Council of the European Union

Brussels, 22 May 2023
(OR. en)

9618/23

| | |
|---|---|
| COPS 269 | JAI 656 |
| POLMIL 123 | RELEX 639 |
| CYBER 130 | JAIEX 22 |
| HYBRID 31 | TELECOM 154 |
| EUMC 230 | IPCR 38 |
| CIVCOM 144 | PROCIV 35 |
| COPEN 162 | COTER 101 |
| COSI 103 | DISINFO 34 |
| DATAPROTECT 146 | CSC 252 |
| IND 256 | CSDP/PSDC 402 |
| RECH 191 | CFSP/PESC 748 |

**OUTCOME OF PROCEEDINGS**

| | |
|---|---|
| From: | General Secretariat of the Council |
| To: | Delegations |
| No. prev. doc.: | ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674 |
| Subject: | Council Conclusions on the EU Policy on Cyber Defence |

Delegations will find attached the Council Conclusions on the EU Policy on Cyber Defence, as approved by the Council at its meeting held on 22 May 2023.

**Council Conclusions on the EU Policy on Cyber Defence**

1. Building on the Cyber Defence Policy Framework of 2014 and its update in 2018, the Council welcomes the ambitious Joint Communication on the EU Policy on Cyber Defence to further invest in our modern and interoperable armed forces, cutting-edge technologies, state-of-the-art cyber defence capabilities and enhance partnerships to address common challenges. Cyberspace has become a field for strategic competition, at a time of growing dependence on digital technologies. Thus, it is essential to maintain an open, free, stable and secure cyberspace. The use of cyber operations that have enabled and accompanied Russia's unprovoked and unjustified war of aggression against Ukraine affects global stability and security, represents an important risk of escalation and adds to the already significant increase of malicious cyber activities outside the context of armed conflict over recent years.

2. The war in Ukraine has provided a new strategic context and confirmed the need for the EU, its Member States and their partners to further strengthen the EU resilience to face cyber threats and increase our common cyber security and cyber defence against malicious behaviour and acts of aggression in cyberspace. The Joint Communication on the EU Policy on Cyber Defence signals our determination to provide immediate and long-term measures to ensure freedom of actions in cyberspace and responses to threat actors seeking, amongst others, to intrude, disrupt or destroy network and information systems of the EU and its partners. Complementing the EU's Cybersecurity Strategy and in line with the Strategic Compass, this Joint Communication represents a significant step towards the EU's full-spectrum approach to resilience, response, conflict prevention, cooperation and stability in cyberspace. In this context, the Council underlines the need for appropriate and coherent responses from the EU, its Member States and their partners, also looking forward to the revision of the implementing guidelines of the EU's Cyber Diplomacy Toolbox as another key step forward in the evolution of the EU's cyber posture.

3. The Council emphasises that recent cyber-attacks against European critical infrastructure, the rapidly evolving cyber threat landscape and the fast pace of technological development also demonstrate the need for enhanced civil-military coordination and cooperation, whilst underlining there is no hierarchy between the civilian and military communities.
The EU Policy on Cyber Defence enables the EU and its Member States to strengthen their ability to protect, detect, defend and deter, making appropriate use of the whole range of defensive options available to the civilian and military communities for the broader security and defence of the EU, in accordance with international law, including human rights law and international humanitarian law.

4. While national security, including in the cyber domain, remains the sole responsibility of each Member State, as noted in article 4(2) TEU, the Council meanwhile stresses the need to substantially invest individually and collaboratively in enhanced resilience and deployment of full-spectrum defensive cyber defence capabilities and leveraging EU cooperation frameworks and financial incentives. The Council emphasises the need for further strengthening actions by Member States and EU institutions, bodies and agencies (EUIBAs) in order to protect the Union, our citizens, EUIBAs and CSDP missions and operations in cyberspace. It furthermore underlines the importance of EU resilience in cyberspace by developing cyber defence capabilities and enhancing cooperation with a trusted private ecosystem.

