EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 10.11.2022
JOIN(2022) 49 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

EU Policy on Cyber Defence

I. INTRODUCTION

The return of war in Europe, with Russia's unjustified and unprovoked military aggression against Ukraine, has been a wake-up call for all questioning the EU's approach to security and defence, its ability to promote its vision and defend its interests, including in cyberspace. Authoritarian regimes are attempting to challenge and undermine the rules-based international order in cyberspace, turning it into an increasingly contested domain along with land, sea, air, and space. Malicious behaviour in cyberspace emanating from both state and non-state actors has intensified in recent years, including a growing number of cyberattacks targeting military and civilian critical infrastructure in the EU as well as in deployed missions and operations.

The lines between the civilian and military dimensions of cyberspace are blurred as seen in the recent attacks on energy networks, transport infrastructure and space assets. It also illustrates the interdependency between physical and digital infrastructure, and the potential for significant cybersecurity incidents to disrupt or damage critical infrastructure. It is a stark reminder that the EU needs close military and civilian cooperation in cyberspace to become a stronger security provider.

The EU needs to take on more responsibility for its own security. This requires modern and interoperable European armed forces. Member States must therefore, with urgency and priority, commit to increase investments in full-spectrum cyber defence capabilities, including active defence capabilities. Whilst remaining fully committed to international law and norms in cyberspace, the EU should signal its willingness to use these capabilities in a coordinated way in case of a cyberattack on a Member State.

To succeed in this, the EU must ensure its technological and digital sovereignty in the cyber field. The EU's capacity to act will depend on its ability to master and develop cutting edge technologies for cybersecurity and cyber defence in the EU. As cyber technologies have a strong dual-use potential, the cybersecurity and cyber defence industries, research and development, and innovation activities must work in a much more synergetic manner to develop better capabilities.

Common prevention and detection are an important part of the EU's defence capabilities. The EU needs to have the capacity to detect attacks in the early stages. Detection data must be turned into actionable intelligence, which can serve both cybersecurity, and cyber defence. Such cooperation between the defence and the civilian cyber communities is the foundation for improved common situational awareness in cyberspace and it is equally crucial for coordinated crisis response at both the technical and operational level.

The armed conflict in Ukraine has also shown the value of close cooperation with the private sector and the necessity of having access to private trusted providers acting as cyber reserves to enhance response in case of major cyberattacks. It is therefore necessary to ensure that Member States can rely on support from trusted cyber reserves, and that this happens in a secure and coordinated manner.

This Joint Communication, while building on the Cyber Defence Policy Framework[1], proposes an ambitious strategy to allow the EU and its Member States to act with self-assurance and

[1] The EU Cyber Defence Policy Framework (CDPF) 2018 Update, 19 November 2018, http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

assertiveness in cyberspace. It aims to boost cyber defence capabilities through the individual or joint action of Member States, and to strengthen coordination and cooperation between the EU cyber communities. It will also work towards reducing the EU's strategic dependencies in critical cyber technologies and strengthen the European Defence Technological and Industrial Base (EDTIB). The policy will set the EU's rules of the game and propose ways to reinforce solidarity at the heart of the EU in the sphere of cyber defence, as well as for cooperating with the private sector to enhance response in case of major cyberattacks. Given the transnational nature of cyber threats, it will develop mutually beneficial and tailored partnerships in the area of cyber defence, including cyber defence capacity building, and enhance the partner countries' cyber resilience.

As proposed in the Strategic Compass for Security and Defence[2] adopted by the Council in March 2022, the present Policy on Cyber Defence will thus enhance the ability to prevent, detect, defend against, recover from, and deter cyberattacks aimed at the EU and its Member States using all means available. This is in line with the Commission's digital priorities, the ambition set out in the 2020 EU Cybersecurity Strategy[3], the announcement of President von der Leyen in her 2021 State of the Union address[4] and the Council conclusions on the development of the European Union's cyber posture[5] of 23 May 2022. The 2022 Joint Communication on defence investment gaps[6] also encouraged the EU and its Member States to launch work towards a full-spectrum cyber defence capability – from research, detection and protection to response.

II. EU CYBER DEFENCE TO PROTECT, DETECT, DETER AND DEFEND AGAINST CYBERATTACKS

1. Act together for a stronger cyber defence

Cyberattacks are often cross-border in nature and may have a physical impact on critical infrastructure in the EU. Significant cybersecurity incidents can be too disruptive for a single or several affected Member States to handle alone. They can also form part of larger hybrid attacks carried out by third countries with the aim to destabilise the economy and society, to weaken critical infrastructure needed to ensure the security of the EU or to undermine and harm the functioning of democracies, including through attacks on election infrastructures.

In 2018, the EU identified cyberspace as a domain of military operations. The 'Military Vision and Strategy on Cyberspace as a Domain of Operations'[7] adopted in 2021 sets the framework conditions and describes the ends, ways and means needed to use cyberspace as a domain of operations in support of the EU's Common Security and Defence Policy (CSDP) operations. Cyber defence and the employment of related capabilities in the entire spectrum of military

[2] A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security
[3] The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final
[4] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701
[5] 9364/22
[6] JOIN(2022) 24 final
[7] EEAS(2021) 706 REV4

cyberspace operations is a national prerogative of Member States, while relying on a wider ecosystem, including a strong industrial base supported by EU-level capability development.

The EU cyber defence community, composed of Member States' defence authorities and supported by EU institutions, bodies and agencies (EUIBAs), has certain specificities in comparison to the other cyber communities[8] and follows a different governance model. The absence of an established framework for information exchange and cooperation among EU military Computer Emergency Response Teams (milCERTs), including in support of military CSDP missions and operations, is problematic in view of the heightened level of cyber threats from state and non-state actors.

Cooperation between civilian, diplomatic and law enforcement cyber communities and their defence counterparts will bring high added value to all actors 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 common understanding.

Furthermore, there is currently only limited mutual operational assistance between Member States. The further expansion of the concept of cyber rapid reaction teams across the EU should be explored, building on the related Permanent Structured Cooperation (PESCO) project Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT)[9], including in the context of Article 42(7) Treaty on European Union (TEU)[10] ('mutual assistance clause') and Article 222 Treaty on the Functioning of the European Union (TFEU)[11] ('solidarity clause'). In a similar vein, one of the lessons learned from the successful Ukrainian cyber defence in the context of Russia's war of aggression is the decisive role played by the private sector. It should therefore be explored to which extent the private sector could also contribute to enhancing cyber response.

