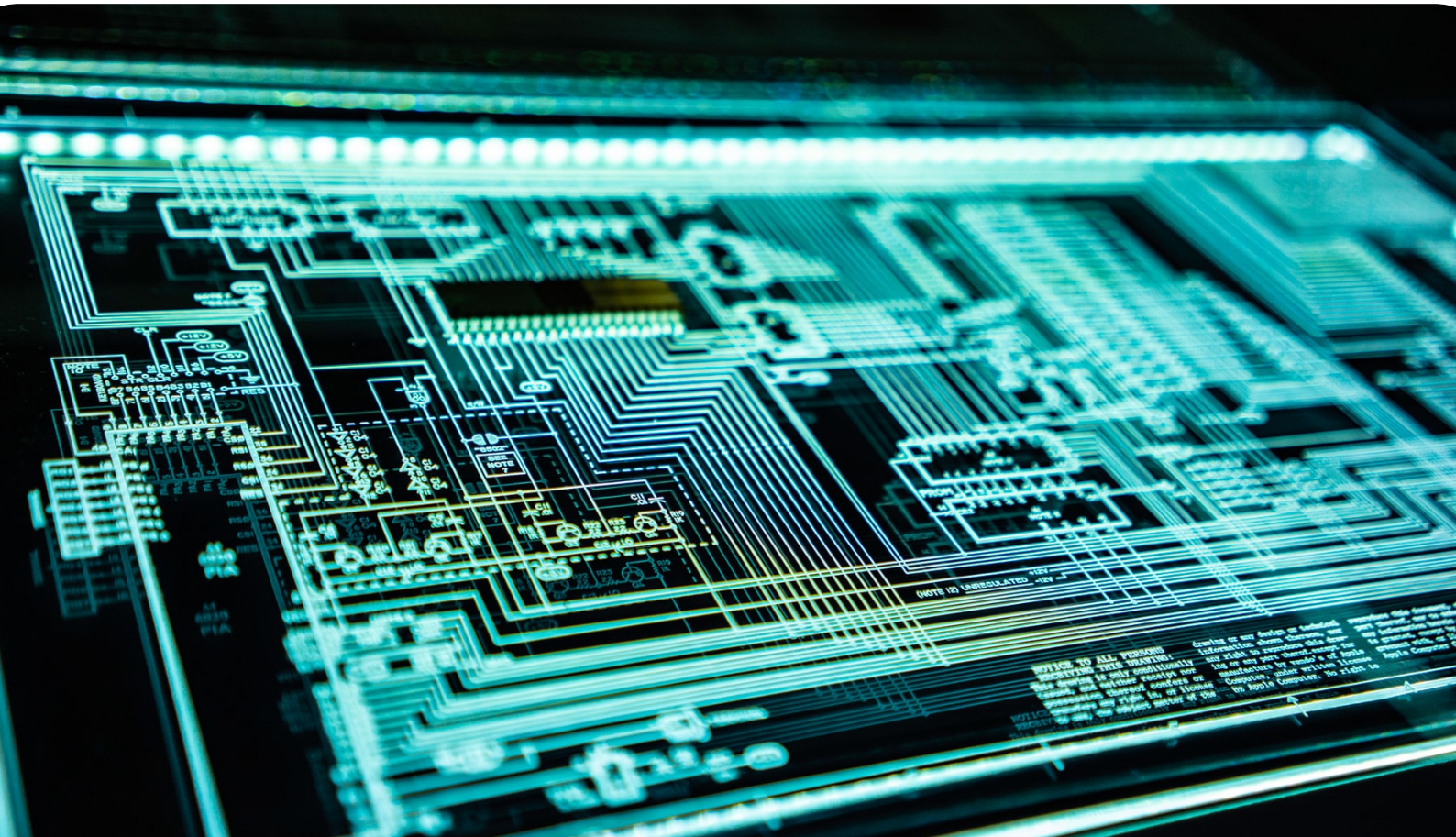
INFO FLASH
Finabel
European Army Interoperability Centre

The ESSOR project: Securing a new system of tactical communications for EU common defence

WRITTEN BY PEDRO SENA

Image credits: https://unsplash.com/photos/EUsVwEOsblE



Introduction: the importance of information and communications technology in today's world of security and defence

In the last decades, the birth of super-fast integrated computer systems and the role of artificial intelligence (AI) in information systems have deeply affected both the civilian sector and the defence and security sectors. Cybersecurity, surveillance systems, state of the art AI, and automated software have played a central role in combating terrorism and establishing effective communication between different organisations without being interfered with or intercepted by the enemy.

