Council of the
European Union

Brussels, 8 June 2023
(OR. en)

10289/23

LIMITE

CYBER 142
COPS 297
POLMIL 137
RELEX 693
JAIEX 30
TELECOM 191
CFSP/PESC 819

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Revised Implementing Guidelines of the Cyber Diplomacy Toolbox

Delegations will find attached the Revised Implementing Guidelines of the Cyber Diplomacy Toolbox.

ANNEX

REV IMPLEMENTING GUIDELINES OF THE CYBER DIPLOMACY TOOLBOX

1. INTRODUCTION

1. In 2017, the EU adopted the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox')[1] to increase the EU's ability to prevent, discourage, deter and respond to malicious cyber activities. With the adoption and implementation of the Cyber Diplomacy Toolbox, the EU took an important step towards a more secure and stable cyber domain, providing an answer to the increased willingness and ability of state and non-state actors to pursue their strategic objectives through malicious cyber activities. In the last few years, however, and particularly since Russia's unjustified and unprovoked war of aggression against Ukraine, the EU and its Member States have seen a significant corrosion of international security, including in cyberspace. Malicious cyber activities against critical infrastructure, including through the use of ransomware and wipers, as well as targeting of supply chains and cyber-espionage, including intellectual property theft activities or similar types of cyber-espionage, are increasingly more sophisticated, with disruptive and destructive effects posing a systemic threat to the EU's security, economy, democracy and society at large. Such activities can also be used to conduct or enable foreign information manipulation and interference (FIMI).

[1] 13007/17 – Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities

2. The increase of malicious cyber activities over recent years has provided lessons for the EU, its Member States and their partners on how to enhance cyber resilience, as well as on how to design and implement an appropriate response, including through the use of diplomatic measures. With the unstable cyber threat landscape, the EU and its Member States need to step up their ability to strengthen situational awareness, prevent, discourage, deter and respond to malicious cyber activities, ensure solidarity and mutual assistance and enforce the United Nations framework for responsible state behaviour in cyberspace endorsed by consensus by the United Nations General Assembly, grounded in the application of international law in cyberspace.

3. At the same time, cyber diplomacy and cyber issues have gained momentum and importance as a component of EU Common Foreign and Security Policy (CFSP). With the pervasiveness and fast pace of digitalization and the magnitude of cyber challenges and of the threat landscape, cyber diplomacy needs to be strengthened and could be further complemented by making use of other policies and activities in order to effectively contribute and promote the European vision of a global, open, free, stable and secure cyberspace, grounded in the rule of law. Strengthening global partnerships as well as pro-active, preventive and constructive diplomatic action is increasingly needed. In this context, a more sustained, tailored, coherent and coordinated EU approach is necessary to advance a comprehensive and effective EU action against malicious cyber activities, large-scale cybersecurity incidents and an accumulation of those activities, as well as to persistent cyber threat actors that conduct, support or condone malicious cyber activities targeting the EU, its Member States and their partners.

4. Building on the main principles of the framework as set out in the 2017 Council conclusions on the Cyber Diplomacy Toolbox[2], the Council conclusions on the EU Cyber Posture of 2022[3], and the lessons learned from diplomatic responses and cyber exercises undertaken since 2017, this document responds to the need to further strengthen the EU Cyber Diplomacy Toolbox as expressed in the 2021 Council conclusions on the EU Cybersecurity Strategy[4], the 2022 Strategic Compass[5], the 2022 Council conclusions on the EU Cyber Posture and the 2023 Council Conclusions on the Joint Communication on the EU Policy on Cyber Defence[6]. The document also relates to the 2022 Council conclusions on EU Digital Diplomacy[7], specifically taking into account that the EU external policies on digital and cyber need to be coherent and mutually reinforcing. This document outlines the revised implementing guidelines to further enhance situational awareness, ensure a strategic approach to persistent cyber threat actors, provides additional response measures[8], and further enables timely decision-making and stronger cooperation with partners. In addition, it includes guidance for the attribution of malicious cyber activities, strategic communications, as well as linkages to other EU toolboxes and crisis management mechanisms and activities, while preserving Member States competences on the matter.