1.1 *Strengthening common situational awareness and coordination within defence community*

Given the scale of the risk associated with cyberattacks, Member States need to have the most complete collective situational awareness at their disposal, including early detection capacity as well as the resources to respond properly and recover in a solidary and coordinated manner.

As far as military situational awareness is concerned, there is a need to establish an **EU Cyber Defence Coordination Centre (EUCDCC)** supporting enhanced situational awareness within the defence community, including all EU military CSDP commanders. The High Representative will present the proposal for the EUCDCC for Member States consideration, building on the PESCO Cyber and Information Domain Coordination Centre (CIDCC) project[12]. It will aim to provide a holistic analysis of cyberspace, the electromagnetic environment, and the cognitive domain by bringing together different sources of information to the military strategic and operational levels. Appropriate links should be established between EUCDCC and the EU Intelligence Analysis Centre (EU INTCEN) as well as the EU Military

[8] Civilian, diplomatic and law enforcement cyber communities
[9] Cyber Rapid Response Teams and Mutual Assistance in Cyber Security
[10] Treaty on European Union, Consolidated version: Official Journal C 326, 26/10/2012 P. 0001 - 0390
[11] Treaty on the Functioning of the European Union, Consolidated version: Official Journal C 326 , 26/10/2012 P. 0001 - 0390
[12] The objective of the project is to develop, establish and operate a multinational Cyber and Information Domain (CID) Coordination Centre (CIDCC) as a standing multinational military element.

Staff Intelligence - under the Single Intelligence Analysis Capacity framework. In addition to external information sources, the EUCDCC should establish and integrate an independent active information technology sensor system to strengthen the monitoring of EU-owned nodes supporting military CSDP missions and operations. It will provide stronger detection capabilities and would create a new layer of information to further enhance the information base for cyber risk assessment and situational awareness.

For these purposes, capabilities are required that enable and ensure the establishment and maintenance of a 24/7 operational and where possible recognised picture of cyberspace, including ongoing and imminent cyber operations of both adversaries and friendly forces. Such a picture would contribute to the planning and conduct of EU military CSDP missions and operations. It will thus become the military contribution to making the EU more aware and responsive towards malicious actions in cyberspace.

To improve trust and to exchange reliable and timely strategic information on major cyber incidents, the **EU Cyber Commanders Conference** will be further developed and strengthened[13]. With the European Defence Agency (EDA) acting as secretariat and the participation of the EU Military Staff, it will meet at least twice per year to discuss operational matters and other topics of relevance.

An operational network for **milCERTs (MICNET)** will be established, supported by EDA. All Member States are called upon to participate in MICNET, which is expected to be operational in January 2023.

By facilitating the exchange of information among milCERTs, 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. MICNET will also allow the processes of training and the continuous identification of new requirements for the milCERTs community to be sustained over time. Over the next four years, an information-sharing infrastructure, as well as related tools and procedures, will be developed by EDA together with Member States to support information-sharing between milCERTs. MICNET will also provide the framework for an annual exercise to test, validate and identify new requirements and solutions.

1.2 Enhancing coordination with civilian communities

MICNET should serve as a framework and infrastructure for information-sharing among the different levels within the cyber defence community and external stakeholders.

As MICNET reaches a higher level of maturity, EDA will support Member States in exploring options for collaboration with the **Computer Security Incident Response Teams (CSIRT)** network, which brings together national CSIRTs and the Computer Emergency Response Team of the EUIBAs (CERT-EU). This collaboration could include joint meetings and exercises. The involvement of the private sector in relevant information-sharing and incident response efforts should also be explored.

To enable more efficient cyber crisis management, the EU Cyber Commanders Conference should engage with the EU Cyber Crises Liaison Organisation Network (CyCLONe) network, which brings together Member States and the Commission to support the coordination and

[13] Building on the first two meetings of the European Cyber commanders strategic Conferences (CyberCo) in January and June 2022, EU Cyber Commanders have decided to establish a more permanent forum at their level.

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 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[14], which was set up to ensure informed decision making and a coordinated EUIBA 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.

Furthermore, the lack of commonly shared or interoperable secure communication tools and platforms between Member States and the relevant EUIBAs remains a major obstacle. 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 of existing tools, the Commission will present its recommendations to the Council at the end of 2022 to agree on further actions.

EU Cyber Solidarity for stronger common detection and situational awareness

Civilian support actions can further increase the common situational awareness. The cyber defence community will be able to benefit from stronger civilian detection and situational awareness capabilities developed for the protection of EU critical infrastructure. To this end, the Commission is preparing an initiative to promote the deployment of an EU infrastructure of Security Operation Centres (SOCs) based on a first phase to be launched in the coming weeks, which would then be expanded and deployed on a larger scale[15]. 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)[16] to supplement national funding. Legislative changes to DEP would permit 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, covering civilian communication networks. 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.

[14] An informal group including relevant Commission services, the EEAS, the European Union Agency for Cybersecurity (ENISA), CERT-EU and Europol, co-chaired by the Commission and High Representative.

[15] The EU's Cybersecurity Strategy for the Digital Decade, (JOIN/2020/18 final) and the EU Security Union Strategy (COM(2020) 605)

[16] In accordance with Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, OJ L 166, 11.5.2021, p. 1–34, subject to possible amendment.

Such multi-country SOCs could also allow for the participation of defence entities by establishing a 'defence pillar' in terms of governance and type of information shared. This 'defence pillar' would be developed together with the High Representative and could include a dedicated mechanism for exchanging information with military actors, including EUCDCC, for which defence-level security standards could be developed.

EU Cyber Solidarity in preparedness, response and recovery

Significant cybersecurity incidents are often too disruptive for a single or several affected Member States to handle alone. In such cases, Member States need to be able to draw on mutual assistance and solidarity including in the context of Article 42(7) TEU and Article 222 TFEU. The High Representative, in cooperation with the Commission and Member States, will explore possibilities for the **expansion of the concept of cyber rapid reaction teams (CRRT)**, building on the related PESCO CRRT project, in order to better support EU Member States and CSDP missions and operations. The role of such teams would be to provide tailored and targeted short-term assistance upon request and depending on the specific needs in each case. It could also include, when relevant, options for the support from trusted private partners to ensure efficient response and recovery actions.

