Council of the
European Union

Brussels, 29 April 2022
(OR. en)

8594/22

LIMITE

CYBER 144	EUMC 141
COPEN 148	IPCR 48
COPS 179	HYBRID 37
COSI 109	DISINFO 32
DATAPROTECT 120	COTER 107
IND 135	CSDP/PSDC 241
JAI 558	CFSP/PESC 554
JAIEX 39	CIVCOM 70
POLMIL 98	RECH 211
RELEX 542	PROCIV 55
TELECOM 177	

NOTE

From:	Presidency
To:	Delegations
Subject:	Draft Council conclusions on the development of the European Union's cyber posture

Delegations will find in Annex the courtesy translation of Draft Council conclusions on the development of the European Union’s cyber posture.

ANNEX

Courtesy translation

DRAFT COUNCIL CONCLUSIONS ON THE DEVELOPMENT OF THE EUROPEAN UNION'S CYBER POSTURE

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING XXX

1. [Challenges] EMPHASISES that malicious behaviour in cyberspace, emanating from both State and non-State actors, has intensified in recent years, including a sharp and constant surge in activities targeting the EU and its Member States’ critical infrastructure, supply chains and intellectual property, as well as a rise in ransomware attacks against our businesses and organisations. NOTES that with the return of power politics, some countries are increasingly attempting to challenge and undermine the rules based order in cyberspace, turning the cyber sphere, along with the high seas, air, and outer space, into an increasingly contested domain. ACKNOWLEDGES that large-scale cyber-attacks through digital supply chains or attempts to intrude, disrupt or destruct systems causing systemic effects have become more common and have shown the readiness of some actors to effectively risk international security and stability. UNDERLINES that the military aggression against Ukraine has demonstrated the growing readiness of hostile state actors to use cyber offensive activities as an integral part of hybrid strategies combining intimidation, destabilisation and economic disruption.

2. REITERATES that facing the current geopolitical shifts, the strength of our Union lies in unity, solidarity and determination, by enhancing the EU's **strategic autonomy** and its ability to work with partners to safeguard its values and interests and **by swiftly implementing the Strategic compass, including in the cyber domain**. UNDERLINES that a stronger and more capable EU in security and defence will contribute positively to global and transatlantic security and is complementary to NATO, which remains the foundation of collective defence for its members. REAFFIRMS the EU's intention to intensify support for the global rules-based order, with the United Nations at its core.

3. [posture] In line with the EU Cybersecurity Strategy and the Strategic Compass, REITERATES the need to develop the Union's cyber posture by enhancing our ability to prevent cyberattacks through capacity building, capability development, training, exercises, enhanced resilience and by responding firmly to cyberattacks against the Union, its Institutions and its Member States using all available EU tools. This includes further signalling the EU's determination to provide immediate and long-term responses to threat actors seeking to deny our secure and open access to cyberspace and affect our strategic interests. In that context, STRESSES that the cyber posture aims to combine the various initiatives that concur to EU actions in favour of an open, free, stable and secure cyberspace and to better coordinate short, medium and long term actions to prevent, discourage, deter and respond to cyber threats and attacks.

4. RECALLS that the Strategic Compass approved by the Council and endorsed by the European Council in March 2022 called for further enhancing our cyber resilience, increasing solidarity and mutual assistance in the event of a large-scale incident, maintaining an open, free, stable and secure cyberspace, enhancing and deepen our cooperation with partners, strengthening the EU's Cyber Diplomacy Toolbox and leveraging the EU and Member States' cyber defence capabilities. EMPHASISES that these elements should be incorporated in the EU's cyber posture, according to five functions of the EU in the cyber domain: **strengthen our cyber resilience and capacities to protect; prepare for solidary and comprehensive crisis management; promote our vision of cyberspace; enhance international cooperation and partnerships; defend against and respond to cyber-attacks**.