[2] 9916/17 – Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")

[3] 9364/22 – Council conclusions on the development of the European Union's cyber posture

[4] JOIN/2020/18 final – Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade

[5] 7371/22 – 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

[6] 9618/23 – Council Conclusions on the EU Policy on Cyber Defence

[7] 11406/22 – Council Conclusions on EU Digital Diplomacy

[8] Listed in a separate annex.

2. FRAMEWORK FOR AN EU DIPLOMATIC RESPONSE AGAINST MALICIOUS CYBER ACTIVITIES

5. Core to the EU Cyber Posture are the following five main components: its cyber resilience and capacities to prevent and protect against malicious cyber activities; its solidarity and comprehensive crisis management capabilities; its vision of a global, open, free, stable and secure cyberspace, with international law, the rules-based order and with the UN framework for responsible state behaviour in cyberspace at its centre; its strong global partnerships, including through capacity building efforts in third countries; and its ability to prevent, discourage, deter and respond to threat actors seeking to deny or disrupt our secure and open access to cyberspace as well as critical functions, and affect the EU's strategic interests, including the security of its partners.

6. In line with this posture, the Cyber Diplomacy Toolbox is part of the EU's full spectrum approach to resilience, response, conflict prevention, cooperation and stability in cyberspace. It should be seen as complementary to existing and continuous cyber diplomacy engagement to advance conflict prevention, cooperation and stability in cyberspace, including substantive EU capacity building support to third countries. In addition it complements the EU effort to enhance cyber resilience, prevent and tackle cybercrime as well as adds value to the development of the wider EU cyber cooperation, solidarity and crisis management eco-system.

7. The joint EU diplomatic response builds on the UN framework for responsible state behaviour in cyberspace grounded in the reports of the UN Groups of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security and Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies, which concluded that existing international law is applicable to the use of cyber operations, and outlines eleven voluntary, non-binding norms of responsible State behaviour in cyberspace. Through the use of diplomatic measures, the EU actively supports the global application of the UN framework of responsible state behaviour, contributes to its enforcement, and enhances transparency and predictability as regards states' conduct in cyberspace. The use of confidence-building measures (CBMs) at regional and international level, notably in those of the Organization for Security and Co-operation in Europe (OSCE), could further reduce the risk of a potential conflict and misunderstanding between States as to their conduct in cyberspace.

8. The measures in the Cyber Diplomacy Toolbox could be used in tandem with other Union measures such as those reflected in the Network and Information Security Directive[9], the Directive on Attacks against Information Systems[10], as well as measures by EUIBAs, including by the EU Cybersecurity Agency (ENISA) and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), and EU networks, in line with their legal mandates and institutional autonomy, to prevent, discourage, deter and respond to and immediately recover from malicious cyber activities which may originate from a state or non-state actor or transit through a States' territory. The measures could inter alia be used to encourage a State to ensure that its territory is not used for malicious cyber activities, or to induce a State to refrain from, or cease activities that are undertaken under its direction or its control.

[9] L 333/80 – Directive (EU) 2022/2555 of the European parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) 10 L 218/8 – Directive 2013/40/EU of the European parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

9. The EU approach will vary in accordance with a situation of peacetime, crisis or armed conflict. The Cyber Diplomacy Toolbox could be used as a response to malicious cyber activities that do not rise to the level of internationally wrongful acts but are considered as unfriendly acts. In addition, the Cyber Diplomacy Toolbox can be used to support further EU or Member States' action in response to internationally wrongful acts directly or indirectly affecting EU interests including armed attacks involving a cyber-component. To this end, consistent with the relevant international law and without prejudice to the specific character of the security and defence policy of Member States, it could also be used in the context of the application of Article 42(7) of the Treaty of the European Union (TEU)[10], when invoked by a Member State or, in case of a Member States being a victim of a man-made disaster, via Article 222 of the Treaty on the Functioning of the European Union (TFEU)[11]. It can also support the wider compliance with existing international law, including the UN Charter, and specifically its Article 2(4) (prohibition of the use of force), Article 33 (peaceful settlement of disputes) and Article 51 (inherent right to act in individual or collective self-defence in response to an armed attack).

10. The Cyber Diplomacy Toolbox allows diplomatic measures to be used in a single response to an immediate cyber threat or activity, or as part of a sustained, tailored, coherent and coordinated strategy towards a particular actor. The EU Cyber Diplomacy Toolbox offers options for consideration. It does not preclude other actions by EUIBAs, in particular law enforcement or judicial action, nor any action of individual Member States or those coordinated between Member States and should strive for alignment.

