protection has been identified as another area for development, viewed from a national security perspective but balanced with personal and industrial requirements. The EDA's focus was placed on cryptology. Since academia in Europe has already built up and networked extraordinary skills in cryptology over the past years, the EDA's intent has been to transfer this academic expertise into innovative and market-competitive products, which the military can also use. The consultations started under the umbrella of the European Framework Cooperation.

> "With our 'training needs analysis', we have set standards for skills development. It has successfully been used by both EU and NATO communities as a reference"

In the field of multinational cooperation beyond EU boundaries, the EDA – together with the EU Military Staff – is actively contributing to the cyber defence focus area of the US-led Multinational Capability Development campaign. In the spirit of Pooling & Sharing of cyber defence knowledge and expertise, they work to collectively develop solutions to common challenges.

Training as the gate to capability

It has become evident that even though there is no need to make everybody a cyber expert, there is a necessity to increase awareness of cyber threats, their implications and impact on traditional military functions and the procedures to be applied if a compromise has been detected. The EDA conducted an elaborate 'training needs analysis' to formulate a training & exercise concept. Consequently, a set of curricula for training & exercises was developed to address different audiences, and their varied expectations and needs. At all times and where applicable, dual-use solutions have been promoted in order to maximise the training results, and also to underline civilian-military synergies.

In general, four broad groups profit from training & exercises programmes: basic users, cyber defence experts, senior decision-makers and their supporting staff. However, strategic senior decision-makers and their supporting staff were recognised as the main target audience, for which the current training landscape is offering almost no courses or exercises customised to their specific requirements. Especially for them, the EDA developed and conducted three exercises: in Portugal (May 2014), the Czech Republic (June 2015) and Austria (September 2015). The overall idea of the series is to offer training in making decisions from a governmental perspective when confronted with the complex nature of cyberspace, as well as the different dimensions to which a cyber crisis may evolve.

> "With defining military cyber defence as the military dimension of cyber security, we enabled the breakdown of traditional barriers of naturally stove piped thinking"

Exercises at technical experts' level are yet another proof of how necessary it is to rely on existing solutions and infrastructure within the civilian sector whilst only selected and critical military gaps can be addressed directly using military solutions. Accordingly, a pilot course was held within the Pooling & Sharing scheme. Such training events, in general, are expected to seal a cyber defence community. Beyond sharing knowledge and expertise, effective cooperation is also about building trust.

The establishment of the Cyber Ranges is another effective implementation of the Pooling & Sharing concept in order to maximise the availability of assets. The ranges are multi-purpose environments supporting three primary processes: knowledge development, assurance and dissemination. Accordingly they may consist of three complementary functionality packages: Cyber Training & Exercise Range, Cyber Research Range as well as Cyber Simulation & Test Range functionalities.

To meet growing expectations on developing and maintaining cyber situation awareness, the EDA initiated deployable Cyber Situation Awareness Packages (CySAP) for headquarters, an ad hoc project to provide a common and standardised cyber defence planning and management platform to assist decision-makers while on missions.

Moreover, the EDA offers direct support to Common Security and Defence Policy operations by increasing cyber defence awareness as well as integrating cyber defence into the military planning and execution of operations. In 2014, for the first time, the EDA conducted a course for the staff of the EU military operation in the Central African Republic (EUFOR RCA) at the operation's headquarters in Larissa, Greece. A similar course has been offered to the operation's headquarters staff of the newest EU mission, the EU military operation in the south-central Mediterranean (EUNAVFOR MED).

The cyber future

Each year the European Network and Information Security Agency reports on current and emerging cyber threats and recent technological developments. To address the changing environment, the Agency has completed or initiated cyber defence related projects with a financial volume of approximately two and a half million euros over the last four years. Out of this budget, about €650,000 were spent on foundational work, about one million euros on Research & Technology and, finally, about €850,000 on training & exercise related projects. Overall, this amounts to approximately 10% of the EDA's operational budget, and proves how high cyber defence stands on the EDA's agenda.

The truth is that there is no turning back to the 'good, old analogue times.' Neither is there any reason to yearn for these times, however. Whilst it is all too easy to allow a virtual threat to limit our ambitions or, worse, be used against us, the Agency's work is moving defence to greater internal awareness of the cyber reality, from which we can manage risks and limit effect.

European companies to confront cyber challenges

Three questions to ***Christian Fredrikson,*** the President & Chief Executive of the F-Secure Corporation since 2012. He is a member of the Steering Board of the European Cloud Partnership bringing together the public sector and industry in order to establish a Digital Single Market for cloud computing in Europe. Previously, he worked for Nokia Siemens Networks

1. What are currently the main challenges faced by the cyber security industry?

There is a strong growth rate in high-profile cyber crimes and security companies face significant challenges to combat them. The incidents that garner the most attention are the compromises involving nation states and organised crime. The number of attacks by organised crime rings appears to be at an all-time high, and the level of organisational infrastructure used by these crime rings is unprecedented.

In the current technological environment, there are growing avenues for cyber crimes against infrastructure within societies and organisations. Cyber security providers have become legitimate targets as well. Regulators around the world are beginning to proactively address cyber risks and provide shelter for all businesses. Nations, businesses and societies in general are becoming increasingly concerned about the potential impact on data privacy and security.

2. What is the way ahead for Small and Medium Sized Enterprises (SMEs) in the cyber innovation domain?

Cyber security is a growing market. There is strong demand for both highly specialised products and services, and the ability to provide complete solutions that cater to specific customers' needs.

SMEs are typically better adjusted to focusing on solutions that require high levels of specialisation and exceptional professional skills. The obvious challenge in this approach is their dependence on key individuals, which puts a heavy burden on recruitment and talent management. SMEs may not consider themselves as being a target but they may have something the attacker wants or they can be a way for the attacker to get into something else. The core for proper protection is end-point protection and a holistic approach to security, along with vulnerability assessment, threat/intrusion prevention and incident response services.

Successful SMEs have also been able to leverage cloudification in terms of providing their services in a scalable fashion. Businesses taking this approach should immediately realise that the market is global from day one.

3. What are the consequences of cyber attacks on corporate institutions?

The most immediate threat involves data loss. It can be either in the form of stolen sensitive data or ransomware malware that effectively denies an organisation access to its own data and computing resources. Financial loss and brand reputation damage are the biggest threats deriving from data loss. In severe cases, attacks against cyber infrastructure may even threaten the foundations of a chosen business model.

© F-Secure

F-Secure is a Europe-based enterprise active in the market for more than 25 years. Founded in 1988 in Helsinki, it currently employs more than 900 employees and operates 25 regional offices around the globe, offering services to tens of millions of users. F-Secure develops and provides security software to protect individuals, companies and corporations against crimeware and cyber attacks. The service addresses cyber security holistically, also covering areas of risk, threat & vulnerability assessment, exposure analysis and intelligence, compliance management, incident response, forensics & breach analysis as well as security consulting.

NATO Centre of Excellence on cyber competences

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) located in Tallinn, Estonia, serves as an add-on to cyber competences built by NATO. As a think tank and training centre, it is another relevant stakeholder to emphasise when describing a European cyber defence community

The Tallinn Centre of Excellence

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was founded in 2008 in the aftermath of cyber attacks on Estonian public institutions in 2007. Estonia had in fact taken a closer look at cyber defence much earlier, but the 2007 events proved the relevance of the concept and speeded up the process.

There are already 21 NATO centres of excellence devoted to various operational areas, and there is a certain peculiarity in how they function. They are all founded and funded by participating Member States – not directly by NATO. Naturally, however, all centres serve both the nations and NATO. "This way we gain intellectual and academic freedom to focus on issues we and indeed our nations believe are important," explains Liisa Past, the CCDCOE Spokesperson.

As many as 18 nations are currently contributing to the NATO Cooperative Cyber Defence Centre of Excellence (as of November 2015): the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the UK and US, and Austria as a non-NATO member. This makes the Tallinn Centre of Excellence the biggest of its kind in terms of participating states.

The role of the Centre is to enhance capability, cooperation and information sharing among NATO, its member nations and partners in cyber defence, by virtue of education, research and development, lessons learned and consultation. "We are the researchers and educators dealing with applied research lessons learned, training and exercises," summarises Past. She also underlines the interdisciplinary approach adopted by the Centre in its work: "You can see people from different backgrounds working together, analysing projects from technological, legal and strategic perspectives at the same time".

Within the cyber community

Secure cyberspace is a common goal for both the EU and NATO. A key issue here is mutual complementarity, in order to counter cyber threats in a comprehensive and effective way. "Given the different purpose of the two organisations, it needs to be seen that the mandates of the two institutions vis-a-vis cyberspace and how to make it secure, are somewhat different," says Siim Alatalu, the International Relations Adviser at the CCDCOE. "Whilst NATO Allies have agreed that NATO's task in cyberspace is to guard its own networks, the role of the EU, quite like in other areas, is to inter alia set general standards for its members to follow – as set forth by the EU's Cyber Security Strategy from early 2013 and the Network and Information Security Directive that stems from it." He adds that, "NATO, despite being only a defence organisation, seems to have come a longer way in forging the Allied consensus, whilst the EU in the long run can have a bigger impact on its Member States' actual cyber posture." According to Alatalu, within this context, complementarity is a good solution.

In the wider context, CCDCOE maintains close ties to all its Member States' governments, industry and the academic world. "In cyber all these three domains are linked by necessity, interest and also the will to cooperate," says Alatalu. "It is important to recognise that we are not an operational institution and, therefore, we do not perform, for example, any cyber defence or offence operations on our own, neither with the involvement of other parties from the aforementioned sectors. We have a clear mandate. Our member nations ask us to do research and training on areas they deem relevant on an annual basis. Given our multinational staff, in most cases we have multinational teams to fulfil these requests."

CCDCOE as a competence enabler

There are a number of ways the CCDCOE addresses the international community's needs in research, training and capability improvement in cyber defence. The flagship projects encompass an elaborate research base, the Locked Shields series of cyber defence exercises, the Tallinn Manual on

Locked Shields, an annual exercise organised by the CCDCOE

© All images CCDCOE

Siim Alatalu has been Head of International Relations at the CCDCOE since January 2015; he previously held several positions at the Estonian Ministry of Defence and the Estonian Delegation to NATO. A graduate of the Maxwell School of Syracuse University, Baltic Defence College and University of Tartu.

Liisa Past is an adviser and spokesperson of the CCDCOE. She has worked as a trainer and consultant in strategic communication and public relations for numerous companies and organisations. She is a human rights' activist. A graduate of Columbia University, University of Oslo and University of Tartu.

international law and an annual conference on cyber conflicts – Cycon.

Following an interdisciplinary approach, the Centre serves as a think tank for NATO and its Member States to deliver applied research. A diverse group of international experts includes legal scholars, policy and strategy experts and technology researchers. They respond to queries in the cyber domain issued by the Member States, NATO and initiated by the Centre on its own.

The Tallinn Centre of Excellence organises the largest technical cyber defence exercise in the world, Locked Shields. Conducted on an annual basis, it is a real-time network defence exercise. "We build separate virtual networks that look realistically like national or corporate networks, which the teams have to defend during the exercise," Past explains. "Only one person is employed full-time to run Locked Shields; all the others are experts from across NATO and Member States put together as a team. It is incredible to see." Every year some new elements are incorporated to follow current technological trends on the market. "This year," continues Past, "we have integrated an 'industrial control system' used to manage energy supply, production and even traffic lights in the civilian world. We also had drones fully integrated into the scenario."

The Centre also offers a wide range of technical and online courses. It has made available 15 courses in different cyber areas, as well as law courses, thereby contributing to the CCDCOE's efforts to raise cyber awareness and knowledge within the international community.

Regarding the legal aspects, the Centre published the Tallinn Manual, a CCDCOE flagship document which systematises law applications within the cyber domain. 'The Tallinn Manual on the International Law Applicable to Cyber Warfare' (2013) confronts the existing international law norms against cyber warfare. The result of this three-year project is a dissertation by an international group of law experts on law applications, along with their valuable commentaries. A follow-on to that, 'The Tallinn Manual 2.0' is to be delivered in 2016. It will widen the scope of analysis by taking into consideration attacks which are not yet classified as warfare but, nevertheless, pose a threat to societies, governments or industry.

Lastly, Cycon, an annual conference held by the CCDCOE, is an excellent forum for discussions on current and future developments in cyber defence. It fosters the community, and enables the exchange of thoughts and ideas.