==========

I. STRENGTHEN OUR CYBER RESILIENCE AND CAPACITIES TO PROTECT

5. [Cybersecurity] REITERATES the need to raise the overall level of EU cybersecurity, LOOKS FORWARD to the rapid adoption of the draft Directive on measures to achieve a high common level of cybersecurity across the Union, the draft Directive on critical entities resilience and TAKES NOTE of the proposal for a Regulation laying down measures on a high level of cybersecurity at the institutions, bodies, offices and agencies of the Union, in order to foster an European Union that protects its citizens, public services and businesses in cyberspace. ENCOURAGES the Commission to finalise the adoption of key proposals to ensure that digital infrastructures, technologies, products and services are secured, in order to send a clear signal about the EU's ambitions on this topic and to support and help companies rise up to the challenge. CALLS upon the Commission to propose EU common cybersecurity requirements for digital products and ancillary services through the **Cyber Resilience Act, which should be proposed by the Commission before the end of 2022**.

6. [resilience of communication infra] INVITES the relevant authorities, such as the Body of European Regulators for Electronic Communications (BEREC), the European Union Agency for Cybersecurity (ENISA) and the Network & Information Security (NIS) Cooperation Group, along with the European Commission, to formulate recommendations, based on a risk assessment, to Member States and the European Commission in order to reinforce the resilience of communications networks and infrastructures within the European Union, including the continued implementation of the 5G toolbox.

7. [incident handling] CALLS upon the EU and its Member States to reinforce efforts on increasing the overall cybersecurity level, for example by facilitating the emergence of trusted cybersecurity service providers, such as cybersecurity audit and incident response. STRESSES that encouraging the development of such EU providers should be a priority for the EU industrial policy in the cybersecurity field and receive appropriate EU funding. To better resist and counter cyberattacks with potential systemic effects, EMPHASISES the need to continue to develop incident handling cooperation with the private sector and INVITES the Commission to propose options, including in view of the upcoming Cyber Resilience Act, to encourage the emergence of trusted cybersecurity service industry and to strengthen the cybersecurity of the digital supply chain, drawing from the lessons of the Solarwinds and Microsoft Exchange cyber operations, as well as to improve cyber threat detection and sharing capabilities in and across Member States, notably through supporting reinforced Security Operation Centres.

8. [developing resilience and capabilities through innovation] REITERATING that investing in innovation and making better use of civilian technology is key to enhancing our **technological sovereignty,** including in the cyber domain, CALLS on the Commission to swiftly operationalise the European Cybersecurity Competence Centre to develop a strong European cyber industrial and technological ecosystem**,** UNDERLINES the need to boost research and innovation, invest more in civilian and defence areas to strengthen the EU's Defence Technological and Industrial Base (EDTIB) and develop the cyber capabilities of the EU and its Member States, including strategic support capabilities. STRESSES thus the importance to make intensive use of new technologies, notably quantum computing, Artificial Intelligence and Big Data, to achieve comparative advantages, including in terms of cyber responsive operations and information superiority.

9. [Cybercrime and public awareness] EMPHASISES the need to strengthen our efforts in the fight against new trends in international cybercrime, in particular ransomware, through the EMPACT mechanism (European Multidisciplinary Platform Against Criminal Threats) and via exchanges between the security, law enforcement and diplomatic sectors. REITERATES its commitment to inform the public about cyber threats and the measures taken nationally and at EU level against these threats, with a view to raise awareness and encourage an appropriate level of cyber protection and cyber hygiene.

10. [operational resilience] Recognising that enhancing our cybersecurity is a way to increase the effectiveness and security of our efforts on land, in the air, at sea and in outer space, STRESSES the importance of mainstreaming cybersecurity considerations in all EU public policies, including sectorial legislation in complementarity of the NIS directive, and **INVITES the Commission to explore options to increase the cybersecurity of the suppliers of the EU's Defence Technological and Industrial Base (EDTIB).**

II. PREPARE FOR SOLIDARY AND COMPREHENSIVE CRISIS MANAGEMENT

11. [exercises] Drawing from the annual cyber exercises, other exercises involving a cyber dimension, as well as the EU CyCLES 2022 exercise, STRESSES the importance of establishing a **programme of cross-community and multi-level cyber exercises** in order to test and develop the EU internal and external response to large-scale cyber incidents, with the participation of **the Council, the EEAS, the Commission and relevant stakeholders such as ENISA, and which will be articulated and contribute to the general EU's exercise policy**. EMPHASISES the importance of further Cyber Europe exercises, combining response across different levels. ACKNOWLEDGES the need to evaluate and consolidate the existing exercises and explore further exercises on specific segments of the cyber domain, notably a military CERT exercise.