[10] C 326/39 – Consolidated version of the treaty on European Union

[11] C 326/49 – consolidated version of the treaty on the functioning of the European Union

11. Enhanced understanding of the application of international law and the norms of responsible state behaviour in cyberspace, and the ongoing conduct of risk assessments and building risk scenarios could help foster a common, coherent and consistent understand of the situations in which the Cyber Diplomacy Toolbox might apply. Elements that could determine whether a cyber-attack or a series of malicious cyber activities have a significant effect as set out in Article 3 of the horizontal cyber sanctions regime[12] could support the considerations in this context.

12. States have a due diligence obligation under international law to not knowingly allow their territory to be used for acts contrary to the rights of other States and may also call on other States to cooperate in managing cyber incidents, in accordance with the UN framework for responsible state behaviour in cyberspace. In addition, agreed norms of responsible State behaviour affirm, *inter alia*, that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, and should respond to appropriate requests for assistance by another State. The EU and its Member States can request States to take appropriate measures to prevent or address cyber incidents that originate from their territory, bearing in mind that the indication that a cyber-attack emanates from the territory or the infrastructure of a State does not, of itself, imply responsibility of that State for the incident, or that notifying a State that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act itself.

[12] 2019/797 Council Decision (CFSP) concerning restrictive measures against cyber-attacks threatening the Union or its Member States

3. EU APPROACH AND MEASURES

13. In line with the 2017 Council conclusions on the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), and its use since then, the measures within the framework should continue to be based on the following six principles: protect the integrity and security of the EU, its Member States and their citizens; take into account the broader context of the EU's external relations with the State concerned; provide for the attainment of the CFSP objectives as set out in the Treaty on the European Union and respect the respective procedures for their attainment; be based on a shared situational awareness among Member States and correspond to the needs of the concrete situation at hand; be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the malicious cyber activity; comply with applicable international law and respect human rights and fundamental freedoms.

14. In line with the above principles, the full spectrum of measures can be used through EU diplomatic engagement, with a view to prevent, discourage, deter or respond to cyber threat actors and malicious cyber activities. The measures part of the Cyber Diplomacy Toolbox presented are forms of diplomatic, political, legal, strategic communication, technical, operational or economic actions, focussing on the delivery of a preventive, stabilising, cooperative, normative, restrictive, supportive or mitigative effect. To strengthen the joint EU diplomatic response to malicious cyber activities, the EU has identified additional measures, including building further global partnerships in view of diplomatic responses, raising awareness, notably making use of the publication of advisories, coordinated action to counter malicious foreign intelligence activities, suspension or cancellation of engagements or dialogues, as well as exploring the possibility to use sectoral sanctions and exploring the possibility to amend or extend the EU cyber sanctions regime. These additional measures may be deployed alongside targeted cyber capacity building in third countries, training and exercise activities, rapid response and mutual assistance actions. The decision-making on the measures should, where relevant and possible, take into account ongoing law enforcement actions against cybercrime, notably those addressing ransomware. Member States and the EU can implement measures individually or jointly, in coordination or in parallel, and where appropriate in cooperation with international partners.

15. Reflecting on the use and exercises of the Cyber Diplomacy Toolbox since 2017, the incident-based approach is complemented with the development of sustained, tailored, coherent and coordinated strategies towards persistent cyber threat actors, to ensure a more strategic, gradual and long-term approach. Supported by the High Representative in coordination with Commission services and relevant agencies and bodies and relevant EU networks, the Council will formulate such strategies and monitor their implementation, in the form of strategic response notes, for the main cyber threat actors. The strategic response notes should be based on risk assessments and risk scenarios, and anchored in relevant geographic strategies and developed in coordination with the corresponding working parties, as appropriate. The strategies should capture the short-term effect of a measure, as well as its longer term effect related to objectives formulated in such strategies. They would also allow the challenges of continued lower level threats and activities stemming from persistent cyber threat actors to be addressed. Notably, it should allow the threat actor's perspective and aims to be better taken into account, noting that individual characteristics and interrelations between the EU and the cyber threat actor play a role in the effectiveness of measures. Risk assessments should support the development of such strategies and support the monitoring of their impact.