The more, the better

Even though the Centre primarily serves the Alliance and its contributing Member States, the common goal in terms of achieving secure cyberspace is what makes the interface between the efforts of the Centre and the European Defence Agency so effective. The EDA and CCDCOE have in fact been cooperating on many occasions. On one side, the Centre supports the EDA operation's headquarters awareness seminars, and acts as an observer for the EDA Cyber Ranges project and cyber decision making exercises; on the other, the EDA observes Locked Shields' exercises, actively participates in Cycon conferences and co-organises workshops on Cyber Ranges.

In conclusion, since cyberspace breaks barriers and boundaries, and since the cyber threats are relevant to any organisation or institution, combining efforts to confront these challenges is quite simply a necessity. In this context, it really is a case of "the more, the better."

European Organisation for Security calls for European industrial strategy in cyber security

The European Organisation for Security (EOS) advocates a harmonised European security market based on an end-to-end approach. It brings together European companies and research centres representing about two-thirds of the European market for security of supply. ***Luigi Rebuffi***, the EOS Chief Executive Officer, presents practical implications of the dual-use concept in cyber security, evaluates the condition of the European security market, and proposes a way ahead for the European cyber industry

What advantages does the dual-use solution bring to the industry?

Although there is a strong distinction between the security and defence markets, today's cyber security cannot be isolated from 'cyber defence'. Cyber attacks can target a wide range of strategic physical and IT infrastructures (including classified information) vital to national security, and potentially disrupt a country's military forces. Therefore, cyber security solutions are genuinely dual-use technologies. The drastic cuts in the Member States' defence budgets and the promotion of the Pooling & Sharing approach have benefited European cyber security solutions suppliers (especially Small and Medium Sized Enterprises – SMEs), providing them with access to another market. However, the challenges are still on the rise. As the European industry has developed its cyber competence, becoming a trusted supplier to national governments eager to protect their sovereignty, the lack of cooperation in sharing information and building common solutions has led to increased market fragmentation in Europe. This has contributed to opening the way to non-EU companies known to be very competitive in commercial applications, who also benefit enormously from defence contracts, thanks to large public and private investments. Despite the high quality of European solutions, the fragmentation of the security market and the insufficient investment to develop solutions in the strategic domains of cyber security are hindering our competitiveness in the global market and putting our data and strategic assets at risk.

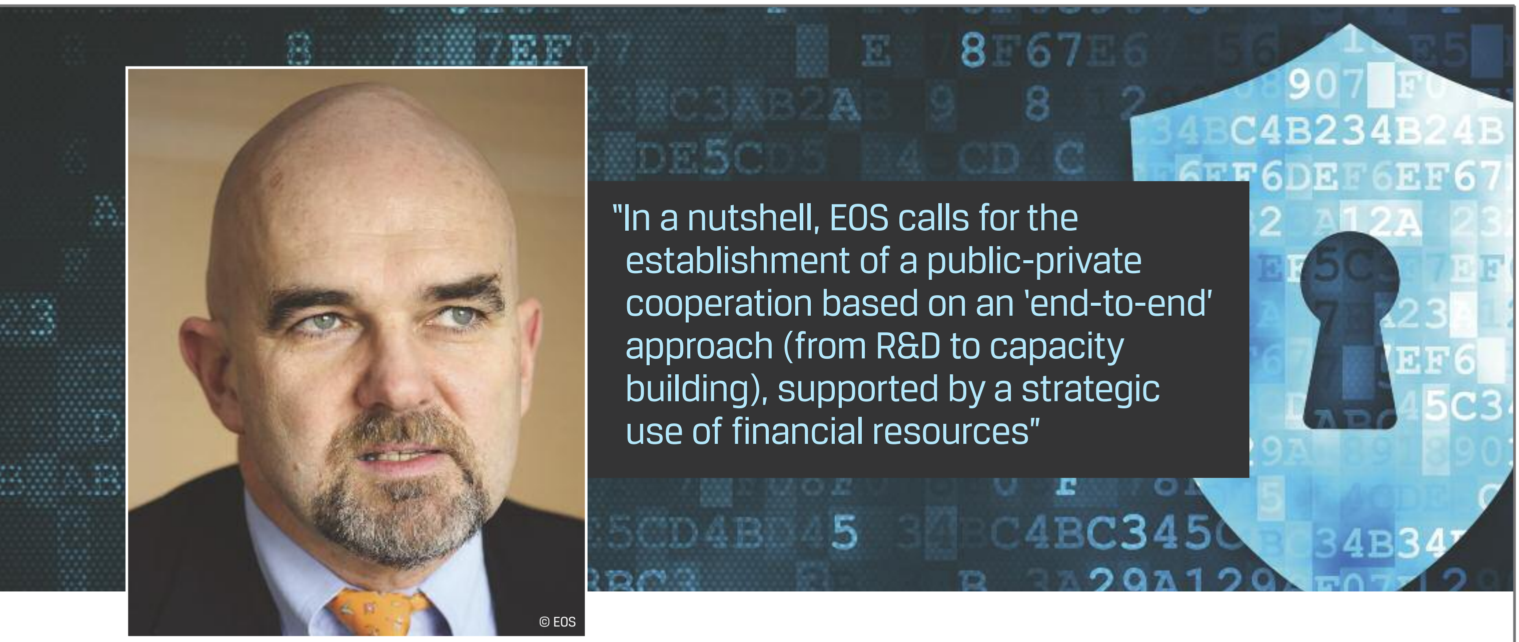
> "Europe has several thousand innovative SMEs with great potential but too few opportunities to grow in this fragmented market"

What benefits do you see to Public-Private Partnerships in cyber security?

Public-Private Partnerships (PPPs) are a useful tool for establishing strong and sustainable collaborations between the public and private sectors. They allow for the sharing of information, boosting strategic research and innovation (R&I) based on a better understanding of the end-users' needs. In Europe, it is anticipated that the PPPs on cyber security will support the improved coordination of the Research & Development (R&D) activities, as well as a structured public-private dialogue for the protection of the Digital Single Market. While this is an encouraging improvement, such PPPs will be largely insufficient to support the effective development of a genuine, competitive and trusted European industry, if not supported by an adequate financial scheme allowing innovation.

How has the industrial landscape of cyber security and defence evolved? What is the profile of a typical cyber security industry nowadays?

Rapidly evolving threats demand continuous investment and technological innovation. Europe has several thousand innovative SMEs with great potential but too few opportunities to grow in this fragmented market. We are not missing ideas; we are missing political and financial support for the development of our industry and a



© EOS

"In a nutshell, EOS calls for the establishment of a public-private cooperation based on an 'end-to-end' approach (from R&D to capacity building), supported by a strategic use of financial resources"

harmonised market with sufficient critical mass. In comparison, the US has envisaged a federal budget for 'cyber security' of $14 billion in 2016, the majority for 'defence' applications. New information and communication technologies (ICT) in which Europe can still claim a leadership position are under development, such as the Internet of Things, cloud security, big data, mobile and cyber physical systems etc. Europe should strategically use its resources for the development of solutions in these sectors, and their applications in leading markets, such as manufacturing (e.g. Industry 4.0), services (e.g. finance) as well as in defence (intelligence gathering to fight terrorism and organised crime).

How does EOS cooperate with the EU, and the European Defence Agency in particular, especially in terms of secure cyberspace?

EOS has been in regular and close contact with the European institutions, as well as with the EDA, to look into how dual-use technologies could support the competence (and competitiveness) of the European industry. Since 2009, EOS has advocated drafting a European Cyber Security Strategy (adopted in 2013) as well as an EU Cyber Security Industrial Policy to support the development of a genuine European cyber security industry and of increased digital autonomy for Europe. EOS is currently working on a study proposing the creation of a cyber security flagship programme which would examine the various steps to achieve these two goals. In a nutshell, EOS calls for the establishment of a public-private cooperation based on an 'end-to-end' approach (from R&D to capacity building), supported by a strategic use of financial resources, agreed together with the Member States and European institutions, and giving priority (when possible) to the procurement of trusted EU solutions. One of the pillars of this approach is the creation of the European Cyber Security Industrial Policy for which the study provides a list of recommendations.

What efforts does EOS take to promote research and innovation induction?

EOS represents the interests of both European security solutions providers and leading research centres with high expertise in cyber security. EOS closely cooperates with national clusters and associations to bridge the gap between the R&I and market deployment at national and European levels. Today, EOS is strongly supporting the creation of the envisaged cyber security PPP announced by the Commission, as it is the first step foreseen in our proposed flagship initiative. This would most definitely lead to a better structured market and improved cooperation across Member States in all sectors. As always, research is an initial step for a deeper cooperation towards market deployment. However, this would benefit the European industry only if it is envisaged within the framework of a strategy developing a strong and competitive European industry and increased Europe's digital autonomy.

Which main recommendation would you give to policy and decision-makers to improve Europe´s cyber security industrial competitiveness and security of supply?

EOS supports the creation of a 'Smart and Secure Digital Europe' to boost growth and jobs but this should be done with a better control and protection of our data, not only for economic reasons but also with respect to our privacy rights. Today, our data is 'exported' (with or without our agreement and knowledge) and further exploited thanks also to value-enhancing techniques, such as big data. It is therefore important to remind the public that data leakage has not ended with Mr Snowden's revelations and that it is of paramount importance that we are able to secure it. To do so, we need a massive and strategic investment plan in Europe within the framework of the European Cyber Security Industrial Policy.

EOS
EUROPEAN ORGANISATION FOR SECURITY

Hybrid warfare: the future of warfare?

"You might not be interested in hybrid warfare, but hybrid threats are definitely interested in you."
***Axel Butenschön**, EDA Project Officer*

© UK MoD

© EU NAVFOR

The hybrid reality

Hybrid warfare falls outside the bounds of conventional definitions. Hybrid threats are designed to exploit vulnerabilities, in this case vulnerabilities of the western world; the nature of these threats, therefore, is in a constant state of evolution, based on the success of their prior applications. Consequently, any agreed definition is redundant from almost the moment it is developed. If anything can be said to 'define' hybrid warfare, it is the combined characteristics of flexibility and adaptation.

These blurred boundaries, along with an uneven distribution of power and ambiguous lines of operation, make hybrid warfare a blended, shifting mosaic of conventional and unconventional warfare, regular and irregular warfare, cyber attacks, as well as diplomatic, economic and information lines of action. Hybrid warfare may easily be applied by both state and non-state actors, and it involves the polarisation of national populations using propaganda and disinformation tactics.

The main characteristic of hybrid attacks is that they are designed to exploit an opponent's vulnerabilities, using a combination of civilian and military actions. It is essential that the targeted communities, Member States or organisations recognise this and draw the appropriate political and operational conclusions in order to respond to such attacks in a timely and appropriate manner. It is important, therefore, to be able to identify that a hybrid attack is going on. This can only be achieved if comprehensive situational awareness is in place, enabling the linkage of singular events. An example would be an adversary cyber attack on a state's own critical infrastructure, combined with military activities and propaganda-led social media campaigns; a hybrid lens enables such a series of events to be viewed as a complete picture. While hybrid warfare has become a popular term amongst experts dwelling on the future shape of warfare, all types of warfare should be considered through this 'hybrid lens' – especially the conventional one.

"We need to avoid falling into the trap and shifting completely from one to 'the other side of the boat' and by that opening another flank. We have to find the right balance between continuity and change, and rather adjust our thinking of conventional warfare to an unconventional future"

"Know before you go"

The European Defence Agency (EDA) is working with the EU External Action Service to fulfil the May 2015 EU Council conclusion task to 'develop a European joint framework with actionable proposals' on how to counter hybrid threats. In accordance with its mandate, the EDA is leading the capability development dimension, adding value and contributing with concrete assessments of hybrid warfare implications for future capabilities. In addition, the Agency is already conducting a significant number of discrete activities and projects which could be directly linked to countering hybrid warfare, such as the very promising work strand on cyber defence.

At this point, it is important to underline the supporting role of the Agency towards national efforts to counter hybrid threats. "Regarding countering hybrid warfare, it is clear that it is a national responsibility to respond to and counter hybrid attacks. However, the EDA's mandate is to support our Member States by providing them with a broader-scoped European lens and helping them identify implications in a wider context relevant to their national planning," explains Axel Butenschön, EDA Project Officer. For that reason, national experts will play a key role in the upcoming tabletop exercises.

Starting in February 2016, the EDA will initiate two tabletop exercises to enable the assessment of available national capabilities. Working with Member States' Ministry of

© UK MoD

© Bundesheer

"One thing is certain, hybrid warfare poses a significant challenge to the EU, its citizens and its interests, and time is of the essence to develop a joint approach to effectively tackle hybrid threats"

Jorge Domecq, EDA Chief Executive

Defence military experts, representatives of the EU Military Committee and Military Staff, Crisis Management and Planning Directorate and other Commission bodies, stakeholders, NATO observers, representatives of the scientific and academic world, the Agency is hoping to 'stress-test' the existing capability priorities, as well as to identify possible gaps or areas for improvement. This is a necessary, yet sensitive step on behalf of the EDA; it aims at concrete results, which will enable Member States to truly assess their capabilities regarding countering hybrid threats. The goal, according to Butenschön, is to "formulate a comprehensive assessment and proposals on the implications of the new hybrid threats from an EU perspective."