12. [shared assessment of impact and severity] UNDERLINES the need to further test and reinforce operational cooperation and shared situational awareness among Member States, including through established networks such as the CSIRTs Network and Cyber Crisis Liaison Organisation Network (CyCLONe) in order to advance EU preparedness to face large-scale cyber incidents. UNDERLINES the importance to work on developing a common language amongst Member States and with EUIBAs, which is tailored for discussion at the political level, to support the establishment of a consolidated assessment of the severity and impact of relevant cyber incidents as well as possible evolution scenarios and the needs arising from them as appropriate. UNDERLINES in that regard the need to improve the complementarity of shared situational assessment reports, including CyCLONE's reports on the impact and severity of large-scale cyber incidents across EU Member States and threat assessments provided by the EU INTCEN in the framework of the EU Cyber Diplomacy toolbox. EMPHASISES the need for secure communication channels to facilitate the exchange of information, and the need to ensure coordinated public communication.

13. [operational cooperation and mutual support] In the event of large-scale cyber incident, STRESSES the need to reinforce the coordination, and, where appropriate, the pooling of our incident response amongst Member States, including in cooperation with the private sector. RECOGNIZES that developing ties with the private sector could be an amplifier of public capacities, in particular in a context of skills shortages across the EU, and that identifying and coordinating these private partners could make a major difference in the event of large-scale incidents. INVITES the **Commission to propose and implement a new Emergency Response Fund for Cybersecurity by the end of Q3 2022**.

14. [Mutual assistance and solidarity] In line with the Strategic Compass, REITERATES the need to invest in our **mutual assistance** under Article 42(7) of the Treaty on European Union as well as **solidarity** under Article 222 of the Treaty on the Functioning of the European Union, in particular through frequent exercises. In this framework, STRESSES the need to work further on the provision and coordination of bilateral civilian and military support, including by exploring possible support provided by EU institutions upon an explicit request from Member States, and on defining appropriate response measures and a communication strategy in the context of the implementation of Article 42 (7), and NOTES that this could also include improving the coordination with existing EU crisis managements mechanisms and the EU Civil Protection Mechanism.

III. PROMOTE OUR VISION OF CYBERSPACE

15. [Cyber diplomacy] RECALLS that the common and comprehensive EU approach to cyber diplomacy aims at contributing to conflict prevention, mitigation of cybersecurity threats and greater stability in international relations. In this context, REAFFIRMS the EU's commitment to the settlement of international disputes in cyberspace by peaceful means. STRESSES the importance of a global, open, free, unfragmented, stable and secure cyberspace where human rights, fundamental freedoms and the rule of law fully apply in support of the social well-being, economic growth, prosperity and integrity of our free and democratic societies. With a view to developing channels for frank and open dialogue with key cyberspace stakeholders, CALLS on the Commission and the EEAS to make cyber issues, including the EU Cyber Diplomacy Toolbox, an integral part of the EU's strategic dialogues with international partners and competitors alike.

16. [multi-stakeholder cooperation] RECALLS the importance of multi-stakeholder cooperation as other stakeholders bear responsibility for cybersecurity as well, notably when it comes to implementing the recommendations and decisions States take in the international and regional fora. CALLS on the EU and its Member States to further disseminate our model of cyberspace through various multi-stakeholder initiatives including the **Paris Call to Action,** emphasising the shared benefits stability in cyberspace, and raising awareness globally about the dangers of a state-centric and authoritarian vision of the Internet, and CALLS upon the EU and its Member States to further strengthen the cooperation with the multi-stakeholder community, including by making use of relevant projects such as the EU Foreign Policy Instrument's EU Cyber Diplomacy Initiative.

17. [International organizations] Notably in the framework of responsible State behaviour in cyberspace developed under the auspices of the United Nations, STRESSES the importance of increasing the EU's role as an upholder of the application of international law in cyberspace and as a bearer of the norms of responsible state behaviour, by continuing to systematically signal the unacceptability of cyberattacks breaching international law or the established norms of responsible state behaviour in cyberspace. EMPHASIZES the importance of further supporting the development and operationalisation of confidence-building measures (CBMs) at regional and international level, and further encouraging the use of existing CBMs at the OSCE, including in times of international tensions.

