Council of the European Union

Brussels, 16 May 2022
(OR. en)

8594/3/22
REV 3

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

On behalf of the Presidency, delegations will find attached the revised draft Council Conclusions on the development of the European Union's cyber posture.

The revised document annexed herewith (8594/2/22 REV 3), takes into account the comments made by delegations at the HWPCI meetings on 3, 10 and 13 May as well as the written comments received (WK 6807/22 + ADD 1).

The CSDP –related paragraphs 14, 22, 27, 28 and 29, as agreed by the PMG on 16 May, are included into the text.

The amendments in the attached revision are indicated in underlined and bold text (**new**) and in strikethrough text (~~deletions~~).

Draft Council Conclusions on the development of the European Union's cyber posture

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING its conclusions on:

– the Joint Communication of 25 June 2013 to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace"[1]

– the EU Cyber Defence Policy Framework[2],

– Internet Governance[3],

– Cyber Diplomacy[4]

– Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[5]

– the Joint Communication of 20 November 2017 to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[6]

– a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox')[7],

– the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises[8],

– EU External Cyber Capacity Building Guidelines[9]

---

1 12109/13

2 15585/14.

3 16200/14.

4 6122/15 + COR 1.

5 14540/16.

6 14435/17 + COR 1.

7 10474/17.

8 10086/18.

9 10496/18.

– Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements[10],

– cybersecurity capacity and capabilities building in the EU[11] ,

– the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G[12]

– the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion"[13],

– complementary efforts to Enhance Resilience and Counter Hybrid Threats[14],

– shaping Europe's Digital Future[15],

– the cybersecurity of connected devices[16]

– the EU's Cybersecurity Strategy for the Digital Decade[17]

– Security and Defence[18],

– exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises[19],

---

10 OJ L 320, 17.12.2018, p. 28–34.

11 7737/19.

12 14517/19.

13 9596/19.

14 14972/19.

15 8711/20.

16 13629/20

17 7290/21.

18 8396/21.

19 13048/21.

– 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[20],

---

[20] 7371/22.

1. 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 malicious activities targeting the EU and its Member States' critical infrastructure, supply chains and intellectual property, **the increased risk of spillover effects** as well as a rise in ransomware attacks against our businesses, organisations and citizens ~~**and the increased risk of spillover effects**~~. NOTES that with the return of power politics, some countries are increasingly attempting to challenge and undermine the rules-based international 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 or attempts to intrude, disrupt or destruct network and information systems causing systemic effects have become more common, might undermine our economic security and affect our democratic institutions and processes, and show the readiness of some actors to risk international security and stability. UNDERLINES that Russia's military aggression against Ukraine has demonstrated that offensive cyber activities can be conducted 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, and that the implementation of the Strategic Compass will enhance the EU's strategic autonomy and its ability to work with partners to safeguard its values and interests, 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 rules-based international order, with the United Nations at its core.

3. In line with the Council Conclusions on 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 EU and its Member States using all available EU tools. This includes further demonstrating 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**, including** ~~or~~ the security of our partners. In that context, STRESSES that the cyber posture aims to combine the various initiatives that concur to EU actions consolidating peace and stability in the cyberspace and in favour of an open, free, global, stable and secure cyberspace, while better coordinating short, medium and long term actions to prevent, discourage, deter and respond to cyber threats and attacks and leveraging cyber 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; enhance solidary and comprehensive crisis management; promote our vision of cyberspace; enhance cooperation with partner countries and international organisations; prevent, defend against and respond to cyber-attacks.

I. STRENGTHEN OUR CYBER RESILIENCE AND CAPACITIES TO PROTECT

4. 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 (NIS), the draft Regulation on digital operational resilience for the financial sector (DORA), the draft Directive on critical entities resilience (CER) 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 these topics and to enable the support for companies in order to rise up to the challenge. CALLS upon the Commission to propose EU common cybersecurity requirements for connected devices **and related** ~~,~~ processes and services through the Cyber Resilience Act, which should be proposed by the Commission before the end of 2022, taking into account the need for a horizontal and holistic approach that covers the whole lifecycle of digital products ~~and services~~, as well as existing regulation, especially in the area of cybersecurity.