As part of the EU Cyber Solidarity initiative, the Commission is preparing 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 –** building on actions already initiated by the Commission 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[17].

The EU Cyber Solidarity initiative could support the **gradual set-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.

Exercises are key element of building preparedness. They foster the development of a common knowledge base and understanding of cyber defence, which in turn enhances operational preparedness. Common cyber defence exercises will also build interoperability and trust between stakeholders, including to support military CSDP missions and operations. Building on the CYBER PHALANX series[18] and the milCERTs exercises, **EDA will establish a new project CyDef-X, bringing together all Member States**, **which will serve as a framework for EU cyber defence exercises**. This project could serve to exercise mutual assistance under Article 42(7) TEU. The use of dedicated cyber defence testing, training and exercises

[17] Nevers Call to Reinforce the EU's Cybersecurity Capabilities
[18] https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx

environments (e.g. Cyber Ranges Federation) should also be explored, including through utilizing the PESCO Cyber Ranges Federations Project[19]

Exercises can also play an important role in improving cooperation between civilian and military entities. When organising exercises, ENISA, EDA and other relevant entities should therefore systematically consider including participants from other cyber communities.

As part of strengthening the EU capacity to prevent, deter and respond to cyberattacks, and in line with the 2020 EU Cybersecurity Strategy and the Strategic Compass, the High Representative will propose in 2023 options for further strengthening the EU Cyber Diplomacy Toolbox[20] drawing from the elements of the EU cyber posture and the lessons learnt from the implementation of the Toolbox since its establishment.

Cyber defence actions

- Establish an EU Cyber Defence Coordination Centre, as the centre for common military situational awareness and explore modalities for cooperation with the Commission situation and analysis centre.
- Further develop and strengthen the EU Cyber Commanders Conference.
- Encourage Member States to actively participate in MICNET, which is the network of Military CERTs, and work towards establishing cooperation with the civilian CSIRT network.
- Develop a new framework project CyDef-X to support EU cyber defence exercises.
- Explore possibilities to further develop the concept of cyber rapid reaction teams, building on the PESCO CRRT project.
- Explore possibilities to further develop Cyber Ranges Federations projects

Civilian support actions

- Prepare an EU Cyber Solidarity Initiative, including a possible Act to make legislative changes to DEP:
    - to strengthen common EU detection, situational awareness and response capabilities.
    - to gradually build an EU-level cyber reserve with services from trusted private providers.
    - to support testing of critical entities for potential vulnerabilities based on EU risk assessments
- Explore the development of EU level cybersecurity certification schemes for cybersecurity industry and private companies.
- Enhance cooperation at the strategic, operational and technical level between cyber defence and other cyber communities

[19] https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

[20] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")

2. Secure the EU defence ecosystem

In recent years, the number of cyberattacks has increased dramatically, including supply chain attacks aiming at cyberespionage, ransomware or disruption. In 2020, the SolarWinds supply chain attack[21] affected more than 18,000 organisations globally, including government agencies, major businesses, and defence companies. The exploitation of a vulnerability in Apache's log4j[22] software highlighted that even software components that are not considered high risk or critical can be weaponised to carry out successful attacks in the EU on major companies or governments, including in the defence domain. This demonstrates a clear need to strengthen further the cyber resilience of entities that are active in the EU defence ecosystem, including military entities, the defence industry, and private operators.

Armed forces depend to a large extent on civilian critical infrastructure be it for mobility, communications or energy. The Russian attack on the KA-SAT satellite network[23] which disrupted communication across several public authorities as well as the Ukrainian armed forces is an example of such interrelation. This demonstrates the need to secure such critical infrastructure.

To address issues related to the security of their communication and information systems (CIS), Member States are developing their own security standards and requirements for military systems, which do not always consider the need for interoperability, nor the existence of civilian standards for dual-use products. This has a negative impact on the capacity of Member States to act together in cyberspace, also in the context of military CSDP missions and operations, and it creates obstacles for mutual assistance. Furthermore, it is also necessary to promote stronger synergies between military and civilian standardisation tracks as having to follow similar but different standards for civilian and military customers increases production costs for the development of dual-use products by industry.

2.1. Enhancing the cyber resilience of the defence ecosystem

Enhancing the cyber resilience of the defence ecosystem requires targeted actions and investments across a broad range of entities from Member States' military infrastructure and CSDP missions and operations to critical infrastructure, defence industry and relevant research entities.

The protection of information required for informed decision-making is necessary for successful CSDP missions and operations. The EU and its' Member States need to strengthen their military command and control structures further and develop and secure their infrastructure. This also holds true for political-military consultation in the early stages of crisis management for the effective employment of the operation headquarters, including the Military Planning and Conduct Capability (MPCC). This will be in particular addressed through the further development of the EU Operation Wide Area Network.

[21] https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/
[22] https://english.ncsc.nl/topics/log4j-vulnerability
[23] Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine: https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/

In the context of military missions and operations, cyber defence actors are dealing with information of different formats, classifications, coming from different sources. This makes the application of secure state-of-the-art technology, such as AI, with the support of industry of utmost importance.

The security of CIS infrastructure needs to be improved by applying mutually agreed management procedures, thus fostering trust in the integrity of information available among stakeholders. In addition, the High Representative including in the capacity as Head of EDA, with the support of the Commission, will assist Member States with the development of **non-legally binding recommendations for the defence community**, **inspired by the Directive on measures for a high common level of cybersecurity across the Union (NIS2)**[24], as defence is excluded from the scope of the Directive. This will contribute to an increased overall cyber defence maturity.

The Commission proposal for a Cyber Resilience Act[25], which aims to lay down cybersecurity requirements for products with digital elements, will also further reduce the attack surface in dual-use products used for instance in CIS by the defence industry and government defence actors. According to the proposal, manufacturers would be required to report actively exploited vulnerabilities within 24 hours to ENISA, which will inform the relevant national CSIRTs. In this regard it would also be important to ensure that the defence community is swiftly informed about vulnerabilities in products with digital elements, as well as of any available and/ or applied patches and mitigating measures.