18. [international discussions in technical fora] RECALLS that shaping international standards in the areas of emerging technologies and the core internet architecture in line with EU values is essential to ensure that the Internet remains global and open, that technologies are human-centric, privacy-focused, and that their use is lawful, safe and ethical. ENCOURAGES the High Representative and the Commission to develop a strategic vision on technical issues that have foreign policy implications and could have an impact on the stability of cyberspace and the Internet in particular, including in the major international technical organisations (International Telecommunications Union etc.).

IV. ENHANCE COOPERATION WITH PARTNERS AND INTERNATIONAL ORGANIZATIONS

19. [Capacity building] EMPHASIZES the need to better connect the EU's cyber capacity building strategy with the UN norms of responsible state behaviour in the cyberspace, including by developing tailored cooperation and capacity-building programmes to support third States in their implementation efforts, and, in doing so, continuing and expanding our efforts to promote the UN Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA). STRESSES the importance of fully integrating cyber capacity building as part of the EU's offer as a security provider, with an adequate coordination of efforts between Member States and EU institutions, bodies and agencies, and, in particular CALLS on the High Representative and the Commission to establish a *Cyber capacity building board* by Q3 2022 and to hold regular exchanges in the Horizontal Working Party on Cyber Issues. CALLS on the Commission and High Representative to further mobilize the Neighbourhood, Development and International Cooperation Instrument (NDICI) and other financial tools, such as the European Peace Facility (EPF), to support the strengthening of the resilience of our partners and the development of cooperation projects, including in the context of crisis, and ENCOURAGES the deployment of EU and Member States' experts to offer support in cyber crises.

20. [outreach and engagement] STRESSES the need to step-up efforts to develop a structured and open EU outreach approach on how to promote a global common understanding of the UN framework of responsible State behaviour in cyberspace, including the initiative for a Programme of Action for advancing responsible State behaviour in cyberspace (PoA), and as part of these efforts REQUESTS the High Representative to present an outreach plan to the Council by the end of 2022. ENCOURAGES the High Representative and Commission services to make full use of its 145 Delegations and develop regular, fruitful collaboration between EU Delegations and Member States' Embassies in third countries, under the auspices of the envisaged EU Cyber Diplomacy Network. CALLS upon the High Representative to establish the EU Cyber Diplomacy Network by Q3 2022, contributing to the exchange of information, joint training activities for EU and Member States' staff, coherent capacity building efforts and strengthening the implementation of the UN framework for responsible state behaviour as well as confidence-building measures between States.

21. [cooperation with partners] STRESSES its commitment to further cooperate with international organisations and partner countries to advance the shared understanding of the cyber threat landscape, develop cooperation mechanisms and identify cooperative diplomatic responses proactively. In full respect of the decision-making autonomy and procedures of both organisations and on the basis of the principles of transparency, reciprocity and inclusiveness, EMPHASIZES the need to further develop cyber cooperation with NATO through exercises and exchanges between experts, including on norms of responsible state behaviour in cyberspace.

V. DEFEND AGAINST AND RESPOND TO CYBER-ATTACKS

22. [reinforcement of the CDT] REITERATES that the EU must be able to swiftly and forcefully respond to cyberattacks, such as state-sponsored malicious cyber activities targeting EU and its Member and therefore needs to strengthen the EU Cyber Diplomacy Toolbox and make full use of all its instruments, including the available political, economic, diplomatic, legal and strategic communication tools to prevent, discourage, deter and respond to malicious cyber activities. UNDERLINES that hostile actors need to be aware that cyberattacks against Member States and EU institutions will be detected early, identified promptly and met with all necessary EU tools and policies. Drawing notably from the elements therein of the cyber posture as well as the lessons learnt from the implementation of the Cyber Diplomacy Toolbox since its inception and from the EU CyCLES exercise, **INVITES the Member States and the High Representative, with the support of the Commission, to work towards a revised version of the implementing guidelines of the EU Cyber Diplomacy Toolbox by the end of 2022.**

