EUROPEAN DEFENCE AGENCY

Annual Conference: 23 November 2017

Closing speech by Jorge Domecq,

Chief Executive, European Defence Agency

- This has been a full day of substantial speeches and rich debates which will inspire and guide us in the months ahead. Rather than draw up a set of conclusions that would risk being incomplete, allow to make some comments on what the EDA is called to do in the cyber domain.
- As mentioned earlier today, we are now firmly in the implementation phase of the Global Strategy, which is why we have decided to focus our annual conference on cyber defence, one of the key priority area for the Agency.

- Cyber will no doubt continue to feature high on the European political agenda.
- Open any newspaper on any day of the week, and you'll find headlines about cyber-attacks.

- Be it the WannaCry ransomware which earlier this year crippled the UK's health services, its successor Petya/NotPetya which affected major pharmaceutical, shipping and oil companies, or the hacks targeting national election campaigns, they demonstrate that the threat is real, ever-changing, and has potentially disastrous consequences on our economies, our infrastructure, and of course our citizens' security.
- The so-called Fifth Domain permeates all aspects of contemporary military capabilities. As such, we must systematically strengthen the cyber resilience elements in the development of all future platforms & systems, across land, air, maritime or space domains. Cyber is the business of all capability developers, not just of the techies. It is NOT just an IT problem.
- Cybersecurity, cyber defence and Digital Europe have been at the top of the Estonian Presidency's agenda, and we had the honour to hear from President Kaljulaid today.
- The CYBRID exercise that the Estonian Presidency and the European Defence Agency co-organised earlier this year was the first ever table-top exercise hosted at ministerial level. It yielded valuable lessons on high-level political awareness of cyber threats and challenges and of decision-making processes in this area.

- The fundamental requirements of our armed forces in the cyber domain will continue to be to prepare for, prevent, detect, respond to, recover from and learn lessons from attacks. In a nutshell, to fulfil the core military task of defending citizens under cyber threat conditions.
- Whilst we can all agree that the primacy of capability development is with Member States, we know that there is great benefit from a common coordinated approach on the military dimension of cyber.
- Cyber threats are by nature transnational, and as such national defences cannot suffice. We must coordinate to avoid fragmentation, to ensure and improve interoperability, and to protect special requirements of the military while providing the flexibility for individual Member States to implement stricter requirements if needed.
- To successfully address the cyber domain's threats and challenges, we need capabilities, and we must tackle the ongoing problem of the warp speed development of offensive and malicious technologies.

- Since this is the EDA's Annual Conference, allow me to spell out what we are doing, and what we should be doing, in the cyber domain.

- The EDA has been involved in the entire spectrum of cyber defence, from policy to capabilities since 2011.
- The EU's 2013 Cyber Security Strategy invited the EDA to support Member States in developing EU cyber defence capabilities and technologies, developing a cyber defence policy to protect CSDP missions and operations, improve cyber defence Training & Exercise Opportunities, and to promote civil-military dialogue in the EU, and with international partners including NATO.
- In that respect, the 2014 Cyber Defence Policy Framework defined the modalities to implement the Cyber Security Strategy by promoting complementarities and synergies. Specifically, the Framework set out five priorities:
    - Supporting the development of Member States' cyber defence capabilities related to CSDP;
    - Enhancing the protection of CSDP communication networks used by EU entities;
    - Promoting civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies as well as with the private sector;
    - Improving training, education and joint exercise opportunities; and
    - Enhancing cooperation with relevant international partners, particularly NATO.

- The EDA is an important actor in the implementation of this Framework, working closely with all CSDP stakeholders. While a lot of work has begun, a lot remains to be done, especially in sensitive areas of national responsibility, to cope with rapidly evolving threats.
- Since the start of the EDA's work on cyber defence, the Agency has spent an average of 10% of its Operational Budget on more than 20 cyber defence related activities and projects. These projects and activities are driven by Member States requirements.
- The Agency's work on cyber has covered a whole range of elements, including Education, Training and Exercises, the European cyber defence industry, highlighting a fundamental civil-military component, awareness seminars for CSDP missions and operations, cyber ranges, and cyber in the aviation domain.
- Just this year, the EDA updated its Strategic Context Case on Cyber Defence, laying out the short to mid-term capability development strategy for cyber defence in an EDA context.
- As regards our cyber work in aviation, the EDA this year conducted a mapping exercise of relevant civil and military EU and international stakeholders and is developing a Military Engagement Plan (MEP) for aviation cybersecurity, covering 4 clusters (SESAR, RPAS, Cooperation, Airworthiness & Supply Chain)

- The military needs a high-level coordination mechanism to enable a systemic approach for aviation cybersecurity, including coordination and cooperation with other relevant stakeholders such as the Commission, EU agencies including ENISA and EASA, and other actors notably NATO and the European Space Agency.
- The future lies in technological advances and information will be the enabling vector for advantage on the future battlefield.
- Interoperability is another key subject, on which the EDA stands ready to add value to the work of its Member States.