The constant development of new technologies within the information and communications technology sector and its central role in the information age have made competing world powers increasingly more competitive with each other in investing in their own industries in order to have the best system and gain a strategic advantage in gaining and managing large quantities of information, with the aim of being economically and militarily more superior.

Both China and the US have strong high-tech ICT industries and are currently developing new systems with artificial intelligence and advanced radio systems. Russia has also made significant advancements and has used them to gain leverage in instrumentalizing them for informational and cyber-warfare and espionage against European democratic societies and the EU.

Consequently, the EU has within this new paradigm of increasing technological competition the strategic geopolitical priority for its defence and autonomy to develop its own high-tech industry for the creation of its own advanced ICT system for the collective defence of the Union and its member states in order to compete with other world powers and have the capabilities that are necessary to secure its interests.

Meeting the challenges of keeping up-to-date with new developments, creating new solutions that effectively protect armed forces, ensuring the successful execution of their missions, and ensuring efficient interoperability is of central importance for the EU.

The strategic plan to develop an effective and united armed force composed of the armed forces of all Member States within the Union is a challenge that can only be overcome with an autonomous communication system used by all the armed forces of EU Member States.

In order for this to be achieved, there must be an effective communication system that is used between all military organisations of the Member States of the EU for operational and tactical coordination success in missions and exercises.

This strategic priority accompanies the changing nature of modern conflicts, where conventional warfare between states is becoming increasingly less frequent. The armed and security forces of modern states have to deal with the new challenges of non-state conflicts, counter-terrorism, fighting extremism, grey zone operations, and one-sided violence against civilians.

In recent years, due to the widespread economic recession in most of the developed world, and specifically Europe, this change in defence has put a strain on public finances, leading to austerity measures reducing the military budget and constraints on political and military capacities to address global and regional security challenges.

Consequently, today, many countries' armed forces face a new reality: having to fulfil mandates with fewer available resources and an uncertain political backing. These conditions have led to a focus on smaller and quicker missions and concepts such as "Pooling & Sharing" military capabilities.

The main idea behind a common ICT system developed and promoted by the EU for its armed forces is that increased flexibility, effectiveness, and inter-organisational, multilateral collaboration will boost collective capacity building, offset budget cuts, and simultaneously promote a strong and autonomous regional and continental defence.

To achieve this goal, increased reliance is put on advanced ICT-based systems to support command and control (C2), intelligence gathering, targeting, logistics, tactical communications and other functions enabling network-centric capabilities through fusing sensor data from multiple systems and platforms within a coalition of actors.

The new paradigm: the challenge of creating a common system for all EU Member State armies

With the digital age and the international integration of computer systems, the world has become globalised through the spread of goods and services, culture, advances in transportation and telecommunications. Through this process of globalisation, existing and emerging threats to the security and safety of modern European societies and their citizens are a central concern of the EU.

Creating an ICT system is a complex challenge. Member States must constantly negotiate which technological and research projects should be given more support.

The creation of a common communication system for all the armed forces of EU Member States also comes with the challenge of ever-evolving technologies that cause communication requirements to have to always explore new means and invest for greater innovation.

Greater amounts of information are continuously needed to provide successful and effective situational awareness, and it should be taken into account that information sharing with collaborating parties is commonly required for active participation in a combined operation, while also having into account that it must be done through a safe system that is resistant to espionage and sabotage by the enemy.

It is commonly believed that having access to more information will result in better decisions. However, as information volumes grow, better information processing is needed to avoid information overloads.

As such, although it is possible to meet these information challenges in security and defence a create a common ICT system for strong interoperability and multi-organisational cooperation, it should be taken into account that when it comes to aspects like cyber security; protection against antagonistic, unintentional or unforeseen threats; and non-technical factors such as education, organisational cultures, and privacy, a given ICT could be of limited utility if these factors are not taken into account while building a common communication system.

The development of a secure and advanced communications system for the EU: The ESSOR project

In an effort to create an advanced ICT system for all of Europe's armed forces, the European Defence Fund has financed a project to create a series of technological projects the best European defence sector companies and corporations that will enable the creation of an interconnected & secured European military software defined radio landscape.

The success of such projects and the standard adoption of this technology by Member States' armies will guarantee the interoperability of EU forces within the framework of joint operations, regardless of which radio platforms are used.