All the more so in the light of the dependence of the military on civilian critical infrastructure, **there is also a need to further increase the protection of critical infrastructure against large-scale cyberattacks**. At the request of the Council[26], the Commission, the High Representative and the NIS Cooperation Group[27], are developing risk scenarios for digital infrastructure security. The focus will in the first instance be on cybersecurity in the energy, telecoms and transport sectors, and space. In addition to this, targeted cybersecurity risk assessments for communications infrastructure and networks in the EU (including fixed and mobile infrastructure, satellite, undersea cables, and internet routing) will also be prepared[28]. Regarding the protection of critical infrastructure against man-made threats, including hybrid threats, the proposal for a Council Recommendation on a coordinated approach by the Union to strengthen the resilience of critical infrastructure[29] calls on Member States to ensure appropriate stress testing and crisis coordination, among other things. The maritime critical infrastructure, including the protection of undersea data cables, will be further addressed through the forthcoming revision of the EU Maritime Security Strategy and its Action Plan.

[24] Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 that has been recently agreed by co-legislators and is expected to be formally adopted by the end of this year.
[25] Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final
[26] Council conclusions on the development of the European Union's cyber Posture; ST09364/22, 23 May 2022
[27] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
[28] Nevers Call to Reinforce the EU's Cybersecurity Capabilities
[29] Proposal for a COUNCIL RECOMMENDATION on a coordinated approach by the Union to strengthen the resilience of critical infrastructure, COM/2022/551 final

Further actions to strengthen the cybersecurity of critical infrastructure in the energy system is set out in the EU action plan for digitalising the energy system.[30]

Space-based services are of increasing relevance for defence, whether they are for surveillance, situational awareness, precise positioning, or ultra-secured communication. They are therefore key strategic assets for technological sovereignty. Disrupting space-based services could have a major impact on defence systems but also on the overall society and economy. Their resilience is central to the overall cyber defence resilience, as they can be targets of malign attacks. In particular, as seen with the attacks on KA-SAT networks, space systems are increasingly exposed to cyber threats that can affect the availability or continuity of space-based services. This creates a risk for the EU's strategic and security interests in the space domain, and also for space capabilities enabling and assisting cyber defence. The EU Space Strategy for Security and Defence announced in the Strategic Compass[31] will outline measures to improve the robustness and cyber resilience of space infrastructures and related services and to deter and respond to any threats on sensitive space systems and services in the EU, addressing specifically cyber threats.

The Commission also calls on Member States to urgently achieve the implementation of the measures recommended in the EU Toolbox on 5G Cybersecurity[32]. Member States which have not yet enacted restrictions on high-risk suppliers should do so without further delay, considering that time lost can increase vulnerability of networks in the EU. Such risks can be relevant for military assets and can have an impact on the overall defence environment of the Member States.

Regarding the **cyber resilience of the European defence industry as well as defence research and development entities**, such entities are covered under the scope of the NIS 2 Directive unless explicitly excluded by Member States. This would require such entities to have a cybersecurity risk-management programme in place that includes supply chain security as well as incident reporting. As the private sector plays a big role in cybersecurity service provision in the defence ecosystem, Member States should furthermore make use of cybersecurity certification schemes. An **EU cybersecurity certification scheme for companies providing services to defence industry** could be explored as a way to bring a harmonised level of trust to the market, building on the experience of ENISA.

2.2. Ensure EU cyber defence interoperability and coherence of standards

Interoperability and commonality are important requirements to consider from the design phase of cyber defence capabilities, also taking into account the lessons learned from ongoing missions and operations as identified under the lead of the EU Military Staff, with the support of EDA. The principles, processes and standards that are agreed within the Federated Mission Networking (FMN)[33] framework should provide the guiding elements for the development of national cyber defence capabilities to ensure interoperability.

[30] Digitalising the energy system - EU action plan COM/2022/552 final

[31] A Strategic Compass for Security and Defence, 21 March 2022 https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

[32] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures | Shaping Europe's digital future (europa.eu)

[33] https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx

Collaborative efforts can be facilitated by harmonising requirements for next-generation cyber defence capabilities, which might possibly lead to joint development and procurement initiatives and integrated life-cycle support. For this reason, EDA and EU Military Staff will develop **recommendations on a set of EU cyber defence interoperability requirements**. Those requirements must be considered throughout all planning horizons to guarantee all aspects of standardisation as the critical enabler for interoperability. Requirements for testing, evaluation and certification are other critical enablers.

Harmonised standards for cybersecurity will be developed for hardware and software products and components in the context of the proposed Cyber Resilience Act[34]. Such standards will concern all civilian and dual-use products with digital elements, which make up a large share of the products used in defence sector. Where possible, the Commission will encourage coherence with defence-related cybersecurity standards for digital products. As set out in the Action plan on Synergies between civilian, defence and space industries[35] (the 'Synergies Action Plan'), the Commission in close cooperation with key stakeholders will present a plan to promote the use of existing hybrid civil/defence standards and the development of new ones . Cooperation should further develop between all relevant stakeholders, including European standardisation organisations, North Atlantic Treaty Organization (NATO) and other partners, making best use to that end of the European Defence Standardisation Committee. In a similar vein, when military standardisation bodies develop new cybersecurity-related standards for products with digital elements for defence use, harmonised standards developed under the Cyber Resilience Act should be used as a baseline[36].

Cyber defence actions

- Support Member States in the development of non-legally binding recommendations for the defence community, inspired by NIS2, to contribute to an increased overall cyber defence maturity at national level.
- Develop recommendations on EU cyber defence interoperability requirements.
- Enhance cooperation with all relevant actors on defence-related standards in the framework of the European Defence Standardisation Committee.

Civilian support actions

- Develop risk scenarios for critical infrastructure of importance to military communication and mobility to target preparedness actions including through penetration testing.
- Foster cooperation between civilian and military standardisation bodies for the development of harmonised standards for dual use products.