5. 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 EU 5G Toolbox.

6. 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, and STRESSES that encouraging the development of such providers should be a priority for the EU industrial policy in the cybersecurity field. In order to better resist and counter cyberattacks with potential systemic effects and drawing from the lessons of handling the Solarwinds, Microsoft Exchange and Apache Log4J- vulnerabilities, INVITES the Commission to propose options to encourage the emergence of trusted cybersecurity service industry, to strengthen the cybersecurity of the ~~digital~~ **and** ICT- supply chain, to address the potential effects of the software vulnerabilities for the EU and its Member States, including in view of the upcoming Cyber Resilience Act, as well as to improve cyber threat detection and sharing capabilities in and across Member States.

7. 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 research, 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.

8. 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 2 Directive, and INVITES the Commission to explore options to increase the cybersecurity across the whole supply chain of the EU's Defence Technological and Industrial Base (EDTIB).

9. ACKNOWLEDGES that ensuring adequate financial and human resources for cybersecurity and measures aiming at creating a conducive environment for the private sector to be competitive are essential to develop the EU's cyber posture and that the issue of stable and long term financing of cybersecurity should also be addressed at the EU level by designing and implementing a horizontal mechanism combining multiple sources of financing, including costs of highly qualified human resources. Therefore, CALLS UPON the Commission to explore options for such a mechanism before the end of 2022, to be discussed in the relevant Council bodies.

10. EMPHASISES the need to strengthen our efforts and increase cooperation in the fight against international cybercrime, in particular ransomware, through the EMPACT (European Multidisciplinary Platform Against Criminal Threats) mechanism, via exchanges between the cyber security, law enforcement and diplomatic sectors, and through strengthening **I**~~L~~law enforcement capabilities in investigating and prosecuting cybercrime. REITERATES its commitment to inform the public about cyber threats and the measures taken nationally and at EU level against these threats by involving civil society, private sector, and academia, with a view to raise awareness and encourage an appropriate level of cyber protection and cyber hygiene. STRESSES the need to focus on cyber security skills and capabilities of the citizens at EU and Member State level and the need to actively involve users in their own protection.

II. ENHANCE SOLIDARY AND COMPREHENSIVE CRISIS MANAGEMENT

11. 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 **regular** 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 the private sector, and which will be articulated and contribute to the general EU's exercise policy. EMPHASISES the importance of further developing Cyber Europe and BlueOLEx exercises, combining response across different levels. ACKNOWLEDGES the need to evaluate and consolidate the existing exercises and explore **the possibility of** further exercises on specific segments of the cyber domain, notably a military CERT exercise **and**~~or~~ an exercise focusing on crisis cooperation amongst EUIBAs. ACKNOWLEDGES that the Union's cyber posture will strengthen our abilities to prevent cyberattacks through various actions including training and thus INVITES Member States to enhance civilian-military cooperation in cyber training and joint exercises.

12. 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 (EU 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 EU 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. INVITES the Commission, the High Representative and the NIS Cooperation group, in coordination with relevant **civilian and military** bodies and agencies **and established networks, including** ~~as well as~~ the EU CyCLONe, to conduct by the end of 2022 risk evaluation and build risk scenarios from a cybersecurity perspective in a situation of threat or possible **attack**~~aggression~~ against Member States or partner countries and present them to the relevant Council bodies. EMPHASISES the need for appropriate and coordinated public communication on the EU response to large-scale cyber incidents.

13. In the event of large-scale cyber incident, STRESSES the need to reinforce the coordination, and, where appropriate, building on the progress achieved and work of PESCO Cyber Rapid Response Teams and drawing from the work of the CSIRT**s** Network and the EU CyCLONe, the voluntary pooling of our incident response capacities amongst Member States. 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 difference in the event of large-scale incidents. ~~With a view to complementing cooperation and mutual support cooperation amongst Member States,~~ **To fully prepare to face large-scale cyber incidents,** INVITES the Commission to **present a** propos**al one** a new Emergency Response Fund for Cybersecurity by the end of Q3 2022.