As such, the ESSOR project will provide the EU Member States that adopt it a secure military communications system, improving voice and data communication between their armed forces on a variety of platforms and, consequently, ensure a more effective means of information sharing, giving a greater tactical capability of interoperability in missions between different armed forces. In addition, it will deliver guidelines related to the validation and verification of waveform portability and platform reconfigurability, setting up a common security basis to increase interoperability between armed forces. By ensuring that military radios are fully accessible, shared, and used by all Member States, the effectiveness of joint operations will be increased substantially.

Participating EU Member States in the ESSOR project include Belgium, Germany, Spain, Finland, France, Italy, the Netherlands, Poland, and Portugal (with Estonia and Ireland as observers). These countries have thus already moved towards implementing a common architecture analysis of software radios in Europe.

The ESSOR project activities are currently performed by the consortium A4ESSOR through a contract managed by OCCAr. A4ESSOR is a joint venture between the following companies: Thales (France), Leonardo (Italy), Indra (Spain), Radmor (Poland), Bittium (Finland), and soon Rohde & Schwarz (Germany).

The ESSOR PESCO project presents exceptional technological characteristics both on an operational and tactical level as it is based on state-of-the-art technology in the field of radio and aims to develop the most advanced concepts and solutions for communications applicable to several waveform layers. The project's goal is to build a complete and advanced set of capabilities that will satisfy the most demanding current and future communication requirements for defence and security.

The project is fully supported by the European Defence Agency. By October 2019, the second ESSOR workshop on the development of a "concept of operations" (CONOPS) was already underway at the Agency and allowed participating Member States to gain insight into process and methodology compliant with NATO Architecture Framework version 4.

The focus of the workshop was the discussion and development of the description of operational needs and expectations that the users of the final product of the PESCO ESSOR project expect to have from the tactical level to the command level in order to develop a system that can be put to use effectively.

It analyses operational scenarios using vignettes and identifies categories of architectural information, which are then further developed into operational and technical requirements.

In order to gather better inputs on software-defined radio's role and its performance in the field, a system of questions has been created and distributed to operational staff in EU Member State armies, navies, and air forces to better ensure effective interoperability in military communication and information systems for successful execution of missions and peace-keeping operations in the future.

It should be noted that PESCO has had a central role in promoting this project and aims to jointly develop a coherent full spectrum force package and make the capabilities available to Member States for national and multinational (EU CSDP, NATO, UN, etc.) missions and operations.

Conclusion: the future of the project and centrality for the development of a common ICT system for all European armies

On a geopolitical level, and in an increasingly competitive, multipolar world order, the EU must have a strong autonomous defence capability and be able to have all its members work toward a common defence as a one-armed force to better protect its interests and protect itself from outside threats. The ESSOR project and the development of a common ICT system will play a critical role in this achievement.

It should be noted that the ESSOR project will only play a part in successfully developing a common ICT system. Different Member States negotiating on a common project and on which resources should be allocated to which project is a challenge in itself, and consequently, the development of a functioning strategic conversation space – including mechanisms for information exchange – is a key enabler for inter-organisational collaboration.

It should also be considered that on a tactical level, ICT equipment is usually required for the successful distribution of information. However, how well the involved players interact through the common network, the degree of adherence to rules and protocols, and the level of mutual trust are also relevant factors that play a role in the project's success.

While problems relating to technical issues, such as system heterogeneity, may temporarily hamper communications between the different armed forces of EU Member States, it should also be taken into account that when it comes to effective communication for better interoperability issues such as the lack of common pre-incident planning, commonly set strategic education, interaction training and cumbersome bureaucratic processes are also tactical and organisational challenges that must be dealt with for more effective communication.

It should also be noted that, on a strategic level, these issues are difficult to solve effectively due to the number of different EU members, each with different cultures and ways of communicating.

Bibliography

-European Defense Agency. “EDA supports work on interconnected & secured European military software defined radio landscape”. October 2019
https://eda.europa.eu/news-and-events/news/2019/10/24/eda-supports-work-on-interconnected-secured-european-military-software-defined-radio-landscape

-European Commission. “Action plan on synergies between civil, defence and space industries”. 2021
https://ec.europa.eu/info/sites/default/files/com-2021-70_en_act_part1_v8_en.pdf

-Sigholm, Johan. “SECURE TACTICAL
COMMUNICATIONS FOR INTERORGANIZATIONAL COLLABORATION
The Role of Emerging Information and Communications Technology, Privacy Issues, and Cyber Threats on the Digital Battlefield”. Swedish Defense University (University of Skövde), 2016
https://www.diva-portal.org/smash/get/diva2:1086521/FULLTEXT01.pdf