3. Invest in cyber defence capabilities

[34] COM/2022/454 final
[35] COM(2021) 70 final
[36] Standardisation work is currently ongoing in relation to cybersecurity requirements concerning radio equipment, on the basis of Delegated Regulation (EU) 2022/30. If the Commission repeals or amends this delegated regulation with the consequence that it ceases to apply to certain products subject to the Cyber Resilience Act, the Commission and the European Standardisation Organisations should take into account the standardisation work carried out in the context of Commission Implementing Decision C(2022)5637 on the standardisation request for the above-mentioned delegated regulation in the preparation and development of harmonised standards to facilitate the implementation of the Cyber Resilience Act.

Over the past years, investments in cyber defence in the EU have increased against the background of growing malicious cyber activities by state and non-state actors. It is critical that the EU strengthens its cyber defence capabilities. Russia's war of aggression against Ukraine further reinforces the need for increased investments, to ensure that Member States have state-of-the-art cyber defence capabilities, both stationary and deployable.

Technology improvements are essential to maintain an advantage over competitors and adversaries, who are also investing heavily in new technologies. Therefore, the EU and Member States also need to enhance their cooperation and interoperability on cyber defence through joint capability development and increased investments in research and development.

In addition, vulnerabilities stemming from strategic dependencies and the fragmentation of the EDTIB[37] need to be addressed. In particular, skills and competences are essential to overcome strategic dependencies on cybersecurity and cyber defence in Europe. The European defence industry needs to retain key skills and acquire new ones to remain in a position to deliver high-tech solutions in a global setting[38]. A lack of skills has a negative impact for the defence sector, as it hampers capability development in all domains. All actions will be fully in line with the approaches announced in the Synergies Action Plan, the Roadmap on critical technologies for security and defence ('the Roadmap')[39] and the Gaps Analysis[40].

3.1. Develop full-spectrum state-of-the-art cyber defence capabilities

Member States bear the responsibility and competence to use cyber defence capabilities, whereas the EU plays an important role in supporting the further development of specific military capabilities across the Doctrine, Organisation, Training, Materiel, Personnel, Leadership, Facilities and Interoperability (DOTMLPF-I) spectrum to create freedom of action in cyberspace. There is a need to unify further the approach to cyber defence across all capability domains and to adapt it to the changing geopolitical environment. It is therefore necessary to identify the missing elements in existing capabilities and support the development of new capabilities in a coordinated and measurable manner.

However, the level of engagement of Member States in collaborative cyber defence development projects remains insufficient to date and should be increased to maximise the impact at the EU level. All Member States must increase their investments in developing full-spectrum cyber defence capabilities and develop these in a collaborative manner. Member States should consider **developing a set of voluntary commitments for the development of national cyber defence capabilities**, also multinational capabilities beyond existing PESCO cyber defence projects[41]. The Coordinated Annual Review on Defence (CARD) process could be used to start a dialogue with Member States on cyber defence requirements and national

[37] E.g. as identified in the Defence Investment Gaps Analysis

[38] Several initiatives have been launched, e.g. the European Defence Skills Partnership.

[39] The Commission in the Roadmap on critical technologies called to reinforce cooperation on technologies that are critical for Europe's long-term security and defence and efforts to reduce related strategic dependencies.

[40] The Joint Communication on the Defence Investment Gaps Analysis and Way Forward where the Commission and the High Representative have proposed several measures to ensure that the EU's industry is equipped to deliver both in the short and long run.

[41] Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT), Cyber and Information Domain Coordination Centre (CIDCC), Cyber Threats and Incident Response Information Sharing Platform (CTIRISP), Cyber Ranges Federations (CRF), EU Cyber Academia and Innovation Hub (EU CAIH).

objectives for cyber defence capability development and assess implementation of the commitments. The Commission is supporting and co-financing full-spectrum cyber defence capability development and research, including for active defence capabilities, through the European Defence Fund (EDF). The Commission has already increased investments in cyber defence through the EDF, which should lead to the development of European common and/or interoperable tools for cyberspace operations and incident management, information warfare defensive operations and preventive measures, and improved resilience of CIS systems. It targets areas such as cyber situational awareness, real-time threat hunting and responsive operation capabilities, cyber operation capabilities and cyber trainings and exercises[42]. To ensure that Member States are able to conduct joint cyber-operations, responsive operations and cyber operations capabilities will be supported under the EDF in upcoming years. Finally, Member States are encouraged to actively engage in the different cooperative frameworks and use all instruments set up at EU level, including the EDA Project Team Cyber Defence[43].

The ongoing revision of the 2018 EU Capability Development Priorities[44] represents a timely opportunity to define updated priorities for cooperative and collaborative development, in turn enabling such an increase in cooperative capability development. The review of the cyber defence specific priority should take into account the outcome of the 2022 CARD, as well as the findings of the Gaps Analysis presented to Member States in May 2022. Subsequently, the CARD will offer a regular framework to review progress on the implementation of this updated priority at national level, and explore new emerging options for collaborative development of cyber defence capabilities with Member States. The updated EU Capability Development Priorities will serve as key reference for PESCO projects on cyber defence.

In this regard, based on the tasking from the EU Military Committee, the EU Military Staff will develop the Cyber domain operations implementation plan in close coordination with Member States to provide an overview of the state of play of the implementation of cyber defence capabilities as well as to provide support to Member States to better align their efforts and activities. These efforts are based on the EU Concept on Cyber Defence for EU-led military Operations and Missions echoing the priority settings of the Capability Development Plan (CDP).

Enhancing research efforts on key technologies for cyber defence

Sustaining state-of-the-art cyber defence capabilities requires staying abreast of technological developments and their applications in defence-related systems, in particular of emerging and disruptive technologies (EDTs, e.g. AI, encryption and quantum computing)[45]. In particular, the EU needs to invest in post-quantum cryptography to ensure that its defence systems remain secure. Given the fast pace of technology, collaborative research and technological development efforts need to be tailored to reach a sufficiently advanced technology readiness

[42] Under the European Defence Industrial Development Programme (EDIDP), 6 projects have been funded (PANDORA, DISCRETION, CYBER4DE, ECYSAP, SMOTANET and HERMES) with a budget of 39 million EUR. Under EDF 2021 almost 40 million EUR will be devoted to 3 collaborative cyber defence R&D projects selected for funding (ACTING, AInception, EU-GUARDIAN)

[43] The Project Team Cyber Defence provides a forum for Member States to discuss cyber defence matters with military implications.