16. Essential to the design of such strategies is the need for a gradual use of diplomatic measures corresponding to the pattern of continuous malicious cyber activities, while promoting conflict prevention, cooperation and stability in cyberspace. In this regard, awareness raising, dialogue, demarches or CBMs should be considered as a preferred option of engagement with a state, in particular in the case of a State's territory used for malicious cyber activities.

4. SHARED SITUATIONAL AWARENESS

17. Before any joint EU response can be considered, timely and continuous sharing of detailed information will be of key importance. Through regular briefings and information exchange, a baseline understanding and shared awareness of the cyber threat landscape will serve as the basis for assessments following a malicious cyber activity or cyber incident. The Horizontal Working Party on Cyber Issues (HWPCI) plays a central role in evaluating the situational awareness provided in view of a joint EU diplomatic response. However, when relevant, threat assessments and briefings can be discussed in other relevant Council formats and EU networks in view of other possible and appropriate EU action; in such cases, HWPCI needs to be informed.

18. Shared situational awareness among Member States has the purpose of enabling the EU and Member States to take a collective decision whether or not to use one or several measures as part of the Cyber Diplomacy Toolbox, including those in support of partners. Member States are not obliged to provide information or analysis. However, Member States are encouraged to strengthen information sharing, including cyber forensic and technical information through the appropriate channels, as the comprehensive and shared situational awareness is the foundation of an effective EU response. Contributions by Member States to the Single Intelligence Analysis Capacity (SIAC) as well as other relevant EUIBAs can support the EU's shared situational awareness and swift, informed and effective decision-making.

19. Ongoing and regular exchanges on the cyber threat landscape and thematic briefings in the HWPCI will enable Member States and the EU to develop and maintain a shared understanding on malicious cyber activities and how these affect the Member States and the EU. Such assessments and briefings should be provided by the SIAC, the central entity providing situational awareness and playing the leading role in analysing all-source information and providing intelligence assessments on cyber threats, with the support of other relevant EUIBAs with responsibilities for situational awareness and/or crisis response, such as the Commission, ENISA, CERT-EU, Europol, and possible future actors.

20. Where appropriate, such knowledge can be complemented by the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) providing information on the severity of the malicious activities conducted. Such assessments and briefings should always take place in respect of each stakeholder’s mandate. Information sharing should be further developed with trusted international partners and international organisations. To this end, partners may be invited to the relevant Council format or EU network if it would support enhanced situational awareness within the EU.

21. Additional operational, law enforcement, judicial, diplomatic or defence channels might also be used to further exchange information between Member States, or request more information from third countries or other relevant bodies such as international partners and international organisations. Where appropriate, cooperation with the private sector or other external stakeholders could further enhance the EU’s understanding of the threat landscape and in this way support EU diplomatic action to respond to malicious cyber activities. In this regard, appropriate attention should be given to the classification of information and the interests of all parties involved. Furthermore, regular exchanges with thematic and geographical working parties should enhance the understanding as regards the broader geopolitical situation and the EU’s international relations, further informing the decision-making process under the Cyber Diplomacy Toolbox, in particular related to the strategic response notes.

5. IMPLEMENTATION OF THE EU CYBER DIPLOMACY TOOLBOX

22. Timely decision-making on a response to malicious cyber activities, taking into account appropriate analysis of the situation, is crucial in ensuring a cyber threat actor's accountability, building on the UN framework of responsible state behaviour in cyberspace. It can enhance also the credibility of the EU in its diplomatic responses and avoid reputational damages.

23. In case of a crisis for which the Integrated Political Crisis Response (IPCR) arrangements[13] have been activated, following the appropriate agreed procedures and decision-making processes to handle a crisis at EU level, measures within the Cyber Diplomacy Toolbox could be part of the EU response at the political level.

24. In relevant situations where the IPCR has not been activated, the Council decision-making procedures and the EU Cybersecurity Crisis Response Framework as set out in Commission Recommendation (EU) 2017/1584[14] apply, in their respective domain of competence, taking into account the respective procedures for the attainment of measures as part of the Cyber Diplomacy Toolbox.