23. [shared situation awareness and Intelligence sharing] UNDERLINES the need to hold regular exchanges on the cyber threat landscape in relevant bodies and committees of the Council, drawing from the assessment on the impact and severity of recent incidents, to increase the overall awareness and preparedness for further applications of the cyber diplomacy toolbox, and develop further tools to support its implementation. While national security remains the sole responsibility of each Member State, NOTES the need to strengthen intelligence sharing and cooperation between Member States as well as with the EU INTCEN in order to be able to share intelligence at the beginning of the decision-making process, in particular on the question of coordinated attribution, and thereby enable an swift and effective response to attacks targeting the EU and its partners. REITERATES the importance to strengthen INTCEN's capacity in the cyber domain, based on voluntary intelligence contributions from the Member States and without prejudice to their competences and to explore the proposal on the possible establishment of a Member States' cyber Intelligence working group.

24. [Signalling] ACKNOWLEDGING that EU declarations and restrictive measures taken in the framework of the EU Cyber Diplomacy Toolbox have sent a strong message that cyber malicious activities targeting the integrity and security of the EU and its Member States are unacceptable and thus contribute to preventing, discouraging, deterring and responding to malicious cyber activities, REITERATES its commitment to use these measures with a view to recall the obligations that apply to cyberspace under international law and foster the UN framework of responsible State behaviour, in particular the obligation for all States to carry out due diligence in order to avoid their territory being used for malicious cyber activity. Noting that strong and swift messages mitigate the risks of escalation and can discourage attackers who target European interests, **INVITES the High Representative to develop and submit to the Member States a coherent communication strategy on the use of the cyber diplomatic toolbox**.

25. [gradual response] ENCOURAGES the development of gradual, targeted and sustained approaches and responses to cyber malicious activities, using the wide range of tools provided by the Cyber Diplomatic Toolbox, including the EU cyber sanctions regime, and envisaging additional measures. EMPHASIZES the need to increase the possibility to mobilise, on a case-by-case basis, all available tools, internal and external, to prevent, discourage, deter and respond to cyberattacks, implementing these in a swift, effective, gradual, targeted and sustained approach. **CALLS upon the EEAS, in cooperation with the Commission, to establish by 2023, and update regularly, a list of possible EU joint responses to cyberattacks, including sanction options, across the spectrum in order to be prepared to take swift and effective action when necessary.**

26. [Cyber defence] Noting that cyber defence is primarily a national responsibility, ENCOURAGES Member States to further develop their own capabilities to conduct cyber defence operations, including proactive measures to anticipate, detect, respond and counter offensive operations against their networks, and possibly in support of other Member States. **EMPHASIZES that further developing these capabilities should be one of the key goals of the upcoming EU Cyber Defence Policy**. NOTES that the EU Cyber Defence Policy should give more consideration to what role the relevant EU institutions and bodies can play to complement this work and develop their own capabilities, as appropriate and according to their respective mandates. **CALLS on the High Representative together with the Commission to complement the development of an EU's cyber posture by proposing an ambitious Joint communication for an EU Cyber Defence Policy before the end of 2022, which will pave the way for the Council's further development of this posture.**

27. [Military cooperation] EMPHASISES the need to increase interoperability and information sharing through cooperation between military computer emergency response teams (Mil CERT). Building on the work of the EDA, **INVITES Member States to create a network of Mil CERT to develop cooperation and facilitate the exchange of information, as well as a network of the military cyber commanders in order to strengthen strategic cooperation between EU cyber commands**.

28. [Missions and operations] On the basis of the EU Military Vision and Strategy on Cyberspace as a Domain of Operations and taking note of the congoing development of the military Concept on Cyber Defence for EU-led military operations and missions, REITERATES the need to integrate the cyber dimension into the planning and conduct of CSDP missions and operations and STRESSES that this will contribute to better cyber situational awareness at EU level.

29. To conclude, NOTES that the Cyber posture will be a step towards establishing an EU doctrine for action in cyberspace, based on enhanced resilience, capabilities and response options, as well as a shared interpretation of the application of international law in cyberspace. WILL TAKE STOCK of the progress made on the implementation of these conclusions in the first semester of 2023 in order to ensure the further development of the EU's Cyber posture.