[44] EDA CDP factsheet (28.06.2018): CDP Factsheet

[45] As identified in the cyber defence Strategic Research Agenda and in the Overarching Strategic Research Agenda (OSRA)

level so that their outcome can be more quickly incorporated into existing and future capabilities.

The Commission under the EDF is funding technological innovation for defence and supporting the development of emerging and disruptive as well as cutting-edge technologies, including for cyber defence. Up to 8% of the EDF budget is allocated to topics addressing disruptive technologies for defence, including some topics pertinent to cyber defence. Special attention under the EDF in forthcoming years will be given to research actions and projects addressing new technologies developed against emerging and evolving threats as well as increasing resilience, cybersecurity and their integration into defence capabilities.

In line with the EDTs Action plan[46], EDA will annually inform Member States on the landscape of emerging technologies, including those applicable to cyber defence. Furthermore, EDA will develop the European EDTs Strategic Assessment to support Member States in taking long-term strategic directions, identifying synergies and collaborative opportunities. The European Cybersecurity Competence Centre (ECCC) will adopt a strategic agenda for investment in key cybersecurity areas, which in turn will guide the preparation of future work programmes of the Digital Europe and Horizon Europe programmes in relation to cybersecurity, respectively supporting research, innovation and market uptake. To foster synergies, ECCC and EDA will also develop a working arrangement to facilitate information sharing among respective staffs on respectively civil, dual use and defence technology priorities.

Acting on the technology needs for cyber defence

Further action and coordination is needed to ensure that the rapid technological evolution in the cyber domain is swiftly taken up by the defence sector. This includes stepping up efforts to identify critical technologies for cyber defence and cybersecurity that should be prioritised to reduce technological dependencies of the EU and assess whether current priority setting and funding instruments sufficiently address these dependencies.

For this, the Commission together with EDA and the Member States will propose in 2023 a **technology roadmap for critical cyber technologies** based on relevant consultations, including with industry where appropriate. The technology roadmap will identify cyber technologies important for the EU´s technological sovereignty, cover both cyber defence and cybersecurity, map technological developments and strategic dependencies and act to reduce them. The cyber technology roadmap will inform strategic priorities for the EU's funding instruments and will propose taking full advantage of civil and defence research and development and capability development programmes and funding instruments in line with their respective governance rules. It will also propose further ways to encourage the development of dual-use research, technology development and innovation on cybersecurity and cyber defence at EU and Member States level.

In this context, the Commission[47] in cooperation with the ECCC and EDA in 2023 will assess technologies that have already been identified as critical for cyber defence and will, possibly with the support of the Observatory of Critical Technologies, map and identify existing

[46] The 'Emerging Disruptive Technologies (EDTs): A capability-driven Action Plan' was approved by the EDA Steering Board in Research & Technology Directors composition on 16 December 2021.
[47] Including JRC

dependencies further[48]. This will take into account work undertaken in the context of the EDA's Annual Monitoring Document[49] and European EDTs Strategic Assessment[50]. Furthermore, the ECCC could launch a dedicated policy support project which could feed into the process of technology roadmapping and bring together and engage with relevant stakeholders from the civilian and military spheres.

As part of the activities outlined under the Synergies Action Plan, the Roadmap and the Gaps Analysis, several actions are already ongoing to strengthen the synergies to exploit better the full potential of dual-use technologies, including in the cyber domain.

Additionally, Member States are encouraged to make full use of the existing initiatives supporting research and technological development, namely for defence the EDA defence Capability Technology Groups[51] and the related OSRA Technology Building Blocks[52], EDA Ad Hoc framework[53], the EDF and PESCO. For civilian and dual-use technologies the ECCC and Network can manage projects with both a defence and civilian dimension as established by its legal base[54].As announced in the Synergies Action Plan and the Roadmap, the Commission will also seek to strengthen synergies between the activities of the ECCC and the EDF in cybersecurity and cyber defence, in line with the EDF governance rules.

3.2. Agile, competitive and innovative European defence industry

The EU needs a strong, agile, competitive and innovative European defence industry, which is capable of delivering a full spectrum of state-of-the-art defence capabilities, including cyber defence capabilities. However, where cyber defence is concerned, the EU defence industry currently relies substantially on civilian solutions and on external markets to provide state-of-the-art solutions. Although technological advances in the civilian domain are rapid and the market for civilian information and cybersecurity products is growing quickly, there are specific military requirements that are not fulfilled by off-the-shelf civilian products. Important parts of hardware and software currently used for cyber defence are not made in the EU, which can create industrial and technological dependencies. The EU also lacks a strong presence in the global cybersecurity and cyber defence industry. Its highly fragmented **EDTIB** greatly

[48] Observatory of critical technologies, announced in the Action plan on synergies between civil, defence and space industries.
[49] First phase of the EDA 2021 EDT Action Plan.
[50] Second Phase of the EDA 2021 Action Plan.
[51] CapTechs provide Member States' experts with a networking fora and a flexible framework for collaborative projects. More information on the CapTechs related to cyber (Cyber, Information, Components) is available at: https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs).
[52] OSRA maps relevant defence R&T areas and details concrete collaborative opportunities. There are 17 Technology Building Blocks along with their technology roadmaps associated to cyber technologies addressing cyber defence situational awareness, the protection of military communication systems, processing information from heterogeneous sources, modelling and simulation, quantum computing and cryptography, as well as exploring synergies between cyber operations and electronic warfare. Artificial intelligence and big data have a key role in information processing.
[53] The EDA Ad Hoc Framework is defined by Council Decision (CFSP) 2015/1835. Currently, 6 projects with cyber technology elements are under execution in this framework, with a budget of approx. 20 million EUR (ANQUOR, CERERE, EDA SOC 2, MASFAD II, PASEI II, ASSAI).
[54] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

reduces its ability to improve its competitiveness[55], with the majority of the cybersecurity companies in the EU being small and medium-sized enterprises (SMEs)[56]. Having a technologically sovereign industrial capacity is a cornerstone for the EU's capacity to act.

