Questions and Answers: The EU Policy on Cyber Defence

Brussels, 10 November 2022

Why is the EU policy on cyber defence needed?

The cyber domain is increasingly contested and the number of cyber-attacks against the EU and its Member States continues to grow. The Russian attack on the KA-SAT satellite network which disrupted communication across several public authorities as well as the Ukrainian armed forces is an example of how much civilian and defence players rely on the same critical infrastructure. This reinforces the need to secure such critical infrastructure.

To protect its armed forces, citizens, as well as the EU's civilian and military crisis management missions and operations, the EU needs to boost cooperation and investments in cyber defence to enhance its ability to prevent, detect, deter, recover, and defend against cyber-attacks.

The need for a review of the EU's cyber defence policy framework was noted in the 2020 EU Cybersecurity Strategy. Furthermore, President von der Leyen called for the development of a European Cyber Defence Policy in her 2021 State of the Union address. The Strategic Compass for Security and Defence approved by the Council in March this year called for an EU Cyber Defence Policy by 2022. In May, in the Council conclusions on the development of the European Union's cyber posture, Member States invited the High Representative together with the Commission to table an ambitious proposal for an EU Cyber Defence Policy in 2022.

What does the EU Policy on Cyber Defence set out to do?

The EU Policy on Cyber Defence is built around four pillars that cover a wide range of initiatives that will help the EU and Member States to be better able to detect, deter and defend against cyber-attacks. Better and stronger cooperation between the military and civilian actors is the common thread running across all these pillars:

ACT TOGETHER FOR A STRONGER EU CYBER DEFENCE

The EU will reinforce its coordination mechanisms among national and EU cyber defence players, to increase information exchange and cooperation, and further support military Common Security and Defence Policy (CSDP) missions and operations. To this effect, the EU will:

1. create an EU Cyber Defence Coordination Centre (EUCDCC) to support enhanced situational awareness within the defence community;
2. set up an operational network for milCERTs (Military Computer Emergency Response Teams);
3. develop and strengthen the EU Cyber Commanders Conference;
4. develop a new framework project CyDef-X to support EU cyber defence exercises;
5. further develop information exchange between the cyber defence community and the other cyber communities;
6. strengthen common EU detection, situational awareness, and response capabilities through the EU civilian infrastructure of Security Operation Centres (SOCs);
7. establish a mechanism to gradually build an EU-level cyber reserve with services from trusted private providers.

SECURE THE DEFENCE ECOSYSTEM
Even non-critical software components can be used to carry out cyber-attacks on companies or governments, including in the defence sector. This calls for further work on cybersecurity standardisation and certification to secure both military and civilian domains. To this effect, the EU will:

1. provide a platform to support Member States in the development of non-legally binding recommendations for the defence community;
2. develop recommendations on EU cyber defence interoperability requirements;
3. develop risk scenarios for critical infrastructure of importance to military communication and mobility to target preparedness actions including through penetration testing;
4. foster cooperation between civilian and military standardisation bodies for the development of harmonised standards for dual-use products.

INVEST IN CYBER DEFENCE CAPABILITIES

Member States need to significantly increase investments in modern military cyber defence capabilities in a collaborative manner, using the cooperation platforms and funding mechanisms available at the EU level, such as PESCO and the European Defence Fund. To address these challenges, the EU will:

1. update priorities for cyber defence capability development and further support Member States in developing their cyber defence capabilities in cooperation;
2. develop an EU cyber technology roadmap to reduce dependencies on critical technologies using all EU instruments;
3. develop Emerging Disruptive Technologies (EDTs) Strategic Assessment to support long-term strategic investment decisions of Member States;
4. explore with Member States the possibility to develop a set of voluntary commitments for the development of national cyber defence capabilities;
5. develop EU cyber defence training and exercises, including through the ESDC Cyber Education, Training, Exercises and Evaluation (ETEE) platform;
6. establish an EU Cyber Skills Academy, considering needs for specific skills for different professional profiles and sectors of activity, including in the defence workforce.

PARTNER TO ADDRESS COMMON CHALLENGES

Building on existing security and defence as well as cyber dialogues with partner countries, the EU will seek to establish tailored partnerships in the area of cyber defence. In this regard, the EU will:

1. strengthen EU-NATO cooperation in the field of cyber-defence training, exercises, education, situational awareness, standardisation and certification;
2. include cyber defence in EU-led cyber as well as security and defence dialogues with key partners;
3. support partners in cyber defence capacity building, including through the European Peace Facility (EPF).