## I. **Act together for a stronger cyber defence**

5. The Council reiterates that an incremental, transparent and inclusive process is essential for enhancing trust which is critical to the further development of an EU cybersecurity crisis management framework, to be done in line with the Cyber Crisis Management Roadmap developed in the Council. The Council reiterates the need to continue enhancing our ability to protect, detect, defend and deter cyberattacks through improved situational awareness, capacity building, capability development, training, exercises, and enhanced resilience and by responding firmly to cyberattacks against the EU, its Member States and EUIBAs, CSDP missions and operations using all appropriate means. In doing so, the Council encourages the High Representative and the Commission to reduce complexity in the field of cyber, avoid unnecessary duplication and ensure cooperation and synergies with existing initiatives. The cooperation and coordination need to be strengthened among the cyber defence actors within and of the EU and Member States, between military and civilian cyber communities and between public and a trusted private ecosystem. In this context, Member States are encouraged to further explore and strengthen civil-military national coordination mechanisms, facilitate common voluntary information sharing, share lessons learned, contribute to the development of interoperable standards and conduct risk evaluations and risk scenario-building, as well as joint exercises particularly at the European level, in full respect of the provisions of the Directive on measures for a high common level of cybersecurity across the Union (NIS2).

6. Recognising the efforts to further enhance the resilience of the Union with NIS2 and the Directive on Critical Entities Resilience (CER), the Council reiterates its recommendation on an EU-wide coordinated approach to strengthen the resilience of critical infrastructure.[1] It calls for measures to further enhance the resilience of critical entities, infrastructure, digital products and services, whilst noting that the proper implementation of NIS2 remains the most important step. While predominantly a civilian responsibility, this also contributes to stronger cyber defence. In this context, the EUIBAs as well as Member States are encouraged to support the further development and deployment of new and existing EU coordination mechanisms, risk assessments, evaluations and scenarios, common voluntary information sharing and exercises, in a manner that adds value and avoids unnecessary duplication with existing initiatives.

7. To further strengthen trust, consolidate cooperation, and facilitate timely information sharing on significant and large-scale cyber incidents affecting defence systems, the Council welcomes the initiative to further develop the EU Cyber Commanders Conference to be organised by each Presidency of the Council of the EU, with the support of the European Defence Agency (EDA) and participation of the European External Action Service (EEAS). The Council encourages all Member States to take part in these meetings. To strengthen the EU's resilience against large-scale cybersecurity incidents, the Council invites the EU Cyber Crises Liaison Organisation Network (EU-CyCLONe) and the EU Cyber Commanders Conference to identify possible ways to cooperate and benefit from a joint military and civilian perspective.

[1] Proposal for a Council Recommendation on a coordinated approach by the Union to strengthen the resilience of critical infrastructure, COM/2022/551.

8. To foster a more robust and coordinated EU-level response, the Council welcomes the establishment and looks forward to reaching the initial operational capability by mid-2024 of the EU Military Computer Emergency Response Teams Operational Network (MICNET) to enhance technical information sharing on cyber incidents affecting defence systems among the participating Member States. The Council encourages all Member States to participate in MICNET in order to ensure the network's effectiveness. Furthermore, the Council invites Member States to build on lessons learned from the Computer Security Incident Response Teams (CSIRTs) Network and strongly encourages to create an effective cooperation and coordination mechanism between the two networks at an appropriate time, in full respect of each entity's governance mechanisms and constituencies.

9. In light of the increase of malicious cyber activities from State and non-State actors on EU CSDP missions and operations, the Council invites the EU and its Member States to strengthen their capabilities to defend and secure CSDP missions and operations. In this regard, the Council welcomes the objectives to further advance the protection of EU military networks and structures, in line with amongst others the EU Military Vision and Strategy on Cyberspace as a Domain of Operations.[2]

[2] EEAS(2021) 706 REV4

10. The Council reiterates the Council Conclusions of May 2022[3] and the need to invest in our mutual assistance under Article 42(7) TEU as well as the solidarity clause under Article 222 TFEU. The Council stresses the importance of further deepening the EU and its Member States' common understanding of the implementation of Article 42(7), including in complex scenarios involving a cyber-attack, consistent with the relevant principles of international law. It welcomes the possibility, at the explicit request of the Member State(s) concerned, of support by the EU when a cyber-attack unfolds, without prejudice to the specific character of the security and defence policy of certain Member States.

11. The Council underlines the progress achieved in the PESCO project Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRTs) and its readiness to act upon request as a capability for Member States' and EU needs, in support of CSDP missions and operations and to provide assistance to EU partners. The Council welcomes further development of PESCO CRRTs' capability, national cyber response teams, and, where appropriate, additional incident response capabilities such as the future Hybrid Rapid Response Teams as envisioned in the Strategic Compass, including by fostering their coordination and cooperation at EU level.

[3] Council conclusions on the development of the European Union's cyber posture, 23 May 2022, 9364/22.