The first exercise, based on a generic scenario, will focus on providing first-hand information to the ministerial level. In July, a further tabletop exercise, far more detailed in scope, will take place at an expert level. "Our aim is not to point out potential adversaries but to identify qualitative challenges to be better prepared for the uncertainties of the future," stresses Butenschön. Indeed, the exercises will be about neither simulation nor decision-making processes at a tactical level, but rather all about detailed capabilities implications.

The key factor here is not the intention to reinvent existing national capabilities per se, but the potential to reshape or refocus their direction with a view to new types of threats.

Multi-purpose toolbox

By nature, the complexity of hybrid warfare implies the involvement of both civilian and military elements. Thus, civil-military synergies are required in order to face hybrid challenges effectively. On the one hand, such a comprehensive response widens the scope of the addressed threats; on the other, it may allow for a reduction of expenditures.

The NATO-EU partnership is yet another example of how countering hybrid threats can be maximised. "In the context of hybrid warfare, this is not an option but an absolute need," stresses Jorge Domecq, the EDA Chief Executive. Indeed, with a different methodology and distinct focal areas, both organisations are supplementary by default. In this context, the EU is not only offering varied economic, diplomatic or legal assistance but also significant military capabilities to the toolbox. Considering the complex nature of hybrid threats, such a diverse toolbox is vital.

To complete the overall picture, one must keep in mind that new technology is not at the core of the solution in tackling hybrid threats. Hybrid warfare's main objective is to target the human and social dimension. Consequently, our responses must also address and involve the population in an effective manner.

The hybrid challenge

Even though the international community has started to recognise the phenomenon of hybrid threats, there are still more questions than available answers. Where and when does hybrid warfare actually start? Which Rules of Engagement are applicable? How can an attack be defined? Is a set of apparently unrelated events – for instance a local riot, an incident at a power plant, diplomatic tension, several cyber attacks – part of a larger hostile hybrid campaign?

"The tabletop exercises don't aim at predicting the future; by thinking through different possible scenarios, we should prepare ourselves better for future surprises. In this context, the EDA approach is to be considered as to support participating Member States' preparation and to act as a shock absorber"

Are we able to take a step back and generate a comprehensive picture? Do we have the appropriate mindset? Amid this uncertainty, however, there are certain questions we can answer without hesitation: yes, the discussion about hybrid warfare is necessary and yes, it is time to check the toolbox to ensure all the tools are in place in case we need them.

"The ability to use the same technology to meet requirements different from those of state and citizen defence and security, guarantees a much higher market potential, at a lower cost, for an increased number of people"

© Finmeccanica

Rationalisation as the key to creating European industrial champions

An in-depth analysis of the European defence market by Ing. ***Mauro Moretti,*** Chief Executive Officer & General Manager of Finmeccanica as well as President of the AeroSpace & Defence Industries Association of Europe (ASD). The analysis includes identification of weaknesses as well as measures for the European defence industry to reach its available potential and become a game-changer in the global market

Upon taking office earlier this year as President of the AeroSpace & Defence Industries Association of Europe (ASD), what was your initial assessment of the European defence and security sector?

I would define it as a sector with great potential, but one which suffers from intrinsic weaknesses as a result of being structured on a national basis. In Europe, the evolution towards a truly continental defence and security market is still very slow and fragmented.

There are examples of industrial collaborations which do not translate into a truly integrated defence market and there are no companies and groups which can claim to be really European, except perhaps the Airbus Group.

This is a situation that appears even clearer when compared with the United States, where the trend towards large group consolidation continues. Certainly, this evolution sees Europe being left behind. On the other hand, defence is a sector that demonstrates its important role daily in the economic system.

In a Europe strongly exposed to the risks of de-industrialisation, defence represents a real driver of technological innovation, capable of creating quality employment and generating a positive contribution to the growth and economy of the single countries, and therefore of the whole continent. Nevertheless, the European defence sector is not completely mature as regards structure and organisation; rather, its fragmented nature leads to the duplication of competencies – in other words into further elements of weakness – which are difficult to sustain in the long term under the investments profile. For example, the Americans only have one fighter jet, while Europe has three, and having three competing systems on the world market means a waste of resources.

What is your analysis of the recent trends in European defence spending?

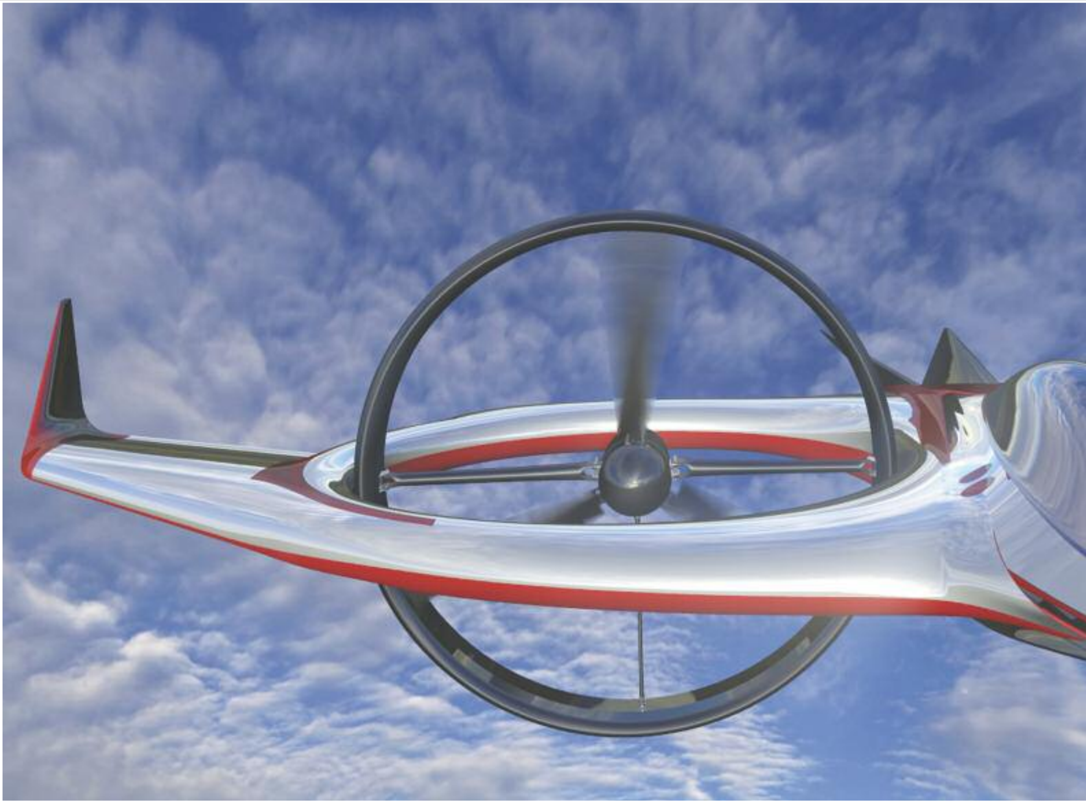
In the last few years Europe has seen a clear decline in resources dedicated to the defence sector. The budgets of single European countries have been under pressure as a result of the economic-financial crisis and the restrictive budget policies implemented by governments in order to respect the European Union's budget restrictions.

Also, in the different national contexts, defence has been one of the sectors most affected by budget restrictions, with a consequent defence spending reduction. It is true that some countries have seen a slight growth, but on average the sector has lost part of the previously available budget. To date, we can say that the trend has stabilised somewhat, however it will be difficult to return to pre-crisis spending levels.

Which measures should be taken to halt the reduction in Research & Development spending?

Rather than ask ourselves how to stop the decline in investment, we should ask ourselves how to better spend the available resources, precisely for the reasons I have just mentioned. It will in fact be difficult to have additional resources available in the future. What we could do is to concentrate investments in the sectors with the best growth prospects, therefore with greater economic impact and with a better chance of making European industry competitive on the global market, also by turning more

"Today we have the opportunity to bring together competencies and capabilities of the different European companies for a common requirement of the different countries. In this sector the real challenge for the European defence industry is to converge towards a really advanced requirement projected to the future"



The AugustaWestland 'Project Zero', a demonstrator based on tiltrotor technology, the result of cooperation of Finmeccanica companies – Selex ES, Ansaldo Breda, Ansaldo Energia, and partner companies from Italy and the UK

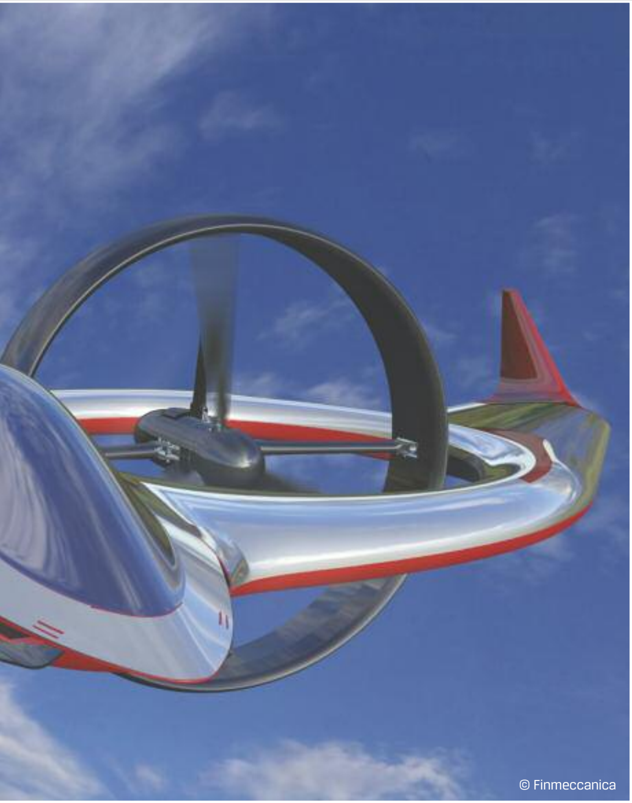
to cooperative programmes which can make the few existing resources available to all. It will also be crucially important to make the best use of research and development related to the application of dual technologies. It is therefore necessary to drive research and development towards technological solutions, with minor adjustments, applicable in both the military and the civil domains. The ability to use the same technology to meet requirements different from those of state and citizen defence and security, guarantees a much higher market potential, at a lower cost, for an increased number of people. The advantages of dual technology are so evident that, according to evaluations, in the last years at least 50% of the expenditure destined for military and security research has been directed towards these types of applications.

Should European defence companies find new ways to promote innovation? Any key learnings from the digital companies to benefit from?

In my opinion the Small and Medium Sized Enterprises (SMEs) and start-ups have not yet fully reached their potential: I refer to their ability to produce technological innovation. Big industry does not necessarily have to develop all the technologies which contribute to creating the great defence platforms on its own; on the contrary, it must be able to 'capture' the innovative solutions developed elsewhere and include them in the system, thereby creating a network of capabilities and a chain of sub-suppliers aimed at converging into a wider and more structured project that only a big company is able to support and take forward. The big defence players support huge investments to make complex systems and platforms which require substantial hardware infrastructures, while smaller companies enjoy greater flexibility in addressing investments in programmes, perhaps smaller but highly qualified, for example in high tech components or sophisticated software programmes. This is the case for digital companies, where software activity is prevalent, requiring lower investment and therefore allowing companies with few employees but with innovative ideas to grow and bring their own solutions to the market. To connect these two worlds and establish mutual synergies leads to the creation of open innovation, a way of partially overcoming difficulties related to innovation process management. Thus the big company reduces the investment's effort, concentrating resources on core technologies and taking advantage of the contribution of creativity and innovation of the small company or of the start-up that, in turn, enters a virtuous circle capable of raising its own activities and capabilities to the level of great projects.

Support to SMEs is of great importance for a healthy European Defence Technological & Industrial Base (EDTIB). How could this be enhanced?