The EU is supporting the development of a strong EDTIB through a range of programmes and initiatives. Whereas the EDF is funding technological innovation for defence and supporting the development of technologies that eventually leads to jointly developed cutting-edge military capabilities and contributes to the competitiveness of the EU defence industry, Horizon Europe and the Digital Europe Programme support cybersecurity research and the development of dual-use technologies including quantum, encryption, secured cloud and AI[57].

Further actions related to critical technologies for cyber defence and industrial needs as identified by the **technology roadmap for critical cyber technologies** should be addressed. It is necessary to identify appropriate support streams, for example to stimulate common procurement efforts, such as through the future European Defence Investment Programme, or facilitate access to equity and loans through the European Investment Fund and the European Investment Bank.

For a strong EDTIB, exploiting and leveraging synergies between civil and defence companies needs to be ensured. Innovation actions as proposed under the EU Defence Innovation Scheme (EUDIS), including outreach to SMEs and technology scouting, could have a positive impact for the EU defence industry and EDTIB.

The Commission will also launch an industry dialogue with the purpose of developing the EU's cyber defence industry, involving as appropriate EDA.

The Commission and the High Representative propose to put in place several measures to make sure industry is equipped to deliver in the short and long terms. This entails, in the immediate term, an in-depth mapping of EU defence industrial manufacturing capabilities, to identify precisely gaps and areas where ramp up is needed.

The reduction of critical dependencies in the field of cyber, such as may be identified in technological roadmaps, could also be addressed by the new European Sovereignty Fund announced by President von der Leyen in her September 2022 State of the Union address.

The EU Foreign Direct Investment Screening Framework will continue to be used to mitigate the risks of acquisitions of European technologies or solutions that present risks as it comes to defence and security risks. Member States that have not yet set up national screening mechanisms should do so without delay.

3.3. EU cyber defence workforce

Europe is facing a real and alarming cyber skills gap, with the European Cybersecurity Organisation (ECSO) estimating a total of 500 000 professionals needed already now in 2022.

[55] As identified in the Joint Communication on the Defence Investment Gaps Analysis and Way Forward.
[56] The total number of SMEs in the EU, operating in the multi-layered and often trans-border defence supply chains, is estimated at 2 500. They are serving defence domain customers with 7.8% of their business relating to cyber.
[57] The Horizon Europe programme envisages that synergies with the EDF will benefit civil and defence research, although activities under the Framework Programme will have an exclusive focus on civil applications.

This skills gap hampers the EU's capacity to develop new technologies and defend our critical infrastructure. For government entities such as the ministries of defence and the military, the fierce competition for skills and the attractive salaries offered by the private sector further exacerbate the difficulties of attracting and retaining cyber talents.

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 objective of increasing the number of professionals trained in cybersecurity. It will bring together the many 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 benefit the cyber defence workforce. The European Security and Defence College (ESDC) will explore how to facilitate the exchange of best practices and further synergies between the military and civilian domains regarding training and the development of cyberspace-specific military skills.

Based on a training requirement analysis of the EU as well as training needs, the ESDC, EDA, and Member States will further develop and organise cyber defence training activities and exercises for EU institutions, CSDP operations and missions as well as 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. This should also include training courses for specific operational domain and multi-domain operations. Synergies should in particular be sought with the EU Cyber Academia and Innovation Hub (EU CAIH) PESCO project[58].

Member States are encouraged to develop specific education programmes in the field of cyber defence, bringing in higher education and academic institutions (civilian and military) to develop and create common cyber defence curricula, sharing best practices, creating partnerships and common projects, and facilitating exchanges of trainers and trainees. To ensure interoperability and a common culture across the EU, the ESDC will foster an exchange between Member States through the ETEE.

Wider cooperation between training and education actors should be enhanced by the Member States, combining both civilian and military aspects in the technical, operational, strategic and legal domains, establishing the basis for creating common and standardised training programmes at different levels for the civilian, law enforcement, diplomatic and cyber defence communities. In addition, the Member States should engage with European private sector training providers, as well as academic institutions, to raise the levels of competencies and skills of personnel in military CSDP missions and operations.

Furthermore, cooperation on cyber defence training standards and certification should be promoted between Member States, EUIBAs, international partners and other actors, including in the private sector and academia. The ESDC, building on existing civilian initiatives such as the European Cybersecurity Skills Framework (ECSF) developed by ENISA, will develop a cyber defence skills certification framework. The Commission would also consider approaches for certifying cyber skills, available on the market and from academia, while seeking to

[58] https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/

stimulate through the Cyber Skills Academy synergies between those approaches and filling gaps, notably with targeted EU funding.

Cyber defence actions

- Develop the EDT Strategic Assessment to support long-term strategic investment decisions.
- Develop a technology roadmap for critical cyber technologies for the EU covering critical technologies for cyber defence and cybersecurity to assess the level of dependencies.
- Propose ways forward to reduce dependencies using all the EU instruments including DEP, Horizon Europe and EDF, and anticipate technological development to increase technological sovereignty and ensure ability to act.
- Support the development of cyber defence skills certification framework.
- Develop EU cyber defence exercises and explore how to further develop the ESDC Cyber ETEE platform to generate more training capacities.

Civilian support actions

- Establish an EU Cyber Skills Academy, considering needs for specific skills for different professional profiles and sectors of activity, including in the defence work force.
- Analyse approaches for certifying cyber skills, while seeking to promote synergies and fill gaps, including through EU funding.

4. Partner to address common challenges

Partners will benefit from a more capable and resilient EU in cyber space, as well as from EU cyber defence assistance and capacity building provided through relevant EU instruments. The EU will seek to establish tailored partnerships in the area of cyber defence where these are mutually beneficial. Partnerships on cyber defence will also be addressed in the context of partner countries' participation in military CSDP missions and operations.