12. The Council welcomes the work of the PESCO-project Cyber Information Domain Coordination Centre (CIDCC), which aims at providing a military capability to collect and analyse information relevant for a common operational cyber picture. The Council furthermore welcomes the proposal to integrate the proof of concept, if successful as an information coordination centre, from 2025 onwards, into an EU Cyber Defence Coordination Centre (EUCDCC), enhancing coordination and situational awareness in particular of EU CSDP mission and operations commanders, as well as the strengthening of the wider EU Command and Control architecture. The Council calls on the High Representative to present a concept and roadmap for the establishment of the EUCDCC, drawing lessons from similar international entities, identifying resources required, avoiding unnecessary duplication and seeking complementarity with the wider EU cybersecurity framework.

13. The Council highlights the importance of strategic intelligence cooperation on cyber threats and activities, and invites Member States, through their competent authorities, to continue to contribute to EU INTCEN's, EUMS Intelligence Directorate's and Member States work under the Single Intelligence Analysis Capacity (SIAC). The Council further highlights the importance of strengthening our cyber intelligence capacities to enhance our cyber resilience, responses and provide effective support to our civilian and military CSDP missions and operations, as well as our armed forces and SIAC's capacity in the cyber domain, based on voluntary intelligence contributions from the Member States and without prejudice to their competences.

14. The Council takes note of the European Commission's cyber situation and analysis centre which aims to enhance the Commission's situational awareness. The Council emphasizes the importance of establishing mutual beneficial cooperation between this centre and other EUIBAs, in particular ENISA and CERT-EU. The Council underlines the importance of ensuring close cooperation with EU cooperation networks when developing situational awareness, as well as respecting confidentiality. The Council notes the need for strengthening the common situational awareness at the EU level and further developing the EU cybersecurity crisis management framework, while avoiding any unnecessary duplication of efforts.

15. The Council recalls that cyber education, training and exercises are essential to ensure preparedness and effectiveness and welcomes national activities as well as those provided by the EU through the European Security and Defence College (ESDC), EDA, ENISA and ongoing PESCO-projects, such as the Cyber Ranges Federations and the EU Cyber Academia and Innovation Hub (CAIH). With a view of further enhancing these efforts, the Council looks forward to the establishment of the EDA framework project CyDef-X to synchronise and support cyber defence exercises. The Council encourages EDA to explore, in close cooperation with Member States and the EEAS, how CyDef-X could further support exercises such as CYBER PHALANX, including on mutual assistance under Article 42(7) TEU and solidarity clause under Article 222 TFEU, as well as with the Commission and ENISA as regards civilian exercises. Furthermore, the Council encourages the use and further development within CyDef-X of existing cyber defence testing and exercises environments, such as Cyber Ranges Federations. To ensure agile and efficient decision-making process in a matter of cyber crisis, the Council underlines the importance of holding regular table top exercises for the Member States' decision-making level.

16. The Council notes the proposal for a Cyber Solidarity Act and the intention to enhance capabilities to detect and respond to cybersecurity threats and incidents in the EU. The Council underlines that proposals in this domain can only be effective when aligned with Member States' crisis management frameworks and needs. The Council underlines the importance of testing critical infrastructure for potential vulnerabilities, where assessed as beneficial, as a national competence, taking into account available EU risk assessments.

17. The Council notes the Commission's proposal to set up a Cyber Emergency Mechanism, which could support the availability of cybersecurity services from trusted private providers to upon request assist Member States in case of large-scale cybersecurity incidents, while underlining the need to scale up a European cybersecurity industry with the support of the ECCC as an essential pillar for this mechanism to be operational. The Council underlines the key role of each Member State in the monitoring and assessment of its national needs.

## II. **Secure the EU defence ecosystem**

18. The Council recalls its encouragement to Member States to further develop their own capabilities to conduct cyber defence operations, including when appropriate proactive defensive measures to protect, detect, defend and deter against cyberattacks. Considering that NIS2 does not apply to public administration entities that carry out their activities in the area of defence, the Council invites EDA, with the support of the Commission and EEAS as appropriate, to assist Member States in developing non-legally binding voluntary recommendations inspired by NIS2 to increase cybersecurity in the defence community, and invites all Member States to actively engage in this effort. These recommendations should be mindful of similar efforts undertaken in other frameworks.

19. As acknowledged in the Strategic Compass, the EU's capacity to act depends on its ability to reduce its strategic dependencies across its cyber defence capabilities and supply-chains as well as developing and mastering cutting-edge cyber defence technologies. This includes strengthening the European Defence Technological and Industrial Base (EDTIB) throughout the EU, and its ability to cooperate with like-minded partners around the world, on a reciprocal basis to ensure mutual benefits. The Council therefore calls for the cybersecurity and the cyber defence industries to closely cooperate to create synergies with the aim to develop and deliver full-spectrum cyber defence capabilities. The Council invites the Commission, in close collaboration with the ECCC, where appropriate, to further support the development of a strong, agile, globally competitive and innovative European cyber defence industrial and technological base, including small- and medium-sized enterprises (SMEs), through further investments, and policy actions.