14. **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/or military support, including by exploring possible support provided by the EU upon an explicit request from Member States, and on identifying appropriate response measures, including through developing a coordinated communication strategy, in the context of the implementation of Article 42(7). NOTES that this should also include exploring the links with existing EU crisis managements mechanisms and the EU Civil Protection Mechanism.**

15. UNDERLINES that a reinforced EU cyber posture will require enhanced secure communications. To this end, REITERATES the orientations given by the Strategic Compass in that regard and INVITES the Commission and other relevant institutions, bodies and agencies to make by the end of 2022 a mapping of existing tools for secure communication in the cyber field to be discussed in relevant Council bodies and with relevant cooperation groups**, such as the CSIRTs network and the EU CyCLONe**.

III. **PROMOTE OUR VISION OF CYBERSPACE**

16. 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 dispute in cyberspace by peaceful means **and** the application of international Law, including International Human Rights Law and International Humanitarian Law~~, where applicable~~ to States' actions in cyberspace. UNDERLINES **the EU and its Member States'** commitment to act in accordance with the voluntary, non-binding norms of responsible State behaviour in cyberspace agreed by all UN Member States. STRESSES the importance of an open, free, global, 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 and REAFFIRMS the commitment of the EU and its Member States to continue promoting those values and principles. With a view to developing channels for constructive, frank and open dialogue with key cyberspace stakeholders, STRESSES the importance to make cyber issues, including the EU Cyber Diplomacy Toolbox, an integral part **of the Union accession negotiations and** of the EU's strategic and political dialogues with international partners and competitors alike, at the same time, CALLS on the High Representative to review the existing bilateral cyber dialogues and, if necessary, propose to start similar cooperation with additional countries or relevant international organizations.

17. 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 taken in the international and regional fora. CALLS on the EU and its Member States to further promote our model of cyberspace and Internet based on the multi-stakeholder approach and through initiatives such as the Paris Call for trust and security in cyberspace and the Declaration on the Future of the Internet, emphasising the shared benefits of 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.

18. COMMITS itself to continuous engagement in relevant international organisations especially in the UN First and Third committees related processes**, while emphasizing that existing international law applies, without reservation, in and with regard to cyberspace**. **STRESSES the importance of continued efforts to uphold and promote the UN Framework for responsible state behaviour, and UNDERLINES that the EU and its Member States will actively work towards strengthening its implementation, including through the establishment of the Programme of Action for advancing responsible State behaviour in cyberspace (PoA).** EMPHASIZES that the EU and its Member States will actively engage in the negotiations for a future UN Convention to serve as an effective instrument for law enforcement and judicial authorities in the global fight against cybercrime, taking into full consideration the existing framework of international and regional instruments in this field, in particular the Budapest Convention on Cybercrime. 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 cyber CBMs at the OSCE, including in times of international tensions.

19. RECALLS that taking a proactive human rights-based approach to ensuring international standards in the areas of emerging technologies and the core internet architecture in line with democratic values and principles is essential to ensure that the Internet remains global, unfragmented and open, and SUPPORTS that the use and development of technologies are human **rights respecting** ~~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 in the digital field that have foreign policy implications and could have an impact on the stability of cyberspace and the Internet in particular, including in the relevant specialised international organisations (International Telecommunications Union etc.).

IV. ENHANCE COOPERATION WITH PARTNER COUNTRIES AND INTERNATIONAL ORGANISATIONS

20. 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 adequate coordination of efforts between Member States and EU institutions, bodies and agencies, and, in particular WELCOMES cooperation among~~st~~ Member States, as well as with public and private sector partners, notably through the EU CyberNet (EU's Cyber Capacity Building Network) and the Global Forum on Cyber Expertise (GFCE), to ensure coordination and avoid duplication.

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), Instrument for Pre Accession Assistance (IPA III) and other financial tools, such as the European Peace Facility (EPF) and the Global Gateway Initiative, to support the strengthening of the resilience of our partners, their capacities to identify and address cyber threats and to investigate and prosecute cybercrimes, and the development of cooperation projects, including in the context of crisis, in particular, ENCOURAGES cooperation with partners in the Western Balkans and in the EU Eastern and Southern Neighbourhood, and the deployment of EU and Member States' experts to offer support in cyber crises, taking into considerations existing legal mandates.