By supporting the Small and Medium Sized Enterprises in their ability to specialise in niches of excellence, complementary to the competencies of the bigger companies. This way, the SMEs are given the chance to enter a network within the framework of important projects with a big company and, at the same time, to promote their involvement in specialised initiatives which envisage an autonomous capability of entering the market. In fact, reaching a partnership with



© Finmeccanica

a big company allows SMEs to draw upon crucial resources in terms of technology and know-how; this leads them to progressively grow and to acquire enough knowledge to no longer be dependent on the big group, obtaining visibility at an international level and achieving new leads into foreign markets. To this end it is clear that, in order to create a balanced and profitable relationship, it is up to the big company to identify activity segments ripe for development and future applications on which the SMEs will converge, contributing their skills. This is a process that generates benefits for both parties: the big company gets the collaboration of highly valuable partners, which bring dynamism and flexibility to its business, while the SMEs participate in technological innovation processes, thereby enhancing their competitiveness.

The development of a European MALE – RPAS (Medium Altitude Long Endurance – Remotely Piloted Aircraft System) has been confirmed by France, Germany and Italy. What is the significance of this programme to the European industry?

The importance of the MALE programme comes from the fact that it is the last chance for Europe to develop an autonomous capability in a segment left for a long period to US or Israeli companies. This is so true that today most European armed forces use American systems. In the past there have been some attempts, at a national level, to develop this type of capability. But they have failed. Today we have the opportunity to bring together competencies and capabilities of the different European companies for a common requirement of the different countries. In this sector the real challenge for the European defence industry is to converge towards a really advanced requirement projected to the future for two reasons. Firstly, to create a product capable of meeting the armed forces' requirements in the medium-long term, reaching a more advanced level than the current Predators or Herons. Secondly, because an advanced system of this kind may well become a first step towards an Unmanned Combat Aerial Vehicle (UCAV) aircraft. In other words, this project could be included in the series of activities necessary for the European Union to keep a combat air capability also in the medium-long term, with the prospect of a possible launch of a project for a European fighter, successor to the Rafale and the Eurofighter.

What are the keys to Europe's success on the international defence market?

Currently it is not Europe that sells on the international markets, but the single companies which propose their products on the market, very often with the support of the respective national governments. In the medium term it will necessarily be that way: waiting for the birth of a real European defence market and of a European foreign defence policy, it will be difficult for Europe to act as a player in the defence market at an international level. This would only be possible with the help of processes of a rationalisation of the European industrial base which can create unique and distinctive European industrial champions, in the interest of most national industries and that, with the joint support of the European governments, may be capable of entering the global market. To obtain this result it is necessary to follow cooperative models which, integrating resources and know-how on a common project, may create a truly supranational reality, with a strong core of technological competencies and adequate size to successfully compete at an international level.

Ing. Mauro Moretti – Chief Executive Officer and General Manager of Finmeccanica Group since May 2014 and President of AeroSpace and Defence Industries Association of Europe (ASD) since March 2015. He is Honorary Chairman of Italian Industries Federation for Aerospace, Defence and Security (AIAD), the Italian Federation for Aerospace, Defence and Security and President of the FS Foundation.

Moretti began his career in 1978 at the Italian State Railways Corporation, and held various managing positions, including Managing Director of the Technological Development Division (1993); CEO of Metropolis SpA (1994); Director of the Rolling Stock and Locomotion strategy business area (1996); Director of the Network Rail strategic business area (1997); Chief Executive Officer of Rete Ferroviaria Italiana SpA (2001). Under his leadership (2006 – 2014), the State Railways Corporation transformed into Ferrovie dello Stato Italiane.

Public-Private Partnerships as incentives for more cooperation in the development of European defence capabilities

Skills and capability development, increased know-how and budget savings are undeniable advantages of public-private initiatives in the defence sector. ***Étienne Schneider,*** Deputy Prime Minister, Minister of Economy, Minister of Internal Security and Minister of Defence of Luxembourg, presents how Public-Private Partnerships work in practice

© SIP (Service information et presse - Luxembourg government)

> "Governments and the private sector should seek approaches that reinforce one another and create win-win situations. Such Public-Private Partnerships are incentives for more cooperation in the development of European defence capabilities"

What are the benefits of a Public-Private Partnership in defence?

The Member States of both the EU and NATO are facing a two-fold challenge: reduced budgets in the wake of the economic and financial crisis and, at the same time, significant and dramatic changes to our security environment. Global events of recent years have led us to conclude that the world has not become a safer place. The importance of defence in creating a safer world has become clearer than ever. The past few years have seen serious cuts to national budgets, however, including defence budgets. Since 2008, defence expenditures in the EU have been in a continuous state of decline. Hence, our mission is clear: we have to do more with less. And there seems to be one obvious way to do that: work in partnerships.

To remain relevant, defence has to be cost-effective, it has to be efficient, and we have to find innovative approaches to achieve our targets. In a nutshell: we have to spend better and work more closely together. Collaboration among Member States is obviously a main means of achieving this, and Luxembourg has a long tradition in that regard – be it in the context of the BENELUX framework, the NATO Airborne Early Warning and Control Force or the A400M military transport programme.

How far is working with the industry and private sector another obvious path to go down?

As Minister of Defence, I currently face quite a comfortable budgetary situation, as Luxembourg will raise its defence budget in the upcoming years by 50%: from 0.4% of Gross Domestic Product at present, to 0.6% by 2020. However, such a budget increase does not mean that we should not still be spending smartly and effectively in order to achieve the best possible results.

The Luxembourg Government, as any other government, cannot fill all the gaps. We have to rely on the additional skills and know-how that can be found in the private sector. Luckily, Europe has a vibrant and competitive industry, innovative Small and Medium Sized Enterprises (SMEs), and top-level research institutes. They are a useful and important asset to have at our disposal, but also an asset that we need to work to preserve and strengthen. Governments and the private sector should seek approaches that reinforce one another and create win-win situations.

Such Public-Private Partnerships are incentives for more cooperation in the development of European defence capabilities.

What is the current situation in Luxembourg?

In recent years, Luxembourg has undergone a remarkable process of dynamic economic diversification in order to face the challenges of an ever-changing world economy. Being both Minister of the Economy and Minister of Defence, I saw an opportunity to deepen and enhance this diversification by seeking to further utilise the talent of Luxembourg companies in the area of defence. Luxembourg does not have an armaments or specific defence industry of its own. We do, however, have great know-how and world-renowned skills in the sector of dual-use technologies: satellite communications, aerospace, logistics, data analysis or IT and cyber security.

A good illustration is the naval operation European Union Naval Force – Mediterranean (EUNAVFOR MED), newly named 'Sophia,' fighting smugglers in the Mediterranean. As a Member State involved in Operation Sophia, the Grand Duchy operates aircraft under a →

© SES

Public-Private Partnership with aerial surveillance and reconnaissance specialist CAE Aviation, a company based in Luxembourg. The Swearingen Merlin IIIC maritime patrol aircraft is operating from the US Naval Air Station at Sigonella, Sicily, in support of the mission for boarding, searching, seizing and turning back boats suspected of being used for smuggling or human trafficking.

Our future Luxembourg Governmental Satellite in military communications – named GovSat – serves as another important and significant illustration of how public and private actors can work together for their mutual benefit. The Luxembourg GovSat will be operated by a joint venture company, which was set up as a partnership between the government and the Luxembourg satellite company, SES, a landmark for satellite telecommunications and now a major player in this sector.

What are the advantages of LuxGovSat?

This joint venture provides reliable and assured communication satellite capacity with military frequency bands exclusively to institutions and governments while fulfilling Luxembourg's NATO commitments. The capacity of this satellite will be used, first of all, for national defence needs. The remaining capacity will be offered either as a contribution, or sold to Allies and Partners, to NATO, the EU or to other international organisations.

Emerging from the national space sector, this project is not only an important contribution from Luxembourg to European defence, but it further supports the government's economic diversification policy in a key technology sector. At the same time, it creates highly qualified jobs, while responding to a pressing need on the part of the international defence community. It is an excellent example of a win-win situation, both for Luxembourg's defence and for its national economy.

It is not too difficult to imagine other examples: logistics in Europe is steadily becoming more relevant to security and defence. Increasingly, the military is relying on civilian service providers to help fulfil their logistical needs. Developing Luxembourg as a European logistics hub is another key priority of the government. New opportunities for Luxembourg firms might arise in the security and defence-related logistics sector.

How will LuxGovSat be key to European SatCom infrastructure?

Satellite communications play a vital role in areas such as defence, security, humanitarian aid, emergency response, diplomatic communications as well as civil and military operations in remote areas. LuxGovSat is aligned with the ongoing work of the European Commission and Council for the development of next generation GovSatComs capabilities across Europe in three main areas: first, in delivering coverage, performance, flexibility, security in X-Band and military Ka-band; second, by addressing governmental and institutional users; and third, through enabling critical SatCom solutions like Comm-on-the-Move products or Remote Piloted Aircraft Systems in both the defence and security segment. As an enabling infrastructure, LuxGovSat can contribute to the GovSatCom initiative throughout its various phases, as led by the European Commission and the European Defence Agency to help fulfilling EU and NATO operational requirements. LuxGovSat can support the communications requirements of the military Common Security and Defence Policy and European External Action Service missions and operations as well as those of other European government agencies, such as FRONTEX or European Maritime Safety Agency.

Presidency of the Council of the European Union GRAND DUCHY OF luxembourg

© SES

Patrick Biewer, Chief Executive Officer, LuxGovSat

LuxGovSat: Luxembourg's military SatCom venture

Jointly operated by the global satellite operator SES and the Luxembourg Government, the objectives of LuxGovSat are the acquisition, launch and operation of a satellite for the provision of governmental and military communication services. The Luxembourg-based company is funded in equal parts by SES and the government, who have each dedicated €50 million to the project. A loan of €125 million completes the funding.

The capacity of the new satellite will satisfy Luxembourg's requirements for satellite communications in military frequencies. The capacity will also be made available to governmental and institutional customers for defence and governmental applications. With its launch scheduled for the second quarter of 2017, the satellite will be positioned at 21.5 degrees east, covering Europe, the Middle East and Africa.

This multi-mission satellite, which the Luxembourg Government has pre-committed to a significant amount of capacity, will use dedicated military frequencies (known as X-band and military Ka-band), providing high-powered and fully steerable spot beams to support multiple operations. Bringing new capacity in governmental frequency bands, the satellite will feature steerable high-powered spot beams to ensure flexibility for ever-changing missions, anti-jamming capabilities and end-to-end managed solutions.

In July 2015, *Patrick Biewer* was appointed Chief Executive Officer (CEO) of LuxGovSat. The former SES senior executive has an in-depth knowledge of the satellite industry and proven experience in developing a start-up business into an established operation. Biewer has held a number of senior positions within SES since he joined in 1993, and has accumulated some impressive leadership experience during his career. "LuxGovSat opens a new chapter in the cooperation between SES and the Luxembourg government, as well as in the strategically important government business vertical. GovSat-1 will ensure flexibility for the ever-changing missions of governments and institutions in the security, defence and civil arenas and will enable the deployment of applications of demanding customers requiring secure, reliable, accessible yet affordable satellite capacity," Biewer says.

›Interface

A review of ongoing defence-related exhibitions and cultural events around Europe

[illegible]

The run-up to D-Day
Permanent Exhibition
The War Museum in Overloon, NL
www.oorlogsmuseum.nl

A 20 meters long and 5 meters high glass facade with comic drawings by Teun Berserik at the entrance to the military hall illustrates the preparations for D-day. The War Museum Overloon, founded in 1946, presents the history of the Second World War dedicated to opposition, persecution and liberation.

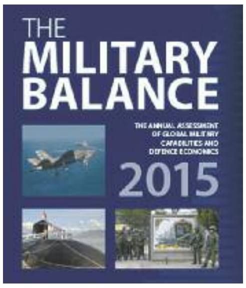
It exhibits more than 200 road vehicles, vessels and aircraft from that time period. A special attention is paid to the Battle of Overloon of 1944 which is known to be the most intense tank battle ever conducted on Dutch soil.

Images courtesy of The War Museum in Overloon

The Military Balance 2015

Edition 2015
International Institute for Strategic Studies
www.iiss.org

A useful handbook for security policy and military affairs containing an assessment of the military capabilities and defence economics of 171 countries. Detailed A–Z entries list each country's military organisation, personnel numbers, equipment inventories, and relevant economic and demographic data. New features in The Military Balance 2015 include equipment analysis graphics, list of military training exercises arranged by region, a wall chart detailing Russia's armed forces and essays on hybrid warfare, US space systems and directed energy weapons.


THE
MILITARY
BALANCE
THE ANNUAL ASSESSMENT OF GLOBAL MILITARY CAPABILITIES AND DEFENCE ECONOMICS
2015

From Ebola to ISIS

Fighting Extremes: From Ebola to ISIS
18 November 2015 – 13 November 2016
Imperial War Museum, London, UK
www.iwm.org.uk

The display shows how Britain's armed forces deal with very different aspects of global security, from the Ebola outbreak in West Africa to being part of coalition efforts to fight ISIS in the Middle East.