- As for the future, the EDA's work programme for 2018 to 2020, approved just two weeks ago by the Agency's Steering Board, was the first to be issued after the Long Term Review of the Agency – the so-called LTR-, which identified cyber as one of the principal cross-Agency areas of work.
- We now have both the political and technical mandate to support our Member States in developing their cyber defences, and as such 2018 will see cyber stay centre stage at the EDA.
- First, we will continue to identify and prioritise cooperation opportunities, through the CDP revision and through the conduct of the CARD trial run.

- The findings of a 2016 EDA Table Top Exercise on hybrid threats, which explicitly highlighted the relevance of the Cyber domain, are expected to significantly influence the 2018 CDP priorities.
- Secondly, as we continue to support technology and capability development. In cyber defence, one of our four priority areas as you know, we look forward to seeing the Initial Operational Capability of the CSDP Cyber Training & Exercise Platform next year in close cooperation with the European Security & Defence College. The project on pooling demand for cyber defence training and exercise support by the private sector should also reach its conclusion.
- And thirdly, on facilitating the interface with wider EU policies, we will continue our work on the implementation of the Cyber Defence Policy Framework.
- Engagement with industry will be of central importance to enable our Member States to develop the capabilities they need to stay ahead in tomorrow's cyberspace. In May of this year, Ministers of Defence gave us clear guidance on how to strengthen our engagement with industry along focused priorities.

- It’s important to note that cyber is still a relatively young domain where industrial innovation is often driven by SMEs or start-ups. These industries may not yet be fully familiar with traditional defence procurement. There is a lot to learn for clients and service providers, and areas where the EDA stands ready to support governments and industry alike on matters of industrial capacity, skills, and technology. Our friends in the civilian cybersecurity sector are working towards a Cyber Industrial Strategy, it could be interesting to conduct a similar exercise in the defence sector.
- On research, the development of the first fully-fledged Overarching Strategic Research Agenda – or OSRA), expected by next summer, will provide a governance framework and a way forward.
- The OSRA will be made up of Technological Building Blocks, and those developed by the Working Group on cyber defence received broad support by Member States during the prioritization phase.
- The EDA has supported Member States in the identification of so-called Key Strategic Activities, aimed at developing the technologies, skills and industrial capacities to support strategic autonomy.
- Two proposals were submitted to the European Commission for possible financial support on cyber topics.

- There is an increasing pace of cyber R&T activity within EDA, which demands the right organisational setting. We currently chair an Ad Hoc Working Group but looking to the future, we are considering longer-term organisational solutions, such as a Capability Technology Group (or Cap Tech) Cyber Defence. Not to do so would be odd given the prominence of this area of R&T.
- Cyber requires innovation. New and disruptive technologies must be sought, and we must continually adapt and look forward to the future – to minimise the risk and impact of attacks by adversaries. You all found the latest issue of the EDA's magazine *European Defence Matters* on your seat, which is dedicated to disruptive defence innovations, and which features articles on Big Data, Defence Internet of Things, Blockchain technology in defence, and Artificial Intelligence in cyber defence.
- Our expertise in the military aspects of cyber will determine how we approach the domain across EU initiatives to ensure synergies and efficiency.
- The advent of PESCO could be a game changer for defence, and could offer a welcome cooperation framework for Member States to take forward priority projects.

- The European Defence Fund will offer a new financing opportunity for cooperative projects. Specifically, at the upstream R&T level, it could support the development of technologies identified in the future OSRA, and of related Technology Building Blocks. And until 2020, dual use technologies can be eligible for EU funding under the Horizon 2020 Research Framework Programme.
- And of course the European Commission's new Cyber Package offers a whole new set of possible cooperation areas. This new package, if properly implemented, can contribute to increased security in the Fifth Domain, provided that duplication is avoided and that the specificities of the military dimension are fully taken on board.
- Equally important is our continuous engagement with other parties such as NATO to ensure continued coherence of output, and with industry to secure our future capabilities and the appropriate degree of strategic autonomy.

- Our work to improve Europe's cybersecurity and cyber defence is still in its initial phases. We must lose no time in embracing this golden opportunity to both plan and implement the next steps together. Only in doing so will we ensure that the advent of the digital era remains an opportunity for European citizens in the 21st century.

- Let me once again thank you all for joining us today. I hope you found today's discussions are enriching as I did. My colleagues and I look forward to continuing to work with you on this important capability domain in the months to come.
- Allow me to express my sincere thanks to all the EDA colleagues who worked so hard to make today's conference a success.
- I wish everyone a safe trip home.