21. 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 application of international Law in cyberspace, UN framework of responsible State behaviour in cyberspace, including the initiative for a Programme of Action for advancing responsible State behaviour in cyberspace (PoA) , as well as on the EU and its Members States' position in the ongoing negotiations of a UN Cybercrime Convention, 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 and systematic use of its 145 Delegations and develop regular, fruitful collaboration between them 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.

22. 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. **RECALLING the key achievements of EU-NATO cooperation in the area of cybersecurity in the framework of the implementation of the 2016 Warsaw and 2018 Brussels Joint Declarations, 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, EMPHASISES the need to further strengthen cyber cooperation with NATO through exercises, information sharing and exchanges between experts, including on capability development, capacity building for partners, and missions and operations, as well as on the applicability of international law and UN norms of responsible state behaviour in cyberspace, and possible coordinated responses to malicious cyber activities.**

V. PREVENT, DEFEND AGAINST AND RESPOND TO CYBER-ATTACKS

23. RECOGNISES that cyberspace has become and arena for geopolitical competition and therefore REITERATES that the EU must be able to swiftly and forcefully respond to cyberattacks, ~~such as state-sponsored~~ **especially, but not limited to,** malicious cyber activities **attributable to third states** targeting **the** EU and its Member States 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 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 Q1 202**3~~2~~, notably by exploring additional response measures**.

24. UNDERLINES the need to hold regular exchanges on the cyber threat landscape in relevant bodies and committees of the Council, while also engaging regularly with the private sector and drawing from the assessment on the impact and severity of recent incidents, to increase the overall awareness and preparedness for further applications of the EU 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 and information 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~~ **including on the question of** ~~coordinated~~ **attribution,** and thereby enable a swift, effective and substantiated response to malicious cyber activities targeting the EU and its partners. REITERATES the importance to strengthen the EU 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.

25. 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 constituting an external threat to the EU, its Member States and partners 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, including the UN Charter in its entirety, and foster the UN framework of responsible State behaviour, **including** ~~in particular~~ the **due diligence** obligation for all States to **not knowingly allow their territory to be used for internationally wrongful acts using ICTs**~~carry out due diligence in order to avoid their territory being used for malicious cyber activity~~, with a view to **further** developing and promoting **the**~~an~~ EU **shared view**~~position~~ on the application of International Law in cyberspace. Noting that appropriate 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 EU Cyber Diplomacy Toolbox.

26. ENCOURAGES the development of gradual, targeted and sustained approaches and responses to cyber malicious activities, using the wide range of tools provided by the EU 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 based on long-term strategic engagement. CALLS upon the High Representative, in cooperation with the Commission, to identify 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 and present them by the end of **Q1** 2023~~2~~ to the Council.

27. 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 protect, detect, defend and deter against cyberattacks, and possibly in support of other Member States and the EU. Each Member State is encouraged to enhance, as necessary, its own abilities to provide and receive aid and assistance. EMPHASISES 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 increase cooperation among the EU's and Member States' relevant cyber defence actors and develop their own capacities, according to their respective mandates. INVITES the High Representative together with the Commission to complement the development of an EU's cyber posture by tabling an ambitious proposal for an EU Cyber Defence Policy in 2022, which will pave the way for the Council's further development of the EU's cyber posture.

28. **EMPHASISES the need to increase interoperability and information sharing through cooperation between military computer emergency response teams (milCERT). INVITES Member States to create, building on the work of the EDA, a network of milCERT to develop cooperation and facilitate the exchange of information, which would also help foster coordination with other cyber communities, as well as a network of the military cyber commanders in order to strengthen strategic cooperation between EU Member States' cyber commands or other corresponding authorities. The setting up of these networks, along with cyber PESCO projects, would contribute to a strengthened cyber defence at EU level. Stresses the importance of cooperation between the proposed milCERT network with the already existing civil (CSIRTs) network to enhance information sharing and improve situational awareness.**

29. On the basis of the EU Military Vision and Strategy on Cyberspace as a Domain of Operations and taking note of the ongoing 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, including by enhancing their cyber capabilities, and STRESSES that this will contribute to better cyber situational awareness at EU level.

30. 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 position on the application of international Law in cyberspace. The Council 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.