British forces were deployed to Sierra Leone in 2014 to help organise the response to Ebola, build treatment centres and provide medical staff and security personnel. The same year, other units were deployed to operate against ISIS, including launching air strikes, gathering surveillance and training local opposition forces.

Using the objects and experiences of personnel involved in these two operations, this display will show the complexity of contemporary conflict and security.

Courtesy of Imperial War Museum

Operation Sophia to stop human trafficking across the Mediterranean

As an expression of a wider comprehensive approach towards migration, the EU is conducting an operation to fight human tragedy and to curb illegal procedures on the Mediterranean

The EU has taken action in response to the deaths of hundreds of people fleeing conflict and poverty in the Middle East and Africa, many of whom have become victims of human smuggling and trafficking across the Mediterranean. On 18 May 2015, the EU Council approved the Crisis Management Concept for a military Common Security and Defence Policy (CSDP) operation to disrupt a business model of human smuggling and trafficking networks in the south-central Mediterranean. Consequently, on 22 June 2015, the EU launched a European Union military operation in the south-central Mediterranean (EUNAVFOR MED).

Following the Political and Security Committee's decision, the EUNAVFOR MED has been codenamed 'Operation Sophia', after a baby girl born on 22 August 2015, to a Somali woman on board a German frigate off the coast of Libya.

The Three Phases of Operation Sophia

Operation Sophia consists of three operational phases, planned in full compliance with international law. These phases focus on surveillance, search operations, and disposal practices, respectively. In the two months since the achievement of Full Operational Capability, on 27 July 2015, the operation has successfully met the objectives laid out for Phase 1. These concerned the surveillance and assessment of human smuggling and trafficking networks across the south-central Mediterranean.

With the necessary intelligence information collected and analysed, the EU Political and Security Committee approved the corresponding Rules of Engagement and authorised a transition to Operational Phase 2. Since 7 October 2015, the command of Operation Sophia has been authorised to take more active steps towards curbing illegal activities in the Mediterranean. The aim is to conduct boarding, search, seizure and diversion, on the high seas, of vessels suspected of being used for human smuggling or trafficking. The UN Resolution 2240 (2015), announced on 9 October, provides an additional political endorsement and authorises Member States to seize vessels confirmed as being used for migrant smuggling and human trafficking from Libya.

The third phase of the operation will lead to the disposal of such vessels and related assets, and the apprehension of traffickers and smugglers.

Common Security and Defence Policy operations have the full support of the European Defence Agency (EDA). To this end, the EDA has taken three steps to facilitate the implementation of Operation Sophia: firstly, the Agency is contributing to the improvement of maritime situational awareness by the provision of the MARSUR networking project. With MARSUR, the existing naval and maritime information exchange systems are linked together, facilitating information flow and control. Secondly, the EDA has offered training in cyber awareness to the military staff of the operation, in order to increase resilience against potential cyber threats. Last but not least, human resources management software developed by the EDA is being employed at the operation's headquarters.

© Bundeswehr

Facts & figures:

Area of operation: central part of southern Mediterranean Sea;

Headquarters: Rome, Italy;

Starting date: 22 June 2015;

Mandate validation: 12 months since Full Operation Capability

Force strength: dependent upon rotation; currently the flagship (the Italian aircraft carrier Cavour) and 5 other naval unis and 6 air assets;

Contributing States: 22 Member States (Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Romania, Slovenia, Spain, Sweden, United Kingdom);

Operation budget: 11.82 million for the whole 12-month mission.

© Bundeswehr

Rear Admiral (UH) Enrico Credendino, the Operation Commander, presents the achievements of Operation Sophia Phase 1 to European Defence Matters, along with the upcoming challenges related to entering Phase 2

© EUNAVFOR MED

How would you summarise the progress and achievements of Operation Sophia Phase 1?

EUNAVFOR MED – Operation Sophia Phase 1 started on 22 June, following the decision of the European Council. A few days later, the appointed EUNAVFOR MED Force Commander, Rear Admiral (LH) Andrea Gueglio, led the flagship, Italian Aircraft Carrier Cavour, into the Joint Operation Area of 525,000 nautical miles in the central Mediterranean (an area six times wider than the length of Italy). One month later, the Force reached Full Operational Capability, following the integration of Germany's frigate FGS Schleswig-Holstein and the auxiliary ship FGS Werra, as well as the UK's hydrographic ship, HMS Enterprise. The surface units were supported by additional airborne surveillance assets, including two Italian EH101 helicopters, a UK Merlin MK 2 MPRA helicopter, a French Falcon 50, a Luxembourg SW3 Merlin III, and a Spanish P3B Orion MPA.

The first phase, conducted entirely in international waters, aimed to collect useful information and gain a clear understanding of the business model used by migrant smugglers and traffickers. Steps were also taken to ensure that the proper joint procedures were in place with all relevant partners, in order to collect data and evidence regarding the criminal activity of the smugglers and traffickers. This will facilitate future prosecutions.

Within two months, EUNAVFOR MED assets reported 22 sightings of suspected smugglers and traffickers on the high sea. These suspects will be the subject of interception and apprehension efforts during Phase 2. Furthermore, as a result of EUNAVFOR MED activities, 16 suspected smugglers and traffickers have so far been prosecuted by the Italian authorities, with 16 boats seized. In addition, 3399 lives have been saved at sea, including 2546 men, 683 women, 166 children and 4 babies.

Without a doubt, the success of this first phase is down to the comprehensive liaison network established by EUNAVFOR MED. This network includes all relevant military actors, such as the Italian Operation Mare Sicuro and Frontex Operation Triton, as well as non-military actors, such as Europol, Eurojust and UN agencies, international governmental and non-governmental organisations as well as local non-governmental organisations.

What changes to the mission have brought about the shift to Phase 2? How do you see the future development of the mission?

Moving from Phase I to Phase 2 in international waters allows for EUNAVFOR MED assets to board, search, seize and, if necessary, divert suspicious vessels on the high seas, under the conditions provided for by applicable international law. This legal framework was further strengthened by the UN Security Council on 9 October 2015 when, acting under Chapter VII of the Charter of the United Nations, it adopted the Resolution 2240 (2015) authorising Member States to seize vessels confirmed as being used for migrant smuggling or human trafficking from Libya.

There are three main pillars to the second phase of the operation in international waters : firstly, the capture and disposal of the vessels used by smugglers and traffickers; secondly, the restriction of smugglers' and traffickers' freedom of movement on the high seas; and, lastly, the apprehension of smugglers and traffickers, including those travelling on migrants' boats. These actions should certainly prove an effective means of disrupting the business model employed by smugglers and traffickers, thereby serving, also, as a deterrent. They cannot, however, be our sole solution, so long as our activities are limited to international waters.

Nevertheless, throughout these activities we will remain committed to saving lives at sea upon request by the competent Maritime Rescue Coordination Centre (MRCC) and in accordance with the International Law of the Sea.

Each mission is also about capability development and experience sharing; from this point of view what lessons learned can you identify?

This mission is a new type of Law Enforcement Operation conducted with military assets and is certainly indebted to the experience gained in the European Operation ATALANTA, working on counter piracy in the Indian Ocean. Therefore, in the Operation planning phase, we received support from an Operation ATALANTA expert team, who directly presented best practices and provided advice regarding areas of possible concern.

On the other hand, during Phase 1 we also had the chance to test our procedures, in particular with regard to information sharing with other military operations with more experience in the area, such as the Italian Operation Mare Sicuro and the Frontex Operation Triton.

Last but not least, we are exchanging information with a few civilian companies to further develop our software in accordance with the lessons identified during the first months of the Operation.

An Anchor for the EU Maritime Security Strategy

Sea power: not a concept many would associate with the EU. Yet it was brought to the fore at the very start of the Maritime Security Conference organised by the European Defence Agency (EDA), the Ministry of Defence of Cyprus and the Luxembourg Presidency of the EU, in Nicosia on 12-13 November 2015. And rightfully so. ***Prof. Dr Sven Biscop*** had the opportunity to attend the Conference – and here he offers some personal reflections

Maritime security is vital to European interests. But it begs the question: Does the EU really aspire to sea power? Does the Union even want to be a power at all?

At the battle of Copenhagen in 1801, Lord Nelson, when ordered to abort the attack that his part of the British fleet was about to undertake, famously put his telescope to his blind eye, declared not to see any signal, and pressed ahead anyway. (And, fortunately for him, won a brilliant victory, or our hero would have risked execution, pour encourager les autres, as Voltaire said of the British and their admirals). European admirals today seem to be in the opposite position: with both eyes wide open they scan the horizon with their binoculars, but no orders are in sight. What is European strategy?

"The Black Sea ought not to be a black hole in European strategic thinking: the crisis in Ukraine should have demonstrated its importance, once and for all"

In Search of Strategy

We do have an EU Maritime Security Strategy, adopted in 2014, which opens with the statement that Europe has "strategic interests" in "the global maritime domain". What follows, however, is less a strategy (i.e. ends, ways and means) than a set of operating principles, without defining clear objectives. It is striking that, both in the document and at the conference, all refer to a global challenge, but when it comes to action, we mostly limit ourselves to the regional: the Mediterranean and the Horn of Africa. As if the Indian Ocean and the Pacific were none of our concern. Of course, to a large extent, foreign and security policy will always be determined by events. Piracy in the Gulf of Aden and especially the tragedy of the refugees in the Mediterranean, evidently absorb much of our attention today. But they cannot be our only focus, certainly not as a driver for future capability development – unless we want our navies reduced to a coast guard. Asking that question of an admiral produces as predictable an answer as asking of a cavalryman whether he would not rather be in the infantry, digging trenches.

To convince our publics and parliaments of the continued need for a blue water navy that can operate across the entire spectrum, our navies need arguments. That means: a definition of a longer-term, more comprehensive level of ambition, geared to the global challenges to maritime security. Fortunately, the debate about a new EU Global Strategy, to be adopted in June 2016, provides an excellent opportunity to do just that: to anchor the Maritime Security Strategy in an overall strategy.

One of the key questions to be addressed by the Global Strategy is which responsibilities Europe wants to assume as a security provider. The question is not whether Europeans will act upon these under the EU or the NATO or an ad hoc flag, but what Europeans are resolved to do alone, if necessary, under any flag. That is a question of grand strategy that can only be addressed at the EU level. The answer can subsequently guide efforts in the Common Security and Defence Policy (CSDP) and NATO alike.

Assuming Responsibility

I see four responsibilities, all of them with important naval implications.

First, our armed forces have a role in contributing to the internal and border security of the EU. Part of that role is saving lives. The EU naval operation in the Mediterranean alone will not solve the refugee crisis, and it is important to state that it will not. Just as important is that it is saving thousands from drowning, and that has to be stated as well.

© LA(Phot) Des Wade, Royal Navy

Obscuring its aims for political reasons has never helped any military operation, nor in the end any political leader. Besides, deploying European navies will directly reduce the burden of search and rescue on our merchant vessels. The answer to the demands of border security is not to turn our navies into coast guards for, once abandoned, the higher-end capabilities will never come back. Navies that are capable of higher-end operations are capable of lower-end operations as well, as one part of a comprehensive approach integrating navies, coast guards and police.

Second, Europe has to take the lead in maintaining peace and stability in its own broad neighbourhood, including the adjacent waters, for nobody else will automatically do that for us. While the Mediterranean and the Gulf of Aden are on the radar screen, more efforts and means must go into implementing the already decided strategy for the Gulf of Guinea. Europe's role must precisely be to act early, before a problem escalates. The Black Sea ought not to be a black hole in European strategic thinking: the crisis in Ukraine should have demonstrated its importance, once and for all. The deployment of the French carrier Charles de Gaulle (with the Belgian frigate Leopold I among its escort) from Toulon to the Persian Gulf in the framework of the campaign against the IS is a clear demonstration that, alas, not all security problems in our broad neighbourhood can be solved by lower-end engagement (such as capacity-building).

Third, Europeans have to contribute to preserving the freedom of the global commons, including space, cyber space, and worldwide maritime security. One of the greatest challenges to the latter is the escalation of tensions involving one or more of the great powers. For sure, European diplomacy is the primary instrument to avert this threat. But such diplomacy can be underpinned by naval assets, not just to assert the importance that Europe attaches to maritime security in, e.g., the South China Sea, but as an active tool to create confidence- and security-building measures by engaging in exchange of expertise, joint education, training and exercises, and even patrolling, with local partners. The Association of Southeast Asian Nations (ASEAN) is a key partner for the EU, but to increase confidence inclusive partnerships can be sought, which encompass China, rather than encircle it. Our cooperation with the navies of China, India, Japan and many others in the Gulf of Aden provides the surest base for such creative partnerships.