In order to implement the Cyber Diplomacy Toolbox, the following step-by-step process applies:

[13] 1078/13 – Integrated Political Crisis Response (IPCR) arrangements

[14] 2017/1584 – Commission recommendation (EU) on coordinated response to large-scale cybersecurity incidents and crises

1. Start discussions on the use of measures part of the EU Cyber Diplomacy Toolbox

When a persistent cyber threat, a malicious cyber activity or a large-scale cybersecurity incident has been detected or a partner's request for support has been made, (the) Member State(s) or European External Action Service (EEAS), with inputs from the Commission services when relevant, can inform Council on the activity, as well as express an interest in exchanging shared situational awareness, and exploring a joint EU diplomatic response.

2. Exchange of shared situational awareness

Building on the consistent level of shared situational awareness of the HWPCI on the cyber threat landscape, SIAC and other relevant actors could upon request provide further specific assessments or briefings, both orally and in writing. Timely contributions to SIAC by Member States are essential for strengthening shared situational awareness. Commission services and other relevant EUIBAs or partners can support the EU's shared situational awareness at all levels, and enable a swift and effective exchange of information in view of decision-making on a diplomatic response. If relevant in the specific situation, the private sector can also be invited to share information.

Where appropriate, geographical working parties should be invited to the HWPCI to enhance the understanding on the EU's broader international relations, further informing the decision-making process under the Cyber Diplomacy Toolbox.

3. Exploration of a possible joint EU diplomatic response

Following the exchanges on the situational awareness provided, any Member State or EUIBAs may propose or request to consult the Council for a joint EU diplomatic response. On the basis of this proposal or request, relevant information should continue to be exchanged to enhance the shared situational awareness and support the ongoing deliberations on whether any action should be taken.

In view of a response to a persistent threat actor or a series of malicious cyber activities, such request may include a call for a 'strategic response note' that outlines or updates a sustained, tailored, coherent and coordinated strategy towards that particular threat actor or malicious activity. Such note should include multiple measures that could be implemented in parallel or sequential, and should be tailored in view of influencing the particular threat actor's malicious behaviour. The proposed measures should take into account the scope, scale, duration, intensity, complexity, sophistication and impact of the malicious cyber activity and their individual implementation as part of the overall strategy is subject to agreement in the relevant Council body. The EEAS will coordinate with the Commission services and relevant agencies and bodies in the development of strategic response notes.

In case of a swift, single joint EU diplomatic response to a malicious cyber activity, the HWPCI could request the EEAS, where relevant with support of the Commission services and relevant agencies and bodies, to outline the possible response options, where necessary by providing an options note. Such immediate response, without undue delay could be part of an existing sustained, tailored, coherent coordinated strategy to a particular persistent threat or threat actor, or could be a single response to a malicious cyber activity.

4. Deliberations on a possible joint EU diplomatic response

The HWPCI plays, under the guidance of the Political Security Committee (PSC) and COREPER, a central role in decision-making as regards a joint EU diplomatic response. Further coordination between the HWPCI and other thematic and geographical working parties and EU networks could take place in view of coherence with other possible and appropriate EU actions. Further coordination between EUIBAs could take place to identify available capabilities, ensure their coordinated deployment when necessary, fully linked with the wider crisis management response. Such coordination could also take place on strategic communication, whether made public or not.

Depending on the timeframe and the case, deliberations may take place orally or in writing, including through the use of the Correspondance Européenne (COREU)/CORTESY network.

Member States may deliberate on accompanying the diplomatic response with attribution.

5. Decision-making on the use of EU Cyber Diplomacy Toolbox

In situations where the IPCR has not been activated, the Council decision-making procedures apply, taking into account the respective procedures for the attainment of measures as part of the Cyber Diplomacy Toolbox. Where the use of restrictive measures is concerned, the competent preparatory bodies within the Council, in addition to the HWPCI, the Working Party of Foreign Relations Counsellors (RELEX) and relevant geographical working parties, should be involved. In addition, the HWPCI, within the framework of the CFSP, EEAS, and where relevant the appropriate Commission services, agencies and bodies, could discuss the implementation of the diplomatic response, including strategic communication efforts. When necessary and appropriate, the High Representative could use its discretionary role within the CFSP to ensure a swift response to a malicious cyber activity that falls within the area of this policy. Depending on the timeframe and case, the use of the COREU/CORTESY network as well as simplified written procedure as set out in Article 12.2.d of the Council Rules of Procedure where it is appropriate could support swift decision-making by the Council.