What has been done since the second Cyber Defence Policy Framework was launched in 2018?

The Joint Communication builds on the Cyber Defence Policy Framework (CDPF) established in 2014 and updated in 2018, as well as the 2020 Cybersecurity Strategy. They have allowed to prepare the ground for many actions proposed in this policy.

In the framework of the Cyber Defence Policy Framework, progress has been achieved in all the six priority areas: supporting the development of Member States' cyber defence capabilities, enhancing the protection of the Common Security and Defence Policy (CSDP) communication and information systems used by EU entities, promotion of civil-military cooperation, development of research and technology, improving education, training, and exercises opportunities and in enhancing cooperation
What will the EU do to step up cooperation within the defence community?

The main goal of this Policy is to strengthen the cyber defence community.

To do that, the Joint Communication proposes to establish the necessary structures for information exchange and cooperation between different military actors. This includes a proposal to create an EU Cyber Defence Coordination Centre (EUCDCC) to support enhanced situational awareness within the defence community. This will be built on currently ongoing PESCO project on Cyber and Information Domain Coordination Centre (CIDCC). The Centre should become the central node for collecting, analysing, assessing and finally distributing cyber defence related information for CSDP missions and operations as well as stakeholders within the framework of CSDP, including Member States, and EU institutions, bodies and agencies upon request.

In addition, the European Defence Agency will establish and support an operational network for Military Computer Emergency Response Teams – MICNET. It will foster a more robust and coordinated response to cyber threats affecting defence systems in the EU, including those used in military CSDP missions and operations.

In order to consolidate the EU Cyber Commanders network and to improve trust as well as to allow exchanges on strategic level information on major cyber incidents, the new Policy proposes to develop and strengthen the EU Cyber Commanders Conference.

Finally, the European Defence Agency will develop a new CyDef-X framework project to support EU cyber defence exercises. This project could also serve to include exercises to test mutual assistance under Article 42(7) TEU.

What will the EU do to enhance cooperation between the defence authorities and the civilian networks?

As everything is interconnected, lines between the civilian and military dimensions of cyberspace are blurred. This is especially seen in relation to cyber-attacks on critical infrastructure, which affect both communities. Thus, cooperation between civilian, diplomatic and law enforcement cyber communities and their defence counterparts will bring high added value to all players concerned. It is therefore crucial to enable such collaboration by providing suitable and secure means for information exchange and engage in exercises and other activities that build trust and mutual understanding.

Once an operational network for military Computer Emergency Response Teams, milCERTs (MICNET) reaches a sufficient level of maturity, the EU will explore options for collaboration with the Computer Security Incident Response Teams (CSIRT) network, which brings together national CSIRTs and the Computer Emergency Response Team of EUIBAs (CERT-EU).

To enable more efficient cyber crisis management, the EU Cyber Commanders Conference would engage with the EU Cyber Crises Liaison Organisation Network (CyCLONE), which brings together Member States and the Commission to support the coordination and management of large-scale cybersecurity incidents in the EU. This engagement will combine military experience and civilian situational awareness at the strategic and operational level.

Whereas the EU Cyber Defence Coordination Centre (EUCDCC) should act as the central node for collecting, analysing, assessing, and finally distributing cyber defence related information, in particular for military CSDP missions and operations, it could also link with the inter-institutional Cyber Crisis Task Force, which was set up to ensure informed decision-making and a coordinated EUIBAs response to major cyber crises at the strategic and operational level. The EUCDCC may also exchange relevant information with a cyber situation and analysis centre which is being set up in the Commission with the support of the European Union Agency for Cybersecurity (ENISA) and CERT-EU to provide analysis and more effective crisis management support.

To address the lack of commonly shared or interoperable secure communication tools and platforms between Member States and the relevant EUIBAs, the Commission and relevant institutions are currently carrying out a mapping of existing tools for secure communication in the cyber field. Based on this mapping, the Commission will present its recommendations to the Council at the end of 2022 to agree on further actions.

What is the EU Cyber Solidarity Initiative about?
The Commission will prepare an EU Cyber Solidarity Initiative to strengthen common EU detection of cyber threats and incidents and situational awareness, as well as preparedness and response capabilities.