Fourth, we need an effective UN because, without it, our own operational effectiveness is limited, as shown by the limits placed on operations in the Mediterranean by the absence of a Security Council mandate. For the collective security system of the UN to be effective, Europe must contribute more, not only when the UN acts in areas of direct interest to Europe, but beyond.

Acquiring Capabilities

No one can assume responsibility without capacity. With ongoing operations in the Gulf of Aden and the Mediterranean, Europe's naval capabilities are already severely stretched. If the future Global Strategy confirms the truly global outlook proposed by the Maritime Security Strategy, it will need to be translated into realistic but real military requirements. The idea that the Global Strategy will have to be followed up by a white book or similar document (in effect an update of the existing Headline Goal) is gaining ground. In such a case, any such document would therefore have to contain a strong naval chapter.

One thing is certain: for navies as for the other forces, far-reaching Pooling & Sharing will increasingly be the only way of maintaining and hopefully increasing significant capabilities across the spectrum. Far-reaching must be read as integrated: a combination of permanent pooling of assets and of dividing tasks between countries will generate real synergies and effects of scale, as Belgian-Dutch naval cooperation has proved. But Pooling & Sharing has no sense if there is no will to use the resulting capabilities. The EDA has successfully created the maritime surveillance tool MARSUR. If our navies do not use it when deployed on EU operations in the Mediterranean, how will they convince their political masters of the need for more investment?

Prof. Dr Sven Biscop is Director of the Europe in the World Programme at the Egmont – Royal Institute for International Relations in Brussels, and teaches at Ghent University and at the College of Europe in Bruges. He chairs the jury of the biennial EDA-Egmont PhD Prize on European Defence, Security and Strategy. In 2015, he was made an Honorary Fellow of the European Security and Defence College.

A stimulus for European defence cooperation: EDA programmes and projects now exempt from VAT

Following a recent decision by the EU Council, all programmes and projects will be subject to VAT exemption, so long as the European Defence Agency adds value to the initiative. ***Jorge Domecq***, the EDA Chief Executive, explains how the new regulation will incentivise defence cooperation at the EU level and should result in more collaborative defence projects in future

The European Defence Agency (EDA) stands at the heart of the European defence community, working to facilitate fruitful defence cooperation between participating Member States. The defence domain, as any other area, requires innovative injections in order to develop, including financial ones. Nowadays, efficient and smart spending, as well as the use of Pooling & Sharing and dual-use concepts, is becoming a necessity. To this end, the Agency has recently been equipped with a new instrument to incentivise defence cooperation at the EU level, and to encourage the launch of new cooperative defence projects.

Following the adoption of the revised EU Council Decision on the statute, seat and operational rules of the European Defence Agency, announced by the Foreign Affairs Council on 12 October 2015 (Council Decision [CFSP] 2015/1835), all projects and programmes held under the EDA umbrella may be subject to VAT exemption, provided that the EDA adds value to them. In other words, such a financial instrument can be applied so long as the project leads to increasing interoperability, achieving synergies or pooling demand to structure the supply side, thus making a difference for EU defence. In fact, there is no limitation whatsoever regarding the nature of the project; it can be research or technical expertise, pooling demand, a project on building a multinational capability. It can also be fully administrative and contractual management of a cooperative initiative that leads to a change in the supply chain and/or the output in terms of capability development.

Member States, the Belgian authorities, and the European Commission Services (Taxud) have been working closely with the EDA to prepare an effective financial solution that will incentivise European cooperative defence projects without distorting the market. The legal basis for the VAT exemption was framed within Protocol No 7 of the EU Treaties on the privileges and communities of the European Union and Council Directive 2006/112/EC of 28 November 2006 on the common system of value added taxes.

Regarding the tax exemption, Jorge Domecq, the EDA Chief Executive, emphasises that "it is not an objective per se, but it is there to make the Member States understand there is a bonus to defence cooperation in Europe." He perceives the new regulation as an excellent add-on and a strong incentive for defence cooperation, explaining that "it generates an attractive business case for cooperative projects and programmes in the framework of the EDA." He adds that the new regulation contradicts a presumption that "multinational cooperation costs more and causes delays". On the contrary, such a financial measure generates considerable savings. In the case of the EU Satcom market project alone, almost €300,000 can be saved out of a single €1.3 million contract recently submitted by one of the participating Member States, and there are more contracts to come. In the framework of the project, the EDA is acting as a procurement authority, providing

"Defence cooperation is not something that comes about naturally; it has to be incentivised"

satellite communications services to 11 currently participating Member States and the Athena mechanism. The Agency is responsible for contracting and managing the payments as well as for providing technical advice, if required.

Another example of where VAT exemption can be applicable is the Biological Joint Deployable Exploitation and Analysis Laboratory, a new project proposal discussed during the last Steering Board on 17 November 2015. With a current estimation of the project value standing at €4 million, the VAT exemption would allow for €800,000 in savings, which could, in turn, be invested in additional complementary activities.

The key issue remains that the Member States are the immediate and only beneficiaries of the VAT exemption. Additionally, it is up to the Member States themselves to decide if the exemption should or should not be applied, even within the framework of one project, proving the variable geometry of the new financial tool. "Not all Member States have to benefit from VAT exemption at the same time, but the project's outcome has to contribute to European defence," explains Domecq.

Another vital aspect is that the Member States in fact receive "more for less" when working together with the European Defence Agency on collaborative defence projects: they are offered better value for a lower price. This is another takeaway of the VAT exemption, which proves the relevance of more European defence cooperation held under the EDA umbrella.

"I want the Agency to devote its efforts towards structuring capabilities, the capabilities that the Member States want to have, which are not possible to acquire individually, considering the decrease in the defence budgets. We need to spend well, which means we need to spend together, and to integrate the fragmented defence industry in Europe," says Domecq. The EDA Chief Executive is also very positive about the implications of the new regulation, stating that "in the long run, it will lead to a higher number of initiatives and defence projects." As testament to the fact this is not simply lip service, the Agency has already prepared roadmaps for potential future cooperative programmes for which the Member States will be able to benefit from the VAT exemption.

"While the VAT exemption should not be an end in itself, it can become an important driving force for defence cooperation. Any breathing space is appreciated when tight defence budgets limit investments in research, innovation and capabilities. By incentivising defence cooperation financially, we will be able to do more and better together," summarises the EDA Chief Executive.

"VAT exemption is not an objective per se, but it is there to make the Member States understand there is a bonus to defence cooperation in Europe. It generates an attractive business case for cooperative projects and programmes in the framework of the EDA"

Making a difference to capability development

Heads of State and Government endorsed four capability programmes on air-to-air refuelling, cyber defence, Remotely Piloted Aircraft Systems and governmental satellite communications in December 2013. Just recently, Ministers of Defence gave the Agency the green light to work on three new capability projects: a deployable laboratory countering biological threats, anti-tank weapons and medical evacuation. All projects are designed to fill concrete European capability shortfalls

At the last EDA Steering Board, Defence Ministers were briefed on the good progress of the four main capability programmes. Each programme comprises several work strands including technology development, training, regulation or interoperability. "The complexity of the four programmes is their strength. Capability development has to take many factors into account. For each programme we define together with the Member States what the concrete requirements are. Needless to say that these can change in the course of a programme", explains Jorge Domecq, EDA Chief Executive.

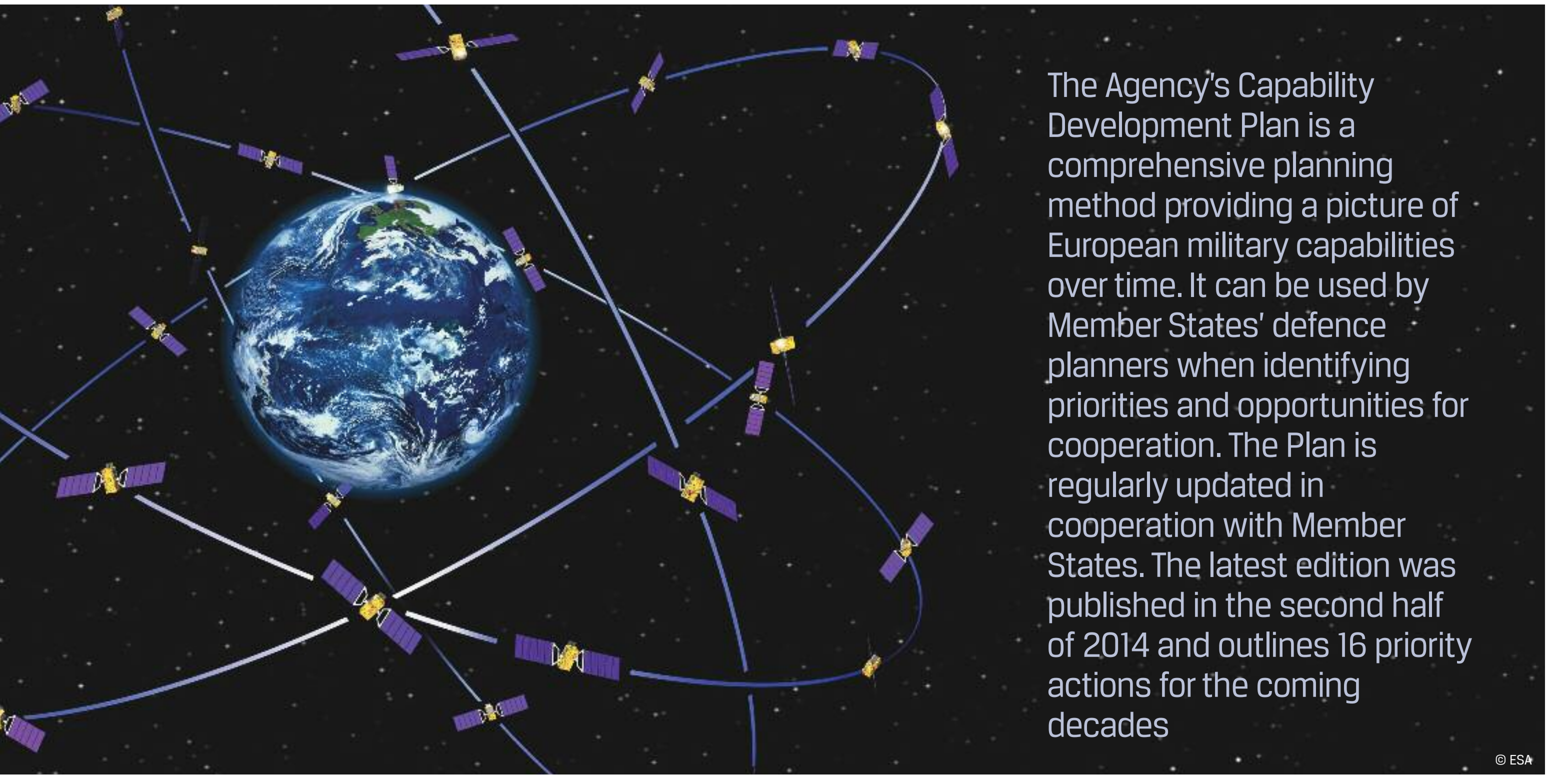
Addressing shortfalls

The mandate to work on air-to-air refuelling is a result of past operations in Mali, Libya and Kosovo where a critical European capability shortfall was exposed. The Agency works on solutions in the short-, mid- and long-term. Regarding the latter, the aim is to increase the strategic tanker capability in Europe by 2020. The procurement process for this capability this capability is advancing quickly. Luxembourg, the Netherlands, Norway and Poland are looking to award the contract in the first half of 2016, with the aim of reaching an Interim Operating Capability by mid-2020. At the same time, the four countries are interested in the participation of additional Member States, in order to achieve synergies with the in-service support on similar fleets in Europe and in training. Work is also on-going regarding the optimisation of existing and future air-to-air refuelling capabilities. Compatibility assessments are currently being conducted on Italian KC767s, and will also soon take place on other tankers such as the A330 MRTT and KC46 to deliver in-flight refuelling clearances to all European receivers.