6. Implementation of the Cyber Diplomacy Toolbox

Depending on the measure(s) chosen, Member States and the EEAS, where relevant in relation to the chosen measure with support of the Commission services and relevant agencies and bodies, implement the measures following the guidance provided by the Council for their attainment.

7. Cooperation with international partners

Where relevant, international like-minded partners, including international organisations, may be involved to support the joint EU diplomatic response to malicious cyber activities or conduct coordinated, and where desirable joint, responses. The EU may also support, where relevant, international like-minded partners in their diplomatic activities. In the context of the Cyber Diplomacy Toolbox, the EEAS has a central role in the coordination with international partners, both in case of the EU requesting support, or in case a request for a joint EU diplomatic response is made to the EU by a partner, provided that the latter directly or indirectly affects EU interests. The EEAS will regularly and timely inform the HWPCI on the coordination and cooperation with international partners. In cases of an international partner requesting a joint EU diplomatic response, the relevant European Commission’s services should also be informed.

The procedure for alignment of EU candidate and associated countries, as implemented by the EEAS, applies.

8. Evaluation of the impact of the joint EU diplomatic response

The HWPCI will continue to follow up on the implementation as well as lessons learned. It will regularly monitor the situation and the effect of the measures with support of the EEAS, Commission services and other relevant EUIBAs, in view of tailoring possible further measures.

This process should, when relevant, feed into strategic response notes.

9. Continued discussion to maintain a sustained engagement

In view of a sustained approach, Member States may request to revisit the relevant steps of the process, should additional measures be required to respond to a cyber threat or a persistent activity.

6. ATTRIBUTION

25. Attribution can be defined as a practice of assigning a malicious cyber activity to a specific state or non-state actor. Political attribution is a sovereign political decision of Member States taken on a case-by-case basis. Based on shared situational awareness and the sharing of detailed information, coordinated political attribution at EU level can be pursued. Technical attribution, the investigation and assessment based on intelligence and technical evidence, contributes to appropriate decision-making.

26. Diplomatic measures may be accompanied by attribution, however, this may not necessarily take place. Coordinated political attribution at EU level, or with the EU's likeminded partners, when communicated to others, either privately or publicly, has the potential to strengthen the ability to influence the behaviour of malicious actors in cyberspace.

27. Not all measures require attribution, for example diplomatic measures may be involved in preventing or resolving a cyber-incident, expressing concerns and signalling them in another way.

28. Political attributions can *inter alia* be used to expose the specific malicious cyber activity or specific actor, enable mitigating initiatives, promote the UN framework for responsible state behaviour, demonstrate capability to identify its origin, discourage future malicious cyber activities, as well as to enable other response options to be used sequentially or in combination with the attribution and raise awareness about the cyber threat landscape.

29. When discussing the appropriateness of coordinating political attribution, and while deciding whether and how to communicate about coordinated attribution, either privately or publicly, it could be useful for the Council to consider the following:

- desired effect of the political attribution
- contribution to the protection of the integrity and security of the EU, its Member States and their citizens and businesses;
- importance of showing unity within the EU and between its Member States or solidarity with a third party;
- contribution to the advancement of responsible state behaviour, including compliance with international law and respect for voluntary norms;
- ability to influence the behaviour of malicious actors in cyberspace;
- impact on the ongoing work of services such as law enforcement or intelligence services;
- likelihood and impact of a counter-response by any actor (risk of escalation);
- consequences for existing EU external relations, at the international, regional and bilateral levels;
- reputation and credibility of the EU (risk of the bystander effect, risk of manipulation, precedence of a malicious cyber activity);
- predictability and coherence of joint EU responses in previous and/or future cases.

These considerations could also be taken into account when deciding on other measures part of the Cyber Diplomatic Toolbox.

7. STRATEGIC COMMUNICATION

30. In order to enhance the EU's ability to prevent, discourage, deter and respond to malicious cyber activities and strengthen the EU's cyber posture in this regard, strategic communication of EU action is essential, both at the EU and at Member States level. Coordination on the use and consistent implementation of EU instruments, products and channels could support and strengthen the EU's sustained, tailored, coherent and coordinated approach. In particular, communication could raise awareness, promote the EU's vision for cyberspace, or the EU cyber policy and legislative cyber standards, and build the EU cyber posture by communicating about targeted EU actions to counter malicious cyber activities. It could also be used to mitigate potentially destabilizing societal effects of malicious cyber activities. While crisis communication plays a particularly important role in mitigating the negative effects of cybersecurity incidents and crises, strategic communication may also be used as a means to influence the behaviour of partners and/or potential threat actors. Aligning these objectives for public communication is essential for a diplomatic response to be effective.