20. Considering the importance of interoperability and commonality of cyber defence capabilities, including when it comes to the collaborative development of next-generation cyber defence capabilities, the Council invites EDA and the EU Military Staff to work on a set of EU cyber defence interoperability requirements, which would build on, and be compatible with, existing principles, processes and standards established in particular in the North Atlantic Treaty Organization (NATO) framework. Furthermore, the Council invites Member States to explore in the framework of the European Defence Standardisation Committee whether specific voluntary standards for defence systems could be required, in close cooperation with all relevant stakeholders, including European standardisation organisations and NATO as appropriate.

21 The Council welcomes the Commission's efforts to present a plan to promote the use of existing standards for civilian cybersecurity and cyber defence uses, as well as the development of new voluntary standards. The Council emphasises the need to align cybersecurity and cyber defence standards, where appropriate. The Council recognises that such voluntary standards could be useful for EU cybersecurity and cyber defence industries and urges closer collaboration between civilian and defence standardisation bodies.

22. The Council calls for recommendations based on the mapping of existing tools for secure communication in the cyber domain, carried out by the Commission and relevant institutions, to be developed swiftly. Where possible, the recommendations should be aligned with existing initiatives on information sharing and should also take into account risks posed by emerging and disruptive technologies to current encryption methods.

23. Moreover, the Council welcomes the initial work undertaken on risk evaluation and scenarios being developed by the Commission, the High Representative and the NIS Cooperation Group in relation to, initially, the energy and telecommunications sectors, at the request of the Council. The Council acknowledges that targeted cybersecurity risk assessments for communications infrastructure and networks in the EU are also being prepared. The Council reiterates that a common understanding of possible impacts of cyber incidents between Member States but also EU institutions, bodies and agencies is of utmost importance. Thus, the Council invites the above-mentioned actors to ensure that risk evaluations, scenarios and subsequent recommendations are taken into account when defining and prioritising measures and support, at EU and where appropriate national level. The Council furthermore calls for the risk scenarios to be considered by all relevant actors in risk assessment processes, as well as in the development of cyber exercises.

III. **Invest in cyber defence capabilities**

24. The Council encourages Member States to increase their investments to build, maintain and further develop interoperable cyber defence capabilities. The Council supports the development of a set of voluntary commitments for the further development of national cyber defence capabilities, mindful of similar efforts undertaken in other frameworks.

25. The Council calls on Member States and EDA to use the opportunity of the revision of the Capability Development Plan to set a high level of ambition when it comes to the development of collaborative cyber defence at EU level. The Council further encourages Member States to build on the updated set of priorities and on their PESCO commitments to increase their level of engagement in collaborative EU cyber defence capability development projects, recognising the direct benefit of collaborative projects at EU level to support the development of national cyber defence capabilities.

26. The Council welcomes collaborative research efforts at EU level to explore the possible applications in defence-related systems of emerging and disruptive technologies, noting also the need to ensure that those technological developments are quickly incorporated into existing and future capabilities. The Council encourages Member States and EU industry to make the best use of collaborative research opportunities at EU level, for example in EDA framework, ongoing PESCO projects, such as the EU Cyber Academia and Innovation Hub (CAIH), the European Defence Fund and, where relevant, Horizon Europe and the Digital Europe Programme for dual use projects. Furthermore, the Council welcomes leveraging the dedicated frameworks to support defence innovation utilising spin-ins from the civilian domain, notably the EU Defence Innovation Scheme and the Hub for European Defence Innovation. Moreover, the Council encourages the European Cybersecurity Competence Centre (ECCC) and EDA to develop a working arrangement to facilitate information sharing among respective staffs on respectively civil, dual use and defence technology priorities, in view of creating synergies and avoiding duplication.

27. The Council welcomes the intention to develop a technology roadmap for critical cyber technologies by the Commission in cooperation with EDA and the ECCC in line with their respective mandates, with Member States and in consultation with, relevant stakeholders such as industry, which through identifying the critical cyber technologies, mapping technological developments and strategic dependencies, provides ways to reduce those, in support of the EU´s strategic autonomy and technological sovereignty, while preserving an open economy. The Council notes that the technology roadmap for critical cyber technologies may inform strategic priorities for the EU's funding instruments, while being in line with the respective modalities in place for these. The Council recalls that the EU should pursue an ambitious and assertive European industrial policy to create a sustainable, attractive and competitive business environment, which can also enable European entities in the cyber domain to scale up.

