Food for Thought Paper by Finland, Estonia, France, Germany, and the Netherlands 17.5.2019

Digitalization and Artificial Intelligence in Defence

As a result of technological developments, the way humans use machines and interact with them is changing. Now it is high time to discuss the consequences for the EU defence sector as well.

Addressing digitalization and related topics such as artificial intelligence (AI)[1] in defence at the European level is indispensable for the development of capabilities of tomorrow. The economic potential of digitalization and AI applications is enormous in the next decade. Investments are market-driven and 'dual-use' commercial off-the-shelf (COTS) technologies and products are used in an innovative way for military purpose. This puts more emphasis on system-integration for the armed forces and requires knowledge of both the COTS AI technology and military platforms. Traditional military stakeholders and prime contractors are challenged by cutting-edge research and development in the private sector, including small and medium-sized enterprises and non-traditional contractors. Given that, these technologies are mainly produced in the commercial civil sector, and noting the remarkable investments of countries like US and China, Europe must keep up with the competition. The development of digitalization and AI in defence will require enablers such as supporting infrastructure, including everything from energy to hardware, software, network resources and services as well as ensuring high quality and quantity of data.

Ethical considerations play a key role in discussing digitalization and AI in defence. Here the EU, with its values, has a lot to offer.[2] The defence administrations should actively take part in this discussion, coordinating their views when needed.

Cooperation is not only essential for success in the EU but also for cooperation with our partners. In the EU–NATO cooperation, for example, thoughts and tools should be aligned from the outset.

This paper poses questions regarding digitalization and AI in defence for discussion during the Finnish Presidency in the latter part of 2019. Furthermore, it is proposed that the EUMC tasks the EUMS to draft a concept paper on digitalisation and AI in defence.

Key questions

1. Disruption and Transformation in Defence

Future battlefields and operational scenarios will be marked by a high level of information transparency paired with immense information density and great speed of processing and assessing that information. In all dimensions, time, speed, and responsiveness will be decisive criteria for the successful conduct of operations. Digitalization is the key.

Digitalization and AI are likely to transform our thinking about security and defence radically. Armed forces have progressively identified short and long-term challenges and opportunities for using AI and systems featuring automated or autonomous functions in future warfare. Advanced AI may even call for fundamental rethinking of security as well as industrial and scientific competences to ensure that armed forces are able to choose technologies for further development and guarantee the security of supply. The next wave of AI[3] requires remarkable resources for research, development and data. As AI comprises of various technologies and applications, the European approach should be focused on the most potential areas[4]. There are multiple possibilities for digitalization and AI defence applications either as a threat or as an opportunity.

[1] EDA presented a Food for Thought paper to the Steering Board (SB) in R&T Directors' composition in December 2018, providing an overview of the field and the Agency's existing activities within the relevant CapTechs (Ref. EDA Food for Thought paper SBID 2018/05 "Artificial Intelligence in Defence"). EDA has proposed a common taxonomy as the first step for further development, coordination and promotion of collaboration on AI (Ref. doc. no. EDA201901130, R&T POC meeting on 24 January 2019: Operational conclusions on the AI topic, 29 January 2019).

[2] For example, the EU High-Level Expert Group on Artificial Intelligence: 'Ethics guidelines for trustworthy AI'.

[3] E.g. https://www.darpa.mil/work-with-us/ai-next-campaign

[4] Government's analysis, assessment and research activities. Finnish AI competencies and how to make them stronger? Policy brief 3/2019. 10 subfields of AI: data analytics; sensing and situation awareness; natural language and cognition; human interaction; problem-solving and computational creativity; machine learning; systems-level architecture, dynamics and complexity; computational environment of AI: platforms and services, ecosystems; robotics and machine autonomy – physical dimension of AI; ethics, morals, regulation and legislation.

EU initiatives such as the European Defence Fund (EDF) and Permanent Structured Cooperation (PESCO) will boost cooperation between member states and European defence industries by leveraging research and development cooperation. Potential of other EU processes and programmes (e.g. CDP, OSRA, CARD, Horizon, Digital EU) must be fully used.

1. Which are the most technologically mature areas for digitalization and AI application for European defence? In which areas would innovative technological solutions potentially be disruptive?
2. How to launch a structured framework to boost European AI research and industry and ensure coherence as well as European awareness of developments in the civil sector? How can the EU mechanisms and institutions contribute?
3. What kind of rising vulnerabilities / threats can be identified in the near future?

2. Impact on Military Capabilities

Digitalization provides armed forces with new capabilities and opportunities both on the physical and virtual battlefield. The spread of digital technology increases information superiority and enhances military capabilities as well as robustness and responsiveness of armed forces on a network-enabled battlefield.

Myriads of possibilities[5] for applying narrow AI (basic tools complementing humans) for defence solutions and military systems have been identified. Main drivers for using AI applications include achieving superior military capabilities, higher cost-efficiency and reducing human workload. Cyber security is important not only in using AI solutions to counter cyberattacks but also in a broader sense in countering security challenges arising from the development of AI such as ensuring data integrity.

1. What are the most relevant and potential European cooperation areas? What kind of digitalization or AI military capabilities should the EU Member States be ready to develop together?
2. What are the possible EU–NATO capability cooperation areas in AI and digital defence?
3. In which capability areas, the armed forces could act as an innovative adapter of civil sector solutions?
4. How to maximize the expertise and competence of relevant stakeholders[6]?

3. Regulatory Aspects

Comprehensive discussion on AI military applications is needed in order to increase European awareness of regulatory aspects. This should contribute to European understanding on how military capabilities possessing autonomous features and functions could be developed and used by applying high ethical standards and in accordance with regulatory framework.[7] For example, sufficient transparency and predictability, reliability of technology, high quality deployment and proper training of personnel using AI based systems are all relevant aspects. A categorical ban on AI or autonomous features is not conducive to wider aim of ethical conduct in military sector. Autonomous weapon systems, as a particular category of AI in military domain, should be discussed and agreed internationally, specifically in the UN CCW forum.[8]

The commercial sector is constantly developing superior technologies, which may be used in innovative ways by military actors. Similarly, the dual use potential in AI solutions needs to be taken into account when drafting standards for usage of AI in various areas of military sector. High ethical standards and policy must be included in developing defence technologies, products and operating principles as a European value itself.

1. How to address different operational environments for military, varying from urban to under water, in research, capability development and deployment of military AI and systems featuring autonomous capabilities and functions?
2. Which operational environments and organisational levels are the most relevant when examining common ethical approaches for AI deployment?
3. How to organise the training of personnel in order to cope with novel and possibly unexpected implications of AI within the ethical and legal framework?

[5] Data collection and analysing, image recognition, simulation tools, logistic models, maintenance tools and unmanned systems are just few examples of these possibilities.

[6] For example, in short-term by utilising existing Centres of Excellence and cooperating with partners by creating a network.

[7] Whilst respecting International Humanitarian Law.

[8] For example United Nations Convention on Certain Conventional Weapons (CCW) on Lethal Autonomous Weapon System (LAWS); cf. https://www.unog.ch/80256EDD006B8954/(httpAssets)/FD148A6783DAC304C12582F30032F633/$file/2018_GGE+LAWS_August_Working+Paper_Estonia+and+Finland.pdf