Regarding detection and situational awareness, an initiative to promote the deployment of an EU infrastructure of Security Operation Centres (SOCs) based on a first phase will be launched in the coming weeks, which would then be expanded and deployed on a larger scale. This would ultimately be made up of several multi-country SOC platforms, each grouping together national SOCs, with support from the Digital Europe Programme (DEP) to supplement national funding. Legislative changes to DEP would allow longer term financial support for joint procurement of next-generation ultra-secure tools and infrastructure. This would enable the envisaged EU SOCs infrastructure to improve collective detection capabilities by using the latest artificial intelligence (AI) and data analytics. This generation of actionable cyber threat intelligence would allow for timely warnings to authorities and relevant entities to enable them to detect and respond effectively to major incidents. The scale and scope of the infrastructure will depend on the overall funding that can be deployed at national level and by the Union, subject to available budget under the Multiannual Financial Framework.

The EU Cyber Solidarity Initiative will also aim at strengthening preparedness and response actions across the EU. This would include the testing of essential entities operating critical infrastructure for potential vulnerabilities based on EU risk assessments – building on actions already started together with ENISA – as well as incident response actions to mitigate the impact of serious incidents, to support immediate recovery and/or restore the functioning of essential services. The EU Cyber Solidarity initiative could support the gradual build-up of an EU-level cyber reserve with services from trusted private providers that would be ready to intervene at Member States' request in cases of significant cross-border incidents. Roles and responsibilities should be clearly identified and fully coordinated with existing bodies to ensure that the support from the EU-level cyber reserve is provided where it is needed and complements other potential forms of assistance. While the scope of action and allocation of costs of specific interventions would depend on the EU funding available, the EU would also add value by ensuring the availability and readiness of such an EU-level reserve. To ensure a high level of trust, the Commission will also consider the options of supporting the development of cybersecurity certification schemes for such private cybersecurity companies.

How is the new EU Cyber Defence Policy connected to the recent work on the protection of critical infrastructure?

The increase in the number and sophistication of cyber-attacks targeting military and civilian critical infrastructure in the EU was one of the main reasons why the EU Policy on Cyber Defence required an urgent update. The interdependency between physical and digital infrastructure, and the potential for significant cybersecurity incidents to disrupt or damage critical infrastructure illustrate that the EU needs close military and civilian cooperation in cyberspace to become a stronger security provider for its citizens. This is also at the heart of the proposal for a Council Recommendation on a coordinated approach by the Union to strengthen the resilience of critical infrastructure presented last month.

Since armed forces depend to a large extent on civilian critical infrastructure, be it for mobility, communications or energy, the new EU Policy on Cyber Defence aims at enabling the cyber defence community to benefit from stronger civilian and military detection and situational awareness capabilities.

At the request of the Council, the Commission, the High Representative, and the NIS Cooperation Group are developing risk scenarios for digital infrastructure security.

Moreover, the Commission will also propose further actions to strengthen preparedness and response actions across the EU. This would include the testing of essential entities operating critical infrastructure for potential vulnerabilities based on EU risk assessments, the gradual set-up of an EU cyber reserve and the development of an EU Security Operation Centre infrastructure, providing a true cybershield for the European Union.

How is the EU Cyber Defence Policy connected to cyber defence capability development?

Supporting the development of cyber defence capabilities is a key element of the EU Policy on Cyber Defence. To this end, we will make full use of the established set of instruments and initiatives at EU
level. For instance, enabling cyber responsive operations is one of the priorities of the 2018 EU Capability Development priorities. All cyber defence collaborative capability development efforts undertaken in the framework of the European Defence Agency (EDA), within the Permanent Structured Cooperation (PESCO) and under European Defence Fund (EDF) contribute to the implementation of this priority. Similarly, the EDA cyber defence capability technology group has developed a cyber defence research agenda. On this basis, specific collaborative defence research projects focused on cyber technology are taken forward. The Policy also suggests using the Coordinated Annual Review on Defence (CARD) framework to prepare with Member States voluntary commitments on national cyber defence capability development and assess their implementation.

Cyber defence capability development and the research activities connected to it cannot be looked at in isolation from the broader cybersecurity development and enhancement. The EU Cyber Defence Policy encompasses existing and proposed measures and instruments, such as the European Defence Fund (EDF) and the EU Defence Innovation Scheme (EUDIS) in the comprehensive context of an open and inclusive European Defence Technology and Industrial Base (EDTIB). These are seen in the synergetic environment of the cyber domain with extensive spin-in and spin-off effects between sectors.