31. The inter-institutional coordination of communication efforts among EUIBAs could further strengthen the EU cyber posture, ensuring coherent communication across communities. The use of visible communication tools and products, such as videos, factsheets, international conferences or the use of social media, could also highlight the EU response to partners and to the public, enhancing the EU cyber posture as to its cyber resilience and response capacities. Member States are encouraged to actively participate in the conceptualisation and implementation of communication efforts, including by amplifying the communication by the EU, reinforcing the effect of a joint EU diplomatic response to malicious cyber activities.

32. The efforts should also focus on reaching out to a wider global audience, supporting the adherence to the UN framework of responsible state behaviour in cyberspace and developing and promoting a narrative on responsible and cooperative behaviour, as well as on accountability in cyberspace and the need to use diplomatic efforts and measures to achieve this. In this context, EU coordination on outreach within multilateral and regional fora and towards third countries is necessary. Regional and cultural aspects should also be taken into account. EU Delegations and Member States' embassies could be involved to further amplify the EU communication, including by translating this into the local context.

8. COHERENCE WITH EU'S DIGITAL DIPLOMACY, OTHER TOOLBOXES AND RELEVANT CRISIS MANAGEMENT MECHANISMS

33. EU external policies on digital and cyber issues, as well as countering hybrid threats, including FIMI, should be coherent and mutually reinforcing. Due to geopolitical dynamics, cyber and digital issues are increasingly intertwined at the international level. Activities carried out as part of the Cyber Diplomacy Toolbox need to be closely coordinated whenever possible with the EU's digital diplomacy, and vice versa.

34. Further, the EU Cyber Diplomacy Toolbox aims to swiftly and resolutely respond to cyber threats and attacks and could contribute to the EU's response to a hybrid campaign, in line with its own rules and procedures. While remaining an autonomous mechanism, it could be used in parallel or in the context of the framework for a coordinated EU response to hybrid campaigns ("EU Hybrid Toolbox"[15]), or in parallel or coherence with the Foreign Information Manipulation and Interference Toolbox ("FIMI Toolbox"[16]), noting the context, threat landscape, potential threat actors as well as potential victims. In a situation that could require or allow multiple toolboxes to be used, the EEAS, appropriate Commission services as well as relevant Council bodies, notably the HWPCI and the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP-ERCHT), as appropriate, should coordinate as regards the design and implementation of measures as well as the appropriate decision-making process. Regular exchanges on the respective strategic, sustained and tailored approaches to threat actors, as well as on the wider context of hybrid campaigns, malicious cyber activities and foreign information, manipulation and interference, including disinformation, threat landscape between the relevant working parties could ensure coherence, effective response and avoiding duplication as regards the EU's external action.

35. The measures as part of the framework can be of use both in response to a large-scale cross border malicious cyber activity, as well as a situation of an accumulation of malicious cyber activities targeting the EU, its Member States or their partners. Being part of the wider EU crisis management eco-system, the Cyber Diplomacy Toolbox can be implemented as part of, or in parallel and in complementarity of crisis management mechanisms, including the EEAS Crisis Management Response Mechanism[17], and its use of the EEAS Situation Room and the EU Delegations Network, IPCR, as well as the Union Civil Protection Mechanism[18].

[15] 15546/22 – Implementing guidelines for the Framework for a coordinated EU response to Hybrid campaigns

[16] 11429/22 – Council conclusions on Foreign Information Manipulation and Interference (FIMI)

[17] https://www.eeas.europa.eu/eeas/crisis-management-and-response_en

[18] https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en

36. To ensure coherence between internal and external EU action, cooperation with Member States, notably with CSIRTs Network and EU-CyCLONe, aiming to be the link between the technical and political levels, and between the EEAS, including SIAC, the Commission services, ENISA, CERT-EU and Europol, is essential.