© Airbus

"In each of our capability programmes you will find elements of classic capability development, armament cooperation as well as research & technology. Additionally we ensure synergies with wider EU policies and entertain close cooperation with our stakeholders. This holistic approach is the true strength of the Agency" *Peter Round, Director Capability, Armament & Technology, EDA*

Heads of State and Government also tasked the Agency to support Member States in elaborating a proposal for a secured satellite communication capability package, coined governmental satellite communications. Under the lead of Spain, this is carried out as direct support to Member States, and in close coordination with both the European Space Agency (ESA) and the European Commission (EC), demonstrating that civil-military synergies are not only an opportunity, but also a reality. Cooperation between the EDA, ESA and the EC is progressing well, with user requirements quickly translated into technical options in a synchronised, transparent manner. Additionally, the Steering Board has just tasked the Agency to better define the governance aspects and proposed mechanisms, which will need to be part of any potential future programme. Success in governmental satellite communications will not only reinforce Common Security and Defence Policy (CSDP) and national capabilities, it will also reinforce



The Agency's Capability Development Plan is a comprehensive planning method providing a picture of European military capabilities over time. It can be used by Member States' defence planners when identifying priorities and opportunities for cooperation. The Plan is regularly updated in cooperation with Member States. The latest edition was published in the second half of 2014 and outlines 16 priority actions for the coming decades

© ESA

confidence in other sensitive cooperative space domains, such as navigation, positioning and timing. In this respect, the Steering Board has confirmed its May 2015 interest in exploring the military dimension of navigation – namely, of Galileo. To this end, EDA will open dialogue with its communities in order to further explore this significant cooperation avenue in Europe.

The Agency's cyber defence programme mainly includes research, technology advancement and collaborative training activities (*see also the cyber defence focus on page 8*). To give an example, the EDA recently started an initiative for the pooling of military demand for private sector cyber training courses. The military often relies on the support of private sector capacities regarding cyber training. The initiative aims to benefit from "economies of scale". Savings are envisaged of up to 30% current expenditures. This initiative could also become part of a potential joint investment programme for cyber defence, for which discussions with EDA Member States have just started.

Regarding Remotely Piloted Aircraft Systems (RPAS), the Agency currently concentrates on three main areas of work. Ministers have just entrusted the EDA to facilitate the development of a dual-use approach to safely operate RPAS in non-segregated airspace. The Agency will work closely with the relevant institutions to develop relevant functional requirements through an integrated aviation safety approach, most notably encompassing the areas of airworthiness, collision avoidance, command and control, satellite communication links and automated recovery. Secondly, the Agency assumes a strong supportive role to facilitate cooperation between Member States in military RPAS operations with a primary focus on common training. Lastly, following the successful inception of MALE (Medium Altitude Long Endurance) RPAS as a future European capability and its on-going transfer to OCCAR, EDA will extend continuous support to the project, especially to the air traffic integration dimension and to efforts to facilitate the integration of additional Member States during the upcoming development phase.

Potential new projects

Given the increasingly volatile and challenging security environment in and around Europe, Defence Ministers have endorsed the Agency's proposals to address other critical capability priorities as identified in the Capability Development Plan: biological joint deployable exploitation and analysis laboratory (Bio-JDEAL), medical evacuation and anti-tank weapons.

The proliferation of biological agents means the biological threat to Member States' forces employed on operations remains real. In order to counter these threats and assess the risk of exposure, a biological laboratory which could be deployed at short notice by a Member State would be able to: a) conduct unambiguous in-theatre biological threat identification; b) provide threat information to command, enhancing the protection of EU forces and local populations and thus limiting casualties; and c) maintain Member States' freedom of movement and action. A dedicated expert group will take up work later this year, with a view to identifying the concrete capability needs by the end of 2016 and a possible project launch by the end of 2017.

The second new project aims at enhancing Europe's medical evacuation capability, an area which is currently characterised by fragmentation and little coordination. However, cooperation, interoperability and common training are paramount, in order for Member States to constitute reliable capabilities in this field. EDA's work will start with a study evaluating interoperability in forward aeromedical evacuation with rotary wings, to be launched later this year. Based on the outcome of the study, the Agency will make proposals for possible cooperative activities regarding interoperability and training.

Another topic of high relevance and interest to Member States is that of anti-tank capabilities. On the one hand, anti-tank weapons are of fundamental importance to national security strategies. On the other, some Member States still have equipment in service that was designed in the late 1970s. In order to move ahead quickly, the Agency, together with Member States, will evaluate different options, including both equipment tailored to urgent requirements and commercial off-the-shelf solutions.

The EDA Annual Conference

The European Defence Agency's Annual Conference is an annual rendez-vous, the aim of which is to help shape defence policies and to identify the most pressing questions relating to the condition of European defence. The grounds for discussion were set by Jorge Domecq, Chief Executive of the European Defence Agency, and Elżbieta Bieńkowska, the Commissioner for Internal Market, Industry, Entrepreneurship and Small and Medium Sized Enterprises. Frontline decision-makers in European defence discussed the future of European capabilities, the defence industry and ways to boost defence cooperation.

Highlights of the conference included special addresses from Federica Mogherini, High Representative, Vice-President of the European Commission and Head of the European Defence Agency, and Jens Stoltenberg, NATO Secretary General. In the second part of the conference, the discussion focused on the areas of defence research considered vital for innovation and the development of future capabilities.

European Defence Ma
s, Member of the EDA
olis, CEO, AKMON & Chairman, H
Material Association-SEKPY
European Defenc
the annual conference by
tence M

EDA Annual Conference: because "European Defence Matters"

On 16 November 2015, the European Defence Agency (EDA) held its annual conference, addressing the most pressing questions relating to the condition of European defence and proposing a way ahead in various defence-related areas. Hosted in Brussels, at the Albert Hall, the conference gathered more than 400 leaders and frontline decision-makers in European defence, coming from the worlds of military, politics, industry and academics

The conference took place at a very significant moment in Europe's history, just a few days after the tragic terrorist attacks in Paris, on 13 November 2015. The conference opened with all guests observing one minute of silence, in order to pay tribute to the victims. In this context, the discussions held throughout the conference referred to important questions, such as: "What is the condition of European defence?" "What is Europe's level of ambition regarding defence?" "What capabilities are already available; which gaps need to be filled and how?" "What is the best way to boost defence cooperation?" "How to reinforce an European industrial base?" and "How can defence research be stimulated?"

In a broader context, the conference precedes two events that are set to shape the future of European defence: the June 2016 release of the Global Strategy on Foreign and Security Policy, currently being prepared by Federica Mogherini, High Representative, Vice President of the Commission and Head of the European Defence Agency, and the NATO Summit in Warsaw, due to take place in July 2016.

European security at stake: keynote and special addresses

"We see security and defence challenges rising in number and complexity. We will only be able to adequately respond to them if the Union's foreign policy ambitions are backed by the right defence capabilities at the right time, supplied by a globally competitive and technologically advanced industrial base in Europe," said Jorge Domecq, EDA Chief Executive. "Political will must be underpinned by action. Cooperation in defence is still not a natural reflex. It needs to become so: to be part of our DNA". At this point Domecq underlined the fact that political decisions need to be translated into military objectives in order to be meaningful.

"Let us keep in mind that the European Union possesses a multitude of policies, instruments, regulations – but few of them take defence into consideration. These tools need to be harmonised. And they need to be used because ultimately they can be of great service for security, defence and our industry," said Domecq. The EDA Chief Executive also referred to the recent decision regarding VAT exemption for EDA programmes and projects, and the possibility of bringing defence research under the umbrella of the EU budget. In times of budgeting constraints rather than lavish spending, such development shows considerable potential. "We need to seize the opportunity to launch effective and pragmatic cooperative programmes that deliver real capabilities. And we should never forget that we depend on our world-leading defence industry for our strategic autonomy. Supporting industry is vital," stressed Domecq.

The significance of European industry was also repeatedly underlined by Elżbieta Bieńkowska, the European Commissioner for Internal Market, Industry, Entrepreneurship,

and Small and Medium Sized Enterprises (SMEs): "We believe that the EU must be able to provide its own security and we believe that the EU should foster international peace and stability: that means having a strong, broad, and competitive European industrial base." Bieńkowska stressed that defence has been given a top priority by the European Commission, which is currently working on a European Defence Plan, in close cooperation with the European Defence Agency and the European External Action Service. "We need to find further synergies between security and defence at the EU level," she said. In detail, she explained that the EU Commission is focusing on a roadmap for European security of supply, support to SMEs and the development of defence research. The Commissioner mentioned the synergies between space and security as a key new area for exploration.

Bieńkowska addressed the issue of defence research funding being reduced by almost one-third in recent years, declaring that "we need to act to reverse the decline and to stimulate defence research." From this perspective, she said she particularly welcomes the agreement signed between the Commission and the Agency regarding the implementation of the first pilot project on defence research, stating that, should this succeed, it will "pave the way for a longer-term defence strategy" and prove that the "European funding of research priorities can be a strong tool to bring all relevant actors together."

"We are desperately trying to meet the challenges of the 21st century with arms and defence structures of the 20th century. We need to become more effective in facing crisis, we have the right tools and structures at our disposal," said Conrad Bruch, Director of Defence at the Ministry of Foreign and European Affairs of Luxembourg, who acted on behalf of Etienne Schneider, Deputy Prime Minister, Minister of the Economy, Minister of Internal Security ando Minister of Defence of Luxembourg. "Only a common response can be effective to provide all the capacities and capabilities," he continued, referring also to the role of the European Defence Agency. The Luxembourg proposals to increase commonalities in common security and defence policy include: the need for decent budgetary perspectives for the European Defence Agency, adequate funding for EU missions and operations, setting a European land transport command, including Common Security and Defence Policy in the new global strategy, and further development of EU-NATO relations.

A prominent feature of Federica Mogherini's address was the development of a new global strategy, to be released in June 2016, with defence and security aspects integrated into each chapter. "The threats we are facing are more complex than ever," said Mogherini. "We cannot afford to act without a rational strategy and a vision of what we want to achieve and how we want to get there." She referred to the wide variety of tools at the EU's disposal, including military ones. "The challenge is to make the full use of all our assets – hard and soft power – in the most effective and coherent way," she said, referring to the hybrid nature of current threats. "When the global strategy is ready, it will have to be translated into military capability needs and implemented with more sectorial papers," added Mogherini.

"Complementarity" was Mogherini's proposal for optimising available tools and capabilities. She stressed that, when it comes to the capability dimension of defence, "there is no security without defence, there is no defence without capabilities, and no capabilities without industry."

"We need to seize the opportunity to launch effective and pragmatic cooperative programmes that deliver real capabilities."

Jorge Domecq,
Chief Executive of the EDA

She also emphasised the important role of the European Defence Agency when it comes to deepening defence cooperation and capability development: "More efficient use of the defence expenditure is precisely why the European Defence Agency plays such a crucial role; its mission is to help reduce the long-standing fragmentation of Europe's defence sector and to deepen European defence cooperation. It allows the Member States to acquire together what is out of reach individually. Crucially, the European Defence Agency is also working closely with the European Commission and Member States both to exploit dual-use technologies, and to support Preparatory Action on Common Security and Defence Policy related research."

Jens Stoltenberg, NATO Secretary General, building on Mogherini's concept of "complementarity" as a defining feature of European defence and security, added a keyword of →

his own: "interconnectivity" – of security, environment and people. Speaking on the nature of EU-NATO relations, he said, "We share the same values and commitment to freedom, democracy, human rights and the view of law. Those values are under threat. Those values must be defended by us. That is why we work together and that is why we will take our cooperation to the next level: not just side by side but also hand in hand." Declaring that "we can achieve far more in partnership," he then listed areas for deepening cooperation, including facing hybrid threats or supporting partners in the neighbourhood. The determination of both organisations to deepen cooperation is now reflected in their choice of words: "must" has been replaced with "can" – an understandable shift, considering the scope of emerging threats on EU and NATO shared territory.

The debate further continued in social media

EU External Action @eu_eeas - Nov 16
.@FedericaMog #Security and #defence will be an integral part of each chapter of #EUglobalstrategy @EUDefenceAgency #defencematters

NATO @NATO - Nov 16
"Terrorism and extremism will not change who we are or how we live our lives." @jensstoltenberg @EUDefenceAgency http://goo.gl/k15f8S

Oana Lungescu @NATOpress - Nov 16
#NATO SG @jensstoltenberg praises #EU for strengthening & boosting #defence coop between EU nations & defence industry @EUDefenceAgency

EU Defence Agency @EUDefenceAgency - Nov 16
Europe needs industrial strategy to better understand where we want to go - Tassos #Rozolis

There was an unanimous agreement among the panellists regarding the necessity for deeper cooperation among Member States and between the EU and NATO, for stronger defence, and for even stronger resolve. The best ways to ensure proper capabilities, the strengthening of the European industrial base and the overcoming of existing barriers, on the other hand, were subject to heated discussions during the two panel talks.