Defence capability acquisition and operation by the armed forces in the Member States remains their responsibility, but the EU can enhance and enable more efficient cooperation. This is particularly the case for capability elements that are of a dual use nature. The ECDP foresees a cyber defence technology roadmap that will identify the most critical vulnerabilities and the actions to mitigate these in a coordinated and cooperative manner. This will in turn lead to elements for more efficient and innovative development actions and at the end to a stronger cyber defence posture.

What will the EU do to develop a Cyber Defence workforce?

In the context of the 2023 European Year of Skills, the Commission will launch an initiative for a Cyber Skills Academy. It will act as an umbrella initiative with the aim of increasing the number of professionals trained in cybersecurity. It will bring together the different initiatives on cyber skills, and ensure coordination, integration, and a common communication around them. Organised around several pillars of action such as funding, community support, training and certification, stakeholder involvement and knowledge generation, the Cyber Skills Academy will also be able to help the cyber defence workforce.

This will complement efforts undertaken in the framework of the European Security and Defence College (ESDC) to further develop and organise, in cooperation with EDA and Member States, cyber defence training activities and exercises for EU institutions, CSDP operations and missions and Members States' officials. The further development of the ESDC Cyber Education, Training, Exercises and Evaluation (ETEE) Platform will also be explored to generate more training capacities.

How will the European Defence Agency contribute to the implementation of the Cyber Defence Policy?

The European Defence Agency (EDA) supports the identification of priorities for defence capability development and defence research at EU level, as well as their implementation through specific collaborative projects. Enabling cyber responsive operations is one of the 11 priorities identified in the current EU defence capability development priorities. The EDA is currently working together with Member States to update the defence capability priorities, which would trigger additional collaborative projects among Member States. The EDA has also developed a dedicated cyber defence research agenda.

Additionally, the EDA will continue to enhance cooperation within the defence community by supporting the development of a new operational network for Military Computer Emergency Response Teams – MICNET. MICNET will foster a more robust and coordinated response to cyber threats affecting defence systems in the EU, including those used in military CSDP missions and operations. In parallel, the Agency will promote the further development of the EU Cyber Commanders conference, to ensure strategic level information exchange as regards major cyber incidents affecting military operations. The Agency will support the development of links between MICNET and the Cyber Commanders Conference and their civilian counterparts, to enhance information exchange across cyber communities.

The Agency will also further develop its cyber defence exercises, training and education activities, notably through the establishment of a new framework for cyber defence exercises at EU level – CyDef-X.
How will the EU step up cooperation with partners on cyber defence?

Cooperation with partners is crucial. Building on existing EU-led security and defence as well as cyber dialogues, the EU will seek to establish tailored partnerships in the area of cyber defence. In this regard, we will aim at strengthening EU-NATO cooperation further in the field of cyber-defence training, education, situational awareness and exercises, building on the cooperation between NATO's Computer Incident Response Capability (NIRC) and the CERT EU. The EU will also start to progressively include cyber defence topics in EU-led cyber as well as security and defence dialogues. This has already been done in the EU-Ukraine cyber dialogue which took place this September (link to press release). The EU will also continue to support partners, especially the EU candidate countries, in cyber defence capability development, including where relevant through the European Peace Facility (EPF).

What are the next steps?

The High Representative, including in the role as Head of EDA, and the Commission call on Member States to develop the relevant aspects of this Policy on Cyber Defence and will liaise with Member States to define practical measures for implementation. An implementation plan could be established in cooperation with Member States. The results of the implementation of the EU Policy on Cyber Defence will contribute to the overall goals of both the EU Cybersecurity Strategy and the Strategic Compass.

An annual report will be provided to Council to monitor and assess the progress of the implementation of the Policy on Cyber Defence. Member States are encouraged to contribute with their inputs on the progress of the implementation measures taking place in national or in cooperation formats.

For More Information

Press release – The new EU Policy on Cyber Defence
Joint Communication on the EU Policy on Cyber Defence
Factsheet Joint Communication 'The EU Policy on Cyber Defence'
Factsheet on the new EU Cybersecurity Strategy
Factsheet on the Strategic Compass for the EU
Cybersecurity Policies: Digital Strategy

QANDA/22/6643

Press contacts:

Peter STANO (+32 2 295 45 53)
Johannes BAHKKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Sonya GOSPODINOVA (+32 2 296 69 53)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email