37. In case of the activation of the IPCR mechanism, the 2017 Blueprint on the EU coordinated response to large-scale cybersecurity incidents and crises[19] addresses the role of all relevant actors, outlining the functioning of the EU cyber crisis management eco-system. In such situation, the HWPCI and other relevant decision-making bodies could consider using measures as part of the EU Cyber Diplomacy Toolbox as part of the Union response. The IPCR is also used to coordinate the response to the invocation of the solidarity clause (Article 222 of the TFEU) to ensure the coherence and complementarity of Union and Member State action[20].

[19] 2017/1584 – Commission Recommendation (EU) on coordinated response to large-scale cybersecurity incidents and crises

[20] OJ L192/53 – Council Decision on the arrangements for the implementation by the Union of the solidarity clause

9. COOPERATION WITH PARTNERS, INCLUDING INTERNATIONAL ORGANISATIONS, THIRD COUNTRIES AND PRIVATE SECTOR

38. Cooperation with international partners can amplify coordinated responses and enhance the ability to influence the behaviour of malicious actors in cyberspace. Such cooperation provides the opportunity to strengthen the international rules-based order and hold threat actors accountable for their behaviour in cyberspace. Building on the lessons learned from cooperative efforts to date, shared situational awareness on the overall cyber threat landscape between the EU and its partners can help setting a baseline understanding and supports the development of a coordinated sustained, coherent and tailored approach to different threat actors, or a joint or coordinated single responses in case of a concrete request. Such requests should be dealt with on a case by case basis. Information in view of a potential coordinated response has to be shared in a timely manner, through the appropriate channels, proportionate to the request, allowing for sufficient decision-making time. Appropriate attention should be given to the origin and classification of information, intelligence and the overall assessment. In addition, continuous exchanges on each other's objectives, criteria, tools and procedures, including as regards attribution, would facilitate the cooperation.

39. Coordination on cyber issues is a key area of EU-NATO cooperation that should be further strengthened in line with the Joint Declarations on EU-NATO cooperation[21]. Such cooperation and coordination is important notably through the exchange of information at technical level and in cases of large-scale cyber-attacks and in the development of sustained, tailored, coherent and coordinated responses to persistent cyber threat actors. While ensuring coherence and complementarity of efforts, to avoid unnecessary duplications, as well as the decision-making autonomy of both organizations, in full respect of the agreed principles of inclusiveness, reciprocity, mutual openness and transparency, the EU and NATO could in particular further strengthen cooperation on 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, as well as to seek potential synergies between the respective crisis management frameworks in the field of cybersecurity, and the protection of critical infrastructure.

[21] Joint Declaration on EU-NATO Cooperation, 10 January 2023 – https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10january-2023/

40. In addition, while recognising that States bear the responsibility to ensure international peace and security, the private sector has a wide range of expertise, knowledge and capabilities to maintain cyberspace global, open, free, stable and secure. The industry has an overview of the most prominent vulnerabilities, threats and activities, to reinforce situational awareness. In addition to the work of ENISA, which is developing channels for exchanging information with private sector providers of managed security solutions and vendors, and complementing the cooperation with the Commission and other relevant EUIBAs, a regular dialogue by the EEAS with the private sector, involving Member States, could support the exchange on relevant cyber diplomacy issues, including situation awareness and information about persistent cyber threat actors. These exchanges could contribute to a further understanding on the cyber threat landscape and effective EU engagement to prevent, discourage, deter and respond to malicious cyber activities. Furthermore, cooperation with academia and non-governmental institutions could also enhance the EU's understanding of the cyber threat landscape, its actors and strategies and policies, which could further inform the development of the EU's approach to diplomatic responses.

10. **EXERCISES**

41. In order to continuously test and improve the cooperation between EU, Member States as well as partners in view of a swift, informed and effective diplomatic response to malicious cyber activities, regular exercises based on the given implementing guidelines will continue to be organised. These exercises can test response to scenarios developed on the basis of regular EU risk assessments. The annual dedicated Cyber Diplomacy Toolbox exercise can continue to be used to test current challenges, and allow for interaction with relevant EUIBAs as well as international partners, including NATO. Moreover, regular exercises in the cyber domain, such, as EU CyCLEs, will contribute to further increasing solidarity and mutual assistance As part of the wider EU's crisis management ecosystem, the Cyber Diplomacy Toolbox will also continue to be part of broader exercises.