Capabilities setting reference points for defence and security

The panel for the first roundtable debate, "European defence capabilities: what's next?," was made up of Jeanine Hennis-Plasschaert, Minister of Defence of the Netherlands, General Mikhail Kostarakos, Chairman of the EU Military Committee, Giovanni Soccodato, Executive Vice President Strategy of the Markets and Business Development at Finmeccanica and Daniel Koštoval, Deputy Minister for Armaments and Acquisition of the Czech Republic. Their discussions regarding the future of European defence capabilities focused on the present situation of expenditures on defence, the need to translate political will into action and the obstacles in the way to deepening defence cooperation.

"I am convinced that if you want to protect your sovereignty through military means, the only way to do it is by cooperation. The challenges are by definition cross-border so cross-border cooperation is the only way to face up to the challenges," said Jeanine Hennis-Plasschaert, emphasising the need to strengthen Common Security and Defence Policy "not tomorrow; but today, or most preferably yesterday." Daniel Koštoval drew attention to the political, rather than economic, nature of defence, pointing out that "there must be a political will to allocate money and formulate where we are going." He also indicated the lack of overall guidance for European defence. Indeed, "an absence of political will" turned out to be one of the key explanations for the lack of proper measures to reinforce defence cooperation at the EU level.

General Mikhail Kostarakos followed up on this theme, stating that "political will without capabilities is a wishful thinking." He went on to bring up the existing budgetary constraints for capability development: "To do more with less? This we have tried. We have become more cost effective but this has reached its limits: we have started looking combat proven capabilities. If we continue like this, we will do less with less." He pointed out that the recommended 2% Gross Domestic Product spending for defence is not followed by all European Member States. In response to this, Hennis-Plasschaert added that "it is high time we ended military investment in national isolation," and advocated working more closely together and sharing capability plans.

Koštoval pushed forward the concept of "balanced armies," and pointed out that expeditionary missions have been much in defence focus to-date. He emphasised the need for immediate response forces but also for "heavily equipped forces with sufficient fire power," in order to ensure that Europe has "the full spectrum" at its disposal when needed. At this juncture, Koštoval also mentioned the tremendous change that has occurred in terms of the time troops are given to be deployed.

Giovanni Soccodato, as a voice from European industry, stressed the necessity of building efficiency and competitiveness through the establishment of a common European market, in order to avoid losing capabilities. In his words: "Only 12% of European defence Research & Technology programmes are cooperative; 84% of procurement is still national. We need to establish a real common market for European defence; an environment which allows the industry to consolidate."

All the speakers agreed that the rate of progress in terms of developing defence capabilities and strengthening European defence is not satisfactory. They considered the prioritising of sovereignty and national interests to be one of the main obstacles to speeding the process, along with a lack of alignment of focus areas and mind sets. The very same reasons were brought up to explain the difficulty in establishing a real European common defence and security market. "We have very interesting national industrial interests undermining a competitive industrial market in Europe; that is definitely not serving our security needs and our armed forces," said Hennis-Plasschaert.

On a positive note, however, all the speakers noted the important role of the European Defence Agency as a relevant defence capabilities provider at the EU level.

Europe's future defence capabilities dependent upon research

Future capabilities, and the development of existing capabilities, depend heavily on defence research, which is directly linked to innovation in technologies. Over the last ten years, however, the financial scope of defence research has been reduced by one-third, posing a potential threat of future capability shortfalls. According to Mogherini, in order to address this, "we must spend better but we also must spend enough."

The second roundtable talks centred around the topic: "New research opportunities at EU level: a game changer for the industry?" During this session, Michel Barnier, Special Adviser to the European Commission President on defence matters, Antoine Bouvier, President & Chief Executive Officer of MBDA Millie Systems, Ana Gomes, Member of the European Parliament and Tassos Rozolis, Chief Executive Officer of AKMON and Chairman of the Hellenic Manufacturers of Defence and Security Material Association, discussed the requirements to set the level of ambition in Research & Technology, as well as the way ahead.

Michel Barnier opened the discussion, stating: "We are at a capability dead-end; no Member State has the means to ensure the full capability spectrum." He also highlighted the formidable shift that has taken place within technology in recent times: "Some 50 years ago, military research and technology were leading in civilian research and application by maybe ten years. Today, this is not the case anymore. In aerospace, cyber, communication and robotics, civilian research is probably more advanced and also more accessible to non-state actors."

Keeping up with high-paced technological advancement is one thing, however; facing financial constraints leading to reduced capacities is another. Antoine Bouvier raised the point that defence research is a long cycle industry, saying, "We start with technology, then we have product development, production, service support, improvement and evolution of products. If we reduce technology spending, we dry up with sequence. And the challenge is that it is not visible immediately." According to him, it is important, therefore, to underline that the defence industry is a "critical contributor to strategic autonomy."

Tassos Rozolis stressed the need for Europe to develop a European industrial strategy, in order to identify and prioritise needs, "so that the European industry know where they should go." A key issue, in this case, is to ensure that results go along with concrete programmes and procurements.

The Preparatory Action of the European Commission is perceived as another, very important, incentive for defence research. However, it has been underlined that money without a wise strategy to back it up may not lead to favourable results. First and foremost, research has to be capability driven.

Barnier pointed out that this will be the first time that the EU budget will be used for research linked to products and military technologies, explaining that all projects taken under the EU umbrella will have to deliver results within three years and have an EU added value. Possible areas for financing may include key defence technologies necessary for security of supply, technology demonstrators supporting joint programmes or projects in favour of interoperability and common standards.

Ana Gomes added that another important objective is "combining the EU money to steer some programmes and then, of course, making sure that Member States also contribute." "We cannot continue to waste capacities," she stressed.

Research being closely interconnected with industry led to discussions on the condition of European defence enterprises. "Being a SME is simultaneously an advantage and disadvantage. We, the SMEs, are innovative and flexible but we lack the strength and the size of the big companies, so-called 'elephants'," said Rozolis, proposing that the EU encourages big players to cooperate with as many SMEs from various countries as possible.

The topic of balancing the co-existence of SMEs and big players, a clear advantage of the dual-use concept, frequently led the discussion back to the EDA and its critical role in this regard. As Bouvier says: "Working with the EDA is of the utmost importance for the development of the European defence industry."

"We must spend better but we also must spend enough"

Federica Mogherini, High Representative, Vice President of the Commission and Head of the EDA

No alternative to defence cooperation

In his closing words, Jorge Domecq, EDA Chief Executive, summarised the discussions, drawing attention back to the necessity of deepening integration and cooperation, including between the EU and NATO. He set the focus on developing a strong European industrial base as an essential element for the upcoming global strategy, along with proper support for defence research and the exploitation of a dual-use format. He emphasised the need to change the way military requirements are defined in future programmes, and to further develop synergies, particularly in the space domain. Security of supply will be the key to achieve a real single defence market in Europe. Once again, he underlined the fact that European defence matters, and that now is the time for everybody to make it a top priority and move forward. Defence should become a catalyst for the European Union, and the only alternative to more defence cooperation in Europe is more dependency.

› The EDA-Egmont PhD Prize as an incentive for research

Both the European Defence Agency (EDA) and the Egmont Institute are very much in favour of promoting scholars who add value to European research in the field of European defence, security and strategy. This year, ***Dr Andrea Gilli***, a post-doctoral fellow at the Centre for Security Studies, Metropolitan University Prague, received the EDA-Egmont Prize for his academic work on armaments cooperation

The award ceremony was carried out during the EDA Annual Conference of 16 November 2015, and the prize itself was handed over by Prof. Sven Biscop, Director of Europe in the World Programme at the Egmont Institute, and Rini Goos, EDA Deputy Chief Executive. "The practitioner's view comes from accumulated experience, realism, pragmatism and an understanding of the practical mechanics of defence and diplomacy. The academic view on the other hand is blessed by being outside the system and provides objectivity, independence, innovation and analysis in a global context. Together, these perspectives provide a complete picture," said Goos. Prof. Biscop pointed out that the winner of the prize delivered a very courageous thesis, based on extensive and empirical material, that presents very concrete ideas for defence policies.

"I am deeply honoured to be here today to receive this prize, and to share the contents of my research with you," said Dr Andrea Gilli. "In an age of fast technological change and budgetary constraints, we often hear that European countries have to increase their cooperation on future military technologies. Because of the process of technological disruption, cooperation maybe extremely difficult for two single reasons: countries may be reluctant to share technologies and countries legitimately want to strengthen their national rather then European defence industrial base."

"What is the technology that is truly revolutionising warfare?" asked the scholar, before suggesting that Remotely Piloted Aircraft Systems (RPAS) or "drones" – could be the answer. Drawing analogies with some modern civilian technologies being more advanced than others, he concluded that the reason for this lies in a primary focus being placed on facing day-to-day challenges and a subsequent lack of anticipation of future developments. He translated this conclusion into the capability dimension and explained why Europe still has a long way with regard to advancing RPAS technologies. Dr Gilli also referred to the obstacle of allocating an adequate amount of resources to the projects, and to the need to stimulate cooperation between Small and Medium Sized Enterprises (SMEs) and their larger counterparts. ■

The aim of the EDA-Egmont Prize is to encourage and stimulate research on European defence, security and strategy. The award targets dissertations carried out in the framework of a defended and approved doctoral thesis at a recognised academic institution in a Member State of the European Defence Agency. The Prize intends to connect frontline research with European policy making mechanisms, making it a truly significant award.

The jury for the 2015 EDA-Egmont PhD Prize comprised Jorge Domecq, EDA Chief Executive; General Patrick de Rousiers, EU Military Committee Chairman; Dr Antonio Missiroli, EUISS Director; Prof. Jolyon Howorth, University of Bath / Yale University; Dr Hilmar Linnenkamp, Adviser SWP; and Prof. Richard Whitman, University of Kent – under the chairmanship of Prof. Dr Sven Biscop, Director of the Europe in the World Programme at the Egmont – Royal Institute for International Relations.

Key Quotes

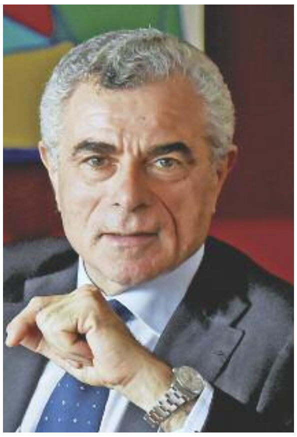
Page 12

"We are living in cyberspace in the condition of 'insecurity by design'. We have to acknowledge that a fully safe and secure Europe is a utopia. But we can do a lot to make it safer. The Agency has completed or initiated cyber defence related projects with a financial volume of approximately two and a half million euros over the last four years."

Wolfgang Röhrig, Project Officer at the European Defence Agency

Page 23

"In a Europe strongly exposed to the risks of deindustrialisation, defence represents a real driver of technological innovation, capable of creating quality employment and generating a positive contribution to the growth and economy of the single countries, and therefore of the whole continent"



Mauro Moretti, Chief Executive Officer & General Manager of Finmeccanica; President of the AeroSpace & Defence Industries Association of Europe (ASD)

Page 26

"Europe has a vibrant and competitive industry, innovative SMEs, and top-level research institutes. **They are a useful and important asset to have at our disposal, but also an asset that we need to work to preserve and strengthen. Governments and the private sector should seek approaches that reinforce one another and create win-win situations. Such Public-Private Partnerships are incentives for more cooperation in the development of European defence capabilities."**

Étienne Schneider, Deputy Prime Minister, Minister of Economy, Minister of Internal Security and Minister of Defence of Luxembourg

Page 32

"All projects and programmes held under the EDA umbrella may be subject to VAT exemption, provided that the EDA adds value to them. Such a financial instrument can be applied so long as the project leads to increasing interoperability, achieving synergies or pooling demand to structure the supply side, thus making a difference for EU defence. It is there to make the Member States understand there is a bonus to defence cooperation in Europe"

Jorge Domecq, Chief Executive of the European Defence Agency

Page 42/43

"We cannot afford to act without a rational strategy and a vision of what we want to achieve and how we want to get there. When the global strategy is ready, it will have to be translated into military capability needs and implemented with more sectorial papers. The challenge is to make the full use of all our assets – hard and soft power – in the most effective and coherent way"

Federica Mogherini, High Representative, Vice President of the Commission and Head of the European Defence Agency

Page 30

As a result of EUNAVFOR MED activities, 16 suspected smugglers and traffickers have so far been prosecuted by the Italian authorities, with 16 boats seized. In addition, ***3399 lives have been saved at sea, including 2546 men, 683 women, 166 children and 4 babies***

Page 44

Only 12% of European defence Research & Technology programmes are cooperative; 84% of procurement is *still national*