28. The Council appreciates the intention to address the significant cybersecurity skills gap by attracting new professionals, including women, upskilling and reskilling and investing in and organising trainings and exercises to build a diverse and inclusive cyber workforce. Recognising the challenges that the EU faces with regards to human capital within cybersecurity and cyber defence, the Council welcomes the Cybersecurity Skills Academy initiative, which may also benefit the cyber defence workforce.

29. The Council invites Member States to exchange information on best practices to develop skilled cybersecurity professionals, leveraging the synergies between military, civilian and law enforcement initiatives and calls on the ESDC, with the support and expertise of EDA and ENISA, to consider options for enhancing the exchange of best practices and further synergies between the military and civilian fields regarding training and the development of cyber-specific defence skills.

30. The Council underlines the importance of a common understanding of the composition of the cybersecurity workforce and of associated skills in order to identify and address the gaps on the cybersecurity labour market, as well as the need to engage all stakeholders, including Member States and industry. The Council recognises that establishing indicators to monitor the cybersecurity labour market would help identify the cybersecurity skills needs and direct funds adequately, while contributing to meet policy-related obligations, notably those deriving from the NIS2. The Council welcomes the proposal for a cyber defence skills certification framework and invites the High Representative, in his capacity as Head of the ESDC to develop this, in cooperation with the EEAS, the Commission and Member States, by leveraging civilian initiatives.

## IV. **Partner to address common challenges**

31. The Council calls on the High Representative and the Commission to strengthen and advance its cooperation and explore mutually beneficial and tailored partnerships on cyber defence policies, including on cyber defence capacity building through the European Peace Facility (EPF). To this end, cyber defence should be added as an item to the EU's dialogues and consultations on cyber, to the overall security and defence consultations with partners. Moreover, dialogues and collaboration with the private sector should be enhanced. The Council underlines that international collaboration on cybersecurity standards and certification would be an added value for the European industry. Therefore, it welcomes the Commission's commitment to make this an essential part of the EU-cyber dialogues with third countries and international organisations.

32. The Council stresses the importance of international cooperation to prevent or reduce risks of conflict in cyberspace, especially through further development and operationalisation of confidence-building measures (CBMs) at regional and international level, including at the UN, and further encouraging the use of existing cyber CBMs like at the Organization for Security and Co-operation in Europe (OSCE), including in times of international tensions. The EU and its Member States emphasise that existing international law applies in cyberspace and stresses the importance of continued efforts to uphold and promote the UN Framework for responsible state behaviour and work towards its implementation, including through the establishment of the Programme of Action for advancing responsible State behaviour in cyberspace (PoA).

33. In line with the Joint Declarations on EU-NATO cooperation, the Council invites the High Representative, also in his capacity as Head of EDA, and the Commission to further strengthen, deepen and expand the partnership in the cyber domain with NATO in full respect of the principles of inclusiveness, reciprocity, mutual openness and transparency, as well as the decision-making autonomy of both organisations. While taking into account the need to ensure complementary and coordinated efforts with the fullest possible involvement of Member States that are not part of NATO and avoid unnecessary duplications, the Council calls for links on relevant levels to be established between EU-NATO on training, education, situational awareness, exercises and R&D platforms, and to seek potential synergies between the respective voluntary commitments for the developments of national cyber defence capabilities and the crisis management frameworks, the protection of critical infrastructure, and the enhancement of exchanges of situational awareness, coordinated responses to malicious cyber activities as well as capacity building efforts in third countries. This includes the Technical Arrangement between NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team – EU (CERT-EU) as well as an enhanced political dialogue on cyber defence issues on all levels.

## V. **Conclusion**

34. Building on the Council Conclusions on the EU Policy on Cyber Defence, the Council calls upon the High Representative and the Commission to develop for approval by Member States an implementation plan by the second quarter of 2023 for the Policy. The Council also invites Member States to voluntarily state their ambition and actions with regards to cyber defence in the context of the EU Policy on Cyber Defence and make full use of non-legally binding voluntary recommendations and commitments to step up their national and multinational cyber defence efforts aiming to maximize the impact at the EU level. The High Representative, the Commission and Member States are invited to report and discuss yearly on the progress of implementing the elements of the Joint Communication and its implementation plan starting by the second quarter of 2024.