Where appropriate, this work will build on existing cyber dialogues, as well as security and defence dialogues. The High Representative will also explore synergies between the **informal EU Cyber Diplomacy Network and the network of defence attachés in EU Delegations.**

4.1. Cooperation with NATO

The EU's strategic partnership with NATO remains essential for Euro-Atlantic security as underlined in the Strategic Compass and NATO's 2022 Strategic Concept[59]. The EU remains fully committed to enhancing this key partnership, including in the area of cyber defence, and further steps need to be taken to develop shared solutions to common threats and challenges. In accordance with the Warsaw and Brussels Joint Declarations on EU-NATO cooperation[60] and based on the principles of transparency, reciprocity and inclusiveness, openness and as well as the decision-making autonomy of both organisations, cybersecurity and cyber defence constitute one of the EU key priority areas for cooperation.

[59] https://www.nato.int/strategic-concept/
[60] Signed in 2016 and 2018 respectively

On the basis of reciprocity, the EU will continue to exchange with NATO on the military conceptual framework concerning the integration of cyber defence aspects into the planning and conduct of military CSDP missions and operations. The EU will strive for compatibility with NATO concepts and doctrine on cyber defence to the maximum extent possible.

With regard to the high demand for cyber defence capabilities, the EU will promote synergies and complementarity with NATO across organisational and national boundaries. The EU will partner with NATO to strengthen the technical and procedural interoperability of cyber defence capabilities, including the development of capabilities in line with the FMN initiative. This will pave the way for the potential mutually supportive development and employment of cyber defence capabilities. Special consideration should be given to the interoperability of standards, contributing to the cyber resilience and interoperability of military communication and information systems, by involving industry where relevant.

To provide coherent training to respective cyber defence personnel, where applicable the EU will also strengthen cooperation with NATO on the harmonisation of training needs and requirements analysis, developing joint curricula, courses and exercises. On the basis of the principles of reciprocity and non-discrimination, the ESDC will open its cyber defence training courses to NATO staff and establish a platform to advertise common courses. The EU will also promote NATO staff participation in cyber exercises and crisis management exercises with cyber elements.

The EU and NATO will also engage in the further improvement of mutual situational awareness and explore avenues for coordination, including by strengthening the cooperation between NCIRC and CERT-EU. To foster cooperation concerning the cyber aspects and implications of crisis management and response, the EU will contribute to the exchange between staffs on military, civilian and common initiatives and, where applicable, to the development of potential synergies of respective crisis management frameworks and initiatives, including in the case of large-scale incidents. In order to ensure mutual complementarity and avoid unnecessary duplication of efforts, the EU will seek closer cooperation and information exchange with NATO on cyber defence capacity-building efforts in partner countries.

4.2. Cooperation with like-minded partners

The High Representative will include cyber defence issues more systematically in existing and future cyber as well as security and defence dialogues with partners. As cyber defence aspects will develop in bilateral dialogues, there will be a growing potential to introduce cyber defence issues in other formats of cooperation with EU partners.

The EU's strategic partnership with the **United States** will continue to deepen cooperation in security and defence in a mutually beneficial way including through structured exchange of information on situational awareness. Regular EU-US Cyber Dialogues and EU-US Security and Defence Dialogues confirm a strong Trans-Atlantic partnership. The High Representative will introduce relevant aspects of cyber defence into these dialogues where appropriate.

Together with its international partners, the EU will continue to support **Ukraine**, including through a cyber dialogue. In view of Ukraine's experience in building cyber resilience and cyber defence capacities, the exchange of best practices on cyber defence, including

information on threat landscape and situational awareness, as well as relevant policy developments is of common interest, will continue and be expanded.

Like-minded partners play an important role maintaining a global, open, stable and secure cyberspace and can complement the EU's ability to prevent, discourage, deter and respond to malicious behaviour in cyberspace. The EU remains open to a broad, ambitious and mutually beneficial security and defence engagement, including on cyber defence, with all like-minded partners.

4.3. Cyber defence capacity building support for partner countries

Global and regional challenges have increased the mutual interdependence of the EU and its partners and highlighted the need to establish closer partnerships on security and defence. This is particularly relevant for the EU candidate countries. Recent large scale cyber-attacks indicate a need for enhanced EU engagement and partnership on cyber security and cyber defence, building on existing programmes. Due to the transnational nature of cyber threats, enhancing the cyber resilience of partner countries, especially those with a lower level of cyber maturity, will contribute towards a safer and more secure cyberspace. Hence, the EU would be better able to prevent, detect, defend against, and deter cyberattacks. The EU will strengthen security and defence cooperation with partner countries to strengthen their cyber resilience, including through existing dialogues. Where applicable and mutually beneficial, the EU will engage with partners, and in particular those EU candidate countries aligned with the EU Common Foreign and Security Policy and Common Security and Defence Policy, in their cyber defence capacity building efforts. This could include support to policy and legislative frameworks, training, advising, mentoring and equipping the armed forces and security forces of partners. Member States could decide to provide cyber defence operational assistance to partners. Moreover, the EU will help partners strengthen their capacity to contribute to military CSDP missions and operations, as this is a valuable input to mutual efforts to promote peace and security.

The European Peace Facility (EPF) will continue to support EU efforts to help build defence capacities, including cyber defence, in partner countries, in particular in the EU's neighbourhood, complementing CSDP crisis management efforts. In this regard, when necessary, the EU will also link cyber defence assistance better with civilian cybersecurity capacity building, in particular through the EU Cyber Capacity Building Board. Efficient coordination among the EU's relevant programmes and instruments, including EPF, and Member States will be necessary for the success of cyber defence and cybersecurity capacity-building actions.

While providing support to partner countries in their cyber defence capacity-building efforts, the EU will work closely with other donors to develop situational awareness and coordination platforms in order to provide the best possible tailored support and ensure coherence and non-duplication of efforts.

Cyber defence actions

- Strengthen EU-NATO cooperation in the field of cyber defence training, education, situational awareness and exercises.
- Include cyber defence topics in EU-led cyber as well as security and defence dialogues with partner countries.

- Cooperate with like-minded countries, including in the context of cyber defence capability development and cyber resilience.
- Increase assistance to partners in cyber defence capability development, including through the European Peace Facility (EPF), in particular in the EU's neighbourhood and in support of EU candidate countries.

Civilian support actions

- Strengthen EU-NATO cooperation in the field of cybersecurity for what concerns situational awareness, crisis response, the protection of critical infrastructure, and standardisation and certification.

III. CONCLUSION

The High Representative, including in the capacity 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 identify 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 objectives 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.